2019

A NOVEL FRAMEWORK FOR SOCIAL INTERNET OF THINGS: LEVERAGING THE FRIENDSHIPS AND THE SERVICES EXCHANGED BETWEEN SMART DEVICES

Javad Abed
Virginia Commonwealth University

A NOVEL FRAMEWORK FOR SOCIAL INTERNET OF THINGS: LEVERAGING THE FRIENDSHIPS AND THE SERVICES EXCHANGED BETWEEN SMART DEVICES

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

By

Javad Abed

Director: Dr. Manoj Thomas
Associate Professor, Information Systems

Virginia Commonwealth University
Richmond, Virginia
June, 2019

Acknowledgment

In my PhD journey, I have received a great deal of support and assistance. First of all, I would like to thank my supervisor, Dr. Manoj Thomas for invaluable research guidelines, support and mentorship.

I would like to acknowledge Professor Dr. Allen Lee for his wonderful mentorship and support from the first year of my PhD program. I thank my committee members for reading this dissertation, for providing constructive comments and for agreeing to be my mentors. Finally, I would like to thank my family for motivating me and encouraging me to complete the PhD requirements.

Table of Contents

Abstract

A NOVEL FRAMEWORK FOR THE SOCIAL INTERNET OF THINGS: LEVERAGING FRIENDSHIPS AND SERVICES EXCHANGED BETWEEN SMART DEVICES

By

Javad Abed

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

Virginia Commonwealth University, 2019

Director: Dr. Manoj Thomas
Associate Professor

As humans, we tackle many problems in complex societies and manage the complexities of networked social systems. Cognition and sociability are two vital human capabilities that improve social life and complex social interactions. Adding these features to smart devices makes them capable of managing complex and networked Internet of Things (IoT) settings.

Cognitive and social devices can improve their relationships and connections with other devices and people to better serve human needs. Nowadays, researchers are investigating two future generations of IoT: social IoT (SIoT) and cognitive IoT (CIoT). This study develops a new framework for IoT, called CSIoT, by using complexity science concepts and by integrating social and cognitive IoT concepts. This framework uses a new mechanism to leverage the friendships between devices to address service management, privacy, and security. The

framework addresses network navigability, resilience, and heterogeneity between devices in IoT settings. This study uses a new simulation tool for evaluating the new CSIoT framework and evaluates the privacy-preserving ability of CSIoT using the new simulation tool. To address different CSIoT security and privacy issues, this study also proposes a blockchain-based CSIoT. The evaluation results show that CSIoT can effectively preserve the privacy and the blockchain-based CSIoT performs effectively in addressing different privacy and security issues.

Chapter I: Introduction

1.1 Research motivation

A complex system is defined as a networked system that contains many components interacting with each other. Complexity science is a multi-disciplinary science that explores the features and capabilities of complex systems. In developing and managing a complex system such as IoT, complexity concepts and features of complex systems need to be considered. Additionally, future generations of IoT, such as social IoT (SIoT) and cognitive IoT (CIoT), are even more complex and complexity science can explore them effectively.

According to Atzori et al. (2014), SIoT is the emerging trend in IoT literature. It considers smart objects (things) as social objects that can have social-like capabilities. In SIoT, social networking concepts can be applied to define relationships and interactions between objects. SIoT is important because it considers handling both the inherent requirements of IoT and users' needs, such as privacy and trust.

Cognitive IoT (CIoT) is another trend in IoT research. In CIoT, the goal is to enable IoT objects to learn and make decisions (Matthews, 2016). Indeed, it is possible to create cognition in smart devices by using cognitive computing methods. In CIoT, objects can learn, understand, and think. The important goal of SIoT and CIoT is to manage complexity in IoT networks. This complexity is increasing due to the rapidly growing number of devices and interactions between them. The other goal of these two frameworks is to provide high quality services for humans.

1.2 Research questions

Adding social and cognitive features to IoT objects makes the system even more complex. However, this complexity can encompass many useful features in IoT settings. More complex devices and technologies can solve more complex problems. Consider the advancements in cell phones over the last decades. Every year companies add new features, making them not only more complex than before but able to provide more complex services (e.g., fingerprint, voice recognition, etc.) and to solve more complex problems (e.g., sociability).

This study addresses different issues in IoT and seeks to answer these main research questions:

1.What complexity concepts can we use to define IoT settings as complex systems? Is it useful to consider IoT as a complex system?

2. What are the important friendship initiation factors that are not considered in the SIoT literature? How can we use them with other factors to have a multi-criteria friendship selection process in SIoT?

3. How can we define a new effective friendship updating and friendship leveraging mechanism in SIoT that considers time and other important factors in device friendship like reciprocity?

4. How can we evaluate the new SIoT (CSIoT) framework?

5. How can we investigate privacy in SIoT environments and specifically, how can we investigate and evaluate the privacy in the proposed SIoT framework (CSIoT)?

6. Can we integrate blockchain and SIoT to address some of the security vulnerabilities of SIoT including the centralized structure?

1.3 Research objectives

This dissertation aims to contribute to IS research by investigating IoT, which is an important topic in the literature. It takes a system-thinking approach to consider IoT as a complex system that can be developed, managed and improved by considering complexity concepts and the nature of complex systems. For example, there are several research issues regarding SIoT and its application in security, healthcare and e-business sectors.

This study seeks to develop a novel framework of SIoT that is based on complexity science concepts and the leveraging of friendship among objects. To achieve this goal, this study uses complexity concepts and Knapp's relational stage model to define relationships and interactions between objects and humans. The relationships among SIoT objects are treated as non-linear relationships. Additionally, using complexity science concepts affects other components and features of SIoT, such as trustworthy management (TM) and relationship management (RM). Another goal of this study is to integrate cognition and sociability in IoT objects, so that these objects are not only able to socialize but can also think.

After developing the SIoT framework, this study aims to improve the framework by considering security and privacy issues. For example, the privacy of the object owner and trust can be examined in the security version of the SIoT framework. Finally, this study aims to further improve and contextualize the proposed SIoT framework by adopting relationships in a blockchain environment.

This study proposes a future generation of IoT that uses social network concepts to define the relationships between devices. It also uses some complexity science concepts (e.g., non-linear relationships, agent, etc.) to develop anew framework for IoT settings that are complex systems. This study suggests considering this system's thinking approach in the development of any future generation of IoT.

The object of this research is to make IoT devices more human-like and, therefore, more capable of solving complex problems and providing high quality services for humans. Specifically, this research's goals include:

- Investigating the SIoT as a complex system and applying complexity concepts
- Utilizing social network concepts for developing a new friendship model for SIoT devices
- Developing a new framework for SIoT
- Developing a new simulation tool for SIoT
- Investigating the new SIoT framework in terms of security and privacy requirements
- Integrating SIoT and blockchain for developing to address security is

In the information systems (IS) field, researchers need to focus more on complexity science since it is a vital tool for exploring complex information systems. The call for papers on this topic by top IS journals (McKelvey et al., 2016; Merali and McKelvey 2006) suggests that more research is needed in this area. IoT and future generations of IoT are not sufficiently addressed in the IS field, particularly since IoT is an important information system that could change our lives in the future. This study uses a design science approach to investigate these issues, as well as to explore IoT in security and blockchain environments that are popular topics in IoT-related research studies.

1.4 Significance of the research

This study investigates several important research topics in the IoT field. The first topic is complexity science. According to two calls for papers (McKelvey et al., 2016; Merali and

McKelvey 2006) in the *Management Information Systems Quarterly* (MISQ) and the *Journal of Information Technology* (JIT), two important and influential journals in IS field, there is interest in considering and using the complexity science perspective in different areas of IS research.

In addition, this dissertation aims to develop a new IoT framework that integrates social and cognitive perspectives. This could play a significant role in designing and deploying future generations of IoT. This integration could lead to the development of different capabilities and benefits in IoT settings by making the objects more human-like. Cognitive and social objects can perform a wider range of tasks in comparison to smart-only objects.

Finally, this study explores the performance of complex, social and cognitive IoT in two important areas: security/privacy and blockchain. Nowadays, security and privacy play a vital role in human life. Patients in healthcare settings are vulnerable not only because they need medical attention but also because they share their private data with healthcare organizations. Enhancing security and privacy in healthcare systems helps a patient feel more comfortable. It also improves the patient-physician bond and allows professionals to provide the most efficient care. Using complex IoT systems can create new opportunities and new threats to be investigated by researchers.

1.5 Roadmap to the dissertation

This dissertation comprises three closely related research components that all use a design science methodology. The first component proposes a new friendship management mechanism in SIoT by using a new friendship development and friendship leveraging model based on Knapp's relational stage theory. The model will consider complexity concepts, including non-linearity in relationships between IoT devices, and will utilize cognitive features including learning and semantic reasoning in IoT devices. The cognition and friendship mechanisms will work together for decision-making in such areas as friendship selection, friendship update, and friendship termination processes as well as service acquisition and service composition. As this study develops a new framework for SIoT, it will propose new simulation tools for evaluating this framework.

The second component will build upon the first by considering security and privacy issues. The complexity of IoT systems can create several opportunities as well as threats in security and privacy areas. This intends to improve and revise the IoT framework by investigating these opportunities and threats and by considering specific security and privacy requirements. Different scenarios, including common security and privacy problems, system performance on the new framework, and possible changes and environmental effects, will be applied in simulation to evaluate the new framework.

Specifically, the second component will utilize a use-case smart city scenario (see Section 2.6) to investigate the new framework's ability to manage security and privacy problems. The main research issue in this component will be developing a SIoT-based smart city and addressing the security-privacy issues of IoT settings.

Three sources of security threats will be examined: a malicious user, a bad manufacturer, and an external adversary (Atamli & Martin, 2014), as well as different types of security threats, including device tempering, information disclosure, privacy breach, denial of service, spoofing, evaluation of privilege, signal injection, and side channels.

This study hypothesizes that the friendship mechanism in a new SIoT framework will perform well in managing threats, such as privacy breach, information disclosure, and device tampering. However, the second component also will use the SIoT framework to address the other issues and will propose new methods and mechanisms for handling such challenges as a denial of service. All these threats will be simulated with a CSIoT simulation tool with results, including new security features, compared with those from the older framework version.

Finally, the third component will explore the convergence of SIoT and blockchain technology to understand the transaction of smart property and paid data on the IoT when utilizing peer-to-peer trade based on blockchains and smart contracts. This issue was previously studied (Zhang and Wen, 2017), but the effect of cognition and sociability of IoT devices on blockchain business models was not addressed.

In this component, the study will revise the SIoT framework to replace the exchange of information and services by trade-based and paid data. The agents will represent smart properties and people (buyer-seller). SIoT, and blockchain will be integrated to develop a new IoT e-business protocol.

This new business model will consider important e-business elements, including pre-transaction preparation, negotiation, contract signing, and contract fulfillment. This study hypothesizes that friendship management in CSIoT will improve IoT e-business by facilitating transactions between highly trusted friends. It is also predicted that such a network of friends and friends of friends would make business transactions more secure, more effective, and more efficient. In addition, including cognition and sociability in smart properties would provide high quality data/information with lower costs.

Chapter II: Literature Review

2.1. Complexity science

Complexity science is a multi-disciplinary science that uses several scientific methods to explore complex systems. Complex systems are open systems with many networked components like the environment that interact with each other. Some complex systems involve social systems (e.g., an anti-money laundry system) that have no clear boundaries. Nonlinearities and emergent behaviors are among the common features of complex systems that complexity science aims to explore (McKelvey et al., 2016).

Complexity science has been a major research topic in different disciplines including math, physics, social science, management, and engineering. Cities, organizations, IT networks, IoT, business markets, and our brains are examples of complex systems. In social science, complexity can help to understand organizational transformation and emergent capabilities (Merali and McKelvey, 2006). There are different concepts in complexity science that can describe a complex system's behavior. Some of these concepts can be found in every complex system. This section discusses these concepts.

2.2 Complexity concepts

Complexity science includes a set of concepts that helps explore complex systems such as complex organizations in a network society that has multiple resolution levels. Complex systems in social science generally refer to networked systems. A networked system contains several nodes that interact with each other. These systems are dynamic and uncertain, and they have some nonlinear features (e.g., non-linear relationships). Other features of complex systems are identified in different disciplines such as physics and math. This section reviews a brief description of complexity concepts that will be used in the SIoT framework.

2.2.1 Agents

Agents are problem-solver entities with a self-organizing capability that can respond to forces and change. In a given organization, departments, employees, and networks are agents.

2.2.2 Heterogeneous agents

If agents are similar to each other, they cannot learn new things. However, if agents are different from each other, they can learn new things and be more innovative. This is related to the "strong tie" and "weak tie" effects among agents explained by Granovetter (1973). A "strong tie" effect occurs when agents frequently connect to each other. This effect increases trust and efficiency because it produces agents that look alike. However, a "weak tie" effect occurs when agents do not connect frequently to each other. In a "weak tie" situation, heterogeneous agents can learn new things and thus increase innovation and entrepreneurship. This is because between connections, there is time for agents to change considerably. Therefore, a complex system needs heterogeneous agents, since there are new things to learn in each connection. This is essential for self-organizing. However, if the agents are similar to each other, they cannot create a new order after the first critical value.

2.2.3 Self-organization

In complex systems, agents should have a self-organizing feature so they can change by themselves. There is no "global controller" or something from outside that motivates agents to change (Holland, 1988).

2.2.4 Connections and connectives

Agents in complex systems should be able to connect to each other. There are two different concepts here: there should always be some way for agent connections (e.g., networks); however, agents do not have to be connected to each other all the time or even frequently. As previously discussed (see Section 2.2.2), if the agents connect to each other frequently, they cannot create novelty and innovation.

For example, if two different people in New York City and Washington, DC are two different agents in a complex system, the road between these two cities is the connectivity that should exist all the times. However, these two people do not necessarily need to meet frequently with each other (connections). If they do meet each other frequently, the trust between them would increase. However, in this case, after a while they might not have new things, stories, or experiences to share with each other.

2.2.5 Motives to connect

Agents need motivations to connect and interact with each other. Therefore, motivations are a primary factor for complex systems creation. The next section discusses one of the main motives for agents' interactions.

2.2.6 Motives to survive and grow

Survival and growth are the main motives for agent interactions. In an organization, every employee tries to maintain his job position and possibly improve his position by working harder. In social systems, each individual tries to maintain his social position by avoiding any situation that is worse than the current situation. For example, you never want to lose your current job and get a job that you think is worse in terms of salary or location. This is motivation for survival.

Additionally, you may always want to have a better job with a higher salary and better location. The willingness to improve and to have a better situation is the motivation for growth. According to McKelvey et al. (2016) there are two types of motivations in agents: passive-dependence and innovation-change. For instance, some employees in a company maintain their position and situation for a long time, while others always try to learn and change as well as to be innovative. The first group only has a motive to survive and the second group has a motive to survive and grow.

2.2.7 Coevolution

If two entities are connected to each other, a change in the first entity causes an adaptive change in second entity. Adaptive changes in the second entity cause reciprocal adaptive changes in the first entity. This can continue and might cause a remarkable emergent new order. Environment entities interact with system components and, based on these interactions, positive or negative feedbacks emerges across the system boundary. Negative feedback means that interactions between the environment and system components enhance system stability and help the system to keep its state of reference. On the other hand, positive feedback decreases system stability and directs the system in a way that changes its state of reference. In this way, butterfly events scale up (Mckelvey, 2016).

Suppose there are two departments, accounting and personnel in an organization. If the accounting department changes the financial policies and pay scales, the personnel department must adapt to these changes and might change employment policies, interview strategies or contracts. Subsequently, the accounting department changes to adapt itself to the new changes in the personnel department. This interchange of actions can continue repeatedly and cause the emergence of a new order.

2.2.8 Nonlinearities

Nonlinearity is one of the important concepts in complexity science and complex systems. Positive and negative feedbacks create nonlinearity in complex systems. Small changes or a butterfly event can change the system considerably and cause state transitions. There are many nonlinear distributions in complex systems including social systems. However, scientists and researchers usually consider normal distributions in defining the relationships, frameworks and workflows in social systems. The relationships between agents in a social system are nonlinear because of the tremendous amount of other inter-relationships between agents and the many positive or negative feedback between them.

Suppose there are two connected agents: A_1 and A_2. Each of these agents is connected to many other agents. If A_1 changes, A_2 will change to adapt itself to A_1. At the same time, there might be tens of other adaptive changes forced by other agents. In addition, the environment might also influence any of these agents.

Thus, it is not possible to consider a linear relationship like $f(x) = ax + b$ between A_1 and A_2. Depending on the number of other connected agents, change forces and their strength, positive or negative feedbacks, and the environmental factors, a nonlinear relationship among agents becomes (e.g., $f(cx) = a\ (cx)^{-k}$).

The third phase of complexity science is related to the causes and consequences of nonlinearity in nonlinear things (e.g., complex systems). In examining 1,200 firms, Crawford et al. (2015) demonstrated that normality assumptions on variables such as firm resources, performance, and outcomes are not always true.

2.3. Complexity science and information systems

In 2006, the *Journal of Information Technology* published a special issue on “Using Complexity Science to effect a paradigm shift in Information Systems for the 21st century”. According to

Merali and McKelvey (2006), complexity science had a significant impact of on management, social, and network sciences and, consequently, there was a need for a paradigm shift in the IS discipline. Ten years later, another top IS journal, MISQ, called for papers for its special issue on "Complexity and Information Systems Research in the Emerging Digital World".

Thomas Kuhn (1996) defined this paradigm as universally accepted scientific achievements that lead the research and education in a specific community of practitioners. Obviously, there are outstanding achievements in complexity science throughout different fields, including agent-based modeling, robotics, data mining, e-science, natural science, and social science. They have had a major impact on different components of IS.

However, IS, as a discipline, has not broadly addressed complexity science and complexity theory. According to Merali and McKelvey, complexity science has had a significant impact and can change the IS research paradigm. However, a review of IS literature indicates that this paradigm shift has not occurred.

There are two major research fields in IS: behavioral studies and design science studies. Published literature related to complexity science is mostly sound in the design science field. In behavioral studies, researchers consider complexity as a construct in cognitive models (Thong 1999; Mallat, 2007; Oliveira et al., 2014; Wang et al., 2015). Generally, these studies do not focus on complexity science or complexity theory and do not use complexity concepts discussed in this study. Instead, they focus mostly on the technical concepts of complexity or investigate the adaptive effect of complexity in IS.

There are few qualitative studies like Merali (2006) and Allen & Varga (2006) that focus on complexity science in the IS field. Few studies (e.g., Wessey and Ward 2013; Carter and Weerakkody 2008) have developed new theories in the IS field based on complexity concepts. Wessey and Ward (2013) utilized a coevolution concept to develop a new theory for sustainable IS alignment. Other researchers (e.g., Allen and Varga 2006; Marjanovic and Kecmanovic 2017) conducted case studies to analyze the effect of complexity concepts in different fields. Marjanovic & Kecmanovic (2017) used different complexity concepts like butterfly events and nonlinearities to investigate the emergence of tension in open government IS.

In the design science field several studies considered different concepts of complexity science. Vidgen and Wang (2009) used complexity science concepts, such as coevolution, self-organizing, and emergence, to develop a new framework for agile software development. Some studies similar to a study by Nan (2011) focused on complex adaptive systems (CAS) and they used some complexity concepts. Nan developed a theoretical framework and an analytical tool for CAS by considering bottom-up IT use and agents.

The dearth of literature suggests that there is considerable space in IS research for using complexity science. More complexity concepts can be used in system development, system analysis, application development, behavioral and qualitative studies in the IS field. The number of complex information systems is also on the rise. Information system researchers can consider complexity science for designing, managing, operating, and maintaining complex systems. According to Merali (2006), the network society, the network economy, and the increasing number of complex systems require a paradigm shift in IS research. Even 12 years since Merali's publication, this shift has not yet occurred. More studies are needed to address this issue in IS discipline.

2.4. Internet of Things (IoT)

IoT is a set of smart objects that are connected via networks and smart sensors to achieve different goals. In IoT settings, different objects or things are integrated wirelessly with smart sensors to perform different tasks in healthcare, transportation, etc. IoT technology aims to connect everyday devices like cell phones, cameras, cars, and home appliances to each other online.

Everyday devices like cell phones have specific capabilities. By connecting and integrating different devices in IoT, new capabilities can be created. IoT technology is growing fast, and, according to Gartner (2016), the number of IoT devices will reach over 30 billion in 2020. This section discusses the major research challenges and opportunities in the IoT arena.

Recently, IoT has attracted the attention of researchers around the world. There are many issues in IoT development that need to be addressed, including infrastructure, standards, wireless connectivity, mobile computing, cold computing, architecture, and business models that are trending IoT research topics. This dissertation focuses on SIoT, CIoT, security IoT, and healthcare IoT. The following sections discuss the research backgrounds for these topics.

2.4.1. Research trends in IoT

Whitemore et al. (2015) conducted a literature review in IoT based on six categories: technology, applications, challenges, business models, future directions, and survey articles. The technology category has three parts: hardware, software, and architecture. Studies about the IoT applications are mostly conducted in the areas of smart infrastructure, healthcare, supply chain/logistics, and social applications. Whitemore et al. (2015) listed four challenges in IoT research: security, privacy, legal/accountability, and general challenges. The authors found that most studies concerned the technological aspects of IoT.

In a survey article, Li et al. (2015) performed a literature review based on service-oriented IoT architecture and enabling technologies. This architecture includes four different layers: sensing layer, network layer, service layer, and interface layer. In the sensing layers, sensors exchange data among IoT devices. Cost, size, and energy consumption of sensors are challenging issues in this layer, while other issues involving deployment, heterogeneity, communication, and network structure have been investigated in IoT studies. In the network layer, there are several research issues including: network management technologies, energy efficiency, quality of service (QoS), mining and searching technologies, signal processing, security, and privacy. The service layer has research issues, such as service discovery, service composition, trustworthiness, and service APIs. Finally, in the interface layer, the compatibility issue among different things is an important topic of research.

There are many research issues in the IoT area. Although this study is interested in IoT issues that are popular and have attracted the attention of many researchers in different disciplines, this study specifically focuses only on security, privacy, and the application of IoT in healthcare. A literature review of these topics is discussed in the next section.

