2022

DESIGN AND EXPLORATION OF NEW MODELS FOR SECURITY AND PRIVACY-SENSITIVE COLLABORATION SYSTEMS

Ramandeep Kaur Sandhu
Virginia Commonwealth University

DESIGN AND EXPLORATION OF NEW MODELS FOR SECURITY AND PRIVACY-SENSITIVE COLLABORATION SYSTEMS

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University

by

RAMANDEEP KAUR SANDHU

Master of Science in Computer and Information Systems Security
Virginia Commonwealth University, USA, 2017

Master’s in International Business
Aston University, United Kingdom, 2010

Master’s in Economics (Hons)
Guru Nanak Dev University, India, 2006

Bachelor of Economics
Guru Nanak Dev University, India, 2004

Director: KWEKU MUATA OSEI-BRYSON
PROFESSOR, INFORMATION SYSTEMS

Virginia Commonwealth University
Richmond, Virginia
May 2022

ACKNOWLEDGMENT

Firstly, I would like to express many thanks to my esteemed dissertation chair Dr. Kweku Muata Osei-Bryson, who has supported me throughout my PhD program and taught me to believe in myself. I learnt so many remarkable qualities from observing and working with him. I can tell that I am more dedicated and focused because of his guidance.

Second, I would like to thank my wonderful committee members Dr. Manoj Thomas, Dr. Brian Brown, and Dr. Elizabeth Baker. Dr. Manoj’s input helped me find my research topic that has been well received by others. Both as a teacher and co-author, he taught me a great deal about scientific research. He showed me, by his example, what a good researcher should be. Dr. Brian Brown’s advice on my research and my career is invaluable. He not only helped me improve the quality of my dissertation, but also helped me prepare my job market application package. I benefited a lot from his guidance before my job interviews and presentations. I will never stop being grateful for his guidance. Dr. Elizabeth Baker served as my committee member despite her busy schedule. She gave me brilliant comments and suggestions, which I am truly grateful for.

A special thanks goes to Dr. Lemuria Carter, who I truly cherish as my mentor in academia. She encouraged me to pursue a PhD when I was her master’s student. I would also like to thank my OMBA team Dr. Vijay, Austen, Robert, Carol, Ginny, Elaine, Keith, Janae, Joey, Kaitlyn, and Margaret for supporting me throughout my PhD journey.

I must also thank my beautiful niece Gurpreet (Preety), and my friends Josephine, Sama, Mauli, Dila, Saleema, Sona, and Rukman for their thoughts, well wishes, prayers, phone calls, texts, and being there when I needed them. A special thanks to my friends Tiago, Antonio, and Joao on giving me suggestions on how to improve my dissertation.

A special thanks my husband, Sohanpreet Singh Sandhu and my precious son Abiraj Singh Sandhu, who is an amazing boy-I am so blessed to be his mummy, for their endless love, support, and encouragement during my PhD Journey.

I must also thank my mother in law who cooked for me and looked after my husband and son during my busy times. Thank you must go to my parents, siblings, and cousins for the endless love and support they have given me throughout my entire life.

Lastly, I want to dedicate this dissertation to my late father in law, S. Baldev Singh Sandhu, who passed away three days after my dissertation defense. He encouraged me to pursue PhD and supported me both emotionally and financially. I remember calling him and telling him that I passed my dissertation defense. He was extremely happy and proud of me. He will always be my daddy and I will always be his “Beto”.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

RS	Recommender system
BCHIES	Blockchain based collaborative information exchange system
ONC	The office of the national coordinator of health information
DSS	Decision support system
BI/A	Business intelligence and big data analytics
KB-DSS	Knowledge based decision support systems
IOT	Internet of Things
GDSS	Group decision support systems
TOPSIS	The technique for order of preference by similarity to ideal solution
VIKOR	VlseKriterijumska Optimizacija I Kompromisno Resenje,'/multi-criteria optimization and compromise solution
MMG	Multi-microgrid systems
SNSs	Social Networking Sites
PSN	Personal social network.
ASNSs	Academic social networking sites (ASNSs
RBAC	Role based access control
ABAC	Attribute-based access control
CCCSs	Community centered collaborative systems
IIOT	Industrial internet of things
PIM	Privacy and Information Management
OSN	Online social networks
SPIT	Spam over internet telephony
CSDS	Collaborative SPIT detection system
CR	Centralized repository
CV	Curriculum vitae
FHIR	Fast Health Interoperability Resources
HL7	Health seven
PHR	Personal health record
C-CDA	Consolidated clinical document architecture
UTAUT	The unified theory of acceptance and use of technology
DSR	Design Science Research
BSR	Behavioral Science Research
PoF	Proof of Familiarity
BUC	Blockchain Use Cases
IUSR	Utility sensitive customer review analyzer
TPR	True Positive Rate
FPR	False positive rate
ACC	Accuracy rate

CHSS	Central heating system simulation
HEMP	Home energy management products
DRAMS	Decentralized run time access monitoring system
GASD	Genetic algorithm-based signal detection
OLS	Ordinary least squares
ML	Maximum likelihood
HIEs	Health Information Exchanges
OM	Ontology Mapping
EHR	Electronic health record
MMGR	Monitoring Manager
OMT	Ontology Matcher
AES	Advanced encryption standard
NLP	Natural language processing
DPs	Data Properties
wup	Wu and Palmer
lch	Leacock and Chodorow
SSN	Social Security number
MUIPC	Mobile user's information privacy concerns
PAYL	Pay-As-You-Live
CFIP	Consumers' concerns for information privacy
IUIPC	Internet user's information privacy concerns
AIPC	App information privacy concerns
ECT	Expectations confirmation theory
ECM	Expectation confirmation model
GUI	Graphical user Interface
SEM	Structural equation modelling

ABSTRACT

DESIGN AND EXPLORATION OF NEW MODELS FOR SECURITY AND PRIVACY-SENSITIVE COLLABORATION SYSTEMS

By Ramandeep Kaur Sandhu

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at Virginia Commonwealth University
Virginia Commonwealth University, 2022

Major Director: Kweku Muata Osei-Bryson
Professor, Information systems

Collaboration has been an area of interest in many domains including education, research, healthcare supply chain, Internet of things, and music etc. It enhances problem solving through expertise sharing, ideas sharing, learning and resource sharing, and improved decision making.

To address the limitations in the existing literature, this dissertation presents a design science artifact and a conceptual model for collaborative environment. The first artifact is a blockchain based collaborative information exchange system that utilizes blockchain technology and semi-automated ontology mappings to enable secure and interoperable health information exchange among different health care institutions. The conceptual model proposed in this dissertation explores the factors that influences professionals continued use of video-conferencing applications. The conceptual model investigates the role the perceived risks and benefits play in influencing professionals' attitude towards VC apps and consequently its active and automatic use.

CHAPTER 1 INTRODUCTION

This chapter in the dissertation is an introductory chapter that provides an overview of my dissertation topic. In this chapter, I first provide a background on collaboration. In the next section, I describe key drivers of collaborations. Later, I discuss factors inhibiting effective remote collaborations. Next, I present the research questions, followed by the importance and expected contributions from this dissertation. Lastly, I conclude the chapter by outlining the structure of the dissertation.

1.1. BACKGROUND

Assel et al. (2009) defines collaborative working environment as "a collaborative working environment is a temporary coalition of resources, services and people from different organizations allowing the exchange of information and knowledge in order to work together and achieve a shared goal". Collaboration represents working together for a shared goal. Collaboration takes place either in the context of small groups, organizations, or large-scale communities (Grudin & Poltrock, 2012). Collaboration has been an area of interest in many domains including education, research (Logunova et al., 2018), healthcare (Pettigrew et al., 2019), supply chain (Im et al., 2019), internet of things (Tang et al., 2019), music (Calefato et al., 2018), and small, medium, and large sized enterprises (Ali et al., 2020). Collaboration enhances problem solving through expertise sharing, ideas sharing, improved decision making (Safa et al., 2016), learning, and resource sharing (Henningsson & Geschwind, 2019).

Collaborations can either be collocated or remote. Collocated collaboration is a collaboration, where all the collaborators are located in the same physical location (Karis et al., 2016; Praharaj et al., 2018). In remote collaboration, which is the focus of the dissertation, the collaborators are located at separate locations. In remote collaborations, collaborating partners can engage in either synchronous real time communications or asynchronous time delayed communications. Synchronous real time communication represents the communications that take place in real time though not necessarily the same location, with all the parties involved in the communications at the same time. On the contrary, asynchronous communication represents communications that take place when the parties engaged are not communicating simultaneously, which involves the possibility that the sender doesn't receive an instant response from the receiver (Lazou & Tsinakos, 2019). Examples of media that enable synchronous communication include video conferencing, audio-conferencing, and chat messages (Ajabshir, 2019; Huang, 2018). On the other hand, media that enable asynchronous communications include email, voice mail or fax (Ajabshir, 2019; Grudin & Poltrock, 2012). Both synchronous and asynchronous media enable communication and information sharing and make the process of working together and keeping in touch efficient (Karis et al., 2016)

1.2. FACTORS AFFECTING SUSTAINABLE REMOTE COLLABORATIONS

Communication (Neiva et al., 2016) and *information sharing (Panahifar et al., 2018; Xiang & Yuan, 2019)* among collaborating partners are the key drivers of sustainable remote collaboration.

Communication consists mainly of three dimensions: syntax, semantics, and pragmatics. Syntax relates to sign, semantics relate to what the sign refers to, and pragmatics refer to impact of syntax on the interpreter. Ensuring interoperability in these three dimensions is essential to achieve complete, meaningful, and effective remote collaborations (Neiva et al., 2016). However, the use of different languages and different communication standards creates syntactic, semantic (Ali & Chong, 2019; Neiva et al., 2016), and pragmatic interoperability conflicts (Neiva et al., 2016), thereby obstructing effective communications in remote collaboration. *Syntactic interoperability* represents the standardization of communication between sender and receiver i.e., the information systems should follow a common data format and protocol to structure the data. Failure to follow a common data format and protocol to structure the data may result in syntactic interoperability conflict between two information systems (Neiva et al., 2016). *Semantic interoperability* represents the ability of systems and services to exchange data in a meaningful way. In other words, what data refers to is shared in an unambiguous way (Ali & Chong, 2019; Neiva et al., 2016). Distinct illustration and representation of the same information in different information systems leads to differences in semantics (Adel et al., 2019) ultimately restricting compatibility and data comprehension (Sri & Bhaskari, 2020). This could further obstruct the collaborative information systems to automatically interpret the information exchanged without additional effort thereby leading to semantic interoperability conflict. Pragmatic interoperability "is concerned with ensuring that the message sender and receiver share the same expectations about the effect of the exchanged messages and the context where this exchange occurs plays an important role" (Neiva et al., 2016, p. 36). Pragmatic interoperability conflict occurs when the intended effect of the message differs from the actual effect of the message (Pokraev et al., 2005). For instance: Hos A sends DNA sequences to Hos B expecting that Hos B will perform a DNA alignment task using a local alignment method. However, Hos B uses a different alignment method, say global alignment method to perform DNA alignment task, resulting pragmatic interoperability conflict between two collaborators.

Information sharing in remote collaborations represents distribution of information across multiple collaborators through collaborative systems. Contents of information sharing, incentive strategies, professional knowledge, and practical requirements (Xiang & Yuan, 2019), are the factors that impact information sharing. Additionally, the presence of mutual trust among collaborating parties (Scott et al., 2017), systems that enable secure information transmission (Liang et al., 2017), privacy protection (Ulusoy & Yolum, 2019) are essential for sustainable remote collaborations. Lack of mutual trust and security mechanisms (Duong-Trung et al., 2020; Zhang et al., 2018), privacy concerns (Aiken, 2020), use of diverse technologies, languages (Navarrete et al., 2010), communication standards (Ali & Chong, 2019), legislations, different actors and networks involved, different economic, social and cultural conditions (Navarrete et al., 2010) are the additional factors that inhibit information sharing in remote collaborations.

1.3. RESEARCH PROBLEM AND SCOPE

The above discussion concludes that there are several factors that may inhibit communication and information sharing in remote collaborative systems, and consequently hinder its successful adoption and implementation. This dissertation aims to address trust, security, privacy, and semantic interoperability conflict issues in collaborative systems.

First, this dissertation seeks to resolve trust, security, and semantic interoperability issues in remote collaborative systems specifically in the context of healthcare domain in chapter 5. Trust is an essential condition for digital communications and data sharing in the collaborative environment, specifically, the healthcare domain. However, trust is difficult to establish when the data receiving healthcare institutions don’t share the same health system with the shared provider directory or the communications between them are not established yet (Duong-Trung et al., 2020; Zhang et al., 2018). This lack of trust among health care institutions further obstructs the remote health care collaborations.

In addition, lack of highly secure network infrastructure to share data across health institutions virtually (Duong-Trung et al., 2020; Zhang et al., 2018) obstructs the remote healthcare collaborations as virtual environments, where face to face interactions are replaced by virtual network interactions are highly susceptible to medical identity thefts (Zhang et al., 2018). Virtual transmission of patient data without a highly secure network infrastructure in place poses a greater risk for pilfering of patient data (Duong-Trung et al., 2020; Zhang et al., 2018), inflicting severe losses to healthcare institutions including fines, litigations (McLeod & Dolezel, 2018), and loss of public trust (Hasselgren et al., 2020), thereby precluding them from remote collaborations.

Furthermore, different health care institutions store patient records using different standards (Ali & Chong, 2019; Roehrs et al., 2017) in distinct systems (Adel et al., 2019), making it difficult to exchange patient data across healthcare institutions. Moreover, patient data in these sources may be represented using different identifiers/naming conventions (Tanwar et al., 2020) and different units of measurement (Adel et al., 2018). Distinct illustration and representation of the same information in different data sources leads to differences in semantics (Adel et al., 2019), ultimately restricting compatibility and data comprehension (Sri & Bhaskari, 2020). This could further obstruct the healthcare information systems to automatically interpret the information exchanged without additional effort (DeSalvo, 2015)

The heterogeneity in the adoption of standards, systems as well as representation and illustrations of patient data leads to uninterpretable healthcare information systems (Adel et al., 2018; Dridi et al., 2020; Satti et al., 2020), thereby making the health data become data silos and only accessible and usable in their respective places with little or no interoperability with others (Peng & Goswami, 2019; Roehrs et al., 2017). With the patient data spread across different healthcare providers and the need for up to date and comprehensive patient information for the healthcare providers to provide better patient care (Zhang et al., 2018), it is important to design a system that enables healthcare institutions to securely share patient information in a virtual environment.

Second aspect of this dissertation aims to explore collaborating individuals' intentions to use collaborative systems, specifically video conferencing applications despite the privacy risks associated with its usage in Chapter 6. Video conferencing applications offers numerous benefits enabling convenient way for individuals to communicate and collaborate (Adom, 2020; Hakim, 2020; Kumar, 2020). However, they also suffer from serious privacy violations that range from theft of personal and financial information to loss of intellectual property, productivity, and reputation (Ahmad, 2020). These violations make the users' fear that their personal information may be at risk (Neustaedter et al., 2018) and their personal information may be shared with third parties without their consent (Aiken, 2020). Despite the privacy risks and concerns associated with its usage, VC apps are surging in popularity as individuals' use of VC apps for work and professional settings has increased substantially (Aiken, 2020). This type of behavior is referred to as a privacy paradox, where contrary to their concerns about privacy infringements, individuals' are still willing to disclose their personal information to online retailers, as long as they have something in return (Kokolakis, 2017). Specifically, individuals engage in risk-benefit evaluations referred to as privacy calculus of information disclosure (Dinev & Hart, 2006). The outcome of such evaluation is perceived value, which, when positive, will favor adoption of a technology, when negative, will result in rejection of a technology (Morosan & DeFranco, 2015; Shaw & Sergueeva, 2019; Wiegard & Breitner, 2019; Xu et al., 2011). With society being pushed towards a new virtual world during pandemic

(Kagan et al., 2020) and the prediction that that widespread adoption of remote work will continue to hold even after pandemic (Russell & Frachtenberg, 2021), it is important to understand, what trade-offs individuals are willing to make in the aspect of information privacy concerns associated with the usage of video conferencing applications.

1.4 RESEARCH OBJECTIVES AND QUESTIONS

Considering the above issues, the objective of this dissertation is to (1) develop a new virtual collaborative system that addresses the deficiencies in the existing collaborative systems and enable secure and interoperable exchange of patient data across different healthcare institutions (2) investigate the attitude of professionals in the calculus of decisions to continue VC apps usage in work related settings (3) investigate the extent to which professionals attitude influence active (lean and rich usage) and automatic (intentions to continue) use of VC apps

Hence, this dissertation is guided by the following research questions:

1. How may a system be designed to enable secure and interoperable exchange of EHR across healthcare institutions in a situation where, (a) healthcare institutions know each other, but don't fully trust each other, and (b) are storing and representing the same health information using distinct protocols and naming conventions?
2. What role do the contrary beliefs (perceived risks and benefits) play in influencing professionals' attitude towards VC apps and consequently its active and automatic use?

1.5 SIGNIFICANCE OF THE RESEARCH

Patients' visit various healthcare providers during their lifetime (Zhang et al., 2018). This results in individual patient's records scattered across several healthcare providers with no specific reference for a complete and up to date database (Al-Karaki et al., 2019). In order to enable better patient care, these healthcare providers should be able to exchange their patient information in a secure and timely manner to ensure the availability of most up to date information about their patients' health conditions (Zhang et al., 2018). Without a highly secure virtual infrastructure and interoperable healthcare information systems, cross-institutional data sharing will be obstructed (Zhang et al., 2018), thereby making the patient data inaccessible when needed (Al-Karaki et al., 2019). To promote secure and interoperable exchange of patient data, the Office of the National Coordinator of Health Information has called for efficient solutions that advance security and interoperability in healthcare collaboration (DeSalvo, 2015). These solutions will not only enable healthcare providers to have comprehensive and timely overview of patients' health (Peng & Goswami, 2019), but also enable efficient and coordinated delivery of care as well as cost savings through reduced manual errors (Jabbar et al., 2020) and duplicative tests respectively (Jabbar et al., 2020; Payne et al., 2019).

Several recent solutions claimed the importance of integrating blockchain with the health information exchange management (Dwivedi et al., 2019; Hylock & Zeng, 2019; Ivan, 2016; Kaur et al., 2018; Wang et al., 2018; Yang & Yang, 2017; Zhang et al., 2018). The literature review revealed that the prior blockchain based solutions rely on enforcement of one specific standard e.g., Fast healthcare interoperability resource aka FHIR to address the trust, security, and semantic interoperability issue in healthcare. These approaches may perform well for the information systems built using that specific standard but may be compatible for the information systems not supporting that specific standard (e.g., information systems built on other standards such as HL7 v2). The fact that no single standard is capable enough to support all the needs of the healthcare organizations and each standard offers variety of distinct features which makes it more or less appealing to healthcare based on their needs (Lyniate, 2019), the prior solutions that rely on normalizing heterogeneous databases through enforcement of one specific standards may not be adopted. Hence, there is a need of a network infrastructure that offers a secure and interoperable exchange of patient health records, in a situation where communications between healthcare institutions have not been established and the healthcare institutions are using distinct protocols (i.e., distinct standards and systems) and naming conventions to store and represent patient data.

Chapter 4 in this dissertation will present a novel system that integrates blockchain and semi-ontology mapping techniques. It addresses many limitations in the existing blockchain based collaborative systems. The significance of this research is twofold. From an academic perspective, this dissertation research will contribute to the IS knowledge base by presenting an artifact that bridges the gap in the current literature. Additional contributions would include as the first attempt to integrate semi-ontology mapping into blockchain technology. Becoming a starting point for the studies that focus on interoperability and security issues, this study paves a new road for the researchers to resolve security and interoperability in other domains by integrating blockchain and ontology mapping techniques. From a practical perspective, this dissertation research contributes to the practices in cross-institutional health information exchange by providing a useful reference on using new features of blockchain technology to solve the weaknesses of traditional health information exchange where patient records are faxed to other health care institutions, thereby improving and simplifying the sharing of electronic health records.

Collaborative tools such as video conferencing represents a unique environment in which its usage and ultimately disclosure of the personal information could be rewarding, but at the same time risky, it becomes crucial to understand how these contrary beliefs (perceived benefits and risks) play a role in shaping individuals attitude and attitude towards VC apps in professional and work related settings. As the organizations move towards a remote working environment, collaborative tools specifically the use of VC apps is predicted to continue to hold post- pandemic. Hence, understanding what drives professionals use of VC apps is not only timely and applicable to COVID-19 pandemic, but also relevant and current as use of VC apps is likely to stay during post pandemic even after professionals start returning back to their offices.

While there has been a plethora of research on VC, to date, what drives VC apps continued use at individual level despite the privacy risks associated with its use remains unknown. Prior research that empirically studied VC apps as a part of collaborative technologies or social media technologies (see Table 3 in Appendix) don't consider the influence of privacy risks and concerns on professionals' use of VC apps, thus making a crucial gap in the literature.

While there has been a plethora of research on VC, to date, what drives VC apps active use (lean and rich use) at individual level remains unknown. Prior research that empirically studied VC apps as a part of collaborative technologies or social media technologies (see Table 3 in Appendix) do not consider the influence of privacy risks and concerns on professionals' active and automatic use of VC apps, thereby making a crucial gap in the literature.

The findings of the chapter 5 in this dissertation will deepen our understanding of the extent to which both socially derived and technological characteristics of VC apps serve as the predictors of professionals' attitude towards VC apps. Researchers may find the conceptual model presented in this study being applicable to other surveillance-based technologies such as internet of Things, smart badges etc. By adopting the privacy calculus, MUIPC, ubiquity, and social presence theory in the context of video-conferencing apps and explain individuals' continuance usage behavior, this study furthers the generalizability of privacy calculus, MUIPC, Ubiquity, and social presence theory to a different context and advances the knowledge base that is a critical step to advance a theory. The rich understanding gained from the findings of the study can assist organizations in the communication technology industry better design such means of communications. The findings of the study can guide the practitioners to understand the key factors that are pivotal for design and development of VC apps that suit the needs of the remotely working professionals. VC apps developers can thus make targeted updates to their system without refurbishing the entire system to achieve higher consumer acceptance and higher rates of continued usage. The designers and developers of VC apps can use the findings to develop VC apps that are secure and preserve the privacy of those who seek to use VC apps in the professional settings.

1.6 OUTLINE

The organization of the dissertation is as follows. Chapter 2 provides a literature review of related research and the gaps in the previous literature. Chapter 3 presents an overview of different methodologies relevant to this research. Chapter 4 represents the new artifact designed to resolve security, trust, and interoperability issues in health care collaborations. Chapter 5 represents a conceptual model designed to investigate the continued use of video-conferencing apps in the professional settings. Chapter 6 concludes with the dissertation with the discussion of contributions, limitations and directions for the future research.

CHAPTER 2 LITERATURE REVIEW

In this chapter, I first provide some background on collaborative systems and types of collaborative tools. Later, I discuss security, privacy as well as the relationship between them. Lastly, I present an overview of studies that focus on collaboration systems and security, collaboration systems and interoperability, and collaboration systems and privacy. I look at these studies in greater depth to provide an overview of research issues and identify research gaps.

2.1. SYSTEMS AND TOOLS IN A COLLABORATIVE ENVIRONMENT

Collaborative systems enable users to communicate and collaborate in common tasks (Tolone et al., 2005). Examples of such systems include: asynchronous collaboration tools such as collaborative document sharing/editing systems, synchronous collaboration tools such as audio/video conferencing systems, workflow management systems, distance learning systems (Tolone et al., 2005), decision support systems (Arnott & Pervan, 2015), recommender systems, social networking systems (McDonald, 2003), and blockchain (Hull et al., 2016) etc. The decision support systems are further categorized into three collaboration systems: 1) Knowledge based decision support systems, 2) real-time decision support systems, and 3) group decision support systems. The following section provides a detailed description of all the collaboration systems mentioned above.

2.1.1 Decision Support Systems

Decision support system (DSS) is a system that supports and improves managerial decision making. The term decision support systems first appeared in an article by Garry and Scott, 1971, where the authors envisaged DSS as a system that supports any semi-structured and structured managerial activities in decision making (Arnott & Pervan, 2015). (Eom et al.,

1998) defined DSS as the one that supports decision makers rather than substitute them, uses data models, solves both structured and unstructured problems, and emphasizes effectiveness rather than efficiency (Eom et al., 1998).

There are three technology levels that can be incorporated in the label "decision support system": specific DSS, DSS generator, and DSS tools. Since, decision support systems are utilized by individuals with distinct levels of technical capabilities, they differ in the nature and scope of tasks for which they are utilized. The system which actually executes the work might be called the specific DSS. It is hardware/software that enables specific decision makers or groups of decision makers to manage specific sets of related problems. DSS generator represents the hardware/software that "provides a set of capabilities to quickly and easily build a specific DSS" (Sprague Jr, 1980, p. 6). The hardware/software that facilitates the development of specific DSS or DSS generators is referred to as DSS tools.

In addition, there are five roles that are spread across three levels of technology described above. The first role involves the manager or the user who faces the problem, makes decisions, takes actions, and is responsible for the consequences. The second role is of the intermediary. Intermediary is the individual who helps the manager/user and acts as a staff assistant to interact and make suggestions. The third role is of the DSS builder aka facilitator. DSS builder is responsible for assembling vital capabilities from the DSS generator to design the specific DSS generator with which the user or the intermediary interacts directly. The fourth role is of technical support who expands components capabilities when they are required as part of the generator. The last role is of toolsmith. Toolsmith in an individual that develops new hardware/software, new technology, new languages etc. Each individual can have more than one role. Out of five roles, the user/manager plays a more active and authoritative role in the development of the system (Sprague Jr, 1980).

Watson (2018) notes that Sprague's DSS development framework remains valid in today's world of business intelligence and big data analytics BI/A. Watson further discusses how BI/A satisfies Sprague' DSS characteristics in today's world. BI/A focuses on all the problems whether structured, semi-structured, or unstructured. They support both independent and dependent decision making and support all phases of decision-making as well as provide group support often known as collaborative, groupware software or collaboration systems. For instance, a software called slack provides group support by allowing the teams to send real time messages, have voice or video calls, store files, screen sharing, rate files using stars, or receive notifications. BI/A have features that make the system faster and easier to use by the non-technical individuals in an interactive way. Today's DSS are flexible and adaptive to the changing environment and the decision approach of the users. They widely recognize agile development methodologies such as scrum, Kanban, XP as the means to develop decision support applications (Watson, 2018). Watson further discusses salient themes or developments that the next generation DSS would have: DSS would involve widespread use of natural language processing languages, it will continue to move to cloud, will greatly use the sensors, IOT and streaming of data, would involve different types of data scientists, and would involve the greater monetization of data (Watson, 2018).

DSS aims to support the automation of decision-making processes (Eibl & Höchtl, 2019). DSS, a part of the information system, supports and improves managerial decision making. The article by Eibl and Höchtl (2019) discusses how officials in the city of Vienna use fuzzy cognitive maps in DSS. Fuzzy cognitive maps are fuzzy graph structures that represent causal reasoning

(Eibl & Höchtl, 2019). In addition, the use of DSS has also been extended to resolve problems such as: climate changes, poverty, general policy development, and business strategy. The most commonly addressed problems by DSS includes business, organizational and strategic decisions (Pretorius, 2017). For instance, A study by Koornneef et al. (2019) developed a mobile DSS to assist in minimizing flight disruptions by providing direct decision support for operational processes involving shorter time spans, by automatically collecting and processing appropriate data from multiple sources, and providing onsite ranked dispatch alternatives to aircraft maintenance technicians through a mobile tool (Koornneef et al., 2019).

Currently, there are various companies that offer decision support products. The key vendors of DSS products in today's environment are IBM, Microsoft and Oracle. These vendors offer a complete BI/A stack that encompasses database, data warehousing, data integration, data access and data analysis tools (Watson, 2018). While discussing the users of DSS in the current era, Watson (2018) categorized users into two categories: internal users and external users. Internal users include casual users as well as data scientists. External users who use DSS are web-developers who include a recommendation engine in organizations'-commercial website, customers and suppliers who access information and systems (Watson, 2018). Eom et al. (1998) further listed three types of decision support systems including: Knowledge based decision support systems, real-time decision support systems, and group decision support systems. The detailed description of each category is provided in the subsequent sections:

2.1.1.1 Knowledge based Decision Support Systems

Knowledge based decision support systems (KB-DSS) incorporate domain knowledge, modelling and analysis to provide users with the competence of intelligence assistance. These systems utilize knowledge-based modules to formulate problems and decision models as well as analyze and interpret the results. Managerial judgements are utilized to discern future uncertainty as well as choose assumptions on which decision models can be made. Decisions can be both knowledge and data intensive. Therefore, a large volume of data usually requires substantial effort for their interpretations and use. Knowledge based tools assist in interpreting these data to identify the source of unsatisfactory results in the manufacturing process (Eom et al., 1998).

DSS might be able to facilitate autonomy of citizens when making choices for their health options. It may also enable professionals to make appropriate decisions at the right moment. It may also assist the policy makers and managers in prioritizing the most required actions in an environment with ever increasing resource constraints and health requirements. But this may not be possible without maintaining the repositories of normalized and dissociated healthcare data from the daily healthcare practice, the contributions of the patients themselves and the open access data of the social environment. Hence, application of KB-DSS in the healthcare domain can provide a wide range of information. One of the uses of KB-DSS is that it can identify situations that were thought to be good but were not explicitly stated by physicians while utilizing the systems. Other uses can include discovering the mistakes committed frequently by professionals when compared to evidence-based guidelines (González-Ferrer et al., 2018).

KB-DSS incorporate data analysis and data mining techniques to assist business in real world. A DSS built by Kukar et al. (2019) is an example of this. Kukar et al. (2019) developed a novel system called AgroDSS that bridges the gap between state of art of DSS methodology and agricultural systems. AgroDSS provides computer assisted decision support to farmers. While using the system, farmers can upload their own data of interest and use several available data mining or statistical analysis tools and get the outputs. These automated decisions support the farmers with decision making, better understanding of the submitted data and explanation of the dependency with the data, and predictions for simulated scenarios (Kukar et al., 2019).

Müller et al. (2018) developed a knowledge-based decision support system to support flexible and scalable production of micro-products. An expert knowledge database acts as a smart optimization tool to reduce human errors in the process planning and to establish maximum resource exploitations. The proposed KBDSS recommends the best possible process chain alternatives and provides automatic reliable outputs to the production systems. This further accelerates the manufacturing platform set up times without requiring expensive investment in new resources (Müller et al., 2018).

2.1.1.2. Real time Decision Support Systems

Real time decision support systems utilize modern technologies related to data acquisition, data processing, and visualization for improving decision making (Zografos et al., 2002)

The improved computer hardware and mathematical programming packages as well as the techniques such as machine learning, core-based reasoning and reasoning led to the emergence of real time decision support systems. These systems utilize the ever-increasing computing power to resolve large scale optimization models in a fraction of second. Real time decision support systems may utilize machine learning approaches, core-based reasoning to obtain knowledge from prior data, decisions, and previous cases to support complex real time decision making (Eom et al., 1998).

Advancements in technology have enabled real time data collection from production tools that can communicate with each other through the Internet of things. Real time data collection enhances production control especially in dynamic production environments (Turker et al., 2019).

The DSS proposed by Turker et al. (2019) is a real time DSS that uses real time data to enhance the performance of dispatching rules in dynamic scheduling and therefore enhances the overall performance of job-shop. When the number of jobs waiting in the queue of any workstations falls lower than the critical value, DSS alters the scheduling order for the preceding workstations to feed the workstation as quickly as possible. For this, it finds the jobs in the preceding workstation to be fed into the current workstations and then identifies the job with high priority number according to dispatching rule and lastly places this job in the first position (Turker et al., 2019).

Similarly, Abdel-Basset et al. (2019) proposed an IOT system based DSS that detects and monitors type 2 diabetes patients in real time. The proposed system uses wireless body area networks (WBAN) and mobile application interfaces to capture the changes and social exchanges in users' bodies. After collecting users' personal data and symptoms, the system categorizes users into uninfected people or type 2 diabetes patients (Abdel-Basset et al., 2019).

2.1.1.3. Group Decision Support Systems (GDSS)

Group decision support systems (GDSS) is a decision support system for groups that combine computing, communications, and decision support systems to facilitate formulation and solutions of unstructured problems in group meetings. GDSS assists a decision-making group (DeSanctis & Gallupe, 1987) by facilitating knowledge acquisition from multiple experts (Eom et al., 1998).

A decision-making group is a group of two or more individuals who are collectively responsible for problem detection, nature of problem elaboration, generation and evaluations of problem solutions or formulate strategies for implementing solutions and implementing the group's decision. A group decision occurs as a result of exchange of information between the group members (DeSanctis & Gallupe, 1987). "The group's approach to making a decision is exhibited in their patterns of interpersonal communications. More specifically, the decision process is revealed in the production and reproduction of positions regarding group's actions, which are directed toward the convergence of members on the final choice" (DeSanctis & Gallupe, 1987)(p.591). Personal and/or opinion exploration, expressions of opinions, argumentation, information seeking, socializing, proposal development are some of the activities exhibited during group decision making. The main goal of GDSS is to change the communication process within the groups. The higher the degree of change brought by GDSS, the higher the impact on the decision process, and presumably, on the decision outcomes (DeSanctis & Gallupe, 1987).

GDSS can be of three types: Level 1 GDSS support group decisions by removing communication barriers such as providing a large common screen to display group ideas instantly, anonymous inputs of ideas and preferences, voting solutions and elicitations, and electronic exchange of messages between group members. Level 2 GDSS support groups' decision by providing automated tools or other aids for group members to work on and view synchronously, using a bigger common screen. Modelling tools such as multi-attribute utility methods, risk analysis, or social judgement formation tools can be introduced in level 2 GDSSS. Level 3, GDSS support decision process can include expert advice in selecting and arranging rules that can be applied during a group meeting. Computer mediated communication system that actively filter and structure information exchange is an illustration of level 3 GDSS (DeSanctis & Gallupe, 1987).

In today's world, the success and survival of any organization depends upon the quality of decisions made. Most of the decisions made in an organization are still made in groups. But with the emergence of global markets, we find that the decision makers are spread across the globe. Due to the fact that the decision makers are dispersed across the globe, in the countries with different time zones, there is a shift from traditional GDSS to web based GDSS. Web-based GDSS assist decision makers at anytime and anywhere (Carneiro et al., 2019). The authors developed a web-based GDSS that allows the automatic assessment of decision makers' satisfaction in a meeting supported by the web-based GDSS (Carneiro et al., 2019).

The technique for order of preference by similarity to ideal solution (TOPSIS) and VlseKriterijumska Optimizacija I Kompromisno Resenje,' meaning multi-criteria optimization and compromise solution (VIKOR) are two popular multiple attribute decision making methods. Many extensions of these techniques have been proposed in the past that either use different techniques to rank the alternatives or use fuzzy logic to handle logic or criteria that are incomplete/an or unquantifiable (Ploskas & Papathanasiou, 2019). Ploskas and Papathanasiou (2019) used TOPSIS and VIKOR to develop a web based GDSS that helps decision makers to compare and contrast various alternatives solutions and understand how vigorous a decision can be (Ploskas & Papathanasiou, 2019).

In addition, because of the complexity and uncertainty of the real decision-making process and fuzziness of human thinking, the decision makers can't always provide the information in quantitative form. They sometimes have to use the linguistic terms to provide the assessments. They can't always use one linguistic term to provide the assessments. Due to lack of sufficient knowledge and fuzziness of human thinking, groups decision makers can use accrue linguistic terms as the assessment information. These uncertain linguistic terms are different from each other (Lin et al., 2017). To resolve this problem, Lin et al. (2017) proposed a new concept called probabilistic uncertain linguistic term sets that extends the existing probabilistic linguistic term sets. The proposed method also discusses how the normalization process, comparison method, basic operators and aggregation operators will be used in the probabilistic uncertain linguistic term sets (Lin et al., 2017).

2.1.2 Recommender Systems

Recommender system (RS) is a web-based tool designed to recommend vendor products and services which might be of interest to a specific customer. The objective of RS is to help individuals find desirable information and objects through the use of inference and prediction (Oard & Kim, 1998). Recommender systems have been used in various contexts such as e-business, e-commerce, e-library, e-learning, e-government, e-tourism, e-resources (Lu et al., 2015), and potential collaborator identification (Kong et al., 2016), research articles identification (Knoth et al., 2017).

To provide recommendations, RS first elicits and collects user information explicitly or implicitly from the users. Explicit user information collection means that the users themselves provide substantive information about their habits, preferences for certain items, their name, zip code, location etc. Based on this information, recommender systems build user profiles to deliver recommendations by utilizing matchmaking approaches (Li & Karahanna, 2015). There are different types of recommender systems such as content-based recommender systems, collaborative recommender systems, demographic based recommender systems, utility-based recommender systems, and knowledge-based recommender systems. The recommender systems that apply to our research include collaborative recommender systems and knowledge-based recommender systems. Below is the detailed description of collaborative recommender systems and knowledge-based recommender systems

2.1.2.1. Collaborative filtering-based Recommender Systems

Collaborative filtering-based recommender system is the most widely adopted recommender system in academia and industry (Kim & Chen, 2015). Collaborative filtering-based RS requires ratings for an item to provide recommendations for it (Schafer et al., 2007). The recommendations are based on opinions/ratings of other individuals who share similar interests (Lu et al., 2015). Collaborative systems are based on the assumptions that individuals with similar tastes and preferences rate items similarly. Traditional collaborative systems use two key approaches to predict ratings and generate recommendations: user based collaborative filtering and item-based collaborative filtering. User based collaborative filtering approach assumes that users with similar historical ratings share similar interests. Hence, an active user's missing ratings for a specific item are predicted based on similar user's ratings on that specific item. In this approach, first the similarity between an active user and other users is calculated. Then, the neighbors with the closest similarity to the active user are selected as the nearest neighbors. Later, the historical ratings from the nearest neighbors are used to predict the ratings and provide top recommendations for an active user (Chen et al., 2018). In an item-based approach, the ratings are also predicted in the similar three steps: calculate similarity between items, find the nearest neighbors and predict the ratings. In this approach, predictions are based on item similarity, rather than user similarity (Chen & Yao, 2018).

2.1.2.2. Knowledge based Recommender Systems

Knowledge based recommender systems (KB-RSS) work on functional knowledge. These RS have knowledge about how a specific item meets a specific user need and consequently can explain the relationship between user needs and the possible recommendations (Friedrich & Zanker, 2011). KB-DSS have explicit knowledge about user's ratings, item assortments, preferences, recommendations contexts. The individuals specify their preferences explicitly in the form of user constraints such as: price, quality, location etc. KB-RSS takes into account these constraints and provides recommendations based on these constraints. The major strength of knowledge-based recommender systems is that there is no cold start problem. Cold start problem represents the situation where the system can't generate inferences for the items or users about which sufficient data is not available. The item domain relevant for knowledge recommendations systems include tourism destinations, electronic purchases, financial services etc.

Ontology based recommenders' systems also known as KB-RSS uses ontologies to represent knowledge about products/items, users in the recommendation process. In e-learning environments ontology-based recommender systems use ontology knowledge about the e-learners as well the e-learning resources in providing recommendations about the learning resources. Ontologies play a crucial role in representing knowledge and knowledge sharing as well as reusing the knowledge representations in recommender systems. Aggregation of ontology domain knowledge about learners and the learning process enhances the accuracy and quality of recommendations (Tarus et al., 2018).

Obeid et al. (2018) proposed an ontology-based recommender system that integrates semantic based methods and machine learning methods to enhance recommendation processes. The proposed RS recommends course majors and universities to high school students by collecting data related to their interest during high school as well as their domain they are actually working in (Obeid et al., 2018).

Thanapalasingam et al. (2018) developed a smart book recommender system, an ontology-based RS that assists computer science editorial teams in deciding which products to market at specific venues. The proposed RS recommended books, journals, and conference proceedings based on semantically enhanced representation of 27K editorial products. It takes the conference series as an input and returns a list of editorial products that might be of interest to conference attendees. For instance, given a conference series of “DSRIT”, SBR will return a list of books, journals, and conference proceedings that are characterized by a set of research topics similar to one of DSRIT (Thanapalasingam et al., 2018).

Subramaniyaswamy et al. (2019) developed a health centric RS called ProTrip RS that exploits users interests and preferences to provide recommendations. It supports travelers with a strict diet and/or having long term diseases. Pro-tip uses am ontological knowledge base and tailored filtering mechanisms to provide food recommendations. Semantic ontologies are used to bridge the gap between heterogeneous user profiles and descriptions (Subramaniyaswamy et al., 2019).

2.1.3 Blockchain

Blockchain, originally designed for keeping the financial ledger (Azaria et al., 2016), is a distributed tamper-proof database (Brodersen et al., 2016) that supports secure and trustless transactions different nodes participating on the blockchain network (Nakamoto, 2008).

Blockchain is a decentralized database that comprises blocks and batches of approved transactions grouped together to form a block (Scott et al., 2017). Blockchain involves two classes of logical computational actors: peers and participants. Peers refers to computational actors that work together to support a given blockchain deployment as well as form a blockchain network. Participants represent the businesses/organizations that are collaborators with each other on the blockchain network (Hull et al., 2016). Blockchain enables participants to access records of every transaction they make, as the transaction history gets stored on every peer node on the blockchain network (Sun et al., 2016).

Transactions in blockchain include the details about the transaction as well as the time stamp. Transactions as well as time stamps can be represented in numerical or string form. Transactions can include transaction time stamps, transaction details such as value or money exchanged between the two parties, hash of the current transaction and hash of previous transaction. When a new record is inserted into the blockchain, the last computed hash is broadcasted to all the peers on the network. Since all peers on the network have the copies of the hash, anyone on the network can verify that the transaction/data is not altered (Di Pierro, 2017).

Blockchain transactions are recorded using public and private keys enabling the participants to remain anonymous, while still allowing the peers to verify their identity (Sun et al., 2016). Since mutual trust is crucial for the successful collaborations (Meng et al., 2018), blockchain technology establishes this mutual trust through encryption, consensus, and other algorithms (Hull et al., 2016). In blockchain, trust is not placed on a central authority rather it is distributed across the entire population of peers. The use of a central authority gets replaced by a community of peers and no one can independently take actions on behalf of the community. Community of peers can't agree on changes without consensus (Sun et al., 2016). Blockchain also ensures transparency, traceability, immutability, and verifiability of information shared across collaboration parties (Mattila et al., 2016).

The benefits of disintermediation, traceability and immutability provide multi-fold opportunities to the business process to attain digitation, automation, and transparency in the collaboration process (Da Xu & Viriyasitavat, 2019).

Blockchain and smart contracts are two key concepts that enable trust of entities involved in business collaborations. The ledger in blockchain is auditable as they contain blocks that are linked together and maintained by every node on the network (Da Xu & Viriyasitavat, 2019).

Blockchain enables collaboration amongst business organizations involving mutually untrusted parties (López-Pintado et al., 2019). Blockchain promotes trust of process execution through consensus process allowing mutually untrusted and uncoordinated parties to agree on transactions and blocks in the network on which the blockchain is operating (Da Xu & Viriyasitavat, 2019).

Blockchain also deploys smart contracts, which are invoked through transactions. A smart contract is a self-executing contract that verifies or enforces the negotiation of a contract in real time. In Ethereum blockchain, the smart contracts are written in solidity language, which then executes on Ethereum virtual machine. Each transaction requires an Ethereum gas to take place. A gas is a unit that measures the computational effort required to carry out a transaction (López-Pintado et al., 2019).

Blockchain has enabled multi-fold opportunities to redesign collaborations in a vast range of fields including healthcare, supply chain, logistics, service agreements etc. Most importantly, it has enabled sufficient gains in terms of cost and time it takes set up and carry out the collaborative business processes, specifically where there is lack of trust between collaborators In addition, blockchain has also enabled fine grained access control mechanisms, thus allowing collaborating parties to selectively share their data amongst each other and to selectively accord permissions for performing transactions on their shared data (Dumas et al., 2019).

Hu et al. (2019) proposed a new collaborative intrusion detection system that utilizes blockchain technology to ensure the security of Multi-microgrid systems (MMG). Based on the blockchain approach, MMG is designed without the requirement of a trusted party. MMG is equipped with a proposed generation method that integrates periodic and trigger patterns to generate intrusion detection target of collaborative intrusion detection i.e., a proposal. Together with correlational models of MMGs, and generated proposals, collaborative intrusion detection is achieved by using the consensus mechanisms. The resulting detection outputs of collaborative intrusion detection are then stored in a sequence on the blockchain (Hu et al., 2019).

2.1.4 Social Networking Systems

Social networks represent a group of individuals as well as relationships among them. Social network systems can be utilized in two ways: as a visualization tool to provide an overview of group membership or group participation and as a mechanism to recommend specific people for collaboration (McDonald, 2003).

In the case of recommending specific people for collaboration, social network systems find the co-authorship and co-citation relationships to build a social network and utilize the resulting visualization to identify possible experts. Some social network systems enable query answering about how far the researchers are from one another and who is between (McDonald, 2003). Social network systems are at least as crucial as “the official organizational structures for tasks ranging from immediate, local problem solving (e.g., fixing a piece of equipment), to primary work functions, such as creating collaborative groups” (Ogata et al., 2001) (p.1). There are two approaches to obtain social networks: socio-centric approach and ego-centric approach. In a socio-centric approach, a whole network (i.e., which is based on some specific criteria of population boundaries) is considered. The whole network explains the ties that the members maintain with all the other members in that specific group. In ego-centric approach, only the relations reported by a local individual are considered. Ego-centric approach is utilized when the population is huge (Ogata et al., 2001).

Chuan et al. (2018) proposed a new measure for link prediction in a co-authorship network. The authors extended the weighted common neighbors metric with similarities among papers of co-authors, among papers of them and among co-authors. The new weighted metric is based on the assumption that higher similarity between two sets of papers is, higher possibility of the link in the future is. The proposed weighted metric is then combined with link prediction to provide better collaborators predictions (Chuan et al., 2018).

Cho and Yu (2018) proposed a new link prediction methodology to identify potential inter-disciplinary collaborations in a university wide collaboration network. The proposed methodology assists the decision makers in introducing or evaluating calls for interdisciplinary research. The authors proposed two methods for assigning similarity scores to individuals: the similarity scores based on co-authorship network and similarity score based on bipartite network. The similarity score based on co-authorship states that if two individuals have collaborated with the same third individual, it is likely that they will collaborate with each other, if they have not done so. It assigns positive weights to individuals who don’t have direct collaboration with each other but have at least one common author. Similarity scores based on bipartite networks is based on the assumption that when the researchers from different organizations have published in the same journals but have not collaborated with each other yet, it shows that they have the potential to collaborate with each other.

Tsai et al. (2019) developed a user-controlled hybrid recommender system for academic conferences. The system recommends potential collaborators as well as the list of articles to the conference attendees. To recommend potential collaborators, the authors used publication similarity between two attendees, similarity between publications of the topics, co-authorship similarity, co-bookmarked papers, co-interest similarity, and geographical distance. The article recommendations were based on publication similarity, bookmark similarity, followee similarity (i.e. they are following the same individual), publication popularity, and author popularity

Yan and Cui (2019) proposed a system that enables the researchers to grow their social network to an expected direction. The proposed system allowed the researchers to visually compare the effects of adding recommended users to his/her personal social network. The user can provide a description of the expectations of the PSN. For instance, he/she can describe that 50 percent of his friends should have a tag machine of machine learning, 30 percent should have a graphics researcher, 20 percent should have blockchain tags. Since, a user can be provided with the list of users to be added to his network and can add multiple users, the proposed system provides a representation of direct effects of adding a user and whether his PSN expectations are met or not (Yan & Cui, 2019).

2.1.5 Social Networking Sites

Social networking sites (SNSs) are the web-based tools that enable users to create a public or private profile within certain systems, articulate a list of users with whom they have a connection as well as see their list of connections and of others within the bounded system (Boyd & Ellison, 2007).

Some social networking sites aim at assisting academia. They assist academics by sharing research articles, tracking citations and collaborating with peers. Researchers use different kinds of social networking sites like Facebook, Google +, MySpace etc, Mendley, Research Gate, Academia.edu, CiteLike or Zotero etc. in academia for professional purposes (Greifeneder et al., 2018).

Social networking sites (SNSs) enable information management, identity and network management, and communication with peers, thus turning social networking systems into a useful tool to support collaboration. In case of information management, SNSs allows individuals to manage their data efficiently. With respect to identify and network management, SNSs facilitate personal contact management and enable self -presentation by allowing the individuals to exhibit their competencies in certain research methods or display their publication. The instant messaging tools built into the social networking sites provides a mechanism for the users to communicate with the users whom they share similar interests (Bullinger et al., 2010).

SNSs play a significant role in enhancing a student's social presence, their well-being and learning performance. SNSs enhances collaborations amongst students. It allows students to reinforce distant relationships. The potential design enhancements of social networking sites foster communications amongst students and hence improve their interactions. Social networking sites enhance students' social presence through the form of web-communities within the environment of social networking sites (Samad et al., 2019).

Social networking sites transform how organizations cooperate, communicate, and connect with the key stakeholders. Social networking sites enable the individuals to reach individuals where they are, engage actively in socializing, getting updates and sharing opinions. Social networking sites have the potential to break silos and enhance productivity, thus enhancing collaborations. Instant access to experts, reduced cost to travel, communication, and marketing are some of the major benefits listed by organizational experts in using social networking sites in a collaborative environment (Stanko & Sena, 2019).

A qualitative study conducted by Jordan and Weller (2018) listed various benefits and problems of using social networking sites in academia. The benefits of using SNSs in academia include access to the directory of academics, identification of information and papers, identification of potential collaborators, improvement in scientific process, raise of own profile, support multiple profiles, recruitment and opportunities. The problems associated with the use of SNSs include the concerns about commercialism, digital inclusion and literacy issues, privacy and security concerns, social aversion, unreliable information (Jordan & Weller, 2018).

Academic social networking sites (ASNSs) are the sites that allow the researchers to create public or semi-public profiles in the systems and receive recommendations (research materials) that are relevant to their preferences. Research gate, Academia.edu, Mendeley are few examples of ASNSs. ASNSs allows two or more groups of researchers to work together in a collaborative manner. ASNSs facilitates communication by providing the users a list of researchers in connection. Different factors impact researchers' intentions to use ASNSs including communication benefits, perceived security, perceived privacy, effort expectancy, social influence, facilitating conditions (Salahshour Rad et al., 2019).

2.2 SECURITY IN COLLABORATIVE ENVIRONMENT

Collaborative environments has its own specifics such as: (1) It constitutes an open and distributed system with diverse organizations, (2) the number of users contributing to the system can be variant, large, and unknown in advance, (3) the security policies may be administered by the party offering the resources, by the party which needs service from the party owning the resource or by both of them or by the party to which the administration is assigned (Toumi et al., 2012).

Collaboration systems contain resources and information with different degrees of sensitivity. The applications used in such systems create, manipulate and enable access to a variety of sensitive resources and information. Balancing the competing goals of collaboration and security is very complex because collaborative systems seeks to make people, information and resources available to all who need it, whereas security seeks to ensure the confidentiality, availability and integrity of all these elements while making it available to those with proper authorization (Tolone et al., 2005).

For the successful inter-organizational collaboration, several requirements from the user as well as provider’s perspective have to be considered. From the provider’s perspective, different concerns such as confidentiality, integrity, and availability of the information provided are of greater importance before any collaboration process could ever be Confidentiality relates to the disclosure of the information; integrity relates to modification of the information and integrity of operations ensures that only authorized users perform specific tasks; availability represents denial of access to the information (Kuang et al., 2011).

Authorization is crucial in collaborative systems because such systems may enable open access to networked resources or local desktops. Users of collaborative systems require a mechanism not only for identifying the collaborators through proper authentication, but also to control which files, applications, or portions of a system they can access during a collaboration session. Deploying access control models in a collaborative environment can enable secure and authorized access to resources and information (Tolone et al., 2005).

The access control models in collaborative systems must satisfy five criteria: complexity, understandability, ease of use, applicability, collaborative support (Tolone et al., 2005). Complexity represents the nature of the access control model. This criterion is crucial because an overly complex model can lead to unforeseen problems and difficulty in implementing the access control model. Understandability represents the transparency of the model and its underlying principles. The consequences of manipulating and altering the access rights should be obvious for the accurate use of the system. Ease of use represents how easy the system is from the end user's point of view in terms of its usage in a collaborative environment. More complex the system is, the less likely the users will favor it. Applicability represents that an infrastructure should exist where the access control model can be executed. Collaborative support is the most crucial aspect of consideration for access control models devised for collaborative environments. For instance: video conferencing tools need to support audio/video conferencing, text-based chat, screen share for collaboration. There are several factors that determine the usability of an access control model in a collaborative environment including group of users, policy specification, policy enforcement, fine grained control, active/passive access control, contextual information.

1. *Group of users:* Collaborative environment in its simplest form implies a common task undertaken by a group of users. The access control model should represent support for manipulation and specification for groups of users as well as individual users.
2. *Policy specification:* Access control models are based on the specification and representation of access control policies that regulate a collaborative environment. The access control model should enable specification of policies and an appropriate syntax or

a language that enables modifications or extensions in a simple and collaborative environment.

3. *Policy Enforcement:* The access control models should ensure that the specified constraints or policies are enforced accurately.
4. *Fine grained access control:* Collaborative environments may be characterized by the situations where it is not may be enough to have access controls for a group of users on a group of objects. Many times, a user in an instance of a role might require a specific permission on an instance of an object at a specific point in a collaborative environment. In such situations, a level of fine-grained control is required without introducing complexities or compromises in the system.
5. *Active/Passive:* The access control models should be active "so as to handle the dynamism of a collaborative system" (Tolone et al., 2005) (p.39).
6. *Contextual information:* Context is the most crucial characteristic of any collaboration, and it is fundamental to know the degree to which the access control model utilized the contextual information to secure the system *(Tolone et al., 2005).*

Role based access control (RBAC) is one such model that has been used extensively in collaborative environments specifically in the field of healthcare. In role-based access controls, the privileges are assigned to roles instead of users. Granting privileges to the abstract and stable roles of users having a similar function in an organization helps reduce the management overhead of formulating and managing access control policies. Adding the role hierarchies to the role-based access control is well suited for the inter-organization collaboration. A role based access control may look like this: Role: (Surgeon in an hospital); Allowed Action (Read Access); Target (MR patient 4562, section: MRI results) or Role (cardiologist in a hospital);

Allowed action (Read or Write access); Target (MR patient 4562, section: MRI results). In addition, attribute-based document encryption (Ivanova et al.) can be combined with the role-based access control policy. Only the individuals with certain roles can be granted privileges to decrypt the information (Fabian et al., 2015).

Tripathi et al. (2003) identified various security requirements that a role-based access control model should meet in the collaboration system. These security requirements include role admission constraint, co-ordination requirements, separation of duties, dynamic access control policies, privacy, and meta-level security policies. The role admission constraint represents the conditions that a user needs to satisfy when requesting to join a role. A role admission constraint must specify a list of users that are allowed to join the role and those who are not allowed to join the role. It can also specify certain events that must take place before a user joins the role. Coordination requirements represent the enforcement of precedence constraints among different roles operations aka inter-role coordination. For instance: an inter-role coordination in a blackboard learning system can be that a student can view the assignment after the instructor has created the assignment. When multiple users are present simultaneously in a role, the users can either participate independently or cooperatively. In an independent participation, each user performs all the role specific responsibilities. An example of an independent participation could be every participant of a reviewer role in a conference has to independently write the review. On the other hand, in the cooperative user -participation, the participants share the task responsibilities cooperatively. For instance: There may be several nurses that may be present in a nursing ward in the nurse-on -duty role. However, there may be procedures that may need to be performed once by a single nurse. However, there may be a procedure that may need to be performed by multiple participants of a role such as: jointly opening a bank vault (Tripathi et al., 2003).

