Multi-Context-based Trust Management Framework and Simulator for Social Internet of Things

Meriem Chiraz Zouzou

A thesis submitted in partial fulfilment of the requirements of Staffordshire University for the degree of Doctor of Philosophy

Staffordshire University

School of Computing and Digital Technologies

United Kingdom

March 2024

ACKNOWLEDGEMENTS

Initially, I want to extend my sincerest appreciation to Prof. Elhadj Ben Khalifa, my supervisor, whose unwavering encouragement, motivation, and significant contributions greatly facilitated the success of this thesis. With his continuous support, this achievement became possible.

I am sincerely thankful to Dr. Dave Dyke and Prof. Hishem Kholidy, my esteemed supervisors, for their unwavering support and guidance throughout my doctoral journey.

I am profoundly grateful to Dr. Asma Adnane for her consistent support throughout my PhD journey. Her guidance and insights have played a crucial role in determining the direction of my research.

I am indebted to my parents, Mr. Farid and Ms. Souad, for not only providing the financial support necessary for my Ph.D., but also for their unwavering encouragement. Their belief in my academic pursuits has been a constant source of inspiration.

My sincere thanks to my husband for his constant support and understanding during the challenges I encountered throughout my PhD research. His presence was a pillar of strength during my most difficult times.

Lastly, I am grateful to express my appreciation to those who believed in my dreams and shared in my achievements. Their belief has been a driving force, and I am truly thankful for their support.

Abstract

The rise of the Social Internet of Things (SIoT) brings forth new challenges in trust management within interconnected device networks. This thesis endeavours to address these challenges by developing and validating a novel Multi-Context-based Trust Management (MCTM-SIoT) framework tailored specifically for SIoT environments. The framework aims to enhance trust assessment by incorporating diverse contextual information into the final evaluation of each node within the SIoT network. This approach enables the selection of the most trustworthy Service Provider (SP) even in the absence of prior behavioural history from the node.

The research objectives encompass a thorough investigation of various research areas, including IoT, SIoT, and trust management in SIoT environments. These investigations pave the way for the development of an MCTM-SIoT framework and model specifically tailored for SIoT. Additionally, a novel SIoT simulator is developed to generate diverse SIoT scenarios and produce realistic datasets, facilitating the evaluation of the proposed framework and model's performance and scalability across different scenarios.

The contributions of this research are manifold. Firstly, it introduces a new MCTM-SIoT framework that elucidates the relationship between different SIoT components and trust management. Additionally, the framework incorporates multiple contextual information into the final trust score of each node in the SIoT network to facilitate trustworthy inference, thereby enhancing the overall security and reliability of the system by selecting the most reliable Service Provider. Secondly, a scalable MCTM-SIoT model is developed, to identify the most trustworthy service provider based on a set of trust contextual metrics, namely user context trust metrics (UCT), device context trust metrics (DCT), environmental context trust metrics (ECT), and task context trust metrics (TCT). Thirdly, a novel simulation tool is designed to simulate diverse SIoT scenarios, generating realistic datasets crucial for testing and evaluating the proposed framework and model. Finally, a proof of concept is developed to demonstrate the efficacy of the MCTM-SIoT framework and model in SIoT environments using the generated datasets and employing machine learning techniques. Testing of the framework demonstrates that the impact of context on SIoT trustworthiness grows with the level of dynamism and complexity of the SIoT environment, highlighting the importance of considering contextual factors in trust management strategies for SIoT.