2.4.2. IoT security

Security and privacy are two important challenges for IoT (Li et al., 2015). There are many activities in IoT, such as personal activities, business processes, and information exchange that need effective security and privacy mechanisms. Several potential threats like radio frequency identification (RFID) tags attacks and data leakage require security standards, protocols, and tools. Li et al. (2015) summarized IoT issues in privacy and security as four major topics: resilience to attack, data authentication, access control, and client privacy.

Generally, IoT devices connect to each other through wireless networks. The common method for securing the wireless network is encryption. In IoT settings, many devices do not have a powerful ability to support appropriate encryption (Whitemore et al., 2015). According to Yan and Wen (2012), more efficient encryption and key distribution methods and algorithms should be developed to support IoT security. Yan & Wen (2012) proposed a new key management protocol based on a trusted third-party to enhance security in tag, reader, and server in mobile RFID.

According to Roman et al. (2011), identity management and the development of effective identifiers for IoT devices is another important challenge. IoT settings need effective identifiers to recognize personal identities, objects, and illegal activities.

Sicaria et al. (2015) performed a survey on IoT security and identified eight key issues in this area: authentication, access control, privacy, policy enforcement, trust, mobile security, secure middleware, and confidentiality. They held that IoT settings need a unified framework for assuring security and privacy among different devices with different communication standards and different technologies.

The important question is why normal Internet security methods and advanced mechanisms cannot be applied in IoT. According to Trappe et al. (2015), IoT devices have limitations such as battery capacity and computing power. Many everyday devices like smoke detectors or home appliances do not have high computing power and battery capacity.

According to Yang et al. (2017), there are three methods to overcome the battery capacity issue. First, battery capacity can be increased in devices. However, most everyday devices are lightweight and small shapes. The second approach is to provide energy from natural resources, but this can be very costly.

In addition to battery capacity, most everyday devices have a low computation power. Therefore, advanced cryptography and encryption algorithms cannot be applied in IoT devices because most everyday devices have memory and computing capabilities that are too low. Third, applying minimum security requirements on devices is not a satisfactory method to protect sensitive data. In addressing this issue, Trappe et al. (2015) suggested applying signal processing at the receiver side in physical layer authentication for transmission verification.

Riahi et al. (2014) proposed a cognitive model for investigating IoT's security issues. This model consisted of four actors or nodes, including a person, process, technological ecosystem, and intelligent object. On the person side, security standards and compliance strategies were required. The process side encompassed risk management, strategy, security controls, monitoring, and updating. In the technological ecosystem there were five key elements: security design and configuration, identification and authorization, enclave internal, enclave boundary, and physical environmental. The authors described these complex and dynamic interactions between these nodes as tensions. The possible tensions between the nodes were listed as privacy, trust, identification, reliability, safety, responsibility, and self-immunity.

By analyzing the IoT security literature, research studies can be categorized from three different perspectives. Table 1 summarizes important research topics based on different perspectives.

Table 1. IoT security research perspectives

IoT Security Research perspectives			
IoT Actors and interactions among them	**IoT architecture**	**Features of IoT components**	**Context of IoT application**
Among IoT devices and objects	Service oriented	Battery capacity of devices	Healthcare
Among people, IoT devices, and objects	Man-Like Neural network (MLN)	Low computing power	Smart cities
Among environment, IoT devices, and objects	Social organizational Framework (SOM)	Cognitive computing	Transportation

The four key perspectives of IoT security are: interactions among different actors, architecture, IoT component features, and the context of IoT application. For each perspective, there are three examples provided in Table 1. Each of these perspectives has different requirements for security and privacy. For instance, developing a new architecture creates new security and privacy requirements, and different application contexts have different security and privacy requirements.

2.5. Cognitive IoT

Suppose that you are cooking chicken by boiling it in a container. After a few minutes, you leave home and forget to turn off the oven. If some home devices have cognition, they can "understand" that you left home without turning off the oven and the home might be in danger of fire. If the oven, door, container, and your cell phone are connected to each other and have cognition, problems like this will be addressed.

Cognitive IoT is a new area of IoT research that is about utilizing cognitive computing technologies for processing data gathered from IoT devices to create cognition in IoT devices (Matthews, 2016). The goal of this dissertation is similar to the cognitive IoT's objective to develop human-like IoT devices that can think or interact like humans. According to Matthews, cognition encompasses three capabilities: understanding, reasoning and learning. Therefore, the main goal of cognitive IoT is to enable IoT devices to understand, reason, learn, and interact with humans in an effective way.

According to Wu et al. (2014), cognitive IoT follows a context-aware, perception-action cycle in which IoT devices can learn from the physical environment and social network. IoT devices can store the semantics and knowledge in databases, adapt themselves to changes, and take appropriate decisions and actions. Wu et al. proposed a cognitive IoT framework that enables IoT devices to learn, think, and understand the physical and social world. Their framework consisted of a sensing control layer, a data-semantic-knowledge layer, a decision making layer, and service evaluation layers. These layers comprise the cognitive process in IoT devices.

For data analytics in cognitive IoT, Wu et al. suggested different methods such as heterogeneous data processing, non-linear data processing, high-dimensional data processing and parallel, and distributed data processing. For semantic derivation and knowledge discovery in cognitive IoT, they discussed different methods including context, ontology, standardization, association analysis, clustering analysis, and outlier analysis. They also proposed a framework for intelligent decision-making that can perform "selecting" in IoT settings. Finally, the authors proposed performance metrics for cognitive IoT that included profit dimension, cost dimension and computational efficiency.

It is important here to stress that cognitive IoT is not artificial intelligence (AI). However, it is possible to utilize AI to develop and improve cognitive IoT. According to Pramanik et al. (2018), using AI in IoT has several advantages, including enhancing user experience, automatically learning the patterns and behavior of system, and anomaly and conflict detection. Pramatik et al. (2018) cited several features of cognitive IoT, such as self-learning, probabilistic, adaptive, flexible, dynamic, interactive, iterative, stateful, highly integrated, scalable, context and situation awareness, and self-management.

2.6. Social IoT (SIoT)

Currently, researchers in the IoT field seek two important objectives. They aim to explore potential functions that IoT devices can perform, and they try to develop more effective models of IoT that can serve the complex and networked human society (Aztori et al., 2014). IoT encompasses many objects in a complex setting. This complexity can create many opportunities as well as many threats. In terms of complexity, IoT is like complex social systems in having a number of smart objects and a networked system.

In social and biological systems, humans and animals address the complexity of social systems and manage potential opportunities and threats. Therefore, the concepts of social systems can be used to develop the same capabilities in IoT devices. The emergence of a new generation of IoT as cognitive IoT will make the IoT objects more human-like. Therefore, to manage emergent opportunities and threats in complex IoT settings, it is necessary to develop and improve new IoT models that use networked social system concepts. In SIoT, objects can interact with each other autonomously, discover services and information in complex IoT environments, and provide services and information to other objects.

According to Aztori et al. (2014), SIoT is the future generation of IoT that can create many capabilities such as object discovery functionalities, evaluation of trustworthiness of objects and their provided information, and deployment of value-added services. The authors believed that defining inter-object relationships is an important open research issue in SIoT. The authors proposed four features of SIoT: First, find server providers, Second, publish information, Third, evaluate trustworthiness, and forth, get filtered information. Finding server providers is about the ability to crawl networks of friends to find other objects that can offer useful services. Publishing information concerns the capability of publishing information through friendship paths and limiting the message exchanges for optimized consumption. Evaluating trustworthiness deals with the trustworthiness of services and information provided by other objects. Getting filtered information is about collaboration of a community of objects having a common view to improve the accuracy of information.

The relationships between objects are defined when developing SIoT. After coding these relationships, an effective SIoT architecture is developed before analyzing SIoT's social network structure. Aztori (2012) used several social network concepts and relationship types to define and coding the relationships between objects in SIoT. A parental object relationship (POR) is for objects that are created in the same period by the same producer. A colocation object relationship (C-LOR) is for objects that are in same location (e.g., smart home), while co-work object relationship (C-WOR) is for objects that work together to provide an IoT application. Finally, a social object relationship (SOR) is for objects that continuously or occasionally are in contact with each other because their owners are contacting each other. The authors developed a SIoT structure that contained three layers including sensing, network and application. According to the authors, the main components of SIoT, such as relationship management, service discovery, service composition, and trustworthiness management, are contained in the application layer.

Relationship management deals with a friendship between objects. Smart objects cannot manage friendships like humans. Therefore, RM can be used to make objects able to update, start, or end a friendship. Objects can use the service discovery (SD) component to find other objects that can provide needed information or services. Service composition (SC) applies to enabling interactions between objects. Finally, TM or trustworthy management is for evaluating the information and services provided by other objects. The reliability factor depends on the objects' friendship managed by RM.

IoT devices should be socialized to interact easily with humans. SIoT is able to increase the sociality/connectivity and pervasiveness/availability of IoT systems (Ortiz et al., 2015). According to Ortiz et al. (2015) there are several research issues concerning SIoT: interactivity, collaboration, and handled-data. Interactivity is about interactions between objects or interactions between humans and objects. Most SIoT studies consider only one type of interaction. Collaborative perspective relates to the collaboration of all types of SIoT components, especially human-object collaboration to increase QoS of quality of service. Finally, handled-data concerns using different data acquisition and processing techniques in SIoT.

According to Ortiz et al. (2015), social role, intelligence, and socialized devices are key features of the SIoT paradigm. The social role uses social network concepts and basics to develop a social structure in IoT objects. Intelligence is defined as the decision-making tools and methods that enable IoT objects to understand each other’s services or manage their friendships. Finally, socialized objects can interact and talk and communicate with humans or other objects.

Kasnesis et al. (2017) proposed two SIoT ontologies for addressing interoperability issues in objects’ interactions. Social smart object relationships (SSOR-Ont) defines relationships between objects and managing friendships. This ontology contains five classes for a *socialfriend* entity that is based on the relationship types proposed by Aztori et al. (2012).

The second ontology, a smart object’s need and service (SONS-Ont), is for determining the requirements and types of agents and the services provided by smart objects. The authors used three types of cognitive agents in a multi-agent system (MAS). The first type of agent was a device agent to represent smart objects and IoT devices. The second was a human agent to humans, and the last one was a task agent to represent applications.

Kasnesis et al. (2017) also integrated cognitive and social aspects in IoT objects by considering friendship management and goal management mechanisms. Friendship management is a smart component that considers trust, quality of data (QoD), quality of information (QoI), and network structure. Goal management is a smart component that includes SD, service orchestration (SO), and service binding (SB).

Table 2 summarizes the SIoT key issues in the literature.

Table 2. SIoT features

SIoT features	Description	Solution
Defining relationships between smart objects	SIoT consists of social objects and these objects should be able to interact with each other, make friendships, terminate friendships and update friendships.	Using concepts of different types of relationships from social networks (e.g., POR) and using ontology.
Trustworthiness	Social objects should be able to evaluate the information and services provided by other objects.	Using friendship management and evaluating service or data based on friendship, QoD, QoI, and network structure.
Collaboration	In SIoT there should be two types of interactions: object-object and human-object. All the actors should be able to collaborate with each other to achieve certain goals. Objects should be able to make relationships with humans.	Integration of cognition and sociability in IoT devices. Goal management mechanism.
Discovery	A social object should be able to discover needed information and service from other objects. A social object also should be able to advertise its presence and the information and services it can provide to the other objects.	Service discovery methods like flooding techniques and Global Sensor networks (GSN) or ontology-based methods.

2.6. Smart city

Because of the rising economy and social transformation, many people move from the country to cities. The urban population is expected to reach five billion by 2013. This will be about 60 percent of the world's population (Neirotti et al., 2014). Unfortunately, cities do not have the fundamental infrastructure and policies to accommodate this large population. Additionally, the rapidly growing population will have a negative impact on climate, the environment, and energy. To address this problem, it will be necessary to develop governance and service delivery and to provide swift, seamless mobility, easy access to public facilities, affordable housing, quality healthcare and education (Zhang et al., 2017). Innovative management of urban operations and various smart services would be required to mitigate developing problems in modern cities.

The main goal of a smart city paradigm is to develop a variety of value-added services to address the problems of urbanization. Smart city solutions involve intelligent services and a comfortable life for local residents through flourishing technologies, including IoT, cyber-physical systems, big data analysis, and real time control (Zanella et al., 2014). Smart city technology also integrates heterogeneous network structures and ubiquitous sensing components to track the physical changes in cities and provides feedback to different computing systems and authorities. The smart city market is expected to reach over $1.2 trillion by 2020 (Neirotti et al., 2014). A typical architecture for a smart city system, includes three main components: the physical world, the communication world, and the information world (Zhang et al., 2017).

Like any advanced technology, the smart city paradigm creates new challenges and problems. A main challenge for smart cities includes a series of security and privacy problems and vulnerabilities. Malicious hackers might disrupt sensing information, which can affect decisions, services, and control in smart cities. They can also conduct other attacks such as a denial of services to decrease the quality of intelligent services in smart cities.

Zhang et al. (2017) discussed the main privacy challenges facing smart cities, including privacy leakage in data sensing, privacy and availability in data storage and processing, and trustworthy and dependable control.

Khatoun and Zeadally (2017) investigated the main cybersecurity vulnerabilities for smart cities. Software products with security vulnerabilities, sophisticated attacks, legislation and complexity are among the main security vulnerabilities for smart cities. These vulnerabilities might cause such problems as software design and bugs, configuration errors, privacy, and scalability with an increase in city size.

Zonnen (2016) discussed three dimensions concerning people's privacy concerns in smart cities that are significant in addressing privacy issues. According to the "kinds of data" factor, people have different conceptions about the sensitivity of different types of data. For instance, people usually think that medical, financial, and civic data are highly sensitive, but that nationality, gender, or age data are not very sensitive. Concerns over the purpose of data means that people often assume there is a tradeoff between the amount of sensitive information sharing and the benefits they receive. There is also a privacy concern over who is collecting the data. People trust some companies to handle their personal data more than others. For example, according to the

Eurobarometer data (Eurobarometer, 2011), people trust banks and medical organizations more than other organizations when it comes to their sensitive data.

Presently, it appears there is no study addressing privacy issues in the social internet of things.

2.7. Research gaps

The motivation for this research is based on several research gaps in the literature. This section discusses the main issues that this study aims to address. Research gaps are found in such areas as system thinking and complexity science in IS, SIoT architecture and concepts, integration of SIoT and cognitive IoT, SIoT security, and SIoT applications in healthcare and e-business.

Figure 1 depicts the dissertation's research focus areas.

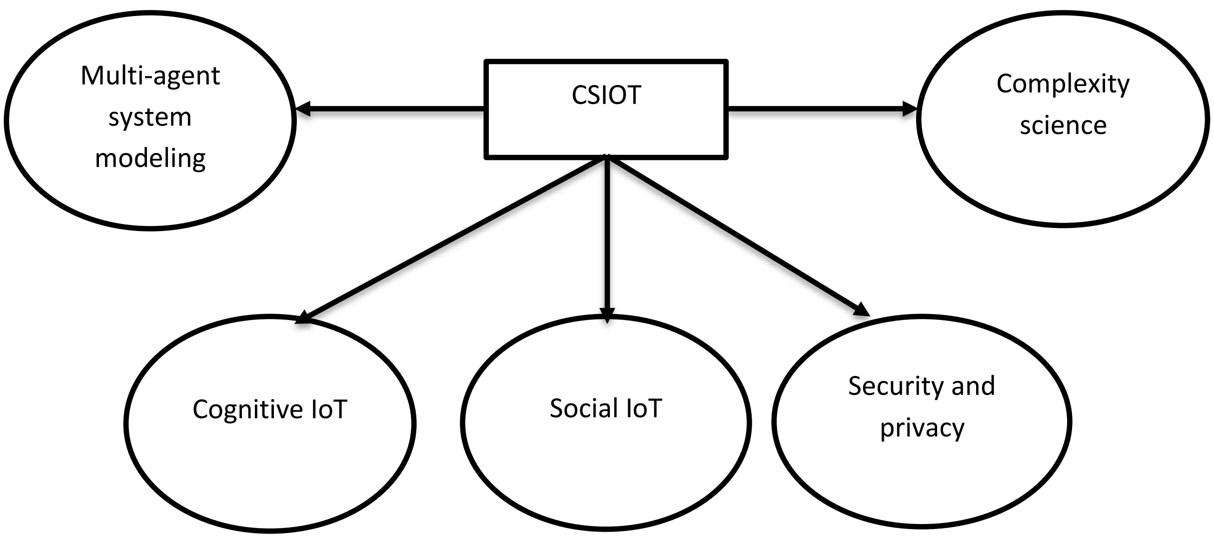


Figure 1. Major research areas addressed in this study

In 2006 and 2016, two major IS journals, MISQ and JIT, called for papers on research that used the complexity science lens in studying information systems (Merali and McKelvey, 2006). Addressing the problems of socio-technical systems is a vital part of IS research since the number of complex and networked social and technological systems is quickly growing. These calls for papers highlighted the relevance of considering complexity science and complexity concepts in IS research and the related need for new research.

A review of the IS literature indicates that a number of research projects study different aspects of various systems that are complex in nature, but these works either fail to use complexity concepts or neglect most of them.

A paradigm shift in IS literature has not yet occurred, even though complexity science can change all aspects of IS research, including design science, behavioral studies, qualitative studies, quantitative studies, and case studies. There is a need for more research that considers complexity issues in the philosophy of IS, problem solving and system development.

According to several studies, SIoT is the future generation of IoT (Aztori et al., 2012; Kasnesis et al., 2017, Goad & Gal, 2017). There are interesting studies on developing SIoT structure and investigating challenges and issues (Khan et al., 2017). However, there are several issues still to be addressed or improved in SIoT, such as integration of cognition and scalability in smart objects, defining relationships between smart objects, analysis of the graph of relationship structure, and definition of applicable architectural modules (Aztori et al., 2014; Kasnesis et al., 2017, Goad and Gal, 2017).

In SIoT security there are several open research issues such as the vulnerability of trust management schemas, limited resources, scalable trust management protocols, development of trust in social relationships, privacy of object owner, SD, and QoS (Khan et al., 2017).

Friendship updating or friendship leveraging in SIoT is not investigated enough in the literature. For instance, Aztori et al. (2012) proposed a SIoT architecture and in this architecture the only factor considered for leveraging friendship between devices was trustworthiness, which is determined by network centrality and prestige. These factors can be important, but there are other factors (e.g., QoI) that are as important in leveraging friendship. Additionally, the authors did not consider time in this process. Suppose that a device has a high trustworthiness at a certain point of time t_1, but a low trustworthiness in t_2. The study did not present an effective mechanism to monitor variations of trustworthiness over time or leveraging friendships based on time.

Kasnesis et al. (2017) considered different factors like QoI, QoD and network structure for leveraging different devices. They divided devices into low importance, medium importance, and high-importance categories, based on a game theory approach. However, they did not actually leverage friend devices and just used this leveraging process in friend selection, friendship termination and accepting friendship request. In other words, they only leveraged the importance of non-friend devices. Additionally, they did not provide a mechanism for considering time and utilizing friendship levels in SoIT. The importance level in friends is not subjected to update in their study.

The literature review demonstrates that IoT has drawn the attention of IS researchers in recent years. There were different research studies that investigated different aspects in IoT. However, this research topic is new in IS literature and more research studies are needed in IS literature to further address IoT issues.

Chapter III Design artifact

This study introduces CSIoT as a new framework for SIoT and then evaluates and simulates CSIoT using a new simulation tool developed particularly for this study. This study proposes a new framework for a blockchain-based SIoT by integrating CSIoT and blockchain concepts to address CSIoT security and privacy issues.

The research methodology for this study is based on design science. Design science in the IS field is a research methodology for designing artifacts based on kernel theories. Therefore, this study is not solely technical or solely practical. Rather, it uses both theoretical and technical concepts for conducting the research.

The study explains the different components of CSIoT, the proposed the new SIoT framework, including the cognition, service, and social modules as well as the fuzzy ontology which manages the relationships, services and devices. The study uses a fuzzy concept because the relationships between smart objects are non-linear and uncertain and they depend on a variety of factors. The major contribution of this study lies in the social module that includes the new friendship development and a friendship update mechanism. The service module is responsible for managing the services exchanged between devices. The methods and sub-components in the cognitive module are designed based on previous studies and are integrated with social and service components.

3.1. Methodology: Deign science

Design science aims to describe how things can be used to satisfy a desire or a goal. Artifacts follow natural rules and are not separated from the natural world. The difference between artificial and natural things is that the former satisfy our desires and goals. Therefore, the main aim of the natural science is to explain how things are and the main aim of design science is to explain how things ought to be in order to attain goals.

According to Hevner et al. (2004), natural science is about truth, while design (artificial) science is about utility. Hevner et al. (2004) believed that IT artifacts can include constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems). Therefore, design science can be defined as a problem-solving paradigm that aims to create and evaluate IT artifacts for solving organizational and business problems.

Hevner et al. (2004) also stated that an effective transition between strategy and infrastructure needs effective design activities. It is important to consider that design is both a process (set of activities) and a product (artifact). Based on the Hevner et al. article, design science explains the world as both acted upon (processes) and sensed (artifacts). This is a platonic view of design that is a basis for a problem-solving paradigm that frequently changes aspects between design processes and designed artifacts for the same complex problem.

This study takes a design science approach, as explained by Gregor and Jones (2007), to develop a new SIoT framework based on complexity concepts and to investigate the proposed framework in the contexts of security, healthcare, and e-business. Gregor and Jones (2007) stated that IS design theory consists of eight components including purpose and scope, justificatory knowledge, principles of form and function, constructs, principles of implementation, testable propositions, expository instantiation, and artifact mutability. This study will follow guidelines established by Hevner et al. (2004) for conducting design science research in the IS field. In this study, the artifact is a novel SIoT framework developed based on complexity science concepts and a new model of friendship. All the other design science components will be addressed in different parts of this dissertation. Table 3 matches the design science components with different parts of this dissertation.