An access control model for collaboration must be able to express “separation of duties” constraints as well as possess context sensitive access control mechanisms in place. “Separation of duties” may include many constraints such as static separation of duty, dynamic separation of duty, user-user conflict, user-role conflict, object-based separation of duty, and operational separation of duty. The concept of static separation of duty requires that two specific roles should never be assigned to the same individual. The notion of dynamic separation of duty requires that two specific roles cannot be simultaneously assigned to or activated by the same individual. The concept of user-user conflict requires that two specific individuals should not be assigned to the same role. The user-role conflict states that a specified user should never be assigned to a specific role. The object-based separation of duty represents that a user cannot perform multiple operations of the same object by engaging in two separate roles. The operational separation of duties represents that no single user of a role can execute all the operations related to a business transaction (Tripathi et al., 2003).

The notion of dynamic access control mechanisms represents that privileges assigned to a user in a specific role may change with time due to actions carried out by other participants in the collaborative environment. In some situations, privileges may change due to the user's own actions such as making a final agreement on a document. Sometimes, a role can only be executed only if another role has performed some action. In addition, the dynamic access control policies have to address the issues such as minimum or maximum number of participants that must be present for an operation to be performed. Though privileges are assigned to roles, they may be specific based on a variety of contexts and can be activated based on these contexts. The context-based access control can also be related to physical environment’s events. For instance: in cloud resource sharing activity, context-based access control may specify that the members can access the computing resources only when they are located in the organization and that too during a pre-defined period. The meta-level security policy represents that an activity requires many administrative security policies such as who can define or instantiate new activity, who can modify various policies and enforce additional constraints on shared objects. These meta-level policies can be specified based on meta-roles such as creator and owner of various entities such as roles, activities, and objects. In addition, the meta-policies should specify who can join or leave these roles (Tripathi et al., 2003).

The execution of various activities in various domains such as business, shopping, entertainment and scientific collaboration may be based on the utilization of remote resources and services. The parties communicating with each other in such domains may be totally strangers or unknown to each other. In a dynamic collaboration, where parties are coming from different security domains and have no pre-existing relationships, two key issues may arise: specification of access control requirements as well as trust management. The specification of access controls for dynamic collaborations can be very difficult “mainly due to limited or lack of knowledge about remote user’s identities and affiliations” (Shaffiq et al., 2005) (p. 104). Instead of using actual identities of the remote users, the access control policies and constraints can utilize attribute identification of the parties to determine users’ authorization over each other’s local resources. The users owning the resource specify the authorization of the remote users based on their attributes and the requesting users proves the possession of attributes by providing credentials. A user may own different credentials certifying different attributes and each credential may serve a different degree of trust. However, all credentials may not be accepted with the same degree of trust. The degree of trust may depend upon the party issuing the credential and each party issuing the credential may not always be trusted to the same extent (Shafiq et al., 2005).

Attribute-based access control (ABAC) is regarded as an efficient and flexible method to establish security guarantees in a collaborative environment (Rubio-Medrano et al., 2013). Employing access control in collaborative environment is fundamental as the overall safety of the collaborative system may rely on the overall access control mechanism that can effectively enable users from remote organizations to access the resources required for collaboration, while still prohibiting unauthorized access to resources. "In ABAC, a given access control request, e.g., reading a confidential data file, is granted upon the satisfaction of constraints involving some security relevant properties, also known as attributes, that are exhibited by the access control entities involved in the request" (Rubio-Medrano et al., 2013) (p.525). Mainly, such access control entities include human agents or computer systems running on behalf of human agents. For instance: Consider a collaborative environment, where collaborators may request an access to a shared file. The access right to read a shared file is represented by a permission called read file permission. A request to access a shared file is only granted if the requesting party happens to be the owner of the file or if the file is labelled as "shared.txt. Such a constraint illustrates a collaborative environment when an access to a shared resource is granted only to the collaborative party only during the working hours. Hence in this example, contraint1 (C1) permits the access to a given file only if its name attribute has a value matching to the "shared.txt" and the time attribute manifested by the context environment fits the certain range. The constraint 2 (C2) permits the access to the given file only if the name attribute presented by the requesting party matches the “ownername” attribute defined for the access permission for the shared file (Rubio-Medrano et al., 2013).

Access control models in a collaborative environment can’t feature security policies of one single organization. It should integrate the security requirements of all the participating organizations. Since each party specifies its security policy independently, the security policies from all participating parties can be integrated together to govern data sharing throughout the collaborating network. Policy integration in one such method that can be utilized to integrate the security requirements of all the organizations participating in a collaborative system. During the policy integration process, the policies from all the collaborating parties are compared and evaluated through similarity and logical reasoning. The resulting features can be utilized to create an access control model for the collaboration system (Kuang et al., 2011).

However, various types of redundancies and inconsistencies during the policy integration process. Redundancies that can occur during policy integration process include redundancy between roles, redundancy between credentials, redundancy between permissions, redundancy between temporal and spatial constraints, and redundancy between metadata information. Similarly, there can be inconsistencies between roles, credentials, permissions, temporal and spatial constraint inconsistencies, and metadata inconsistencies. Role Inconsistencies exist when the role specified in the policy of one organization has no comparable role in the policy of another organization. Permission inconsistencies exist when organizations grant different permissions to the similar role. Credential inconsistencies exist when similar roles in two organizations have access to the same permissions, but with the less rigorous authorization requirement in one organization. Temporal and spatial constraints exist when the location and time of the user to access the information in one organization don’t match the temporal and spatial constraint of the comparable role in another organization. When the level of sensitivity in one organization doesn't match the sensitivity in another organization, it is referred to as Metadata inconsistency (Kuang et al., 2011).

In recent years, the demand and interest of community centered collaborative systems (CCCSs) has increased immensely. The community centered collaborative systems include cloud computing and social networking sites. These systems create an environment where "users can collectively create, share and manage resources" (Paci et al., 2018) (p.61). As CCCSs have emerged and gained popularity, the requirement to protect the sensitive resources shared amongst these systems is becoming an issue. The traditional access controls such as mandatory access control or role-based access controls are too rigid, too structured, or not too powerful, hence making them unsuitable for CCCSs (Paci et al., 2018).

Paci et al. (2018) listed various security requirements which CCCSs should fulfill, which are as below:

- The access control models in CCCSs should provide elements that enable the specification of access control policies in CCCSs context i.e., the access control models should support interpersonal relationships and related constraints. One way to implement this is to "constrain access rights with respect to interpersonal relationships or level of trust between the resource owner and resource requester.
- There are multiple stakeholders involved in CCCSs and they can potentially have conflicting security goals on the same resource. Due to lack of a central authority, these conflicts may be resolved using automated conflict resolution solutions or pre-defined conflict resolution strategies or that strive for mutual agreement.

- The complexity of CCCSs where resources are managed by multiple users, can make specification and configuration of access preferences more challenging and error prone as compared to traditional access control systems. In addition, the access control models don't inform users about the privacy risks associated with making collaborative decisions. Hence, in the collaborative environment, it is imperative for the users to understand and be aware of access decision making reasons in order to ensure usability and transparency (Paci et al., 2018).

The advancements in technology has enabled the industrial internet of things (IIOT) to collaborate with each other. IIOT interconnects different supply chains, production labs, cyber-physical systems with each other nationally and internationally. Collaborations among IIOT and resulting data exchanges pose significant risks in the terms of information security. While an increasing amount of collaborations among IIOT enhances productivity, it also poses a threat regarding loss of data sovereignty i.e., loss of control over data and processes, proprietary known how, intellectual property and process. In addition, collaboration between IIOT can also lead to information leakage which can further enable imitation, vertical integration by suppliers, counterfeit products by competitors. Every shared piece of information can lead the adversary to reverse engineer the sensitive information (Pennekamp et al., 2019).

Temporary business relationships are formed during dynamic cross-organizations collaborations. In order to integrate their business processes, organizations are required to grant each other the short-term access to their information systems. However, access controls mechanisms in different organizations often rely on non-standard attributes to describe the roles and permissions of their employees which complicates cross-organizational authorizations when business relationships expand quickly (Preuveneers et al., 2018). To resolve this issue, Preuveneers et al. (2018) presented an attribute access control proof of concept framework that enables policy re-conciliation in authorization scenarios that cross the enterprise trust boundaries of the organizations. The proposed solution aligns identity relationship management and dynamic entitlements to accommodate different attribute usage across organizations security systems (Preuveneers et al., 2018).

2.3. PRIVACY IN COLLABORATIVE ENVIRONMENT

The concept of privacy as a legal right was discussed in an article “The right to privacy” by Brandeis and Warren (1890). This article was published as a debate over the privacy infringements caused by newspapers and photography. The authors in this article discussed how the exact nature of the law that provides full protection to an individual in person and in property got redefined and how the scope of such protection developed from time to time. The authors discussed that in early times, the law providing full protection to an individual in person included only protection from battery and the protection in property secured individuals land and his cattle. Later, due to recognition of an individual's spiritual nature, his feeling and his intellect, the extent of these legal rights broadened from “right to life” to “right to enjoy life”. The right to enjoy life included “right to be left alone; the right to liberty secures the exercise of extensive civil privileges” (Brandeis & Warren, 1890) (p.193). The right to be left alone is an individual’s right to privacy (Brandeis & Warren, 1890). Later in 1967, Westin defined Information privacy as “the claim of individuals, groups, or institutions to determine themselves when, how, and to what extent information about them is communicated to others” (Westin, 1967) (p.67). Hence, the concept of privacy extended from “right to be left alone” to “right to control”.

No doubt the concept of privacy has changed drastically over the past years, Westin’s definition of privacy still holds true (Buck & Burster, 2017) as Bélanger and Crossler (2019) notes that many researchers have agreed that privacy is an individual's ability to control information about herself/himself. So, what is personal information then?

An article by Privacy and Information Management (PIM) taskforce notes that personal information "includes any information about an identifiable individual, except business title and contact. A simple image on a video system that is clear enough to identify a person or the activities in which they are engaged is classified as personal information and is protected under the Acts" (PIM, 2008) (p.250).

"Recent technological advancements have made the transmission of audio, video and other media across digital networks quite economical" (Hudson & Smith, 1996) (p.248). This enabled the use of audio, video and shared objects to support distributed collaborative work groups. While the rich communications media such as audio and video enable the distributed collaborative groups to operate smoothly, they also impose certain privacy risks. In shared physical space, it is often the case that we have a well-established set of protocols to deal with the issue of privacy. For instance: the difference between public and private is instantly clear, and most individuals are aware of how to adjust their behavior for each with very little effort. However, in the virtual space, the cues for public and private are often absent. Working in the video-based media presents similar situations as working in front of a one-way mirror. One never knows who might be watching or when someone is watching (Hudson & Smith, 1996).

The introduction of advanced technologies such as mobile devices have increased productivity, flexibility, and more efficient ways to coordinate tasks and people. The distinct feature of ubiquity provides individuals the ability to do anything, anytime and anywhere. It enables them to do things that they couldn't do before thereby increasing their whole set of competencies. Mobile technology is considered a tool for personal and private communication.

Now, freed from temporal and spatial constraints, individuals are constantly taking private conversations into public spaces creating friction and interference with another individuals' privacy. The same technology that empowered the individuals in their workplaces in so many ways also took away "long cherished freedom in others". It has increased individuals' work pressure, close monitoring and supervision, and their inability to keep work and personal space separate (Jarvenpaa & Lang, 2005). This effect is amplified by the advancements in the technology

A key challenge for software designers is to design systems and services in such a way as to mitigate the privacy risks. This is so because the notion of privacy is different for different individuals, organizations and nations. "Rather than exposing an unambiguous public representation for all to see and comprehend, it cloaks itself behind an assortment of meanings, presenting different interpretations to different people" (Lederer et al., 2004) (p.440). When socialists consider privacy, they look at nuances that the system engineers may overlook. When cryptologists consider privacy, they consider technological mechanisms that the general public may overlook. When the European see privacy, it discerns moral expectations that American policy makers ignore. Amidst these heterogeneous perceptions, practices and technologies that characterize privacy, software designers face continuous pressure to design privacy sensitive systems that meet all user's needs, which is a very challenging task (Lederer et al., 2004).

While some individuals may not consider location tracking devices infringing their privacy, others may question location tracking devices and doubt whether their implementation should be beneficial. For instance, while parents view location tracking devices as a way to ensure safety and maintenance of peace of mind, their children may view the location tracking devices as a source to infringement of their privacy (Iachello & Hong, 2007).

In addition, software designers may lack privacy knowledge. Although, to support software designers, some organizations have developed privacy guidelines for their developers. But the software engineers may not be motivated to read the lengthy and complex privacy guidelines and often rely on their interpretations, leading to an error prone system (Pearson & Benameur, 2010). In a collaborative environment, it may be required to hide the identities of one participant from another. In such cases, the presence of a participant can be made visible through his/her role or using a pseudonym in role, but not by name. It may also be required to hide the identities of the participants of a role from other roles (Tripathi et al., 2003).

The online social networks not only allow individuals to share ideas, news, create forums, upload professional profiles and search for jobs, but also raise the issue of personal privacy. The data collectors may use the information from users' profiles for product promotion and could violate users' personal privacy. The data collectors can use data mining techniques on data shared by users with the online social networks such as account profile, text messages, audio, videos. This data then can be refined and sold to third parties by the online social network providers (Kukar et al., 2019).

The existing online social networks are not suitable for sharing collaborative content because in collaborative content the content not only relates to one individual, but also co-owners of the content (Ali et al., 2019). To allow the dissemination of data amongst legitimized users, Ali et al. (2019) introduced a secure collaborative content sharing technique in which the users are classified in three categories: 1) Data owner is the individual who publishes and controls the rights of published data. 2) The data co-owners are the individuals who share co-ownership with the data owner and the data owners share data directly with the co-owner through the access management server. 3) The third category includes the individuals who get access to the data contents while getting threshold secret shares from data co-owners. The data owner provides a list of co-owners that will be allowed to get access to the data. The access management server acts as an intermediary between social media servers and users and as a virtual access management system to manage the security keys, control users' access, and protect users' privacy. The data owners upload the encrypted data to the social media server and tag the co-owners and later the access control management server then allows the co-owners and viewers to have access to contents of the data (Ali et al., 2019).

Spammers and telemarketers target a large number of recipients who are spread across many service providers. Collaboration and information sharing between service providers increases accuracy detection of these spammers and telemarketers. The effectiveness of the accuracy detection depends upon the amount of information shared between service providers. Having service providers share detailed call records would enhance accuracy and would require significant network resources. In addition, the service providers would feel uncomfortable in sharing their customers' call records because call records not only contain the operational details of their network, but also contain users' private information. Therefore, it is very crucial to develop a collaborative system that detects spam over internet telephony (Hakim et al., 2020) with high accuracy, while still protecting the privacy of users as well the service providers (Azad & Morla, 2019).

Azad and Morla (2019) developed a collaborative SPIT detection system (CSDS) where service providers collaborate to effectively and early detect the SPLIT callers without raising privacy concerns. The proposed system relies on trusted centralized repository and exchange of non- sensitive reputation scores. The trusted centralized repository calculates global reputation scores of the users by combining the reputation scores provided by respective collaborating service providers. The data exchanged with the central repository can’t be used to infer the relationship network of the users and is not sensitive regarding users’ privacy (Azad & Morla, 2019).

Collaborative e-health enables the collection and exchange of patient data eliminating the location and accessibility barriers in the healthcare domain. But there are a number of privacy challenges that can be encountered when collecting and sharing patient data during collaborative e-health such as loss of control over outsourced data and virtualization issues. The loss of control over outsourced data means that the patient loses control over his/her data once it gets outsourced to the cloud. The data residing over the cloud can get exposed to various privacy breaches such data breaches due to malicious insiders, data loss because of malicious attacks, data breaches, and insecure interfaces and APIs. The malicious insider can be an employee who can illegally take patient data either for economic reasons or to hurt the patient. Patient data can also be lost due to malicious attack, accidental deletion by cloud service providers and natural disasters. In addition, due to the multi-tenancy nature of the cloud, the compromises that happen in one virtual environment can impact another virtual environment residing in the same physical machine. Lastly, the insecure APIs can also grant access rights to intruders. In addition, due to the virtualization nature of cloud, several side channel attacks can take place. Side channel attacks take the advantage of cloud virtualization to learn sensitive information. The attackers may reside in the same machine and share the same cache and processor as the victim and hence can steal sensitive information about the victim (Edemacu et al., 2019).

Two categories of access control mechanisms have been proposed in the literature to mitigate the privacy challenges: Encryption-independent access control method and encryption-based access control over method. The encryption independent access control method requires the patient and providers to collaborate and create access control policies on the access control server.

The encryption-based access control method involves use of encryption and decryption techniques to mitigate the privacy challenges. Further, encryption-based access control method has two categories: public key infrastructure access control method, identity-based access control and attribute access control method. Under public key infrastructure access control, the identities of users are established through public keys. Certificate keys bind the public keys to the user identities. Once the user's identities are verified, they are provided with the private keys, which can be used to decrypt the data. In identity-based access controls the public keys of the users are used as the identities and the user's data is authenticated based on his/her identity. In the attribute access controls, decryption keys and the cipher text are labelled with the attributes. The access policies are then embedded in either the cipher text or decryption keys. A data user can successfully decrypt the ciphertext the attributes of the user match the attributes in the access policy(Edemacu et al., 2019).

2.4. RELATIONSHIP BETWEEN PRIVACY AND SECURITY

Privacy and Security are related, but not identical. Security emphasis on the protection of data, whereas privacy emphasis on use and governance of personal information (Heckman, 2017). Security represents protecting the electronic data, networks and network users from cyber-attacks such as phishing, spam, hacking, and identity theft etc.(Anderson, 2006), Whereas privacy represents enforcing the policies in place to ensure that individuals' personal information is collected, shared and utilized in appropriate ways (Heckman, 2017).

Security protects the sensitive information that could be accessed by others such as paper or electronic documents. Security policies don't protect those things that are personal and not documented. However, these are protected by privacy policy makers. The general role of information security is to support information privacy, but in some situations, one might be compromised for the sake of the other. For instance: access of threatening emails leads to privacy violations, while protecting the victim's security (Anderson, 2006).

Theoretically, security should protect privacy. Although security and privacy don't match perfectly, they overlap with each other. There are several areas of concern that are common to both privacy and security: establishment of policies, communications of policies, training and enforcement, detection and discovery of intrusions and response to intrusions (Anderson, 2006). The relationship between privacy and security is often misunderstood. A typical incarnation of this view is the all too common argument "if you have nothing to hide, you have nothing to fear". This view has been criticized because it approaches security and privacy in abstract terms and reduces public opinion to one particular attitude, which contemplates surveillance technologies to be beneficial in terms of security, but potentially detrimental in terms of privacy. There are different views on the relationship between privacy and security. While some view that increase in security leads to decrease in privacy, others view security not infringing privacy at all. There are some individuals who question surveillance technologies and doubt whether their implementation should be beneficial, while others consider these surveillance technologies neither problematic nor threatening their privacy at all. There are some individuals who doubt that surveillance technologies are effective enough to prevent crimes and terrorism to justify the infringement of the privacy caused by these surveillance technologies (Friedewald et al., 2015).

The relationships between privacy and security is not a binary relation in which one can be traded for the other, until a balance is found. "One fallacy common in privacy and security discourse is that trade-offs are effective or even necessary. Consider the remarks of New York Police Department Commissioner Ray Kelly shortly after the Boston Marathon bombing, 'I'm a major proponent of cameras. I think the privacy issue has really been taken off the table'" (Conti et al., 2014) (p.28). Organizations' consideration of security and privacy is often skewed by its missions, current events, leadership opinions and various other factors, often resulting in organizations giving importance to either security or privacy. Unfortunately, it is easy to compromise privacy, when seeking to improve security. But this should not prevent individuals/organizations to strive for balancing both security and privacy. There are solutions that benefit both privacy and security. Through proper education, rational analysis, communication and planning, it is possible to achieve both security and privacy. It is crucial to facilitate dialogue among end users, security solution developers, and privacy policy makers in order to seek a common ground among all participants and further strive the balance between security and privacy (Conti et al., 2014).

2.5 STUDIES ON BLOCKCHAIN BASED COLLABORATION SYSTEMS AND INTEROPERABILITY IN THE HEALTHCARE DOMAIN

This section provides a review of articles that focus on solving security and interoperability issues in the healthcare domain through blockchain technology.

Azaria et al. (2016) proposed a blockchain system named MedRec that uses generic strings for data sharing and retrieval. The use of generic strings allows MedRec to interface with providers' existing local data storage solutions hence resolving system interoperability conflict. However, the proposed system doesn't address how the record a transaction reference to is meaningfully interpreted by systems using different EIES.

Peterson et al. (2016), Sri and Bhaskari (2020), and Margheri et al. (2020) proposed a system proposed a blockchain based framework which utilizes Fast Health Interoperability Resources (FHIR) standard as an exchange format for HIE in the network. In both the studies, the participating nodes reach network consensus through proof of interoperability. The proof of interoperability requires the nodes to provide a proof that the incoming data is interoperable with regards to the known set of structural and semantic constraints. These structural and semantic constraints are facilitated through the FHIR profiles. FHIR profiles are the mechanisms that can be further utilized to constrain a FHIR resource by introducing a model for computable compliance statements. The compliance is both structural and semantic, enabling not only structural constraints on attributes such as data type and cardinality, but also semantic constraints of value sets. Under proof of interoperability, the network consensus is not achieved programmatically, rather using human based processes, where participating nodes negotiate and collaborate with the assistance of both clinicians and terminology specialists. Achieving consensus over an allowable set of profiles manually can be both time consuming and labor intensive.

A study by (Zhang et al., 2018) enforced the use of the FHIR standard to share clinical data in their proposed blockchain based solution named FHIRChain. FHIRChain employs a cryptographic public and private key pair to create digital signatures and identities of the participating providers. Similarly Hylock and Zeng (2019) proposed a patient centric blockchain system that uses proxy re-encryption to share information through smart contracts. The proposed solution uses the FHIR standard to exchange patients' records.

Yang and Yang (2017) also resolved semantic interoperability challenges by requiring the healthcare institutions to agree on the same standard for expressing electronic health records (EHR). Lyniate (2019) notes that each healthcare standard offers a variety of distinct features that makes them more or less appealing to the healthcare institutions based on their needs. FHIR offers high speed, bandwidth and efficiency that makes it appealing to the organizations that require real time data exchange. But for healthcare use cases that don't require higher bandwidth or real time data exchange, HL7 2.0 is widely adopted (Lyniate, 2019). The fact that the healthcare institutions can adopt different healthcare standards based on their needs and even implement a single standard in different ways (Lyniate, 2019), the proposed solutions that mandates the use of a specific standard may pose adoption issues.

Similarly Ivan (2016) proposed a conceptualized blockchain based patient centric personal health record (PHR) solution that enforces consolidated clinical document architecture (C-CDA) generated documents for sharing data across various EHR systems. Since there may be variations in implementation of C-CDA from EHR to EHR, healthcare institutions might not be able to exchange information accurately, which is a barrier to interoperability (Lyniate, 2019).

Kaur et al. (2018) proposed a framework that integrates blockchain and cloud computing for storing, transferring, sharing and processing healthcare data. The transaction between each node is stored using a series of signatures called e-stamp. However, the study doesn't explain how the heterogeneity issues will be resolved if the two healthcare institutions are using different standards or interpreting data differently such as using different naming conventions.

The study by Wang et al. (2018) proposed a blockchain based framework that combines the Ethereum blockchain, decentralized storage system, and attribute-based encryption to achieve fine grained access control over the data in decentralized systems. Similarly Dwivedi et al. (2019) utilizes Ethereum blockchain, decentralized storage systems to secure and anonymize patient data. The proposed solution uses ring signatures for signing messages. Both Wang et al. (2018) and Dwivedi et al. (2019) 's work focuses only on security and privacy and don't address semantic interoperability issues.

The review of the literature concludes that there is no such study that has resolved security and semantic interoperability challenges in the healthcare domain by providing the flexibility to the healthcare institutions to adopt the healthcare standards of their own choice and still receive interoperable healthcare records from other healthcare institutions in a secure and reliable manner.

2.6 STUDIES ON VIDEO-CONFERENCING APPS AND PRIVACY

The past literature has explored the usage of video- conferencing in the context of teaching (Guo et al., 2015; Liu & Alexander, 2017; Padilla-Meléndez et al., 2008). (Maruping & Magni, 2015) conducted a field study to examine the impact of team empowerment, intentions to continue exploring and expectation to continue exploring on employees' exploration of collaboration technology.

The study by Gruzd et al. (2012) utilized qualitative research methodology to discover the factors that influence intentions and use of social media usage. The social media studied included use of video-conferencing tools such as Skype, social networking sites such as Facebook, Academia.edu, and other online media repositories such as Flickr. The study used unified theory of acceptance and use of technology (UTAUT) to interpret the scholarly use of social media. Lack of privacy, losing control of content, professional/personal boundary loss were some of the privacy related concerns expressed by scholars when using social media.

The study by Dermentzi et al. (2016) employed decomposed theory of planned behavior and *The Uses and Gratification theory* to investigate the factors that influence academics intentions to use online social networking sites and online technologies to disseminate their research. The online technologies investigated in this study included webpages, blogs, forums, portals etc. The study hypothesized that the ability of academics to exercise privacy control in SNS positively influences perceived behavioral controls of academics.

Prior studies (Brown et al., 2010; Bullinger et al., 2011; Silic et al., 2017) explored the prediction of collaboration technology usage, acceptance of collaboration technologies, and acceptance and use of collaboration technologies in a cross-cultural environment respectively. The collaboration technologies tested in the study by Brown et al. (2010) included students' use of SMS for collaboration as well as employee's usage of in-house collaboration technologies such as telephone, videoconferencing and desktop messaging for collaboration. The authors explored the prediction of collaboration technology usage by integrating UTAUT constructs with the key constructs from collaboration technologies such as social presence theory, channel expansion theory and task closure model. The study by Bullinger et al. (2011) investigated adoption and acceptance of online collaboration technologies by researchers. The collaboration technologies explored in the study included technologies that enabled researchers to organize their network and literature, share information about themselves and their research activities, retrieve information from other researchers as well as information about new publications or trends. The study by Silic et al. (2017) explored the acceptance and usage of communication and collaboration technologies in a cross-cultural environment.

However, prior literature (Brown et al., 2010; Bullinger et al., 2011; Silic et al., 2017) didn't explore the impact of privacy concerns on the continuance usage of video-conferencing apps in the professional context.

An extensive body of work has addressed privacy concerns in the context of smart phone (Sutanto et al., 2013), location-based services (Gutierrez et al., 2019; Schade et al., 2018), online shopping (Bandara et al., 2020), contact tracing apps (Rowe, 2020), smart watch users (Kang

& Jung, 2020), location aware marketing (Xu et al., 2011), location based mobile commerce (Lee et al., 2019), but there is a gap in the literature concerning the impact of privacy concerns intentions to use video-conferencing apps.

CHAPTER 3 RESEARCH METHODOLOGY

3.1 INTRODUCTION

This research involves the use of both the Design Science Research (DSR) and Behavioral Science Research (BSR) methodologies. The objective of our first research question is to develop a system that resolves the issue of data interoperability and security in health information exchanges. Hence, for the first research question, this research employs DSR methodology because DSR methodology is applicable when the goal of the researchers is to construct a new reality i.e., create and evaluate IT artifacts to solve identified/observed organizational problems (Hevner et al., 2004; Peffers et al., 2007). An IT artifact can be "any designed object with an embedded solution to an understood research problem" (Peffers et al., 2007) (p.6).

The objective of our second research question is to investigate and understand what motivates/influences researchers to utilize video-conferencing tools for their research collaborations despite the susceptibility of these video-conferencing tools to privacy violations. The second research question seeks to investigate the dilemma that on one hand the researchers demand privacy when collaborating with their peers, but on the other hand, they continue to use these privacies violating video-based platforms for communicating and collaborating with their peers. This dilemma can be understood by conducting quantitative research using BSR methodology because BSR methodology is best suited where the aim of the researchers is to investigate and understand some reality (Goodhue et al., 2012; Hevner et al., 2004; Peffers et al., 2007).

3.2 DESIGN SCIENCE RESEARCH (DSR) METHODOLOGY

A methodology implies a system of principles, procedures, and practices applied to a particular branch of knowledge. As such, design science research methodology implies the set of principles, procedures and practices that might assist IS researchers to produce and present design science research that is accepted as of high quality, rigorous, valuable and publishable in IS research outlets (Peffers et al., 2007).

DSR methodology involves a rigorous process to design and build artifacts to solve identified problems, evaluate the artifacts, to make research contributions, and communicate the results to the intended audiences (Hevner et al., 2004). DSR methodology acts as a roadmap to the researchers who desire to utilize design as a research mechanism for information systems research (Peffers et al., 2007).

3.2.1 DSR Process

This section first provides the description of the DSR guidelines provided by (Hevner et al., 2004). Second, it explains the DSR process model provided by (Hevner & Chatterjee, 2010). Lastly, it provides the DSR process model by (Vaishnavi et al., 2004).

3.2.1.1.DSR Guidelines by Hevner et al. (2004)

Hevner et al. (2004) provided six guidelines for design science research, which are as follows:

- *Design as an Artifact:* “DSR must produce a viable artifact in the form of a construct, a model, a method, or an instantiation”. Viability suggests that the artifact must have a practical usage, workable, and realistic (Hevner et al., 2004).
- *Problem Relevance*: The objective of DSR is to obtain knowledge and understanding that facilitates the development and implementations of technology-based solutions to solve unsolved and critical business-related problems (Hevner et al., 2004). The relevance of the DSR effort in information systems is with respect to its constituent community that comprises practitioners who plan, manage, design, implement, and evaluate Information systems and those who plan, manage, design, implement and evaluate the technologies that facilitate the development of information systems.

  To be relevant to this community, the researchers “must address the problems faced and the opportunities afforded by the interaction of people, organizations, and information technology” (Hevner et al., 2004) (p.85).
- *Design Evaluation*: The proposed artifact must be evaluated via well executed methods to demonstrate its utility, quality and efficacy. The evaluation of a designed artifact requires the definition of appropriate matrices and likely the gathering and analysis of relevant data. The utility, quality and efficiency of a design science artifact must be evaluated via well executed evaluation methods.

A design science artifact is considered to be complete and effective, when it satisfies all the constraints and requirements of the problem it was meant to resolve. An artifact can be evaluated in terms of its completeness, consistency, usability, functionality, performance, reliability, and fit with the organization. For instance,, search algorithms can be evaluated using information retrieval matrices such as precision and recall or distributed database algorithms can be evaluated using average response time or expected given cost for a given characterization of information processing requirements (Hevner et al., 2004).

- *Research Contributions:* DSR holds the possibility of three types of research contributions: the design artifact, foundations, and methodologies. The design artifact in DSR is mostly an IT artifact. An IT artifact may extend the existing knowledge base or apply existing knowledge base in new and innovative ways. DSR can also develop novel, properly evaluated constructs, methods or instantiations that extend and improve the previous foundations are also significant contributions. Modeling formalisms, ontologies, design algorithms, problem and solution representations, and innovative information systems are examples of the artifacts that fall into the foundations category. The creative development and use of evaluation methods and evaluation matrices are also significant contributions (Hevner et al., 2004).

- *Research Rigor*: In DSR, rigor is achieved by the effective use of a knowledge base such as theoretical foundations and research methodologies. The success depends upon the researchers' selection of suitable techniques to develop or construct a theory or an artifact and selection of appropriate means to justify the theory or evaluate an artifact. Since an artifact is often a component of the human-machine problem solving system, the knowledge of appropriate behavioral theories and empirical work are necessary for constructing and evaluating an artifact.
- *Design as a search process*: Citing Simon (1996), Hevner et al. (2004) notes that "Design is essentially an iterative process to discover an effective solution to a problem. Problem solving can be viewed as utilizing available means to reach desired ends while satisfying laws existing in the environment" (Hevner et al., 2004) (p.88). Abstraction and representation of suitable means, ends and laws are important components of DSR. These factors are a problem and environment dependent and invariably involve innovation and creativity. Effective design necessitates knowledge of both the application domain and the solution domain.

DSR often simplifies a problem by decomposing it into sub-problems or representing only a subset of the relevant means, end and laws. Solutions to these sub- problems may represent a starting point for the researchers to solve the larger problems by expanding its scope. It is clearly infeasible to determine the relevant ends, means or laws. In such cases, heuristics can be utilized to construct "satisficing" artifacts i.e., the search for satisfactory solutions.

- *Communications*: The results of DSR must be presented to both technologies oriented as well as management-oriented audiences. Technological oriented audiences require sufficient detail to enable the construction of an artifact as well as its utility within an appropriate organizational context. “This enables the practitioners to take advantage of the benefits offered by the artifact and it enables researchers to build a cumulative knowledge base for further extension and evaluation” (Hevner et al., 2004) (p.90) It is crucial for such audiences to understand the process by which the artifact was developed and evaluated. This enables the researchers to expand the artifact and build a knowledge base for future research extensions (Hevner et al., 2004).

3.2.1.2.DSR Process Model by Peffers et al. (2007)

Peffers et al. (2007) developed a process model that acts as a framework for conducting research based on design science principles. The process model was developed by synthesizing design science process elements from seven influential prior articles.

The process model by Peffers et al. (2007) consists of six activities including:

- *Problem identification and Motivation:* This activity involves defining the specific research problem and justification of the value of the solution. Problem definition is utilized to develop an artifact that can effectively solve a problem. Justification of the value of the solution helps the researchers to pursue the solution and the audiences to accept the results. In addition, it helps the audiences to understand reasoning associated with the researchers’ understanding of the problem. Knowledge of the state of problem and the importance of its solution are the sources required for this activity.

- *Define the objectives for a solution:* This activity involves inferring the objectives of the solution from the problem definition as well as knowledge of what is feasible. The objectives can be either qualitative or quantitative. Quantitative objectives can be expressed in specific numerical terms such as to increase the sales of a product Y by 30% in 2020. The qualitative objectives can be a description of how the solution i.e., an artifact will provide solutions for the problems not previously addressed. The knowledge of the current state of the problems and current solutions and their efficacy are the sources for this activity.

- *Design and Development:* This artifact involves designing and developing an artifact. "A designed artifact can be any designed object in which a research contribution is embedded in the design" (Peffers et al., 2007). Designing and developing the artifact involves determining the desired functionality of the artifact and its architecture and then developing the actual artifact. The resources required for this activity involve the *knowledge of a theory* (Peffers et al., 2007). Hevner and Chatterjee (2010) notes that "to insist that all design decisions and design processes be based on grounded behavioral or mathematical theories may not be appropriate or even feasible for a truly cutting-edge design artifact. Such theories may as yet be undiscovered or incomplete and the research activities of design and evaluation of the artifact may advance the development and study of such theories" (Hevner & Chatterjee, 2010) (p.18).

- *Demonstration:* This activity involves demonstrating the utility of the artifact to solve one or more instances of the problem identified. This could involve its use in case studies, simulation, experimentation, or other appropriate activities. Resources for this activity include effective knowledge of how to utilize the artifact to solve the problem (Peffers et al., 2007).

- *Evaluation:* This activity involves observation and measurement of how well the proposed artifact supports the solution to the problem. It involves comparison of the objectives of the proposed solution to the actual observed results obtained from the utilization of the artifact in the demonstration phase. An artifact can be evaluated by utilizing various relevant matrices and analysis techniques. Depending on the nature of the problem and the proposed artifact, evaluation could take various forms. This could include comparing an artifact's utility with those of solution objectives from the study. The evaluation could include quantitative performance measures such as items produced or budget, results of simulation, satisfaction surveys, or client feedback. It could also include quantifiable measures of the artifact such as availability or response times. At this point of activity, the researchers make two choices: iterate back to activity 3 to try to enhance the effectiveness of the artifact or to continue on to communicate the results of the artifact and leave further the refinement to the future projects. It is the nature of the research venue that determines whether such an iteration is possible or not (Peffers et al., 2007).
- *Communication:* This activity involves communicating the problem and its significance, the proposed artifact, its utility and novelty, the rigor of its design, and its effectiveness to the research community and other relevant audiences. The researchers can use the structure of this process to publish their scholarly research publications. Although this process is structured in a nominally sequential order, it is not required that the researchers should always proceed from activity 1 through activity 6. In reality, the researchers can start at any activity and move outward. If the idea for the research initiated from the observation of a problem or from suggested future work from a prior published research, then the researchers could proceed from activity 1 to activity 6.

An objective centered approach would start from activity 2. The objective centered approach could be precipitated by any research need or by an industry that can be addressed by an artifact development. A design and development approach would start from activity 3. “It would result from the existence of an artifact that has not yet been formally thought through as a solution for the explicit problem domain in which it will be used. Such an artifact might have come from another research domain, it might have already been used to solve a different problem, or it might have appeared as an analogical idea” (Peffers et al., 2007) (p.56).

3.2.1.3.DSR Process Model by Vaishnavi et al. (2004)

Vaishnavi et al. (2004) proposed a design science research process model that includes five steps: Problem relevance, suggestion, development, evaluation, and conclusion.

- *Problem Relevance:* Problem relevance includes awareness of the problem. This awareness can come from different sources such as identification of the problem within a reference discipline or new developments in the industry. The output of this phase includes a proposal, formal or informal.
- *Suggestion:* This phase involves envisioning a tentative design based on the awareness of the problem. The integral part of the proposal should include a tentative design and performance of a prototype based on that design.
- *Development:* This phase involves further developing and implementing a tentative design. The techniques for implementing vary depending on the artifact to be created. The implementation needs not to involve novelty beyond the state of art of practice. The novelty should be in the design, but not in how the artifact is constructed.

- *Evaluation:* The artifact should be evaluated according to the criteria explicitly or implicitly stated in the awareness of the problem phase (i.e., the proposal). Divergence from the expectations should be carefully noted and must be explained tentatively. This includes an analytic sub-phase, where the hypotheses regarding the behavior of the artifact are developed and evaluation either confirms or contradicts a hypothesis. In design science, it is very rare that the initial hypothesis concerning the behavior are completely borne out. Instead, the information gained during the construction and running of an artifact and the evaluation phase are brought together and fed back into another round of suggestions. Vaishnavi et al. (2004) further notes that while (Hevner et al., 2004) suggested that an artifact should be evaluated for its utility, the others such as (Gill & Hevner, 2013) suggested that an artifact should be evaluated for "its fitness to adapt and survive within an environment" (Vaishnavi et al., 2004) (p.10). Vaishnavi et al. (2004) further notes that the explanatory hypotheses are never completely disregarded, rather they are modified in accordance with the new observations. The new observations further suggest a new design, a new search preceded by new library search in directions suggested by deviations from the theoretical performance.

- *Conclusion:* This phase not only involves the consolidation and writing of the results of the effort, but also the "knowledge gained in the effort is frequently categorized as either "firm"—facts that have been learned and can be repeatedly applied or behavior that can be repeatedly invoked—or as "loose ends"—anomalous behavior that defies explanation and may well serve as the subject of further research" (Vaishnavi et al., 2004) (p.10).

3.2.2 Types of Theories that can be used in Design and Development of Artifacts

Gregor and Jones (2007) notes that a term theory encompasses conjectures, frameworks, models, or body of knowledge. Further, the outputs of the design science research such as constructs, models and methods are also regarded as the components of theory (Gregor & Jones, 2007). Gregor and Jones (2007) classified information system theories in five categories: *Theory for analyzing, theory for explaining, theory for predicting, theory for explaining and predicting, and theory for design and action.*

3.2.2.1. Theory for Analyzing

This category of theory relates to "what is". It describes and discusses specified dimensions or characteristics of groups, individuals, events by providing a summary of commonalities identified in distinct observations. Different forms of this theory include frameworks, taxonomies, or classification schemas. In addition, the research that focuses on describing certain constructs and their related measures also fall in this category. Also, the research where the grounded theory gives rise to explanations of categories of interest also fall into this category. The descriptions presented by the research represent "what is". The causal explanation, testable propositions, and prescriptive statements are not present in this type of theory (Gregor & Jones, 2007).

3.2.2.2. Theory for Explaining

This category of theory provides an explanation of "why" and "how" some phenomenon occurs. These explanations provide a greater understanding by others about how a world may be envisioned in a specific way, how things are and why they are as they are. These explanations are provided by relying on various views of causality and methods of argumentation. Research approaches that can be used to develop this theory include interpretive field studies, surveys, phenomenological, hermeneutic, and ethnographic approaches, case studies etc. The statement of relationships includes the causal explanations (Gregor & Jones, 2007).

3.2.2.3. Theory of Prediction

This category of theory deals what is and what will happen in the future, if these pre-conditions hold true. "These theories are able to predict outcomes from a set of explanatory factors, without explaining the underlying causal connections between the dependent and independent variables in any detail" (Gregor & Jones, 2007) (p.625), meaning the theory doesn't include statements of causality. Gregor et al. (2006) provided one example of such theory such as: captain cook theorized that regular intakes of citrus fruit helped prevent scurvy without having knowledge of why it was so (Gregor & Jones, 2007).

3.2.2.4. Theory for Explaining and Predicting

This type of theory states deals with what is, how, when, why and what. These types of theories imply both casual and prediction as well as description of theoretical constructs and the relationships. The key examples of these theories include a grand theory called general systems theory which provides a testable hypothesis such as law of requisite variety i.e., "only variety in a system's responses can keep down variety in outcomes when the system is subjected to a set of disturbances" (Gregor & Jones, 2007)(p.628).

3.2.2.5. Theory for Design and Action

This type of theory explains how to do something. "It is about the principles of form and function, methods, and justifiable theoretical knowledge that are used in the development of IS" (Gregor & Jones, 2007) (p.628). The design theory claims that it assists designers of other systems with the identical requirements.

Thakurta et al. (2017) conducted a structured literature review on 275 design science articles to determine the current state of art of design science research. The review revealed that justification of design artifacts is based on theoretical abstractions, artifacts (new or the existing ones), and/or argumentative reasoning.

In 33 articles, the authors have used kernel theories to govern the design requirements. In 40 articles, the design rationale of a proposed solution was based on previous artifacts of various nature: models (21), methods (7), framework (7), guidelines (1), architecture (1), logic (1), principle (1), and meta-model (1). In nine articles, the authors proposed a new artifact and then used it as a basis for underlying design. In the remaining articles, either the design rationale was based on argumentative reasoning on literature or was unspecified.

3.2.3 Artifact and Artifacts Types

Artifacts represent the innovations that define the practices, ideas, technical capabilities, and products through which the analysis, design, implementation, and utilization of information systems can be accomplished effectively and efficiently (Hevner et al., 2004). Further, the authors note that the outcome of design science research is in the form IT artifacts that includes instantiation, constructs, models and methods applied in the development and use of information systems (Hevner et al., 2004). Hevner et al. (2004)'s definition of IT artifacts was narrow in the sense that it neither included people and organizations, nor the process by which the artifacts evolved over time. Further, Hevner et al. (2004) conceive IT artifacts not as independent, but interdependent and co-equal to people, organizations and social contexts in which they are used in meeting business needs. The detailed description of four categories of artifacts provided by (Hevner et al., 2004) is as below:

- *Construct:* Construct provides the vocabulary and symbols to define the problems (Hevner et al., 2004). Constructs can further have three categories: *language, meta-model,* and *concept. Language includes* a set of concepts, or commonly symbols, rules to combine the symbols (syntax), and rules to interpret the combination of symbols (Mwilu et al., 2016). *Meta-mode*l is a set of concepts represented in graphical notation, with rules for combining them (concepts) (Mwilu et al., 2016). A *Concept* can be a new construct added to the language or meta-model (Mwilu et al., 2016).

- *Model:* A model utilizes constructs to represent a real-world situation. "Models aid problem and solution understanding and frequently represent the connection between problem and solution components enabling exploration of the effects of design decisions and changes in the real world" (Mwilu et al., 2016) (p.79). A model is obtained, when the constructs are utilized to build more structured objects. The most common artifact in this category includes the system design. The other categories that are included in the model category are *system design, ontology, taxonomy, framework, architecture, and requirement* (Mwilu et al., 2016). System design represents a structural or behavioral related description of a system, often using some graphic notations or some text (Mwilu et al., 2016). Ontology represents an explicit specification of concepts and relationships that can exist for an agent or community of agents (Mwilu et al., 2016). Taxonomy represents classification of things or concepts in a domain of interest based on shared conceptualizations (Mwilu et al., 2016). A logical structure to organize complex information is referred to as framework (Mwilu et al., 2016). *Architecture i*s a blueprint that represents the "fundamental organizations of a system embodied in its components, their relationships to each other, and to the environment" (Mwilu et al., 2016) (p.5). Ming et al. (2019) proposed an architecture of prototype sequence network (ProSeNet) model that combines prototype learning with the variants of recurrent neural networks to acquire both accuracy and interpretability for sequence modelling. Engelenburg et al. (2017) proposed a business to government information sharing architecture to enable for an information sharing process acceptable by the businesses. The architecture consisted of five main components: blockchain to record events, business rules to set the conditions for information sharing, access controls ensuring only authorized access, metadata and context information to whether context enables information sharing, encryption and decryption. *A Requirement is a* capability or a condition that must be present or met in a system (Mwilu et al., 2016).

- *Methods*: Methods provide guidelines on how to solve the problems and how to search the solution space (Hevner et al., 2004). Methods include different artifacts such as: *methodology, guidelines, algorithm, method fragment, and a matric.* Methodology represents a predefined set of guidelines or steps, with related tools and techniques. Methodologies are aimed at or utilized by individuals working in a discipline (Mwilu et al., 2016). Guidelines represent suggestion/s regarding behavior in a specific situation (Mwilu et al., 2016). *Algorithm is an* executable sequence to perform a specific task is referred to as an algorithm (Mwilu et al., 2016). *Method fragment* is a method component that can be treated as an individual unit and reutilized in different situations. Design patterns are illustrations of method fragment (Mwilu et al., 2016). Metric is a function that assigns a symbol or number to an entity in order to represent an attribute or group of attributes (Mwilu et al., 2016).
- *Instantiations:* Instantiation depicts that a construct, model or a method can be implemented (Hevner et al., 2004). Instantiations can be of two categories: Implemented

systems and examples. *Implemented system* is a hardware or a software system that can either be prototypes or finalized tools (Mwilu et al., 2016). *Example* represents "any other concrete materialization of an abstract artifact"(Mwilu et al., 2016). Examples are proposed either as a first step of the validation of the utility of an artifact or illustrating an artifact. It may be an illustration of a design theory framework with concrete examples of design theory or an application of query language to an illustrative scenario (Mwilu et al., 2016).

Aiken (2020) notes that the outcome of design science research is a design knowledge for the professionals in the field i.e., design knowledge that will be applied by individuals who received formal education in that field. And this design knowledge will be used to "support the design of interventions or artifacts by professionals and to emphasize its knowledge orientation: a design-science is not concerned with action itself, but with knowledge to be used in designing solutions, to be followed by design-based action" (Aiken, 2020) (p.226). Design knowledge can fall into three categories: Object knowledge, realization knowledge, and Process knowledge. Object knowledge represents the knowledge on the settings and properties of the interventions or the artifacts to be designed. Realization knowledge represents the knowledge about various categories such as various knowledge about a variety of surgeries for a surgeon or various types of manufacturing methodologies for a mechanical engineer. Finally, process knowledge typically represents knowledge on how to handle the actual design process. Most professionals gain this knowledge through their own experience or by emulating their teachers or peers (Aiken, 2020). Within each category of design knowledge, prescriptions are a significant category. Prescriptions describe potential opportunities to aid the transfer process from their preliminary problematic state towards the desired state. The typical research product in design science is prescriptions. However, many prescriptions in design science are heuristic in nature.

For instance: “if you want to achieve Y in situation Z, then something like action X will help’. ‘Something like action X’, means that the prescription is to be used as a design exemplar” (Aiken, 2020)(p.227). Further, Järvinen (2007) notes that Jarvinen (2004(a)) extended the view of Hevner et al. (2004) (technical view) and (Aken, 2004) (social) view on design science by adding third resource type i.e., information resources utilized in the development of new innovations. “Hence, new innovation can be based on properties of technical, social, and/or information resources or their combination” (Järvinen, 2007)(p.49).

Peffers et al. (2012) synthesized the list of artifacts from the previous literature. The authors categorized artifacts into six categories: Algorithm, construct, framework, instantiation, method and model. Detailed description along with the examples from literature for each category is provided below.

- *Algorithm:* “An approach, method, or process described largely by a set of formal logical instructions” (Peffers et al., 2012)(p. 401). (Peterson et al., 2016)proposed two algorithms for sharing data using blockchain in the healthcare domain. The first algorithm relates to the process of adding the blocks on the blockchain. The second algorithm known as proof of interoperability acts as an alternative method to reach network consensus. It describes the process by which all the incoming transactions are compared to the specified FHIR profile in order to ensure the conformance of the incoming message to a known set of structural and semantic constraints. Similarly, Yang et al. (2019) developed a proof of familiarity (PoF) algorithm for collaborative medical decision making in the healthcare domain. The PoF consensus gathering algorithm considers skills, experience, and collaborative success rate of patients, cured patients, doctors and insurance companies to select and store final collaborative decision making. Similarly Wang et al. (2020) proposed five sets of algorithms to preserve privacy in the financial sector.

- *Construct*: An assertion, syntax, or a concept that has been constructed from a set of assertions, statements or other concepts. Flory et al. (2017) proposed a construct named review quality analysis. Flory et al. (2017) defined review quality analysis as “an automated approach to help consumers make sense of online reviews” (Flory et al., 2017)(p.85). The main objective of this construct was to identify the review that assists customers make informed purchase decisions. Based on the definitions taken from both literature and business practice literature.
- *Framework*: Framework can also be referred to as a meta-model. (Wang et al., 2020) developed a data privacy management framework. The framework comprises three components: a data privacy classification method, collaborative filtering-based model and confirmation data disclosure scheme. Liu et al. (2020) developed a collaborative quality of service prediction framework to resolve the issue of quality of services that may arise due to dynamic internet environment and different measurement between users.
- *Instantiation:* The structure and organization of a system’s software or hardware (Klör et al., 2018) designed a DSS that assists decision makers with repurposing used batteries. The designed DSS consists of language constructs, models to represent batteries and scenarios in a database, decision models to match the batteries to scenarios, and graphical user-interface. The authors designed a graphical user interface of their proposed DSS for repurposing used batteries to instantiate the generic process of decision making from modeling the available products and scenarios to assigning each product to each scenario. Graphical User interface consisted of four components: battery selection, scenario selection,

consistency check, and decision matrix. Battery selection component was used for selecting battery instances for decision making. The scenario selection component was used for selecting scenarios. Based on available data on selected batteries and scenarios, the consistency check component identifies the eligible decision models (Klör et al., 2018).

- *Method*: The actionable instructions that are conceptual, not algorithmic. A study by (Dou et al., 2019) proposed a privacy preservation method to address the challenge of multimedia in social network contexts. The proposed method is based on a weighted noise injection method. The core users are extracted from the entire list of users. Next, the extracted core users are used to represent the features of all the users. Later, the relevant data of the extracted core users is used to rate prediction. Then, different noises are injected to the rating matrix of extracted core users. Lastly, a perturbed matrix is utilized to predict the ratings of unused multimedia resources for target users. Fridgen et al. (2018) proposed a method for developing viable blockchain use cases (BUC) which consists of six steps: understanding the technology, getting creative unbiased, glancing at the market, structuring the ideas, and prototyping.
- *Model*: "A simplified representation of a reality documented using a formal notation or a language" (Peffers et al., 2012)(p.401). Klör et al. (2018) designed a DSS system that assists decision makers in matching used batteries to the second life applications scenarios. Hence (Klör et al., 2018) developed two decision models for matching used batteries and scenarios (second life application scenarios). The first decision model identifies a technical fit between all products and scenarios i.e., identifies all the feasibility assignments. The second model identifies an optimal assignment i.e., the parameters of each battery should match the requirements of scenarios as closely as possible (Klör et al., 2018).

The structural literature review conducted by typology Thakurta et al. (2017) revealed that the typology of artifacts presented in design science research are not limited to constructs, models, methods and instantiation (as proposed by Hevner et al., 2004), but also include: application, architecture, design pattern, framework, infrastructure, methodology, ontology, portal, process model, system, system landscape, taxonomy, and typology (Thakurta et al., 2017).

3.2.4 Types of Evaluation Methods

This section first explains evaluation methods discussed by Hevner et al. (2004). Later, it discusses evaluation methods discussed by Peffers et al. (2007).

3.2.4.1. Evaluation Methods discussed by Hevner et al. (2004)

Hevner et al. (2004) listed different methods for evaluating an artifact. These include observational methods, Analytical methods, experimental methods, testing, and descriptive methods.

- *Observational Methods*: The observational methods are further categorized into two categories: Case study and field study. Case study involves an investigation of a phenomenon with its real-life context. In the case of a design artifact, it can involve having an in-depth investigation of an artifact in business context. Field study involves observing the usage of an artifact in different contexts (Hevner et al., 2004). Wang et al. (2020) conducted a field experiment to evaluate their proposed framework. The authors conducted the *field experiment* to validate that the financial characteristics of the customers implies his/her tendency to protect data, hence verifying the usability of their proposed framework. The field experiment was conducted by interviewing randomly selected 1000 loan customers. The field experiment was conducted to communicate and understand the customers' willingness to disclose personal information to attain better banking services. Ming et al. (2019) evaluated the interpretability of their proposed model ProSetNet using four different *case studies:* case study one related to predictive diagnostic based on vehicle fault log data, case study two related to sentiment classification task on reviews of restaurants, third case study related to evaluation of ProSetNet in biology domain using UnitProtKB database, case study four involved investigating the ProsetNet in healthcare domain.

- *Analytical Methods*: Hevner et al. (2004) listed four methods under this category: static analysis, architectural analysis, optimization, and dynamic analysis. Static analysis involves investigating the structure of an artifact for its static qualities such as: complexity. Architectural analysis involves "study fit artifact into technical IS architecture" (Hevner et al., 2004)(p.86). Optimization involves providing optimal bounds on the behavior of an artifact or demonstrating its intrinsic properties. Dynamic analysis involves investigating the artifacts in use for its dynamic qualities such as: performance.

Flory et al. (2017) proposed utility *sensitive customer review analyzer* (IUSR) whose main aim was to achieve high efficiency and effectiveness. The effectiveness of the IUSR was measured by using precision and F-measures. In order to evaluate the effectiveness, the authors used reviews from Trip advisor and amazon. com. To measure the effectiveness and run the experiments, the authors simulated consumer inputs and gold sets. Gold sets is the set of reviews that are regarded as highly relevant by the consumers. The gold set is used as the benchmark to compare the accuracy of the IUSR analyzer. Since it was too expensive to collect a high volume of real-world consumer inputs and gold sets, the industry experts helped the authors build consumer inputs and gold sets. In addition, the effectiveness of IUSR was validated through implementing it in a North American firm.

Abbasi et al. (2019) proposed a framework to examine key design elements for voice of customer listening platforms. In addition, (Abbasi et al., 2019) developed a novel heuristic-based method to detect adverse events. In order to evaluate their proposed framework, Abbasi et al. (2019) created two large test beds including millions of tweets, posts, forums, search query logs regarding adverse events related to the automobile and pharmaceutical industries. To evaluate the performance of their proposed method, the authors then compared their proposed method with several basic mention models, machine learning models, and general event detection methods. All the methods including the proposed method were evaluated using standard aforementioned metrics: recall, precision and timeliness. Similarly, Azad and Morla (2019) used information retrieval performance metrics to evaluate their proposed system: the detection accuracy or True positive rate (TPR), the false positive rate (FPR) and the accuracy rate (ACC).