In summary, this research contributes significantly to the field of SIoT by providing a comprehensive framework for trust management that addresses the dynamic nature of contextual information. The developed framework and model offer promising solutions to the challenges posed by trust assessment in SIoT environments, paving the way for enhanced security and reliability within interconnected device networks.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

SIoT	Social Internet of Things
IoT	Internet of Things
SN	Social Network
TM	Trust Management
TMS	Trust Management Systems
SOA	Service-Oriented Architecture
DSR	Research Design Science
SP	Service Provider
SR	Service request
ML	Machine Learning
H2H	Human To Human
T2T	Things to Things
H2T	Human To Things
POR	Parental Object Relationship
CWOR	Co-Worker Object Relationship
CLOR	Location Object Relationship
OOR	Owner Object Relationship
SOR	Social Object Relationship
BMA	Bad Mouthing Attacks
BSA	Ballot Stuffing Attacks
CA	Collusion Attacks
SPA	Self-Promoting Attack
WA	Whitewashing Attack
OSA	Opportunistic Self-Attack
SA	Sybil Attack

OOA	On-Off Attack
QoS	Quality of Service
OSN	Online Social Networks
DCT	Device Context Trust metrics
UCT	User Context Trust metrics
TCT	Task Context Trust metrics
ECT	Environmental Context Trust metrics
CoI	Community of Interest
OR	Object Relationship
M2M	Machine to Machine

List of Publications

Zouzou, M.C., Benkhelifa, E., Kholidy, H. and Dyke, D.W., 2023, June. Multi-Context-aware Trust Management framework in Social Internet of Things (MCTM-SIoT). In *2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS)* (pp. 99-104). IEEE.

Zouzou, M.C., Shahawy, M., Benkhelifa, E. and Kholidy, H., 2023, October. SIoTSim: Simulator for Social Internet of Things. In *2023 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* (pp. 149-155). IEEE.

Chapter 1

Introduction

1.1. Introduction

Technology has become a fundamental component of our modern society. The Internet of Things (IoT) is a concept that links physical objects with the digital realm. with the digital world to enable the development of intelligent applications and infrastructure. By allowing various smart objects, including wearables, sensors, smartphones, cars, and computers, to communicate with one another using specific addressing schemes and communication protocols. This connection promotes cooperation and collaboration in the pursuit of a common goal.

According to Domingo (2012) and Shammar and Zahary (2020), the innovative solutions offered by these connected objects are enabled by their collective intelligence, which is responsible for a paradigm shift in user experience. Despite the many advantages of IoT across a variety of applications, it also presents several challenges when planning and building IoT infrastructures including trust management, network navigability and service discovery (Sisinni *et al.,* 2018). Additionally, current solutions face limitations due to the sheer number of objects involved (Zhang, Wen and Fan, 2014).

To extend the current solution, one possible solution is to mimic human sociological behaviour. The idea of social relationships makes it easier for human societies to form around shared needs and interests, even though humans are diverse, complex and dynamic. The small world phenomenon initially proposed by Jon Kleinberg, describes the short chains of connections that link individuals within social networks, thereby enhancing information discovery among people (Kleinberg, 2000). The integration of Social Networks (SN) into the IoT has been the subject of recent research by academic and industrial researchers (Ning and Wang, 2011; Guinard, Fischer and Trifa, 2010). Furthermore, Holmquist *et al.* (2001) proposed the concept of object socialisation and a technique for building relationships between objects through close proximity.

The Social Internet of Things (SIoT) paradigm involves integrating SN concepts into the IoT, allowing any object to record environmental features and establish connections with other objects within the network. As a result, the social objects are equipped with advanced capabilities that enable them to function autonomously. These objects are capable of collaborating with one another, developing their own social networks, and maintaining social relationships and communities. This enables them to make intelligent decisions independently without the intervention of human beings.

SIoT has the potential to address a number of research challenges, including service discovery, social relationship management between intelligent social objects, network navigation by leveraging object relationships to exploit smart world phenomena, and trust management (Nitti *et al.,* 2016). The social aspects of SIoT have created opportunities for the development of the next generation of IoT, enabling service discovery through social relationships with nearby objects. However, reliability and trust issues associated with these social objects present a significant risk to the importance of the SIoT (Cai *et al.,* 2016).

Multiple service providers can offer to provide the requested service when an object in the SIoT makes a service request. Since in such a case the requester would select the service provider with the highest level of trust. However, the reliability of the providers is crucial. In addition, trust is an important concern for the successful deployment of SIoT services.