Table 3. Design science guidelines

Dissertation sections	**Design science guidelines**
CSIoT framework	Design as an artifact
Implementation and simulation	Problem relevance
Evaluation (Simulation)	Design evaluation
Discussion and future work	Research contributions
CSIoT frame work and evaluation	Research rigor
Literature review	Design as a search process
Discussion and future work	Communication of research

For the design as a search process, we have done a literature review in different research areas including: IoT, SIoT, friendship development in social networks, IoT security, IoT privacy, and blockchain. The research gaps mentioned earlier are found after literature review and they were the main motivation for designing new artifacts.

Different sections in this dissertation addresses the research communication. Introduction, conclusion and other section in this research aim to introduce main gaps, provide the research questions and research objectives, and show the results of the research, the main contributions and the future works.

The research rigor is considered in introducing the new framework for SIoT and developing a new simulation tool for evaluation of the framework.

The research contributions are clearly mentioned in the conclusion section. The contributions of this research are listed below:

- We proposed a new friendship development model in the social internet of things.
- We developed a new friendship update mechanism in the social internet of things.
- We designed a new simulation tool using multi-agent system modelling and Cytoscape.
- The proposed models performed effectively in the social internet of things network.

The problem relevance and the design evaluation are considered in literature review and the simulation sections of this study. According to Hevner et al., 2004, the simulation method is a valid method for evaluating the artifact when the actual data is not available. The CSIoT framework is for the future generation of IoT. Thus the actual data is not available yet for SIoT or CSIoT environment.

The main artifact of this design science research is the CSIoT framework. There are different modules in CSIoT namely: friendship module, service module and the cognitive module. The main contribution of this research is in friendship module. The list of artifacts is provided as follows:

1) CSIoT framework

-New friendship development model

-New Friendship leveraging method

-Fuzzy ontology

2) New simulation tool

3) Experimental framework for blockchain-based CSIoT

3.2. Design artifact

There are two important relationships in SIoT: object-object and object-human relationships. CSIoT devices are social and cognitive meaning they can start, update, and terminate friendships and they also have learning, reasoning, and understanding capabilities. Figure 2 demonstrates the relationship types in the proposed framework.

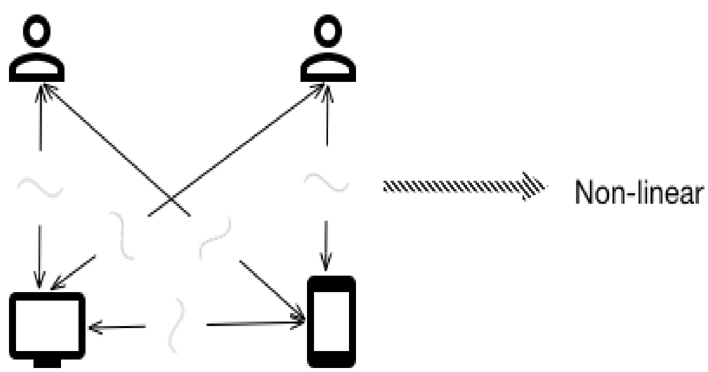


Figure 2. Relationship types

The important factor in developing a SIoT architecture is to define the relationships and interactions between objects. Before coding the relationships, this study discusses the different concepts of complexity science that are applied in CSIoT. This study considers SIoT as a complex system and therefore defines the relationships that are based on complexity. Some complexity concepts, such as the first critical value and tension, can be traced and investigated in simulation. Non-linearity and agent concepts are used to define relationships.

3.2.2. Complexity concepts in CSIoT

In CSIoT, agent modeling is performed and the concept of an agent is defined as a software entity that performs the application functionalities of each object. CSIoT deploys a multi-agent system that encompasses several interactions between social-cognitive entities. This study uses a variety of agents including human agents, device agents and task agents. These agents represent humans, IoT devices, and applications, respectively. The agents are heterogeneous and can learn new things. Figure 3 shows the three types of agents.

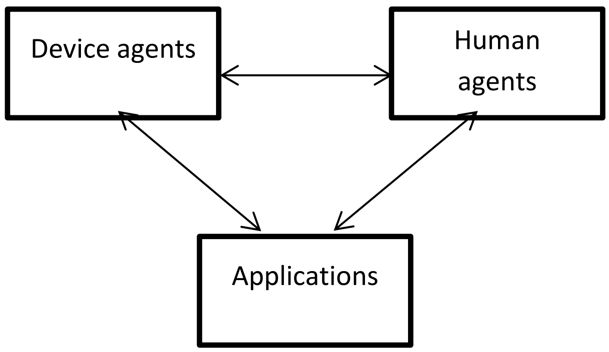


Figure 3. Agent types

Agents can change and update themselves and have a self-organizing feature. Therefore, cognitive objects can learn, understand, and reason. This cognition increases the self-organization level in CSIoT objects.

In CSIoT, objects (agents) connect through a cloud network. In terms of connectivity, they do not have to interact with each other all the time and or even frequently. According to their weak tie effect, these objects can learn more and evolve over the time. If they are made to always interact with each other (strong tie effect), they would not be able to learn many new things. Therefore, the policy here is that there is always a connection path through cloud but objects do not have to interact with each other all the time or frequently.

There are two important motives to connect for SIoT agents. First, they want to connect because they want to advertise their presence and the information or services that they can provide to other objects. Second, they want to connect because they want to receive needed information and services from other objects.

This concept of complexity science exists in social-cognitive objects because the agents can start, update, and terminate friendships based on their needs. For instance, if the QoI of an object is low, or this object has trust issues, the other interacting object can terminate the friendship. In another case, objects can learn from different experiences to improve their connections. These factors demonstrate that social-cognitive objects have a motivation to survive and grow.

There is no global controller for upward and downward influences in CSIoT. Nothing will block or control the influences because objects can create innovative structures and useful ideas.

Coevolution exists in CSIoT objects (agents). Since they have cognition, the change in one object will cause a change in other interacting objects. For instance, if there are two friend objects, the friendship update in one object will cause a friendship update in the other object.

All the relationships in CSIoT are nonlinear. This non-linearity in relationships can cause non-linear outcomes and should definitely be considered in CSIoT strategies and policies.

3.3. High level concept of Complex Social Internet of Things (CSIoT) framework

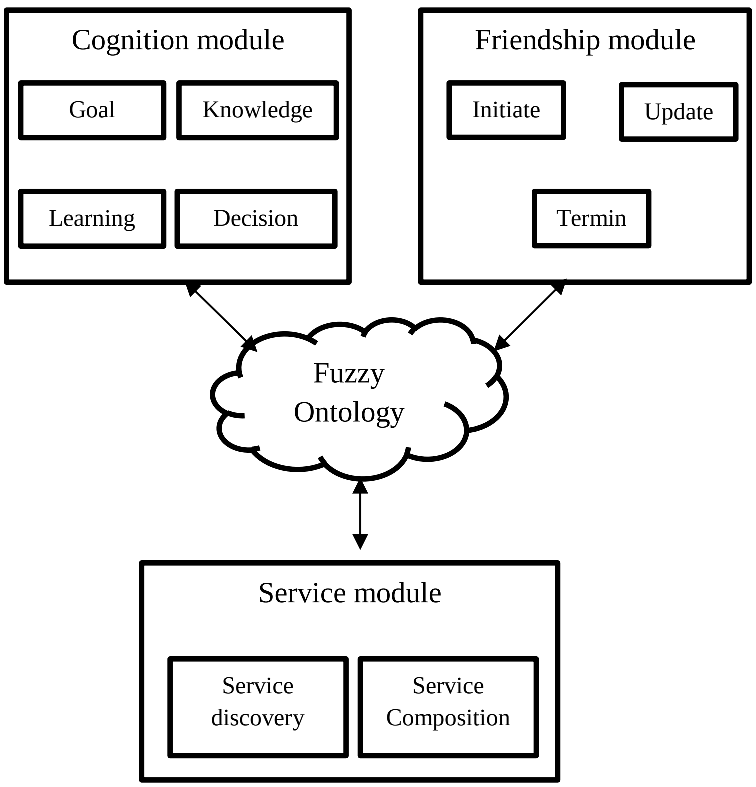


Figure 4. CSIoT framework

Figure 4 shows the CSIoT framework. The description of CSIoT components is provided below.

3.3.1 Fuzzy ontology

This study extends the relationship types that Atzori et al. (2011) used in their SIoT structure: parental object relationship (POR), colocation object relationship (COR), co-work object relationship (CWR) and ownership object relationship. The difference between relationships here and the relationships espoused by Atzori et al. (2011) is that in this current study, all relationships are non linear. To define non-linear relationships, this study uses fuzzy ontology, which can be defined as a set of five elements (Calegari et al., 2007):

$O_f = \{I, C, R, F, A\}$

where *I* is the set of individuals, *C* is the set of concepts, *R* is the set of relationships, *F* is the set of fuzzy relationships, and *A* is the set of axioms. Fuzzy ontology can be developed using Web Ontology Language (OWL) and generated by Protégé (Morente-Molinera 2016) to help add non-linearity and uncertainty to relationships.

3.3.2 Cognition module

Goal management (GM): Kasnesis et al. (2017) integrated cognitive and social aspects in IoT objects by considering friendship management and GM mechanisms. Friendship management is a smart component that considers trust, QoD, QoI, and network structure. Goal management is also a smart component that includes SD, SO, and SB. This research uses GM in the cognition module. In CSIoT, the GM mechanism is located in service management component.

3.3.3 Decision making

The decision-making component uses the knowledge and semantics from the knowledge discovery component for reasoning, understanding, and learning better. Because this study considers SIoT as a complex system, it applies uncertainty and non-linearity in decision making. That is why this research will use one of the fuzzy decision trees, such as fuzzy ID3 proposed by Mitra et al. (2002).

3.3.4 Knowledge discovery

This study will use the semantic derivation and knowledge discovery framework proposed by Wu et al. (2014) for the knowledge discovery component. This framework has two parts: semantic derivation and knowledge discovery. The semantic derivation has three elements (context, ontology and standardization), while the knowledge discovery part has three elements (association analysis, clustering analysis and outlier analysis). This component makes objects able to derive semantics from data analysis and discover patterns or rules as knowledge for decision-making.

3.3.5 Learning

This study will use supervised cooperative machine learning algorithms to assist agents with learning. This is the most important part of the cognition module. The sparse cooperative Q-learning algorithm (KOK & Vlassis, 2004) is designed for cooperative multi-agent systems and is used for agent learning. Q-learning refers to a learning method that is model-free and includes reinforcement learning techniques.

3.3.6 Friendship module

3.3.6.1 Friendship evolution factors

The friendship evolution has been studied in multiple disciplines, including social science, psychology, and communication. There are two important questions here that are important for understanding friendship networks:

1. What are the main factors in friend selection?

2. What are the main reasons for friendship evolution and maintenance of the relationship?

The SIoT paradigm applies social network concepts in IoT settings to create new capabilities and manage problems such as network navigability. One of the vital factors in social networks is friendship evolution. In SIoT literature, researchers proposed new methods to develop human-like capabilities (e.g., socialization and cognition) in connected devices (objects). Therefore, friendship management is important in SIoT architecture. Objects should be able to start, update and terminate relationships with other objects.

In SIoT literature there are different mechanisms for friendship management based on pre-defined and independent relationships that objects can establish in IoT settings. In this study, the focus is on the mixture of factors that can start and maintain friendship between objects. This study investigates the main friendship evolution factors in SIoT to use these factors in friendship selection and updating or terminating friendship.

Four important factors for friendship evolution, including physical proximity, similarity, reciprocity and competence, are proposed to be used in friendship management to provide a broader view in the friendship process. The main idea here is that instead of having pre-defined and independent relationship types, object socialization can be managed by investigating the main causes for friendship and socialization. Additionally, this study investigates the role of these factors in maintaining and updating friendship in SIoT.

Friendship in CSIoT consists of three procedures: friendship initiation, friendship update and friendship termination. Figure 5 illustrates these three procedures in CSIoT friendship management. In friendship initiation, any device D_i can send a friendship request to device D_j based on certain criteria (e.g., proximity). In a friendship update, two friend devices can increase or decrease the friendship level based on certain factors (e.g., competence). And finally, two friend devices can terminate their friendship.

Figure 5. Friendship procedures

The description of friendship evolution factors is explained below.

Proximity

Proximity is identified in a number of studies as an important factor for friendship development among humans (Schutte & Light, 1978; Sias & Cahill, 1997; Clark & Pataki). The basic idea here is that we choose our friends mostly from people who are physically near us. Physical proximity makes interactions among people easy. Frequent interactions in same environment (e.g., workplace, gym, and school) increases the chance of friendship.

Proximity is also an important factor of friendship development within social networks. According to Backstrom et al. (2010), physical proximity makes people to interact more in Facebook. In a review article, Rivera et al. (2010) held that proximity had a high impact on people's attachment and friendship development in social networks.

Physical proximity is used as a colocation relationship, which is one of the device friendship factors in SIoT (Aztori et al., 2012; Kasnesis et al., 2017). In the SIoT framework developed by Aztori et al., a colocation relationship is one of the relationship types that devices can establish within close distances. The proximity here can be defined as in one room, a smart home or even a smart city. Indeed, some devices in the same area might not interact with each other, but physical proximity is a useful factor for friendship selection and creating short links in networks. In CSIoT, physical proximity is one of the factors that can initiate friendships.

Similarity

Similarity is another key factors in friend selection and initiating relationships among people. Several articles (Kandel 1978; Klepper et al., 2010; Aboud & Mendelson 1996) indicate that similarity eases mutual understanding and it can attract and attach people to each other. Having similar cars, jobs, personalities, interests, and other factors can initiate a relationship among people in social networks. Obviously, not all the people with similar factors become friends but similarity is a good starting point for relationships.

The similarity concept in SIoT literature is referred to as a parental object relationship, an ownership object relationship, a colocation object relationship or a co-work object relationship. In other words, objects with the same production company, same owner, similar location and same applications can establish friendships in CSIoT.

The maximum score for similarity can be 5. The method for assigning similarity score is defined as follows.

If two devices have similar owner, then similarity score = 5

If two devices produced in same company, then similarity score = 3

If two devices have same applications, then similarity score = 4

If two devices have similar batch numbers, then similarity score = 3

If two devices are physically close to each other, then similarity score = 2

If two devices are produced in same company but the difference in production date is more than 10 years, then similarity score = 1

Reciprocity

Reciprocity is a well-established factor for initiating or continuing friendships. Reciprocity is defined as a tendency to reciprocate a relationship. According to Selfhout et al. (2010), reciprocity significantly increases friendship selection. In addition, reciprocity is important in friendship influence and in continuing or maintaining the relationship (Leider et al., 2009).

In SIoT literature, reciprocity is part of friendship initiation. A device sends a friendship request to other devices. If the request is accepted by a device, that device will be added to a friend list. However, the role of reciprocity in friendship influence and updating friendship in SIoT friendship management has not been studied in SIoT literature.

Competence

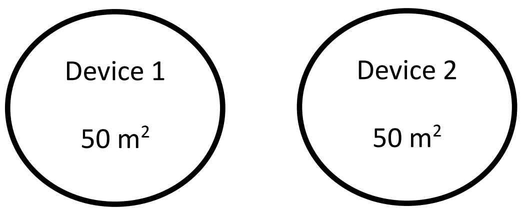
There are different definitions for social competence, but the term generally refers to effectiveness in social interactions (Rose-Krasnor 2006). Competence also can be defined as having a set of skills (e.g., communication, problem solving, and cognition) to manage everyday life. Several research studies demonstrated that people have a high tendency to be friends with socially skilled people. Therefore, competence is very important when initiating and maintaining the friendship (Pinquart & Sörensen 2000; Cause 1986; Buhmester 1998).

In SIoT literature, competence is not considered as one of the factors important to friend selection or friendship updates. Rather, SIoT studies have applied varying factors for leveraging and updating friendship. Aztori et al. (2012) uses trustworthiness to leverage friendship in SIoT, while Kasnesis et al. (2017) use QoD and QoI to leverage SIoT friendship.

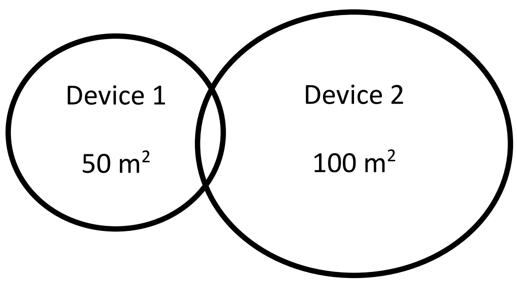
3.3.6.2 Friendship evolution factors in CSIoT

Proximity

Physical proximity in CSIoT is one of the friendship initiation factors. Similar to colocation friendship in SIoT, objects can select friends located within close distances. The locality (L) can be set by user preferences and context. A room, home or even city can be considered as a locality factor. The user (device owner) can set the locality to any range, considering the device's technology and context. Obviously, the locality for a smart home is different from a smart city. In other words, for a device, a close distance range or locality (L) area could be 100 m^2 and for another device it could be 200 m^2. To initiate a friendship, two devices must share the locality.



a. Two devices with the same "L" that do not share a locality area



b. Two devices with different "L" and a shared locality area

Figure 6. Locality and physical proximity

Figure 6 illustrates two different cases in CSIoT. In the first case, two devices have the same "L" but they do not share the locality area. In the second case, two devices have different "L"s but they share a locality area. In latter case, each of these devices can initiate the friendship. Therefore, the physical proximity factor can be formulated as:

If $L \geq d = \sqrt{(x2 - x1)^2 + (y2 - y1)^2}$, then initiate friendship.

Where L is the locality and *d* is the distance between two objects and (*x*,*y*) are the device location information.

Similarity

In CSIoT, similarity is used in two forms: owner similarity and product similarity. Two devices are considered similar when they have the same owner or the owners are trusted friends. Two devices are also considered similar when they are produced by the same company over the same period of time.

The owner similarity is similar to the object owner relationship (OOR). However, this relationship is extended to friend owners. In other words, when the owners of two devices are trusted friends, they can initiate friendship. Devices with same owner can establish a strong friendship because they might interact with each other frequently to satisfy the owner's needs. In addition, any device owner can consider trusted friends' devices to be friends with his own devices. There is also a high possibility for owners to interact frequently with their friends.

Among the device friendship factors in CSIoT are owners and owners' friends. The strength of friendship between an owner and his/her friends affects the strength of friendship in devices.

This study considers three levels of friendship between an owner and his/her friends: highly trusted friends (best friends), average trusted friends (close friends) and lowly trusted friends (acquaintances). These levels are subjective and are based on an owner's opinion. Two devices with best friend owners can initiate a friendship and their friendship score (strength) can be the highest at the beginning. Two devices with close friend owners can initiate a friendship with an average score and finally, two devices with lowly- friends can initiate a friendship with a low friendship score.

Product similarity is similar to the POR relationship. This factor is useful for software problems and sharing information processes because smart objects with the same batch number are compatible and homogeneous (Aztori et al., 2012, Kasnesis et al., 2017).

Reciprocity

Reciprocity is important in initiating friendship as well as in maintaining the friendship in CSIoT. If Device 1 sends a friendship request to Device 2, then Device 2 accepts or rejects the friendship. In the case of acceptance, both devices can add the other to a friend list. Reciprocity is also considered one of the factors in friendship updates.

Suppose that Device 1 and Device 2 are friends. After a while, Device 2 rarely responds to Device 1 for various possible reasons (e.g., malfunction or a busy node). Thus, Device 1 should decrease the friendship strength since there are not a satisfying number of responses or services from Device 1. Therefore, the accessibility of friend devices and the number of appropriate responses and services during a certain amount of time are the main components of reciprocity. Most probably, the link between two devices with low reciprocity will not be useful most of the time. However, high reciprocity between two devices can increase friendship strength. Reciprocity can be formulated as:

$R = n/t$

where R is reciprocity, n is the number of appropriate responses (in terms of messages and services), and t represents time. The reciprocity factor will affect friendship strength in SIoT.

Competence

Competence is defined as a set of factors that are socially important for smart objects in selecting and maintaining friends: QoD (Karkouch et al., 2016), QoI (Wu et al., 2014) and network structure (Nitti et al., 2015). These factors are important for communication between nodes and friendship selection. The social effectiveness of nodes appears to be highly dependent on these factors.

In CSIoT settings, nodes are equipped with sensors that can exchange data with other nodes. The quality of the sensed data is an important measure of node performance. Assume that a person has heart problems and his average heart rate should be monitored regularly. This person has a wearable device and a smart phone application that report two different values for the average heart rate during a day. Here, data quality evaluation can find the most reliable value for average heart rate. Sometimes sensed data might be noisy, corrupted, or incomplete. Therefore, a node that consistently provides high quality data is more popular than other nodes.

There are different criteria for evaluating QoD in IoT settings, but the most important factors include interpretability, accuracy, completeness, timeliness, and reliability (Karkouch et al., 2016). A comprehensive QoD evaluation is out of scope of this study. Interpretability refers to data clarity in terms of format and meaning. Accuracy represents data precision and completeness as the ratio of non-interpolated items to all items available. Timeliness identifies how up-to date the data are, and reliability represents the consistency of data.

QoI represents the importance of information received from each node. Objects in CSIoT have different decision-making processes (e.g., friend selection). It is important for each node to evaluate the information received from other nodes for decision-making. QoI is represented as below.

QoI = Q*P*R*A*D*T*V

where *Q* is quantity, and it indicates how much useful information is received for a specific task. If a node receives all required information, then $Q = 1$. *P* represents precision and reflects the proportion of relevant information to all information received. So, if half of the information is relevant, then $P = 0.5$. *R* denotes recall and represents the proportion of the relevant information to the number of all relevant information. *A* represents the accuracy of information for decision-making. *D* denotes the complete degree of information received for decision-making, and *T* represents the timeliness of information. Finally, *V* denotes validity and represents the trueness of information. If the received information is completely false, then $V = 0$. All the QoI factors should be normalized in (0,1) range.

Each object in CSIoT has a computational limit and needs time to cope with large numbers of connections and service searches. That is why this study adopts the heuristic method proposed by Nitti et al. (2015) for friend selection in CSIoT. First, the maximum number of connections allowed (N_{max}) is defined. Then a node utilizes a minimum local clustering strategy to manage any further friendship requests. Based on this strategy, a node ranks its friends based on the number of common friends. Then it compares the node sending a friendship request with its friends. If this node has more common friends compared to other friend nodes, then it rejects the friendship request.