- *Experimental Methods*: Under this category, an artifact can be evaluated through controlled experiment or simulation. *Controlled experiment* involves studying the artifact in a controlled environment for qualities such as usability. Venkatesh et al. (2017) developed a shopping assistance artifact that provides product information as well as product information as well as product reviews. To evaluate the proposed artifact, Venkatesh et al. (2017) designed a retail store laboratory to appear similar to retail store layout. The retail store laboratory was set up as a mock store front for the Acme products. The individuals who were agreed to be on the mailing list to receive advertisements and promotions from retail stores were contacted to participate in the experiment. The participants were asked to shop in the simulated retail store and told to feel free to walk in the store as they would do in the actual retail store. In the experimental conditions, each participant was provided with the iPhone 5 and the instructions related to availability of the app. In addition, they were also given the demonstration on how to use the artifact. In the control condition, where the participants didn't receive any shopping assistance artifact, the participants were given the same instructions, but without any information related to iPhone and information related apps. At the end of their shopping experience, the participants were asked to fill out a survey regarding their entire shopping experience.

Wang et al. (2020) conducted a laboratory experiment to verify the functionality of their proposed framework. The main objective of the proposed framework was to resolve the financial data privacy protection challenge in the financial sector. In conducting the laboratory experiment, the authors used a PC with 4-core CPU, 8GB memory connected with LAN with the bandwidth of 100MPS. The experiment was conducted in a banking environment and in conducting the experiment, the authors used the desensitized customer data disclosure scheme. Liu et al. (2020) evaluated their proposed QOS framework using a real web of service QoS dataset and used Root mean squared error and mean absolute error to measure the performance of their framework.

Simulation involves executing the artifact with artificial data for its performance tuning, usability etc. Wastell et al. (2009) created a PC-based simulation named central heating system simulation (CHSS) to simulate a generic central heating system in order to carry out the experiment and generate meaningful user engagement and obtain relevant knowledge about the energy consumption and comfort levels of the central heating systems. Lim et al. (2017) created a test site to simulate a restaurant environment to conduct experiments to test the performance of their proposed MobileApp. Venkatesh et al. (2017) simulated a retail store environment by creating a retail store laboratory to evaluate their proposed retail assistance artifact. A study by Sierra et al. (2019) used a scenario-based simulation to test the usability of three conceptual designs for home energy management products (HEMP), a specific category of smart energy products and services. The authors developed short testing sequences to validate prototype operation utilizing the simulation environment from Smart EST Lab. In these testing sequences, the authors simulated energy production and consumption independently to model different states of the system. In addition, the authors created four different scenarios reflecting adequate and inadequate performance according to weather conditions. Azad and Morla (2019) evaluated their proposed system by using the synthetic dataset that was generated by simulating realistic behavior of spammers and non-spammers.

- *Testing*: Functional and structural testing falls into this category. Functional testing involves execution of artifact interfaces to identify failures and defects. Structural testing involves performing “coverage testing of some matrices (e.g., execution paths) in the artifact implementation” (Hevner et al., 2004)(p.86).
- *Descriptive Analysis*: Informed argument and scenarios are two methods that fall into the category of descriptive analysis. Informed argument represents the use of information from the knowledge base i.e., use of prior relevant literature to build a

convincing argument about the utility of an artifact. Zhang et al. (2018) evaluated various functionalities of its proposed FHIR blockchain based system i.e., modularity, integrity, access control, trust and identification and authentication through arguments from previous literature. Scenarios represent construction of a detailed synopsis around the artifact to demonstrate its utility (Hevner et al., 2004). van Engelenburg et al. (2019) used an illustration of business to government sharing in the container shipping domain to illustrate how their proposed architecture can be used to share information.

3.2.4.2. Evaluation Methods discussed by Peffers et al. (2012)

Peffers et al. (2012) classified evaluation methods into eight categories:

- *Logical Argument*: Logical argument represents "an argument with the face validity" (Peffers et al., 2012)(p.402). Logical argument is similar to the informed argument category of descriptive analysis in (Hevner et al., 2004).
- *Expert Evaluation*: This method involves experts' validation i.e.; one or more experts assess the proposed artifact (Peffers et al., 2012). Morschheuser et al. (2018) developed a gamification method for engineering a gamified software. To evaluate their proposed method, Morschheuser et al. (2018) developed interviewed 25 gaming experts. The gaming experts were asked to evaluate the gamification method in terms of feasible completeness, feasible validity, feasible understandability, feasible comprehension, and practical utility.
- *Technical Experiment*: This method involves technical evaluation, rather than artifact's performance in relation to the real world. During this method, the performance of an algorithm implementation can be assessed by using real world data, synthetic data, or no

data (Peffers et al., 2012). This evaluation method is similar to the experimental evaluation category of (Hevner et al., 2004).

- *Subject based Experiment*: This method involves the use of human research subjects to evaluate whether an assertion that motivated the development of an artifact is true or not (Peffers et al., 2012).Chen and Lee (2003) interviewed three small business executives to elicit their comments on the proposed system. In addition, three additional business executives were asked to test the prototype of the system and fill out a survey designed to assess the proposed systems ‘usefulness. Wimmer and Yoon (2017) employed human subjects from Amazon Turk to validate their proposed artifact. Lim et al. (2017) evaluated the functionality of their MobileApp by creating a test site similar to a local restaurant and the subject based experiment was conducted to test the utility of the Mobile App. Three local students and three foreign students were invited in the experiment. The local students were given the role of local staff and the foreign students were given the role of visitors. The experiment was conducted in two conditions: first condition, where the participants were allowed to use the mobile app, second condition where the participants were not allowed to use the mobile app. After the experiment, the participants were interviewed to evaluate the effectiveness of the proposed MobileApp.

Oyelere et al. (2018) developed a MobileEdu mobile learning application. To evaluate MobileEdu in a real environment, the authors conducted an experiment with 142 third year undergraduate students in a Nigerian university. The experiment was conducted to validate that the students who learn through MobileEdu accomplish better learning engagements, results and experience better pedagogical experiences than those learnt by attending face to face classes. In addition, the experiment was conducted to assess the attitudes and perceptions of students towards MobileEdu. Ming et al. (2019) recruited human participants on Amazon mechanical Turk to evaluate the interpretability of explanations provided by ProSetNet, an interpretable and steerable deep sequence modeling technique.

- *Action Research*: Utilizing an artifact in a real-world situation as part of research intervention to evaluate its effects in the real world. Fridgen et al. (2018) proposed a blockchain use case (BUC) development method. In developing their method, the authors established a team of researchers and banking practitioners to develop the alpha version of their method. To evaluate their proposed method, the authors conducted workshops with additional practitioners from different domains such as *banking, automotive, construction and insurance.* Through these workshops, the authors received direct feedback, and gathered the qualitative data regarding the quality of their method as well its output. This allowed the researchers to observe the overall nature of their proposed BUC development method and to acknowledge mutually derived changes to the alpha version of their method.
- *Prototype*: Implementing an artifact to demonstrate its utility and feasibility (Peffers et al., 2012). Schweizer et al. (2017) developed a prototype of their proposed solution. The authors implemented crowdfunding platform's software specifications through smart contracts on Ethereum blockchain. Since, the investments are only accepted in ether in Ethereum, Schweizer et al. (2017) developed a smart contract using solidity programming language. Each fundraising auction that represented a student project in a search for funding and associated entities was implemented in a separate smart contract.

  Flory et al. (2017) developed a prototype of the proposed architecture and two algorithms of the IUSLR Analyzer. The prototype included a review spam detector, a user interface, and the backend block. The review spam detector implemented an ASM model that offers an advanced and well accepted spam detection method. The user interface integrated three web 2.0 frameworks: Java script, CSS and XHTML. The backend block integrated five technologies: PHP, R, XML, C++, and MySQL. In addition, the prototype used an internal lexicon base that included 26,000 terms selected from Thesaurus.

Ferdous et al. (2017) developed a prototype of all the components of their proposed decentralized run time access monitoring system (DRAMS) to test its effectiveness. Later, the authors deployed these components on a self-generated cloud federation scenario. The authors used WSO2 Balana, Go programming language to implement the components of access control policy, solidity to implement smart contract, and Node.js a server side Javascript platform to implement Logging interface and Ethereum web3.js an adaptor to interact with blockchain smart contract via a web server. Similarly, Azad et al. (2018) implemented the functionalities of their proposed system in Java programming using bouncy castle cryptographic library.

Lim et al. (2017) developed a prototype of their proposed mobile application named EATJOY by using Axure RP Team Edition 8.0. Axure Team allows creating interactive prototypes of mobile applications with designed functionalities and systems.

- *Case Study:* This method involves applying an artifact to a real-world situation and assessing its impact on the real-world situation. In addition to evaluating the gamification method through expert evaluation, Morschheuser et al. (2018) also used a case study method to evaluate their proposed method. The gamification method was utilized in a gamified software engineering project. The proposed gamification method was successful in meeting its objectives of developing parking maps through crowdsourcing. Abbasi et al.

(2019) used a case study from the perspective of a risk management group at Pfier to evaluate the efficacy of their proposed user generated adverse event detection method. The authors analyzed twenty products from their portfolio, some of which had adverse events such as product recall or drug safety communications. The authors ran their proposed Genetic algorithm-based signal detection (GASD) model on the twitter, search and forum channel in their test bed and computed recall, precision and timeliness.

- *Illustrative Scenario*: Applying an artifact to a synthetic or a real-world situation with an aim to illustrate its suitability or utility. Ferdous et al. (2017) created two different scenarios: The first scenario simulated user interactions and their access control rights in the access control policy. The second scenario simulated a suite of attacks where the users try to access the forbidden service. The authors used JMeter, an open source application to load functional behaviors of the users. JMeter was then configured to define the access controls for each user. Later, the authors used these scenarios to test the resiliency, cost, and latency of implementing their proposed system. Wang et al. (2020) created two scenarios by including some frequently used financial operations to test the privacy preservation analysis of their proposed framework developed to resolve privacy issues in the financial sector.

3.4.2.3 DSR Evaluation Framework

Venable et al. (2012) proposed a DSR evaluation strategy selection framework, a DSR evaluation method selection framework, and a four-step method for the design of the evaluation components in a DSR project.

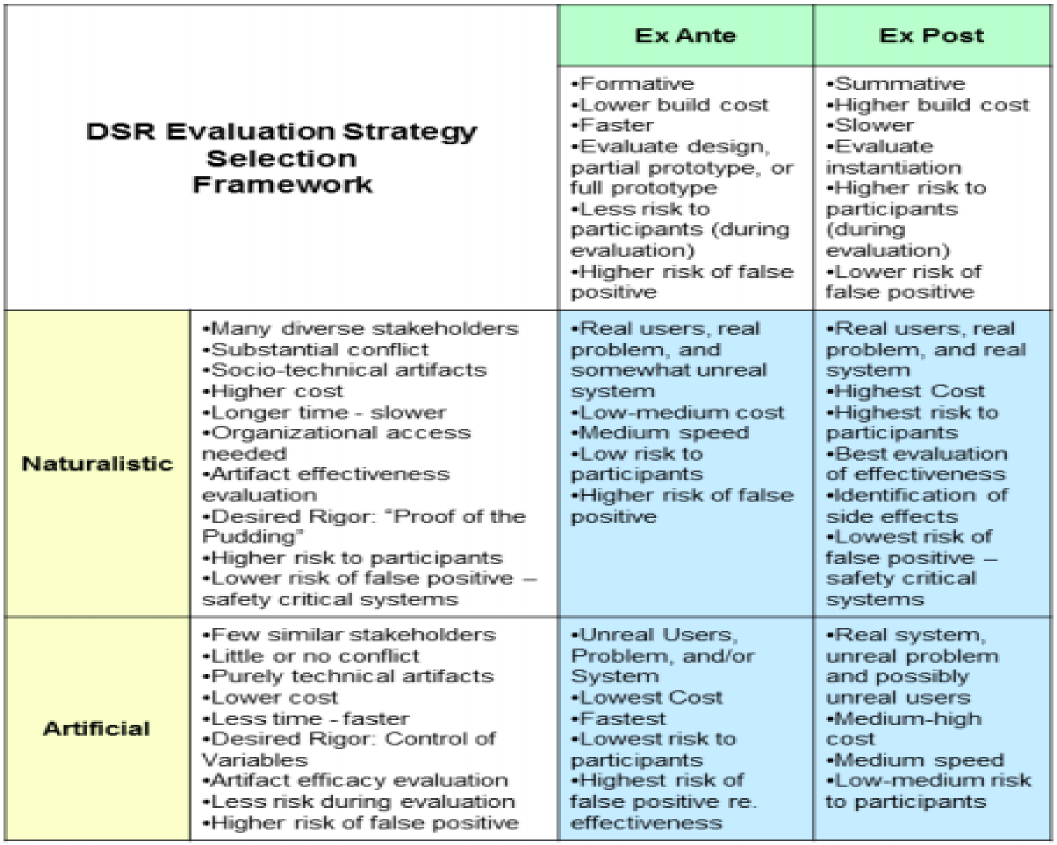
The framework proposed by Venable et al. (2012) is a 2 * 2 framework that combines one dimension contrasting naturalistic and artificial evaluation and another dimension contrasting ex-ante and ex-post evaluation. In addition, it explains the criteria mapped to naturalistic, artificial, ex-ante and ex-post evaluation.

Naturalistic evaluation represents the exploring the performance of the proposed solution in the real-world settings i.e., within the organizations. Real world settings mean real people, real systems, and real settings. It includes all the complexities of human practice in real organizations. It is always empirical and can be positivist, interpretive and/or critical. The naturalistic evaluation methods include field *studies, case studies, surveys, hermeneutic methods, ethnography, phenomenology, and action research* (Venable et al., 2012).

Artificial Evaluation involves "abstraction from the natural setting and is necessarily 'unreal'" (Venable et al., 2012)(p.429). Unreal settings mean unreal people, unreal systems, and unreal systems. Artificial evaluations may include *mathematical or logic proofs, criteria-based evaluation, lab-based experiments, computer simulations, role playing simulations, computer simulations, and field experiments.* Artificial evaluation could include simulated or imaginary settings.

Ex-ante evaluation represents evaluation of an un-instantiated artifact. Ex-ante evaluation can be conducted without building an instantiation initially. *Ex- post* evaluation represents the evaluation of an instantiated artifact.

The white box in the Figure 1 represents the criteria that are mapped to ex-ante, ex-post, naturalistic and artificial evaluation.



DSR Evaluation Strategy Selection Framework		Ex Ante	Ex Post
		•Formative •Lower build cost •Faster •Evaluate design, partial prototype, or full prototype •Less risk to participants (during evaluation) •Higher risk of false positive	•Summative •Higher build cost •Slower •Evaluate instantiation •Higher risk to participants (during evaluation) •Lower risk of false positive
Naturalistic	•Many diverse stakeholders •Substantial conflict •Socio-technical artifacts •Higher cost •Longer time - slower •Organizational access needed •Artifact effectiveness evaluation •Desired Rigor: "Proof of the Pudding" •Higher risk to participants •Lower risk of false positive – safety critical systems	•Real users, real problem, and somewhat unreal system •Low-medium cost •Medium speed •Low risk to participants •Higher risk of false positive	•Real users, real problem, and real system •Highest Cost •Highest risk to participants •Best evaluation of effectiveness •Identification of side effects •Lowest risk of false positive – safety critical systems
Artificial	•Few similar stakeholders •Little or no conflict •Purely technical artifacts •Lower cost •Less time - faster •Desired Rigor: Control of Variables •Artifact efficacy evaluation •Less risk during evaluation •Higher risk of false positive	•Unreal Users, Problem, and/or System •Lowest Cost •Fastest •Lowest risk to participants •Highest risk of false positive re. effectiveness	•Real system, unreal problem and possibly unreal users •Medium-high cost •Medium speed •Low-medium risk to participants

Figure 1 DSR Evaluation Strategy selection Framework; Source: Venable et al. (2012)

Criteria 1: The extent to which the cost and resources restrict the evaluation.

Criteria 2: Whether or not early, formative evaluation is desirable or practicable.

Criteria 3: The extent to which the artifact being designed has to please heterogeneous groups of stakeholders or if there is likely to be conflict, which will complicate evaluation.

Criteria 4: whether the system is purely technical or socio-technical in nature.

Criteria 5: How critical strong rigor concerning effectiveness in real world settings is

Criteria 6: How critical strong rigor concerning whether benefits are particularly due to the designed artifact, rather than some other potential source.

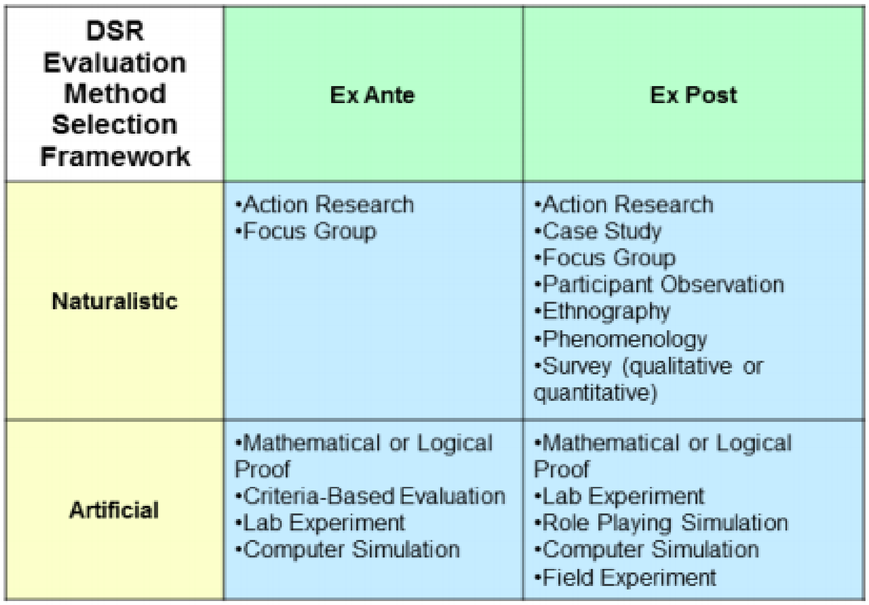
Criteria 7: Whether or not access to a site for naturalistic evaluation can be obtained or available.

Criteria 8: Whether the level of risks to the participants is acceptable or not.

It is very critical to prioritize these different criteria, as they are likely to conflict. For instance: obtaining the rigor in naturalistic evaluation may conflict with the requirement to reduce cost and minimize risks to evaluation participants. If cost and risk minimization override the rigorous evaluation of effectiveness in real world settings, then artificial evaluation strategy may be chosen

The DSR evaluation strategy framework can assist the researchers in identifying relevant, high priority criteria in white and blue cells, which can further help in choosing an appropriate quadrant i.e., appropriate blue cells. The authors advise that it is not advisable to pick a single quadrant, rather than one quadrant can be chosen to resolve the conflicts.

After deciding the evaluation strategy, the next step is to decide an evaluation method for the chosen evaluation strategy. For this, Venable et al. (2012) proposed an evaluation method selection framework. Figure 2 represents the design evaluation method selection framework for each evaluation strategy.



DSR Evaluation Method Selection Framework	Ex Ante	Ex Post
Naturalistic	•Action Research •Focus Group	•Action Research •Case Study •Focus Group •Participant Observation •Ethnography •Phenomenology •Survey (qualitative or quantitative)
Artificial	•Mathematical or Logical Proof •Criteria-Based Evaluation •Lab Experiment •Computer Simulation	•Mathematical or Logical Proof •Lab Experiment •Role Playing Simulation •Computer Simulation •Field Experiment

Figure 2 Design Evaluation Method Selection Framework: Source: Venable et al. (2012)

In addition, Venable et al. (2012) provides four steps to design an evaluation section of the project, which are as follows.

1). Identify, analyze and prioritize the goals of the context of the evaluation. This first step involves additional sub-steps.

a) The first phase involves identification of the evaluands i.e., whether the evaluands will be concepts, models, methods, or instantiation or design theories.

b) The second phase involves determining the nature of the artifact i.e., is the artifact to be produced by a process, product or both. Is the artifact purely technical or socio-technical?

c) Identify what properties need to be evaluated such as whether to evaluate utility/effectiveness, efficiency/effectiveness, ethicality or some other aspects?

d) Determine the objective of the evaluation? Do you want to evaluate the artifact against artifact goals? Do you want to evaluate the artifact against any existing artifacts, or do you want to evaluate the proposed artifact for undesired consequences or for side effects?

e) Identify the research constraints such as what resources are available - time, budget, research site, people?

f) Identify how rigorous the evaluation must be? Is there a requirement to have a detailed rigorous requirement or can it be just preliminary evaluation? Can some parts of evaluation be performed after the conclusion of the project?

g) Prioritize the above contextual factors to determine which aspects are crucial, relevant, more important or less important. Prioritizing these factors will assist in addressing conflicts in evaluation design goals.

2). Match the required contextual factors (from step1) to the criteria in DSR evaluation strategy framework. The contextual factors that match the criteria statements will help determine which quadrant/s applies most. It may be that more than one quadrant applies to your project indicating the requirement for the hybrid methods evaluation design.

3). Select the appropriate evaluation methods listed in the DSR evaluation method selection framework. If more than one box is selected than selecting a method present in more than one quadrant may be helpful.

4). Design the evaluation phase in detail. Ex-ante evaluation will be performed before ex-post evaluation, but if more than one evaluation is performed and more than one evaluation methods are used, in which case the decisions regarding the order of their use and how these different evaluations will fit together must be made prior to the evaluation.

3.3 BEHAVIORAL SCIENCE RESEARCH (BSR) METHODOLOGY

There are two main categories of research that involve human participants: Qualitative v/s Quantitative and Nomothetic v/s idiographic. The research that involves the use of statistical analysis to obtain their main findings is referred to as Quantitative research. The key features of quantitative research include formal and systematic measurement as well as the use of statistics. Qualitative research involves the use of interviews and observations without formal measurements and statistical analysis. For instance: a case study, which involves an in-depth examination of an individual is a form of qualitative study. Nomothetic approach involves the study of groups to determine general laws that apply to large populations. The objective of nomothetic approach is to determine the average performance of a group member or the average member of the group being studied. The idiographic approach involves the study of an individual (Marczyk et al., 2005).

Since, we attempt to answer our second research question: *How do expected positive outcomes and privacy concerns associated with using video-conferencing apps influences* *individuals' decision to continue using video-conferencing apps*? through the use of statistical analysis, we follow a step by step procedure discussed by (Marczyk et al., 2005) in obtaining the key finding for our third research question.

Marczyk et al. (2005) discussed various research designs, the basic processes by which different research studies that involve human participation can be conducted. In this research we focus only on the step by step procedure that a researcher must follow to conduct a quantitative study.

The first step that is common to all the research studies including quantitative study involves selection of a research topic. There are several possible sources of research topics. A research idea may step from researcher's interest in a specific topic, a researcher's motivation to solve a specific problem, from the results of prior research in order to extend the finding of that prior research to different populations or settings or from the existing theories (Marczyk et al., 2005).

3.3.1 Conduct a Literature Review

After selecting a research topic, the first and foremost step is to conduct a thorough literature review in the chosen topic area. The main objective of literature review is to assist researchers in becoming familiar with the work that is already being done and determining the research gap. If a researcher has a research question already in hand, literature review helps the researcher in determining whether the research question has already been answered or not. There are various electronic databases that provide access to existing literature such as Google Scholar, EBSCOhost, Medline, PyscINFO, Web of science etc. Researchers can conduct literature review manually or by using various qualitative tools such as NVIVO, Atlas ti, Quirkos, MAXQDA etc. Other tools that assist researchers in aggregating evidence for research articles for the literature review include: Zotero, MediaWiki, Mendley, Endnote, Wrapping up (Marczyk et al., 2005).

3.3.2 Formulate a Research Problem

Marczyk et al. (2005) listed three criteria that must be met to formulate a good research problem (1). A research problem should describe the relationship between two or more variables. (2). A research problem should be in the form of a research question (3). A research problem must be capable of being verifiable empirically

3.3.3 Articulate Hypotheses

The next step in conducting a quantitative study is articulating the hypotheses. "Hypotheses attempt to explain, predict and explore the phenomenon of interest"(Marczyk et al., 2005) (p.38). The hypotheses should stem from the research problem being studied and must meet two conditions: (1). A hypothesis must be falsifiable i.e., it must be capable of being refuted based on the results of the study (2). A hypothesis must make a prediction i.e.; it should predict the relationship between two or more variables.

There are two categories of hypothesis: Null hypothesis and Alternative hypotheses. Null hypothesis predicts that there is no relationship between variables being studied. Alternate hypothesis predicts that there is a relationship between variables being studied. The number of null and alternative hypotheses included in a specific research depends upon the research question and the scope and complexity of the research. The number of null hypotheses determine the number of research participants that will be required for the study. As the number of null hypotheses increases, the number of research participants required for the study also increases. It is always the null hypothesis that is being tested. It is either confirmed or refuted.

If the null hypothesis is refuted based on the results of the statistical analysis, it means that there is a relationship between the variables being studied (Marczyk et al., 2005).

3.3.4 Selection of the Variables for the Study

"A variable is anything that can take on different values" (Marczyk et al., 2005)(p.42). For instance: height, age, race, attitude can be different for different individuals, therefore they can be referred to as variables. On the other hand, if something can't take on different values, it is referred to as constant.

The most commonly used variables include independent variables v/s dependent variables, categorical v/s continuous variables. Independent variables are the variables that are manipulated or controlled by the researcher. Independent variables are the one that cause or influence the outcome. In contrast, dependent variables are the ones that are influenced by independent variables. Independent and dependent variables can be determined based on the examination of the research problem and related hypotheses. Categorical variables are the one" that can take on specific values only within a defined range of values" (Marczyk et al., 2005)(p. 48). For instance: Gender is a categorical variable i.e., it can take on only two values: male or female. An individual can be either male or female and can't be both. Continuous variables are the one that can take any values between any two values. For instance: Age is a continuous variable. An individual can be of any age. A continuous variable can take the form of categorical variables.

3.3.5 Choice of Research Design

There are three types of research design: Experimental design, Quasi-Experimental and Non-experimental. If the goal of the research is to explain and the research question relates to causal relationships, then the experimental designs are used. If the goal of the research is to describe or predict, then the non-experimental designs are used (Price et al., 2017).

Experimental design represents the design in which research participants are randomly assigned to experimental or control groups. (Campbelli & Stanley, 1963) discussed three true experimental designs: The Pretest-Posttest control group design, The Solomon four group design, and the posttest only control group design. The Pretest-Posttest control group design takes the form of:

R	**O1**	**X**	**O2**
R	**O3**		**O4**

Where R represents random assignment, X represents treatment, and O represents observation or measurements.

In the Soloman Four-Group Design, the subjects are assigned to four different groups: experimental with pre-test and post-test, experimental with no pretest, control with pre-test and post-test and control with no pre-test. This experiment takes the form of:

R	**O1**	**X**	**O2**
R	**O3**		**O4**
R		**X**	**O5**
R			**O6**

The Posttest only control group Design is suitable when the post-tests are not acceptable. This design is similar to the last two groups in the Soloman four group design (Campbelli & Stanley, 1963). This design is expressed as below:

R X O1

R O2

Quasi-Experimental research designs are conducted when random assignment of research participants is not possible. There are two main categories of quasi-experimental designs: nonequivalent comparison group designs and interrupted time-series designs. Non-equivalent comparison group designs represent the design in which the groups are non-randomized, and one group receives the treatment while the other doesn't. Interrupted time series designs represent the design in "which periodic measurements are made on a group prior to the presentation of the intervention to establish a stable baseline" (Marczyk et al., 2005). Non-experimental designs that include both descriptive and correlational designs represent the designs that lack manipulation of independent variables and random assignment of the participants. In this kind of research, the variables are measured as they occur naturally in the real world or the laboratory (Price et al., 2017).

Non-experimental research designs are preferred in many situations including when:

1). The hypothesis or the research question relates to a single variable rather than statistical relationship between two or more variables.

2). The research question relates to a non-causal statistical relationship between variables.

3). The research question pertains to a causal relationship, but the independent variable can't be manipulated, or the research participants can't be randomly assigned.

4). The research question is broad and exploratory (Price et al., 2017).

There are three broad categories of non-experimental research: *cross-sectional research, correlational research, and observational research.* Under Cross- sectional research, the two or more pre-existing groups of people are compared. Under this research, neither the independent variables are manipulated, nor the research participants are randomly assigned. *Correlational research* is considered when the focus of the research is on statistical relationship between two or more variables, but the independent variables are not manipulated. Rather than comparing two pre-existing groups, the correlational research involves correlating two continuous variables. *Observational research* emphasizes making observations of the behavior of an individual in a laboratory or natural setting without manipulating independent variables (Price et al., 2017).

Further, there are four main approaches used in non-experimental designs: *case studies, naturalistic observations, surveys, and focus groups*. *Case studies* represent an in-depth examination of a single individual or a few individuals. *Naturalistic observations* represent making observations of organisms in the natural setting. In *Survey studies,* a large number of individuals are asked questions about their behaviors, opinions and attitudes. When surveys are utilized to determine relationships, they are known correlation studies. "Focus groups are formally organized, structured groups of individuals brought together to discuss a series of topics during a specific period of time" (Marczyk et al., 2005)(p.154).

3.3.6 Data Collection

3.3.6.1. Participant Selection

The selection of research participants is determined by research questions being investigated, the research design being utilized as well as the availability of appropriate number and type of research participants. Since it is not possible to include every member of the population of interest in the study, researchers study a representative subset i.e., a sample of the population of interest. If the sample being studied is representative of the population, then the results obtained with the sample can be used to draw conclusions about the population (Marczyk et al., 2005).

Researchers can choose a representative sample through probability sampling method and non-probability sampling method. Random techniques are also known as probability techniques such as *simple random sampling* and *stratified random* sampling. Simple random sampling represents the procedure through which each member of the population of interest has an equal chance of being selected. *Stratified random sampling* represents the sampling method "in which subjects are placed into groups ahead of time according to a variable that strongly influences the outcome (eg, presentation with incomplete facial paresis vs complete facial paralysis). Randomization of each stratum occurs separately in stratified random sampling" (Slattery et al., 2011) (p. 833).

Non-probability methods include *convenience sampling* and using *an index person* for introduction to other individuals. Convenience sampling relies on easily obtained subjects or volunteers (Slattery et al., 2011).

3.3.6.2. Instrument Development

"Measurement can be described as the process through which researchers describe, explain, and predict the phenomenon and constructs of our daily existence" (Marczyk et al., 2005)(p. 95). Measurement allows researchers to measure abstract constructs and variables of interest. Variables in a research study must be operationalized before being studied.

Barkman (2002) listed three main instruments that can be used for data collection in quantitative research: Tests, Surveys/Questionnaires, and Observation checklists. Tests may be used to ask the respondents about the awareness or what is true or factual. Tests are generally used for knowledge-based questions and offer choices such as accurate v/s inaccurate or correct v/s incorrect. Surveys/Questionnaires are used to acquire information about what individuals do, what individuals have, what they think, know, feel. They can be used to measure skills, knowledge, behavior, attitudes, and practice. Observation checklists enable the evaluator to observe how an individual behaves in a social setting.

Since we will be using questionnaires in our research, we will describe what the questionnaire is. In addition, we will describe how questions for a questionnaire can be designed and also how the structure and order of the questions should be determined.

Questionnaire also referred to as an instrument consists of a series of self-administered questions. The questions include items or specific concepts of interest considered worthy of investigation and can be communicated in a variety of ways such as via email, internet or even read to research participants (Slattery et al., 2011). Slattery et al. (2011) discussed key points that need to be considered when building a questionnaire:

A questionnaire need not be developed from scratch. Pre-existing questionnaires are often adapted or used directly for various uses.

In some cases, if there are no pre-established questionnaires for a given objective, then a new questionnaire needs to be built. When designing new questionnaires, items need to be agreed upon by experts in the field.

Once the items are agreed upon, the next step includes structuring the language of items. It is the language of the items that helps obtain maximus information from the research participants. The language of the questions should be concrete, simple and easy to understand. The questions should avoid biased phrases.

The questions in the questionnaire can be of two categories: closed ended and open ended. Closed ended questions can be multiple choice or either yes or no. Closed ended questions enable ease of scoring and comparison of results from scoring. But closed ended questions may decrease the breadth of response and can take an unnatural form. In contrast, closed ended questions enable respondents to fill in responses that enhance individuality and accuracy.

The questions can be categorized by types of responses such as nominal, ordinal or continuous (described later).

The order of the questions should also be taken into consideration. The introduction including initial questions should be simple and clear. Initial questions should be closed ended for attention grabbing. Keep the closed ended questions to minimal. Place the demographic questions at the end (Slattery et al., 2011).

There are two categories of data: Metric and non-metric data. Metric data aka quantitative data exists in varying amounts or degrees and reflects distance or quantity. It enables researchers to examine magnitude and amounts. In contrast, non-metric data is the data that can't be quantified and can be used to describe and categorize. Further, there are two main non-metric scales: nominal scales and ordinal scales. Nominal scales are only used to quantitatively classify or categorize and are least sophisticated scales of measurement. Ordinal measurement scales measure the variable in terms of both identity and magnitude. Both nominal and ordinal data are qualitative in nature and lack mathematical properties necessary for sophisticated statistical analysis. Further, metric measurement scales have two categories: interval scale and ratio scale. Interval scales build on the ordinal measurement. The variables in the interval scale are measured in actuals, not in relative manner. Interval scales don't have absolute zero point i.e., the presence of zero is arbitrary. Lack of absolute zero makes the multiplication and division impossible. It equates distance or interval between two variables i.e., subtraction is defined between two variables. In contrast, ratio scales have absolute zero points. Therefore, all mathematical operations are possible in ratio scales.

3.3.7 Data Analysis

This phase involves three steps: (1) Preparing the data for analysis. (2) Statistical analysis (3) Interpreting the data (Marczyk et al., 2005).

3.3.7.1. Preparing the Data for Analysis

Due to the critical nature of the data, the data should be treated with utmost care and respect. The research data should be collected according to the policy. The research data should be stored in such a way that it ensures security and confidentiality. Hence following steps are the key steps that a researcher must follow (Marczyk et al., 2005).

- *Track and log the data collection*

Tracking and logging of the data provides up-to-date information throughout the research participants throughout the study. This can be done using several databases such as: MS Excel, SPSS, SAS. The recruitment log records the number of individuals approached for research participation. The recruitment log keeps track of participants' enrollment and to determine how representative the resulting participants are of the population the researcher is trying to investigate.

- *Data screening: Data* screening ensures that responses are eligible, complete, within an acceptable range, and all the necessary information has been included. Data screening can be done manually or electronically. Computerized assessment instruments check for the skipped fields or blank fields i.e.; it can be programmed in such a way that only responses within a certain range are accepted.
- *Constructing a Database:* Once data is screened, the data should be entered into the database. It would be beneficial to think backwards by anticipating how data will be analyzed. This will help researchers in determining the variables that need to be entered, the order of the variables, and how they will be formatted.
- *Data Codebook:* A comprehensive data code book is essential during data analysis. A data codebook is a written or a computerized list that provides a clear and comprehensive description of the variables used for the study. Lack of a comprehensive data code book may make a database unpredictable and useless.
- *Data entry:* Data entry means inputting the data into the database. One way to ensure accurate data entry is through a double entry procedure. In the double entry procedure, data is entered twice, and the data is compared to see any discrepancies. Another way to check the accuracy of the data entry is to design standard procedures. These procedures involve careful review of the inputted data for missing values, out of the range values, and incorrect formatting. Many databases such as MS excel, SPSS allow the researchers to define the ranges, types of data and formats.

- *Transforming the data:* This phase involves transforming the data before analysis. The transformation of the data involves identification and coding missing values, computation of total and new variables, reversing of the scale items, recoding and categorization of some variables.

3.3.7.2**.** *Empirical Analysis*

Structural equation modeling can be used to empirically assess the research model. To study the conceptual models that have not been tested before, partial least squares, a variance-based technique is more appropriate (Ke et al., 2009). There are various software systems available to evaluate the reliability and validity of measurement models and analyze the structural model. And smart PLS software is widely used.

In behavioral research, the researchers develop constructs from an underlying reality and hypothesize the relationships between those constructs. The set of the constructs and the relationship between them is known as a structural model. In addition, the researchers use various indicators to measure each of the constructs used in the study. The set of measures of all constructs as well as the proposed relationship between indicators and constructs is referred to as a measurement model (Goodhue et al., 2012).

The primary purpose of empirical analysis is the same for all researchers: to confirm that the measurement model is adequate in the terms of reliability and validity, to generate the path strengths in the structural model and to establish the statistical significance of those path estimates.

1. *The Measurement Model*

The measurement model has two categories: Reflective and Formative model (Lehner & Haas, 2010). In the reflective model, the latent construct is existing i.e., it exists independent of the indicator variables. In a formative model, the latent variable is determined by the combination of the indicator variables (Coltman et al., 2008). Reflective models show the causality from the latent variables to the indicator. In reflective models, the value of indicator variables is determined by the construct value. If the construct value changes, then the value of indicator variables also changes. This also means that the indicators are interchangeable and the elimination of one indicator variable would not affect the construct. To increase the measurement model's validity, the indicators with lower correlating variables should be eliminated (Coltman et al., 2008; Lehner & Haas, 2010). Formative models show the causality from the indicator variables to the latent construct. Adding or dropping an indicator variable can impact the conceptual domain of the construct (Coltman et al., 2008).

The indicators in the formative model should have high positive inter-correlations. The empirical test that can be used to test the inter-correlations can be done through internal consistency and reliability. The internal consistency and reliability can be assessed via Cronbach alpha, average variance extracted, and factor loadings. In reflective models, the items can have any pattern of inter-correlationships but should possess the same directional relationship. In the formative model, indicator reliability can't be assessed empirically (Coltman et al., 2008).

In reflective models, the indicators have similar i.e., whether positive, negative, or significant or non-significant relationships with the antecedents/ consequences as the construct. The item relationships with construct antecedents and consequences can be accessed via content validity (Coltman et al., 2008). Content related validity relates to the relevance of the measurement strategy or the instrument to the construct being studied (Marczyk et al., 2005). Content validity can be assessed empirically via convergent validity and divergent validity.

Convergent validity takes two measures that purportedly captures the same construct and shows that they are related. Divergent validity shows that two measures that are not purportedly related to each other are in fact not related to each other (Marczyk et al., 2005). In formative models, the indicators may not have a similar significance of the relationships with the antecedents or the consequences as they don't share a common theme. There are three approaches that can be used in case of formative models: relating the indicators to a simple overall index variable, multiple indicators and multiple causes model, or structural linkage with another criterion variable (Coltman et al., 2008).

In the reflective model, the measurement error for each indicator can be identified and eliminated using common factor analysis. Common factor analysis can be used to identify and extract measurement error (Coltman et al., 2008). In the case of a formative model the only approach to overcome the measurement error is "to design it out of the study before collecting the data" (Coltman et al., 2008)(p.10).

2. *The. Structural Model*

The structural model is used to indicate how the latent variables are related. The structural equation model is specified to determine the extent to which the a priori hypothesized relationships are supported by the obtained data (Schumacker & Lomax, 2004).

The researchers have three alternatives for statistical techniques for :an analysis with equally weighted composites such as regression, latent variables analysis a CB-SEM technique such as LISREL, or the analysis with composites employing optimized weights(PLS) (Goodhue et al., 2012).The choice of the statistical technique should be compatible with the research question being investigated. Out of these three, the PLS method has been used frequently in IS research and is advantageous at small sample sizes. The main concern of a behavioral researcher when choosing a statistical technique is “the relative efficacy of the different statistical techniques in terms of their path estimate accuracy, their statistical power, and the extent to which they are subject to false positives” (Goodhue et al., 2012)(p.708).

Accuracy can be determined by average bias which can be further computed by subtracting the true path value from the average path estimate and then dividing the resulting output by true path value. The ideal accuracy has a zero bias (Goodhue et al., 2012).

Statistical power for a given path can be determined by counting the number of statistically significant path estimates and dividing by the number of data sets in each sample. Since the statistical power will be in proportion, the standard deviation around a proportion value can be calculated. A statistical power value of 0.80 or more is the accepted value. The false positive for each statistical technique can be calculated by including a zero path (a construct that has no impact on the dependent variable) in the underlying research model and testing whether each technique indicates that zero paths are statistically significant. All such zero paths are false positives and no more than 5 percent of false positives are acceptable (Goodhue et al., 2012).

First of all, the input data needs to be standardized. When the input data is not standardized, the researchers using PLS or LISREL need to be mindful of the mismatch of parametrization. Indicator values are only estimated in PLS, whereas in regression, they are pre-specified. The LISREL method doesn’t estimate indicator weights. The indicator weights in PLS can be calculated by three structural model weighing schemes: centroid weighting scheme, factor weighting scheme, and centroid weighing scheme (Goodhue et al., 2012). Out of these three schemes, a path weighing scheme is the recommended approach. Path recommended approach provides the highest R2 value for endogenous variables. Centroid weighting scheme should not be used when the path model includes high order constructs often known as second order models.

In the PLS and LISREL method, researchers can choose both *formative* v/s *reflective* measurements. But reflective measurements are the most commonly used method in IS research. In PLS and regression, the indicator co-variances are assumed to be zero. In LISREL, the researchers have the choice to specify or estimate the indicator co-variances. Exogenous construct correlations are estimated in PLS and regression, whereas they are optional in the LISREL method. PLS algorithms for weights and ordinary least squares (Jacoby & Olson) for path estimates are the two estimation methods used in the PLS method. For the LISREL, maximum likelihood (ML) is the most common approach. The researchers use bootstrapping, the recommended approaches to determine the standard deviations in PLS method (Goodhue et al., 2012).

CHAPTER 4 BLOCKCHAIN BASED COLLABORATIVE HEALTH INFORMATION EXCHANGE

4.1 INTRODUCTION

As health information is shared across different health care institutions, its semantics must be consistently maintained in order to maximize its value and usage (DeSalvo, 2015). This is referred to as semantic interoperability. Semantic interoperability provisioning in healthcare institutions is pivotal. However, due to lack of adoption of a single authoritative standard, semantic interoperability still poses a major challenge (Ali & Chong, 2019; Batra et al., 2015; do Espírito Santo & Medeiros, 2017). The lack of semantic provisioning in healthcare systems further obstructs the automated and seamless exchange of patients' data across healthcare institutions (Ali & Chong, 2019; do Espírito Santo & Medeiros, 2017) as well as limit the utility of the health and patient data (Peterson et al., 2016).

Healthcare institutions have been gradually transitioning from paper based patient medical records to digital records by implementation of Electronic Health Records (Naveed et al., 2020). Since patients' visit various healthcare providers during their lifetime, cross-institutional EHR sharing for its collaborative use is very crucial to enable effective patient care (Zhang et al., 2018). The collaborative use of EHR has the potential to not only enable comprehensive and timely overview of patients' health (Peng and Goswami, 2019), but also provide efficient and coordinated delivery of patient care as well as cost savings through reduced manual errors (Jabbar et al., 2020) and duplicative tests respectively (Jabbar et al., 2020; Payne et al., 2019).

Despite the need for collaborative use of EHR, the healthcare domain has encountered failure in cross-institutional EHR sharing (Naveed et al., 2020). There exist three main barriers in healthcare technical infrastructure that obstruct the cross-institutional EHR sharing and consequently its collaborative use. These barriers include (1) security and privacy concerns of patient data during virtual transmissions of EHR (Duong-Trung et al., 2020; Zhang et al., 2018), (2) lack of trust amongst healthcare institutions EHR (Duong-Trung et al., 2020; Zhang et al., 2018), (3) and lack of semantic interoperability amongst different healthcare information systems (Adel et al., 2019; Ali & Chong, 2019; Dridi et al., 2020; Peng & Goswami, 2019; Satti et al., 2020).

Despite the need for cross-institutional data sharing, concerns remain regarding protecting the privacy and security of patient data (Duong-Trung et al., 2020; Zhang et al., 2018). For secure exchange of EHR across cross-institutions, confidentiality, authentication, data integrity and an auditability of accessed information remains the primary objective of any healthcare system (Hasselgren et al., 2020; Jabbar et al., 2020). Virtual environments, where face to face interactions are replaced by virtual (network) interactions are highly susceptible to medical identity thefts (Zhang et al., 2018). Virtual transmission of EHR without a highly secure network infrastructure in place poses a greater risk for pilfering of EHR (Duong-Trung et al., 2020; Zhang et al., 2018), inflicting severe losses to healthcare institutions including fines, litigations (McLeod & Dolezel, 2018), and loss of public trust (Hasselgren et al., 2020), precluding the healthcare institutions to share data across their borders.

Trust is an essential condition for digital communications and data sharing in the healthcare domain. Healthcare institutions need to identify and trust each other’s identities before making any cross-institutional interactions and data exchange. Trust is difficult to establish when the data receiving healthcare institutions don’t share the same health system with the shared provider directory or the communications between them are not established yet

(Duong-Trung et al., 2020; Zhang et al., 2018). For instance, public v/s private hospital. Larger public healthcare institutions may be networked, but communications between smaller and private institutions may not be established (Duong-Trung et al., 2020; Zhang et al., 2018), thereby precluding the cross-institutional EHR exchange.

Interoperability among healthcare information systems is very crucial in order for healthcare institutions to exchange and understand data and ultimately make its collaborative use (Ali & Chong, 2019). However, EHR are usually stored using different standards (Ali & Chong, 2019; Roehrs et al., 2017), in distinct systems (e.g., standard base databases, local databases such as MySQL, SQLServer, DB2, Oracle with different schemas, XML files, data files etc (Adel et al. 2019) in different healthcare institutions, making it difficult to exchange EHR across healthcare institutions. Furthermore, EHR in these sources may be represented using different identifiers/naming conventions (e.g., An element might be called "Physician" in one data source, whereas it might be called "Doctor" in another) (Tanwar et al., 2020), different units of measurement (e.g., measurement of height in inches v/s in feet), and aggregated differently (e.g., date is represented using separate attributes i.e., month, date and year in one data source, whereas it is represented as combined attribute in another) (Adel et al., 2018). Distinct illustration and representation of the same information in different EHR sources leads to differences in semantics (Adel et al., 2019), ultimately restricting compatibility and data comprehension (Sri & Bhaskari, 2020). This could further obstruct the healthcare information systems to automatically interpret the information exchanged without additional effort.

Hence, heterogeneity in the adoption of standards, systems as well as representation and illustrations of EHR leads to uninterpretable healthcare information systems (Adel et al., 2019; Dridi et al., 2020; Satti et al., 2020), thereby making the health data become data silos and only accessible and usable in their respective places with little or no interoperability with others (Peng & Goswami, 2019; Roehrs et al., 2017).

Several studies have emerged proposing a diverse range of blockchain based solutions to address the issues above. However, many solutions rely on enforcement of one specific standard (e.g., Fast healthcare interoperability resource aka FHIR) for EHR sharing across various healthcare institutions (Azaria et al., 2016; Dwivedi et al., 2019; Hylock & Zeng, 2019; Ivan, 2016; Kaur et al., 2018; Peterson et al., 2016; Wang et al., 2018; Yang et al., 2019; Zhang et al., 2018). While these approaches may perform well for the information systems built using that specific standard but may not be compatible for the information systems built using different standard (e.g., information systems built on other standards such as HL7 v2). The fact that no single standard is capable enough to support all the needs of the healthcare organizations and each standard offers variety of distinct features which makes it more or less appealing to healthcare based on their needs (Lyniate, 2019), the prior solutions that rely on normalizing heterogeneous databases through enforcement of one specific standards may not be adopted by healthcare institutions whose healthcare information systems are built using standards other than the one enforced by the prior solutions. For instance: FHIR, a version of HL7 standard offers high speed, bandwidth, and efficiency that makes it appealing to the institutions that require real time data exchange. But for healthcare use cases that don't require higher bandwidth or real time data exchange, HL7 2.0 is widely adopted (Lyniate, 2019).

Taken together, the above situation demands a network infrastructure that offers a secure and interoperable exchange of EHR in a situation where communications between healthcare institutions have not been established and the healthcare institutions are using distinct protocols (i.e., distinct standards and systems) and identifiers to store and represent EHR. Considering the above issues, the objective of this study is to answer:

How may a system be designed to enable secure and interoperable exchange of EHR across healthcare institutions in a situation where healthcare institutions know each other, but don't fully trust each other and are storing and representing the same health information using distinct protocols and naming conventions?

We answer the above research question by proposing a novel architecture named blockchain based collaborative health information exchange (BCHIE), which relies on key properties of blockchain and semi-ontology mapping to enable secure and interoperable cross-institutional EHR exchange. With some of its key attributes such as decentralization, immutability, transparency, and ability to cut middle man, blockchain has many appealing properties that can be used to enhance and obtain high level of data sharing, confidentiality, authentication, data integrity, auditability and transparency among the healthcare institutions, thereby creating a virtual and secure infrastructure for building and maintaining trust (Hasselgren et al., 2020). With its capability to resolve semantic heterogeneity by identifying semantic correspondences between entities of different ontologies (Adel et al., 2019; Kaza & Chen, 2008), ontology mapping can be useful in various tasks such as query answering, ontology merging, and/ or data translation (Song et al., 2017).

The proposed architecture (1) relies on permissioned blockchain to enable secure and reliable exchange of EHR virtually as well as maintain trust amongst the healthcare institutions; and (2) utilizes semi-ontology mapping to generate semantic mappings between entities of candidate ontologies of different healthcare institutions and later use those mappings to translate the incoming message from source party format to destination party format to resolve semantic interoperability conflict

4.2 METHODOLOGY

This is a design science study and as such it will result in an artifact, in this case, an architecture named blockchain based collaborative health information exchange system (BCHIES). This study follows the design science guidelines proposed by (Hevner et al., 2004).

- *Design as an artifact***:** The study presented an architecture named BCHIES for secure and interoperable HIE.
- *Problem Relevance*: The study reviewed the past literature which clearly indicates that security and semantic interoperability is still a major challenge in the healthcare domain.
- *Design Evaluation*: The study presented an architecture named BCHIES that will be evaluated using an illustrative scenario and informed arguments.
- *Research Contribution*: The study provided a definition, an illustration and evaluation of the proposed architecture BCHIES.
- *Research Rigor*: The design rationale for an artifact can be based on kernel theories, previous artifacts of various nature including models, methods, framework, guidelines, architecture, logic, principle and meta-model (Thakurta et al.,2017). Hence, this study utilized *the office of the national coordinator of health information (Carneiro et al.)'s guidelines* on security and semantic interoperability in the healthcare domain, ontology mapping and security literature to define, build and justify the proposed solution.
- *Design as a Search Process*: The study used ONC's guidelines, previous literature on ontology mapping, blockchain, encryption techniques and other relevant literature to inform the design of BCHIES.
- *Communication of Research*: The study presents the results to the research community in the form of a conference paper.

4.3 RELATED WORK

Our review of prior literature consists of two sections. The first section reviews prior blockchain based solutions on secure and interoperable healthcare data sharing. We highlight the novelty of our design artifact within the blockchain space, in particular by identifying gaps in the prior literature and the second section provides a background on blockchain and semi-ontology mapping and an assessment of applicability of both blockchain and semi-ontology in our proposed solution.

4.3.1 Blockchain based Solutions on Secure and Interoperable Healthcare Data Sharing

Azaria et al. (2016) proposed a blockchain system named MedRec that uses generic strings for data sharing and retrieval. The use of generic strings allows MedRec to interface with providers' existing local data storage solutions hence resolving system interoperability conflict. However, the proposed system doesn't address how the record a transaction reference to is meaningfully interpreted by systems using different EIES.

Peterson et al. (2016), Sri and Bhaskari (2020), and Margheri et al. (2020) proposed a system proposed a blockchain based framework which utilizes Fast Health Interoperability Resources (FHIR) standard as an exchange format for HIE in the network. In both the studies, the participating nodes reach network consensus through proof of interoperability. The proof of interoperability requires the nodes to provide a proof that the incoming data is interoperable with regards to the known set of structural and semantic constraints. These structural and semantic constraints are facilitated through the FHIR profiles. FHIR profiles are the mechanisms that can be further utilized to constrain a FHIR resource by introducing a model for computable compliance statements. The compliance is both structural and semantic, enabling not only structural constraints on attributes such as data type and cardinality, but also semantic constraints of value sets. Under proof of interoperability, the network consensus is not achieved programmatically, rather using human based processes, where participating nodes negotiate and collaborate with the assistance of both clinicians and terminology specialists.

Achieving consensus over an allowable set of profiles manually can be both time consuming and labor intensive.

A study by Zhang et al. (2018) enforced the use of the FHIR standard to share clinical data in their proposed blockchain based solution named FHIRChain. FHIRChain employs a cryptographic public and private key pair to create digital signatures and identities of the participating providers. Similarly Hylock and Zeng (2019) proposed a patient centric blockchain system that uses proxy re-encryption to share information through smart contracts. The proposed solution uses the FHIR standard to exchange patients' records.

Yang and Yang (2017) also resolved semantic interoperability challenges by requiring the healthcare institutions to agree on the same standard for expressing electronic health records (EHR). Lyniate (2019) notes that each healthcare standard offers a variety of distinct features that makes them more or less appealing to the healthcare institutions based on their needs. FHIR offers high speed, bandwidth and efficiency that makes it appealing to the organizations that require real time data exchange. But for healthcare use cases that don't require higher bandwidth or real time data exchange, HL7 2.0 is widely adopted (Lyniate, 2019). The fact that the healthcare institutions can adopt different healthcare standards based on their needs and even implement a single standard in different ways (Lyniate, 2019), the proposed solutions that mandates the use of a specific standard may pose adoption issues.

Similarly, Ivan (2016) proposed a conceptualized blockchain based patient centric personal health record (PHR) solution that enforces consolidated clinical document architecture (C-CDA) generated documents for sharing data across various EHR systems. Since there may be variations in implementation of C-CDA from EHR to EHR, healthcare institutions might not be able to exchange information accurately, which is a barrier to interoperability (Lyniate, 2019).

Kaur et al. (2018) proposed a framework that integrates blockchain and cloud computing for storing, transferring, sharing and processing healthcare data. The transaction between each node is stored using a series of signatures called e-stamp. However, the study doesn't explain how the heterogeneity issues will be resolved if the two healthcare institutions are using different standards or interpreting data differently such as using different naming conventions.

The study by Wang et al. (2018) proposed a blockchain based framework that combines the Ethereum blockchain, decentralized storage system, and attribute-based encryption to achieve fine grained access control over the data in decentralized systems. Similarly Dwivedi et al. (2019) utilizes Ethereum blockchain, decentralized storage systems to secure and anonymize patient data. The proposed solution uses ring signatures for signing messages. Both Wang et al. (2018) and Dwivedi et al. (2019) 's work focuses only on security and privacy and don't address semantic interoperability issues.

The review of the literature concludes that there is no such study that has resolved security and semantic interoperability challenges in the healthcare domain by providing the flexibility to the healthcare institutions to adopt the healthcare standards of their own choice and still receive interoperable healthcare records from other healthcare institutions in a secure and reliable manner.