In the realm of SIoT networks, certain entities intentionally disrupt the network's fundamental operations for their own gains. Adding complexity to the issue, these entities diminish the reputation of properly functioning objects while bolstering the credibility of those behaving maliciously (Fan et *al.,* 2019; Bahutair, Bouguettaya and Neiat, 2022). Addressing misbehaving nodes that could disrupt network functionalities, an efficient trust management (TM) system in SIoT, which incorporates contextual information in trust evaluation due to the dynamic nature of SIoT is essential. This ensures the integrity of the information provided by these objects by limiting the functions of these nodes and choosing dependable and trustworthy objects.

1.2. Background of the study

The concept of the SIoT involves the convergence of social networking technologies and the IoT to create a more connected and interactive network of devices and users (Alam *et al.,* 2022). IoT is a concept that refers to the interconnectedness of objects and devices via the internet, enabling communication and data exchange without human intervention. These devices are collected from everyday items such as watches, phones, and household appliances to more specialised items such as industrial machinery, and medical devices (Hassan *et al.,* 2020). Social networking technologies facilitate online interaction and connections between individuals. Through the collaborative exchange of knowledge, insights, and resources, these innovations have transformed the way humans interact, communicate, and share information, while opening up new business, government, and personal opportunities (Deshpande *et al.,* 2015). As a result, SIoT leverages both SN and IoT to establish a more dynamic and interconnected network of humans and things. SIoT facilitates more meaningful and collaborative interactions between humans and their devices by enabling the sharing of resources, experiences, and insights, along with socially intelligent interaction. Numerous areas of life, such as healthcare, education, transportation, and entertainment, stand to be completely transformed by this technology. Furthermore, it raises concerns regarding security, privacy, and data ownership that need to be addressed as technology continues to evolve (Amin, Ahmad and Choi, 2019). The architecture of the SIoT network ensures scalability, service discovery, and network navigability (Abdelghani et *al.,* 2016).

As SIoT environments become more complex and interconnected, the significance of trustworthiness becomes increasingly significant. In SIoT, TM is the process of building, assessing, and maintaining trust between humans and devices. This includes systems for determining the identity of devices and humans and assessing their security and reliability. SIoT poses unique challenges to TM because there is a diverse range of devices and users involved, each with different levels of trustworthiness and security requirements. Additionally, due to the dynamic nature of the SIoT environment, trust levels must be continuously monitored and evaluated. Numerous TM frameworks and models, such as context-based and context-free models, have been proposed for SIoT to address these issues. However, these models generally assess trust scores based on a combination of subjective and objective factors, direct and indirect trust, or incorporate signal or dual contextual information. The concept of trust is still up for debate, especially when it comes to integrating different contextual information into trust assessment to ensure trustworthy communication (Sagar *et al.,* 2023; Khan *et al.,* 2020; Alam *et al.,* 2022). To overcome this issue, a new framework that forwards a trustworthiness inference for SIoT environments could be developed. This framework is based on multiple contextual information to support continuous assessment of the trustworthiness of devices and their interactions in the SIoT network.

1.3. Research motivation

SIoT is an evolving concept in IoT that identifies smart objects as smart entities with social behavioural capabilities. SIoT leverages SN principles to facilitate connections and interactions between objects. SIoT is important because it can meet both user needs and the requirements that IoT inherently presents. Users in SIoT ecosystems may not always have full trust in devices or the information they collect. Additionally, the increasing ubiquity of wearables, social media, and smart homes in the IoT highlights the need to validate the reliability of these devices and the information they collect and process. Likewise, sensitive personal information is often collected and shared by SIoT devices. However, determining device reliability is critical to protecting data security and privacy. There are several reasons that led to the development of a context-based TM framework to determine trustworthiness in SIoT environment. First, the increasingly complex reality of SIoT, characterised by a multitude of devices and users interacting with one another, increases the risk of security breaches. This makes it difficult to build and maintain trust between different network entities. Therefore, a TM framework that evaluates trustworthiness based on the current contextual information helps to guarantee secure communication. Second, traditional TM systems often use predefined and static rules in trust assessment but may not be sufficient for the extremely diverse and dynamic SIoT environment. A contextual TM framework can help mitigate this by considering various contextual information such as device type, location, and time for final trust assessments. Finally, the use of technologies such as machine learning has enabled an accurate validation of TM systems. Thus, using these technologies in a contextual TM framework can improve the accuracy and effectiveness of trust assessments, thereby increasing the overall security and reliability of the SIoT ecosystem.