The overall competence score is calculated based on the following formula:

Competence score (C) = QoI*QoD* N

Where QoI represents the quality of information, QoD represents quality of data and N represents the network structure. The QoD is calculated based on the usefulness of data in running required applications. In this study we consider random values of QoD for each service and the maximum QoD can be 5. The network structure score can be calculated based on the number of common friends and its maximum is also 5.

3.3.6.3 Leveraging friendship

Managing friendships and relationships is important in SIoT. Smart objects can socialize with each other and are able to start, update and terminate the friendships. The friendship and relationship between objects can create short links in the SIoT network and can increase network navigability and decrease network latency.

A review of the literature indicates that SIoT architecture and frameworks heavily focus on friendship initiation and termination. In other words, they focus on friendship selection and the different types of relationships that objects can establish (e.g., OOR). However, updating relationships and differentiating levels of friendship are rarely considered in the literature.

As in social networks, the level of friendship is important for assessing trust and social interaction capabilities. In real life, we as humans have acquaintances, close friends, best friends, and perhaps enemies. For each category, we have a different level of trust and a different level of communication. We do not share our private and personal information with acquaintances or strangers. We might need to interact more often with our best friends and have high level of commitment to our relationship.

Although the friendships between smart objects seem different from friendships between people, they are similar, but in different ways. In SIoT, objects have cognitive and socialization capabilities that make them human-like things. Features are created in objects to serve people. The more human-like objects have more capabilities to serve humans. That is why considering the important factors in human friendship and applying them in object relationships can be useful and valuable.

One of the important factors in human relationships and friendships is leveraging. In real life, different values and strengths are considered for our friendships. Leveraging friendship is a process based on such factors as time, commitment, reliability, and trust. Other factors such as privacy, communication, and interaction are also important in leveraging friendships.

Leveraging friendship is also important in smart objects' communications, and there should be an effective mechanism for that in SIoT. The information and services to be exchanged between devices have different values and levels of importance, which is why there should be different levels of communication between devices. Leveraging friendship can set boundaries for communication between devices.

Suppose that Device 1 has three friends (Device 2, Device 3 and Device 4). Leveraging friendship can indicate the level of friendship for each of these friend devices and the strength of the friendship link between Device 1 and the friend devices. Device 1 can use this information to manage communication between itself and friend devices. It can share sensitive and private information only with high-level friends. It can expect receiving vital and high-quality services from high-level friends. It can commit more or less friendship based on the level of friendship. Finally, Device 1 has a clear level of trust for each of the friend devices based on a friendship level.

Leveraging friendship in SIoT is not studied enough in the literature. For example, Aztori et al. (2012) proposed a SIoT architecture and the only factor considered for leveraging friendship between devices was trustworthiness, which was determined by network centrality and prestige. These factors are important, but there are other factors (e.g., QoI) that are also important in leveraging friendship. Additionally, the authors did not consider time factors in this process. Suppose that a device has high trustworthiness at a certain point of time (t_1) but a low trustworthiness in t_2. There is not an effective mechanism in Aztori et al. (2012) study to monitor the variation of trustworthiness over time and the leveraging of friendship based on the results.

This study takes a continuous and comprehensive approach to leveraging friendship between devices. In CSIoT, friendship can grow and end during a given timeframe based on several factors, including similarity, competence, reciprocity, and proximity. These factors can affect friendship initiation as well as friendship growth or termination. In CSIoT, friendship is not a linear relationship. It can grow and end gradually over time based on various factors.

Knapp’s relational stage model inspires the model of friendship in CSIoT in this study. This model provides a good understanding of friendship development and termination and is useful in applying basic concepts to SIoT friendship management.

3.3.6.4 Knapp’s relational stage model

Knapp’s (1987) relational stage model is one of the well-known theories about interpersonal communication and friendship development. This model is like a dual staircase that shows how a relationship can grow and how it can end. Figure 7 depicts Knapp’s relational stage model.

This model consists of two interrelated sets of stages (depicted in blue and red): relationship escalation and relationship termination models. The important factor in this model is that the speed of growth and time for changing scales can vary in different relationships and even some stages can be skipped in some relationships. This model shows that relationships between people generally grow and end in different stages. Obviously, time is an important factor here.

Each stage in this mode has some unique characteristics (Fox et al., 2013). The *initiating* stage includes first impression and uncertainty. Two people have a willingness to meet each other and start a relationship, but they do not know each other well.

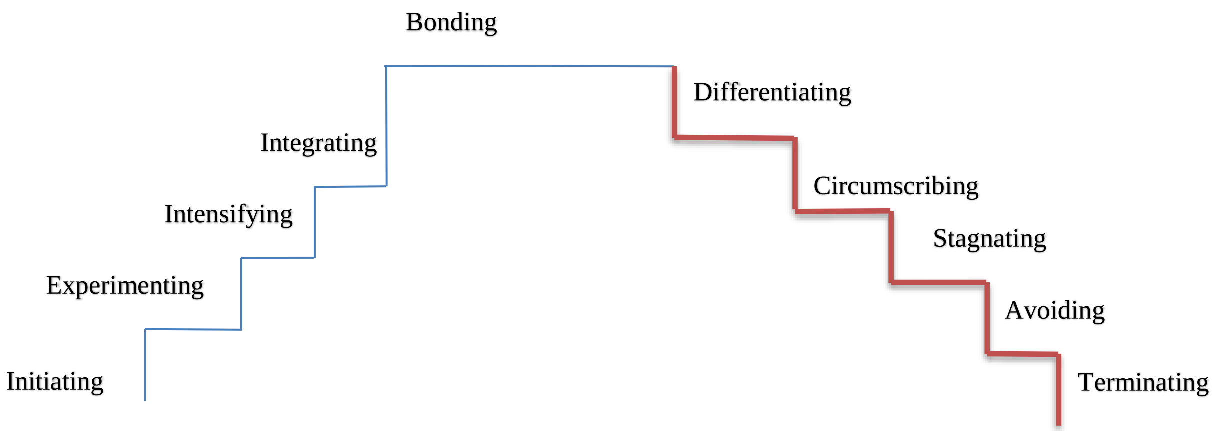


Figure 7. Knapp's (1987) relational stage model

During the *experimenting* stage people explore each other to find commonalities or interesting factors that encourage them to continue the relationship, although self-disclosure levels are low and people usually do not share sensitive information about themselves.

After experimenting, people begin sharing their personal information, which impacts relationship growth (*Intensifying*). In this stage, the participating parties have commitment expectations and will find different ways (e.g., gifts) to strengthen the relationship.

Oneness is an important characteristic of the *integrating* stage when participating persons refer to themselves as "we" or "us". They consider themselves best friends and will have a private commitment to the relationship. For two people to reach this stage, they need to know each other very well over time.

The last stage in relationship growth is *bonding* when two persons have a shared identity and a public commitment. In business relationships, partnership and a durable relationship for lowering costs and increasing benefits can be considered as the bonding stage.

Differentiating is the first stage in coming apart and terminating the relationship. Because of various reasons, including different attitudes, different interests, and different personalities, participating parties begin fighting over conflicts and the relationship will start to fade.

In *circumscribing,* partners will limit their conversations. They still hope to continue the relationship, but they set boundaries in their communications.

In the *stagnating stage,* partners limit their conversations even more than during the circumscribing stage, as partners want to reduce and even end the relationship, but because of some unavoidable factors they cannot completely terminate the relationship.

Partners in the *avoiding* stage intentionally avoid any conversation and contact. They are always too busy to see each other. Finally, partners end the relationship in the *terminating* stage.

3.3.6.5 Friendship model in CSIoT

Obviously, friendship between devices is different in some ways from friendships between humans. Smart objects in SIoT are human-like but they are not human. They do not have emotions, attitudes, and other complicated human features. However, the basics of friendship development and termination can be applied in smart objects in SIoT to create new capabilities and useful in SIoT setting features.

To model device friendship, this study utilizes the basic elements of Knapp's model, such as growth or termination in different stages over time. Friendship in CSIoT has three main components: initiating, growth and terminating. Several factors such as time, similarity, proximity, reciprocity, and competence can affect stage changes in friendship.

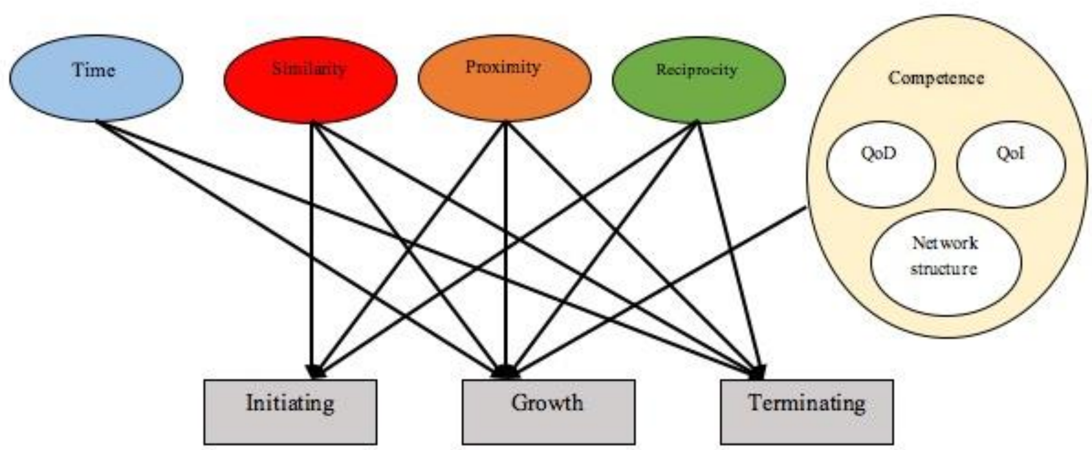


Figure 8. Relationship model in CSIoT

Proximity, similarity, reciprocity, and competence are important factors for initiating a friendship and friend selection. In CSIoT, objects will use the following algorithm to initiate a friendship (see Table 4).

Table 4. Friendship initiation Algorithm I

```
Suppose Owner and Agent are data structures including following properties and methods:

Def Agent = {
 X: Number,
 Y: Number,
 Locality: Number,
 owner: Owner,
 batch_id: Number,
 friends: Map<Agent,Int>,
 function send_init_friendship(to:Agent),
 function send_friendship_result(to:Agent, result:Number)
 }
Def Owner = {
 Id: Number,
 highly_trusted: List<Owner>,
 medium_trusted: List<Owner>,
 low_trusted: List<Owner>
 }
Algorithm Friendship_Initiation_I(a: Agent, all_agents:List<Agent> )
Begin
 Foreach Agent b in all_agents:
 Def D = sqrt( (a.x - b.x)^2 + (a.y - b.y)^2 )
 If a.locality >= D or
 a.owner.id == b.owner.id or
 a.batch_id == b.batch_id
 Then
 Def reciprocity = a.send_init_friendship(b)
 If reciprocity == 1
 Then
 If Competency > α Then score = 1 End
 If b in a.owner.highly_trusted Then score = 5 End
 If b in a.owner.medium_trusted Then score = 3 End
 If b in a.owner.low_trusted Then score = 1 End
 a.fiends.insert(b, score)
 End # If
 End # If
 End # For
End # Algorithm
```

This algorithm has two parts. In the first part, a device checks the friendship initiation criteria and in the case of a satisfactory condition, it sends a friendship request. In the second part, if the device receives an acceptance message from any device, it adds that device to its friends list and calculates the new friendship score.

α in Algorithm I is a threshold for an overall competency score for initiating friendship and it can change based on user rules and context. Reciprocity_I is a part of the reciprocity criteria that is important in initiating friendship and it has acceptance/rejection values.

In CSIoT, initiating friendship deploys two algorithms: one for sending a friendship request and another for accepting a friendship request. The first is proposed earlier, and the latter is illustrated in Table 5.

Table 5. Friendship initiating Algorithm II

```
Algorithm Friendship_Initiation_II(a: Agent, b: Agent)
Begin
 Def D = sqrt( (a.x - b.x)^2 + (a.y - b.y)^2 )
 If a.locality >= D or
  a.owner.id == b.owner.id or
 a.batch_id == b.batch_id
 Then
 If b in a.owner.highly_trusted Then score = 5 End
 If b in a.owner.medium_trusted Then score = 3 End
 If b in a.owner.low_trusted Then score = 1 End
 a.fiends.insert(b, score)
 a.send_friendship_result(b,1)
 Else:
 a.send_friendship_result(b,0)
 End # If
End # Algorithm
```

These two algorithms are almost identical, with the only difference being the reciprocity_I factor. Also, the second algorithm does not need to check reciprocity_I. In the second part of the friendship initiation when a device receives a friendship request, it evaluates the sender based on the same criteria and if the sender satisfies the criteria, then it accepts the friendship request, adds that device to its friends list, and assigns a friendship score.

For leveraging friendship in CSIoT, this study considers different friendship scores that show different stages of friendship. In Knapp's model, each friendship stage has some unique characteristics. Some of these characteristics, like public commitment, are special features of human relationships. This study aims to mimic Knapp's relational stage model by considering the different stages and characteristics that are suitable for smart devices and SIoT settings. Figure 9 shows the friendship leveraging model for SIoT.

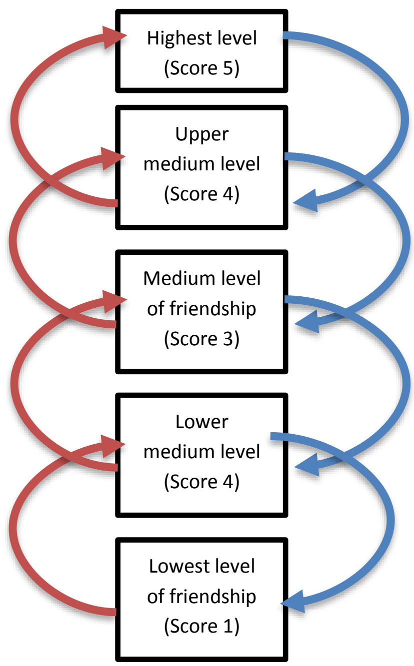


Figure 9. Friendship levels

This study considers five levels of friendship with five different scores. Score 1 is for the lowest level of friendship and Score 5 is for the highest level of friendship. Several factors including time, competence, reciprocity, proximity, and similarity can level up and level down the friendship between devices. Except for Level 1, which is the friendship initiating level, all other levels are dependent on a cumulative score of time, similarity, proximity, competence and reciprocity. The algorithm illustrated in Table 6 is used to assign friendship scores and is the main process of updating friendship in CSIoT. This algorithm is used after friendship initiation.

Table 6. Friendship updating algorithm

Input: Similarity score (S_i), Proximity score (P_i), Competence score (C_i), Reciprocity_II score (R_i), Time score (T_i), Grand Minimum score of each level (GMS_i), Level 2 min time (T_2), Level 3 min time (T_3), Level 4 min time (T_4), Level 5 min time (T_5), Minimum tolerable time (T_m)

Output: Friendship score

If $S_i + P_i + C_i + R_i \geq GMS_2$ **and** $T_i > T_2$

Then Friendship score = 2

If $S_i + P_i + C_i + R_i \geq GMS_3$ **and** $T_i > T_3$

Then Friendship score = 3

If $S_i + P_i + C_i + R_i \geq GMS_4$ and $T_i > T_4$

Then Friendship score = 4

If $S_i + P_i + C_i + R_i \geq GMS_5$ **and** $T_i > T_5$

Then Friendship score = 5

Else if $S_i + P_i + C_i + R_i \leq GMS_i$ **and** $T_i > T_m$

Then Friendship score $\longleftarrow$ Friendship score – 1

If the friendship score = 1 and $S_i + P_i + C_i + R_i \leq GMS_1$

Then remove the device from friends list

Return friendship score

The scores for similarity, proximity, reciprocity, competence, and time are normalized in (0, 10) range. GMS_i is the minimum cumulative score for each level. T_i represents the friendship duration, while T_m denotes the minimum time tolerable for a low cumulative score in each friendship level.

This algorithm continuously checks the friendship criteria, and it considers time in increasing or decreasing the level of friendship. There are some exceptional cases (e.g., devices with same owners) in which some levels can be skipped. The cumulative score and minimum time scores can be changed based on context and user rules.

Service management

This study divides all the services into five categories. Each of the CSIoT categories listed in Table 7 illustrates the level of importance for the services.

Table 7. Service categorization

Service type	**Importance level**	**Can be sent to or received from**
5	High	Friends with a score of 5 or friends of these friends with a score of 5 etc.
4	Upper medium	Friends with a score of 4 or friends of these friends with a score of 4 etc.
3	Medium	Friends with a score of 3 or friends of these friends with a score of 3 etc.
2	Lower medium	Any device (Friend or non-friend), a priority with friends and friends of friends with a score of 1 and above.
1	Low	Any device (Friend or non-friend), a priority with friends and friends of friends with a core of 1 and above.

The importance of the service is calculated based on three important factors: time, privacy, and functionality. These factors are subjective to each device. Each device needs some services and provides some services. Each device can prioritize the services that it needs and provide services based on certain factors. Time means how quickly the device needs to receive the service. Privacy means how sensitive and the degree of private information the service contains. Finally, functionality means the degree of accuracy, QoI, and QoD.

Service importance (SI) = T*P*F

This formula is used to calculate service importance. Each device, based on user rules, context, and situational factors, can rank the services using this formula.

Service discovery (SD) and service composition (SC)

CSIoT objects should be able to discover services and information that they need for different purposes. This study uses the SD and SC components proposed by Aztori et al. (2012). SD and SC collaborate with RM to find the proper information and services from other objects. Service discovery performs four important tasks: service search, serving friend search, search for a friend of a friend and service ranking. The SC component filters the services by using service-ranking outputs.

Relationship management (RM)

Relationship management is an important SIoT component. This study uses the revised version of RM as presented by Aztori et al. (2012). The main duty of RM is to start, update and terminate friendships. This study adds the complexity concept to RM. Friendships and relationships are analyzed by considering non-linearity and using fuzzy ontology. In addition, RM collaborates with the cognition module to make better decisions in friendship management.

RM also plays an important role in SD and SC. The friendship level can be a factor of trust and reliability. RM will make it easier to discover needed services and information and to compose available services. Figure 10 illustrates the main inputs and outputs of an RM component.

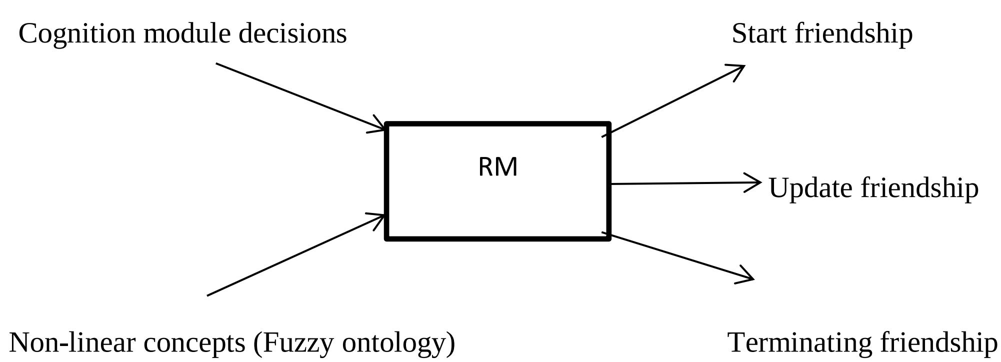


Figure 10. Relationship management

3.4 Illustrative example of framework

For better understanding of the proposed framework and its functionalities, we provide an illustrative example here. Suppose that we want to apply the CSIoT framework in the smart car system. In this example we have different agents representing the smart devices in the smart car system and in the environment. The agents specifically represent GPS, temperature system, breaking system, entertainment system and, smart traffic lights system. Each of these agents has required services and the services that they can provide. The table below summarizes the agents and the services that can be exchanged between them.

Table 8. Illustrative example of the smart car system

Agents	Services required	Services provided
GPS	Map update	Location information, speed limit information, Traffic information, speed
Breaking system	Traffic information, Speed limit,	Intensity of break
Entertainment system	Audio, Video	Music suggestion, video suggestion
Smart traffic lights	Speed, Location, Intensity of break	Traffic information, Road condition

If we apply the CSIoT framework for this system, the agents will start to interact with each other and exchange the services and information. For instance, the breaking system can request traffic information and the speed limit from GPS and the smart traffic lights. The traffic light can request the intensity of break information from the breaking system. The entertainment system in one car can ask for music or video suggestions from the entertainment system in another car. Each agent will also evaluate the other agents to initiate, update or terminate the friendship based on the mentioned criteria.

Suppose that the entertainment system in car A (S_1) initiates a friendship with the entertainment system in car B (S_2) and the friendship request is accepted based on physical proximity factor. During the time and by exchanging more services and information, these two agents will update the friendship score. If the required criteria are satisfied and a certain time is passed from the friendship initiation, the agents will increase the friendship score. Otherwise, the agents will decrease the score or terminate the friendship.

The friendship update process during the time is important because the functionality of a friend agent can change during the time. Suppose that agent S_1 and S_2 are friends but after a while S_2 is not responsive and the reciprocity factor decreases. Therefore, S_1 should decrease the friendship level and ask the required services from higher level friends first. This process helps to enhance the service discovery.

The friendship update also enhances the privacy. Suppose that S_2 is a malicious agent and it tries to access the private information of S_1. S_1 might have some information about the entertainment that is considered private and sensitive. Because the friendship update mechanism considers time, it takes a longer time for S_2 to be a close friend of S_1 and access to the private information. S_1 also can send the sensitive services and information based on the friendship score (e.g. only close friends).

3.5 SIoT and privacy

According to *Business Insider* the IoT market will grow to over $3 trillion annually by 2026. Overpopulated and large networks of IoT devices present many opportunities and challenges. Currently, researchers aim to explore the potentials that can be performed by IoT devices and to develop more effective IoT frameworks that can serve increasingly complex human society.