4.3.2 Blockchain

Blockchain was first introduced by Nakamoto (2008) as a completely decentralized electronic money trading system (Liu & Li, 2020). Blockchain can be described as an immutable ledger that records transactions (data entries) in a decentralized fashion i.e., there is no centralized trusted third party that controls the content added on the blockchain. Instead the transactions broadcasted on the blockchain are agreed upon in a peer to peer fashion through consensus mechanism (Hasselgren et al., 2020). This immutability property of blockchain ensures that the transactions (data entries) that are considered valid by the network nodes can no longer be altered or deleted (Carvalho, 2020). Blockchain's encryption mechanism that involves encrypting data (the identification of the parties exchanging data and the content) before sharing on the distributed ledger enables secure information sharing across different parties. The verification of the transactions by multiple nodes, the process of immutable record-keeping, and encryption mechanism enhances trust between the organizations that don't fully trust each other (e.g., private organizations and government agencies (Ølnes et al., 2017).

The ledger in blockchain is replicated across the whole network such that every node on the blockchain network has an identical copy of the ledger (Agbo et al., 2019). This property of blockchain makes the hacking and unauthorized changes extremely difficult to make without getting noticed thereby preventing fraud, manipulation, and corruption (Ølnes et al., 2017). In addition, storing the data at multiple nodes ensures that information is changed only when all relevant parties agree (Ølnes et al., 2017).

In blockchain, each new block in the blocklist is linked to the previous block by including the hash of the latter and in this manner, forming a complete chain from first to last block (Hasselgren et al., 2020; Roehrs et al., 2017). The process of chaining the blocks together ensures that the transactions are time stamped, thereby forming an audit trail of who did what and when (Agbo et al., 2019). Being able to keep track of transaction history and audit trail ensures transparency and auditability in the business process (Ølnes et al., 2017).

4.3.4 Types of Blockchain

Blockchain are of two types: permissionless blockchain and permissioned blockchain. In permissionless blockchain, anyone can join the network and everyone on the network has the access to view the transactions (data entries) as well as participate in the consensus protocol (Hasselgren et al., 2020). This means that the transactions (are public, but users remain anonymous in that they are identified by their pseudo identities (Carvalho, 2020). However, anonymity (pseudo identities) and transparency (everyone can view the data) aspects of public blockchain might cause some serious privacy problems in the domains such as healthcare because the healthcare data is highly sensitive, and it can only be shared across known and authorized entities (Ølnes et al., 2017).

Unlike permissionless blockchain, in a permissioned blockchain, a permissioned network is created in which only known and vetted participants have the permission to join the network (Carvalho, 2020). Permissioned blockchain are appropriate where the group of members know each other, but might not fully trust each other (Carvalho, 2020). This is precisely the case with the healthcare domain, which is the focus of our paper. Further, permissioned blockchain can be categorized into public permissioned blockchain and private permissioned blockchain. Depending upon whether public verifiability (i.e., any node in the network can verify the correctness of the state of the system) is required, anyone can be allowed to read the state of the system in public permissioned blockchain, whereas in private permissioned blockchain, only selected participants have the permission to verify the state of the system (Wüst & Gervais, 2018). Private permissioned blockchain replaces anonymity by privacy, in the sense that not everyone has the access to the transactions involving a specific node (Carvalho, 2020).

4.3.5 Assessment of blockchain in our proposed solution

Blockchain doesn’t make sense in every situation. Wüst and Gervais (2018) introduced a decision model that has been used in various studies (e.g., (Carvalho, 2020)) as an assessment to use blockchain and select and design appropriate blockchain systems (See figure 1).

First and foremost, blockchain is about data storage. If no data storage is required, then blockchain is not required. To exchange data with other institutions in the healthcare domain, data integrity and provenance is crucial (Hasselgren et al., 2020). Data provenance in healthcare implies that healthcare institutions are required to maintain historical record of the data and their origins to deliver auditability and transparency in EHR (Hasselgren et al., 2020). Blockchain creates an immutable audit trail that permanently stores transactions, so that the critical transactions (e.g., patient EHR access log or with whom data is shared) are always available for anyone in the network to examine (Kuo et al., 2019).

Second, if there is only one user, then a centralized database, as opposed to a blockchain system performs better in terms of throughput and latency (Wüst & Gervais, 2018). In our specific problem, several healthcare institutions should be able to exchange data across each other, the historical record of which will be stored in the blockchain.

Third, if a centralized third party is trusted, then blockchain is not needed (Wüst & Gervais, 2018). To enable electronic data sharing across healthcare institutions in a secure manner, current healthcare infrastructure relies on centralized third-party intermediaries (Patel, 2019). For instance: to overcome the shortcomings of physical media transfer, the Radiological Society of North America developed an image sharing network in which the participating institutions share data across each other through a third-party clearing house. The participating institutions upload the media (medical images to be shared) to the clearinghouse, where they are stored and indexed by a cryptographic hash of a secret token for 30 days. Although, RASA addressed the issue of physical media exchange across sites, it poses another issue in that the provider fulfilling the role of clearing house now has the access to patient's sensitive data and the internal or external malicious actors in that clearing house may compromise the network, potentially gain access to patient data (Patel, 2019), alter the images, edit and manipulate the existing transactions etc. In addition, the clearing house can exert significant control over which PHR vendors can have access to the information sharing network (Patel, 2019). The ledger replication in blockchain eliminates the problem of network dominance and data stewardship by a centralized service provider along with the problems of high network latency and a single point of failure (Ismail & Materwala, 2019). In such instances, blockchain is suitable for applications where independently managed healthcare stakeholders (e.g., hospitals, providers, payers, patients etc.) wish to collaborate with one another without ceding control to one centralized third-party intermediary (i.e., keeping full control of their own computational resources) (Kuo et al., 2017). While centralized databases support various functions such as create, read, update, and delete functions, the blockchain only supports create and read functions (i.e., it is very difficult to alter the record or data). In addition, the ownership of the digital assets can be easily modified by system administrators in the centralized databases, while on blockchain, the ownership of the data can only be changed by the owner itself, and origins of the data ownership are easily traceable through validated transactions (Kuo et al., 2017). Hence, blockchain is suitable as an immutable ledger to record critical information such as history of transactions (e.g., insurance claim records, EHR access or exchange records) that can be shared across multiple nodes thereby decentralizing the power and enhancing trust (Kuo et al., 2017).

Lastly, if the users are unknown, mutually trust each other, and public verifiability of the transactions is required, then public blockchain is likely the most effective solution (Wüst & Gervais, 2018). Permissioned blockchain systems are most effective where the users are known, but trust between them is not fully established. This is precisely the case with different health care institutions such as public and private hospitals, which is the focus of this paper. Since, in permissioned blockchain system, all “the participants do not necessarily have permission to retrieve information about the transactions in the network (Carvalho, 2020)(p.1), in our case, several permissions will be defined so that the network is only accessible to vetted and registered healthcare institutions, with different healthcare institutions having different views of the transactions, hence protecting patients’ privacy.

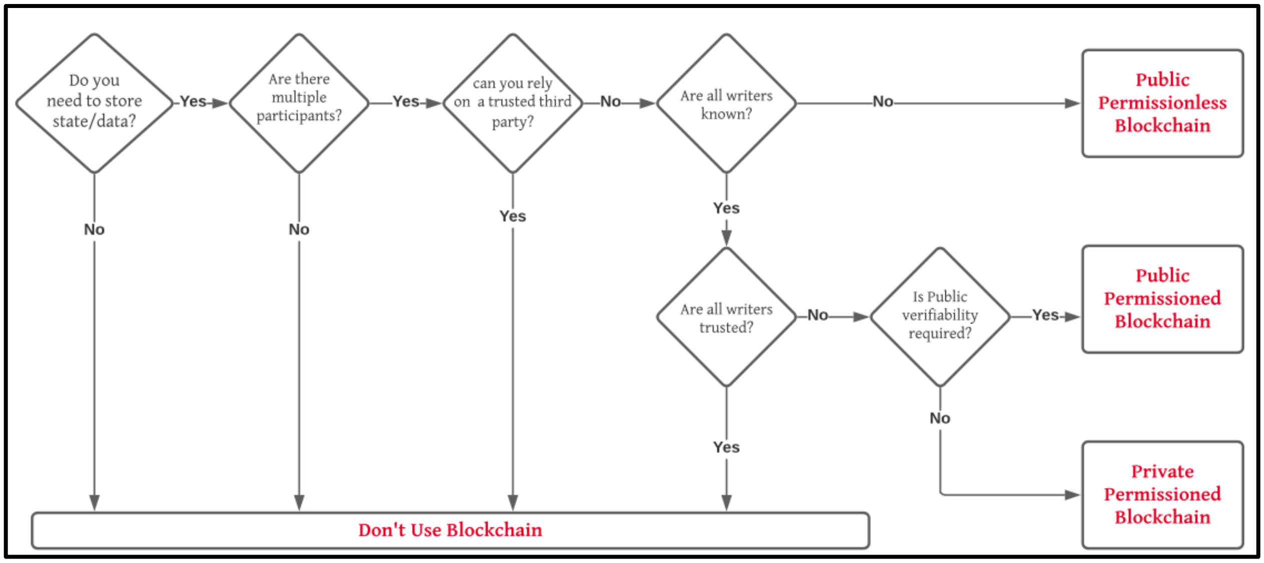

Do you need to store state/data?
Yes
Are there multiple participants?
Yes
can you rely on a trusted third party?
No
Are all writers known?
No
Public Permissionless Blockchain
No
No
Yes
Yes
Are all writers trusted?
No
Is Public verifiability required?
Yes
Public Permissioned Blockchain
No
Yes
Private Permissioned Blockchain
Don't Use Blockchain

Figure 3 Blockchain adoption decision model adapted from (Wüst & Gervais, 2018).

4.3.6 Ontology Mapping

Ontology, an abstraction of reality, provides a formal description of a set of entities within a domain or artifact and through a systematic descriptive process represents the relationships and constraints between those entities (McMurray et al., 2015). Ontology is application specific, and when it is required for two applications to communicate with each other in order to resolve a problem interactively, it is needed that they are able to map their semantic domains (Karimi & Kamandi, 2019). And in most of the semantic web applications, this work is accomplished through ontology mapping process. Ontology mapping process involves identifying semantic correspondences between entities of candidate ontologies (Adel et al., 2019; Kaza & Chen, 2008).

However, due to increased size and complexities of ontologies, generating ontology mapping manually can be a complex and cumbersome task. Various ontology mapping systems have been developed to provide cognitive support to users during the ontology mapping process (Ivanova et al., 2015). These mapping systems can be fully automated or semi-automated. In fully automated ontology mapping systems, the algorithms automatically compute potential mappings between entities of candidate ontologies, providing total cognitive support to users. Semi-automatic ontology mapping systems combine both automatic mapping process and user validation. In the initial stages, the automated process identifies semantic correspondences between entities of candidate ontologies and later requires experts to validate the mappings identified by automated identified by the automated mapping algorithms (Falconer & Storey, 2007; Ivanova et al., 2015). Semi-automated ontology mapping systems are considered better for most scenarios (Kaza & Chen, 2008), because having users validate semantic mappings generated by automated mapping system enables detection and removal of inaccurate mappings, and potentially the addition of alternative mappings or new ones, not detected by automated mapping systems (Dragisic et al., 2016).

4.3.7 Related Work on Ontology Mapping

Otero-Cerdeira et al. (2015) conducted the literature review on ontology matching articles published from 2003 till 2013. While conducting their review, the authors identified a larger number of articles related to theoretical solutions and approaches, but very few applied ones i.e., articles where ontology matching systems developed have been applied to real- life applications. To understand this situation, the authors conducted an open-ended questions-based survey where they asked the ontology matching practitioners about the future evolution as well as future challenges of the field that still need to be addressed. The main challenges that need to be addressed included automatic discovery of complex relations to correctly align large ontologies and focus on applying automatically created mappings to real-life projects. The other future challenges included: automated acquisition of reference alignment for evaluating large scale matching systems; creating large datasets to asses matching algorithms; define good tools that are easy to use for non-experts; develop high quality and fast intelligent combinations of string-based and new semantic-similarity measures; holistic ontology matching; how to effectively complement automatic computation with human validation; how to minimize involvement of users when turning matches into mapping; human readable explanations for matches; improving the mapping process through semi-automatic machine learning; integration of domain knowledge into alignment techniques; learning what metrics to choose in which scenario; precision and recall of automatic methods; scalability and parallelization of the matching.

Later, Karimi and Kamandi (2019) classified related work on ontology mapping in four different approaches. Their classification was an improvement to the ontology mapping classifications proposed by Euzenat and Shvaiko (2013). Karimi and Kamandi (2019) classified related works on ontology mapping into four fundamental groups of approaches (1) based on terminological similarity, (2) based on structural similarity, (3) based on external sources, and (4) based on instances. Terminological similarity-based approach uses terminologies in the ontologies, words and types of thesauruses to find similarities between the entities. These similarities can be of different kinds: lexical similarity, linguistic similarity, and string similarity etc. Structural similarity approach focuses on structure of ontologies such as is_a or part_of relationships between different entities, location of entities, dependencies between entities, hierarchies of entities, children and leaves of entities. In an external sources-based approach, external sources such as: WordNet, dictionaries, or other set of semantic synonyms are used to identify the semantic correspondences between entities of two ontologies. Instance based approach utilizes a number of common instances to identify and determine semantic correspondences between the entities when the ontologies have some common instances of classes. Later, Karimi and Kamandi (2019) described the related works that fall under each approach.

Karimi and Kamandi (2019) in their work proposed a new learning-based approach that involves using inductive logic programming to identify correspondences between elements of two different ontologies. In this approach the mappings between elements are identified from structural similarities between instances using induction and each element and its relationship in ontologies is translated into logical predicates. In addition, each instance is transformed into horn clause and some general predicates (that are corresponding to ontology mapping) are generated by applying logical induction.

In the study by Geng et al. (2020), the authors used NLP algorithms to construct domain ontologies from online product reviews. Next, a new ontology alignment approach was proposed where semantic based Word2Vec algorithm and structure based Node2vec algorithm were integrated together for ontology mapping on the constructed domain ontologies. Finally, from the ontology mapping, a cross ontology alignment was constructed to assist consumers in utilizing online product reviews to make purchase related decisions when comparing cross-domain products.

The approaches used in the related works presented by Karimi and Kamandi (2019) as well as Geng et al. (2020) emphasize on merely discovering mappings between entities automatically or are restricted over just the mapping tasks. As a difference, Karimi and Kamandi (2019) proposed an approach that instead of being just restricted over a mapping task, also generates a set of rules that can be used to determine when two elements should be mapped with each other. However, one of the weaknesses of the proposed approach by Karimi and Kamandi (2019) is that induction is a time-consuming process and requires optimization before it is applied to real world and practical projects.

The review of the prior literature reveals that the future challenges identified by Otero-Cerdeira et al. (2015) still need to be addressed. As a difference, our proposed semi-ontology mapping approach is not merely restricted over identifying the possible matches between entities of different ontologies, but also a presents a user interface where the data experts can visualize the suggested mappings provided by the automated mapping algorithm, view the human readable definitions of all the entities as well as hierarchy between elements and use that information to understand the suggested mappings, validate the accurate mappings, detect and remove inaccurate mappings, and potentially add the alternative mappings or new ones not detected by automated mapping algorithm. By doing so, our proposed semi-ontology mapping approach addresses four future challenges highlighted by Otero-Cerdeira et al. (2015). By presenting a mapping validation user interface where the data experts can visualize the suggested mappings between elements of different ontologies accompanied by the definitions of each entity, our proposed research addresses the challenge of providing human readable explanations for the suggested mappings. Secondly, by providing the suggested mappings to the data experts before they can validate them, our approach provides cognitive support to data experts because due to increased size and complexities of ontologies, manually mapping the elements of different ontologies can be a complex and cumbersome task. By doing so, it addresses the challenge of minimizing user involvement when turning matches into mappings. The user is involved only during the validation process. Lastly, by enabling the data experts to validate the suggested automated mappings, delete the erroneous mappings and find the additional ones not detected by automated mapping algorithm based on the definitions of each entity, our proposed approach addressees the challenge of effectively complementing the automatic computation with human validation and improving the mapping process through semi-automatic process. Detailed description of our proposed semi-ontology mapping approach is presented in the global ontology manager section.

4.4 BLOCKCHAIN BASED COLLABORATIVE HEALTH INFORMATION EXCHANGE SYSTEM (BCHIES)

Blockchain based Collaborative health information exchange system (BCHIES) is based on the guidelines proposed by *The office of the national coordinator of health information*

(Carneiro et al., 2019). ONC published a set of guidelines to advance interoperability in the healthcare domain. ONC's listed ten essential guidelines to enable interoperability in HIEs (DeSalvo, 2015). This study used only those guidelines whose main focus is to provide a roadmap for secure and semantic HIE. These guidelines include ubiquitous secure network infrastructure, verification of identity and authentication of all participants, and consistent data semantics aka semantic interoperability.

- *Ubiquitous secure network infrastructure* represents that stable, secure, trusted and widely available network infrastructure is pivotal for the success of interoperable learning health systems. ONC states that for secure infrastructure, encryption is essential during data transit as well as storage. For the encryption to work, the provider or the system using the information must be able to decrypt it. BCHIES uses both symmetric and asymmetric encryption to ensure secure data transit.
- *Verification of identity and authentication of all participants* refers to the identification and authentication of all the participants regardless of their role to access a system. ONC requires all the participating users or systems to use the credentials such as username and password to access a system. Also, when provider systems connect and communicate with each other automatically, they should recognize each other as authentic, not nefarious (DeSalvo, 2015). BCHIES uses public key cryptography as well as healthcare institutions' credentials such as their identification number for verification and authentication purposes. In addition, it uses a new mechanism where the healthcare institutions have to decrypt an encrypted message (encrypted with its public key) using its private key to ensure that the member is the authenticated member.
- *Consistent data semantics aka semantic interoperability* represents that "as electronic health information is shared and exchanged amongst different stakeholders, its meanings must be consistently maintained in order to maximize its usage and value in a learning health system" (DeSalvo, 2015) (p.25). BCIES uses semi-ontology mapping to ensure semantic interoperability.

4.5 COMPONENTS OF BCHIES

In this study, we propose a permissioned blockchain system known as blockchain based collaborative health information exchange system (BCHIES) that enables secure and interoperable HIE among participating healthcare institutions. It comprises four main components: Members (Hospitals), Monitoring Manager (MMGR), Ontology Matcher (OMT), and Administrative Manager (AMGR) (See Figure 4).

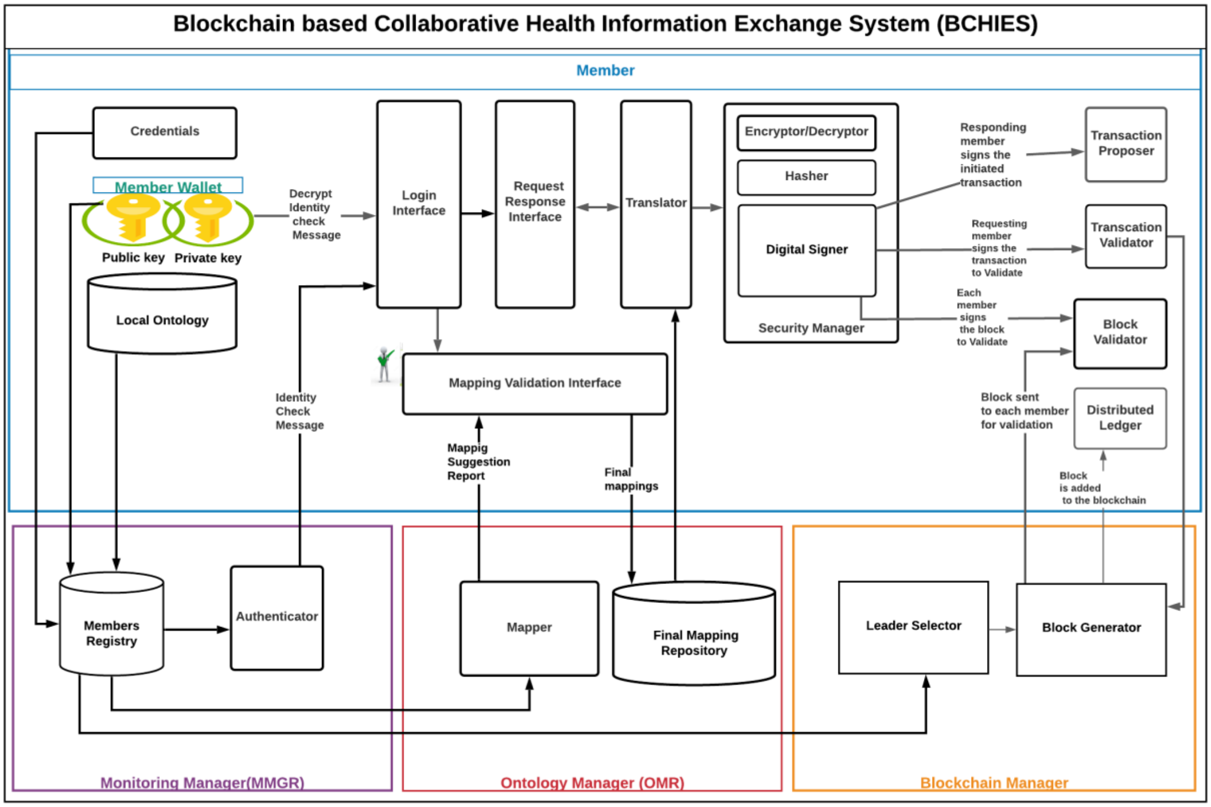


Figure 4 Overview of Blockchain based Collaborative Health Information Exchange System (BCHIES)

4.5.1 Monitoring Manager (MMGR)

MMGR has two main components (1) Member Registrar (2) Authenticator

4.5.1.1. Member Registry

Member registry manages the registration of new members in BCHIES. When a new hospital wishes to be the member of BCIES, this component registers the new hospital by adding it to the members' list. Members' list includes the members' name, its identification number, local ontology, and the public key.

4.5.1.2. Authenticator

This component ensures the identity check. Whenever a member logs in into the system through the logging interface, the authenticator component sends an encrypted message (i.e., encrypted with the public key of the respective member as MMGR has the access to public keys of all the respective members) to the member who is logging in. In order to prove the authentication, the respective member, in addition to entering its identification number, also has to decrypt the message using its private key. If the logging member is able to decrypt the message, the authenticator displays an authentication successful message, otherwise the logging member receives an error. When a member successfully logs in, the authenticator records the information in its log repository.

4.5.2 Member

Each hospital in BCHIES is represented as an individual Member. Each member has different components

4.5.2.1. Credentials

Each member has its credentials such as its name and identification number.

4.5.2.2. Wallet

Each member owns a wallet that includes a pair of uniquely related cryptographic keys: public and private keys. Each member shares its public key with MMGR, whereas it retains its private key to itself.

4.5.2.3. Local Ontology

We assume that each hospital has an ontology. If a hospital doesn’t have an ontology, then the respective EHR sources of the participating members (e.g. A hospital can store patient records using relational databases, XML files, spreadsheet files, EHR standards-based databases) will be transformed into ontologies using mapping rules proposed by (Adel et al., 2019).

4.5.2.4. Login Interface

This component allows each member to log in to BCHIES. The login member enters its identification, name as well as decrypt an encrypted message sent by the authenticator (detailed description in MMGR section) using its private key to authenticate. Once the member is authenticated, the login interface displays the login successful message.

4.5.2.5. Mapping Validation Interface

Mapping validation interface displays a list of elements of the respective hospital that matched and didn’t match to the elements of other participating hospitals during the automated ontology mapping process. In addition, it also displays the annotations of each element in the matched and unmatched list. Data experts of each member utilize annotation of each element to verify the accuracy of the suggested mappings, delete the erroneous matches, and identify a potential match for the elements that didn’t match during the automated ontology mapping process. Once the data experts submit the final mappings, these final mappings automatically get stored in the final mapping dictionary of ontology Manager. The mapping validation interface has an inbuilt rule called *MembersCanValdiateOwnMappings* which allows the member to retrieve information about mappings between the elements of its own ontology with elements of another members’ ontology. It doesn’t allow the member to retrieve information about the mappings of other members.

4.5.2.6 Request and Response Interface

Each member will have a request and response interface. This component allows each member to request patient data from and send patient data to other members in BCHIES. This component displays the members' list. The requesting member selects the member from the list from which it is requesting the patient data from and creates the request. The request contains the request number, the identification of the member generating the request, as well as the identification of the member from whom the patient data is requested. When another member receives a request or response from another hospital, this component sends the notification to the respective hospital notifying it of the request or response received.

4.5.2.7 Translator

This component performs the major role in resolving semantic interoperability conflict between different hospitals. It is the input and output gateway of the requests and responses coming to and from the respective hospitals. By default, this component is triggered when a respective hospital sends a request or receives a response. This component has the access to validated mappings from the mapping validation interface where based on the validated mappings, it translates the request and response message from source party format to destination party format.

4.5.2.8 Security Manager

This component performs various authentication and data integrity related tasks. The tasks include (1) encryption and decryption (2) hashing (4) digital signature

Encryptor uses a hybrid encryption approach i.e., uses both symmetric and asymmetric encryption to encrypt the message included in request/response message. When a member sends a request/response message, through the encryptor, it encrypts the message with the AES key. Later, it encrypts the AES key with the public key of the member receiving the request/response message. The encrypted AES key is passed along with the encrypted message. Upon receiving the request/response, the member receiving the request/response message, through the decryptor, decrypts the shared AES key with its public key and then decrypts the original message with the decrypted AES key.

Hasher ensures the data integrity check. Through this component, the requesting/responding member generates the hash of the request/response message and attach it to the message before sending it to the data responding/requesting member. When the responding/requesting member receives the message, it first decrypts the message (stated above) and later creates the hash of the message to check if the message is altered during the transmission or not. If the hash of the message sent by the requesting/responding member matches the hash of the message generated by the responding/requesting member respectively, then the message is not corrupted or altered, otherwise, the message is altered/corrupted, and the system gives an error.

Digital Signer allows the member sending the request/response message to generate the digital signature using its private key. This component can be executed when the members want to send the request message, response message, propose the transaction, and/ or validate the transaction. Digital signature is used for user authentication. The authenticity of the digital signatures can be verified by others in the network by using the public key of the signer.

4.5.2.9 Transaction Proposal

This component allows the data responding member to propose the transaction, once it sends the patients' data to the requesting member. The proposed transaction includes (1) requestor identification (2) responder identification (3) request number (4) response number (5) hash of the translated data sent to the requesting member , and (6) responder digital signature. Note: in our case, the transaction doesn't include the actual data that is exchanged between both the members, but instead it includes the hash of the data shared by the responding member. This is done to ensure scalability, but most importantly to keep the sensitive healthcare data out of the blockchain.

4.5.2.10 Transaction Validator

This component enables the requesting member to validate the transaction proposed by the responding member in two steps (1) verify if the records received from the responding member are complete and accurate, and (2) sign the transaction by creating a digital signature using its private key. The validated transaction includes 1) requestor identification (2) responder identification (3) request number (4) response number (5) hash of the translated data sent to the requesting member (6) responder digital signature (7) requestor digital signature. The validated transaction is then sent to the blockchain administrator instead of distributing it to the entire network to be added to the block. This resolves privacy issues as we argue that hospitals will not be willing to disclose the information about their personal affairs. i.e., with whom and what time a hospital sent or received the data from. In addition, it also eliminates the wasted computational effort, because the members know at the start of the block where to send the transactions to.

4.5.2.11 Block Validator

Each member verifies the validity of the block by checking the correctness of (1) block timestamp i.e., the time stamp of the current block should be greater than the timestamp of the previous block (2) block-hash (3) the hash value of the previous block (4) leaders' signature (i.e., the node who is responsible for generating and distributing the block), and (5) block height and size. Once each member verifies the correctness of the block, it signs the block by signing the block with its digital signature and later appends the block to its own copy of the ledger

4.5.2.12 Distributed Ledger

Each member in the blockchain can have a copy of the blockchain. Blocks have an inbuilt rule called *MembersCanReadOwnTransactions* which allows a member to retrieve information about its own transactions. That being said, the transaction view included in each block will be different for each member in the blockchain meaning each member can have an entire copy of the blockchain, but its access to the transactions included within the block will be restricted i.e., it will only be able to view the transactions in which it participated.

4.5.3 Ontology Matcher (OMT)

OMT performs three functions: Generate automatic mapping suggestions, send automatic mapping suggestions to each member, and store final mappings in a mapping dictionary.

4.5.3.1. Mapper

Mapper identifies semantic correspondences between entities of each member's ontology with entities of other participating members' ontologies. Once it creates the automated mappings, it sends the automated mapping suggestions to the mapping validation interface of each member for further validation. Note: each member only receives automated mapping suggestions between elements of its own ontology with elements of other participating members' ontologies. For instance: There are four members A, B, C, and D. Member A will receive the automated mapping suggestions between its own ontology elements with the ontology elements of B, C, and D. It will not receive the mappings suggestions of member B's ontology elements with the ontology elements of C and D. Automated mappings process is a three-step process: Entity-term level Mapping, Entity-definition level mapping, and Structure level mapping.

4.5.3.1.1 Entity-term Level Mapping

Entity term level mapping involves employing techniques such as string similarity, WordNet, and fuzzy wuzzy partial token set ratio to the element labels/terms of different ontologies to identify matches. As noted in prior literature (Kaza & Chen, 2008), entities with the same term names are considered similar to each other. During our string similarity comparison, the entities identified as having same term names are labeled as matched items and saved in the mapped items list. The remaining entities which didn't match during the string similarity are then compared using WordNet.

WordNet, a widely used electronic dictionary of English, serves as the lexicon for a variety of different NLP applications such as word sense disambiguation (WSD), information retrieval (IR), and machine translation (MT) (Fellbaum, 1998). WordNet apparently resembles thesaurus in that it groups different words together based on their meaning including synonyms, hyponyms, and meronyms. Wordnet groups synonyms into Synsets accompanied by the explanatory gloss and usage examples (Fellbaum, 1998). Wordnet Synsets are used to determine semantic similarity and relatedness between two entities. WordNet supports six measures of similarity and three measures of relatedness (Pedersen et al., 2004). Three similarity measures are path length based and the remaining three are based on information content. Path length-based similarity measures include Leacock and Chodorow(lch), Wu and Palmer (wup), and path (Pedersen et al., 2004). Previous literature (Helou, 2019; Mahadzir et al., 2018) notes that out of three path-based similarity measures, Wup similarity has the best performance and is simple to implement (Helou, 2019; Mahadzir et al., 2018). Hence, in our mapping process, we employ Wup similarity to determine synonymous entity terms. Wup similarity utilizes the depth of two Synsets in the WordNet taxonomies and the depth of the least common entity (lsc) that subsumes the two compared entities (Helou, 2019). The similarity of two entities s1 and s2 using Wup similarity is computed as follows:

$$sim_{wup}(s1, s2) = \frac{2*d(lcs(s1,s2))}{d(s1)+d(s2)} \qquad (1)$$

Where $d(s1)$ represents the depth of Synset s1 using edge counting in the semantic hierarchy, $lcs(s1, s2)$represents the least common subsumer of $s1$ and $s2$, $d(lcs(s1, s2)$ represents length between lcs of $s1$ and $s2$ and the root of hierarchy. In our ontology mapping process, the entities found synonymous in the WordNet similarity comparison are labelled as matched entities and added to the mapped items list. One of the major limitations of WordNet is that it doesn't work on entities that are composed of more than one word. For instance: An entity in one ontology may be labeled as "Birth_Date" and "Date_of_Birth" in another ontology. These entity labels are entirely different in terms of their length and the order. In such a case, the use of Wordnet wouldn't be helpful, since Wordnet works only on a single word. In this case, the FuzzyWuzzy package can be utilized to determine a match.

Fuzzy-Wuzzy is a python library package that measures the degree of closeness between two strings using Levenshtein distance. It supports four fuzzy matching logic: ratio, partial ratio, token sort ratio, and token set ratio (Cao et al., 2018)Out of these four logics, token set ratio is more flexible and yields better outcomes (Novack et al., 2018). Fuzzy token set ratio works on the strings that are of different lengths and are widely in different order. Fuzz token set ratio first tokenizes the strings in question, and later performs a set operation, where the intersection (common tokens) and remainder are compared (Cao et al., 2018).

4.5.3.1.2 Entity-definition Level Mapping

Entity definition level mapping involves determining similarity between entities that are terminologically heterogeneous by comparing their definitions. For instance: both "Social Security number" and "SSN" are neither synthetically similar nor synonyms of each other but have similar meanings and are used interchangeably. In such a case, neither WordNet nor FuzzyWuzzy logic would be able to identify similarities between them. To resolve this issue, Ngo and Bellahsene (2016) employed an information retrieval-based similarity technique on entity labels. The approach by Ngo and Bellahsene (2016) involves normalization of the annotated entity labels first (i.e., tokenizing the labels, removing the stop words in the annotated label, stemming the words and arranging them into an alphabetical order) and then computing the similarity scores by considering both syntactic similarity as well as information content of the words. The weakness of the above approach is that when the two strings are compared, the stop words are removed, stemmed, and the remaining words are arranged in an alphabetical order. Although the function words such as of, the, an, by etc may contribute less to the sentence meaning than other words, they cannot be ignored if a text is very short because they carry syntactic information which is very useful in explaining meaning of a short text (Li et al., 2006). In their second approach, Ngo and Bellahsene (2016) identifies similarity between concepts by exploiting the contextual information of each concept that includes annotation description (i.e, labels, synonyms and comments of a given entity) of the concept itself, its ancestors and descendants. From these three set of documents, the terms are tokenized first and then assigned a weight by Lucene weighing scheme to calculate the similarity between concepts. In both the approaches, Ngo and Bellahsene (2016) doesn't take into account the word order. For instance, let's consider two sentences or short texts S1 and S2 that contain exactly the same words in the same order except two words in S1 which occur in reverse order in S2.

S1: A patient saw the doctor

S2: A doctor saw the patient

Since two sentences contain the same words, the first approach used by Ngo and Bellahsene (2016) will conclude that both the words are exactly the same. However, in reality, these sentences are not similar. The dissimilarity between these two sentences is due to difference in word order. In addition, in the second approach, Ngo and Bellahsene (2016) noted that vocabularies describing the context of a concept in the same domain are highly similar. This heuristic may not be true in all the cases as due to intrinsic property of natural language processing, the individuals are able to express similar meanings using sentences different in terms of structure and word content (Li et al., 2006). Therefore, in short texts, the co-occurrence of words may be rare or even null (Li et al., 2006).

Hence, in this article, we resolve terminologically heterogeneous entity issues by comparing the definitions of the entities by employing sentence similarity method proposed by Li et al. (2006). Sentence similarity method proposed by Li et al. (2006) has been used by Johann et al. (2017) and Cheng et al. (2019) for feature matching and finding semantic similarity between two users respectively. In this article, we utilize definitions of terminological heterogeneous entities to identify matches, as prior literature (Dean et al., 2016) notes that definitions are critical, potentially very critical in understanding a concept as they provide clarity and several potential theoretical directionalities to the lost leader (Dean et al., 2016). Hence, when a concept is used in a technical context, it becomes crucial to consult its definition to understand its meaning, otherwise errors may occur (Vinner, 2002). Based on the prior literature, we argue that the entities' definitions are the best descriptors of a semantic entity/instance in an ontology. Ontology software such as Protégé and OWL ready 2 enables entities to be annotated with various pieces of information and metadata. For instance: the annotation property rdfs: comment in Protégé can be used to provide human readable descriptions of a resource1.

3.3.2 Final Mapping Repository

The final mapping repository stores the validated mappings of all the participating members.

4.5.4 Blockchain Administrator

This component is responsible for performing two functions (1) leader selection (2) block generation. Hence, it has two components

4.5.4.1. Leader Selector

This component uses a random number to select the leader from the member list. For the simplicity purposes, we in this research represent the block size by number of transactions. In our study, every block will include two transactions. Hence, after every two validated transactions, a new block is generated. Consequently, after every two validated transactions, a new leader is selected. This leader will then execute the block generation process.

4.5.4.2. Block Generator

This component enables the leader to generate a new block and distribute it to the entire network for the validation purposes. A selected leader initiates the block generation process. Each block in BCHIES includes (1) block number, (2) current block hash, (3) timestamp, (4) leader Id (5) hash of the previous block (6) merkle root, and (7) block-size (i.e., represented by

[1] (https://www.w3.org/TR/2002/WD-rdf-schema-20020430/)

two transactions). Merkle is computed by calculating the summarized hash of hashed values of all the transactions. The leader signs the block by creating the digital signature and later broadcasts the block to the entire network for validating purposes.

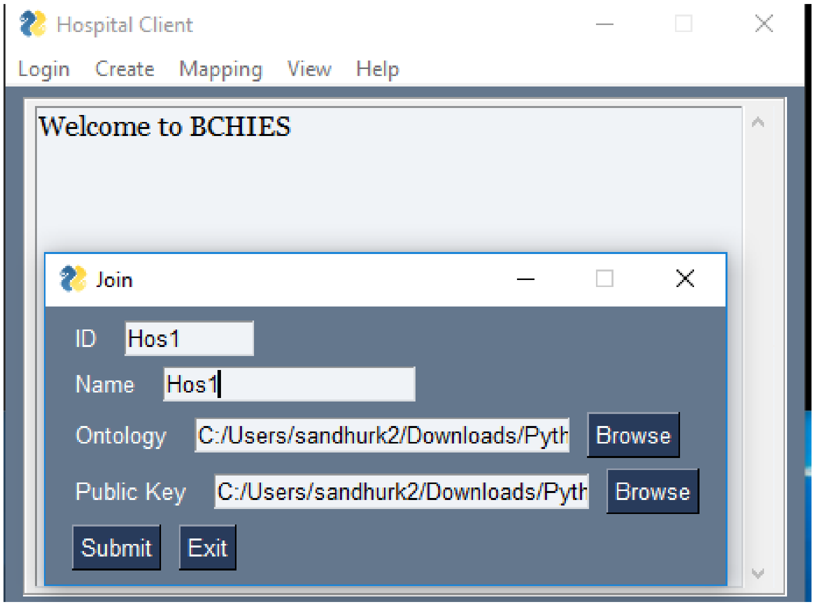
4.6 EVALUATION

This section involves evaluating the proposed artifact i.e., BCHIEs by demonstrating how well it resolves security and semantic interoperability issues. A proposed artifact can be evaluated through various methods including case studies, field experiments, simulations, illustrative scenarios, and informed arguments, expert evaluations, subject based experiments, prototype etc. (Hevner et al., 2004; Peffers et al., 2012). Similar to prior studies (Azad & Morla, 2019; Carvalho, 2020; Lim et al., 2017; Sierra et al., 2019), we evaluated our proposed artifact via development of a prototype of BCHIES. We used Python programming language, Protégé, Owlready2 and graphical user interface to build the prototype of our proposed architecture.

4.6.1 Illustrative Scenario

Similar to van Engelenburg et al. (2019), we also used an illustration of hospital to hospital patient data sharing in the virtual environment to illustrate how our proposed artifact and its prototype can be used to share patient data across different hospitals. We created three hospitals willing to participate in EHRs virtual exchange using BCHIES: Hos1, Hos 2, and Hos 3. Hos 1 has a new patient named Rupal Roxanne, who was a patient in Hos 2. The provider of the Hos1 wants to get the prior records of Rupal Roxanne from Hos 2 to get an overview of her health history. Similarly, Hos 2 wants to get records of patient name Steve Apple’s records from Hos 3. Similar to Azad and Morla (2019), we created a synthetic dataset that simulates realistic hospital patient databases in Hos 1, Hos 2, and Hos 3. The patients’ records for each hospital was created using different naming conventions to illustrate semantic interoperability conflict among information systems of three hospitals. Steps below depicts the illustration of the functioning of BCHIES.

Step 1: Hos1 joins BCHIES by providing its name, identification number, and its local ontology (See Figure 5). Once the member enters the required information and hits submit, the system directs Hos1 to share its public key. Hos 1 creates a pair of public and private keys using public key cryptography. Hos 1 shares its public key with BCHIES and keep its private key safe with itself (See Figure 6). Similarly, Hos 2 and Hos 3 join BCHIES.



Welcome to BCHIES

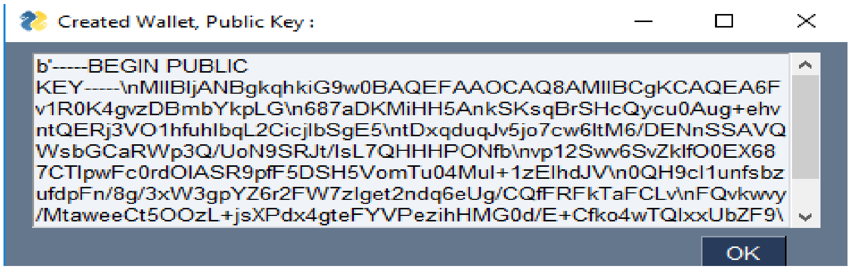
ID Hos1

Name Hos1

Ontology C:/Users/sandhurk2/Downloads/Pyth

Public Key C:/Users/sandhurk2/Downloads/Pyth

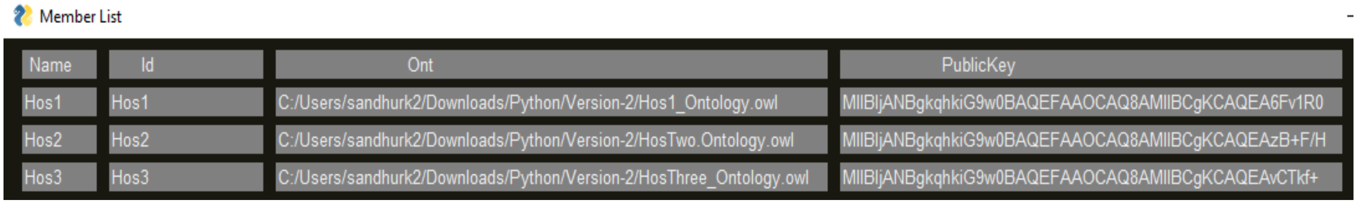
Figure 5 Hos 1 joining the system (BCHIES)



```
b'-----BEGIN PUBLIC
KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6F
v1R0K4gvzDBmbYkpLG\n687aDKMiHH5AnkSKsqBrSHcQycu0Aug+ehv
ntQERj3VO1hfuhlbqL2CicjlbSgE5\ntDxqduqJv5jo7cw6ltM6/DENnSSAVQ
WsbGCaRWp3Q/UoN9SRJt/IsL7QHHHPONfb\nvp12Swv6SvZklfO0EX68
7CTlpwFc0rdOlASR9pfF5DSH5VomTu04MuI+1zElhdJV\n0QH9cl1unfsbz
ufdpFn/8g/3xW3gpYZ6r2FW7zIget2ndq6eUg/CQfFRFkTaFCLv\nFQvkwvy
/MtaweeCt5OOzL+jsXPdx4gteFYVPezihHMG0d/E+Cfko4wTQlxxUbZF9\
```

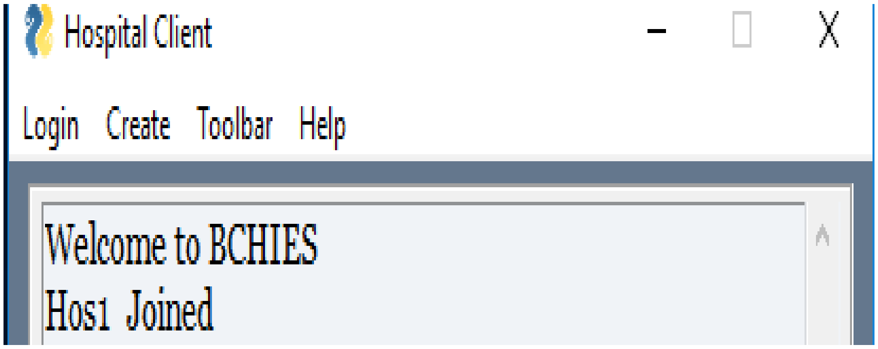
Figure 6 Public Key Creation for Hos1

Step 2: Once, Hos1, 2, and 3 join BCHIES by entering the required information and sharing their public keys, MMGR registers Hos1, 2, and 3 as members and saves their credentials, local ontologies, and their public keys in the members' list (See Figure 7). Next, Hos1 gets the "Welcome to BCHIES" message in its member's interface, indicating that Hos1 joined BCHIES (See Figure 8).



Name	Id	Ont	PublicKey
Hos1	Hos1	C:/Users/sandhurk2/Downloads/Python/Version-2/Hos1_Ontology.owl	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6Fv1R0
Hos2	Hos2	C:/Users/sandhurk2/Downloads/Python/Version-2/HosTwo.Ontology.owl	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzB+F/H
Hos3	Hos3	C:/Users/sandhurk2/Downloads/Python/Version-2/HosThree_Ontology.owl	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvCTkf+

Figure 7 Members' list in Members' Registrar



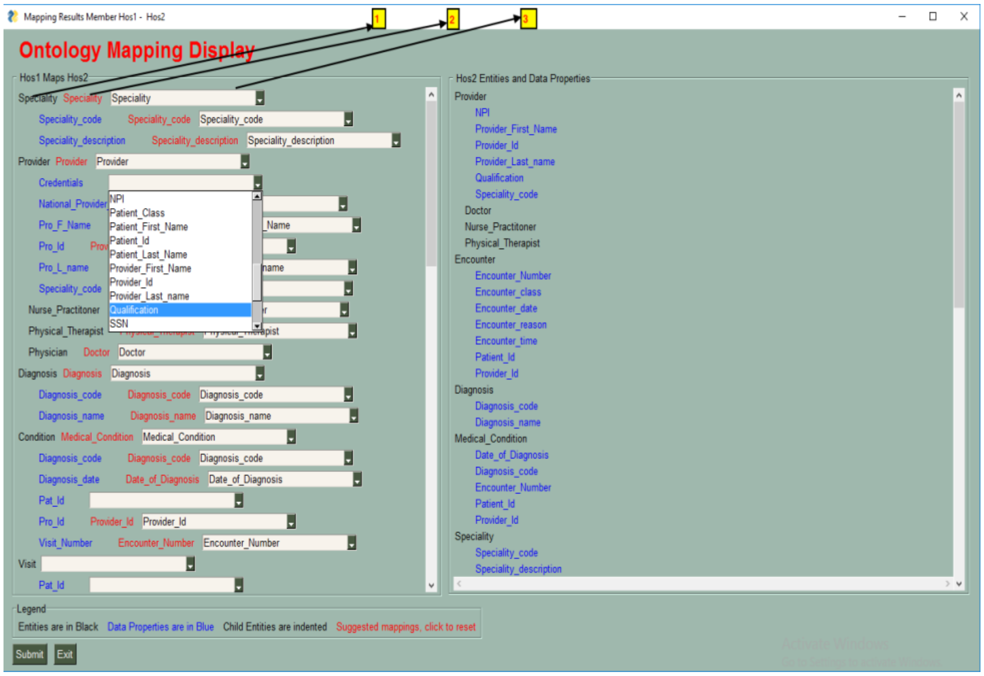
Welcome to BCHIES

Hos1 Joined

Figure 8 Hos 1 joining illustration

Step 3: MMGR shares local ontologies of Hos 1, 2, and 3 with Mapper in Ontology Manager. Mapper generates the automated mappings between ontology elements of Hos 1, 2, and 3 using methods described in section 3.3.1. Once the automated mappings are generated, mapper shares the automated mappings suggestions with Hos1, 2, and 3. Each member can view the automated mapping suggestions in their mapping validation interface. Figure 4.7 depicts the mapping validation interface for Hos1, displaying mappings suggested between Hos

1 and Hos 2 ontology elements. On the left side of the interface, the mappings between elements of Hos 1 and Hos 2 are displayed. In Figure 9, 1 represents the entities and data properties of Hos 1 ontology, where entities are represented in black and data properties are represented in blue; 2 represents the suggested mapped elements from Hos 2 ontology. In case a data expert choses an inaccurate mappings in dialogue box (described next) by accident, then the data expert can click on the element in red to reset it back to mapping suggested by automated mapping process ; 3 represents the dialogue box where the data experts can verify the accuracy of the suggested mappings, delete the erroneous matches, and identify an additional match for the elements that didn’t match during automated ontology mapping process. The drop down includes the list of elements of Hos 2 ontology. It enables the data experts to choose an accurate match if the match suggested by automated mapper was an erroneous one and find an additional match if the automated mapper found no match. Note: If there was no match found during the automated mapping process, then the mapping validation interface will display an empty dialogue box representing no match. On the right-hand side of the interface, ontology elements of Hos 2 as well as hierarchy between them is displayed. When a data expert moves the cursor over a specific element of Hos 2 ontology, the interface displays the definition of that specific element, which the data experts can view to validate, update or delete the automated suggested mappings. Figure 10 represents Hos 1 and Hos 3 matches. It also depicts the procedure of display of definition of an element “credentials” from Hos 2 ontology. Upon finalizing the mapping suggestions, data experts from Hos 1 can click the submit button. Upon clicking the submit button, these final mappings automatically get stored in final mapping repository of ontology matcher.



Mapping Results Member Hos1 - Hos2

Ontology Mapping Display

Hos1 Maps Hos2

Speciality	Speciality	Speciality
Speciality_code	Speciality_code	Speciality_code
Speciality_description	Speciality_description	Speciality_description
Provider	Provider	Provider
Credentials		
National_Provider		
Pro_F_Name		_Name
Pro_Id	Prov	
Pro_L_name		name
Speciality_code		
Nurse_Practitoner		r
Physical_Therapist	Physical_Therapist	Physical_Therapist
Physician	Doctor	Doctor
Diagnosis	Diagnosis	Diagnosis
Diagnosis_code	Diagnosis_code	Diagnosis_code
Diagnosis_name	Diagnosis_name	Diagnosis_name
Condition	Medical_Condition	Medical_Condition
Diagnosis_code	Diagnosis_code	Diagnosis_code
Diagnosis_date	Date_of_Diagnosis	Date_of_Diagnosis
Pat_Id		
Pro_Id	Provider_Id	Provider_Id
Visit_Number	Encounter_Number	Encounter_Number
Visit		
Pat_Id		

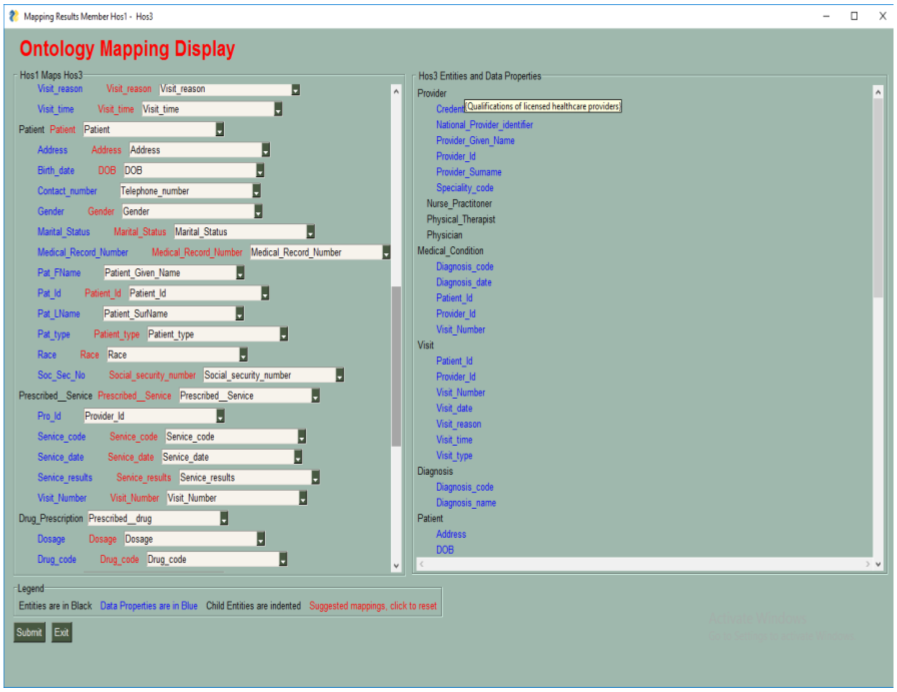
NPI
Patient_Class
Patient_First_Name
Patient_Id
Patient_Last_Name
Provider_First_Name
Provider_Id
Provider_Last_name
Qualification
SSN

Hos2 Entities and Data Properties

Provider
NPI
Provider_First_Name
Provider_Id
Provider_Last_name
Qualification
Speciality_code
Doctor
Nurse_Practitoner
Physical_Therapist
Encounter
Encounter_Number
Encounter_class
Encounter_date
Encounter_reason
Encounter_time
Patient_Id
Provider_Id
Diagnosis
Diagnosis_code
Diagnosis_name
Medical_Condition
Date_of_Diagnosis
Diagnosis_code
Encounter_Number
Patient_Id
Provider_Id
Speciality
Speciality_code
Speciality_description

Legend
Entities are in Black Data Properties are in Blue Child Entities are indented Suggested mappings, click to reset

Figure 9 Mapping Validation Interface for Hos1 (Mappings between Hos1 and 2)



Mapping Results Member Hos1 - Hos3

Ontology Mapping Display

Hos1 Maps Hos3

Visit_reason	Visit_reason	Visit_reason
Visit_time	Visit_time	Visit_time
Patient	Patient	Patient
Address	Address	Address
Birth_date	DOB	DOB
Contact_number		Telephone_number
Gender	Gender	Gender
Marital_Status	Marital_Status	Marital_Status
Medical_Record_Number	Medical_Record_Number	Medical_Record_Number
Pat_FName		Patient_Given_Name
Pat_Id	Patient_Id	Patient_Id
Pat_LName		Patient_SurName
Pat_type	Patient_type	Patient_type
Race	Race	Race
Soc_Sec_No	Social_security_number	Social_security_number
Prescribed__Service	Prescribed__Service	Prescribed__Service
Pro_Id		Provider_Id
Service_code	Service_code	Service_code
Service_date	Service_date	Service_date
Service_results	Service_results	Service_results
Visit_Number	Visit_Number	Visit_Number
Drug_Prescription		Prescribed__drug
Dosage	Dosage	Dosage
Drug_code	Drug_code	Drug_code

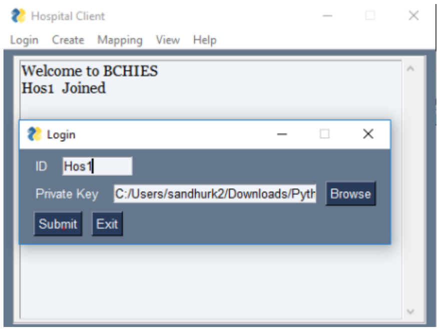
Hos3 Entities and Data Properties

Provider
Credent Qualifications of licensed healthcare providers
National_Provider_identifier
Provider_Given_Name
Provider_Id
Provider_Surname
Speciality_code
Nurse_Practitoner
Physical_Therapist
Physician
Medical_Condition
Diagnosis_code
Diagnosis_date
Patient_Id
Provider_Id
Visit_Number
Visit
Patient_Id
Provider_Id
Visit_Number
Visit_date
Visit_reason
Visit_time
Visit_type
Diagnosis
Diagnosis_code
Diagnosis_name
Patient
Address
DOB

Legend
Entities are in Black Data Properties are in Blue Child Entities are indented Suggested mappings, click to reset

Figure 10 Mapping Validation Interface for Hos1 (Mappings between Hos1 and 3)

Step 4: Once Hos1 joins BCHIES and updates the mappings, Hos 1 can log in to BCIES using the login interface. To prove its identification, Hos 1 enters its identification number and decrypts an encrypted Identity check message sent by authenticator using its private key as illustrated in Figure 11. If Hos 1 Is able to decrypt the identity check message, then the authenticator sends an authentication successful message to Hos1 as illustrated in Figure 12. This information is also updated in authenticators' log repository indicating Hos 1 "found" or authenticated as illustrated in Figure 13. Similarly, Hos 2 and Hos 3 can login following the same procedure. If Hos 1 is unable to decrypt the identify check message, Hos 1 gets an error message.