1.4. Significance of the research

This study conducts a critical review of various relevant topics including SIoT, IoT and TM. The main aim is to develop a novel SIoT framework that demonstrates the relationships between SIoT elements and the TM module as well as to forward a trustworthiness inference for SIoT environments by incorporating different contextual information. IoT devices are increasingly becoming part of everyday life and often collect private data, so protecting this information is essential. Therefore, TM is fundamental to verify the reliability and security of IoT devices and stop illegal data usage. This study provides important new insights into the development of SIoT security standards and schemes necessary to build a reliable infrastructure. The proposed framework makes informed decisions about device trustworthiness by leveraging variable contextual information, including environmental conditions, user behaviour, and device status. The development of this innovative MCTM-SIoT provides valuable insights into the design and implementation of secure and reliable SIoT environments. These insights can benefit industry, government, and individuals using IoT devices and systems in various areas, such as industrial mechanisation, healthcare, transportation, and home automation. Additionally, this innovative SIoT framework helps address privacy concerns related to the collection and use of sensitive data by IoT devices by ensuring that only trusted devices have access. This work has significant implications for secure and trustworthy SIoT systems. It helps establish SIoT security standards and guidelines.

1.5. Research questions

Based on the issues and problems identified in the different studies (Abdelghani *et al.,* 2016; Sagar *et al.,* 2023; Kuseh *et al.,* 2022; Chahal, Kumar and Batra, 2020), privacy concerns in the SIoT are closely related to trust management. A set of research questions have been formulated to address the issues.

The main research question:

1) How can the integration of multi-contextual information advance TM frameworks in SIoT for optimising the selection of trustworthy service providers, while addressing challenges in dynamic network conditions?

Sub-research questions:

2) What is the nature of the relationship between the core components of the SIoT and TM models, and how do these relationships impact network reliability?
3) What are the theoretical foundations and practical considerations for developing a novel TM framework in SIoT that leverages contextual information to improve trust evaluation and decision-making in the selection of trustworthy service provider?

1.6. Aim

This study aims to develop and validate a novel Multi-Context-based Trust Management framework in SIoT environments that incorporates different contextual information in the final trust assessment of each node presented in the SIoT network to select the most trustworthy Service provider in the absence of prior behavioural history from the node.

1.7. Objectives

The specific objectives of this research encompass:

1. To systematically investigate and analyse existing research in the fields of the IoT, SIoT, and TM, identifying key challenges and gaps in multi-contextual trust evaluation mechanisms.

2. To design and develop a MCTM-SIoT framework, illustrating the interconnections between the foundational components of SIoT environments and TM, while integrating contextual factors that enhance decision-making in the selection of trustworthy service providers.
3. To formulate a dynamic MCTM-SIoT model within the developed framework, utilising advanced computational techniques to effectively address the dynamic nature of SIoT environments.
4. To design and develop an innovative SIoT simulator capable of generating realistic datasets, enabling the testing and validation of the MCTM-SIoT model under various scenarios.
5. To conduct a comprehensive evaluation of the performance of the MCTM-SIoT framework and model through the SIoT simulator, employing machine learning algorithms, assessing their effectiveness and adaptability across diverse operational scenarios.