The Social Internet of Things is one of the proposed frameworks for future generations of IoT. SIoT uses social networking concepts to define relationships and interactions between objects (things). In a SIoT framework, objects can interact with each other autonomously, discover services and information in the complex IoT environment and offer services and information to other objects. Objects can start, update, and terminate friendship with other objects. SIoT can increase the sociality/connectivity and pervasiveness/availability of IoT systems (Ortiz et al., 2014). In addition, SIoT can create many capabilities such as object discovery functionalities, evaluation of trustworthiness of objects and the information provided by them, and deployment of value-added services (Aztori et al. 2014). SIoT also enhances network navigability by creating short links between friend devices.

Privacy in the IoT is an important challenge (Li et al., 2015). Many activities in the IoT environment, such as personal activities, business processes, and information exchange, need effective security and privacy mechanisms. Designing new privacy-preserving frameworks for future generations of the IoT is a crucial issue of concern (Zhou et al., 2015).

The privacy issue is also an important challenge in a SIoT framework. Inadvertently, exchange of services that contain private and sensitive information can violate the privacy of device owners. Malicious objects can also violate owners' privacy by misusing friendship connections. Therefore, an effective mechanism is needed in SIoT to manage privacy breaches in service exchanges between objects.

An important factor that might cause privacy breaches in SIoT is the lack of an effective mechanism to update friendships between devices. SIoT frameworks in the literature do not have clear and effective methods for objects to monitor continuously other objects' behavior and update their levels of friendship.

This study will propose a novel SIoT framework that leverages friendship and services to create a rigorous trust measurement mechanism between devices. Leveraging friendship means that objects can continuously monitor other objects' behaviors and update friendship levels over time. This framework also considers leveraging services that would be exchanged between objects. Each object would be able to categorize services in different groups, from low importance to high-importance levels. Thus, services containing highly private information and data will be exchanged between high level (highly trusted) friends and vice versa.

The new framework can improve the privacy of owners in a SIoT environment by decreasing the number of malicious objects that seek to misuse friendship links between devices. In addition, by leveraging friendships between IoT devices in an effective way, a valuable trust evaluation mechanism can be developed that will enhance the device owners' privacy.

For evaluating the new framework, this study uses the smart city use-case scenario to evaluate the role of new SIoT framework in managing privacy breaches in a SIoT-based environment. A new simulation tool (CSIoT) is used to simulate the interactions and relationships between devices and evaluating the privacy-preserving ability in the new framework.

3.6 Blockchain-based SIoT

Bitcoin is an online cryptocurrency introduced in 2008 (Nakamoto, 2008). Blockchain technologies emerged after the introduction of bitcoin. Because of a lack of control from any centralizes financial entity or authority, bitcoin use spread quickly all around the world. A decentralized network of nodes securely held and stored bitcoin currency in a transparent and auditable way. Figure 11 depicts a sample data structure of such blocks.

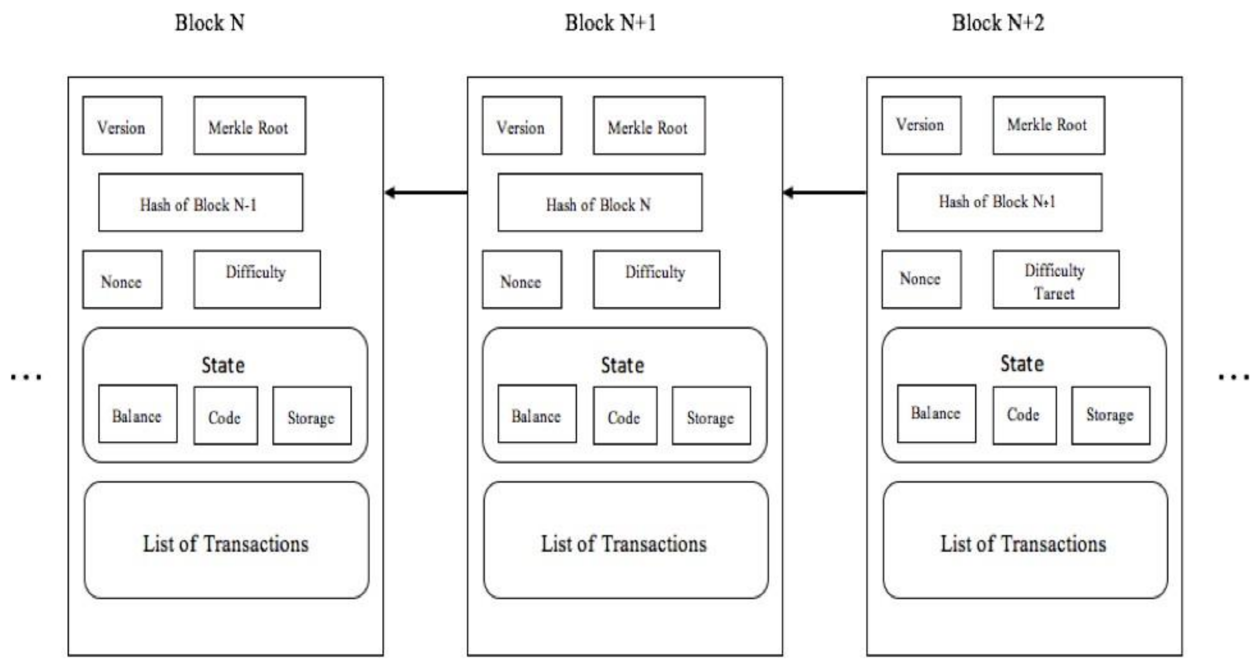


Figure 11. Data structure of blocks

The basic functionality of blockchain is found in the decentralized and distributed ledger system shared between blockchain nodes. Transparency is a main feature of blockchain technology. Every transaction in the blockchain is auditable because the information on the ledger is open and transparent. The transactions are also immutable meaning that transactions cannot be removed or overwritten in the ledger. This feature creates a solid trust mechanism because users are sure that their currency can be tracked and safe. After running each transaction, new information is stored in the block using the ledger. This information includes the type of transaction, the value of the transaction, and the timestamp of the transaction. Each block contains the transaction-set information and a reference to the previous block. Thus, the blocks are connected through this structure called blockchain (Reyna et al., 2018).

The main eight characteristics of blockchain technology include transparent log, no third party interference, secure transaction, decentralized network, easy backtracking, peer-to-peer communication, time-stamped transactions, and digital ledger to maintain updated records (Hassan et al., 2019). Hassan et al. also cited three types of blockchain: private, public and consortium.

In a public blockchain, every individual, regardless of organization or background, can join the open, decentralized platform and can conduct mining or transaction operations (Tschorsch & Scheuermann, 2016). However, in a private blockchain, only specific organizations or groups of people can join the decentralized network. Since these selected individuals or specific organizations control the mining operation, a new individual cannot access the blockchain without a special invitation (Puthal et al., 2018). A consortium blockchain is a mix of private and public blockchains. In such a consortium, a group of people or organizations make decisions about block validation and consensus. These groups of people or organizations also decide how new node participation and mining nodes are performed and created. Thus, to mine a block in this type of network, a multi-signature scheme is required. Giving read-or-write permissions is another responsibility of these controlling nodes (Gu et al., 2018).

Blockchain can address major security and privacy issues previously discussed because it provides a decentralized, secured and trusted data sharing service. Information in IoT could be tracked easily by utilizing block chain technology.

One of the main reasons to integrate blockchain and IoT is its decentralized nature that can address the main problems of centralized IoT architectures, such as bottlenecks and central points of failure (Veena et al., 2015). In a decentralized structure, there is no controlling company that controls the storage and process of data. Thus, privacy issues due to the illegitimate use of sensitive data by controlling companies can be resolved.

All the transactional information of applications in blockchain-based IoT is encrypted (Prisco, 2015) and, therefore, the data is secure. Another reason for integrating blockchain and IoT is the immutable and reliable feature of blockchain-based IoT. This feature can develop a trust mechanism because any transaction can be traced and verified without any risk of tampering. It can also improve the reliability of the sensor's data.

Another reason for integrating IoT and blockchain is blockchain-based IoT's identity management feature. By using unique identifiers for every device, the data from each device can be tracked easily. Additionally, trusted distributed authorization and authentication services can be provided.

3.5.1 Experimental framework for blockchain-based SIoT

Blockchain technology can integrate and store data in a distributed way while improving the security of data access. It addresses the major security and privacy challenges of SIoT by adding decentralized, immutable and transparent features to the SIoT environment. Figure 12 shows the experimental framework for integrating SIoT and blockchain.

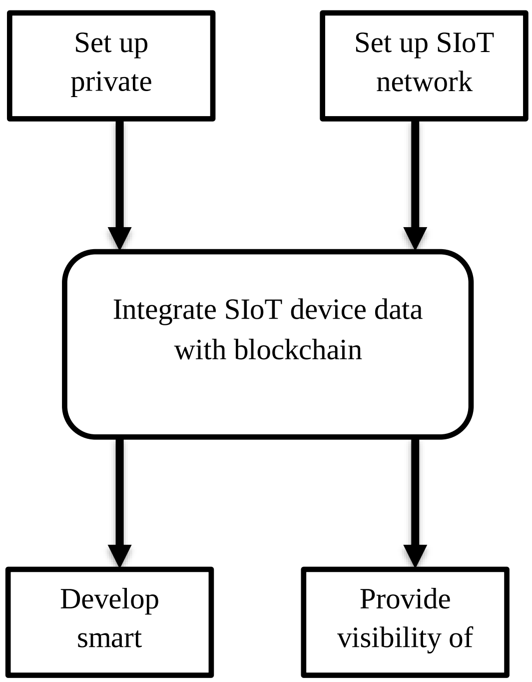


Figure 12. Blockchain based SIoT framework

Smart contracts manage the interaction between nodes and are implemented as codes in blockchain. Smart contracts are applied to all transactions in a SIoT environment. A transaction in SIoT is any service exchange between devices. This study uses Ethereum in the blockchain-based SIoT environment. Ethereum is the second generation of cryptocurrency following bitcoin and also stores the transaction information in blocks.

This study develops a private blockchain that includes the distributed storage of data, consensus formation, and operation of smart contracts.

Here is the pseudo-code of a smart contract:

```
Contract CSIoT
Struct SIoT device data {
Unit SIoTdata;
Unit date;
Unit time;
{
mapping (address => SIoTdevice data (Address device ID, Unit i date, Unit i time, Unit i data
SIotDeviceDates(DeviceID).SIoTdata = i data
SIotDeviceDates(DeviceID).SIoTdate = i date
SIotDeviceDates(DeviceID).SIoTtime = i time
}
}
```

Because a private blockchain is used, authorized users are friend devices only. When Device B requests any data (service) from Device A, Device A first checks if Device B is a friend device. Then, based on the sensitivity degree of data and friendship level, Device A can accept or reject the request.

Chapter IV: Implementation and Evaluation

In this chapter, this study uses MAS modeling to simulate the CSIoT environment. Each agent represents a device, and in the simulation process, agents can interact with each other and exchange services. Fuzzy ontology is at the core of the framework and is proposed for managing interactions between device agents. This ontology is used in friendship decision-making.

After presenting the ontology, the details of simulation tool and different components and steps of simulation are discussed. Then this tool is used to simulate the CSIoT environment and the friendship network between device agents.

The first step of implementation and evaluation is to develop fuzzy ontology. Figure 13 illustrates an example of fuzzy ontology developed by Morente-Molinera et al. (2016).

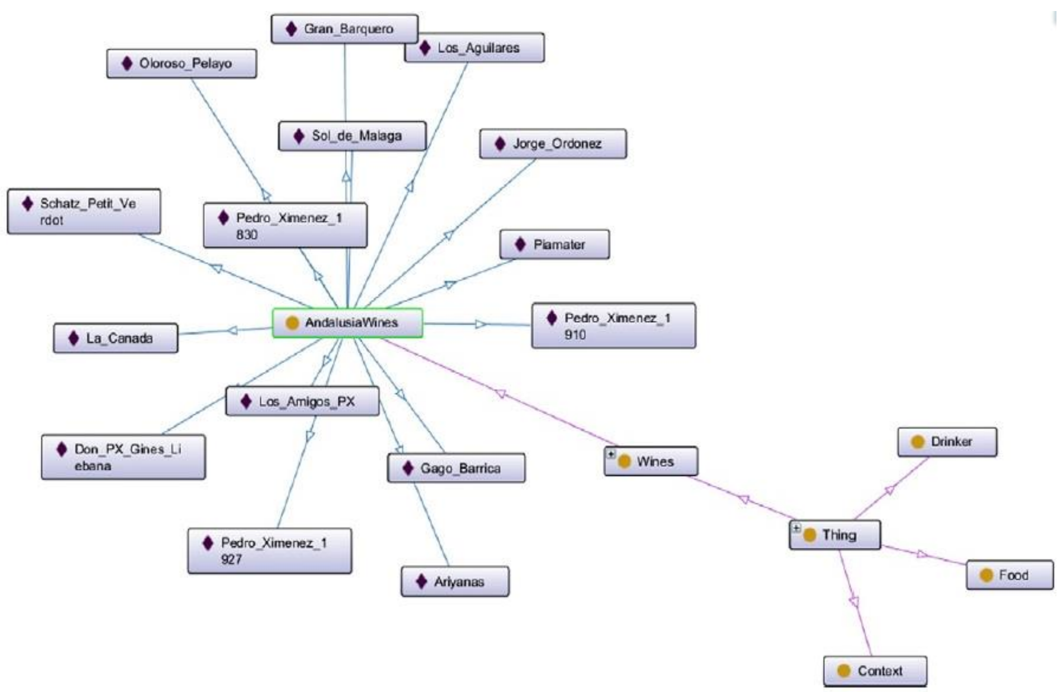


Figure 13. Wine fuzzy ontology adopted from Molinera et al. (2016)

The fuzzy ontology for CSIoT contains different entities such as an object, social friend agents, and complexity. This ontology also has several classes based on friendship types and complexity concepts. Figures 14 and 15 illustrate the ontologies developed by Kasnesis et al. (2017) for a cognitive and social IoT. The main goal in this study is to revise these ontologies and add complexity and fuzzy elements to them.

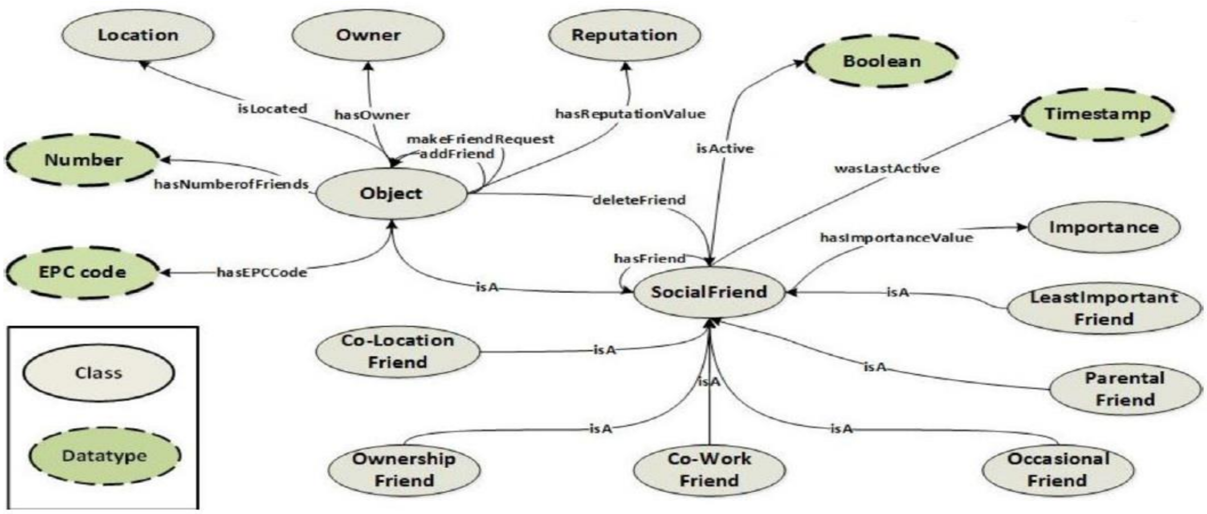


Figure 14. SSOR ontology adopted from Kasnesis et al. (2017)

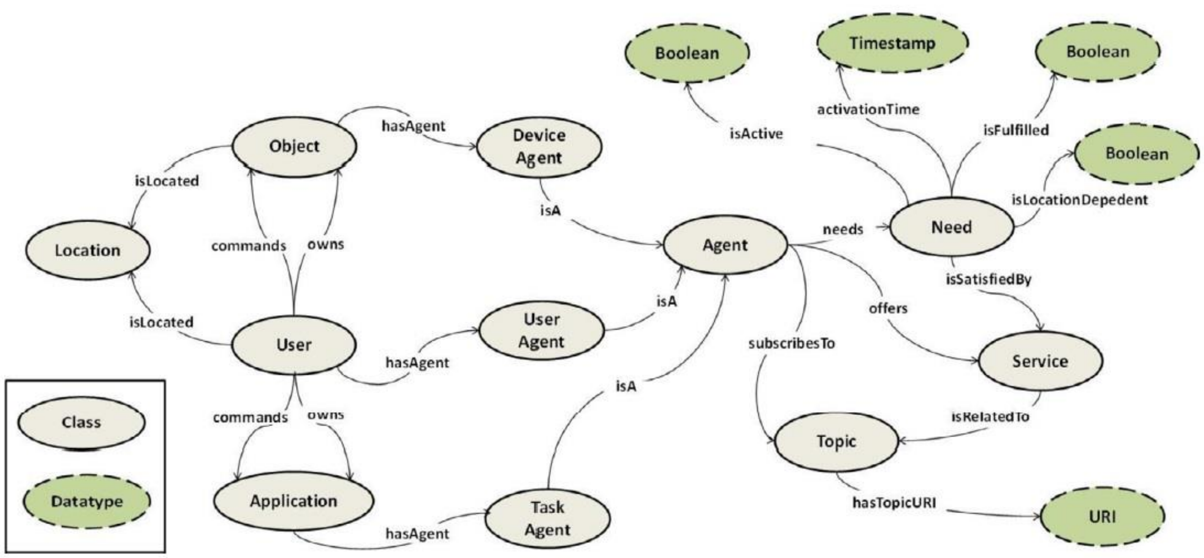


Figure 15. SONS ontology adopted from Kasnesis et al. (2017)

For all other steps, this study revises and improves the Kasnesis et al. (2017) and Aztori et al. (2014) works to develop different components that use fuzzy ontology and complexity science concepts. The Figure 16 shows the fuzzy ontology generated for CSIoT.

On the CSIoT platform, all the devices can interact with each other. A small world phenomenon is used to explore required services. The heterogeneous nature of devices causes interoperability issues. To manage that interoperability, this study uses semantic web technologies, including the Resource Description Framework (RDF) and Web Ontology Language (OWL). These tools explain the services and data exchanged between different devices. Because of the non-linearity and uncertainty nature of relationships between devices, this study developed a fuzzy ontology that is used in all framework modules (social, cognitive, and service).

CSIoT fuzzy ontology includes two types of agents: human agents and device agents. Human agents represent the owner of the devices. Each owner might have several friends with different trust levels. Each device also has a friend list that is continuously updated by the device agents. The friendship level, which has an impact on socialization and service management, includes four factors affecting the friendship level: proximity, similarity, competence and reciprocity.

There are two types of services in this ontology: services provided and services needed. Each device can provide services for other devices and each device will need services from other devices. Each service also has an importance level. Functionality, time, and privacy affect the importance level of the services.

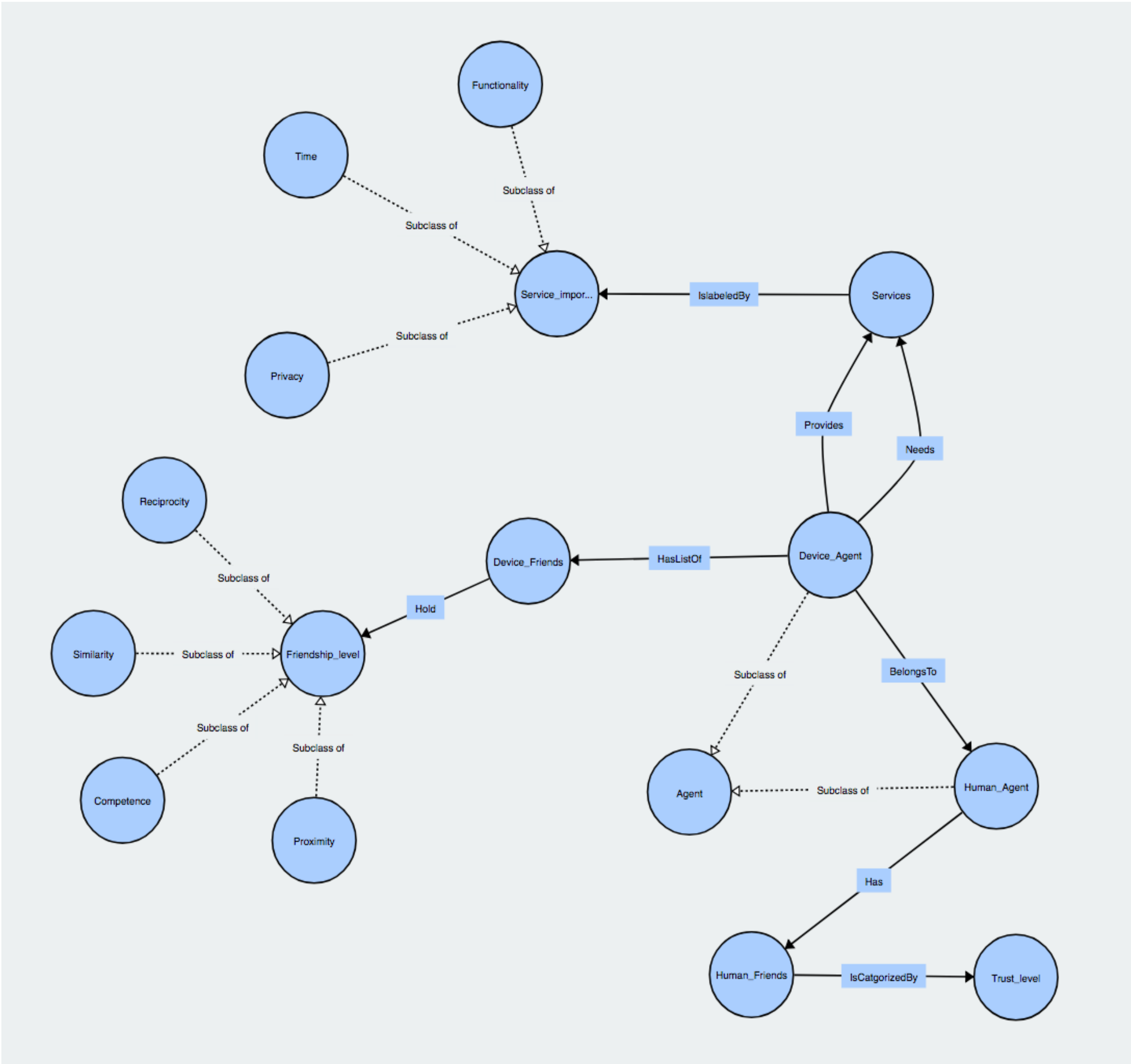


Figure 16. Fuzzy ontology for CSIoT

The final step of evaluation and implementation is conducted through simulation, which includes different tools for SIoT simulation. This study uses a new simulation tool and makes required extensions to previous ones.