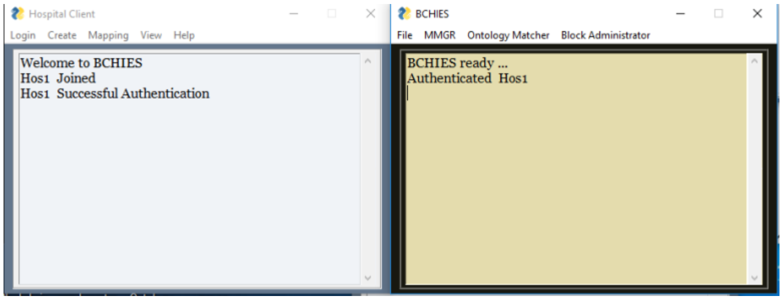


```
Welcome to BCHIES
Hos1  Joined
```

ID Hos1

Private Key C:/Users/sandhurk2/Downloads/Pyth

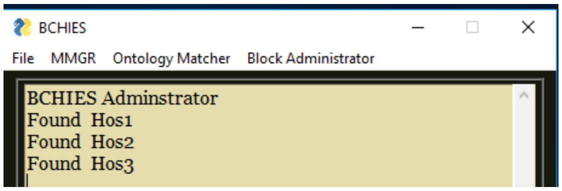
Figure 11 Hos 1 login interface


Hospital Client
Login Create Mapping View Help
BCHIES
File MMGR Ontology Matcher Block Administrator

```
Welcome to BCHIES
Hos1  Joined
Hos1  Successful Authentication
```

```
BCHIES ready ...
Authenticated  Hos1
```

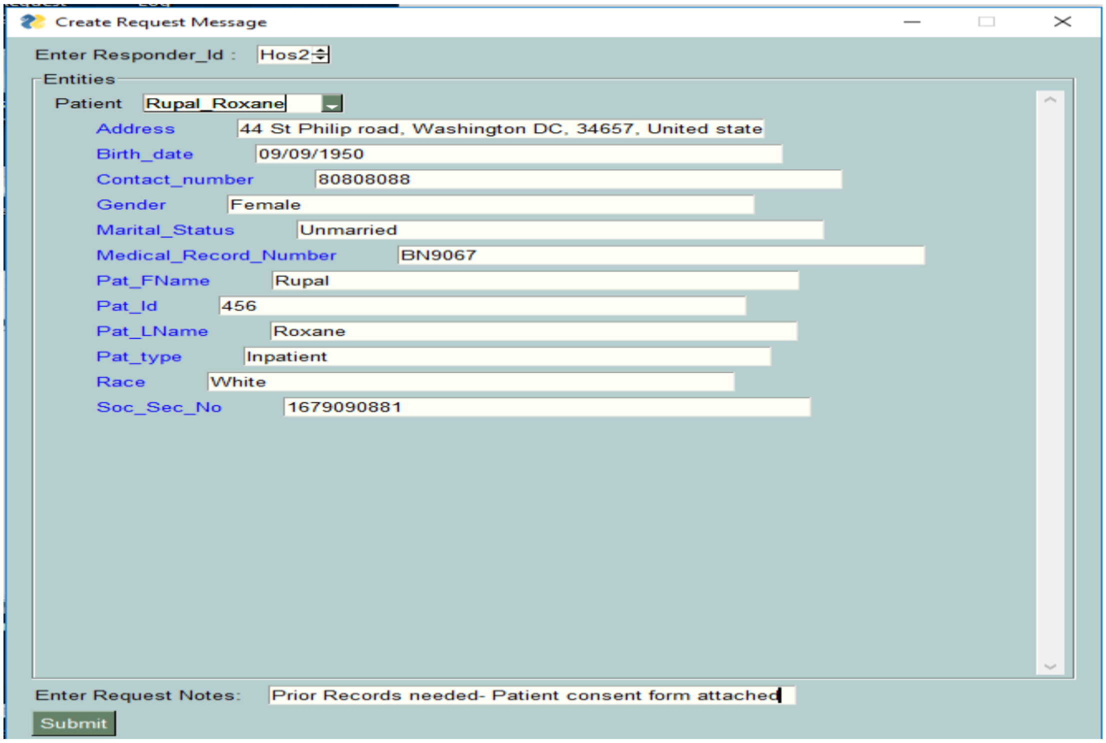
Figure 12 Hos 1 Successful Login



```
BCHIES Adminstrator
Found  Hos1
Found  Hos2
Found  Hos3
```

Figure 13 Log Repository in Authenticator

Step 5: Now Hos 1 wants to request the records of a patient named Rupal Roxanne for Feb 15, 2019 from Hos 2. Hos 1 clicks on the create tab from the client interface. Next, Hos 1 select request option to create a request message as illustrated in Figure 14. Hos 1 selects the Hos 2 from responder Id list. Next it selects the patient whose records it is requesting from Hos2. Once the patient name Rupal Roxane is selected, her identifying information automatically pops up. Next, Hos 1 enters the additional information in request notes and click the submit button. The translator component becomes active as soon as the submit button is hit. Translator translates the labels of data elements in request message to data labels of Hos 2 format as illustrated in Figure 15. Once the message is translated, Hos 1 uses the security manager to encrypt, hash, and sign the message before sending it Hos 2. The translated message is first encrypted with AES key, next AES key is encrypted with Hos 2's public key, then the hash of the translated message is created. Lastly, Hos 1 creates a digital signature using its private key and attaches the hash of the message and digital signature to the encrypted request message and sends it to Hos 2.



Enter Responder_Id : Hos2

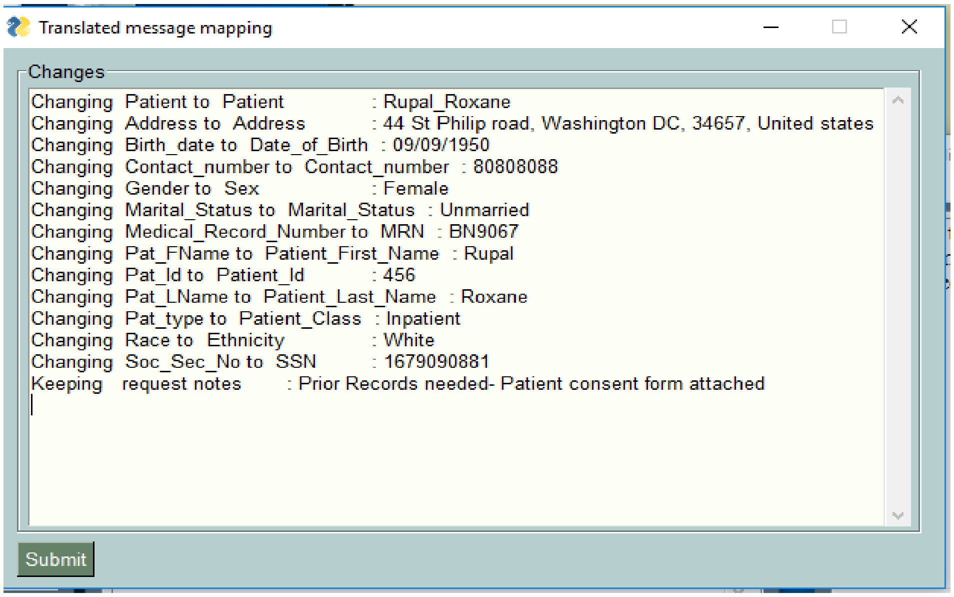
Entities

Patient: Rupal_Roxane

Address: 44 St Philip road, Washington DC, 34657, United state
Birth_date: 09/09/1950
Contact_number: 80808088
Gender: Female
Marital_Status: Unmarried
Medical_Record_Number: BN9067
Pat_FName: Rupal
Pat_Id: 456
Pat_LName: Roxane
Pat_type: Inpatient
Race: White
Soc_Sec_No: 1679090881

Enter Request Notes: Prior Records needed- Patient consent form attached

Figure 14 Request Message Interface

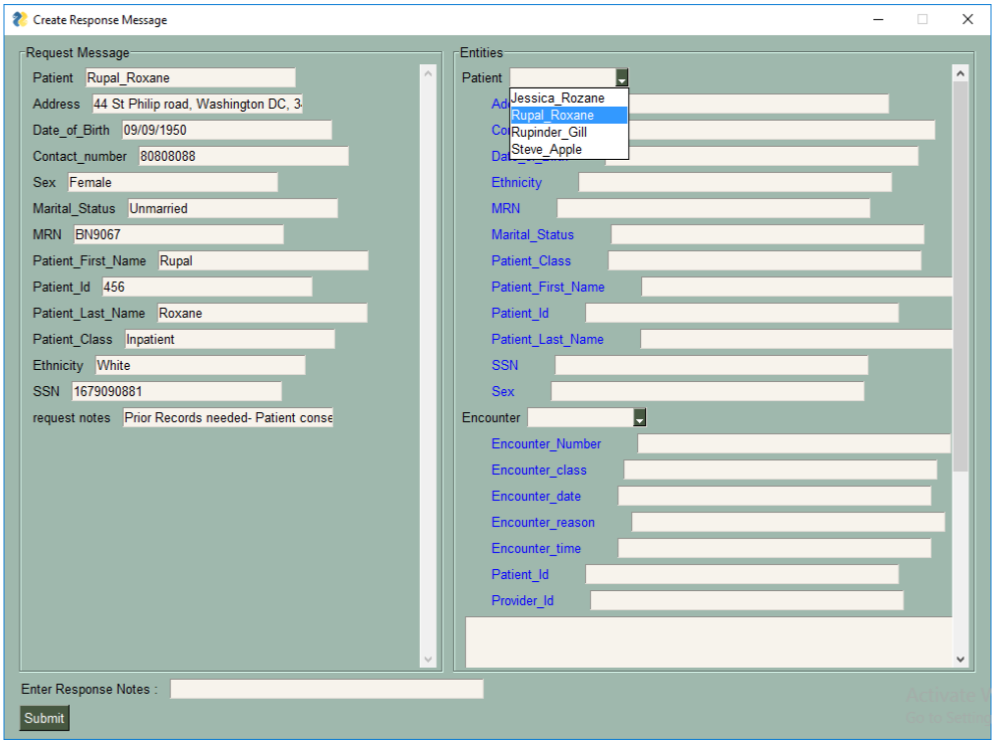


Changes

```
Changing  Patient to  Patient              : Rupal_Roxane
Changing  Address to  Address              : 44 St Philip road, Washington DC, 34657, United states
Changing  Birth_date to  Date_of_Birth  : 09/09/1950
Changing  Contact_number to  Contact_number  : 80808088
Changing  Gender to  Sex                   : Female
Changing  Marital_Status to  Marital_Status  : Unmarried
Changing  Medical_Record_Number to  MRN  : BN9067
Changing  Pat_FName to  Patient_First_Name  : Rupal
Changing  Pat_Id to  Patient_Id            : 456
Changing  Pat_LName to  Patient_Last_Name  : Roxane
Changing  Pat_type to  Patient_Class  : Inpatient
Changing  Race to  Ethnicity               : White
Changing  Soc_Sec_No to  SSN               : 1679090881
Keeping   request notes        : Prior Records needed- Patient consent form attached
```

Figure 15 Translated Request Message

Step 6: Hos 2 receives notification about the request message. The security manager in Hos 2 first decrypts an encrypted AES key using Hos 2's private key and then decrypts the message using the decrypted AES key. Next it creates the hash of the request message received to check the message integrity. If the hash created by the security manager matches the hash received in the request message from Hos1, then the request message passes the data integrity check, otherwise the security manager gives an error. If the message passes an integrity check, then Hos2's security manager decrypts the digital signature of Hos 1using Hos 1's public key to check to validate the authenticity of Hos1. Once Hos 1 is authenticated, Hos 2 creates a response message. Figure 16 depicts the response message interface. Response message interface displays the request message from Hos 1 on the left side with the elements labeled in Hos 2 format. On the right side, data elements of Hos 2 are displayed. Upon selecting the patient "Rupal Roxanne, her other information including her id, first and last name, SSN, and gender is displayed as illustrated in Figure17. Next, the interface displays the encounter related information of Rupal Roxane. Rupal Roxane may have more than one encounter in Hos 2. Upon selecting a specific encounter number V021520198080, Rupal Roxanne's records for May 15, 2019 are displayed. If Hos 2 wants to send some additional message, it can enter it in the response notes. This procedure is illustrated in Figure 17.



Request Message

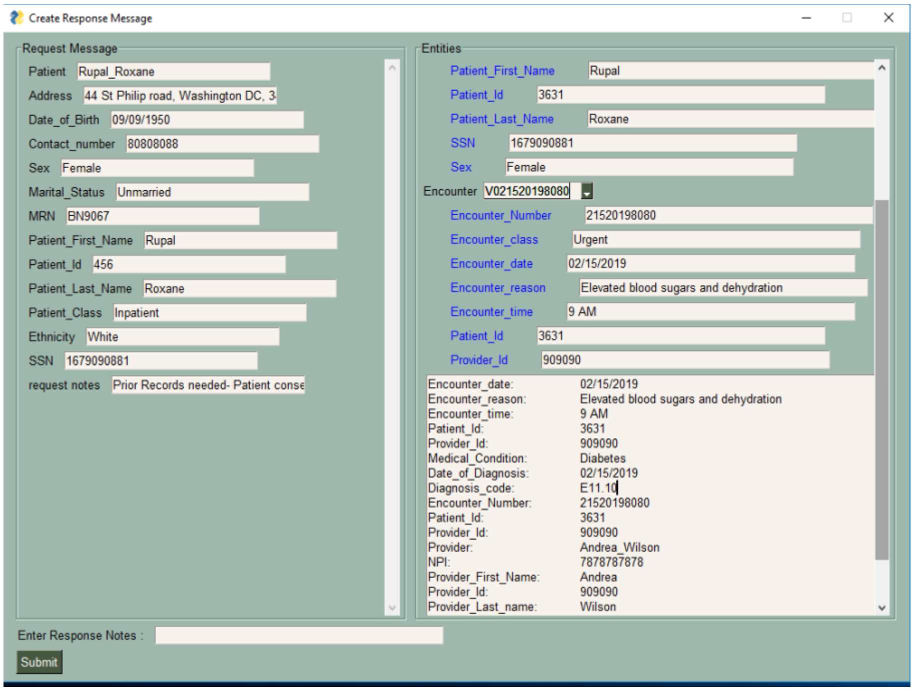
Patient: Rupal_Roxane
Address: 44 St Philip road, Washington DC, 3
Date_of_Birth: 09/09/1950
Contact_number: 80808088
Sex: Female
Marital_Status: Unmarried
MRN: BN9067
Patient_First_Name: Rupal
Patient_Id: 456
Patient_Last_Name: Roxane
Patient_Class: Inpatient
Ethnicity: White
SSN: 1679090881
request notes: Prior Records needed- Patient conse

Entities

Patient: Jessica_Rozane / Rupal_Roxane / Rupinder_Gill / Steve_Apple
Ad
Co
Da
Ethnicity
MRN
Marital_Status
Patient_Class
Patient_First_Name
Patient_Id
Patient_Last_Name
SSN
Sex
Encounter
Encounter_Number
Encounter_class
Encounter_date
Encounter_reason
Encounter_time
Patient_Id
Provider_Id

Enter Response Notes :

Figure 16 Hos 2 Response Message Interface-1



Request Message

Patient: Rupal_Roxane
Address: 44 St Philip road, Washington DC, 3
Date_of_Birth: 09/09/1950
Contact_number: 80808088
Sex: Female
Marital_Status: Unmarried
MRN: BN9067
Patient_First_Name: Rupal
Patient_Id: 456
Patient_Last_Name: Roxane
Patient_Class: Inpatient
Ethnicity: White
SSN: 1679090881
request notes: Prior Records needed- Patient conse

Entities

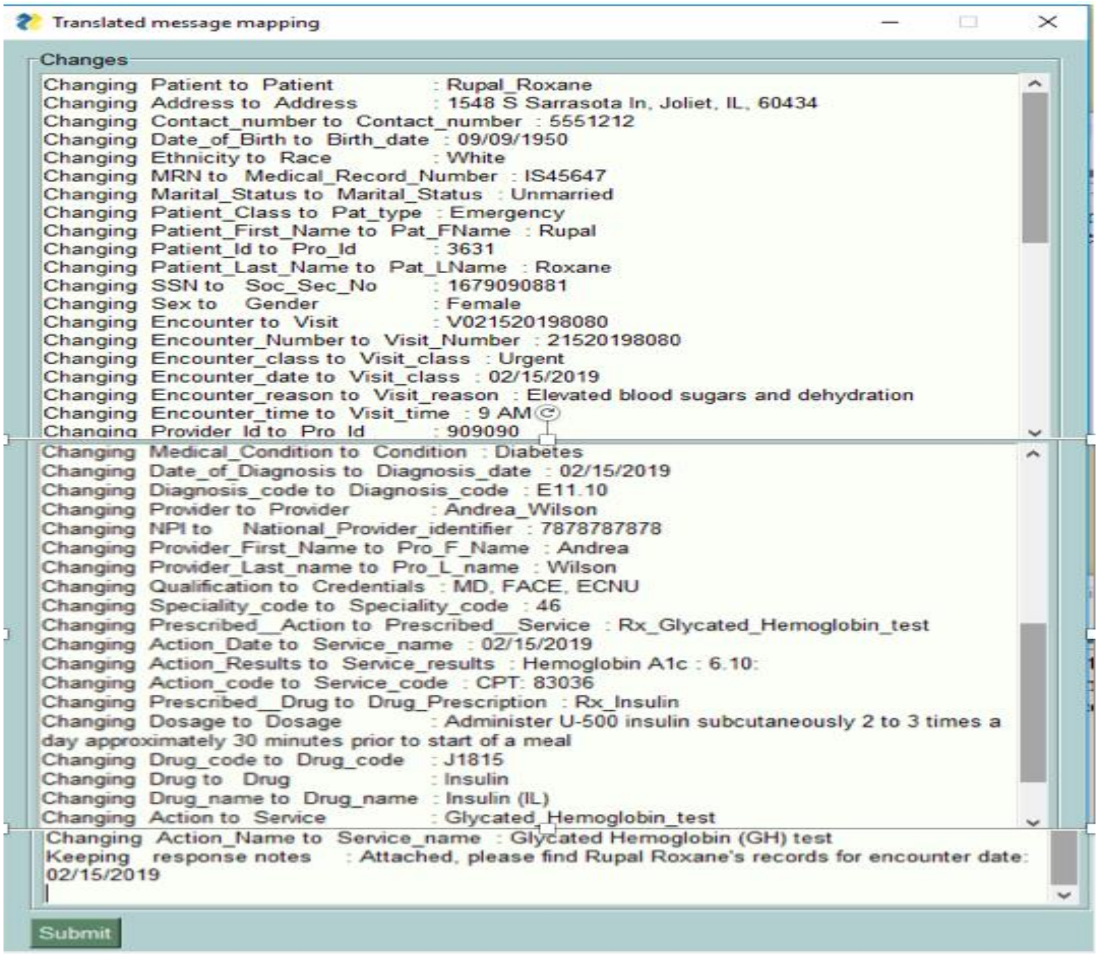
Patient_First_Name: Rupal
Patient_Id: 3631
Patient_Last_Name: Roxane
SSN: 1679090881
Sex: Female
Encounter: V021520198080
Encounter_Number: 21520198080
Encounter_class: Urgent
Encounter_date: 02/15/2019
Encounter_reason: Elevated blood sugars and dehydration
Encounter_time: 9 AM
Patient_Id: 3631
Provider_Id: 909090

```
Encounter_date:          02/15/2019
Encounter_reason:        Elevated blood sugars and dehydration
Encounter_time:          9 AM
Patient_Id:              3631
Provider_Id:             909090
Medical_Condition:       Diabetes
Date_of_Diagnosis:       02/15/2019
Diagnosis_code:          E11.10
Encounter_Number:        21520198080
Patient_Id:              3631
Provider_Id:             909090
Provider:                Andrea_Wilson
NPI:                     7878787878
Provider_First_Name:     Andrea
Provider_Id:             909090
Provider_Last_name:      Wilson
```

Enter Response Notes :

Figure 17 Hos 2 Response Message Interface-2

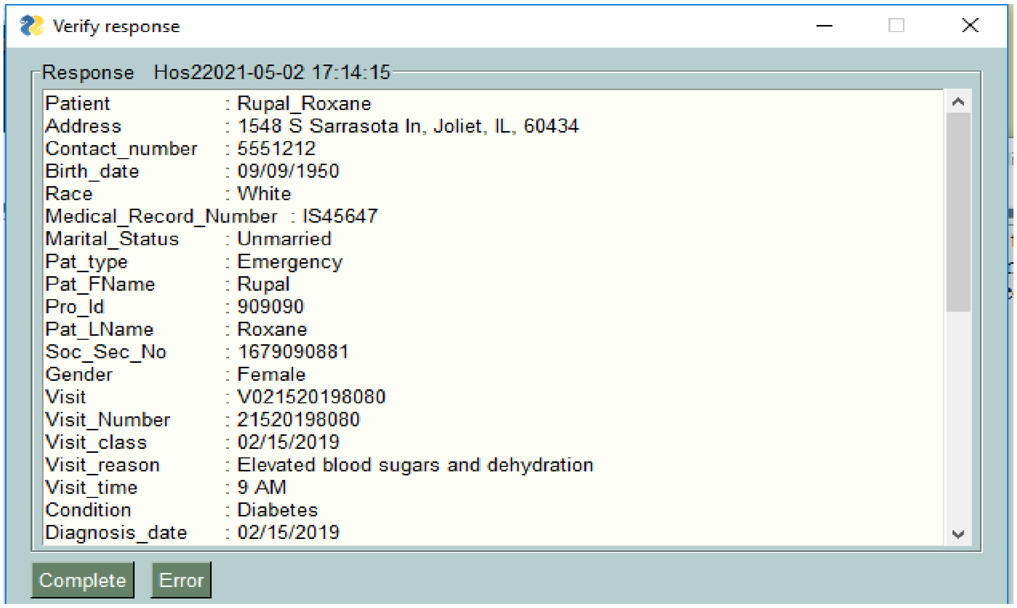
Step 7: Upon entering the additional notes, if any, Hos 2 activates the translator to translate the data elements labels in the response message to Hos 1 format as illustrated in figure 18. Upon translation, the security manager in Hos 2 follows the same procedure to encrypt, hash, and create the digital signature as discussed in step 3 and sends the message to Hos1. Next, Hos 2 activates the transaction proposer to initiate the transaction process by including its identification, digital signature, requesting member's Id i.e., Hos 1's Id in this case, request number, response number (the combination of Hos 2's Id and the date the response was sent), time stamp (the combination of date and time), and the hash of the translated response message (translated Rupal Roxane's data) being sent to Hos 1.



```
Changing  Patient to  Patient            : Rupal_Roxane
Changing  Address to  Address            : 1548 S Sarrasota ln, Joliet, IL, 60434
Changing  Contact_number to  Contact_number  : 5551212
Changing  Date_of_Birth to  Birth_date  : 09/09/1950
Changing  Ethnicity to  Race             : White
Changing  MRN to  Medical_Record_Number  : IS45647
Changing  Marital_Status to  Marital_Status  : Unmarried
Changing  Patient_Class to  Pat_type  : Emergency
Changing  Patient_First_Name to  Pat_FName  : Rupal
Changing  Patient_Id to  Pro_Id          : 3631
Changing  Patient_Last_Name to  Pat_LName  : Roxane
Changing  SSN to   Soc_Sec_No           : 1679090881
Changing  Sex to    Gender              : Female
Changing  Encounter to  Visit           : V021520198080
Changing  Encounter_Number to  Visit_Number  : 21520198080
Changing  Encounter_class to  Visit_class  : Urgent
Changing  Encounter_date to  Visit_class  : 02/15/2019
Changing  Encounter_reason to  Visit_reason  : Elevated blood sugars and dehydration
Changing  Encounter_time to  Visit_time  : 9 AM
Changing  Provider_Id to  Pro_Id          : 909090
Changing  Medical_Condition to  Condition  : Diabetes
Changing  Date_of_Diagnosis to  Diagnosis_date  : 02/15/2019
Changing  Diagnosis_code to  Diagnosis_code  : E11.10
Changing  Provider to  Provider          : Andrea_Wilson
Changing  NPI to    National_Provider_identifier  : 7878787878
Changing  Provider_First_Name to  Pro_F_Name  : Andrea
Changing  Provider_Last_name to  Pro_L_name  : Wilson
Changing  Qualification to  Credentials  : MD, FACE, ECNU
Changing  Speciality_code to  Speciality_code  : 46
Changing  Prescribed__Action to  Prescribed__Service  : Rx_Glycated_Hemoglobin_test
Changing  Action_Date to  Service_name  : 02/15/2019
Changing  Action_Results to  Service_results  : Hemoglobin A1c : 6.10:
Changing  Action_code to  Service_code  : CPT: 83036
Changing  Prescribed__Drug to  Drug_Prescription  : Rx_Insulin
Changing  Dosage to  Dosage              : Administer U-500 insulin subcutaneously 2 to 3 times a
day approximately 30 minutes prior to start of a meal
Changing  Drug_code to  Drug_code       : J1815
Changing  Drug to   Drug                 : Insulin
Changing  Drug_name to  Drug_name  : Insulin (IL)
Changing  Action to  Service             : Glycated_Hemoglobin_test
Changing  Action_Name to  Service_name  : Glycated Hemoglobin (GH) test
Keeping   response notes    : Attached, please find Rupal Roxane's records for encounter date:
02/15/2019
```

Figure 18 Translated Response Message

Step 8: Upon receiving the response message, the security manager in Hos1 first decrypts the message, creates its hash, and later decrypts the digital signature of Hos 2 using Hos 2's public key. Once the response message passes the security check, the transaction validator is initiated, where Hos1 first checks if the response is complete or not (Figure 19). We assume that the records received are complete and are the one that were requested by Hos1. Hos1 clicks complete button. Upon clicking the complete button, the digital signer gets activated, which allows Hos1 to create its digital signature and digitally sign the transaction indicating that the request has been fulfilled. The transaction (Rupal Roxanne's record exchanged between Hos1 and 2) includes: Hos1's id (requestor), Hos 2's id (responder), request number (the combination of Hos1 id and date the request was sent), response number (Hos 2 Id and the date the response was sent), hash of the data exchanged between both Hos1 and Hos2, digital signatures of Hos1 and Hos2. Next, Hos 1 sends the validated transaction to the blockchain administrator to be included in the blockchain.

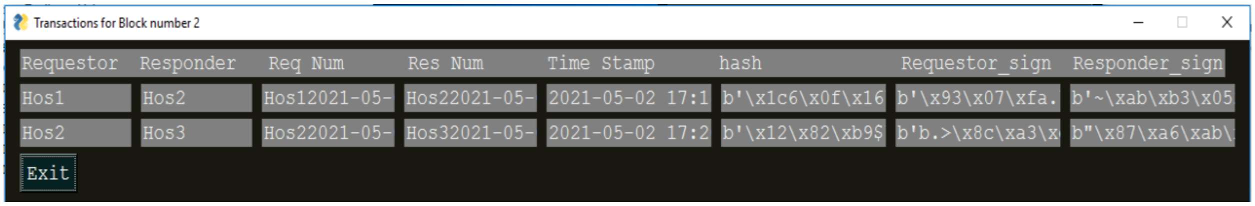


```
Response   Hos22021-05-02 17:14:15
Patient               : Rupal_Roxane
Address               : 1548 S Sarrasota ln, Joliet, IL, 60434
Contact_number        : 5551212
Birth_date            : 09/09/1950
Race                  : White
Medical_Record_Number  : IS45647
Marital_Status        : Unmarried
Pat_type              : Emergency
Pat_FName             : Rupal
Pro_Id                : 909090
Pat_LName             : Roxane
Soc_Sec_No            : 1679090881
Gender                : Female
Visit                 : V021520198080
Visit_Number          : 21520198080
Visit_class           : 02/15/2019
Visit_reason          : Elevated blood sugars and dehydration
Visit_time            : 9 AM
Condition             : Diabetes
Diagnosis_date        : 02/15/2019
```

Figure 19 Response Verification Interface

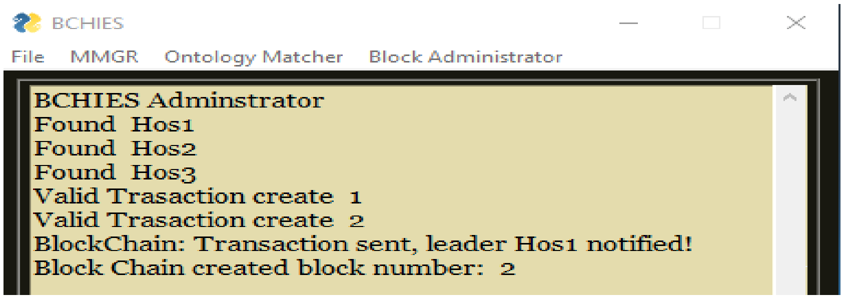
Similarly, Hos 2 receives Steve Apple's health records from Hos 3 by following the above process (similar to Hos 1 and Hos 2) and sends the validated transaction to blockchain administrator.

Step 9: Blockchain administrator receives two transactions to be added to the blockchain: one between Hos 1 and Hos2, and the other Hos 2 and Hos3 (Figure 20). Leader selector first selects a leader from members' list by generating a random number. Since there are three members' in our illustration, Hos1 gets selected as a leader randomly and is notified about it (Figure 21). Next Hos 1 creates a block labelled as block number 2. Block I represent a genesis block for the blockchain. Block number 2 includes: block number 2, hash of block number 2, time stamp, leader id i.e., Hos 1, leader signature i.e., Hos 1 digital signature, hash of genesis block i.e., block 1, merkle root, and number of transactions (that represents the block size) (Figure 22).



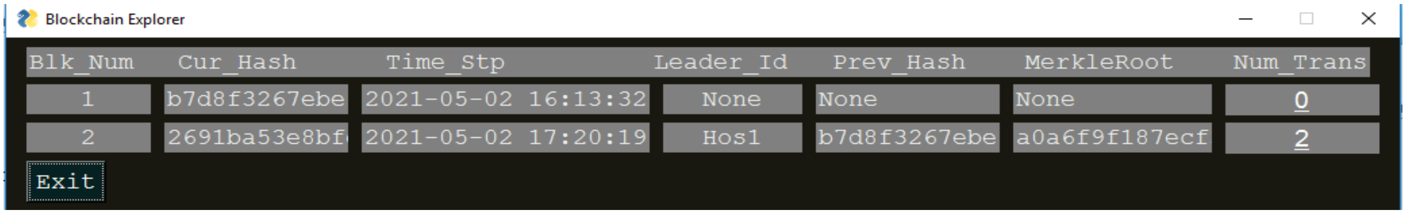
Requestor	Responder	Req Num	Res Num	Time Stamp	hash	Requestor_sign	Responder_sign
Hos1	Hos2	Hos12021-05-	Hos22021-05-	2021-05-02 17:1	b'\x1c6\x0f\x16	b'\x93\x07\xfa.	b'~\xab\xb3\x05
Hos2	Hos3	Hos22021-05-	Hos32021-05-	2021-05-02 17:2	b'\x12\x82\xb9$	b'b.>\x8c\xa3\x	b"\x87\xa6\xab\

Figure 20 Transactions for Block 2



```
BCHIES Adminstrator
Found  Hos1
Found  Hos2
Found  Hos3
Valid Trasaction create  1
Valid Trasaction create  2
BlockChain: Transaction sent, leader Hos1 notified!
Block Chain created block number:  2
```

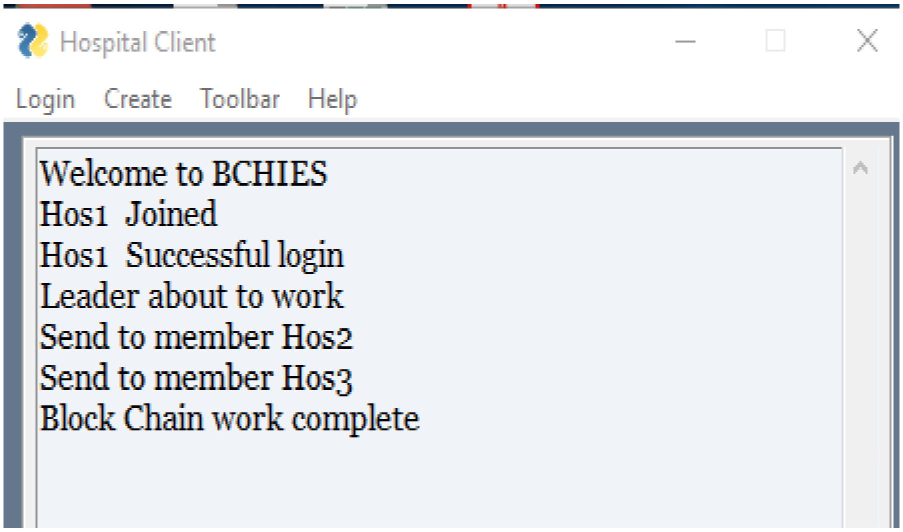
Figure 21 Leader Notification and Block Number 2 Creation



Blk_Num	Cur_Hash	Time_Stp	Leader_Id	Prev_Hash	MerkleRoot	Num_Trans
1	b7d8f3267ebe	2021-05-02 16:13:32	None	None	None	0
2	2691ba53e8bf	2021-05-02 17:20:19	Hos1	b7d8f3267ebe	a0a6f9f187ecf	2

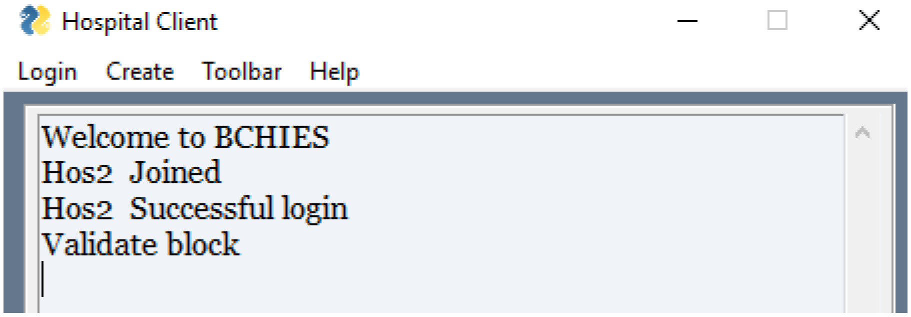
Figure 22 Block number 2

Step 10: After Hos 1 generates the block, it broadcasts the block to the entire network i.e., (members' other than the leader get the notification to validate the block). In this case the leader i.e., Hos 1 sends the block to Hos 2 and Hos 3 (Figure 23). Next, Hos 2 and Hos 3 get the notification to validate the block (Figure 24and 25). Hos 2 and Hos 3 validate the block by checking the correctness of the block by checking (1) hash of block 1 (2) the timestamp of the block i.e, block 2 should be greater than time stamp of the block 1 (3) the block size i.e., represented by number of 2 transactions in each block in our case (4) the hash of the block i.e., hash of the block 1 included in the block 2 should match the current hash value in block number 1 (5) authenticity of leader, which can be validated decrypting the digital signature of Hos 1 (leader) to validate authenticity and checking the context of the block. Once block 2 is validated, the message stating that "Block 2 is validated" is broadcasted to the entire network.



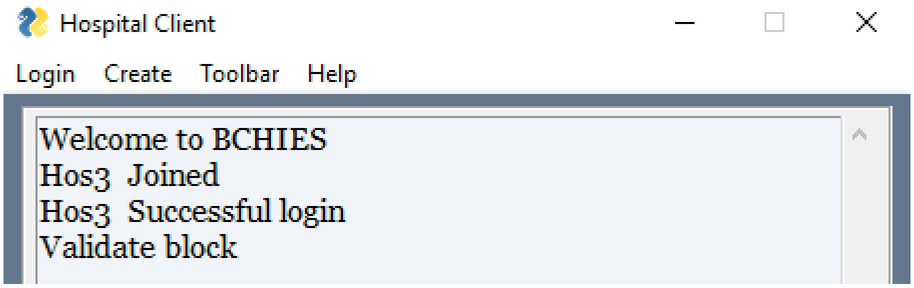
```
Welcome to BCHIES
Hos1  Joined
Hos1  Successful login
Leader about to work
Send to member Hos2
Send to member Hos3
Block Chain work complete
```

Figure 23 Block distribution to members' other than Leader



```
Welcome to BCHIES
Hos2  Joined
Hos2  Successful login
Validate block
```

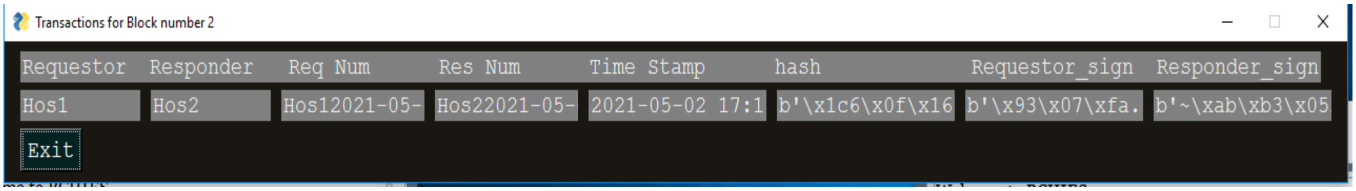
Figure 24 Hos 2 notified to validate the Block



Welcome to BCHIES
Hos3 Joined
Hos3 Successful login
Validate block

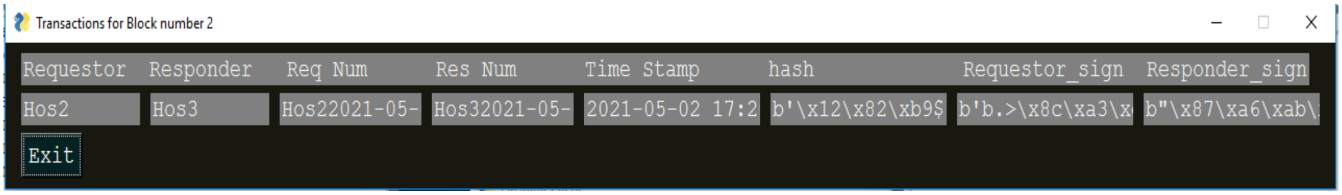
Figure 25 Hos 3 notified to validate the Block

Step 11: Next, Hos 1, 2 and 3 append the validated block to their own ledger. However, due to access control policies, the transaction view for Hos1, 2, and 3 will be different. Hos 1 will only be able to view transaction 1 in the block 2 (Figure 26). Hos 2 will be able to view both transaction 1 and 2 in block 2 as in both the transactions the data was either sent or received by Hos 2; Hos 3 will only able to view transaction 2 (Figure 27)



Requestor	Responder	Req Num	Res Num	Time Stamp	hash	Requestor_sign	Responder_sign
Hos1	Hos2	Hos12021-05-	Hos22021-05-	2021-05-02 17:1	b'\x1c6\x0f\x16	b'\x93\x07\xfa.	b'~\xab\xb3\x05

Figure 26 Transaction view of Hos 1



Requestor	Responder	Req Num	Res Num	Time Stamp	hash	Requestor_sign	Responder_sign
Hos2	Hos3	Hos22021-05-	Hos32021-05-	2021-05-02 17:2	b'\x12\x82\xb9$	b'b.>\x8c\xa3\x	b"\x87\xa6\xab\

Figure 27 Transaction view of Hos 3

4.6.2 Informed Argument

The informed argument (see Table1below) provides the relevance of the solution approach used in BCHIES from the previous studies as well as how each component resolves the issue stated in the article.

Table 1 Informed Argument

Challenges	**Components of BCHIES**	**Justifying comments of each component in BCHIES from previous literature**
Semantic interoperability conflict in HIE	Mapper, Mapping Validation Interface	Ontology mapping is one of the most effective ways to resolve semantic interoperability conflicts in different information systems. As ontologies are increasing in size and complexity, manually mapping different ontologies is tedious, erroneous, and not possible (Song et al., 2017). Manually mapping ontologies is a cognitively demanding task that involves high memory load and complex decision making (Dragisic et al., 2016). Therefore, there is a need to develop automatic ontology mapping approaches that assist domain experts by providing ontology mapping suggestions (Song et al., 2017). Automatic ontology mappings should be considered a first step in ontology mapping process, with the validation by domain expert at the later stages to ensure mapping quality (Dragisic et al., 2016). Having ontology mapping suggestions provide cognitive support to the users (Ivanova et al., 2015) and users validating automated ontology mapping suggestions ensures mapping quality. User validation enables the detection and removal of incorrect mappings and addition of potential mappings not detected by automated ontology alignment systems (Dragisic et al., 2016). Semantic annotations enable users to provide an explanation of the concept and verify the semantic relatedness between concepts (Pech et al., 2017). Ontology mappings can be used for various tasks such as ontology merging, query answering and data translation (Song et al., 2017).
Privacy of Healthcare organizations.	Mapping validation Interface:*MembersCanVaIdiateOwnMappings* *Rule*	(Carvalho, 2020) set a trader rule which only allowed traders to create, update, and retrieve information about their own assets as opposed to any information about any other traders. Setting different privileges for different users is important for proper functioning of blockchain in several domains where the organizations are not willing to disclose their local affairs and assets (Carvalho, 2020).
Privacy of the patients	Security Manager: Encryptor and Decryptor	Cryptography is used to conceal sensitive information from unauthorized parties (Siahaan, 2018). Studies such as (Harba, 2017; Prakash & Rajput, 2018; Siahaan, 2018) used a hybrid approach for secure data communication. The AES, a symmetric key algorithm, is one of the most effective and fast algorithms to encrypt and decrypt a large amount of data. It considerably reduces encryption times. But the major weakness of symmetric key encryption is finding a safe way to share the AES key with the other parties involved in the communication process (Castaldo and Cinque, 2018). On the other hand, asymmetric key involves both public and private keys. The strength of asymmetric cryptography is that it is a highly secure method and offers efficient scalability. However, its major weakness is that it is computationally intensive and thousand times slower than a symmetric key.

		Hence, using AES key allows encryption of vast amounts of data, increases speed, whereas encrypting AES with a symmetric key and sharing it with the recipient ensures high security (Harba, 2017; Prakash & Rajput, 2018; Siahaan, 2018).
Security: Data integrity	Security Manager: Hasher and Digital Signer	Digital signatures enable secure transferability of digital content by offering authenticity and integrity as well as non-repudiation of digital content (Amiri et al., 2018). A party can bind its identity to a piece of information by signing it with digital signature (Menezes et al., 1996). The seminal work by (Menezes et al., 1996) notes that hash function is one of the most efficient cryptographic methods to maintain the integrity of the data exchanged or shared between two entities. Instead of signing the document directly, the sender can hash the document and digitally sign the outputted hash. Signing the outputted hash instead of signing the whole document, speeds up the process (Thompson, 2017).
Security: User identifiability and Authentication	Authenticator	Public key cryptography is a mathematically related pair of public and private keys. Since it is computationally impossible to obtain a private key given its paired public key, public keys can be shared freely with anyone and can be used for identity, authentication and tamper-proofing (Zhang et al., 2018). In our research, we used a new mechanism where the authenticator requires the member to decrypt the encrypted authenticated message (one encrypted with members' public key) using its private key.
Secure privacy of patient data	Transactions storing hash of data exchanged	A well-designed healthcare application should limit the storage of encrypted sensitive patient data on blockchain. Instead, it may store some identifiable or some encrypted meta data that refers to actual patient data. In addition, it should allow the nodes obtaining or exchanging the data through a trusted channel that allows the nodes to retrieve data outside the blockchain, while ensuring data is genuine and untampered (Zhang et al., 2017). In a blockchain system, all patient data can be stored in the existing health system i.e., off-chain and can be shared across sites through secure blockchain network via API (Tanwar et al., 2020) using cryptographic algorithms (such as SHA-256 and 256 bit Elliptic curve digital signature) (Kuo et al., 2017), thus keeping the sensitive data out of blockchain.
Privacy of healthcare organizations	Distributed Ledger with*MembersCanReadOwnTransactions* Rule	Permissioned blockchain with appropriate permissions alleviates the problems of privacy of organizations who are not willing to disclose their local affairs. By setting appropriate permissions to make the transactions data viewable to few participants in the network, the challenge of privacy of organizations can be mitigated (Carvalho, 2020). To do so, (Carvalho, 2020) set a trade rule which prevent the other traders from having access to transactions involving a specific trader.
Trust among healthcare institutions	Member Registry	Knowing the identities of the participating nodes in the permissioned blockchain and allowing only known and vetted participants in the network makes the blockchain system more efficient and enhances trust among parties who know each other, but don't blindly trust each other (Carvalho, 2020).
Data provenance	Distributed Ledger	By replicating audit logs over a set of peers, blockchain deliver audibility, transparency (Hasselgren et al., 2020) as well as tamper-proof view of the system (Ahmad et al., 2018).

4.6.3 Comparison of BCHIES with Prior Blockchain based Solutions

The main purpose of this research was to design a new system that balances the need of resolving both security and semantic interoperability conflicts in HIE and healthcare institutions' requirement of storing and representing health information using distinct standards and naming conventions. Table 2 shows the comparison where system capabilities of BCHIES are compared with capabilities of the blockchain based systems proposed in the prior literature. The technical features of BCHIES can be divided into two groups: security (features 1 through 7) and semantic interoperability (features 8 through 11)

Table 2 Comparison of BCHIES with Prior Blockchain based Studies

Major BCHIES features	Explanation	Prior studies	BCHIES
1. Member Registry	Only known and vetted participants are allowed to join the network	(Yang & Yang, 2017; Yang et al., 2019; Zhang et al., 2018)	Y
2. Encrypted Authentication message	Verify member's authentication upon successful decryption of the authentication message that is encrypted with the public key of the member.	-	Y
3. Digital Signer	A message or data is indeed shared by the sender.	(Hylock & Zeng, 2019; Peterson et al., 2016; Wang et al., 2018; Yang et al., 2019; Zhang et al., 2018)	Y
4. Hasher	Protect the message from being tampered with or unauthorized modification	(Hylock & Zeng, 2019; Margheri et al., 2020; Peterson et al., 2016; Sri & Bhaskari, 2020; Wang et al., 2018; Yang et al., 2019)	Y

5. Double Encryptor and Decryptor	Encryption of the message with the AES key to enable large data sharing and later, encryption of the AES key with the recipient's public key to enable strong encryption mechanism to protect the shared AES key against unauthorized access and spoofing.	(Wang et al., 2018; Yang & Yang, 2017)	Y
6. Transactions storing hash of the data exchanged	Keep sensitive data out of the blockchain	(Peterson et al., 2016; Yang et al., 2019)	Y
7. Distributed Ledger with *MembersCanReadOwnTransactions* Rule	Privacy of the members who are not willing to disclose their local affairs.	-	Y
8. Mapper	Automated mappings of semantic correspondences between ontology elements of different members.	-	Y
9. Mapping Validation Interface	Manual inspection of the ontology mappings from the automated mapping process by the medical and health data experts.	-	Y
10. MembersCanValdiateOwnMappings Rule	Privacy of the members who are not willing to disclose their assets.	-	Y
11. Translator	Translate the incoming message from sender's format to recipient's format and vice-versa.	-	Y

4.7. THEORETICAL CONTRIBUTIONS

First, this research contributes to the literature on blockchain technology and healthcare by proposing an architecture to address the security and interoperability issues in health information exchange management. Several recent literatures claimed the importance of integrating blockchain with the health information exchange management (Dwivedi et al., 2019; Hylock & Zeng, 2019; Ivan, 2016; Kaur et al., 2018; Wang et al., 2018; Yang & Yang, 2017; Zhang et al., 2018). This novel architecture fills the gap by designing a blockchain based systems of cross -institutional health information exchange, which supports secure health data exchange, trust, and interoperability. This research presents solutions and guidelines on integrating blockchain technology and ontology mapping in the context of healthcare domain and presents methodological insights on blockchain structure design, data exchange, trust, and data interoperability.

Second, with the development of blockchain technology, increasing attention has been paid towards extending its applicability to health information systems (Hasselgren et al., 2020), thereby encouraging the development of collaborative applications (Ismail & Materwala, 2019). By developing a working prototype in which the proposed architecture is analyzed and also the functioning of the system in the healthcare domain is demonstrated, this research provides an example of applying blockchain technology into the healthcare domain. The research provides theoretical guidelines on integrating blockchain and ontology mapping together in health information exchange. The method proposed including blockchain structure design, data exchange, and data governance, and data interoperability contributes to the methodological and practical research on the implementation of blockchain to other non-financial sectors.

Third, the novel architecture and methods also contribute value to ontology literature. A formal ontology mapping interface is presented that is not merely restricted over identifying the possible matches between entities of different ontologies, but also a mean where the data experts can visualize the suggested mappings provided by the automated mapping algorithm, view the human readable definitions of all the entities as well as hierarchy between elements, and use that information to understand the suggested mappings, validate the accurate mappings, detect and remove inaccurate mappings, and potentially add the alternative mappings or new ones not detected by automated mapping algorithm. The proposed ontology mapping method and validation interface forms an effective solution to addresses the challenge of effectively complementing the automatic computation with human validation, providing human readable explanations for the suggested mappings, and minimizing user involvement when turning matches into mappings (Otero-Cerdeira et al., 2015). Hence, this research provides significant insights for ontology mapping research.

4.8 MANAGERIAL IMPLICATIONS

This research makes five managerial implications

First, this research helps with security, trust, and interoperability issues in healthcare practice. Different set of methods and tools have been developed in terms of addressing security, trust, and interoperability issues including data exchange, provenance, and interoperability. While the application area of blockchain in the healthcare domain is continuously expanding, the challenges of security, trust, and interoperability are still open issues in the healthcare domain. This research presents blockchain application in the context of healthcare domain with designing and presenting blockchain structure, working prototype, ontology mapping method, and ontology mapping verification interface. Development of proposed architecture and set of methods and toolkits have practical implications and insights on application of blockchain technology to other non-financial sectors.

Second, this research builds an organization centric blockchain based architecture named BCHIES that enables different healthcare providers to request access to their patients' records from the other healthcare providers virtually while still maintaining the security, privacy and integrity of EHRs. Since healthcare data is very highly sensitive, the proposal systems can encourage the healthcare institutions to share patient's data virtually without having to be overly concerned about hackers gaining unauthorized access to patients' data during virtual transmission. Hence, this research contributes to the practices in cross-institutional health information exchange by providing a useful reference on using new features of blockchain technology to solve the weaknesses of traditional health information exchange where patient records are faxed to other health care institutions, thereby improving and simplifying the sharing of electronic health records.

Third, this research also supports the healthcare institutions in practice in several ways. First, the strong authentication, and cryptographic algorithms (such as SHA-256 and 256-bit Elliptic curve digital signature) improves the security and trust level of the system, which is a vital issue in the virtual environment. Second, by defining several access permissions to enable the network only accessible to vetted and registered healthcare institutions with different views of the transactions in blockchain, the proposed research replaces the characteristic of anonymity and transparency with the privacy, which is vital in the healthcare domain.

Fourth, based on the validated ontology mappings, the proposed solutions automatically translate the incoming patient data from one healthcare provider format to another healthcare provider format. By doing so, the proposed solution relieves the healthcare providers from performing tedious work of translating and interpreting the data before reusing it, which ultimately can enable better patient care.

Lastly, this research also contributes to the practices in ontology mapping. Our semi-ontology mapping process provides cognitive support to data experts during ontology mapping process relieving them from the burden of manually mapping the elements of different ontologies which can be complex and cumbersome tasks.

4.9 LIMITATIONS AND FUTURE RESEARCH

Lack of adoption of a single authoritative messaging standard by different healthcare institutions has raised the issue of semantic interoperability conflict in HIE. In addition, secure HIE across cross institutions is still a major challenge. This study presents a blockchain based collaborative health information exchange system (BCHIES) that integrates blockchain and semi-automated ontology mapping to enable secure and interoperable HIE among healthcare institutions, while still enabling healthcare institutions to follow the messaging standards of their own choice. There are three categories of semantic conflicts that may arise due to adoption of different healthcare messaging standards: naming conflict, scaling conflict and confounding conflict. The proposed system is only restricted to resolving the naming conflict. The other conflicts such as scaling conflict and confounding conflict are out of the scope of the study. In the future, the proposed system will extend to resolve scaling and confounding conflicts. Secondly, performing a large number of transactions on blockchain can be expensive in terms of time and processing power. Our study doesn’t account for performance and scalability issues in the design of the proposed solution

CHAPTER 5 A NEW CONCEPTUAL MODEL FOR THE PRIVACY CONCERNS AND RICH USAGE OF VIDEO-CONFERENCING APPS FOR VIRTUAL COLLABORATIONS

5.1 INTRODUCTION

In recent years, consumer graded video conferencing applications (apps) such as Zoom, Skype, Microsoft teams, Google hangouts, CiscoWebEx etc. have become predominant communication tools for interacting and collaborating with others. VC apps enable the remotely present professionals to have direct two-way face to face dialouge with each other (Li et al., 2020). VC apps have the competence to enable audio, video, screen sharing, recording, digitally retrieving the recorded sessions (Li et al., 2020) as well as enable polling, white-board, and file sharing during the live conferencing session.

Because of the distinct capabilities listed above and its ability to transmit both verbal and non-verbal cues (Archibald et al., 2019; Hambley et al., 2007), and being a convenient (Archibald et al., 2019) and time effective substitute for face to face communications (Archibald et al., 2019; Hambley et al., 2007), video-conferencing has become a powerful means for individuals to maintain normalcy and continuity in their day to day operations during natural disasters or pandemic situations. For instance, during global COVID-19 pandemic, when social distancing and quarantine practices led to restructuring of workflows in many domains (Odedra et al., 2020) and consequently work from home became a new norm (Ahmad, 2020), VC apps became the most commonly used communication tool amongst the top business executives, government officials, researchers, schools, and organizations across the globe (Odedra et al., 2020; Walcott, 2020).

The ability to host webinars, conduct meetings, conferences and online training virtually rather than traveling onsite (Li et al., 2020) enabled the professionals to maintain continuity and normalcy in their working environment (Madrigal, 2020) while still adhering to the social distancing and quarantine practices. By transitioning their services from traditional face to face format to online format and being able to use various devices including mobile phones and laptops in the presence of reliable internet connection, VC apps enabled the individuals to reap the additional benefits of time saving, spatial flexibility, and convenient portability(Li et al., 2020).

Video conferencing tools emulates in person communications as well as enable the rapid exchange of information (Quan-Haase, 2012), circumvent the time-consuming process (Denstadli et al., 2012) and scheduling conflicts (Quan-Haase, 2012) of setting up a face to face meetings that the collaborators must attend, eliminates the cost (Denstadli et al., 2012; Quan-Haase, 2012) and inconvenience of travel as well as reduce the environmental stress (Denstadli et al., 2012).

Video conferencing tools are less costly and sometimes free of charge such as Skype (Denstadli et al., 2012), Zoom, and Google hangouts (Liu & Alexander, 2017) than the traditional communication tools such as telephone. These tools only require fairly basic terminal equipment (Negi Advocate, 2015) such as computers with an internet connection, a headset, and a webcam (Michels & Chang, 2011).

Although VC apps enable immense benefits, they also suffer from privacy risks (Boyle et al., 2009; Goodyear, 2019). For instance, in 2019, Zoom faced a security flaw that would leave the system open to malicious attacks that would have allowed the attackers to forcibly invite users to ghost zoom calls, reactivate the uninstalled zoom apps, without user permissions and stage denial of service attacks (Doffman, 2019), leaving 4 million users facing privacy violations (Heller, 2020). Despite individuals' concerns about privacy infringements by the video conferencing platforms, the use of VC in the professional contexts has significantly increased. For instance, a survey conducted by Morning consult 2 reported that about 17 percent of users who use VC apps use to communicate and interact with their peers are concerned about their security and privacy violations during VC calls. About 48 percent of respondents were worried that the content of their calls can be accessed by unauthorized users, consequently their privacy at risk. The above discussion concludes that while video conferencing delivers huge benefits and utility to professionals, this often comes at the expense of users' privacy violations. It becomes crucial to understand this double-edged dilemma: on one hand, individuals have strong beliefs about their privacy in the workspace; on the other hand, there has been a significant rise in their adoption and usage of these video conferencing applications. While the issue of privacy violations in video conferencing platforms is critical, it has not achieved much attention in the prior literature. The review of the literature reveals (Table 3 in Appendix) that there is no such study in the past which has investigated individuals' intentions to use video-conferencing platforms for collaboration, despite the privacy risks associated with its usage. For instance, prior research (Brown et al., 2010) has only investigated the use of proprietary collaborative technologies. The investigation of consumer off the shelf video conferencing applications is lacking in the prior literature. Third, prior studies in collaborative technologies have only investigated the continued intentions to use VC apps. Investigation of rich usage and its effect on continued intentions is not investigated in the VC apps, which is the focus of this

[2] https://morningconsult.com/wp-content/uploads/2020/04/200415_crosstabs_CONTENT_CORONAVIRUS_Adults_v1_AUTO.pdf

study. Thatcher et al. (2018) categorize the system use in two categories: active use and automatic use. Deep structure usage and trying to innovate falls under active use and continuance intentions falls under automatic use. While the existence of different levels of system usage and their antecedents and consequences are widely recognized in the IS literature (Burton-Jones & Straub Jr, 2006), prior studies in the context of VC apps have only investigated the automatic use (continuance intentions) of VC apps. None of the studies investigated rich usage and lean usage of VC apps. By investigating the rich and lean usage, the studies can provide rich insights into the nature and use of technology in specific contexts (Burton-Jones & Straub Jr, 2006). Hence, to fill the gap in the prior research, this research is guided by the following research question: *How do the contrary beliefs i.e., perceived risks and benefits influence professionals' attitude towards VC apps and consequently its active (lean usage and very rich use) and automatic use (continuance intentions)?*

We address the above research question by developing a conceptual model that combine privacy calculus theory, social presence theory, ubiquity and mobile user's information privacy concerns (MUIPC). In addition, we investigate the active (lean and rich use) and automatic (continued intentions) use of VC apps. i.e. we investigate lean usage by investigating professional's intensity of use of VC apps through use behavior and rich usage by investigating both cognitive absorption and deep structure usage of VC apps.

This study makes four significant contributions. First, this study increases our understanding of professionals' attitude towards VC apps, despite the privacy risk associated with its usage. It throws light on the usefulness of the dual path of privacy calculus theory to analyze novel and emerging technologies that have reshaped the professional environment during pandemic. Second, this study builds on the prior literature in the areas of privacy calculus, MUIPC, and ubiquity that are significant to the virtual collaborative technologies. Hence, this study contributes to the continuum of knowledge that parallels the progression of contemporary technologies as they move through stages of inflated expectation to the plateau of productivity. Third, this study investigated the impact of both socially derived and technologically derived characteristics in influencing professionals' perceptions of benefits achieved with using VC apps. Yoo and Alavi (2001) notes that to gain a better understanding of how user's perceptions of media are formed, it is very crucial to form a theoretical integration of both mechanical (physical characteristics) and socially constructed characteristics (Yoo & Alavi, 2001). Therefore, the lack of investigation of both social and technological characteristics of VC apps in the prior literature obstructs us from having a complete understanding of what media characteristics of VC apps facilitates its usage and continued use in professional context. By Investigating both socially derived and technological characteristics, this study enhances our understanding of how professionals' perceptions of VC apps are formed.

5.2 THEORETICAL BACKGROUND

5.2.1 Privacy Calculus Theory

Culnan and Armstrong (1999) noted that individuals are willing to disclose their personal information in exchange for social and economic benefits, provided their personal information will be used fairly (Culnan & Armstrong, 1999).

The concept of calculus was introduced by Laufer and Wolfe (1977) where the authors stated that an individual's decision to disclose personal information depends on *expected benefits and unpredictable consequences*.

Later Culnan and Armstrong (1999) found that an individual's decision to disclose personal information involves privacy calculus wherein the expected benefits are weighed against the unpredictable consequences. Further, Culnan and Armstrong (1999) noted that Individuals are willing to disclose their personal information to vendors, when they are explicitly informed that fair information practices have been deployed by the vendors to protect their personal information (Culnan & Armstrong, 1999).

Later Dinev and Hart (2006) extended the privacy calculus model in the context of e-commerce. In this model the authors argue that when making transactions over the internet and disclosing the personal information, individual's behavior is influenced by a set of contrary beliefs including privacy risks, privacy concerns, trust, and personal interest. In such cases, the influence of one belief may outweigh the other resulting in either positive intentions to disclose personal information or rejection of disclosure of information.

Next Wilson and Valacich (2012) extended privacy calculus by adding situational factors to the privacy calculus model and argued that within privacy calculus, economic and social benefits, personalization or convenience benefits tend to override the perceived risks (Wilson & Valacich, 2012). In utilizing privacy calculus, Dinev and Hart (2006) and (Wilson & Valacich, 2012) used perceived risks and benefits as an independent construct.

Privacy calculus has been empirically examined in technologies other than VC apps such as location-based services in mobile devices (Xu et al., 2009), location aware marketing in mobile devices (Xu et al., 2011), e-commerce (Li et al., 2010), social networking systems (SNSs) (Krasnova et al., 2012), location based social network services (Zhao et al., 2012), mobile applications (Keith et al., 2016), hotel apps (Morosan & DeFranco, 2015), healthcare wearable devices (Li et al., 2016), personalized nutrition services (Berezowska et al., 2015), mobile Applications (Pentina et al., 2016), mobile hotel booking loyalty (Ozturk et al., 2017), and pay-As-You-Live (PAYL) services (Wiegard & Breitner, 2019). However, privacy calculus has never been tested in the context of VC applications, which is the focus of this study.

5.2.2 Social Presence Theory

Users are motivated to utilize media to modulate social presence for diverse activities including problem solving and making decisions, exchanging opinions, resolving conflicts, getting to know someone or maintaining family relations. Various technologies are progressively designed, engineered and manufactured to increase social presence and are referred to as social presence technologies (Biocca et al., 2003). Few examples of evolving social presence technologies include mediated collaborative environments, mobile and wireless telecommunications, high bandwidth teleconferencing interfaces, agent-based e-commerce and help interfaces, speech interfaces, and 3D social virtual environments (Biocca et al., 2003).

Research on social presence in the context of mobile devices is clearly of importance to researchers and typically seeks to explore the impacts of social presence on various dependent variables such as: intentions to use, greater purchases, positive attitude, learner satisfaction etc.

The concept of social presence was introduced by (Short et al., 1976). Short et al. (1976) notes that social presence is a significant factor in understanding individual to individual communications. (Short et al., 1976) defined social presence as the "the degree of salience of the other person in the interaction and the consequent salience of the interpersonal relationships" (Short et al., 1976)(p.65). In other words, it represents the degree to which an individual in the communication is perceived as "real person". The authors consider social presence as the quality of the medium. They hypothesize that communications media differ in their degree of social presence and these disparities are critical in determining the way individuals interact. The factors such as: the capacity to transmit information about facial expression, posture, direction of looking, dress, and non-verbal cues, all contribute towards social presence of a communication medium. Thus, the social presence is highest in face to face communications, followed by video, audio, and written memos.

Short et al. (1976) also noted that social presence impacts the nature of interaction and interacts with the objective of the interaction to influence the medium chosen by the user who wishes to communicate. Short et al. (1976) also hypothesized that users of any given communications medium are in some sense familiar with the degree of social presence of the medium and prefer to avoid utilizing the medium for specific types of interactions, specifically, the interactions that demand a higher degree of social presence than they perceive the medium to have. Short et al. (1976) conceived social presence of a medium as a perceptual or attitudinal dimension of the individual utilizing the medium, and it is the individuals who determine how the factors listed above contribute towards social presence of a communication medium. The individuals provide self-report measures of the subjective quality of the communication medium and judge it as being unsociable-sociable, insensitive-sensitive, cold-warm and impersonal - personal (Short et al., 1976).

5.2.3 Ubiquity

Ubiquity is clearly of importance to researchers in various fields including IS and typically seeks to explore the effects of ubiquity on various dependent variables, such as the attitudes and intentions to adopt mobile services, post adoption behaviors/continuance intentions to use mobile services etc.

The conceptualization of ubiquity came into existence in 2002. At that time, ubiquity was discussed in the context of U-commerce (Watson et al., 2002), wireless advertising (Barnes, 2002), and mobile commerce (Balasubraman et al., 2002). Each study provided a different notion of ubiquity. In 2002, Watson et al. (2002) envisioned an advent of a multi-faceted u-commerce, where u represents ubiquitous, universal, unique and unison. (Watson et al., 2002) stated “ubiquity or omnipresence of computer chips means not only that they are everywhere but also they are in, a sense ‘nowhere ‘for they become invisible as we no longer notice them” (Watson et al., 2002) (p.336). Barnes (2002) noted that “Ubiquitous interactivity can give the customer ever more control over what they see, read and hear” (Barnes, 2002) (p.412). Balasubraman et al. (2002) later introduced as ubiquity as a concept of “anywhere anytime”.

Later Junglas and Watson (2006) proposed four high level constructs of u-commerce: ubiquity, uniqueness, universality, and unison. The authors described ubiquity as “the drive to have access to information unconstrained by time and space” (Junglas & Watson, 2006) (p.578). The authors also proposed that ubiquity consists of three sub-dimensions: reachability, accessibility and portability. However, the study by (Junglas & Watson, 2006) was also purely conceptual.

Okazaki et al. (2012) conceptualized ubiquity as “the interconnectedness dimension of time savings and spatial flexibility” (p.172). Time savings refers to the mental calculation performed by the user of the time saved when performing tasks using a mobile service. Spatial flexibility refers to the perceived mobility provided by the mobile service to a user to perform tasks without being restricted at one place (Okazaki et al., 2012).

Later Okazaki and Mendez (2013) developed and tested a formal measurement instrument for perceived ubiquity for mobile services including four dimensions: continuity, immediacy, portability, and searchability (Okazaki & Mendez, 2013). The resulting scale is composed of 12 items. Immediacy relates to the speed or quickness of an action or occurrence and represents the extent to which a mobile service makes an action or occurrence as quick, rapid and instant. Portability, a synonym to mobility relates to the physical characteristics of the mobile devices. It refers to the quality or state of being light enough or mobile, and specifically pertains to something that can be utilized while in transit. Continuity relates to the capability of being always connected and represents the extent to which mobile services can be used without interrupting ongoing tasks. Searchability refers to the capability of mobile services to enable users to search information or data without the restrictions of time and space(Okazaki & Mendez, 2013).

In a review of prior studies, Biocca (2003) identified four key themes where social presence has been measured: perceived social richness of the medium, involvement, immediacy or intimacy, social judgement of others, and sense of being together. Of the four themes, Biocca (2003) noted that perceived social richness of the medium was the most widely used construct. As per this construct, users do not assess their experience of others, but indirectly assess the effect of the medium, i.e., the social and emotional capabilities of the communication medium (Biocca, 2003). In this study we use perceived social richness of the medium, since one of our research objectives was to determine how professionals assess the social and emotional capabilities of VC apps.

5.3 RESEARCH MODEL

Figure 28 represents the proposed research for our study.

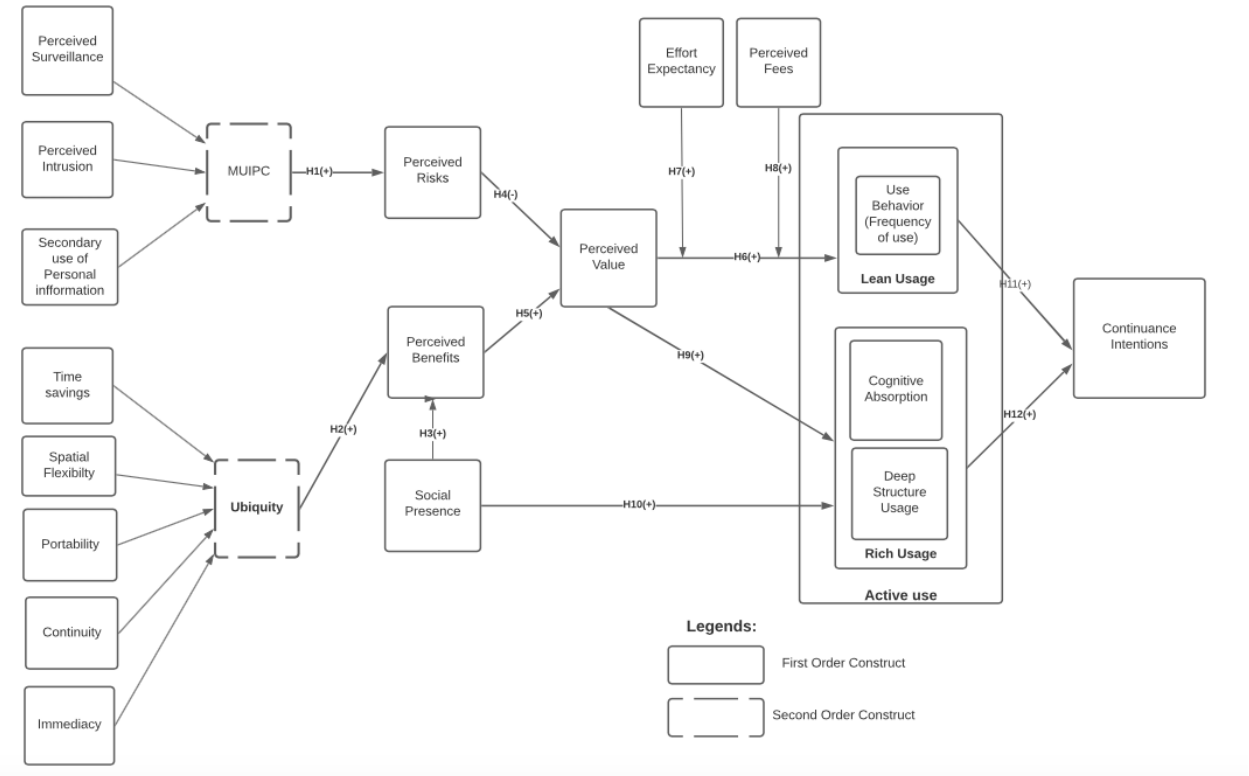


Figure 28 Research Model

5.3.1 Mobile Users Information Privacy concerns (MUIPC)

Privacy concerns is one of the most commonly studied constructs in the empirical literature (Belanger & Crossler, 2019). Related research has mainly investigated two key conceptualizations of privacy concerns: concerns for information privacy (CFIP) proposed by (Smith et al., 1996) and the Internet user’s information privacy concerns (IUIPC) proposed by (Malhotra et al., 2004). CFIP was developed to measure individuals’ concerns around organizational information privacy practices, whereas IUIPC was proposed to measure Internet user’s information privacy concerns. Building upon these two privacy related constructs and drawing on communication privacy management theory, (Xu et al., 2012) proposed mobile users’ information privacy concerns (MUIPC) to measure users’ privacy concerns in the context of mobile environment.

Due to aggressive practices of data collection and sharing employed by applications running on mobile devices, privacy concerns of mobile users are likely to be different from online users (Xu et al., 2012). Enhanced capabilities of mobile devices such as sensors, cameras, microphone, GPS, and accelerometer enable mobile applications to profile and target specific individuals. Mobile apps have the potential to record extremely sensitive and private information such as contacts, photos, videos, daily conversations, and location information. Such powerful eavesdropping capabilities aptly raise significant privacy concerns (Mirzamohammadi & Sani, 2018). MUIPC is thus considered a suitable and valid instrument to investigate privacy concerns of users in the mobile environment (Degirmenci, 2020). It is important to note that, regardless of the context, prior privacy literature has considered privacy concerns as a predictor of both perceived privacy risks and trust (Kehr et al., 2015; Malhotra et al., 2004; Van Slyke et al., 2006; Wu et al., 2015).

MUIPC consists of three dimensions: perceived surveillance, perceived intrusion, and secondary use of personal information. Perceived surveillance is the mobile users' concern regarding personal information watched, listened or recorded. Perceived intrusion relates to mobile users' concern of mobile apps possessing or soliciting users' personal information, and creating discomfort, interruption, and harm through unwanted presence. Secondary use of personal information relates to concerns about vendors using personal information for secondary purposes or revealing it to unauthorized entities without consent or awareness of the mobile app user (Xu et al., 2012).

We use MUIPC as the instrument of our study because our main interest is mobile VC apps, and our focus is on professionals utilizing the mobile environment for virtual collaboration and communication.

5.3.1.1. Perceived Surveillance

Perceived surveillance represents mobile users' concern regarding their personal information including activities getting watched, listened to or recorded by various entities including vendors (Xu et al., 2012), government (Solove, 2005). Surveillance of mobile users has drastically increased over the past years' due rapid advancements in mobile technologies and its various functionalities such as emails, web-browsers, photos, calendars, contact lists etc. (Xu et al., 2012) . Through these functionalities, vendors are able to collect information about users' identities, schedules, real time location, time spent on different applications, contact lists etc. (Xu et al., 2012). The highly interactive nature of video-platforms not only provides indisputable advantages (Venkatesh et al., 2009), but also raises concerns of surveillance of the users participating in these video-based calls (Shupei Yuan et al., 2016).

5.3.1.2. Perceived Intrusion

Perceived intrusion relates to mobile users' concern regarding malicious apps interrupting their daily activities through the unwanted presence (Xu et al., 2012). Malware is an increasing concern for mobile devices and malware developers can access excessive amounts of data including keyword stroke cache, usage pattern of apps, and browser history etc. (Xu et al., 2012). Video based calls can be invasive since they reveal too much information about the user's appearances, place or behavioral context (Neustaedter et al., 2015). In a study by (Neustaedter et al., 2015), the individuals raised the desire to maintain autonomy over what was visible over video-based calling (Neustaedter et al., 2015). The flaws in the implementation or even deliberate backdoors in the system can allow others (Clarke & Ali, 2017) to monitor or record user's activities through video-conferencing platforms. In a study by (Lupton, 2014), the professionals have stated that the use of mobile based apps either for collaboration or interaction with their peers have blurred the boundaries of professional and personal life (Lupton, 2014). The professionals have raised the concerns of their ideas getting plagiarized, if an attacker intrudes into the mobile devices (Dermentzi et al., 2016; Lupton, 2014), record their conversations (Neustaedter et al., 2015) or leak their ideas (Dermentzi et al., 2016) .

5.3.1.3. Secondary use of Personal Information

Secondary use of personal information relates to mobile users' concern over the vendors using their personal information for secondary purposes or revealing it to unauthorized entities without their consent or awareness (Xu et al., 2012). Zoom clearly states in its privacy policy that whether a user has a Zoom account or not, Zoom may collect the user's personal information when a user uses Zoom or otherwise interacts with its product. Zoom collects this information from users' devices or from someone who communicates with the user using Zoom services. Zoom also gathers users' personal information from third party vendors and also shares users' information with Google Ads and Analytics. Zoom stated they process users' information with users' consent (where necessary). Under selling personal information section in their privacy policy, zoom states that it may use certain advertising tools such as Google Analytics and Google Ads. Sharing users' information may fall under the broader definition of sale of the personal information under certain state laws. Google may further use this data for advertising purposes. In their privacy policy, Zoom states that they process users' personal information with users' consent "where necessary". This "where necessary" suggests that zoom processes users' information and shares it with other parties with or without users' consent. Individuals' worries about the opportunistic behavior of online vendors with regards to information handling can increase individuals' risks beliefs and lower their trusting beliefs in online vendors (Bansal et al., 2016; Malhotra et al., 2004) in the similar manner that distrust tends to augment and perpetuate distrust (Bansal et al., 2016).

Based on the above discussion, we postulate that

H1. Mobile Users' Information Privacy Concerns (MUIPC) have a positive effect on Perceived risks of video-conferencing applications

5.3.2 Ubiquity

Perceived ubiquity of mobile devices overcomes the three time-space spatial constraints of Information technology: Coupling (i.e., requiring the user to be present at a specific time and space) and capability “which refers to the user’s resources and ability to overcome spatial separation at a specific moment” (Okazaki et al., 2009) (p.67), time- space zones which limits users access to particular schedules or hours of services.

In order to measure, ubiquity, (Okazaki & Mendez, 2013) developed and tested a formal measurement instrument for perceived ubiquity for mobile services including four dimensions: continuity, immediacy, portability, and searchability (Okazaki & Mendez, 2013). Continuity relates to the state or aspect of being continuous i.e., the unique ability of mobile devices to provide continuous access to services that can’t be offered by traditional channels. Immediacy relates to quickness of an action or occurrence. Portability represents the quality of being light enough to be carried out and therefore refers to the physical attribute of a mobile device. Searchability refers to the ability of making thorough examinations (Okazaki & Mendez, 2013).

In this research context, ubiquity means that with the help of mobile terminals, users can access video-conferencing apps at anytime and anywhere.

5.3.2.1. Time savings

Time is a critical resource that impacts consumers' decision making. For any given consumer, time is scarce and exists in limited and finite quantities. Therefore, time has value. It can be both antecedent, a consequence, or both (Jacoby et al., 1976). Time savings means reallocating the time from one activity to another to achieve higher efficiency (Feldman & Hornik, 1981). "The satisfaction derived from many products and services depends upon both the amount of time spent and the time during which they are consumed" (Feldman & Hornik, 1981) (p.407). Time unlike monetary income and price constraints choice (Becker, 1965). Every human activity utilizes three resources: time, space and money and each of these resources are utilized in varying degrees. An individual's time allocation decision is impacted by the availability of all of three resources (Feldman & Hornik, 1981). Thus, the consumers, for whom time, space, and money are scarce (e.g., a researcher) may choose videoconferencing meeting over traditional face to face meeting.

Time and space are interrelated dimensions of human behavior. A temporal deadline often obstructs space (Feldman & Hornik, 1981). Consumers' attitude and perceptions are really critical for service industries in which waiting time impacts consumer's satisfaction as well as service quality (Durrande-Moreau & Usunier, 1999). The author categories time into two categories: objective time and subjective time. Objective time is a time that can be measured by clocks, watches and chronometers (Durrande-Moreau & Usunier, 1999). On the contrary, the subjective time is the time that can be measured by recording users' perception of time saved or spent while performing any activity (Davis & Vollmann, 1990). During subjective measurement, consumers perform a mental calculation of the perceived time that could be saved by participating in any activity (Okazaki et al., 2012). Our study focuses on subjective time i.e., measure individuals' perceptions of time that could be saved by using video-conferencing apps.

Video- conferencing apps enable the collaborating partners to meet, communicate and get their work accomplished without physically getting together in one place (Armfield et al., 2015) (Jimenez et al., 2017), resulting in considerable amount of time savings (Armfield et al., 2015).

5.3.2.2. Spatial Flexibility

One of the main characteristics of mobile devices/services is that the communications in mobile devices/services is not dependent upon a physical fixed location meaning mobile devices/services enables spatial flexibility (Balasubraman et al., 2002). This characteristic of spatial independence enables several benefits such as enhanced productivity, ability to contact anyone from anywhere and anytime, and flexibility to coordinate meetings with peers and family (Jarvenpaa et al., 2003). For instance, when attending a traditional face to face meeting, the meeting attendee is constrained to the meeting at the scheduled time and at a location where all the other attendees are present. By contrast, with the video-conferencing apps, the ubiquity enabled by VC apps have expanded the professional's communications beyond the office environment by enabling flexibility in scheduling and eliminating time restrictions that would otherwise restrict the professionals to collaborate with their peers from 9 till 5 in their office. The spatial flexibility feature of video-conferencing apps allows the individuals to get their task accomplished without physically getting together in one place (Jimenez et al., 2017). Video-conferencing apps enable the researchers to bridge the geographical and spatial distance to work on different research projects that otherwise wouldn't exist if they were separated by space and time (Boateng & Tutu, 2018).

5.3.2.3. Portability

Portability refers to the physical attribute of a mobile device. *Portability* represents the quality of being light enough to be carried out for long periods of time (Junglas & Watson, 2006). In their definition of mobile devices, Junglas and Watson (2006) included cellular phones, wireless laptops, smartphones, communicators, personal digital assistants etc. Junglas and Watson (2006) further note that this distinct characteristic of mobile devices enables the other constructs such as reachability, accessibility, spatial and time flexibility to be unique and distinct from traditional e-commerce settings. Reachability, accessibility, spatial and time flexibility are built in characteristics of the mobile world -if -and only if -they occur in the context of portability (Junglas & Watson, 2006). The fact that the individuals can always carry their mobile devices with them, and the device is nearly always on makes the synchronized communications possible whenever and wherever (Gao et al., 2009). Portability has enabled high levels of mobility in our professional and social life. Portability has enabled individuals to rethink how they can perform their jobs effectively and efficiently (Garfield, 2005). In the previous literature, portability has been one of the main factors that influences the users' intentions to use mobile devices/services (Zhou, 2012).

5.3.2.4. Continuity

Continuity relates to the state or aspect of being continuous i.e., the unique ability of mobile devices to provide continuous access to services that can't be offered by traditional channels (Okazaki et al., 2012). The continuity characteristic of mobile devices enables the consumers to use these devices while they are on the move, at anytime and anywhere (Wang et al., 2016). The video conferencing platforms such as Skype, Zoom, Hangout Meets supports both smartphones and laptops. The ability to access video-conferencing tools on smartphones or utilize mobile data to connect laptop or iPad to the internet gives researchers an "always available link" to reach their peers beyond their spatial differences.

5.3.2.4. Immediacy

The tasks such as negotiation, decision making or instant feedback which require back and forth transmission of small quantities of information, require availability of both the parties at the same time (Straub & Karahanna, 1998). Individuals chose collaboration technologies based on their ability to reach their partner i.e., whether the collaborating partner is immediately available for communication or not (Straub & Karahanna, 1998). This is referred to as Immediacy. The greater the likelihood that a communication partner is available for communication, the less likely is an individual to choose an asynchronous medium such as email (Straub & Karahanna, 1998). The technologies with higher immediacy are perceived to be more effective and efficient (Brown et al., 2010). Since professionals use video-based collaboration tools for discussion and negotiation etc., they likely need immediate availability of their partners and will perceive benefits in using video-based conferencing tools.

Based on the above discussion, we hypothesize that:

H2. Ubiquity has a positive effect on Perceived Benefits

5.3.3 Social Presence

The collaboration technologies with low social presence can lead to slower interaction and can make communication difficult, which can further have negative impact on efficiency, effectiveness and consumer's satisfaction (Brown et al., 2010; Hassanein & Head, 2004). The greater social presence a technology exhibits, the more useful a technology is seen (Hassanein & Head, 2004).

The ability of video-conferencing platforms to emulate in person communications is mainly due to the presence of social cues that promote more interactivity and reciprocity among communicators (Choi, 2016). The video-based platforms are regarded as the second best to face to face interactions due to presence of variety of verbal and non-verbal cues including facial expressions (Rincón-Nigro & Deng, 2013; Zamir et al., 2018), voice prosody and gestures (Rincón-Nigro & Deng, 2013), eye gaze, head orientation which are not present in asynchronous and telephone calls (Zamir et al., 2018), instant messaging in mobile devices (Rincón-Nigro & Deng, 2013), or social network systems (Choi, 2016). The presence of these cues enables the individuals to express personal feelings and emotions similar to face to face communications and hence promote higher social presence and may therefore foster reactions such as perceived usefulness, ease of use (Hew et al., 2018) to enhanced performance and usefulness (Brown et al., 2010).

H 03: Social presence positively impacts perceived benefits of *video-conferencing apps*

5.3.4 Privacy Calculus

Despite the potential risk associated with personal information disclosure in varying contexts, individuals continue to share their personal information, when conducting business transactions or communicating with others offline or online (Kordzadeh & Warren, 2017). This inconsistent behavior is explained by privacy calculus theory. Privacy calculus, also consistent with the widely used economic technique called cost-benefit analysis (Culnan & Bies, 2003) claims that consumers perform risk benefit analysis of the motivational factors that enable and prevent information disclosure, before allowing product/ service producers to access their personal information (Culnan & Armstrong, 1999). The individuals are willing to disclose their personal information in exchange for social and economic benefits, provided their personal information will be used fairly (Culnan & Armstrong, 1999). "Cost/benefit analysis is used for evaluating the costs and benefits of a course of action in monetary terms to decide on whether to follow that course of action or not" (Kordzadeh & Warren, 2017)(p.49). The cost benefit analysis not only applies to monetary contexts, but also has been extended to non-monetary contexts as well (Kordzadeh & Warren, 2017). However, consumers disclose their personal information when they use these products/services. Therefore, in this research we use privacy calculus to investigate the simultaneous impacts of perceived benefits and perceived privacy costs on professionals' perceptions of value and in turn continued intentions to use video-conferencing apps. In line with the privacy calculus theory, we assert that when professionals use the video-conferencing apps for their work related tasks, they perform the cost (risk)-benefit analysis of the motivational factors that influences their perceptions of value that further enable or inhibit their intentions to use/continuance usage of video-conferencing apps.

5.3.4.1. Perceived Benefits

Users can derive many benefits from using mobile apps including but not limited to, personalization (Xu et al., 2009), perceived usefulness, ease of use (Keith et al., 2016), positive community outcomes of communicating personal health information (Kordzadeh & Warren, 2017). Perceived benefits impact individuals' intentions to use/ adopt a mobile app or disclose personal information on these mobile apps (Keith et al., 2016). Video-conferencing apps can provide various benefits such as social presence (Brown et al., 2010), ubiquity (Jimenez et al., 2017) and monetary and non-monetary cost savings (Armfield et al., 2015; Denstadli et al., 2012; Quan-Haase, 2012). If professionals feel that they can gain these benefits from using video-conferencing apps, they will generally renounce some levels of their privacy for potential benefits while using video-conferencing apps. VC apps through its unique characteristics of ubiquity and social presence offer unique advantages to professionals' in terms of ease of use and their enhanced performance, effectiveness in competing work-related tasks. Thus, higher anticipation of VC apps' benefits should lead to a higher perception of utility of VC apps leading to positive influence of perceived benefits on perceived value achieved with using VC apps.

5.3.4.2. Perceived Risks

Perceived risk is one of the critical factors in several IS adoption models. "It reflects user's perceptions of the uncertainty and adverse consequences of engaging in any activity" (Shunbo Yuan et al., 2016)(p.24). Perceived risk is a negative factor that impacts consumers' trust and discourages them from using or intent to use the product/service (Rouibah et al., 2016). In terms of mobile apps usage, some studies claimed that perceived risk is one of the main determinants of user's continuance intentions (Natarajan et al., 2018; Qin et al., 2016). Perceived risks perforate the technology adoption/usage decisions when the circumstances of decision state situation create discomfort and /or anxiety, feeling of uncertainty, concern, conflict arouse in the consumer, pain due to anxiety, cognitive dissonance, and psychological discomfort (Featherman & Pavlou, 2003). Perceived risks have been recognized as having many dimensions including performance, financial time, safety, social, privacy, and psychological risks (Featherman & Pavlou, 2003). Perceived privacy risk can be more influential than economic risks in discouraging individuals from conducting online transactions. Perceived risks relate to an opportunistic behavior related to obtaining personal information submitted by internet users (Dinev & Hart, 2006). Sources of opportunistic behavior include selling and sharing users' personal information with the parties not involved in immediate transactions such as: third parties, financial institutions, and government agencies (Dinev & Hart, 2006). Perceived risks indicate a belief that amounts to an assessment of a technology in general, may it be internet websites (Dinev & Hart, 2006), mobile payment platforms (Shao et al., 2019). Privacy risks relate to an assessment of organizational opportunistic behavior related to obtaining personal information of users (Dinev & Hart, 2006). In the context of video-conferencing apps, improper handling of personal information could result in jeopardizing professionals' careers, plagiarism of researcher's ideas, commercialization of copyright and content issues (Dermentzi et al., 2016; Lupton, 2014) and therefore negatively influence their perceptions of value (Shaw & Sergueeva, 2019; Wiegard & Breitner, 2019; Xu et al., 2011). In privacy literature, privacy risk is considered as a single dimensional construct (Dinev & Hart, 2006; Malhotra et al., 2004). Consistent with the literature, we also measure privacy risks as single dimensional and hypothesize that:

H04. Perceived Risks have a negative effect on Perceived Value

H05. Perceived Benefits have a positive effect on Perceived Value

5.3.5 Perceived Value

Perceived value represents "the consumer's overall assessment of the utility of a product based on perceptions of what is received and what is given" (Zeithaml, 1988). Perceived value can therefore be thought of as an overall estimation of the choice object and once that overall estimation is internalized, it becomes a criterion for a consumer to decide their choice behavior (Kim et al., 2007; Xu et al., 2009) such as adoption intentions (Kim et al., 2007), use intentions (Shaw & Sergueeva, 2019), or willingness to have personal information used by service vendors (Xu et al., 2009). While most of the extant literature have excluded perceived value as an explicit latent variable in the framework of privacy calculus model, (Morosan & DeFranco, 2015; Shaw & Sergueeva, 2019; Xu et al., 2011) considered perceived value as an explicit variable that completes privacy calculus model, as it represents a natural evaluative artifact that aggregates the benefit risk assessment process of users' guiding their behavioral decisions (Morosan & DeFranco, 2015). Similar to (Morosan & DeFranco, 2015; Shaw & Sergueeva, 2019; Xu et al., 2011) we also include perceived value as an explicit construct and part of the privacy calculus model. Following the conceptualization of (Zeithaml, 1988), we therefore refer to the perceived value of video conferencing in this study as the professionals' overall perception of videoconferencing based on the consideration of benefits obtained from and sacrifices made to use it.

5.3.5.1 Perceived Value to Lean Usage

System usage can be measured through lean or rich measures. Lean measures attempt to reflect usage alone. The lean measures range from very lean to lean measures. The very lean measure attempts to measure the presence of use alone such as use/nonuse. The lean measure reflects the extent or duration of use (Burton-Jones & Straub Jr, 2006).

Prior studies (Al-Qeisi et al., 2014; Isaac et al., 2019; Lallmahomed et al., 2013) noted that when individuals realize that a technology provides value in accomplishing their tasks, they will be motivated to use it more frequently. As professionals are often very busy and they explore different ways to enhance their performance and when they realize the value of VC apps in enhancing their efficiency and effectiveness in completing their work-related tasks, they will be motivated to use VC applications more often. Hence, we hypothesize that:

H6: Perceived Value positively impacts lean usage of VC apps.

5.3.5.2 Perceived Value to Rich Usage (Cognitive Absorption and Deep Structure usage)

Burton-Jones and Straub Jr (2006) noted that system usage can be measured through lean or rich measures. Lean measures are not precise in the sense that they don't refer to the aspect of usage that may be most pertinent in a particular context and hence a respondent may not be clear on what part of usage activity is being measured. Rich measures, on the other hand, subsume the nature of the usage activity by incorporating user, system and/or a task. The rich measures include somewhat rich, rich and very rich measures. The somewhat rich measures incorporate both system and usage. It measures the extent to which the system is used i.e., it measures the breadth of use of the system such as the number of features used. Rich measures may involve a user and system or a task and system. Rich measures that include the user and system context (also referred to as cognitive absorption) captures a user's employment of a system. Rich measures that include task and system context (also referred to as deep structure usage) measures the degree to which the system is employed to carry out a task. The very rich measure of a usage can be formed by combining two rich measures of usage: the rich measure involving the user context (aka cognitive absorption) and the rich measure involving the task context (aka deep structure usage).

Lou et al. (2021) noted that when users feel that a technology is highly valuable in fulfilling their functional needs, the individuals will be willing to spend more time and effort in interacting with the technology and making full use of its features. Similarly, Zhang and Venkatesh (2018) argued that when individuals realize that a specific technology is valuable in communicating some complicated knowledge, they are more likely to combine its core features or explore specific ones in much depth to complete their task. In addition, Thatcher et al. (2018) argued that the usefulness of the technology in accomplishing various tasks positively influences the deep structure usage of the technology. In the case of our study, we argue that when professionals recognize the value of video conferencing in enhancing the effectiveness and efficiency of their work related tasks in virtual environment and is highly valuable in completing their work related tasks, the tasks that usually involve data access, analysis, reporting, idea -generations, and decision making, they are more likely to exhibit deep structure usage of VC apps i.e., using the audio, video along with file sharing, screen sharing and enabling poll will facilitate better discussion, idea generation and makes it easier and faster.

Cognitive absorption is a state of deep involvement with a technology in which a behavior is performed for itself to experience intrinsic pleasure and satisfaction (Lin, 2009). Agarwal and

Karahanna (2000) noted that cognitive absorption is positively influenced by perceived social richness of the medium as well as individuals' attitude towards the technology used in virtual communications. Further Chandra et al. (2012) noted that if a technology fulfills individuals' objectives, ideas, and expectation, they are motivated to use the technology more broadly and intensely. This deeper use of technology would involve increasing more of the user's cognitive resources while utilizing a technology. This cognitive involvement would be more pronounced for adopting the technology for the work-related tasks or recreational tasks. Hence, compatibility of individuals objectives with those achievable by the technology would serve as the main reason for individuals to be actively and deeply involved in using the technology (Chandra et al., 2012). Given that the main objective of professionals is to complete their work related tasks, and when professionals perceive that VC apps are valuable in achieving these objectives, they will be motivated to use VC apps more extensively and deeply. Hence, we hypothesize that:

H9: Perceived value positively impacts rich usage of VC apps

5.3.6 Effort Expectancy as the Moderator

Effort expectancy related to the ease of use related to technology. Prior literature Rahi et al. (2019) noted that when a technology is perceived to be easy to use and doesn't require mental effort, it has higher chances of adoption and use. Similarly Kim et al. (2007) noted that when individuals perceive that the use of technology involves higher physical and mental effort, individuals' perceptions of value achieved with technology decreases. Conversely, if the use of technology involves lower mental effort, the individuals' perceptions of value achieved with technology increases. In this study we argue that effort expectancy moderates the relationship between perceived value and user behavior in such a way that individuals' perceptions of value and consequently their frequency of use of VC apps increases, if individuals perceive that VC apps are easy to use.

H7: Effort expectancy positively moderates the relationship between perceived value and use behavior.

5.3.7 Perceived Fees as the Moderator

Perceived fees represent the encoding and internalization of the objective monetary transaction cost of using a technology (Kim et al., 2007). Kim et al. (2007) noted that without any experience with new technologies, consumers can't decide whether the fees cited to them is reasonable or not (Kim et al., 2007). In such cases consumers make decisions by equating the new stimuli value to the anchor points (Grewal et al., 1998). When a consumer is presented with any item of new information that is harmonious to his/her anchor point and falls within his/her latitude of acceptance, assimilation occurs. Assimilation is a process of accepting and integrating new beliefs into existing attitudes. Conversely, if the comparison falls with the consumers' latitude of rejection, the item is rejected (Sherif & Hovland, 1961). Prior literature (Kim et al., 2007; Venkatesh et al., 2012; Wang & Wang, 2010) has indicated that perceived fees negatively influence consumers' attitude towards a technology.

Although some VC apps are free to use, some VC apps require the users to pay a monthly/yearly subscription fee to use their pro, business and enterprise versions. In the case of paid accounts, the professionals may get access to robust features of VC apps such as increased number of attendees, extended time for video conferencing, and access of recordings on cloud, and customized notifications as opposed to free versions of VC which limits the group video conferencing to 40 minutes and lesser customization. Hence, paid versions provide higher value in the context of professional context. Hence, we postulate that the effect of perceived value on use behavior increases, if the users are paying higher fees.

H8: Perceived fees positively moderate the relationship between perceived value and use behavior.

5.3.8 Social presence to Rich Usage

Zhang and Venkatesh (2018) noted that social presence and telepresence rich technologies foster higher social bonds and more favorable interactions among individuals. These favorable interactions will undoubtedly result in more heighted enjoyment and deep involvement as it will supersede more impersonal and machine-like interactions with more and personal feel (Zhang & Venkatesh, 2018). Similarly, we argue that when individuals realize that a specific technology is capable of delivering humanizing, sociable, and warm interactions, they are motivated to explore more of its core features or combine its specific features to make the virtual interactions more similar to face to face interactions.

Hence, we postulate that

H10: Social presence in VC apps positively impacts rich usage of VC apps.

5.3.9 Lean Usage (Use behavior) to Continuance Intentions

Ouellette and Wood (1998) noted that the past behavior has a direct influence on the future behavior mainly when individuals have copious opportunities to perform the behavior under constant circumstances (Ouellette & Wood, 1998). Performing a behavior enhances its cognitive accessibility which in turn positively influences intentions to perform it again in the future (Trafimow & Borrie, 1999). Martins et al. (2019) noted that when individuals use technology more frequently, they are motivated to use it in the future. We argue that when professionals use VC apps more frequently, they will be motivated to continue using it in the near future.

H11: Lean usage (Use behavior) positively impacts continuance intentions

5.3.10 Rich usage (Cognitive Absorption and Deep structure Usage) to Continuance Intentions

Agarwal and Karahanna (2000) noted that cognitive absorption forms perceptions of lower cognitive burden because an individual is experiencing heightened enjoyment from using it and is willing to expend more time in it. Individuals who experience higher cognitive absorption are more willing to self-disclose their personal information (Alashoor & Baskerville, 2015) or have a higher enticement to return to a website (Ghasemaghaei, 2020) or use technology in the future (Al-Shaikhli et al., 2021). Jumaan et al. (2020) noted that when using the internet, “users find that their surroundings tend to lose significance and their sense of time becomes distorted” (Jumaan et al., 2020, p. 3). As this happens, users may become gradually immersed in the experience; this state of engagement may influence individuals intentions to use the technology in the near future (Jumaan et al., 2020). Similar to the argument above, we postulate that, when using VC apps, professionals find that their surroundings become insignificant and they experience less distractions. As with this experience, they become gradually immersed in completing their tasks when using VC apps, which consequently influence their intentions to continue using VC apps in the future.

In addition, we argue that Individuals who exhibit deep structured use of technology i.e., are willing to spend more time and effort in interacting with the technology and making full use of its features will be more likely motivated to use it in the near future. Hence, we hypothesize that:

H12: *Rich usage of VC apps positively impacts continuance intentions.*

5.4 RESEARCH METHODOLOGY

5.4.1 Measurement

In order to collect the data, an instrument was developed, and a survey questionnaire was developed. The constructs for the questionnaire were taken from prior literature with adjustments to the context of VC applications (as shown in Table 4 in Appendix). Construct items were measured on a range of seven-point scale, ranging from 1 (strongly disagree) to 7 (strongly agree).

5.4.2 Data collection

A survey instrument was developed and shared online on LinkedIn, a social media network, via its direct messages feature. In order to conduct the collection of data, a two-step approach was used. First, the "key informant" data collection approach (Pinsonneault & Kraemer, 1993) was performed. This was essential in order to identify fitting respondents to whom direct messages were sent on LinkedIn throughout eight consecutive weeks for two hours a day. Second, follow-up messages were sent to the users who did not express any kind of feedback or confirmation that the survey would be answered and submitted. This was translated into a total of 2471 direct messages sent to LinkedIn users, with 487 complete and valid responses, corresponding to a 19.7% response rate. Our sample size satisfies the minimum sample size requirements based on two methods: 10 times rule method and minimum R squared method.

There are various methods for minimum sample size estimation in PLS-SEM including the Monte-Carlo simulation method, 10 times rule method, and minimum R squared method (Kock, 2018). However, the 10 times rule method by Hair et al. (2011) and minimum R^2 method proposed by (Hair Jr et al., 2016) are also the most commonly used approaches to calculate the appropriate sample size (Kock, 2018).

Citing Barclay et al. 1995, Hair Jr et al. (2016) notes that "“sample size should be equal to the larger of (1) 10 times the largest number of formative indicators used to measure one construct or (2) 10 times the largest number of structural paths directed at a particular latent construct in the structural model" (Hair Jr et al., 2016) (p.24). Prior research Van Raaij and Schepers (2008) has shown that established results could be obtained with the 10 times rule method.

For our model, there are two formative constructs: MUIPC and Ubiquity. With respect to MUIPC, there are three indicators (PS, PI, SU) and for ubiquity, there are five indicators (TS, SF, Pr, Im, Cn). Hence, the application of the aforementioned guideline 1 would yield a minimum sample size of 50 (10 times 5) for our research. Our model also satisfies the guideline 2 stated above. We can observe that (see Figure 29) in our model, a total of 3 arrows (structural paths) point to use behavior (PR). Thus, the application of guideline 2 would yield a minimum sample size of 30 for our research.

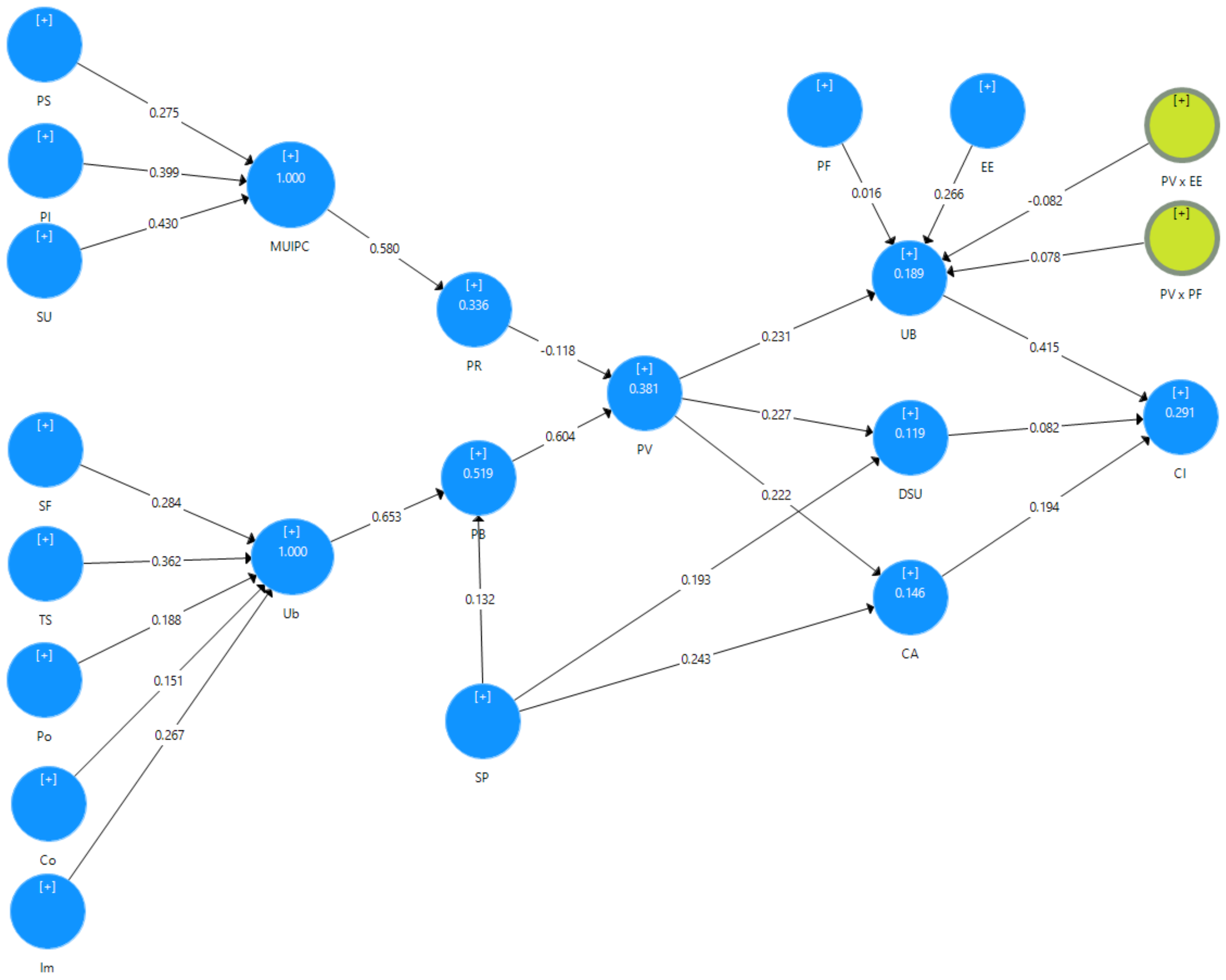
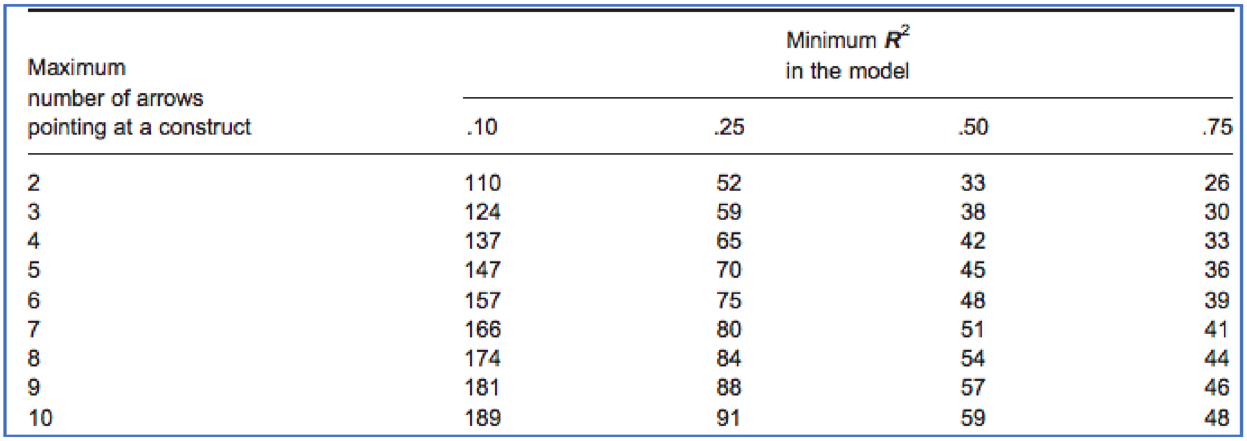


Figure 29 PLS path and R2 for the Proposed Model by Smart PLS

Hair Jr et al. (2016) also proposed a minimum R squared method, an alternative to 10 times for sample size calculation. This method relies on a table (see Figure 30) that lists minimum sample size based on three components (1) maximum number of arrows pointing towards a latent construct in a model ie., the complexity of a PLS path model (2) the level of significance used in the model (3) the minimum R^2 in the model (Kock, 2018). Kock (2018) presented the reduced version of the minimum R^2 method with the focus on significance level of 0.05 with the commonly used level of statistical power of 80%.

In our proposed model, the maximum number of arrows pointing at the latent variable (i.e., use behavior) is 5 and the minimum R² is .189. There is no cell in the table for the minimum R squared method for which these values intersect. However, the closest cell (R².25) shows a minimum sample size of minimum of 70, which is used as an estimate in our model. Hence, our sample size represents an appropriate sample size with an adequate level of accuracy and statistical power. This method was used by TUNCER and ŞAHİN (2019).



Maximum number of arrows pointing at a construct	Minimum R^2 in the model			
	.10	.25	.50	.75
2	110	52	33	26
3	124	59	38	30
4	137	65	42	33
5	147	70	45	36
6	157	75	48	39
7	166	80	51	41
8	174	84	54	44
9	181	88	57	46
10	189	91	59	48

Figure 30 Minimum R-Squared Method; Source: (Kock, 2018)

.

The Kolmogorov–Smirnov (K–S) demonstrates the absence of non-response bias (Ryans, 1974) while measuring the early and late respondents. Third, it was offered to the respondents the option of received the results of this study. As for the common method bias, it was confirmed with the usage of Harman’s one-factor test (Podsakoff et al., 2003) that none of the components singly defines the variance. The second way of analyzing the common method bias was using a marker viable approach (Lindell & Whitney, 2001), with the addition of a theoretically irrelevant marker variable in our model, retrieving 0.023 (2.3%) as the maximum shared variance with other variables, which may be treated as low (Johnson et al., 2011). No significant common method bias was found in our model. The demographic characteristics are shown in Table 5 in Appendix.

5.5 DATA ANALYSIS

In order to perform this research, the partial least squares (PLS) technique was utilized. The reason behind using the PLS technique relies on the fact that it is quite helpful to analyze topics that have never been used before (Ke et al., 2009; Teo et al., 2003). According to Goo et al. (2009), the PLS analysis enables the usage of formative indicators in order to model latent constructs. Furthermore, this technique mitigates the factor of restrictive distributional assumptions (at the moment path coefficients are being elaborated) being significantly different from zero (Fornell & Bookstein, 1982; Gefen & Straub, 2005; Goode et al., 2015). The PLS technique is an applicable technique for our study due to the fact that it includes formative constructs, it has never been tested before, and the variables are not normally distributed ($p < 0.01$, Kolmogorov–Smirnov's test) (Chin et al., 2003).

5.5.1 Measurement Model

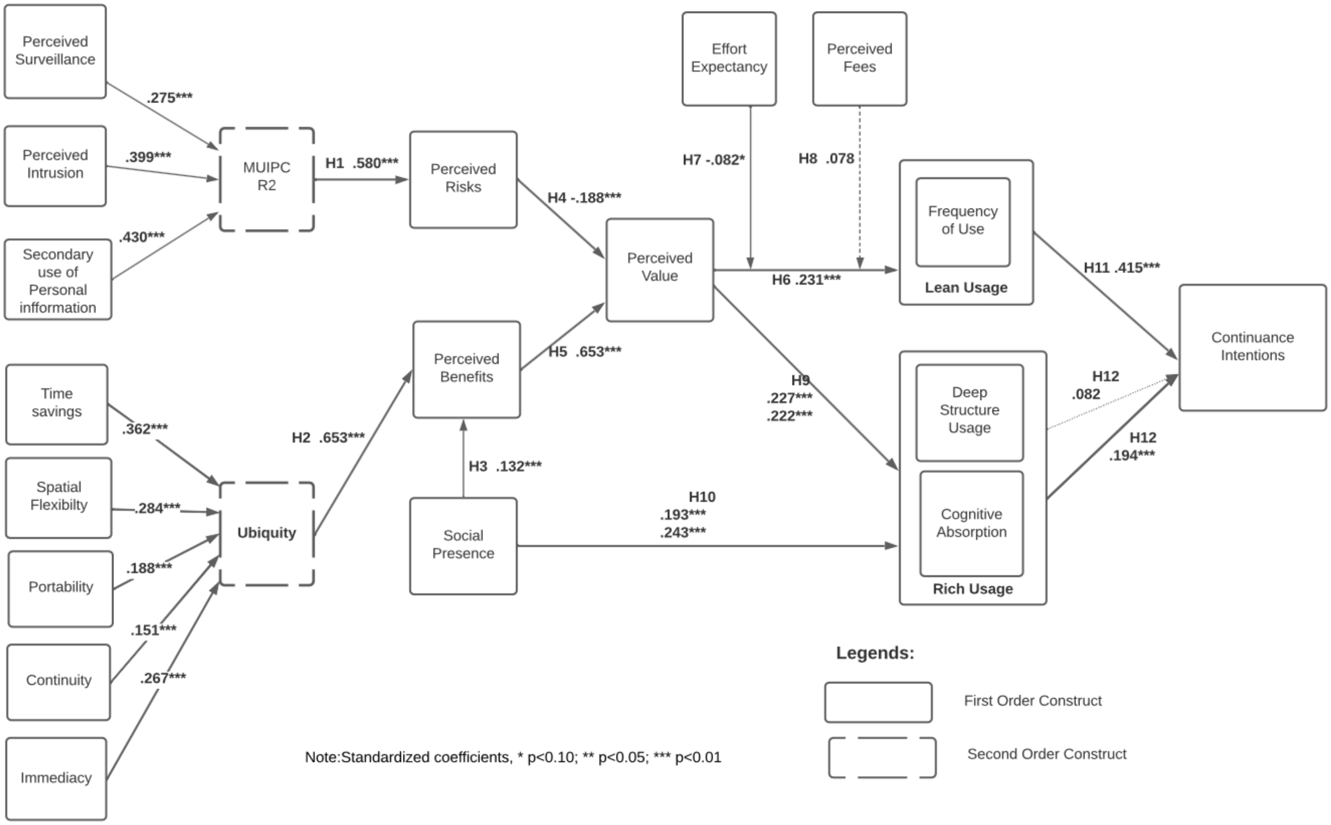
A measurement model was developed to assess the construct reliability, discriminatory validity, indicator reliability, and convergent validity. The measurement model results are demonstrated in, Tables 6 and 7 (see Appendix). The composite reliability was used in order to test construct reliability. As shown in Table 6 (see Appendix), the CR results are higher than 0.7 for all constructs, indicating the suitability and internal consistency of the constructs (Henseler et al., 2009; Straub, 1989). Table 6 (see Appendix) shows that the AVE results are higher than 0.50 for all constructs, thereby demonstrating the convergent validity of the measurement model (Fornell & Larcker, 1981; Hair et al., 2012). Furthermore, Table 7 (see Appendix) shows that all the loadings are higher than 0.7, therefore demonstrating indicator reliability (Churchill Jr, 1979; Henseler et al., 2009), and except item PS1(this item was removed). In order to assess the constructs' discriminant validity, cross-loadings, Fornell-Larcker criterion and Heterotrait-

Monotrait ratio (HTMT) were performed (Henseler et al., 2009). The correlation between constructs and AVE squared root was used in order to assess discriminants validity of the constructs. Table 6 (see Appendix) shows that the square root of each construct (in the diagonal position) is higher than the correlations between the constructs. Hence, the first criterion for discriminant validity of the constructs is supported (Fornell & Larcker, 1981). Also, in order to achieve discriminant validity, the second criterion was applied where the loadings (in bold) should be greater than cross-loadings (Chin, 1998), supported in Table 7 (Appendix). At last, discriminant validity is achieved as all the HTMT are lower than the threshold of 0.9 as seen in Table 8 (Appendix). The results support the construct reliability of the measurement model. Therefore, the constructs were appropriate for usage in order to test the structural model.