There are two simulation tools, Small World In Motion (SWIM) and ASSIST, that were developed previously for SIoT simulation (Aztori et al., 2012; Kasnesis et al., 2016). Kasnesis et al. (2016) developed ASSIST, an agent-based simulation tool for SIoT. Figure 17 shows the ASSIST GUI.

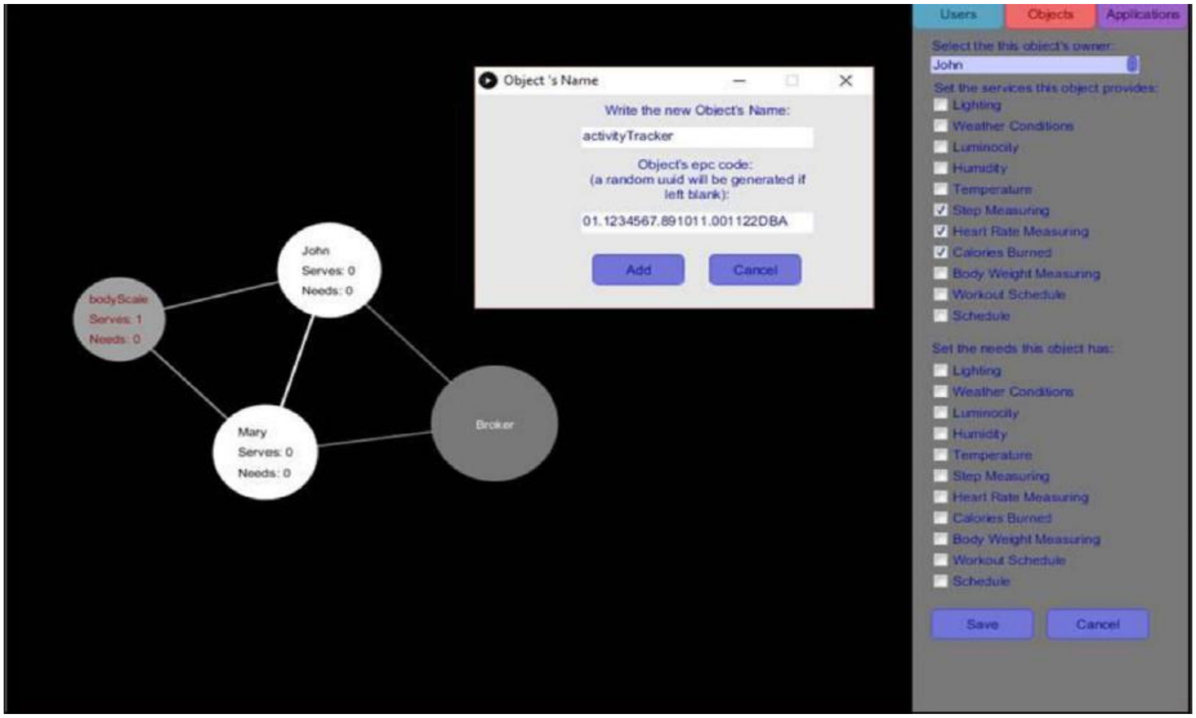


Figure 17. ASSIST GUI 1 adopted from Kasnesis et al. (2016)

This study revises previously proposed tools to develop a new tool for CSIoT simulation. Revising ASSIST includes two major strategies. The first is changing the ontologies it uses and replacing them with new fuzzy ontologies. Second, the new friendship model and service management mechanism is applied in the simulation tool.

The second simulation tool that can be revised and improved to simulate CSIoT is SWIM that was proposed by Kosta et al. (2010). The basic logic of SWIM is that humans consider two factors for choosing their destination. These factors are the distance from home and the popularity of destination.

Aztori et al. (2012) extended SWIM to simulate SIoT, but they considered a normal distribution in the number of owned things and did not include friendship leveraging, non-linearity, or cognition aspects.

4.1. Simulation

To evaluate a CSIoT framework, this study conducts Multi-Agents System (MAS) modeling where each agent represents a smart device and a virtualization technique is used to manage the heterogeneity of devices. CSIoT is web-based and developed in the Python language.

The simulation tool includes three assumptions. First assumption is that the agents represent smart devices in IoT environment. Before running the simulation, the agents should be created.

The second assumption is that agents have services provided and services required. We assign two sets of services (Provided, required) to each agent randomly. After running the simulation agents can exchange these services. So the service functionality and application is not in the scope of this study. In simulation process, all of the agents are created randomly. We had two sets of services including 2000 services. Each agent can have maximum 10 required or provided services.

Finally, the third assumption is that each device owner has set of friends with different trust levels. This can affect the friendship initiation and friendship scores.

The expected output of the simulation is the network of agents with friendship links and the information saved in simulation log. The log saves information about time stamp of the important events (Friendship initiation, update, and termination), friendship requests, number of friends, path length for obtained services and the time of service discovery. All of these information will be used to analyze the network structure, privacy and processing time evaluations. The main goal in evaluation is to see if the CSIoT framework performs effectively. So the evaluation of each component of artifact is not in the scope of this study and we only evaluate the general performance of the proposed framework comparing to the conventional SIoT framework.

For a CSIoT GUI, this study utilizes Cytoscape 3.6.1, an open source software for visualization and analysis of a complex network. Each node in this network represents an agent, and each agent represents a device. To create a new agent, the following information should be provided:

- Agent Id
- Owner Id
- Batch Id
- Locality
- Location (x,y)
- High-trusted friend IDs
- Medium trusted friend IDs

- Low trusted friend IDs

Figure 18 shows the “new agent” component in CSIoT when creating a new agent and registering a new device.

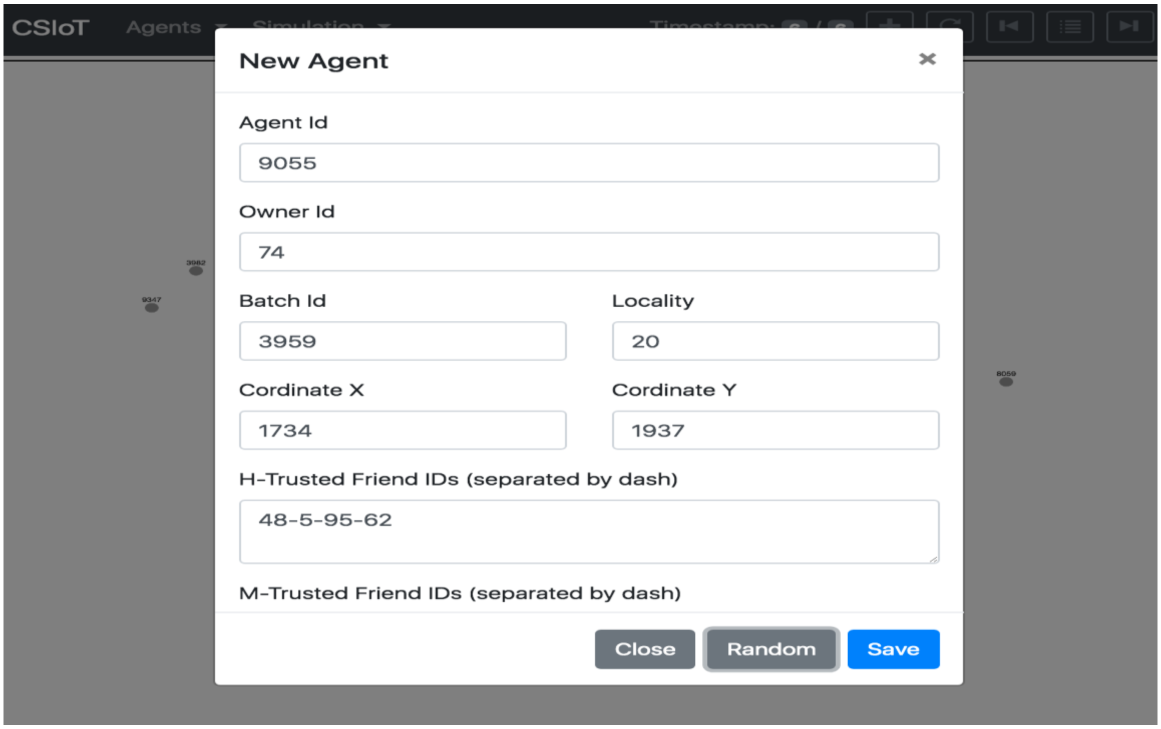


Figure 18. Creating a new agent

An important factor in CSIoT is the connection between human friendship and device friendship. Each device can recognize its owner’s friends and those friends’ devices. Based on trust level, a device can establish different levels of friendship with agents of other devices. Figure 19 shows an example of created agents.

After creating agents, this study then runs the CSIoT simulator. Figure 20 depicts the simulator module in CSIoT.

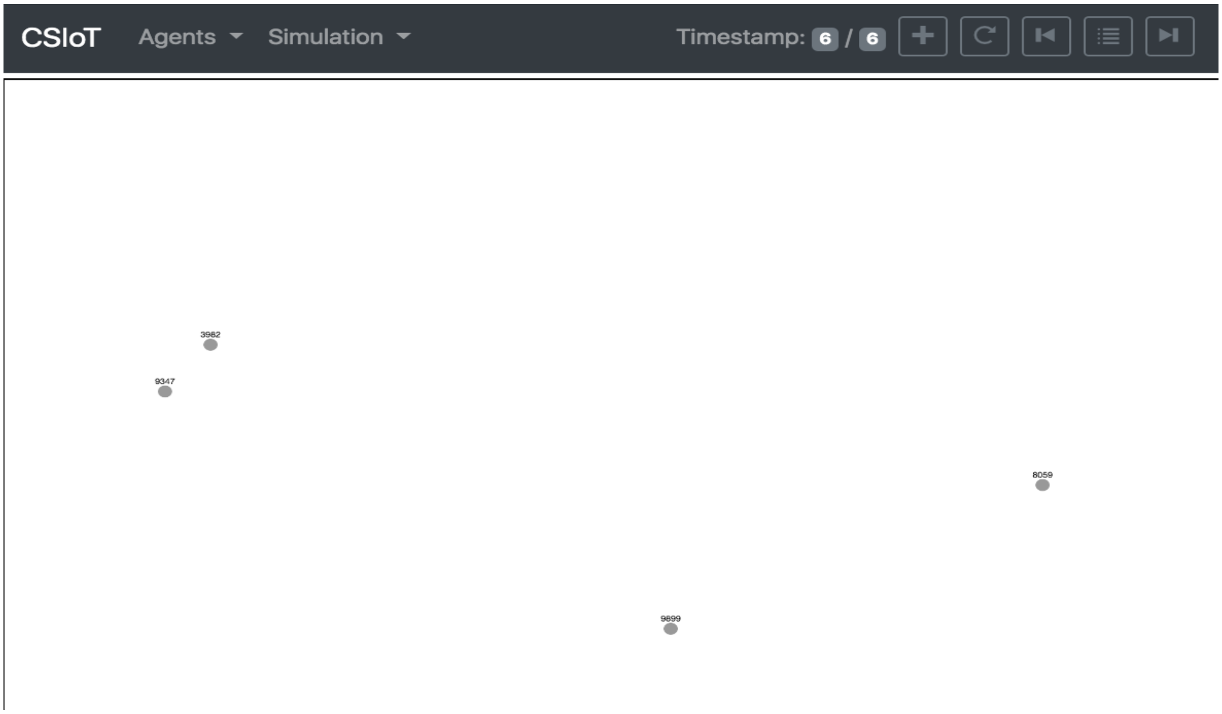


Figure 19. New agents

The simulation includes different steps. Each step represents a certain time slot. The “start simulation” option sets the number of steps and time slots for simulation. For example, “Simulation Step 1” includes the main function of the simulation. In this step, agents begin sending or receiving two types of messages. The first type is related to friendship. Agents send and receive friendship requests based on particular criteria (see Algorithm I). They also accept or reject friendship requests based on the criteria (see Algorithm II).

The second type of message concerns services. Each agent has two lists of services: services_needed and services_provided. Based on the applicable criteria, agents begin SD and SC. Service discovery, service compositon, and service acquisition are all dependent on the friendship management mechanism in CSIoT.

At the end of step one, the CSIoT simulator visualizes the friendship network of agents. The important factor in this network is the link between agents. This link represents the friendship strength between agents. Note that two friend devices can have two different friendship scores for each other. The average of two agents’ friendship scores is used to show the friendship strength (link weight) in the CSIoT network. Figure 21 shows an example of a friendship link between agent 1453 and agent 2580. The friendship strength is 4, which is the average of friendship scores for both agents.

After running the simulator for 1,000 steps, the weighted graph of the CSIoT network can be used to apply social network analysis. The simulation log is used in a semantic engine and learning process in both friendship management and service management.

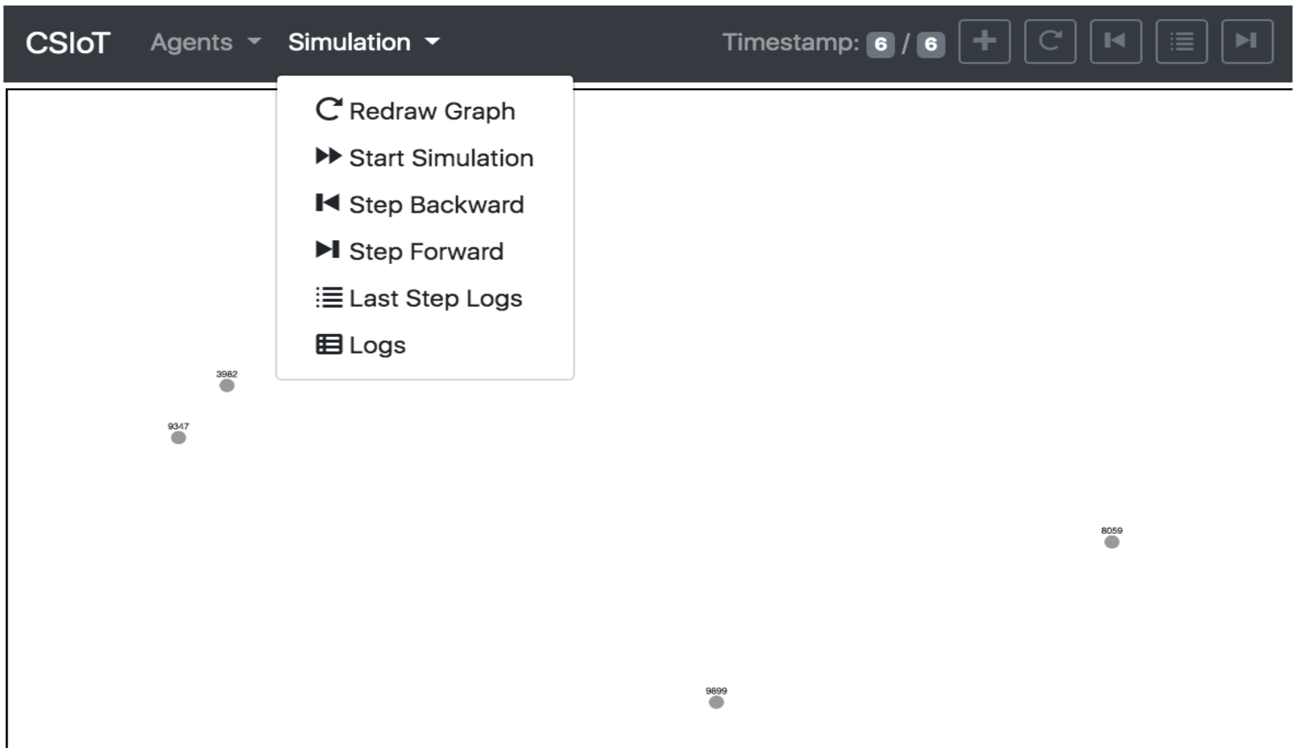


Figure 20. Simulation in CSIoT

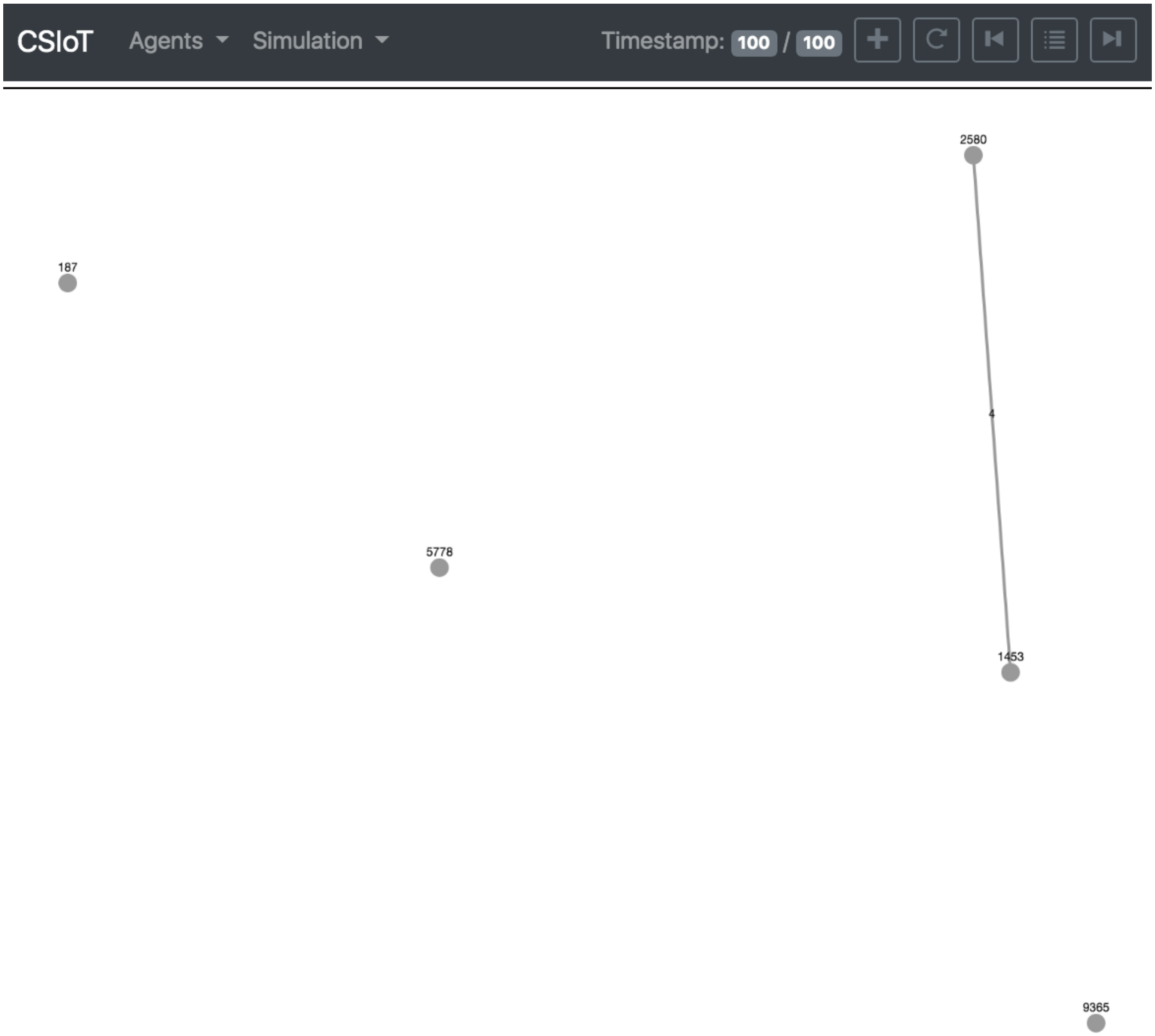


Figure 21. Friendship link

4.2. CSIoT evaluation results

To evaluate the CSIoT framework, the SIoT setting was simulated by adding 800 device agents and 200 human agents. The agents were randomly created using the "random" button on the "creating new agent" tab. The simulation included different steps, and each step represented a different time slot. In each simulation step, the device agents could interact with each other for an hour. Between simulation steps, the device agents performed decision-making, friendship updates, and service evaluation.

The study ran the simulation step 1,000 times. During the simulation steps, agent devices parsed the “services provided”, “services needed”, and “service importance” files for exchanging services. In the simulation, the time stamp information for service exchange and friendship update was recorded.

The first important factor evaluated after simulation was latency. The latency factor represented the average delay of SD and SC. The study compared the average latency of a conventional SIoT with the average latency of CSIoT. The conventional SIoT did not utilize the new mechanism for leveraging friendship and services. In addition, the conventional SIoT did not consider non-linearity and uncertainty in relationships and concepts. The conventional SIoT includes the main component of SIoT freameworks proposed by Aztori et al. (2012) and Kasnesis et al. (2017) without the conventional friendship development model and friendship update mechanism.