The MUIPC was modeled as a second-order construct of the reflective-formative type (Ringle et al., 2012), with perceived surveillance, perceived intrusion and secondary use of personal information as reflective constructs. Similar method was applied for ubiquity as a second-order construct, where time savings, spatial flexibility, portability, immediacy and continuity. Regarding the two formative constructs, a measurement model was executed in order to analyze the significance, the sign of weights and the multicollinearity. The variance inflation factor (VIF) statistic was performed in order to assess the multicollinearity (see Table 9 in Appendix). As Table 9 (Appendix) demonstrates, the range of the VIF is between 1.53 (lowest) and 2.871 (highest). According to (Lee & Xia, 2010), the absence of multicollinearity among the variables is supported since the VIF values are below the threshold of 3.3. Furthermore, all weights are statistically significant, therefore we can conclude that the formative constructs also present a good measurement model.

5.5.2 Test of the Structural Model

The structural model (Fig. 31) presents the variation explained along with the path coefficients. The significance levels of the hypothesized construct were performed using bootstrapping with 5000 resamples. All constructs present VIF lower than 1.377, thereby representing absence of multicollinearity in our measurement model (Hair Jr et al., 2017).



Note: *** p < 0.01; ** p < 0.05; * p < 0.10.

Figure 31 Structural Model

In our model, perceived risks explain 33.6% of the variation with MUIPC (β= 0.58; p < 0.01) being statistically significant, thereby supporting H1.

In our model, perceived benefits explained 51.9% of the with Ubiquity (β= 0.653; p < 0.01) and social presence (β= 0.132; p < 0.01) being statistically significant, thus supporting H2 and H3.

Our model explains 38.1% of the variation in perceived value. Perceived risks β= -0.118; p < 0.01), as well as perceived benefits (β= 0.653; p < 0.01) are statistically significant, thereby supporting H4 and H5.

The model explains 18.9% of variation in lean usage (UB) and confirms the positive effect of perceived value (β̂=0.231; p<0.01) on lean usage (use behavior). The moderating role of effort expectancy (β̂=-0.082; p<0.10) on the relationship between perceived value and use behavior was found to be statistically significant, but with negative effect, which is contrary to our hypothesis. Therefore, H6 is supported, while H7 is not supported. The moderating role of perceived fees (β̂=-0.078; p<0.10) on the relationship between perceived value and use behavior was not found to be statistically significant, thereby rejecting H8.

The model explains 11.9% of variation in deep structure use and 14.6% of variation in cognitive absorption. The effect of PV on rich use (deep structure usage - β̂=0.227; p<0.01; cognitive absorption - β̂=0.22; p<0.01) is statistically significant, thus confirming H9. The effect of social presence on rich use (deep structure usage - β̂=0.193; p<0.01; cognitive absorption - β̂=0.243; p<0.01) is statistically significant, thus confirming H10

Lastly, our model explains 29.1% variation in continuance intentions. The effect of lean usage (use behavior) (β̂=0.415; p<0.01) on continuance intentions is statistically significant, thus confirming H11. The effect of rich usage -deep structure β̂=0.082; p<0.01) is not statistically significant, whereas the effect of rich usage -cognitive absorption ($\hat{\beta}=0.194$; $p<0.01$) is statistically significant, thereby partially supporting H12.

5.6 DISCUSSION

The objective of this study is to investigate how do contrary beliefs influence professionals' attitude towards VC apps and consequently its rich usage and automatic usage.

The findings indicate that professional's privacy concerns have a significant effect on their perceptions of risk involved in using VC apps. A closer look at the findings imply that professionals are more worried about the secondary use of their personal information and intrusion aspects of VC apps when compared to surveillance capabilities of VC apps. This implies that professional belief that VC apps provides the VC app vendors and service providers the direct and indirect access to their personal information and consequently use their personal information for other purposes. Professionals also believe that the information that they consider private is readily available to others than they would want, which consequently invades their privacy.

With regards to ubiquity, the findings confirm that professionals' value the benefits of portability, time savings and spatial flexibility enabled by VC apps. They believe that a VC app fits their schedule and makes their life easier by allowing them to effectively manage their time. They also believe that VC apps enabled them to communicate with their peers at any time, thereby allowing them to overcome spatial limitations. The professionals also believe that VC apps enable higher social presence. Professionals believe that the ability of VC apps to mirror face to face communications through the use of both visual and non-visual cues enabled them to have humanizing, sociable, warm, and personal interaction with their peers.

The findings also indicate that perceived risks negatively influence perceived value and perceived benefits positively benefit the perceived risks. However, a closer look at the findings indicate that professionals' perceptions of value are strongly influenced by perceived benefits than perceived risks. The findings indicate that professionals recognize the benefits of VC apps in providing the benefits of ubiquitous connectivity and social presence. However, these benefits are tempered by professionals' concerns regarding the secondary use of personal information, intrusion and surveillance aspects of VC apps. However, when evaluated in parallel, perceived benefits have strong influence on professionals' perceptions of value achieved in using VC apps than the perceived risks. In sum, this also points towards the existence of the privacy paradox in professionals' attitude towards VC apps i.e., they are ready to risk their privacy in exchange for the benefits of ubiquitous connectivity and social presence enabled by VC apps.

The findings also indicate that social presence has a significant effect on the rich usage of VC apps. The professionals believe that the social presence enabled by VC apps enabled them to experience heightened enjoyment and deep involvement with VC apps. The professionals believe that when using VC apps, they use features that help them compare and contrast different aspects of their tasks with their peers. The professionals believe that they are able to experience higher cognitive absorption due to personal, warm, and human-like interactions provided by VC apps. They are also able to block all distractions and their attention doesn't get diverted when using VC apps.

The findings also indicate that perceived value has a significant effect on both lean usage (Use behavior) and rich usage (cognitive absorption and deep structure usage) of VC apps. This implies that when professionals perceive that VC apps deliver a good value, their intensity of VC apps usage in their professional work increases. When professionals perceive that VC apps are highly valuable in accomplishing their work-related tasks, they spend more time and effort in using VC apps and making full use of its features to test their assumptions with their peers and derive insightful conclusions with their peers. These findings are in line with the findings by Zhang and Venkatesh (2018). In addition, when professionals perceive that using VC apps is worthwhile to them, they are motivated to use VC apps more extensively and deeply. These findings correspond to the findings by Chandra et al. (2012).

Contrary to our hypothesis, effort expectancy has a negative moderating effect on the relationship between perceived value and lean usage (use behavior). The findings indicate that professionals' perceptions of value and consequently their intensity to use VC apps decreases if they experience higher mental effort in using VC apps. A plausible explanation may be that the data collection was done during the pandemic. Many professionals may have just started using the VC apps and have experienced some difficulty when learning to use VC apps. In addition, VC apps were continuously introducing refreshed user interfaces with additional features to make VC apps more inclusive and productive. Although, these functionalities were introduced to make the meeting more immersive; it may also have introduced some learning curve on the part of the participants to learn to use new functionalities and get used to the often-changing VC user interface.

Lastly, the findings indicate that both lean usage and one aspect of rich usage i.e., cognitive absorption of VC apps positively influence professionals' intentions to continue using it. This implies that actual usage of VC apps thus served as the foundation for the development of favorable judgments and intentions among the professionals to continue using VC apps in the future. However, the effect of deep structure usage of VC apps doesn't have a significant effect on continuance intentions to use VC apps. These findings need further investigation.

5.6.1 Theoretical Contributions

Our study investigated how the contrary beliefs of perceived risks and benefits shape the attitude of professionals towards VC apps and consequently its active use and automatic use. This research not only investigated the impact of technological characteristics of VC apps i.e., ubiquity, but also the socially derived characteristics i.e., social presence. By combining both socially derived and technological characteristics, this research provides a comprehensive picture of the factors that influence professionals' attitude towards VC apps. This study thus adds to the literature of both the privacy and collaborative technologies.

Brown et al. (2010) only investigated the use of proprietary collaborative technologies. The investigation of consumer off the shelf video conferencing applications is lacking in the prior literature. By investigating professionals' attitude towards consumer off the shelf video conferencing, this study provides a deeper understanding of how professionals engage with the consumer off the shelf-video conferencing. Further, our study focused only on the use of VC apps in the professional context. By separating the professional context from personal context, this study addresses the call by (Brown et al., 2010) to investigate video conferencing in professional and personal context separately.

Privacy calculus has been empirically examined in technologies other than VC apps such as location-based services in mobile devices (Xu et al., 2009), location aware marketing in mobile devices (Xu et al., 2011), e-commerce (Li et al., 2010), social networking systems (SNSs) (Krasnova et al., 2012), location based social network services (Zhao et al., 2012), mobile applications (Keith et al., 2016), hotel apps (Morosan & DeFranco, 2015), healthcare wearable devices (Li et al., 2016), personalized nutrition services (Berezowska et al., 2015), mobile Applications (Pentina et al., 2016), mobile hotel booking loyalty (Ozturk et al., 2017), and pay-

As-You-Live (PAYL) services (Wiegard & Breitner, 2019). This study contributes to the literature on privacy calculus, a specific type of collaborative technology that has gained popularity in the workplace during pandemic. By applying privacy calculus in the context of consumer off the shelf VC apps, this study addresses the call by (Xu et al., 2009) for additional research that investigates how the users of surveillance based technologies trade off their risks and benefits when using such technologies. The findings of this study can be applied in the context of other surveillance-based technologies such as facial recognition, electronic Ids, smart badges etc.

Third, the study extends the privacy calculus model (Dinev & Hart, 2006) by proposing three additional factors to the dual path of privacy calculus i.e., ubiquity and social presence influencing perceived benefits and MUIPC influencing privacy risks. The findings have the implications for the development of VC apps that preserves the privacy and security of those who seek to use VC apps to communicate and collaborate with their peers in the professional's context.

Lastly, the study investigated how professionals' attitude towards the active (lean usage and rich usage) and automatic use (continuance intentions). While the existence of different levels of system usage and their antecedents and consequences are widely recognized in the IS literature (Burton-Jones & Straub Jr, 2006), prior studies in the context of VC apps have only investigated the automatic use (continuance intentions) of VC apps. By investigating the active usage of VC apps at deeper level, i.e., incorporating both lean and rich usage measures, this study addresses the call by (Burton-Jones & Straub Jr, 2006) to investigate the nature of system use, its antecedents and consequents in different contexts. As such this research provides rich insights into the nature and use of video conferencing in the workplace environment.

5.6.2 Practical Contributions

The study offers key insights into what influences professionals' attitude towards VC apps and consequently its active and automatic usage in professional context. As remote work becomes a new norm, professionals will continue to engage in the cost-benefit analysis in which they will weigh the risks against benefits of using VC apps. The study provides insights into what ensures the professionals to have a positive attitude towards VC apps and consequently use and continue its use in the future. Our findings suggest that both VC apps vendors and policy makers can play a significant role in ensuring that the privacy calculus of professionals favors the adoption of VC apps.

VC apps vendors should consistently target improvements in ubiquity and social presence enabled by VC apps. For instance, to enhance ubiquitous connectivity of VC apps, VC app vendors can work on their backend systems in order to enable reliable and immediate access to the VC. In order to enhance social presence, VC app vendors can introduce humanizing cues such as the introduction of emoticons, gestures, and humorous content (Ye et al., 2020). In addition, when making updates to the systems and introducing new features, VC apps should provide video tutorials on how to use the new features in order to reduce the learning curve involved in using VC apps.

With regards to privacy concerns, VC app vendors should implement procedural fairness in the form of fair information practices when collecting personal information (Culnan & Armstrong, 1999). When developing privacy policies, VC app vendors should ensure the consumers that effort has been made to protect the sensitive information of users. In addition, they should communicate the reasons for collecting the personal information and how the collection of personal information is going to impact the services provided to the users. They should ensure that the information is getting collected only to enhance the features that are related to services the users are getting. In addition, consumers should be communicated that effort has been made to protect the personal information of the users that is collected by VC app vendors.

As noted by Cloarec (2020) providing consumers with the information sharing controls reduces the reactance to the advertised messages. Hence, VC app interfaces should be integrated with simplified information sharing controls to empower users over when, how and whom to share their personal information. As prospects of remote work become a new norm, the organizations should also put an effort in enhancing their employee’s privacy literacy and self-efficacy. For instance, the employees can be educated on how cameras and microphones can be managed so that sensitive personal and professional data is not unwillingly compromised through VC platforms. By providing experiential learning through games, simulations, and quizzes, the employees will not only become knowledgeable in managing their privacy, but also be actively engaged in preventative strategies.

In order to enhance cognitive absorption, VC app vendors can provide immediate feedback mechanisms to the user to collect information on their desires, satisfy their requirements, and respond to their issues quickly. Designing user- friendly interfaces with the goal of maximizing interactivity and user control are some of the ways VC apps can also enhance cognitive absorption of users (Lin, 2009).

5.7 LIMITATIONS AND FUTURE RESEARCH

Although this research provided several theoretical and practical implications, this study is not free from its limitations.

Our study omitted several important factors such as that could affect professionals' perceptions of perceived value in using VC apps such as perceived fees, trust, technicality, synchronicity, system quality, and service quality. Another study can be conducted by using these factors as predictors of professionals' continuance intentions to use VC apps.

Second, the collection of the data at a single point in time may serve as a limitation to the findings of this study. However, measurement of a specific technology's continuance use is more likely to involve retrospective analysis. Therefore, future studies can be conducted by carrying out longitudinal investigation to obtain more convincing explanations on how professionals' perceptions towards VC apps changes over time.

Third, the collection of the data during the COVID-19 pandemic may also have served as a limitation to the findings of this study. It would be interesting to conduct the same research after COVID-19 pandemic to see if the professionals' perceptions of rich and continued use of VC apps at individual level remain the same or not.

Fourth, the study didn't measure actual usage of VC apps. Although continuance intentions is a valid predictor of user's post adoption behavior and it is not the equivalent of behavior (an actual act) and that there may be cases where individuals may intend to act in specific way but yet act very contrarily from their intentions (Bhattacherjee & Barfar, 2011). Therefore, it is very crucial for continuance research to operationalize and measure actual IT usage behavior in addition to continuance intentions (Bhattacherjee & Barfar, 2011). Therefore, a future study may be conducted in order to investigate the professionals' actual usage of VC for professional purposes.

Fifth, this study only investigated professionals' use of VC apps usage at individual level. Professionals' use of VC apps at organizational level is not considered in this research. A future study can be conducted to investigate professionals' use of VC apps at organizational level.

CHAPTER 6 CONCLUSION

This chapter provides a conclusion of the dissertation with the motivation behind the research, the solutions proposed, and limitations and future work.

Collaborative systems have been an area of interest in many domains including education -teaching and research, healthcare, supply chain, Internet of things, music, and small and medium sized enterprises and larger corporations. Collaborative systems offer myriad benefits including problem solving through expertise sharing, ideas sharing, improved decision making, learning and resource sharing. However, lack of trust, security attacks, privacy violations, and semantic interoperability conflict are the major inhibitors of collaborative systems use. This dissertation aims to address the above issues by designing an artifact for collaborative systems that resolves trust, security, and interoperability issues in collaborative systems and developing a conceptual model that explores individuals' intentions to use collaborative systems.

The artifact designed in this dissertation is blockchain based collaborative system (BCHIES) (Chapter 4) that addresses trust, security, and semantic interoperability issues obstructing organizations to collaborate with each other. In chapter 4, I also highlight why blockchain can be applicable to collaborative systems and summarize the differences between BCHIES and other collaborative systems. BCHIES is evaluated using informed argument and an illustrative scenario. A detailed scenario was built in the context of the healthcare domain where it was demonstrated how different healthcare institutions can share and receive interoperable patient records from each other virtually in a secure and reliable manner, while still storing patient data using different standards and naming conventions.

Hence, this research makes important contributions.

- The most important contribution of this dissertation is the design artifact, the BCHIES itself. The proposed system BCHIES is designed to address three important challenges in data exchange across collaborating organizations, namely trust, security and semantic interoperability issues.
- Second, the development of an appropriately evaluated, comprehensive system named BCHIES, with the detailed documentation supporting its illustration in the real-world scenario has contributed to the knowledge base in collaborative systems literature. The process of building BCHIES, the proposed artifact has also provided contributions to the knowledge base through uncovering and explaining new methods that enable secure and interoperable exchange of data across collaborating institutions not described by existing collaborative systems.
- From a practical perspective, this dissertation research contributes to the practices in cross-institutional health information exchange by providing a useful reference on using new features of blockchain technology to solve the weaknesses of traditional health information exchange where patient records are faxed to other health care institutions, thereby improving and simplifying the sharing of electronic health records.

Future research will explore the evaluation and effectiveness of BCHIES through expert evaluations where the real business decision makers will provide the feedback on the proposed system. I will demonstrate how BCHIES will work in the healthcare domain. Later, the experts will be interviewed to elicit their comments on the proposed systems. Next, an analytical testing approach will be used to assess the usefulness and quality of BCHIES. The experts will be presented with a questionnaire to assess their perceptions of the usefulness of BCHIES that help collaborating institutions to share interoperable data across each other in a secure manner virtually.

Statistical analysis will be done to analyze experts' perceptions towards BCHIES. The Information gained from the expert evaluation can be used to refine the proposed artifact until a satisfactory solution can be found. Currently, BCHIES is limited to resolving semantic interoperability conflicts caused due to naming conflicts. Future research will extend the system to resolve scaling and confounding conflicts in collaborative data sharing processes.

Second, the conceptual model (Chapter 5) developed in this study explores professionals' intentions to use collaborative systems despite their susceptibility to privacy violations. Given the importance of privacy to the professionals in the work-related settings, and the prediction that remote work will continue to hold after COVID-19 pandemic, both academicians and practitioners have to strive to improve their understanding of professional's attitude and behavior towards collaborative systems. As noted by (Yoo & Alavi, 2001), to gain a better understanding of an individual's attitude and behavior towards technology, it is important to form a theoretical framework that incorporates both social and technological constructs of a technology. In chapter 5, I attempt to bridge the gap in the extant literature through exploration of the factors (both social and technological constructs) that influences the continued use of collaborative systems amidst the privacy concerns associated with its usage. A theoretical model rooted in the theoretical foundations of privacy calculus, along with socially and technological derived constructs including social presence, ubiquity, mobile users' information privacy concerns (MUIPC), effort expectancy, and perceived fees was developed. An empirical study was conducted using a questionnaire for data collection with 487 working professionals using collaborative systems. The research presented an integrated model of determinants of continued use of collaborative systems, an empirically validated model, and made several theoretical and practical contributions. The second research makes the following contributions:

- The research adds insights and richness to our understanding of professional’s attitude towards collaborative systems in the professional settings. Knowing as much as possible about individuals’ attitude towards collaborative systems is crucial in today’s virtual environment specifically post-pandemic, where it has been predicted that post pandemic, virtual collaborative tools will be among the preferred tools of communication for the remote work (Taylor, 2021). The factors examined in the proposed model comprises a set of contrary beliefs (perceived risks and benefits), which are weighed against each other. The outcome of such comparison is that the strength of one outweighs the influence of others. The notion of calculus in professional’s decision-making highlights the perspective that factors influencing individuals’ attitude towards collaborative systems can be contrary and their relative influence needs to be taken into account when attempting to understand any surveillance-based technologies adoption or acceptance including collaborative systems. Hence, our study provides the theoretical and empirical support for the influence of perceived benefits (Ubiquity and social presence) and perceived risks (MUIPC) in influencing individuals’ perceptions of value, suggesting that perceived benefits have more influence on perceived value than perceived risks when both perceived risks and benefits are evaluated in tandem. Hence, this research extends the privacy calculus model by identifying three underlying factors that can influence dual paths of perceived risks and benefits leading to perceived value of collaborative systems. By doing so, this research builds and expands the growing body of IS research on the impact of contrary beliefs on the privacy paradox involved in individuals’ decision-making process when making decisions to disclose personal information or use a technology.

- The research also highlights the moderating role of effort expectancy. The significant role of effort expectancy indicates that the effect of perceived value on user behavior varies with the ease of use experienced from the use of VC. This has important theoretical implications since this relationship opens up new avenues for the exploration of the effect of effort expectancy on the relationship between perceived value and use behavior. This research calls for future research to investigate this relationship in other virtual technologies such as Internet of things, smart badges etc. This important theoretical relationship also has an important practical value as VC application vendors have been making changes to VC interfaces continuously. Given that there are numerous collaborative systems, the professionals will stop using a collaborative system as they experience frustration, anxiety, tension, and mental fatigue due to mental effort involved in using collaborative systems.
- By investigating the active use that comprises the lean and rich usage of VC apps and consequently its effect on the automatic use, this research addresses the call by (Burton-Jones & Straub Jr, 2006) to choose rich measures over just the lean measures to capture system’s usage in a specific context.
- By investigating a model focused on a collaboration technology, the research provides actionable guidance to designers and developers on how to develop the collaborative systems that preserves the privacy of the professionals in the remote work settings and consequently augment adoption and use of a collaborative system.

In addition to economic, social, and convenience benefits as well as general privacy concerns, the irrationality in individuals’ decision making process is influenced by many other situational factors including benefit immediacy and risk diffusion (Wilson & Valacich, 2012), type of information being collected by the vendor, and perceived relevance of information Li et al. (2010), emotions, information sensitivity, and awareness of privacy statement (Li et al., 2011). Our research didn’t account for these factors. Future research can investigate how these situational factors influence irrationality in professionals’ decision-making process to use and continue to use collaborative systems.

REFERENCES

Abbasi, A., Li, J., Adjeroh, D., Abate, M., & Zheng, W. (2019). Don’t mention it? analyzing user-generated content signals for early adverse event warnings. *Information Systems Research*, *30*(3), 1007-1028.

Abdel-Basset, M., Manogaran, G., Gamal, A., & Chang, V. (2019). A novel intelligent medical decision support model based on soft computing and IoT. *IEEE Internet of Things Journal*, *7*(5), 4160-4170.

Adel, E., El-Sappagh, S., Barakat, S., & Elmogy, M. (2018). Distributed electronic health record based on semantic interoperability using fuzzy ontology: A survey. *International Journal of Computers and Applications*, *40*(4), 223-241.

Adel, E., El-Sappagh, S., Barakat, S., & Elmogy, M. (2019). A unified fuzzy ontology for distributed electronic health record semantic interoperability. In *U-Healthcare Monitoring Systems* (pp. 353-395). Elsevier.

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS quarterly*, 665-694.

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: a systematic review. Healthcare,

Ahmad, A., Saad, M., Bassiouni, M., & Mohaisen, A. (2018). Towards blockchain-driven, secure and transparent audit logs. Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services,

Ahmad, T. (2020). Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. *Available at SSRN 3568830*.

Aiken, A. (2020). Zooming in on privacy concerns: Video app Zoom is surging in popularity. In our rush to stay connected, we need to make security checks and not reveal more than we think. *Index on Censorship*, *49*(2), 24-27.

Ajabshir, Z. F. (2019). The effect of synchronous and asynchronous computer-mediated communication (CMC) on EFL learners' pragmatic competence. *Computers in Human Behavior*, *92*, 169-177.

Aken, J. E. v. (2004). Management research based on the paradigm of the design sciences: the quest for field-tested and grounded technological rules. *Journal of management studies*, *41*(2), 219-246.

Al-Karaki, J. N., Gawanmeh, A., Ayache, M., & Mashaleh, A. (2019). DASS-CARE: a decentralized, accessible, scalable, and secure healthcare framework using blockchain. 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC),

Al-Qeisi, K., Dennis, C., Alamanos, E., & Jayawardhena, C. (2014). Website design quality and usage behavior: Unified Theory of Acceptance and Use of Technology. *Journal of Business Research*, *67*(11), 2282-2290.

Al-Shaikhli, D., Jin, L., Porter, A., & Tarczynski, A. (2021). Visualising weekly learning outcomes (VWLO) and the intention to continue using a learning management system (CIU): the role of cognitive absorption and perceived learning self-regulation. *Education and Information Technologies*, 1-29.

Alashoor, T., & Baskerville, R. (2015). The privacy paradox: The role of cognitive absorption in the social networking activity.

Ali, M. S., Vecchio, M., Putra, G. D., Kanhere, S. S., & Antonelli, F. (2020). A decentralized peer-to-peer remote health monitoring system. *Sensors*, *20*(6), 1656.

Ali, S., & Chong, I. (2019). Semantic Mediation Model to Promote Improved Data Sharing Using Representation Learning in Heterogeneous Healthcare Service Environments. *Applied Sciences*, *9*(19), 4175.

Ali, S., Rauf, A., Islam, N., & Farman, H. (2019). A framework for secure and privacy protected collaborative contents sharing using public OSN. *Cluster Computing*, *22*(3), 7275-7286.

Amiri, R., Abidin, A., Wallden, P., & Andersson, E. (2018). Efficient unconditionally secure signatures using universal hashing. International Conference on Applied Cryptography and Network Security,

Anderson, A. (2006). Effective management of information security and privacy. *Educause Quarterly*, *29*(1), 15-20.

Archibald, M. M., Ambagtsheer, R. C., Casey, M. G., & Lawless, M. (2019). Using zoom videoconferencing for qualitative data collection: perceptions and experiences of researchers and participants. *International Journal of Qualitative Methods*, *18*, 1609406919874596.

Armfield, N. R., Bradford, M., & Bradford, N. K. (2015). The clinical use of Skype—For which patients, with which problems and in which settings? A snapshot review of the literature. *International Journal of Medical Informatics*, *84*(10), 737-742.

Arnott, D., & Pervan, G. (2015). A critical analysis of decision support systems research. In *Formulating Research Methods for Information Systems* (pp. 127-168). Springer.

Assel, M., Wesner, S., & Kipp, A. (2009). A security framework for dynamic collaborative working environments. *Identity in the Information Society*, *2*(2), 171-187.

Azad, M. A., Bag, S., & Hao, F. (2018). PrivBox: Verifiable decentralized reputation system for online marketplaces. *Future Generation Computer Systems*, *89*, 44-57.

Azad, M. A., & Morla, R. (2019). Rapid detection of spammers through collaborative information sharing across multiple service providers. *Future Generation Computer Systems*, *95*, 841-854.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data (OBD),

Balasubraman, S., Peterson, R. A., & Jarvenpaa, S. L. (2002). Exploring the implications of m-commerce for markets and marketing. *Journal of the academy of marketing science*, *30*(4), 348-361.

Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, *52*, 101947.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1-21.

Barkman, S. J. (2002). A field guide to designing quantitative instruments to measure program impact. *West Lafayette, IN: Purdue Extension*.

Barnes, S. J. (2002). Wireless digital advertising: nature and implications. *International journal of advertising*, *21*(3), 399-420.

Batra, U., Sachdeva, S., & Mukherjee, S. (2015). Implementing healthcare interoperability utilizing SOA and data interchange agent. *Health policy and technology*, *4*(3), 241-255.

Becker, G. S. (1965). A Theory of the Allocation of Time. *The economic journal*, *75*(299), 493-517.

Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*, *28*(1), 34-49. https://doi.org/10.1016/j.jsis.2018.11.002

Bélanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*, *28*(1), 34-49.

Berezowska, A., Fischer, A. R., Ronteltap, A., van der Lans, I. A., & van Trijp, H. C. (2015). Consumer adoption of personalised nutrition services from the perspective of a risk–benefit trade-off. *Genes & nutrition*, *10*(6), 1-14.

Bhattacherjee, A., & Barfar, A. (2011). Information technology continuance research: current state and future directions. *Asia Pacific Journal of Information Systems*, *21*(2), 1-18.

Biocca, F., Chad Harms, and Judee K. Burgoon. (2003). Toward a more robust theory and measure of social presence: Review and suggested criteria. *Presence: Teleoperators & virtual environments,, 12(5), 456-480.*

Biocca, F., Harms, C., & Burgoon, J. K. (2003). Toward a more robust theory and measure of social presence: Review and suggested criteria. *Presence: Teleoperators & virtual environments*, *12*(5), 456-480.

Boateng, J. K., & Tutu, R. A. (2018). Navigating the Uncertain Path of Research Partnerships. *Journal of Higher Education in Africa/Revue de l'enseignement supérieur en Afrique*, *16*(1/2), 77-94.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of computer-mediated Communication*, *13*(1), 210-230.

Boyle, M., Neustaedter, C., & Greenberg, S. (2009). Privacy factors in video-based media spaces. In *Media Space 20+ Years of Mediated Life* (pp. 97-122). Springer.

Brandeis, L., & Warren, S. (1890). The right to privacy. *Harvard law review*, *4*(5), 193-220.

Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., Truscott, A., & Accenture, L. (2016). Blockchain: Securing a new health interoperability experience. *Accenture LLP*, 1-11.

Brown, S. A., Dennis, A. R., & Venkatesh, V. (2010). Predicting collaboration technology use: Integrating technology adoption and collaboration research. *Journal of management information systems*, *27*(2), 9-54.

Buck, C., & Burster, S. (2017). App information privacy concerns.

Bullinger, A., Renken, U., & Moeslein, K. (2011). Understanding online collaboration technology adoption by researchers–a model and empirical study.

Bullinger, A. C., Hallerstede, S., Renken, U., Soeldner, J.-H., & Moeslein, K. M. (2010). Towards Research Collaboration-a Taxonomy of Social Research Network Sites. AMCIS,

Burton-Jones, A., & Straub Jr, D. W. (2006). Reconceptualizing system usage: An approach and empirical test. *Information Systems Research*, *17*(3), 228-246.

Calefato, F., Iaffaldano, G., & Lanubile, F. (2018). Collaboration success factors in an online music community. Proceedings of the 2018 ACM Conference on Supporting Groupwork,

Campbelli, D., & Stanley, J. (1963). Experimental, and guasi= experimental desions for research-Boston» MA Houghlin Mifflin.

Cao, X., Liu, X., Zhu, B., Miao, Q., Hu, C., & Xu, F. (2018). Semantic Matching Using Deep Multi-Perception Semantic Matching Model with Stacking. CCKS Tasks, Carneiro, J., Saraiva, P., Conceição, L., Santos, R., Marreiros, G., & Novais, P. (2019). Predicting satisfaction: perceived decision quality by decision-makers in web-based group decision support systems. *Neurocomputing*, *338*, 399-417.

Carvalho, A. (2020). A permissioned blockchain-based implementation of LMSR prediction markets. *Decision Support Systems, 130*, 113228.

Chandra, S., Srivastava, S. C., & Theng, Y.-L. (2012). Cognitive absorption and trust for workplace collaboration in virtual worlds: An information processing decision making perspective. *Journal of the Association for Information Systems*, *13*(10), 3.

Chen, C.-C., & Yao, J.-Y. (2018). What drives impulse buying behaviors in a mobile auction? The perspective of the Stimulus-Organism-Response model. *Telematics and Informatics, 35*(5), 1249-1262.

Chen, J. Q., & Lee, S. M. (2003). An exploratory cognitive DSS for strategic decision making. *Decision Support Systems*, *36*(2), 147-160.

Chen, R., Hua, Q., Chang, Y.-S., Wang, B., Zhang, L., & Kong, X. (2018). A survey of collaborative filtering-based recommender systems: From traditional methods to hybrid methods based on social networks. *IEEE Access*, *6*, 64301-64320.

Cheng, S., Zhang, B., Zou, G., Huang, M., & Zhang, Z. (2019). Friend recommendation in social networks based on multi-source information fusion. *International Journal of Machine Learning and Cybernetics*, *10*(5), 1003-1024.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. In: JSTOR.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, *14*(2), 189-217.

Cho, H., & Yu, Y. (2018). Link prediction for interdisciplinary collaboration via co-authorship network. *Social Network Analysis and Mining*, *8*(1), 1-12.

Choi, S. (2016). The flipside of ubiquitous connectivity enabled by smartphone-based social networking service: Social presence and privacy concern. *Computers in Human Behavior*, *65*, 325-333.

Chuan, P. M., Ali, M., Khang, T. D., & Dey, N. (2018). Link prediction in co-authorship networks based on hybrid content similarity metric. *Applied Intelligence*, *48*(8), 2470-2486.

Churchill Jr, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of marketing research*, *16*(1), 64-73.

Clarke, D., & Ali, S. T. (2017). End to end security is not enough. Cambridge International Workshop on Security Protocols,

Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. *Technological Forecasting and Social Change*, *161*, 120299.

Coltman, T., Devinney, T. M., Midgley, D. F., & Venaik, S. (2008). Formative versus reflective measurement models: Two applications of formative measurement. *Journal of Business Research*, *61*(12), 1250-1262.

Conti, G., Shay, L., & Hartzog, W. (2014). Deconstructing the relationship between privacy and security. *IEEE Technology and Society Magazine*, *33*(2), 28-30.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, *10*(1), 104-115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of social Issues*, *59*(2), 323-342.

Da Xu, L., & Viriyasitavat, W. (2019). Application of blockchain in collaborative Internet-of-Things services. *IEEE Transactions on Computational Social Systems*, *6*(6), 1295-1305.

Davis, M. M., & Vollmann, T. E. (1990). A framework for relating waiting time and customer satisfaction in a service operation. *Journal of Services Marketing*.

Dean, E., Elardo, J., Green, M., Wison, Benjamin Berger, & Sebastian. (2016). *Principles of Microeconomics: Scarcity and Social Provisioning*

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management*, *50*, 261-272.

Denstadli, J. M., Julsrud, T. E., & Hjorthol, R. J. (2012). Videoconferencing as a mode of communication: A comparative study of the use of videoconferencing and face-to-face meetings. *Journal of Business and Technical Communication*, *26*(1), 65-91.

Dermentzi, E., Papagiannidis, S., Toro, C. O., & Yannopoulou, N. (2016). Academic engagement: Differences between intention to adopt social networking sites and other online technologies. *Computers in Human Behavior*, *61*, 321-332.

DeSalvo, K. B. (2015). *Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap*. https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

DeSanctis, G., & Gallupe, R. B. (1987). A foundation for the study of group decision support systems. *Management science*, *33*(5), 589-609.

Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering*, *19*(5), 92-95.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

do Espírito Santo, J. M., & Medeiros, C. B. (2017). Semantic interoperability of clinical data. International Conference on Data Integration in the Life Sciences,

Doffman, Z. (2019). *Semantic Interoperability of Clinical Data. In International Conference on Data Integration in the Life Sciences* https://www.forbes.com/sites/zakdoffman/2019/07/09/warning-as-millions-of-zoom-users-risk-webcam-hijack-change-your-settings-now/?sh=26e84c0242d9

Dou, K., Guo, B., & Kuang, L. (2019). A privacy-preserving multimedia recommendation in the context of social network based on weighted noise injection. *Multimedia Tools and Applications*, *78*(19), 26907-26926.

Dragisic, Z., Ivanova, V., Lambrix, P., Faria, D., Jiménez-Ruiz, E., & Pesquita, C. (2016). User validation in ontology alignment. International Semantic Web Conference,

Dridi, A., Sassi, S., Chbeir, R., & Faiz, S. (2020). A Flexible Semantic Integration Framework for Fully-integrated EHR based on FHIR Standard. ICAART (2),

Dumas, M., Hull, R., Mendling, J., & Weber, I. (2019). Blockchain technology for collaborative information systems (dagstuhl seminar 18332). Dagstuhl Reports,

Duong-Trung, N., Son, H. X., Le, H. T., & Phan, T. T. (2020). Smart care: integrating blockchain technology into the design of patient-centered healthcare systems. Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy,

Durrande-Moreau, A., & Usunier, J.-C. (1999). Time styles and the waiting experience: an exploratory study. *Journal of Service Research*, *2*(2), 173-186.

Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors*, *19*(2), 326.

Edemacu, K., Park, H. K., Jang, B., & Kim, J. W. (2019). Privacy provision in collaborative ehealth with attribute-based encryption: Survey, challenges and future directions. *IEEE Access*, *7*, 89614-89636.

Eibl, G., & Höchtl, B. (2019). Decision Support in Smart Cities: An Assessment by the City of Vienna. *EGOV-CeDEM-ePart 2019*, 13.

Engelenburg, S. v., Janssen, M., & Klievink, B. (2017). Design of a software architecture supporting business-to-government information sharing to improve public safety and security. *Journal of Intelligent Information Systems*, *52*(3), 595-618.

Eom, S. B., Lee, S. M., Kim, E. B., & Somarajan, C. (1998). A survey of decision support system applications (1988–1994). *Journal of the Operational Research Society*, *49*(2), 109-120.

Euzenat, J., & Shvaiko, P. (2013). User involvement. In *Ontology Matching* (pp. 353-375). Springer.

Fabian, B., Ermakova, T., & Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems*, *48*, 132-150.

Falconer, S. M., & Storey, M.-A. (2007). A cognitive support framework for ontology mapping. In *The Semantic Web* (pp. 114-127). Springer.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: a perceived risk facets perspective. *International Journal of Human-Computer Studies*, *59*(4), 451-474.

Feldman, L. P., & Hornik, J. (1981). The use of time: An integrated conceptual model. *Journal of consumer research*, *7*(4), 407-419.

Fellbaum, C. (1998). Towards a representation of idioms in WordNet. Usage of WordNet in Natural Language Processing Systems,

Ferdous, M. S., Margheri, A., Paci, F., Yang, M., & Sassone, V. (2017). Decentralised runtime monitoring for access control systems in cloud federations. 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS),

Flory, L., Osei-Bryson, K.-M., & Thomas, M. (2017). A new web personalization decision-support artifact for utility-sensitive customer review analysis. *Decision Support Systems*, *94*, 85-96.

Fornell, C., & Bookstein, F. L. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. *Journal of marketing research*, *19*(4), 440-452.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, *18*(1), 39-50.

Fridgen, G., Lockl, J., Radszuwill, S., Rieger, A., Schweizer, A., & Urbach, N. (2018). A Solution in Search of a Problem: A Method for the Development of Blockchain Use Cases. AMCIS,

Friedewald, M., Van Lieshout, M., & Rung, S. (2015). Modelling the Relationship between Privacy and Security Perceptions and the Acceptance of Surveillance Practices. IFIP International Summer School on Privacy and Identity Management,

Friedrich, G., & Zanker, M. (2011). A taxonomy for generating explanations in recommender systems. *AI Magazine*, *32*(3), 90-98.

Gao, Q., Rau, P.-L. P., & Salvendy, G. (2009). Perception of interactivity: Affects of four key variables in mobile advertising. *International Journal of Human-Computer Interaction*, *25*(6), 479-505.

Garfield, M. J. (2005). Acceptance of ubiquitous computing. *Information Systems Management, 22*(4), 24-31.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example. *Communications of the Association for Information systems*, *16*(1), 5.

Geng, Q., Deng, S., Jia, D., & Jin, J. (2020). Cross-domain ontology construction and alignment from online customer product reviews. *Information Sciences*, *531*, 47-67.

Ghasemaghaei, M. (2020). The impact of in-depth online recommendation agents on consumer disorientation and cognitive absorption perceptions. *Behaviour & Information Technology*, *39*(4), 414-430.

Gill, T. G., & Hevner, A. R. (2013). A fitness-utility model for design science research. *ACM Transactions on Management Information Systems (TMIS)*, *4*(2), 1-24.

González-Ferrer, A., Seara, G., Cháfer, J., & Mayol, J. (2018). Generating Big Data Sets from Knowledge-based Decision Support Systems to Pursue Value-based Healthcare. *International Journal of Interactive Multimedia & Artificial Intelligence*, *4*(7).

Goo, J., Kishore, R., Rao, H. R., & Nam, K. (2009). The role of service level agreements in relational management of information technology outsourcing: an empirical study. *MIS quarterly*, 119-145.

Goode, S., Lin, C., Tsai, J. C., & Jiang, J. J. (2015). Rethinking the role of security in client satisfaction with Software-as-a-Service (SaaS) providers. *Decision Support Systems*, *70*, 73-85.

Goodhue, D. L., Lewis, W., & Thompson, R. (2012). Comparing PLS to regression and LISREL: A response to Marcoulides, Chin, and Saunders. *MIS quarterly*, 703-716.

Goodyear, M. (2019). The Dark Side of Videoconferencing: The Privacy Tribulations of Zoom and the Fragmented State of US Data Privacy Law. *HLRe: Off Rec.*, *10*, 76.

Gregor, S., & Jones, D. (2007). The anatomy of a design theory.

Greifeneder, E., Pontis, S., Blandford, A., Attalla, H., Neal, D., & Schlebbe, K. (2018). Researchers' attitudes towards the use of social networking sites. *Journal of documentation*.

Grewal, D., Monroe, K. B., & Krishnan, R. (1998). The effects of price-comparison advertising on buyers' perceptions of acquisition value, transaction value, and behavioral intentions. *Journal of marketing*, *62*(2), 46-59.

Grudin, J., & Poltrock, S. (2012). Taxonomy and theory in computer supported cooperative work. *The Oxford handbook of organizational psychology*, *2*, 1323-1348.

Gruzd, A., Staves, K., & Wilk, A. (2012). Connected scholars: Examining the role of social media in research practices of faculty using the UTAUT model. *Computers in Human Behavior*, *28*(6), 2340-2350.

Guo, R., Li, L., Shen, Y., & Zheng, G. (2015). Which Collaboration Technologies Best Support Student Teamwork? An Empirical Investigation.

Gutierrez, A., O'Leary, S., Rana, N. P., Dwivedi, Y. K., & Calle, T. (2019). Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor. *Computers in Human Behavior*, *95*, 295-306.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice*, *19*(2), 139-152.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the academy of marketing science*, *40*(3), 414-433.

Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2016). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*.

Hair Jr, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2017). *Advanced issues in partial least squares structural equation modeling*. saGe publications.

Hakim, A. A., Kellish, A. S., Atabek, U., Spitz, F. R., & Hong, Y. K. (2020). Implications for the use of telehealth in surgical patients during the COVID-19 pandemic. *The American Journal of Surgery*, *220*(1), 48-49.

Hambley, L. A., O'Neill, T. A., & Kline, T. J. (2007). Virtual team leadership: The effects of leadership style and communication medium on team interaction styles and outcomes. *Organizational behavior and human decision processes*, *103*(1), 1-20.

Harba, E. S. I. (2017). Secure data encryption through a combination of AES, RSA and HMAC. *Engineering, Technology & Applied Science Research*, *7*(4), 1781-1785.

Hassanein, K., & Head, M. M. (2004). Manipulating social presence through the web interface and its impact on consumer attitude towards online shopping.

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences—A scoping review. *International Journal of Medical Informatics*, *134*, 104040.

Heckman, M. R. (2017). *The Difference between Data Security and Privacy*. https://www.uscybersecurity.net/csmag/data-security-privacy/

Heller, M. (2020). *Zoom vulnerability reveals privacy issues for users*. https://searchsecurity.techtarget.com/news/252466678/Zoom-vulnerability-reveals-privacy-issues-for-users

Helou, M. A. (2019). Effects of Semantic Gaps on Arabic WordNet-Based Similarity Measures. 2019 International Conference on Innovative Computing (ICIC),

Henningsson, M., & Geschwind, L. (2019). Senior industry practitioners as part-time visiting professors: the various benefits of collaboration. *Higher Education Policy*, *32*(1), 109-128.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In *New challenges to international marketing*. Emerald Group Publishing Limited.

Hevner, A., & Chatterjee, S. (2010). Design science research in information systems. In *Design research in information systems* (pp. 9-22). Springer.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly,* 75-105.

Hew, J.-J., Leong, L.-Y., Tan, G. W.-H., Lee, V.-H., & Ooi, K.-B. (2018). Mobile social tourism shopping: A dual-stage analysis of a multi-mediation model. *Tourism Management*, *66,* 121-139.

Hu, B., Zhou, C., Tian, Y.-C., Qin, Y., & Junping, X. (2019). A collaborative intrusion detection approach using blockchain for multimicrogrid systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(8), 1720-1730.

Huang, X. (2018). Improving communicative competence through synchronous communication in computer-supported collaborative learning environments: A systematic review. *Education Sciences*, *8*(1), 15.

Hudson, S. E., & Smith, I. (1996). Techniques for addressing fundamental privacy and disruption tradeoffs in awareness support systems. Proceedings of the 1996 ACM conference on Computer supported cooperative work,

Hull, R., Batra, V. S., Chen, Y.-M., Deutsch, A., Heath III, F. F. T., & Vianu, V. (2016). Towards a shared ledger business collaboration language based on data-aware processes. International conference on service-oriented computing,

Hylock, R. H., & Zeng, X. (2019). A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. *Journal of medical Internet research*, *21*(8), e13592.

Iachello, G., & Hong, J. (2007). *End-user privacy in human-computer interaction* (Vol. 1). Now Publishers Inc.

Im, G., Rai, A., & Lambert, L. S. (2019). Governance and resource-sharing ambidexterity for generating relationship benefits in supply chain collaborations. *Decision Sciences*, *50*(4), 656-693.

Isaac, O., Abdullah, Z., Aldholay, A. H., & Ameen, A. A. (2019). Antecedents and outcomes of internet usage within organisations in Yemen: An extension of the Unified Theory of Acceptance and Use of Technology (UTAUT) model. *Asia Pacific Management Review*, *24*(4), 335-354.

Ismail, L., & Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry*, *11*(10), 1198.

Ivan, D. (2016). Moving toward a blockchain-based method for the secure storage of patient records. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST,

Ivanova, V., Lambrix, P., & Åberg, J. (2015). Requirements for and evaluation of user support for large-scale ontology alignment. European Semantic Web Conference,

Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT),

Jacoby, J., & Olson, J. C. (1977). nconsumer response to price: An attitudinal, information processing perspective, oin moving ahead with attitude research, y. *Wind and P. Greenberg, eds. Chicago: American Marketing Association*, *73*, 86.

Jacoby, J., Szybillo, G. J., & Berning, C. K. (1976). Time and consumer behavior: An interdisciplinary overview. *Journal of consumer research*, *2*(4), 320-339.

Jarvenpaa, S. L., & Lang, K. R. (2005). Managing the paradoxes of mobile technology. *Information Systems Management*, *22*(4), 7-23.

Jarvenpaa, S. L., Lang, K. R., Takeda, Y., & Tuunainen, V. K. (2003). Mobile commerce at crossroads. *Communications of the ACM*, *46*(12), 41-44.

Järvinen, P. (2007). Action research is similar to design science. *Quality & Quantity*, *41*(1), 37-54.

Jimenez, A., Boehe, D. M., Taras, V., & Caprar, D. V. (2017). Working across boundaries: Current and future perspectives on global virtual teams. *Journal of International Management*, *23*(4), 341-349.

Johann, T., Stanik, C., & Maalej, W. (2017). Safe: A simple approach for feature extraction from app descriptions and app reviews. 2017 IEEE 25th International Requirements Engineering Conference (RE), Johnson, R. E., Rosen, C. C., & Djurdjevic, E. (2011). Assessing the impact of common method variance on higher order multidimensional constructs. *Journal of Applied Psychology, 96*(4), 744.

Jordan, K., & Weller, M. (2018). Academics and social networking sites: Benefits, problems and tensions in professional engagement with online networking. *Journal of Interactive Media in Education, 2018*(1).

Jumaan, I. A., Hashim, N. H., & Al-Ghazali, B. M. (2020). The role of cognitive absorption in predicting mobile internet users' continuance intention: An extension of the expectation-confirmation model. *Technology in Society, 63*, 101355.

Junglas, I., & Watson, R. T. (2006). The u-constructs: four information drives. *Communications of the Association for Information systems*, *17*(1), 26.

Kagan, D., Alpert, G. F., & Fire, M. (2020). Zooming into video conferencing privacy and security threats. *arXiv preprint arXiv:2007.01059*.

Kang, H., & Jung, E. H. (2020). The smart wearables-privacy paradox: A cluster analysis of smartwatch users. *Behaviour & Information Technology*, 1-14.

Karimi, H., & Kamandi, A. (2019). A learning-based ontology alignment approach using inductive logic programming. *Expert Systems with Applications*, *125*, 412-424.

Karis, D., Wildman, D., & Mané, A. (2016). Improving remote collaboration with video conferencing and video portals. *Human–Computer Interaction, 31*(1), 1-58.

Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *Journal of medical systems*, *42*(8), 1-11.

Kaza, S., & Chen, H. (2008). Evaluating ontology mapping techniques: An experiment in public safety information sharing. *Decision Support Systems*, *45*(4), 714-728.

Ke, W., Liu, H., Wei, K. K., Gu, J., & Chen, H. (2009). How do mediated and non-mediated power affect electronic supply chain management system adoption? The mediating effects of trust and institutional pressures. *Decision support systems*, *46*(4), 839-851.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607-635.

Keith, M. J., Babb, J., Furner, C., Abdullat, A., & Lowry, P. B. (2016). Limited information and quick decisions: consumer privacy calculus for mobile applications. *AIS Transactions on Human-Computer Interaction (THCI), 8*(3), 88-130.

Kim, D., Park, K., Park, Y., & Ahn, J.-H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior, 92*, 273-281.

Kim, H.-W., Chan, H. C., & Gupta, S. (2007). Value-based adoption of mobile internet: an empirical investigation. *Decision support systems, 43*(1), 111-126.

Kim, M. C., & Chen, C. (2015). A scientometric review of emerging trends and new developments in recommendation systems. *Scientometrics*, *104*(1), 239-263.

Klör, B., Monhof, M., Beverungen, D., & Bräuer, S. (2018). Design and evaluation of a model-driven decision support system for repurposing electric vehicle batteries. *European Journal of Information Systems, 27*(2), 171-188.

Knoth, P., Anastasiou, L., Charalampous, A., Cancellieri, M., Pearce, S., Pontika, N., & Bayer, V. (2017). Towards effective research recommender systems for repositories. *arXiv preprint arXiv:1705.00578*.

Kock, N. (2018). Minimum sample size estimation in PLS-SEM: an application in tourism and hospitality research. In *Applying partial least squares in tourism and hospitality research*. Emerald Publishing Limited.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134.

Kong, X., Jiang, H., Yang, Z., Xu, Z., Xia, F., & Tolba, A. (2016). Exploiting publication contents and collaboration networks for collaborator recommendation. *PloS one*, *11*(2), e0148492.

Koornneef, H., Verhagen, W. J., & Curran, R. (2019). A Mobile decision support system for aircraft dispatch. 2019 Annual Reliability and Maintainability Symposium (RAMS),

Kordzadeh, N., & Warren, J. (2017). Communicating Personal Health Information in Virtual Health Communities: An Integration of Privacy Calculus Model and Affective Commitment. *Journal of the Association for Information Systems*, *18*(1), 1.

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: the role of culture. *Business & Information Systems Engineering*, *4*(3), 127-135.

Kuang, T. P., Ibrahim, H., Udzir, N. I., & Sidi, F. (2011). Security extensible access control markup language policy integration based on role-based access control model in healthcare collaborative environments. *American Journal of Economics and Business Administration*, *3*(1), 101-111.

Kukar, M., Vračar, P., Košir, D., Pevec, D., & Bosnić, Z. (2019). AgroDSS: A decision support system for agriculture and farming. *Computers and Electronics in Agriculture*, *161*, 260-271.

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211-1220.

Kuo, T.-T., Zavaleta Rojas, H., & Ohno-Machado, L. (2019). Comparison of blockchain platforms: a systematic review and healthcare examples. *Journal of the American Medical Informatics Association*, *26*(5), 462-478.

Lallmahomed, M. Z., Rahim, N. Z. A., Ibrahim, R., & Rahman, A. A. (2013). Predicting different conceptualizations of system use: Acceptance in hedonic volitional context (Facebook). *Computers in Human Behavior*, *29*(6), 2776-2787.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of social Issues*, *33*(3), 22-42.

Lazou, C., & Tsinakos, A. (2019). Computer-Mediated Communication for Collaborative Learning in Distance Education Environments.

Lederer, S., Hong, J. I., Dey, A. K., & Landay, J. A. (2004). Personal privacy through understanding and action: five pitfalls for designers. *Personal and ubiquitous computing*, *8*(6), 440-454.

Lee, G., & Xia, W. (2010). Toward agile: an integrated analysis of quantitative and qualitative field data on software development agility. *MIS quarterly*, *34*(1), 87-114.

Lee, J.-M., Lee, B., & Rha, J.-Y. (2019). Determinants of mobile payment usage and the moderating effect of gender: Extending the UTAUT model with privacy risk. *International Journal of Electronic Commerce Studies*, *10*(1), 43-64.

Lehner, F., & Haas, N. (2010). Knowledge management success factors-proposal of an empirical research. *Electronic Journal of Knowledge Management*, *8*(1), 79.

Li, C. H., Rajamohan, A. G., Acharya, P. T., Liu, C.-S. J., Patel, V., Go, J. L., Kim, P. E., & Acharya, J. (2020). Virtual read-out: radiology education for the 21st century during the COVID-19 pandemic. *Academic radiology*, *27*(6), 872-881.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*(1), 62-71.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434-445.

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, *88*, 8-17.

Li, S. S., & Karahanna, E. (2015). Online recommendation systems in a B2C E-commerce context: a review and future directions. *Journal of the Association for Information Systems*, *16*(2), 2.

Li, Y., McLean, D., Bandar, Z. A., O'shea, J. D., & Crockett, K. (2006). Sentence similarity based on semantic nets and corpus statistics. *IEEE transactions on knowledge and data engineering*, *18*(8), 1138-1150.

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC),

Lim, C., Mostafa, N., & Park, J. (2017). Digital Omotenashi: Toward a smart tourism design systems. *Sustainability*, *9*(12), 2175.

Lin, H.-F. (2009). Examination of cognitive absorption influencing the intention to use a virtual community. *Behaviour & Information Technology*, *28*(5), 421-431.

Lin, M., Xu, Z., Zhai, Y., & Yao, Z. (2017). Multi-attribute group decision-making under probabilistic uncertain linguistic environment. *Journal of the Operational Research Society*, 1-15.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *86*(1), 114.

Liu, A., Shen, X., Xie, H., Li, Z., Liu, G., Xu, J., Zhao, L., & Wang, F. L. (2020). Privacy-preserving shared collaborative web services QoS prediction. *Journal of Intelligent Information Systems*, *54*(1), 205-224.

Liu, J. C., & Alexander, R. (2017). Factors affecting faculty use of video conferencing in teaching: A mixed-method study. *Journal of Educational Technology Development and Exchange (JETDE)*, *10*(2), 3.

Liu, Z., & Li, Z. (2020). A blockchain-based framework of cross-border e-commerce supply chain. *International journal of information management*, *52*, 102059.

Logunova, O., Ilina, E., Sibileva, N., & Arefyeva, D. Y. (2018). Identification of scientific collaborations: information model and quality features. *DEStech Transactions on Social Science, Education and Human Science*(icems).

López-Pintado, O., Dumas, M., García-Bañuelos, L., & Weber, I. (2019). Dynamic role binding in blockchain-based collaborative business processes. International Conference on Advanced Information Systems Engineering,

Lou, J., Deng, L., & Wang, D. (2021). Understanding the deep structure use of mobile phones–an attachment perspective. *Behaviour & Information Technology*, 1-19.

Lu, J., Wu, D., Mao, M., Wang, W., & Zhang, G. (2015). Recommender system application developments: a survey. *Decision Support Systems*, *74*, 12-32.

Lupton, D. (2014). 'Feeling better connected': Academics' use of social media.

Lyniate. (2019). *Recognizing Technical Challenges to Healthcare Interoperability*. https://mhealthintelligence.com/news/recognizing-technical-challenges-to-healthcare-interoperability

Madrigal, E. (2020). Going remote: maintaining normalcy in our pathology laboratories during the COVID-19 pandemic. *Cancer cytopathology*, *128*(5), 321-322.

Mahadzir, N. H., Omar, M. F., & Nawi, M. N. M. (2018). Semantic similarity measures for Malay-English ambiguous words. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *10*(1-11), 109-112.

Maican, C. I., Cazan, A.-M., Lixandroiu, R. C., & Dovleac, L. (2019). A study on academic staff personality and technology acceptance: The case of communication and collaboration applications. *Computers & Education*, *128*, 113-131.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355.

Marczyk, G., DeMatteo, D., & Festinger, D. (2005). Essentials of Research Design and Methodology. In.

Margheri, A., Masi, M., Miladi, A., Sassone, V., & Rosenzweig, J. (2020). Decentralised provenance for healthcare data. *International Journal of Medical Informatics*, *141*, 104197.

Martins, R., Oliveira, T., Thomas, M., & Tomás, S. (2019). Firms' continuance intention on SaaS use–an empirical study. *Information Technology & People*.

Maruping, L. M., & Magni, M. (2015). Motivating employees to explore collaboration technology in team contexts. *MIS quarterly*, *39*(1), 1-16.

Mattila, J., Seppälä, T., & Holmström, J. (2016). Product-centric information management: A case study of a shared platform with blockchain technology.

McDonald, D. W. (2003). Recommending collaboration with social networks: a comparative evaluation. Proceedings of the SIGCHI conference on Human factors in computing systems,

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57-68.

McMurray, J., Zhu, L., McKillop, I., & Chen, H. (2015). Ontological modeling of electronic health information exchange. *Journal of biomedical informatics*, *56*, 169-178.

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Applied cryptography. *CRC, Boca Raton*.

Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When intrusion detection meets blockchain technology: a review. *IEEE Access*, *6*, 10179-10188.

Michels, B. J., & Chang, C.-W. (2011). Attending a presentation at a distance in real-time via Skype. *TechTrends*, *55*(1), 23-27.

Ming, Y., Xu, P., Qu, H., & Ren, L. (2019). Interpretable and steerable sequence learning via prototypes. Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, Mirzamohammadi, S., & Sani, A. A. (2018). Viola: Trustworthy sensor notifications for enhanced privacy on mobile systems. *IEEE Transactions on Mobile Computing*, *17*(11), 2689-2702.

Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management*, *47*, 120-130.

Morschheuser, B., Hassan, L., Werder, K., & Hamari, J. (2018). How to design gamification? A method for engineering gamified software. *Information and Software Technology*, *95*, 219-237.

Müller, T., Hagenmeyer, V., Schmidt, A., Scholz, S., & Elkaseer, A. (2018). A knowledge-based decision support system for micro and nano manufacturing process chains. 2018 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA),

Mwilu, O. S., Comyn-Wattiau, I., & Prat, N. (2016). Design science research contribution to business intelligence in the cloud—A systematic literature review. *Future Generation Computer Systems*, *63*, 108-122.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Natarajan, T., Balasubramanian, S. A., & Kasilingam, D. L. (2018). The moderating role of device type and age of users on the intention to use mobile shopping applications. *Technology in Society*, *53*, 79-90.

Navarrete, C., Gil-Garcia, J. R., Mellouli, S., Pardo, T. A., & Scholl, J. (2010). Multinational e-government collaboration, information sharing, and interoperability: An integrative model. 2010 43rd Hawaii International Conference on System Sciences,

Naveed, A., Sigwele, T., Hu, Y. F., Kamala, M., & Susanto, M. (2020). Addressing Semantic Interoperability, Privacy and Security Concerns in Electronic Health Records. *Journal of Engineering and Scientific Research*, *2*(1), 31-38.

Negi Advocate, C. (2015). Concept of Video Conferencing in ADR: An Overview--Access to Justice. *Available at SSRN 2662344*.

Neiva, F. W., David, J. M. N., Braga, R., & Campos, F. (2016). Towards pragmatic interoperability to support collaboration: A systematic review and mapping of the literature. *Information and Software Technology*, *72*, 137-150.

Neustaedter, C., Jones, B., O'Hara, K., & Sellen, A. (2018). The Benefits and Challenges of Video Calling for Emergency Situations. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems,

Neustaedter, C., Pang, C., Forghani, A., Oduor, E., Hillman, S., Judge, T. K., Massimi, M., & Greenberg, S. (2015). Sharing domestic life through long-term video connections. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *22*(1), 1-29.

Ngo, D., & Bellahsene, Z. (2016). Overview of YAM++—(not) Yet Another Matcher for ontology alignment task. *Journal of Web Semantics*, *41*, 30-49.

Novack, T., Peters, R., & Zipf, A. (2018). Graph-based matching of points-of-interest from collaborative geo-datasets. *ISPRS International Journal of Geo-Information*, *7*(3), 117.

Oard, D. W., & Kim, J. (1998). Implicit feedback for recommender systems. Proceedings of the AAAI workshop on recommender systems,

Obeid, C., Lahoud, I., El Khoury, H., & Champin, P.-A. (2018). Ontology-based recommender system in higher education. Companion Proceedings of the The Web Conference 2018, Odedra, D., Chahal, B. S., & Patlas, M. N. (2020). Impact of COVID-19 on Canadian radiology residency training programs. *Canadian Association of Radiologists Journal*, *71*(4), 482-489.

Ogata, H., Yano, Y., Furugori, N., & Jin, Q. (2001). Computer supported social networking for augmenting cooperation. *Computer Supported Cooperative Work (CSCW)*, *10*(2), 189-209.

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of advertising*, *38*(4), 63-77.

Okazaki, S., & Mendez, F. (2013). Perceived ubiquity in mobile services. *Journal of Interactive marketing*, *27*(2), 98-111.

Okazaki, S., Molina, F. J., & Hirose, M. (2012). Mobile advertising avoidance: exploring the role of ubiquity. *Electronic Markets*, *22*(3), 169-183.

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. In: Elsevier.

Otero-Cerdeira, L., Rodríguez-Martínez, F. J., & Gómez-Rodríguez, A. (2015). Ontology matching: A literature review. *Expert Systems with Applications*, *42*(2), 949-971.

Ouellette, J. A., & Wood, W. (1998). Habit and intention in everyday life: The multiple processes by which past behavior predicts future behavior. *Psychological bulletin*, *124*(1), 54.

Oyelere, S. S., Suhonen, J., Wajiga, G. M., & Sutinen, E. (2018). Design, development, and evaluation of a mobile learning application for computing education. *Education and Information Technologies*, *23*(1), 467-495.

Ozturk, A. B., Nusair, K., Okumus, F., & Singh, D. (2017). Understanding mobile hotel booking loyalty: an integration of privacy calculus theory and trust-risk framework. *Information Systems Frontiers*, *19*(4), 753-767.

Paci, F., Squicciarini, A., & Zannone, N. (2018). Survey on access control for community-centered collaborative systems. *ACM Computing Surveys (CSUR)*, *51*(1), 1-38.

Padilla-Meléndez, A., Garrido-Moreno, A., & Del Aguila-Obra, A. R. (2008). Factors affecting e-collaboration technology use among management students. *Computers & Education*, *51*(2), 609-623.

Panahifar, F., Byrne, P. J., Salam, M. A., & Heavey, C. (2018). Supply chain collaboration and firm’s performance: the critical role of information sharing and trust. *Journal of Enterprise Information Management*.

Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health informatics journal*, *25*(4), 1398-1411.

Payne, T. H., Lovis, C., Gutteridge, C., Pagliari, C., Natarajan, S., Yong, C., & Zhao, L.-P. (2019). Status of health information exchange: a comparison of six countries. *Journal of global health*, *9*(2).

Pearson, S., & Benameur, A. (2010). A decision support system for design for privacy. IFIP PrimeLife International Summer School on Privacy and Identity Management for Life,

Pech, F., Martinez, A., Estrada, H., & Hernandez, Y. (2017). Semantic annotation of unstructured documents using concepts similarity. *Scientific Programming*, *2017*.

Pedersen, T., Patwardhan, S., & Michelizzi, J. (2004). WordNet:: Similarity-Measuring the Relatedness of Concepts. AAAI, Peffers, K., Rothenberger, M., Tuunanen, T., & Vaezi, R. (2012). Design science research evaluation. International Conference on Design Science Research in Information Systems,

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45-77.

Peng, C., & Goswami, P. (2019). Meaningful integration of data from heterogeneous health services and home environment based on ontology. *Sensors*, *19*(8), 1747.

Pennekamp, J., Dahlmanns, M., Gleim, L., Decker, S., & Wehrle, K. (2019). Security considerations for collaborations in an industrial IoT-based lab of labs. 2019 IEEE Global Conference on Internet of Things (GCIoT),

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65*, 409-419.

Peterson, K. J., Deeduvanu, R., Kanjamala, P., & Mayo, K. (2016). A Blockchain-Based Approach to Health Information Exchange Networks.

Pettigrew, L. M., Kumpunen, S., Rosen, R., Posaner, R., & Mays, N. (2019). Lessons for 'large-scale'general practice provider organisations in England from other inter-organisational healthcare collaborations. *Health Policy*, *123*(1), 51-61.

Pillet, J.-C., & Carillo, K. D. A. (2016). Email-free collaboration: An exploratory study on the formation of new work habits among knowledge workers. *International journal of information management*, *36*(1), 113-125.

PIM. (2008). *PIM ToolKit* https://www.pimedu.org/files/toolkit/PIMtoolkit.pdf

Pinsonneault, A., & Kraemer, K. (1993). Survey research methodology in management information systems: an assessment. *Journal of management information systems*, *10*(2), 75-105.

Ploskas, N., & Papathanasiou, J. (2019). A decision support system for multiple criteria alternative ranking using TOPSIS and VIKOR in fuzzy and nonfuzzy environments. *Fuzzy Sets and Systems*, *377*, 1-30.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, *88*(5), 879.

Pokraev, S., Reichert, M., Steen, M. W., & Wieringa, R. (2005). Semantic and Pragmatic Interoperability: A Model for Understanding.

Praharaj, S., Scheffel, M., Drachsler, H., & Specht, M. (2018). Multimodal analytics for real-time feedback in co-located collaboration. European Conference on Technology Enhanced Learning,

Prakash, S., & Rajput, A. (2018). Hybrid cryptography for secure data communication in wireless sensor networks. In *Ambient Communications and Computer Systems* (pp. 589-599). Springer.

Pretorius, C. (2017). Exploring procedural decision support systems for wicked problem resolution. *South African Computer Journal*, *29*(1), 191-219.

Preuveneers, D., Joosen, W., & Ilie-Zudor, E. (2018). Policy reconciliation for access control in dynamic cross-enterprise collaborations. *Enterprise Information Systems*, *12*(3), 279-299.

Price, P., Jhangiani, R., Chiang, I., Leighton, D., & Cuttler, C. (2017). Research Methods in Psychology (3rd American Edition). *Washington: PressBooksPublications*.

Qin, L., Kim, Y., & Tan, X. (2016). Understanding the intention of using mobile social networking apps.

Quan-Haase, A. (2012). Research and teaching in real time: 24/7 collaborative networks. In *Social media for academics* (pp. 39-57). Elsevier.

Rahi, S., Mansour, M. M. O., Alghizzawi, M., & Alnaser, F. M. (2019). Integration of UTAUT model in internet banking adoption context: The mediating role of performance expectancy and effort expectancy. *Journal of Research in Interactive Marketing*.

Rincón-Nigro, M., & Deng, Z. (2013). A text-driven conversational avatar interface for instant messaging on mobile devices. *IEEE Transactions on Human-Machine Systems*, *43*(3), 328-332.

Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). Editor's comments: a critical look at the use of PLS-SEM in" MIS Quarterly". *MIS quarterly*, iii-xiv.

Roehrs, A., Da Costa, C. A., & da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of biomedical informatics*, *71*, 70-81.

Rouibah, K., Lowry, P. B., & Hwang, Y. (2016). The effects of perceived enjoyment and perceived risks on trust formation and intentions to use online payment systems: New perspectives from an Arab country. *Electronic Commerce Research and Applications*, *19*, 33-43.

Rowe, F. (2020). Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world. *International journal of information management*, *55*, 102178.

Rubio-Medrano, C. E., D'Souza, C., & Ahn, G.-J. (2013). Supporting secure collaborations with attribute-based access control. 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing,

Russell, A., & Frachtenberg, E. (2021). After the Pandemic: Tech, Work, and the Tech Workforce.

Ryans, A. B. (1974). Estimating consumer preferences for a new durable brand in an established product class. *Journal of marketing research*, *11*(4), 434-443.

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, *2016*(2), 15-18.

Salahshour Rad, M., Nilashi, M., Mohamed Dahlan, H., & Ibrahim, O. (2019). Academic researchers’ behavioural intention to use academic social networking sites: A case of Malaysian research universities. *Information development*, *35*(2), 245-261.

Samad, S., Nilashi, M., & Ibrahim, O. (2019). The impact of social networking sites on students’ social wellbeing and academic performance. *Education and Information Technologies*, *24*(3), 2081-2094.

Sarwar, B., Zulfiqar, S., Aziz, S., & Ejaz Chandia, K. (2019). Usage of social media tools for collaborative learning: The effect on learning success with the moderating role of cyberbullying. *Journal of Educational Computing Research*, *57*(1), 246-279.

Satti, F. A., Khan, W. A., Ali, T., Hussain, J., Yu, H. W., Kim, S., & Lee, S. (2020). Semantic bridge for resolving healthcare data interoperability. 2020 International conference on information networking (ICOIN),

Schade, M., Piehler, R., Warwitz, C., & Burmann, C. (2018). Increasing consumers’ intention to use location-based advertising. *Journal of Product & Brand Management*.

Schafer, J. B., Frankowski, D., Herlocker, J., & Sen, S. (2007). Collaborative filtering recommender systems. In *The adaptive web* (pp. 291-324). Springer.

Schumacker, R. E., & Lomax, R. G. (2004). *A beginner's guide to structural equation modeling*. psychology press.

Schweizer, A., Schlatt, V., Urbach, N., & Fridgen, G. (2017). Unchaining Social Businesses-Blockchain as the Basic Technology of a Crowdlending Platform. ICIS,

Scott, B., Loonam, J., & Kumar, V. (2017). Exploring the rise of blockchain technology: Towards distributed collaborative organizations. *Strategic Change*, *26*(5), 423-428.

Shafiq, B., Bertino, E., & Ghafoor, A. (2005). Access control management in a distributed environment supporting dynamic collaboration. Proceedings of the 2005 workshop on Digital identity management,

Shao, Z., Zhang, L., Li, X., & Guo, Y. (2019). Antecedents of trust and continuance intention in mobile payment platforms: The moderating effect of gender. *Electronic Commerce Research and Applications*, *33*, 100823.

Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International journal of information management*, *45*, 44-55.

Sherif, M., & Hovland, C. I. (1961). Social judgment: Assimilation and contrast effects in communication and attitude change.

Short, J., Williams, E., & Christie, B. (1976). *The social psychology of telecommunications*. Toronto; London; New York: Wiley.

Siahaan, A. P. U. (2018). Comparative analysis of rsa and elgamal cryptographic public-key algorithms.

Sierra, A., Gercek, C., Übermasser, S., & Reinders, A. (2019). Simulation-supported testing of smart energy product prototypes. *Applied Sciences*, *9*(10), 2030.

Silic, M., Back, A., & Sammer, T. (2017). Employee acceptance and use of unified communications and collaboration in a cross-cultural environment. In *Remote Work and Collaboration: Breakthroughs in Research and Practice* (pp. 1-22). IGI Global.

Slattery, E. L., Voelker, C. C., Nussenbaum, B., Rich, J. T., Paniello, R. C., & Neely, J. G. (2011). A practical guide to surveys and questionnaires. *Otolaryngology--Head and Neck Surgery*, *144*(6), 831-837.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly*, 167-196.

Solove, D. J. (2005). A taxonomy of privacy. *U. Pa. L. Rev.*, *154*, 477.

Song, S., Zhang, X., & Qin, G. (2017). Multi-domain ontology mapping based on semantics. *Cluster Computing*, *20*(4), 3379-3391.

Sprague Jr, R. H. (1980). A framework for the development of decision support systems. *MIS quarterly*, 1-26.

Sri, P. A., & Bhaskari, D. L. (2020). Blockchain technology for secure medical data sharing using consensus mechanism. *Materials Today: Proceedings*.

Stanko, T., & Sena, J. A. (2019). Exploring the impact of social networking on communication in organizations. *Journal of Computer Information Systems*, *59*(4), 334-343.

Straub, D., & Karahanna, E. (1998). Knowledge worker communications and recipient availability: Toward a task closure explanation of media choice. *Organization science*, *9*(2), 160-175.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS quarterly*, 147-169.

Subramaniyaswamy, V., Manogaran, G., Logesh, R., Vijayakumar, V., Chilamkurti, N., Malathi, D., & Senthilselvan, N. (2019). An ontology-driven personalized food recommendation in IoT-based healthcare system. *The Journal of Supercomputing*, *75*(6), 3184-3216.

Sun, J., Yan, J., & Zhang, K. Z. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, *2*(1), 1-9.

Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS quarterly*, 1141-1164.

Tang, B., Kang, H., Fan, J., Li, Q., & Sandhu, R. (2019). Iot passport: A blockchain-based trust framework for collaborative internet-of-things. Proceedings of the 24th ACM symposium on access control models and technologies,

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407.

Tarus, J. K., Niu, Z., & Mustafa, G. (2018). Knowledge-based recommendation: a review of ontology-based recommender systems for e-learning. *Artificial Intelligence Review*, *50*(1), 21-48.

Taylor, E. (2021). *What will happen to remote work after pandemic?* https://azbigmedia.com/business/what-will-happen-to-remote-work-after-pandemic/#:~:text=Considering%20past%20trends%2C%20this%20data,remote%20from%20this%20year%20forward

Teo, H.-H., Wei, K. K., & Benbasat, I. (2003). Predicting intention to adopt interorganizational linkages: An institutional perspective. *MIS quarterly*, 19-49.

Thakurta, R., Mueller, B., Ahlemann, F., & Hoffmann, D. (2017). The state of design–a comprehensive literature review to chart the design science research discourse. Proceedings of the 50th Hawaii International Conference on System Sciences,

Thanapalasingam, T., Osborne, F., Birukou, A., & Motta, E. (2018). Ontology-based recommendation of editorial products. International Semantic Web Conference,

Thatcher, J. B., Wright, R. T., Sun, H., Zagenczyk, T. J., & Klein, R. (2018). Mindfulness in information technology use: Definitions, distinctions, and a new measure. *MIS quarterly*, *42*(3), 831-848.

Thompson, S. (2017). The preservation of digital signatures on the blockchain. *See Also*(3).

Tolone, W., Ahn, G.-J., Pai, T., & Hong, S.-P. (2005). Access control in collaborative systems. *ACM Computing Surveys (CSUR)*, *37*(1), 29-41.

Toumi, K., Cavalli, A., & Maarabani, M. E. (2012). Role based interoperability security policies in collaborative systems. 2012 International Conference on Collaboration Technologies and Systems (CTS),

Trafimow, D., & Borrie, W. T. (1999). Influencing future behavior by priming past behavior: A test in the context of Petrified Forest National Park. *Leisure Sciences*, *21*(1), 31-42.

Tripathi, A. R., Ahmed, T., & Kumar, R. (2003). Specification of secure distributed collaboration systems. The Sixth International Symposium on Autonomous Decentralized Systems, 2003. ISADS 2003.,

Tsai, C.-H., Brusilovsky, P., & Rahdari, B. (2019). Exploring User-Controlled Hybrid Recommendation in a Conference Context. IUI Workshops,

TUNCER, B., & ŞAHİN, F. (2019). Exploring Entrepreneurial Intention in the Context of Theory of Planned Behavior: A Cross-Cultural Comparison.

Turker, A. K., Aktepe, A., Inal, A. F., Ersoz, O. O., Das, G. S., & Birgoren, B. (2019). A decision support system for dynamic job-shop scheduling using real-time data with simulation. *Mathematics*, *7*(3), 278.

Ulusoy, O., & Yolum, P. (2019). Emergent privacy norms for collaborative systems. International Conference on Principles and Practice of Multi-Agent Systems,

Vaishnavi, V., Kuechler, W., & Petter, S. (2004). Design science research in information systems. *January*, *20*, 2004.

van Engelenburg, S., Janssen, M., & Klievink, B. (2019). Design of a software architecture supporting business-to-government information sharing to improve public safety and security. *Journal of Intelligent Information Systems*, *52*(3), 595-618.

Van Raaij, E. M., & Schepers, J. J. (2008). The acceptance and use of a virtual learning environment in China. *Computers & Education*, *50*(3), 838-852.

Van Slyke, C., Shim, J., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, *7*(6), 16.

Venable, J., Pries-Heje, J., & Baskerville, R. (2012). A comprehensive framework for evaluation in design science research. International conference on design science research in information systems,

Venkatesh, M. V., Zhao, J., Profitt, L., & Sen-ching, S. C. (2009). Audio-visual privacy protection for video conference. 2009 IEEE International Conference on Multimedia and Expo,

Venkatesh, V., Aloysius, J. A., Hoehle, H., & Burton, S. (2017). Design and evaluation of auto-id enabled shopping assistance artifacts in customers' mobile phones: two retail store laboratory experiments. *MIS quarterly*, *41*(1), 83-113.

Venkatesh, V., Thong, J. Y., Chan, F. K., Hu, P. J. H., & Brown, S. A. (2011). Extending the two-stage information systems continuance model: Incorporating UTAUT predictors and the role of context. *Information Systems Journal*, *21*(6), 527-555.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, *36*(1), 157-178.

Vinner, S. (2002). The role of definitions in the teaching and learning of mathematics. In *Advanced mathematical thinking* (pp. 65-81). Springer.

Walcott, J. (2020). *Foreign Spies Are Targeting Americans on Zoom and Other Video Chat Platforms, U.S. Intel Officials Say*. https://time.com/5818851/spies-target-americans-zoom-others/

Wang, H., Ma, S., Dai, H.-N., Imran, M., & Wang, T. (2020). Blockchain-based data privacy management with nudge theory in open banking. *Future Generation Computer Systems*, *110*, 812-823.

Wang, H.-Y., & Wang, S.-H. (2010). Predicting mobile hotel reservation adoption: Insight from a perceived value standpoint. *International Journal of Hospitality Management*, *29*(4), 598-608.

Wang, S., Zhang, Y., & Zhang, Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *Ieee Access*, *6*, 38437-38450.

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International journal of information management*, *36*(4), 531-542.

Wastell, D., Sauer, J., & Schmeink, C. (2009). Time for a "design turn" in IS innovation research? A practice report from the home front. *Information Technology & People*.

Watson, H. J. (2018). Revisiting Ralph Sprague's framework for developing decision support systems. *Communications of the Association for Information systems*, *42*(1), 13.

Watson, R. T., Pitt, L. F., Berthon, P., & Zinkhan, G. M. (2002). U-commerce: expanding the universe of marketing. *Journal of the academy of marketing science*, *30*(4), 333-347.

Westin, A. F. (1967). Privacy and freedom Atheneum. *New York*, *7*, 431-453.

Wiegard, R.-B., & Breitner, M. H. (2019). Smart services in healthcare: A risk-benefit-analysis of pay-as-you-live services from customer perspective in Germany. *Electronic Markets*, *29*(1), 107-123.

Wilson, D., & Valacich, J. S. (2012). Unpacking the privacy paradox: Irrational decision-making within the privacy calculus.

Wimmer, H., & Yoon, V. Y. (2017). Counterfeit product detection: Bridging the gap between design science and behavioral science in information systems research. *Decision Support Systems*, *104*, 1-12.

Wu, K., Vassileva, J., Noorian, Z., & Zhao, Y. (2015). How do you feel when you see a list of prices? The interplay among price dispersion, perceived risk and initial trust in Chinese C2C market. *Journal of Retailing and Consumer Services*, *25*, 36-46.

Wüst, K., & Gervais, A. (2018). Do you need a blockchain? 2018 Crypto Valley Conference on Blockchain Technology (CVCBT),

Xiang, P., & Yuan, T. (2019). A collaboration-driven mode for improving sustainable cooperation in smart industrial parks. *Resources, Conservation and Recycling*, *141*, 273-283.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42-52.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of management information systems*, *26*(3), 135-174.

Yan, K., & Cui, W. (2019). A visual recommendation system for co-authorship social networks (ChinaVis 2018). *Journal of Visualization*, *22*(2), 385-399.

Yang, H., & Yang, B. (2017). A blockchain-based approach to the secure sharing of healthcare data. *Nisk Journal*, 100-111.

Yang, J., Onik, M. M. H., Lee, N.-Y., Ahmed, M., & Kim, C.-S. (2019). Proof-of-familiarity: a privacy-preserved blockchain scheme for collaborative medical decision-making. *Applied Sciences*, *9*(7), 1370.

Ye, S., Lei, S. I., Shen, H., & Xiao, H. (2020). Social presence, telepresence and customers' intention to purchase online peer-to-peer accommodation: A mediating model. *Journal of Hospitality and Tourism Management*, *42*, 119-129.

Yoo, Y., & Alavi, M. (2001). Media and group cohesion: Relative influences on social presence, task participation, and group consensus. *MIS quarterly*, 371-390.

Yuan, S., Hussain, S. A., Hales, K. D., & Cotten, S. R. (2016). What do they like? Communication preferences and patterns of older adults in the United States: The role of technology. *Educational Gerontology*, *42*(3), 163-174.

Yuan, S., Liu, Y., Yao, R., & Liu, J. (2016). An investigation of users' continuance intention towards mobile banking in China. *Information development*, *32*(1), 20-34.

Zamir, S., Hennessy, C. H., Taylor, A. H., & Jones, R. B. (2018). Video-calls to reduce loneliness and social isolation within care environments for older people: an implementation study using collaborative action research. *BMC geriatrics*, *18*(1), 1-13.

Zeithaml, V. A. (1988). Consumer perceptions of price, quality, and value: a means-end model and synthesis of evidence. *Journal of marketing*, *52*(3), 2-22.

Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2017). Metrics for assessing blockchain-based healthcare decentralized apps. 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom),

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: applying blockchain to securely and scalably share clinical data. *Computational and structural biotechnology journal*, *16*, 267-278.

Zhang, X., & Venkatesh, V. (2018). From design principles to impacts: A theoretical framework and research agenda. *AIS Transactions on Human-Computer Interaction*, *10*(2), 105-128.

Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce*, *16*(4), 53-90.

Zhou, T. (2012). Examining mobile banking user adoption from the perspectives of trust and flow experience. *Information Technology and Management*, *13*(1), 27-37.

Zhou, T., Lu, Y., & Wang, B. (2010). Integrating TTF and UTAUT to explain mobile banking user adoption. *Computers in Human Behavior*, *26*(4), 760-767.

Zografos, K. G., Androutsopoulos, K. N., & Vasilakis, G. M. (2002). A real-time decision support system for roadway network incident response logistics. *Transportation Research Part C: Emerging Technologies*, *10*(1), 1-18.

APPENDIX

Table 3 Summary of the Studies on Video Conferencing (VC) apps

Study	Collaboration technologies including Videoconferencing	Adoption Theory	Dependent variable
(Brown et al., 2010)	Collaboration technology usage such as SMS and in-house collaboration	Unified Theory of Acceptance and Use of Technology, Social presence theory, Channel expansion theory, and task closure model	Use and Intentions to use collaborative technologies
(Gruzd et al., 2012)	Social media tools	Technology acceptance model and Unified technology acceptance model.	Examine how the social media impacts research practices in academia.
(Guo et al., 2015)	Collaboration technologies suitable for student team project	TTF	Identify which collaborative technologies suit the collaborative needs of the students.
(Pillet & Carillo, 2016)	Collaborative technologies	-	How collaborative technologies improve knowledge sharing
(Liu & Alexander, 2017)	Blackboard collaborate, VC apps	-	Factors affecting usage and non-usage of VC in academia.

(Sarwar et al., 2019)	Social media	Technology acceptance model and Constructivism Theory	Social media use, collaborative learning, and learner performance
(Maican et al., 2019)	Online collaboration applications	Unified Theory of Acceptance and Use of Technology	How online collaboration applications impact behavioral intentions as well as use behavior

Table 4 Survey Questionnaire

Constructs	Authors
Perceived Surveillance	
PS1. I believe that the location of my video conferencing apps is monitored at least part of the time.	(Xu et al., 2012) (Dropped)
PS2. I am concerned that video conferencing apps are collecting too much information about me.	(Belanger & Crossler, 2019)
PS3. I am concerned that video conferencing apps may monitor my activities on my mobile device.	(Belanger & Crossler, 2019)
Perceived Intrusion	(Belanger & Crossler, 2019)
PI1. I feel that as a result of my using video conferencing apps, others know about me more than I am comfortable with.	
PI2. I believe that as a result of my using video conferencing apps, information about me that I consider private is now more readily available to others than I would want.	
PI3. I feel that as a result of my using video conferencing apps, information about me is out there that, if used, will invade my privacy.	
Secondary Use of Personal Information	(Belanger & Crossler, 2019)
SU1. I am concerned that video conferencing apps may use my personal information for other purposes without notifying me or getting my authorization.	
SU2. When I give personal information to use video conferencing apps, I am concerned that apps may use my information for other purposes.	
SU3. I am concerned that video conferencing apps may share my personal information with other entities without getting my authorization.	
Time Savings	(Okazaki et al., 2012)
TS1. Using video conferencing apps is an effective way to manage my time.	
TS2. Using video conferencing apps makes my life easier.	
TS3. Using video conferencing apps fits my schedule.	
TS4. Using video conferencing apps enables flexibility in my schedule.	
Spatial Flexibility	(Okazaki et al., 2012)
SF1. Using video conferencing apps enables me to find information at any place.	
SF2. Using video conferencing apps gives me the ability to overcome the spatial limitation.	
SF3. Using video conferencing apps fits any location, wherever I go.	
SF4. Using video conferencing apps enables me to interact with peers at any place.	
Portability	(Okazaki & Mendez, 2013)
P1. Video conferencing apps are practical because I can use them without difficulty wherever I am.	
P2. Using video conferencing apps outside my home or my workplace is not a problem for me.	

P3. I find it convenient to use video conferencing apps because they don't make me dependent on any fixed installation.

Immediacy (Brown et al., 2010)

I1. Video conferencing apps enable me to quickly reach my peers.

I2. When I communicate with peers using video conferencing apps, they usually respond quickly.

I3. When my peers communicate with me using video conferencing apps, I try to respond immediately.

I4. The use of video conferencing apps to communicate with peers provides a chance for social interaction.

Continuity (Okazaki & Mendez, 2013)

C1. Using video conferencing apps keeps me well informed at all times.

C2. With video conferencing apps, I can always keep up with my peers.

C3. When I use video conferencing apps, I don't have to interrupt my current task. Dropped

Perceived Risks (Malhotra et al., 2004)

PR1. It would be risky to share information using video conferencing apps.

PR2. There would be a high potential for loss associated with sharing information using video conferencing apps.

PR3. There would be too much uncertainty associated with sharing information using video conferencing apps.

PR4. Sharing information using video conferencing apps would involve many unexpected problems.

Perceived Benefits (Kim et al., 2019)

PB1. Using video conferencing apps improves my performance.

PB2. Using video conferencing apps enhances my effectiveness.

PB3. Using video conferencing apps enables me to accomplish my tasks more quickly.

PB4. Using video conferencing apps is very useful for me.

Social Presence (Choi, 2016)

SP1. The interaction with my peers is personal.

SP2. The interaction with my peers is warm.

SP3. The interaction with my peers is close.

SP4. The interaction with my peers is humanizing.

Perceived Value (Kim et al., 2007)

PV1. Compared to the fee value I need to pay, the use of video conferencing apps offers value for money.

PV2. Compared to the effort I need to put in, the use of video conferencing apps is beneficial to me.

PV3. Compared to the time I need to spend, the use of video conferencing apps is worthwhile to me.

PV4. Overall, the use of video conferencing apps delivers me good value.

Use Behavior (Zhou et al., 2010)

UB1. I often use video conferencing apps in my professional work.

UB2. I often use video conferencing apps to share my work

UB3. I often use video conferencing apps to meet with my peers.

Effort Expectancy (Venkatesh, 2012)

EE1. Learning how to use video conferencing is easy to me.

EE2. My interactions with video conferencing apps is clear and understandable.

EE3.I find video conferencing easy to use.

EE4. It is easy for me to become skillful at using video conferencing apps.

Perceived Fees (Kim et al., 2007)

PF1. The fees I have to pay to use of video conferencing apps is too high.

PF2. The fees I have to pay to use of video conferencing apps is unreasonable.

PF3. Overall, I am displeased with the fee that I have to pay to use video conferencing apps.

Use (Cognitive Absorption) (Burton-Jones & Straub Jr, 2006)

U1. When I use video conferencing apps, I use features that help me compare and contrast aspects of my tasks with my peers.

U2. When I use video conferencing apps, I use features that help me test different assumptions with my peers.

U3. When I use video conferencing apps, I use features that would help me derive insightful conclusions with my peers

U4. When I use video conferencing apps, I use features that help me perform my tasks with my peers.

Focus (Deep Structure Usage) (Burton-Jones & Straub Jr, 2006)

F1. When I use video conferencing apps, I am able to block other distractions.

F2. When I use video conferencing apps, I feel totally immersed in what I was doing.

F3. When I use video conferencing apps, I feel completely absorbed in what I am doing.

F4. When I use video conferencing apps, my attention don’t get diverted easily.

Continuance Intentions (Venkatesh et al., 2011)

CI1. I intend to continue using video conferencing apps.

CI2. I plan to continue using video conferencing apps.

CI3. I will continue using video conferencing apps.

Table 5 Demographic Characteristics

Sample (N=487)

Gender	n	%
Female	147	30%
Male	337	69%
Prefer not to answer	3	1%

Age		
0 - 17	0	0%
18 – 24	38	8%
25 – 34	204	42%
35 – 44	168	34%
45 – 54	74	15%
55 – 64	0	0%
65 – 74	1	0%
> 74	0	0%
Missing	2	0%

Occupation		
Employed worker	402	83%
Self-employed	50	10%
Student	26	5%
Unemployed/Retired	9	2%

Firm Size		
Large (More than 250)	270	59%
Medium (50 - 249)	81	18%
Small (10 - 49)	61	13%
Micro (less than 10)	48	10%

Table 6 Descriptive Statistics, Composite Reliability, Correlation, and Average Variance Extracted

	Mean	SD	CR	PS	PI	SU	SF	TS	Po	Co	Im	PR	PB	SP	PV	PF	EE	UB	DSU	CA	CI
PS	4.2859	1.706	0.945	**0.947**																	
PI	3.886	1.6211	0.943	0.774	**0.92**																
SU	4.4948	1.7301	0.959	0.709	0.707	**0.942**															
SF	5.2849	1.1426	0.875	0.033	0.01	-0.026	**0.798**														
TS	5.3353	1.2538	0.928	-0.03	-0.073	-0.04	0.637	**0.873**													
Po	5.7369	1.1426	0.879	-0.055	-0.076	-0.094	0.605	0.528	**0.841**												
Co	4.7005	1.1843	0.802	0.027	-0.02	0.032	0.469	0.474	0.367	**0.761**											
Im	5.4085	1.1041	0.881	0.046	-0.001	-0.008	0.561	0.537	0.456	0.536	**0.807**										
PR	4.1404	1.3206	0.937	0.497	0.497	0.569	0.03	-0.037	-0.089	0.015	0.024	**0.888**									
PB	5.222	1.1958	0.939	-0.028	-0.041	-0.006	0.593	0.692	0.42	0.448	0.541	-0.017	**0.891**								
SP	4.4045	1.3578	0.94	-0.065	-0.095	-0.077	0.376	0.337	0.204	0.374	0.426	-0.056	0.419	**0.893**							
PV	5.4282	1.1121	0.936	-0.113	-0.125	-0.096	0.475	0.517	0.347	0.362	0.452	-0.128	0.606	0.351	**0.886**						
PF	2.9015	1.5391	0.946	0.184	0.207	0.152	-0.008	0.011	-0.042	0.012	-0.095	0.163	-0.016	0.013	-0.24	**0.924**					
EE	6.0469	0.9093	0.946	-0.033	-0.076	-0.047	0.265	0.244	0.368	0.22	0.322	-0.108	0.329	0.154	0.372	-0.229	**0.903**				
UB	5.8783	1.1897	0.873	-0.054	-0.051	-0.075	0.292	0.3	0.296	0.28	0.376	-0.05	0.306	0.199	0.308	-0.094	0.377	**0.834**			
DSU	4.7901	1.4829	0.95	0.072	0.072	0.07	0.374	0.382	0.226	0.296	0.411	0.082	0.451	0.272	0.294	0.058	0.199	0.459	**0.9**		
CA	4.3914	1.4243	0.957	-0.043	-0.048	-0.027	0.316	0.309	0.2	0.237	0.254	-0.068	0.39	0.321	0.307	0.028	0.11	0.199	0.4	**0.92**	
CI	6.2007	1.0961	0.976	-0.056	-0.107	-0.066	0.356	0.393	0.34	0.229	0.371	-0.111	0.441	0.207	0.522	-0.101	0.405	0.491	0.3	0.31	**0.965**

Note: Standard Deviation (SD); composite reliability; values in diagonal (bold) are square root of AVE

Table 7 Loadings and Cross Loadings

Construct	Item	PS	PI	SU	SF	TS	Po	Co	Im	PR	PB	SP	PV	PF	EE	UB	DSU	CA	CI
PS	PS2	**0.947**	0.734	0.675	0.015	-0.042	-0.084	0.011	0.017	0.466	-0.032	-0.054	-0.117	0.167	-0.044	-0.059	0.061	-0.048	-0.067
	PS3	**0.946**	0.732	0.666	0.047	-0.014	-0.019	0.042	0.071	0.474	-0.021	-0.068	-0.098	0.182	-0.018	-0.043	0.076	-0.034	-0.038
PI	PI1	0.730	**0.905**	0.628	-0.002	-0.080	-0.090	-0.018	-0.017	0.435	-0.032	-0.088	-0.141	0.237	-0.072	-0.044	0.099	-0.046	-0.090
	PI2	0.704	**0.931**	0.638	0.010	-0.082	-0.060	-0.001	0.002	0.459	-0.056	-0.095	-0.114	0.155	-0.057	-0.021	0.110	-0.046	-0.099
	PI3	0.705	**0.925**	0.685	0.018	-0.040	-0.060	-0.035	0.012	0.477	-0.024	-0.080	-0.091	0.180	-0.080	-0.075	0.107	-0.040	-0.106
SU	SU1	0.669	0.689	**0.937**	-0.031	-0.046	-0.090	0.025	-0.001	0.542	-0.028	-0.082	-0.101	0.173	-0.036	-0.057	0.073	-0.028	-0.077
	SU2	0.679	0.663	**0.953**	-0.031	-0.024	-0.094	0.024	-0.014	0.531	-0.005	-0.099	-0.106	0.120	-0.053	-0.092	0.076	-0.023	-0.055
	SU3	0.654	0.645	**0.936**	-0.012	-0.042	-0.083	0.041	-0.009	0.535	0.016	-0.036	-0.064	0.137	-0.045	-0.063	0.050	-0.025	-0.053
SF	SF1	0.095	0.092	0.026	**0.731**	0.519	0.363	0.394	0.415	0.107	0.445	0.283	0.259	0.047	0.099	0.200	0.366	0.262	0.170
	SF2	0.043	0.027	-0.032	**0.796**	0.549	0.392	0.363	0.490	0.021	0.487	0.315	0.461	-0.044	0.201	0.260	0.294	0.191	0.356
	SF3	-0.021	-0.022	-0.026	**0.810**	0.462	0.615	0.342	0.384	-0.027	0.457	0.261	0.355	0.023	0.225	0.211	0.259	0.269	0.264
	SF4	-0.006	-0.057	-0.047	**0.850**	0.503	0.552	0.399	0.497	0.001	0.499	0.337	0.429	-0.045	0.309	0.256	0.281	0.287	0.335
TS	TS1	0.000	-0.028	0.000	0.531	**0.877**	0.480	0.441	0.461	-0.007	0.587	0.262	0.409	0.060	0.160	0.237	0.322	0.289	0.270
	TS2	-0.054	-0.097	-0.053	0.560	**0.899**	0.447	0.437	0.483	-0.050	0.662	0.323	0.517	0.020	0.205	0.286	0.351	0.283	0.393
	TS3	-0.048	-0.088	-0.060	0.564	**0.868**	0.517	0.381	0.499	-0.053	0.568	0.272	0.439	-0.048	0.268	0.305	0.364	0.273	0.387
	TS4	0.000	-0.040	-0.024	0.570	**0.849**	0.397	0.395	0.431	-0.018	0.599	0.323	0.441	0.007	0.220	0.218	0.296	0.232	0.319
Po	P1	0.007	-0.031	-0.021	0.563	0.513	**0.875**	0.359	0.472	-0.049	0.413	0.183	0.325	-0.035	0.335	0.225	0.180	0.161	0.308
	P2	-0.087	-0.073	-0.131	0.453	0.352	**0.808**	0.220	0.253	-0.092	0.251	0.134	0.207	-0.013	0.294	0.223	0.143	0.149	0.193
	P3	-0.072	-0.093	-0.103	0.500	0.447	**0.839**	0.328	0.394	-0.090	0.374	0.191	0.327	-0.055	0.296	0.301	0.241	0.194	0.342
Co	C1	0.063	0.024	0.051	0.346	0.360	0.264	**0.817**	0.392	0.026	0.344	0.269	0.290	0.036	0.171	0.254	0.233	0.188	0.188
	C2	-0.036	-0.079	0.002	0.416	0.411	0.367	**0.855**	0.516	-0.014	0.402	0.324	0.369	-0.078	0.263	0.314	0.252	0.189	0.271
	C3	0.055	0.031	0.025	0.300	0.303	0.179	**0.584**	0.282	0.034	0.262	0.257	0.127	0.110	0.025	0.016	0.186	0.166	0.018

Im	I1	0.020	0.003	0.022	0.473	0.470	0.418	0.486	**0.821**	0.038	0.465	0.317	0.396	-0.057	0.254	0.345	0.295	0.151	0.323
	I2	0.053	0.008	-0.014	0.490	0.474	0.355	0.473	**0.878**	0.012	0.454	0.324	0.391	-0.053	0.243	0.288	0.353	0.246	0.307
	I3	0.099	0.029	0.035	0.450	0.403	0.382	0.402	**0.853**	0.060	0.381	0.240	0.316	-0.095	0.310	0.310	0.341	0.173	0.312
	I4	-0.034	-0.052	-0.083	0.392	0.378	0.310	0.355	**0.657**	-0.042	0.449	0.530	0.356	-0.109	0.235	0.268	0.343	0.262	0.247
PR	PR1	0.461	0.428	0.503	0.052	-0.022	-0.061	0.031	0.052	**0.882**	0.019	-0.030	-0.093	0.101	-0.040	-0.020	0.052	-0.067	-0.078
	PR2	0.467	0.472	0.519	0.049	-0.018	-0.072	0.001	0.027	**0.916**	-0.023	-0.073	-0.114	0.170	-0.105	-0.053	0.088	-0.074	-0.086
	PR3	0.460	0.457	0.541	0.045	-0.049	-0.053	0.018	0.027	**0.909**	-0.016	-0.038	-0.120	0.124	-0.092	-0.042	0.075	-0.079	-0.098
	PR4	0.368	0.404	0.454	-0.047	-0.044	-0.137	0.004	-0.025	**0.842**	-0.043	-0.058	-0.130	0.191	-0.150	-0.063	0.074	-0.017	-0.138
PB	PB1	0.000	-0.015	0.011	0.512	0.594	0.362	0.368	0.456	0.015	**0.913**	0.378	0.489	0.016	0.281	0.263	0.396	0.362	0.334
	PB2	0.005	-0.015	0.017	0.521	0.624	0.372	0.392	0.491	0.016	**0.923**	0.406	0.515	0.013	0.285	0.267	0.411	0.347	0.360
	PB3	-0.016	-0.028	0.001	0.544	0.633	0.328	0.417	0.501	0.034	**0.889**	0.366	0.492	0.015	0.224	0.232	0.443	0.339	0.341
	PB4	-0.081	-0.081	-0.047	0.529	0.608	0.424	0.413	0.474	-0.116	**0.835**	0.342	0.645	-0.091	0.370	0.319	0.358	0.341	0.518
SP	SP1	-0.052	-0.083	-0.051	0.363	0.350	0.201	0.356	0.402	-0.032	0.407	**0.858**	0.328	-0.004	0.132	0.186	0.239	0.239	0.150
	SP2	-0.065	-0.096	-0.072	0.348	0.293	0.197	0.350	0.381	-0.037	0.381	**0.922**	0.350	0.022	0.149	0.191	0.242	0.313	0.201
	SP3	-0.059	-0.078	-0.084	0.353	0.305	0.193	0.370	0.394	-0.058	0.381	**0.927**	0.287	0.037	0.126	0.157	0.248	0.313	0.193
	SP4	-0.055	-0.083	-0.068	0.273	0.255	0.134	0.250	0.343	-0.074	0.324	**0.862**	0.287	-0.014	0.143	0.177	0.243	0.277	0.196
PV	PV1	-0.079	-0.060	-0.083	0.375	0.340	0.257	0.281	0.316	-0.062	0.400	0.210	**0.760**	-0.191	0.227	0.232	0.220	0.186	0.322
	PV2	-0.100	-0.133	-0.101	0.423	0.483	0.304	0.342	0.409	-0.133	0.570	0.302	**0.933**	-0.227	0.330	0.269	0.274	0.271	0.486
	PV3	-0.095	-0.110	-0.047	0.447	0.515	0.310	0.343	0.439	-0.092	0.591	0.357	**0.923**	-0.225	0.335	0.280	0.280	0.298	0.503
	PV4	-0.125	-0.129	-0.111	0.437	0.474	0.352	0.315	0.425	-0.155	0.564	0.353	**0.917**	-0.209	0.405	0.307	0.265	0.316	0.513
PF	PF1	0.184	0.199	0.154	0.018	0.030	0.008	0.083	-0.038	0.165	0.031	0.047	-0.179	**0.905**	-0.190	-0.065	0.059	0.056	-0.074
	PF2	0.167	0.183	0.123	0.014	-0.007	-0.020	0.039	-0.072	0.160	0.005	0.038	-0.239	**0.919**	-0.199	-0.062	0.047	0.039	-0.093
	PF3	0.166	0.193	0.144	-0.034	0.009	-0.077	-0.044	-0.126	0.140	-0.052	-0.023	-0.240	**0.947**	-0.233	-0.114	0.055	0.002	-0.106
EE	EE1	-0.003	-0.057	-0.023	0.238	0.223	0.324	0.210	0.288	-0.085	0.292	0.132	0.360	-0.223	**0.907**	0.362	0.182	0.108	0.429
	EE2	-0.038	-0.060	-0.068	0.233	0.200	0.329	0.180	0.284	-0.085	0.275	0.127	0.314	-0.213	**0.903**	0.323	0.157	0.084	0.336
	EE3	-0.028	-0.066	-0.044	0.211	0.185	0.302	0.146	0.244	-0.123	0.268	0.100	0.316	-0.208	**0.900**	0.303	0.177	0.083	0.322
	EE4	-0.049	-0.091	-0.040	0.271	0.266	0.368	0.248	0.339	-0.099	0.346	0.189	0.348	-0.185	**0.902**	0.364	0.199	0.120	0.366
UB	UB1	-0.035	-0.060	-0.068	0.171	0.199	0.243	0.158	0.227	-0.042	0.173	0.064	0.192	-0.086	0.311	**0.811**	0.238	0.101	0.415
	UB2	-0.065	-0.041	-0.079	0.259	0.280	0.256	0.261	0.343	-0.063	0.297	0.180	0.256	-0.063	0.319	**0.868**	0.455	0.193	0.403
	UB3	-0.035	-0.028	-0.042	0.296	0.270	0.243	0.278	0.367	-0.020	0.291	0.248	0.319	-0.086	0.313	**0.824**	0.449	0.200	0.411
DSU	UV1	0.097	0.157	0.120	0.340	0.334	0.200	0.277	0.363	0.125	0.407	0.247	0.265	0.066	0.209	0.426	**0.915**	0.283	0.297

	UV2	0.106	0.123	0.062	0.359	0.328	0.217	0.261	0.376	0.091	0.375	0.249	0.214	0.080	0.151	0.406	**0.922**	0.335	0.279
	UV3	0.070	0.113	0.029	0.308	0.313	0.201	0.264	0.339	0.066	0.365	0.222	0.208	0.071	0.134	0.370	**0.909**	0.309	0.271
	UV4	0.006	0.040	0.044	0.347	0.396	0.203	0.271	0.403	0.026	0.470	0.264	0.351	0.009	0.213	0.450	**0.890**	0.353	0.371
CA	FV1	-0.014	-0.034	-0.006	0.265	0.280	0.159	0.218	0.232	-0.020	0.358	0.270	0.283	0.052	0.114	0.185	0.352	**0.894**	0.265
	FV2	-0.075	-0.064	-0.045	0.298	0.288	0.191	0.208	0.229	-0.107	0.370	0.309	0.296	-0.011	0.108	0.171	0.306	**0.939**	0.280
	FV3	-0.028	-0.026	-0.006	0.305	0.287	0.224	0.237	0.248	-0.053	0.351	0.298	0.266	0.013	0.113	0.217	0.350	**0.937**	0.306
	FV4	-0.041	-0.052	-0.041	0.295	0.283	0.161	0.208	0.228	-0.070	0.358	0.302	0.286	0.051	0.071	0.159	0.299	**0.911**	0.273
CI	CI1	-0.041	-0.089	-0.048	0.356	0.394	0.340	0.240	0.379	-0.081	0.430	0.212	0.488	-0.087	0.366	0.474	0.330	0.283	**0.958**
	CI2	-0.048	-0.094	-0.064	0.327	0.363	0.313	0.187	0.341	-0.104	0.419	0.187	0.501	-0.099	0.417	0.474	0.324	0.273	**0.966**
	CI3	-0.073	-0.125	-0.078	0.347	0.381	0.333	0.236	0.354	-0.136	0.429	0.200	0.524	-0.107	0.390	0.474	0.334	0.327	**0.972**

Table 8 Heterotrait-Monotrait Ratio (HTMT)

Construct	PS	PI	SU	SF	TS	Po	Co	Im	PR	PB	SP	PV	PF	EE	UB	DSU	CA	CI
PS																		
PI	0.864																	
SU	0.779	0.765																
SF	0.067	0.072	0.047															
TS	0.041	0.08	0.048	0.75														
Po	0.087	0.092	0.117	0.747	0.615													
Co	0.091	0.08	0.055	0.659	0.631	0.494												
Im	0.076	0.043	0.056	0.69	0.627	0.551	0.73											
PR	0.552	0.545	0.615	0.089	0.042	0.11	0.049	0.068										
PB	0.035	0.047	0.031	0.689	0.764	0.48	0.585	0.629	0.06									
SP	0.072	0.105	0.083	0.435	0.373	0.235	0.492	0.508	0.062	0.458								
PV	0.126	0.135	0.105	0.552	0.568	0.399	0.459	0.524	0.138	0.654	0.379							
PF	0.206	0.226	0.163	0.06	0.046	0.044	0.14	0.103	0.184	0.061	0.042	0.259						
EE	0.04	0.082	0.052	0.165	0.266	0.426	0.262	0.37	0.12	0.353	0.165	0.398	0.24					
UB	0.065	0.061	0.088	0.364	0.357	0.376	0.406	0.469	0.06	0.358	0.233	0.363	0.1	0.44				
DSU	0.086	0.129	0.075	0.432	0.412	0.26	0.386	0.471	0.092	0.482	0.293	0.31	0.07	0.208	0.529			
CA	0.047	0.052	0.029	0.363	0.336	0.23	0.312	0.296	0.078	0.421	0.345	0.328	0.05	0.117	0.23	0.38		
CI	0.06	0.114	0.069	0.4	0.422	0.381	0.271	0.418	0.12	0.465	0.221	0.551	0.1	0.426	0.566	0.35	0.32	

Table 9 Formative Measurement Model Evaluation

Formative construct (second-order construct)	Constructs (first-order reflective)	Weights	VIF
MUIPC	Perceived Surveillance (PS)	0.275***	2.871
	Perceived Intrusion (PI)	0.399***	2.856
	Secondary Use (SU)	0.430***	2.296
Ubiquity	Time Savings (TS)	0.362***	1.949
	Spatial Flexibility (SF)	0.284***	2.212
	Portability (Po)	0.188***	1.692
	Immediacy (Im)	0.267***	1.790
	Continuity (Co)	0.151***	1.535

Note: *** p < 0.01; ** p < 0.05; * p < 0.10

VITA

Ramandeep Kaur Sandhu is a Ph. D candidate in the Department of Information Systems at Virginia Commonwealth University. Her research involves use of both design science and behavioral science research methodologies to design and explore new models for security and privacy-sensitive collaborative systems. More specifically she uses ontology mapping and disruptive technologies such as blockchain to design secure and interoperable collaborative systems. She also uses structural equation modeling to explore the influence of privacy concerns and risks on the individuals' use of collaborative systems in both professional and personal context. She has presented at international, national and regional information systems conferences on topics such as blockchain, ontology mapping, recommender systems, and collaborative systems. She enjoys teaching information systems security, business information systems, system analysis and design, and database management systems to both undergraduate and graduate students. She will be joining Oakland University as a tenure track Assistant Professor with a specialization in teaching and research in Information systems.