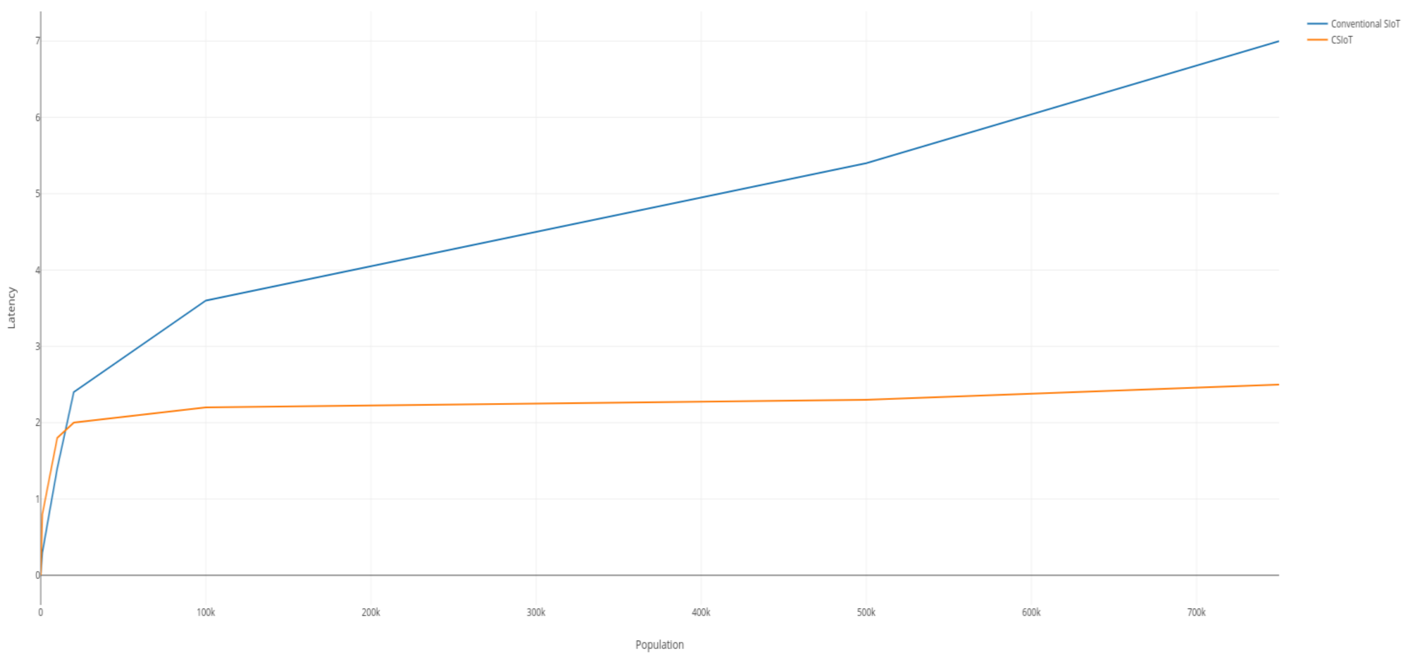


Figure 22. Average latency distribution in different agent population sizes

Figure 22 indicates that in small populations the conventional SIoT performs better than CSIoT. This is because CSIoT runs several queries for semantic reasoning and for leveraging friendship and services. In large populations, CSIoT outperforms the conventional SIoT in terms of latency. This is because CSIoT can find the smallest and most efficient paths in networks.

The second important factor for evaluating the CSIoT framework is the probability distribution in different path lengths. This factor represents the probability distribution of the minimum path length between a pair of randomly selected devices in CSIoT. Figure 25 shows that the network diameter is 6 and the average path length is 2.57.

The probability distribution of a random IoT network was compared with the CSIoT probability distribution. The average path length for the random network was 3.45. In addition, the diameter of the random network was 9 and 2% of the devices were isolated. Briefly, Figure 23 reveals that CSIoT performed well in terms of average path length.

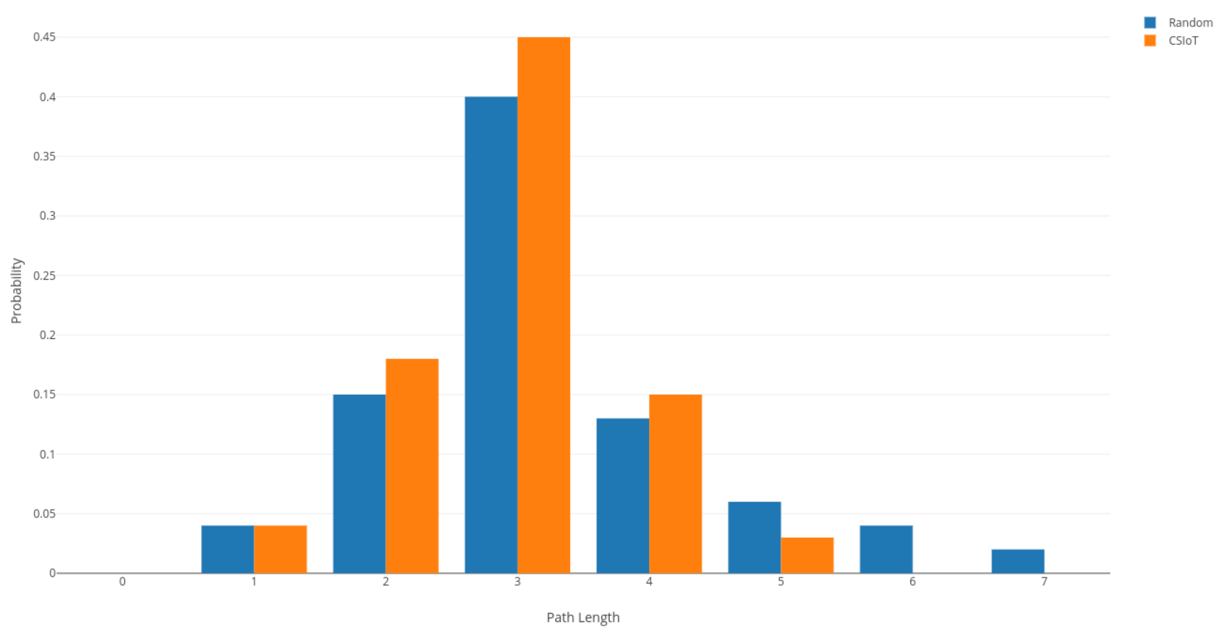


Figure 23. Probability distribution in different path lengths

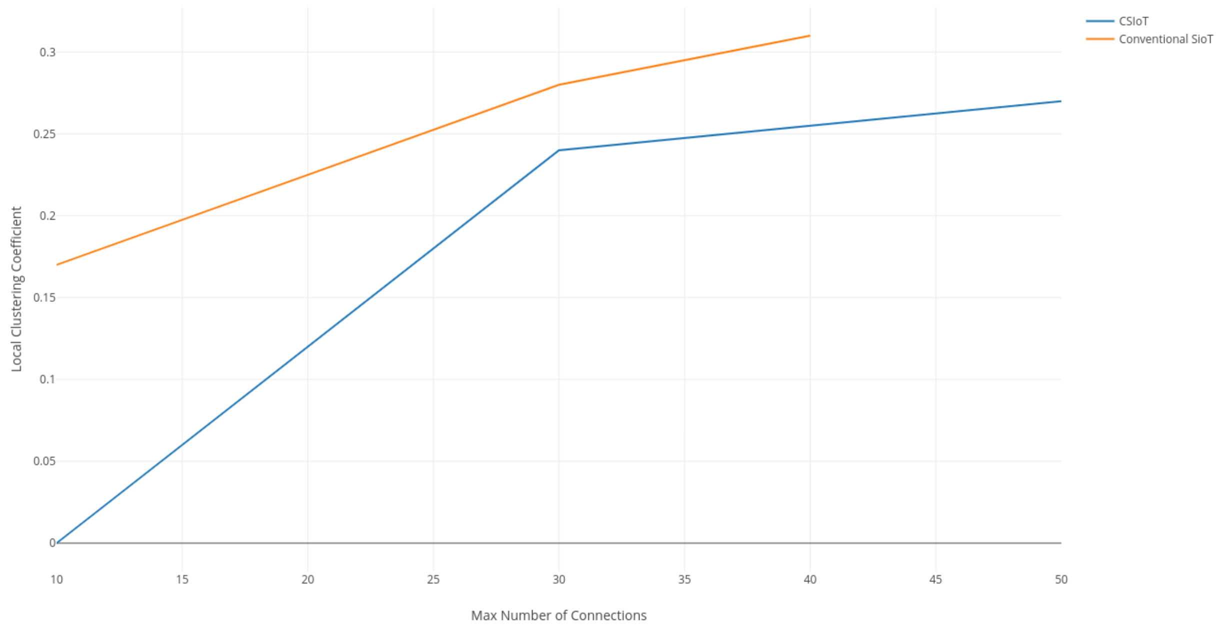


Figure 24. Local clustering coefficient for different max number of connections

The last factor for evaluating the CSIoT framework was the local clustering coefficient for a different max number of connections, which indicates a network's navigability performance. Figure 24 shows that CSIoT outperforms the conventional SIoT in terms of network navigability and managing the friendships and path among them.

The evaluation results demonstrated that the CSIoT framework performs well in service management, friendship management, and network navigability. CSIoT can find the most efficient and shortest paths for SD and service acquisition.

4.3. Privacy evaluation results

Table 9 contains the simulation's descriptive information. The study created 500 agents, while 30 malicious agents were added after the 500th step of the simulation. These agents were programed to access the private information (service Type 3 and above) by developing the friendship and maintaining it by satisfying different friendship criteria including similarity, reciprocity and competence. The services were predefined and were representative of typical services in smart cities. These services can be categorized in five areas, including commerce, entertainment, transportation, housing and offices, and municipalities and utilities.

Table 9. Descriptive information about simulation

Number of agents	Number of malicious agents	Total number of exchanged services	Number of Type 1 services exchanged	Number of Type 2 services exchanged	Number of Type 3 services exchanged	Number of Type 4 services exchanged	Number of Type 5 services exchanged	Number of simulation steps
500	30	3000	1000	800	600	400	200	1000

After simulating the CSIoT environment, the study evaluated the effectiveness of proposed friendship development and updated mechanisms in different aspects of privacy. The first aspect was the average time for malicious agents to access sensitive information. The Figure 25 illustrates the average time (in terms of simulation steps) for accessing different amounts of sensitive data in terms of the number of important services (Type 3 and above).

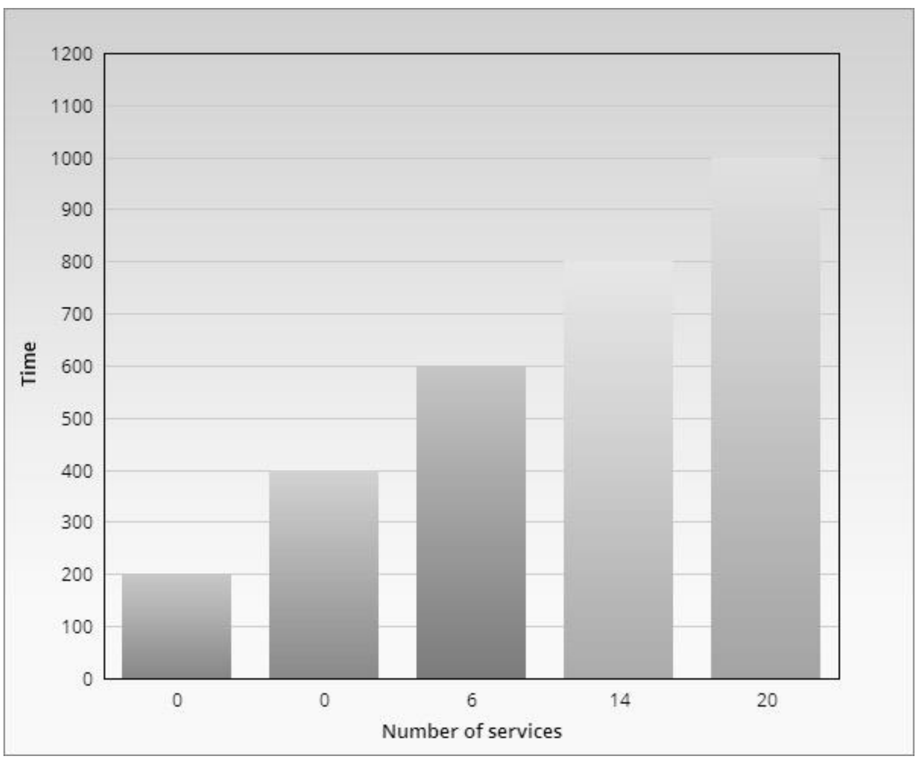


Figure 25. Rate of sensitive information disclosure during the time

These results show that the study's mechanism was very effective in terms of preserving user privacy. Figure 27 demonstrates that malicious agents were not able to access sensitive information until 200 steps of simulation. Between Step 200 to Step 100 total number of important services that were acquired by malicious users was 40, which is only 0.03 percent of the total number of important services. This indicates that the malicious user success rate for privacy violation was very low and such malicious users must spend a long time to access only a few number of important services.

To validate the results, the study also simulated the SIoT environment within a conventional framework (without a friendship leveraging mechanism). Figure 26 shows the results of simulation.

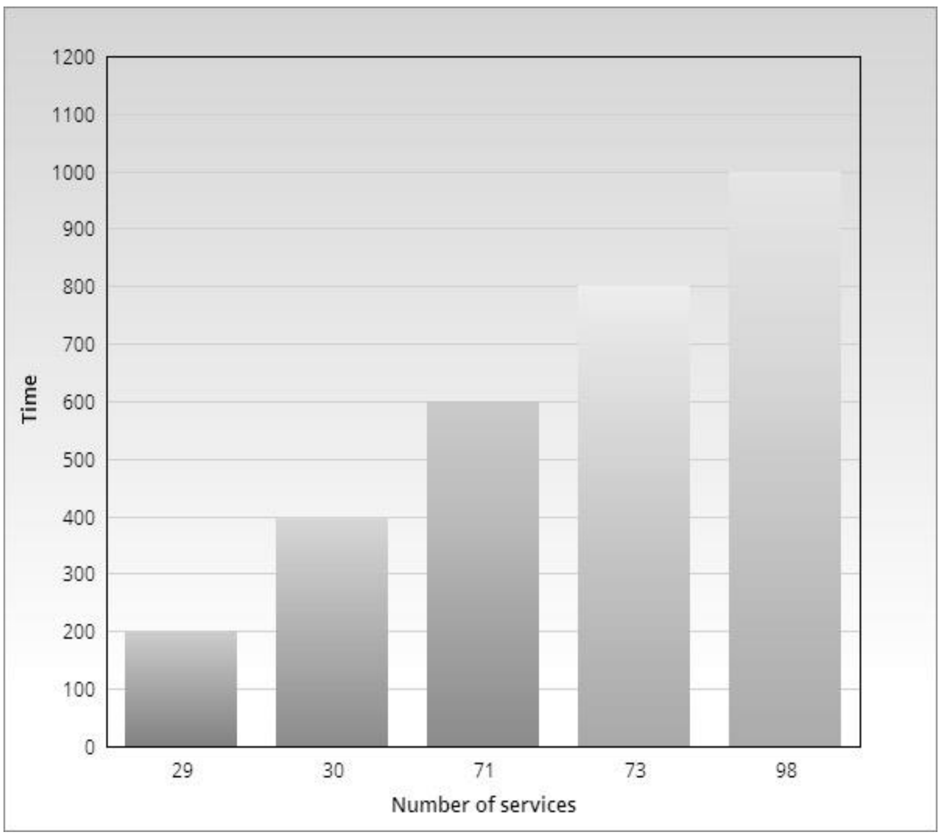


Figure 26. Rate of sensitive information disclosure during the time

These results confirm the effectiveness of CSIoT. The number of important services acquired by malicious agents in conventional SIoT was considerably higher than in CSIoT. The information disclosure began in SIoT even from the first steps, and in total, over 25% of important services were acquired by malicious agents.

4.4 Blockchain-based SIoT evaluation results

In the blockchain-based simulation, the study created 650 agents. The simulation had 1,000 steps and 432 transactions that were performed by agents. Nodes in the overlay were grouped in clusters to reduce the network overhead and delay. Nodes in one cluster, Cluster Head (CH), included a trust rating for other CHs in an overlay network based on direct and indirect evidence (Dorri et al., 2017). Direct evidence was acquired when “CH A” verified a block developed by “CH B”. Indirect evidence referred to the situation where “CH A” had no direct evidence about a block received from “CH B” but other verified CHs verified the validity of that block. A function of the number of successfully verified blocks for the corresponding CH changed the portion of the transactions that needed to be verified. The table below shows an example of this function.

Table 10. Trust table adopted from Dorri et al., 2017

Number of successful verified blocks	20	30	40	50	60
Percentage of transactions should be verified	80%	60%	40%	30%	20%

The study evaluated different overheads after the blockchain-based SIoT simulation. Table 10 indicates the average performance metrics for the key transactions in a blockchain-based SIoT. Next, a network of 650 nodes with 223 CHs was simulated to evaluate the processing and computation overhead in the study framework. Figure 27 shows the simulation results for a blockchain-based SIoT.

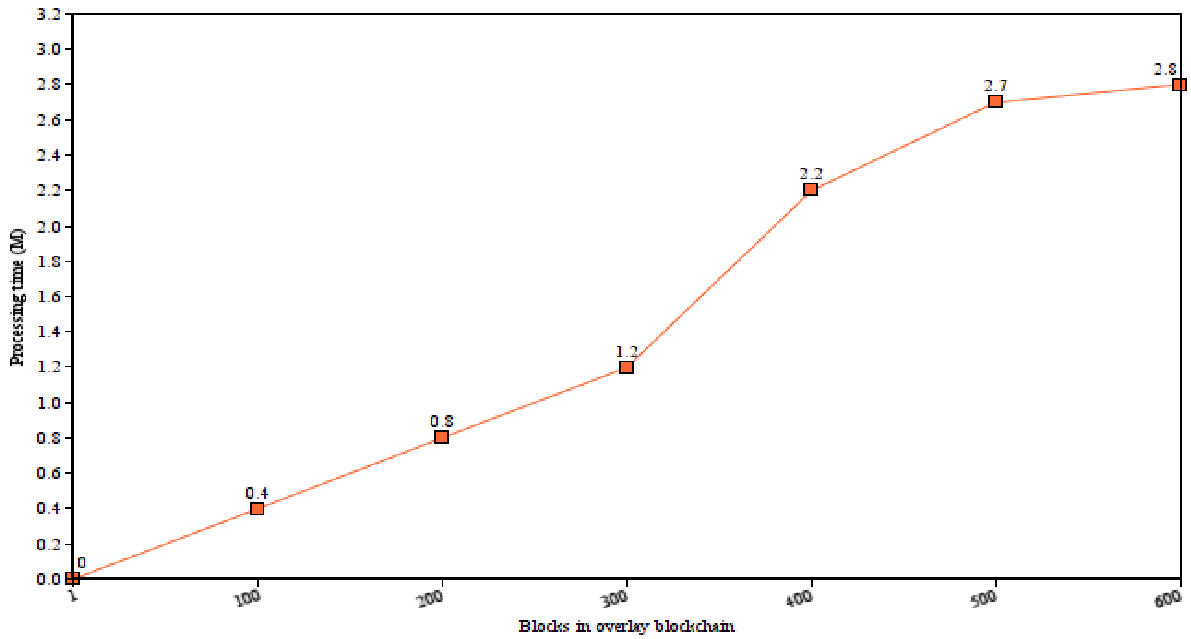


Figure 27. Processing overhead

Comparing these results with the trust table shows that the blockchain-based SIoT performs well in terms of processing time. The processing time increases considerably by adding more blocks because the blockchain-based SIoT processes had not only the smart contracts but also the friendship levels.

Chapter V: Conclusion

5.1 Summary of research and research findings

IoT technology is growing quickly and its growth is a transformative force across all modern organizations. According to the *Business Insider*, the IoT market will grow to over $3 trillion annually by 2026. Technology advancements in IoT create new opportunities and threats, and scientists are working to explore and manage these new IoT challenges.

The growing number of connected smart devices enhances the complexity of IoT settings. This complexity can create new security and privacy concerns, and it can also create new features that are useful for humans. Nowadays, researchers are investigating new models and future generation frameworks for IoT. SIoT is one of these future generation IoT frameworks that uses the social network concepts to define the relationships and interactions between smart objects. SIoT can create new capabilities, such as object discovery functionalities, evaluation of trustworthiness of objects, and the information provided by objects, network navigability, and deployment of value-added services.

One of the important factors in SIoT is its friendship management mechanism. There should be effective methods and criteria for defining the relationship between objects and leveraging the friendships during the time that the objects exchange information and services. The literature review indicates that there is not an effective method that uses comprehensive criteria for friendship development and friendship update in SIoT settings.

This study proposes a new friendship management mechanism for SIoT settings. CSIoT utilizes a new friendship management model for continuously updating the friendships between devices. This study proposed a new friendship development model in SIoT using multi-aspect friendship development factors as well as a new friendship leveraging mechanism to update friendships effectively and to create an effective trust criterion.

The results of the simulation and evaluation of CSIoT show that leveraging friendships and services can improve the SIoT framework from different aspects. First, leveraging enhances the SD and SC in SIoT settings, allowing devices to acquire appropriate services in a shorter time.

Second, leveraging friendships and services can improve the network navigability in SIoT network.

This study uses a fuzzy ontology for semantic reasoning and decision-making in a SIoT environment. The results show that CSIoT outperforms conventional SIoT frameworks that were previously proposed.

IoT has a big impact on our lives by connecting millions of everyday devices. Researchers are working to develop new models, frameworks, architecture, and methods for effective use of this technology and for addressing the potential problems and challenges rising from this technology. One of the proposed future generations of IoT is the Social Internet of Things. In SIoT smart devices can initiate, update and terminate relationships. SIoT uses social network concepts to define the interactions between smart devices.

Privacy is a major issue in IoT settings. There appears to be no study that evaluates privacy in a SIoT environment. This study presents a new simulation tool to evaluate the privacy of the new SIoT environment. The simulation results confirm that the new friendship development and friendship update methods are significantly effective in preserving the privacy of device owners. When comparing the privacy-preserving ability in both conventional SIoT and CSIoT, the results demonstrated that CSIoT out performs conventional SIoT in terms of protecting users' privacy.

CSIoT can also improve the privacy in IoT settings by continuous leveraging of friendships. Effective friendship updates can create useful trust criteria for smart objects in IoT. Therefore, they can share information with different levels of privacy with friends with different levels of trust.

IoT technology provides various value-added services and innovative applications for end users. IoT also has potential challenges and issues that should be addressed. Because of the centralized structure of the IoT there are several security and privacy issues to be addressed. By integrating IoT and blockchain, these problems can be managed and mitigated. Several studies integrate IoT and blockchain but there does not seem to be any study that integrates the SIoT and blockchain.

This study proposed a new framework for SIoT that includes a new friendship development and friendship update models and then integrated the blockchain and SIoT by defining smart contracts and transactions. A blockchain-based SIoT was simulated using MAS modeling. The simulation results show that the integration of SIoT and blockchain is effective in improving the device owner's privacy and it outperforms the conventional SIoT framework.

5.2 Answers to research questions

The research questions and answers to these questions are listed as follows:

1.What complexity concepts can we use to define IoT settings as complex systems? Is it useful to consider IoT as a complex system?

Before designing the new framework for SIoT, the IoT setting is defined as a complex system. The complexity concepts that are mentioned in the dissertation, are used for exploring the IoT or SIoT and for designing different components of CSIoT including agents, connections and service discovery and the friendship between devices. The general evaluation results show that CSIoT performs well and it is better than conventional SIoT in terms of latency and probability distribution.

2. What are the important friendship initiation factors that are not considered in the SIoT literature? How can we use them with other factors to have a multi-criteria friendship selection process in SIoT?

This study has used multi-criteria for friendship selection in SIoT. We have extended the existing friendship selection criteria by considering similarity, proximity, and reciprocity. This study uses broader definition for this factors and it uses every possible reason for friendship selection in SIoT. The general evaluation results show that CSIoT performs well and it is better than conventional SIoT in terms of latency and probability distribution and path length.

3. How can we define a new effective friendship updating and friendship leveraging mechanism in SIoT that considers time and other important factors in device friendship like reciprocity?

This study has developed a new method for updating the friendship by considering different factors including time. So the agents are able to update the friendship level during the time by considering multi-criteria approach. The general evaluation results show that CSIoT performs well and it is better than conventional SIoT in terms of latency and probability distribution and path length.

4. How can we evaluate the new SIoT (CSIoT) framework?

This study proposes a new simulation tool that is developed based on multi-agent system modeling. This tool can simulate the SIoT environment by considering the main concepts included in fuzzy ontology.

5. How can we investigate privacy in SIoT environments and specifically, how can we investigate and evaluate the privacy in the proposed SIoT framework (CSIoT)? This study has investigated the privacy in SIoT setting specifically, in CSIoT environment. We have evaluated the privacy by comparing the privacy preserving ability in both CSIoT and conventional SIoT. The results of evaluation show that CSIoT is better than conventional SIoT in terms of protecting privacy and sensitive data.

6. Can we integrate blockchain and SIoT to address some of the security of SIoT including the centralized structure?

This study integrates blockchain and CSIoT to address the general security problems of SIoT environment. This study proposes an experimental framework for this integration. The results of evaluation show that the integration is successful.

Table 11 shows the research questions, corresponding kernel theories, corresponding artifacts and results.

Table 1. Summary of the design science research components

Research questions	Kernel theories	Artifact	Results
1	Complexity science, Complex systems	Fuzzy ontology	The results of Path length, clustering coefficient, and latency show that CSIoT performs

			well
2	Friendship development factors in social networks,	New friendship development model	Simulation results (Path length, clustering coefficient, and latency) show that CSIoT outperforms conventional SIoT
3	Knapp's relational stage theory,	New friendship and service leveraging model	Simulation results (Path length, clustering coefficient, and latency) show that CSIoT outperforms conventional SIoT
4	Virtualization, multi-agent systems modelling	CSIoT Simulation tool	CSIoT environment is simulated using new simulation tool
5	Trust evaluation in friendship, multi-	CSIoT simulation	Comparison of CSIoT

	agent systems modelling	tool	and conventional SIoT shows that CSIoT performs better than conventional SIoT in protecting device owner privacy
6	multi-agent systems modelling, blockchain architecture can enhance the IoT security	Experimental framework for blockchain-based CSIoT	Blockchain-CSIoT performs well in terms of processing overhead

5.3 Significance

This study addresses an important gap in SIoT literature by proposing a new friendship development model and a new method for updating friendships in SIoT environment. We also develop a new simulation tool (CSIoT) for simulation and evaluation the SIoT and the methods proposed in this study.

This study will target a broad range of audiences. These audiences will include researchers in different disciplines such as computer science, electrical engineering and information systems. Social IoT is a trending research topic and it is considered as a new paradigm in IoT research. In addition, this paper will be useful for the practitioners who want to develop new IoT frameworks and architectures for their business. This study will provide information about developing new generation of IoT that has several new capabilities and it is able to address new privacy and security issues.

5.4 Future work

In future work we want to expand this study from two aspects. First of all, we want to simulate different common and possible security and privacy issues in SIoT and develop new methods in CSIoT framework to address these issues. Second, we want to propose a detailed framework of blockchain-based CSIoT with public and private blockchain architecture to enhance the security of CSIoT. In this study we showed that the integration of CSIoT and blockchain is successful but we did not evaluate the experimental framework for specific security and privacy issues. Therefore, in future work we will consider different scenarios to evaluate the blockchain-based CSIoT in addressing security and privacy.

References

Aboud, F. E., & Mendelson, M. J. (1996). Determinants of friendship selection and quality: developmental perspectives. in W. M. Bukowski, A. F. Newcomb, & W. W. Hartup (eds.), Cambridge studies in social and emotional development. the company they keep: friendship in childhood and adolescence (pp. 87-112). New York, ny, US: Cambridge university press.

Ahmad W. Atamli and Andrew Martin, Threat-Based Security Analysis for the Internet of Things, 2014 International Workshop on Secure Internet of Things.

Aimad Karkouch, Hajar Mousannif, Hassan Al Moatassime, Thomas Noel, “Data quality in Internet of things: A state-of-the-art survey”. Journal of Network and Computer Applications 73 (2016) 57–81

Arbia Riahi, Enrico Natalizioy, Yacine Challaly, Nathalie Mittonz & Antonio Iera (2014), “A systemic and cognitive approach for IoT security”, International Conference on Computing, Networking and Communications (ICNC).

Ana Mari Cauce 1986. “Social networks and social competence: Exploring the effects of early adolescent friendships”. American Journal of Community Psychology. December 1986, Volume 14, Issue 6, pp 607–62.

Anderson, P.W., Arrow, K.J. and Pines, D. (eds.) (1988). The Economy as an Evolving Complex System, Reading, MA: Addison-Wesley.

Andrew Whitmore, Anurag Agarwal & Li Da Xu (2015), “The Internet of Things—A survey of topics and trends”, Information systems frontiers, 17, 261-274

Antonio M. Ortiz, Dina Hussein, Soochang Park, Son N. Han, and Noel Crespi (2014), “The Cluster Between Internet of Things and Social Networks: Review and Research Challenges”, IEEE Internet of Things Journal, Vol. 1, No. 3.

Arthur, W.B., Durlauf, S.N. and Lane, D.A. (eds.) (1997). The Economy as an Evolving Complex System, Proceedings of the Santa Fe Institute, Vol. XXVII. Reading, MA: Addison-Wesley.

Attitudes on data protection and electronic identity in the European Union Special barometer 359, European Commission, Directorate-General for Communication, Brussels (2011).

A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for Smart Cities,” IEEE Internet of Things Journal, vol. 1, no. 1, 2014, pp. 22—32.

Barboutov, K.; Furuskär, A.; Inam, R.; Lindberg, P.; Öhman, K.; Sachs, J.; Sveningsson, R.; Torsner, J.; Wallstedt, K. Ericsson Mobility Report. Available online: https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf (accessed on 30 March 2018).

Bill McKelvey, Huseyin Tanriverdi and Yoyungjin Yoo, 2016, Call for papers MISQ special issue on “Complexity and Information SystemsResearch in the Emerging Digital World”.

Buhrmester, D. (1998). Need fulfillment, interpersonal competence, and the developmental contexts of early adolescent friendship. In W. M. Bukowski, A. F. Newcomb, & W. W. Hartup (Eds.), Cambridge studies in social and emotional development. The company they keep: Friendship in childhood and adolescence (pp. 158-185). New York, NY, US: Cambridge University Press.

Clark, M., & Pataki, S. (1995). Interpersonal processesinfluencing attraction and relationships. In A. Tesser(Ed.), Advanced social psychology (pp. 283–331).St. Louis: McGraw Hill.

Cowan, GA, Pines, D and Meltzer, D. (eds). (1994). Complexity: Metaphors, models, and reality, Proceedings of the Santa Fe Institute, Vol. XIX, Reading, MA: Addison-Wesley.

Cramer, F. (1993). Chaos and Order: The Complex Structure of Living Things (trans. D. L. Loewus) New York: VCH.

Crawford, G. C., H. Aguinis, B. Lichtenstein, P. Davidsson, & B. McKelvey 2015. “Power law distributions in entrepreneurship: Implications for theory and research.” Journal of Business Venturing,” [In press].

David Goad & Uri Gal, “IoT Design Challenges and the Social IoT Solution”, Twenty-third Americas Conference on Information Systems, Boston, 2017.

Denise B. Kandel, "Homophily, Selection, and Socialization in Adolescent Friendships," American Journal of Sociology 84, no. 2 (Sep., 1978): 427-436.

Dorri A, Kanhere S Salil, Jurdak Raja, “Towards an Optimized BlockChain for IoT”, IoTDI 2017, April 2017, Pi,sburgh, PA USA.

Feng Xia, Li Liu, Jie Li, Jianhua Ma, and Athanasios V. Vasilakos (2015), “Socially Aware Networking: A Survey”, IEEE Systems Journal, Vol. 9, No. 3.

Fernandez and Pallis, 2014, Opportunities and challenges of the Internet of Things for healthcare, IEEE international Conference on Wireless Mobile Communication and Healthcare.

Granovetter, M. 1973 “The strength of weak ties.” American Journal of Sociology, 78: 1360–1380.

Haken, H. 1983. Synergetics, An Introduction (3rd ed.). Springer-Verlag, Berlin.

Gu J., Sun B., Du X., Wang J., Zhuang Y., Wang Z. Consortium blockchain-based malware detection in mobile devices IEEE Access, 6 (2018), pp. 12118-12128.

Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst. 2013, 29, 1645–1660.

Hevner, A.R.; March, S.T.; and Park, J. Design research in information systems research. MIS Quarterly, 28, 1 (2004), 75–105.

Holland, J. H. 1988. “The global economy as an adaptive system.” In P. W. Anderson, K. J. Arrow & D. Pines (eds.), The Economy as an Evolving Complex System, Vol. 5. Reading, MA: Addison- Wesley, 117–124.

J.A. Morente-Molinera, R.Wikström, E. Herrera-Viedma, C. Carlsson (2016), “A linguistic mobile Decision Support System based on fuzzy ontology to facilitate knowledge mobilization”, Decision Support Systems 81 (2016) 66–75.

James Y.L. Thong (1999), An Integrated Model of Information Systems Adoption in Small Businesses, Journal of Management Information Systems, 15:4, 187-214.

Jelle R. Kok & Nikos Vlassis, “Sparse Cooperative Q-learning”, Proceedings of the 21 st International Confer- ence on Machine Learning, Ban, Canada, 2004.

Jesse Fox, Katie M. Warber, and Dana C. Makstaller 2013. “The role of Facebook in romantic relationship development: An exploration of Knapp’s relational stage model”. Journal of Social and Personal Relationships. 30(6) 771–794.

Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos (2017), Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions, IEEE Communications Magazine, Volume: 55, Issue: 1, P:26 – 33

Kauffman, S. A. 1993. The Origins of Order. New York: Oxford University Press.

Knapp, M. L. (1978).Social intercourse: From greeting to goodbye. Needham Heights, MA, USA:Allyn & Bacon.

Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. Comput. 2017, 50, 80–84.

Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin (Sherman) Shen, “Security and Privacy in Smart City Applications: Challenges and Solutions”, IEEE Communications Magazine, January 2017.

Lars Backstrom, Eric Sun and Cameron Marlow 2010. “Find me if you can: improving geographical prediction with social and spatial proximity”. Proceedings of the 19th international conference on World wide web, Pages 61-70

Lemuria Carter and Vishanth Weerakkody (2008), “E-government adoption: A cultural comparison”, Information Systems Frontiers, Volume 10, Issue 4, pp 473–482.

Liesbetvan Zoonen, “Privacy concerns in smart cities”, Government Information Quarterly

Volume 33, Issue 3, July 2016, Pages 472-480.

Linda Rose-Krasnor 2006. “The Nature of Social Competence: A Theoretical Review”. Social development. Volume6, Issue1.

Li X, Lu R, Liang X, Shen X, Chen J, Lin X. Smart community: an internet of things application. Communications Magazine, IEEE Nov 2011;49(11):68e75.

Lorenz, E. N. 1972. "Predictability: Does the flap of a butterfly's wings in Brazil set off a tornado in Texas?" Paper presented at the 1972 meeting of the American Association for the Advancement of Science. Washington, DC.

Luigi Atzori, Antonio Iera, and Giacomo Morabito (2011), "MAKING THINGS SOCIALIZE IN THE INTERNET– DOES IT HELP OUR LIVES?", ITU-T Kaleidoscope academic conference.

Luigi Atzori, Antonio Iera & Giacomo Morabito (2014), "From "Smart Objects" to "Social Objects": The Next Evolutionary Step of the Internet of Things", IEEE Communications Magazine, January 2014, 97-105.

Luigi Atzori, Antonio Iera, Giacomo Morabito & Michele Nitti (2012), "The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization", Computer Networks 56 (2012) 3594–3608.

Maarten Selfhout William Burk Susan Branje Jaap Denissen Marcel Van Aken Wim Meeus 2010 "Emerging Late Adolescent Friendship Networks andBig Five Personality Traits: A Social Network Approach". Journal of personality. Volume 78, Issue 2, Pages 509-538.

Martin Pinquart, Silvia Sörensen 2000 "Influences of Socioeconomic Status, Social Network, and Competence on Subjective Well-Being in Later Life: A Meta-Analysis". Psychology and Aging, 15(2), 187-224.

Mainzer, K. (1994). Thinking in Complexity: The Complex Dynamics of Matter, Mind, and Mankind (4th edn), New York: Springer-Verlag (published in 2004).

Maurits de Klepper, Ed Sleebos, Gerhard van de Bunt, Filip Agneessens 2010, "Similarity in friendship networks: Selection or influence? The effect ofconstraining contexts and non-visible individual attributes". Social Networks 32 (2010) 82–90.

M Nitti, L Atzori, IP Cvijikj. "Friendship selection in the social Internet of things: challenges and possible strategies". IEEE Internet Things J, 2 (June (3)) (2015), pp. 240-247

M. Ul Hassan, M.H. Rehmani and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions", Future Generation Computer Systems 97 (2019) 512–529.

Nakamoto S. Bitcoin: A peer-to-peer electronic cash system (2008) (online), http://bitcoin.org/bitcoin.pdf

Newsroom, G. Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018. Available online: https://www.gartner.com/newsroom/id/3869181 (accessed on 30 March 2018).

Olivera Marjanovic, Dubravka Cecez-Kecmanovic (2017), “Exploring the tension between transparency and datification effects of open government IS through the lens of Complex Adaptive Systems”, Journal of Strategic Information Systems 26 (2017) 210–232.

Panagiotis Kasnesis, Charalampos Z. Patrikakis, Dimitris Kogias, Lazaros Toumanidis, Iakovos S. Venieris (2017), “Cognitive friendship and goal management for the social IoT”, Computers and Electrical Engineering 58 (2017) 412–428.

Panarello A, Tapas N, Merlino G, Longo F and Puliafito A, “Blockchain and IoT Integration: A Systematic Survey”, Sensors 2018, 18(8), 2575.

Pijush Kanti Dutta Pramanik, Saurabh Pal and Prasenjit Choudhury (2018), “Beyond Automation: The Cognitive IoT. Artificial Intelligence Brings Sense to the Internet of Things”, Lecture Notes on Data Engineering and Communications Technologies 14.

Pines, D. (ed.) (1988). Emerging Syntheses in Science, Proceedings of the Santa Fe Institute, Vol. I. Reading, MA: Addison-Wesley.

P. Kasnesis, C.Z. Patrikakis, D. Kogias, L. Toumanidis, I.S. Venieris, Cognitive friendship and goal management for the social IoT, Comput. Electr. Eng. 58 (2017) 412–428.

Prisco G. Slock. it to introduce smart locks linked to smart ethereum contracts, decentralize the sharing economy Bitcoin Mag. (Nov) (2015).

Prigogine, I. (with I. Stengers) 1997. The End of Certainty. New York: Free Press.

P. Neirotti et al., “Current Trends in Smart City Initiatives: Some Stylised Facts,” Cities, vol. 38, 2014, pp. 25–36.

Puthal D., Malik N., Mohanty S.P., Kougianos E., Das G., “Everything you wanted to know about the blockchain: Its promise, components, processes, and problems”, IEEE Consumer Electron. Mag., 7 (4) (2018), pp. 6-14.

Qihui Wu, Guoru Ding, Yuhua Xu, Shuo Feng, Zhiyong Du, Jinlong Wang, and Keping Long (2014), Cognitive Internet of Things: A New Paradigm Beyond Connection, IEEE Internet of Things Journal, VOL. 1, NO. 2.

R. Benabdessalem, M. Hamdi, Tai-Hoon Kim, A Survey on Security Models, Techniques, and Tools for the Internet of Things 7th International Conference on Advanced Software Engineering & Its Applications, 978-1-4799-7761-1/14 2014 IEEE.

Reyna A, Martín C, Chen J, Soler E and Díaz M, “On blockchain and its integration with IoT. Challenges and opportunities”, Future Generation Computer Systems, Volume 88, November 2018, Pages 173-190.

Richard Vidgen & Xiaofeng Wang (2009), “Coevolving Systems and the Organization of Agile Software Development”, Information Systems Research, 20, 3.

Rivera MT, Soderstrom SB, Uzzi B (2010) Dynamics of dyads in social networks: As-sortative, relational, and proximity mechanisms.Annu Rev Sociol36:91–115.

Roman, R., Najera, P., & Lopez, J. (2011b). Securing the Internet of Things. IEEE Computer, 44(9), 51–58.

S. Calegari, D. Ciucci, Fuzzy ontology, fuzzy description logics and fuzzy-owl, Applications of Fuzzy Sets Theory 4578 (2007) 118–126.

Schutte, J. G., & Light, J. M. (1978). The relative importance of proximity and status for friendshipchoices in social hierarchies.Social Psychology, 41,260–264

S. Gregor, D. Jones, The anatomy of a design theory, Journal of the Association for Information Systems, 8(5) (2007) 312.

Shancang Li, Li Da Xu & Shanshan Zhao (2015), “The Internet of things: a survey”, Information systems frontiers, 17, 243-259

Sias, P. M., & Cahill, D. J. (1997). From coworkers to friends: The development of peer friendships inthe workplace.Western Journal of Communication, 62,273–299.

S.Sicaria, RizzardiaL, Griecob & Coen-Porisini (2015), “Security, privacy and trust in Internet of Things: The road ahead”, Computer networks, 76, 146-164.

Sicari, S.; Rizzardi, A.; Cappiello, C.; Miorandi, D.; Coen-Porisini, A. Toward data governance in the Internet of things. In New Advances in the Internet of Things; Springer: Cham, Germany, 2018; pp. 59–74.

Sky Matthews (2016), “What is cognitive IoT?”, www.ibmbigdatahub.com.

S. Rosenblatt, "Google's self-driving car turns out to be a very smart ride", 2014.

Stephen Leider, Markus M. Möbius, Tanya Rosenblat, Quoc-Anh Do; Directed Altruism and Enforced Reciprocity in Social Networks, The Quarterly Journal of Economics, Volume 124, Issue 4, 1 November 2009, Pages 1815–1851

Sushmita Mitra, Kishori M. Konwar, & Sankar K. Pal (2002), Fuzzy Decision Tree, Linguistic Rules and Fuzzy Knowledge-Based Network: Generation and Evaluation, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 32, NO. 4.

S. Kosta, A. Mei, J. Stefa, Small world in motion (SWIM): modeling communities in ad-hoc mobile networking, in: Proc. of IEEE SECON 2010, June 2010.

Tschorsch F., Scheuermann B., “Bitcoin and beyond: A technical survey on decentralized digital currencies”, IEEE Commun. Surv. Tutor., 18 (3) (2016), pp. 2084-2123.

Veena P., Panikkar S., Nair S., Brody P. Empowering the edge-practical insights on a decentralized Internet of things Empowering the Edge-Practical Insights on a Decentralized Internet of Things, vol. 17, IBM Institute for Business Value (2015).

Wazir Zada Khan, Mohammed Y Aalsalem, Muhammad Khurram Khan, Quratulain Arshad (2017), “When social objects collaborate: Concepts, processing elements, attacks and challenges”, Computers and Electrical Engineering 58 (2017) 397–411.

W. Trappe, R. Howard, and R. S. Moore, “Low-energy security: Limits and opportunities in the Internet of Things,” IEEE Security Privacy, vol. 13, no. 1, pp. 14–21, Jan./Feb. 2015.

Yan, T., & Wen, Q. (2012). A trust-third-party based key management protocol for secure mobile RFID service based on the Internet of Things. In H. Tan (Ed.), Knowledge discovery and data mining, AISC 135 (pp. 201–208). Berlin: Springer.

Yasmin Merali (2006), “Complexity and Information Systems: the emergent domain”, Journal of Information Technology, 21, 4.

Yasmin Merali and Bill McKelvey, 2006, Introduction to the Special Issue Using Complexity Science to effect a paradigm shift in Information Systems for the 21st century, Journal of information technology, 21

Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao (2017), “A Survey on Security and Privacy Issues in Internet-of-Things”, IEEE Internet of things journal, 4, 5.

Yu Zhang and Jiangtao Wen, “The IoT electric business model: Using blockchain technology for the Internet of things”, Peer-to-Peer Networking and Applications, July 2017, Volume 10, Issue 4, pp 983–994.