1.8. Research methodology

This research presents the MCTM-SIoT framework as a novel approach within SIoT. The framework is evaluated using a newly developed simulator tool specifically designed for this research. The main aim of the proposed framework is to illustrate the relationship between the SIoT components and trust management as well as infer trustworthiness within SIoT environments by incorporating various contextual information factors including environmental conditions and user behaviour, task type, and device status into the final trust assessment, thus reinforcing the security and privacy aspects surrounding IoT devices. The research design of this research study is based on Design Research Science (DSR). In the field of information systems (IS), DSR represents a robust research design aiming at creating artifacts based on kernel theories. DSR focuses on the creation and evaluation of artifacts or solutions to meet particular requirements and to solve specific practical issues as shown in Figure 1 (Van Der Merwe, Gerber and Smuts, 2017). DSR involves collaboration between researchers and practitioners in a specific area to ensure that the solutions developed are useful and effective. The aim of this research design is to develop efficient and successful solutions to real-world problems. The solutions created through DSR are usually evaluated for their quality and efficiency (Van Der Merwe, Gerber and Smuts, 2017). DSR can be particularly helpful when new technologies need to be developed to address emerging problems or when existing solutions are not sufficient. Therefore, the scope of this research is not limited to practical dimensions. Rather, it draws on both theoretical and practical dimensions to guide the research process. Table 1 assigns the different DSR components to the diverse objectives and sections of this research.

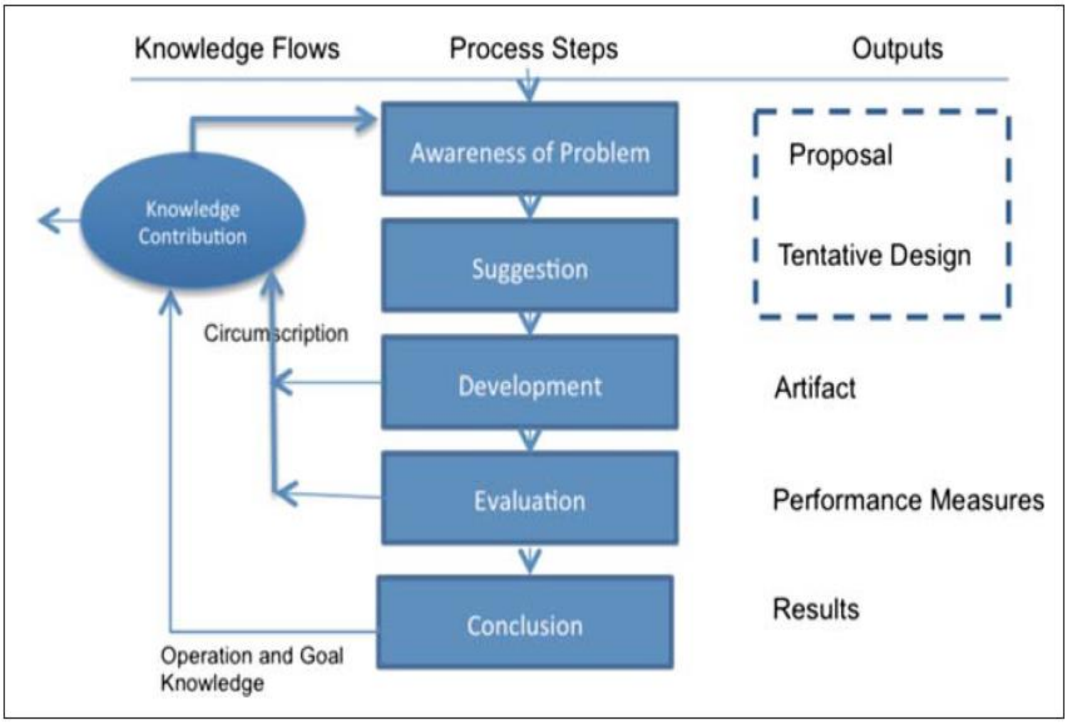


Figure 1 Design Science Search (DSR) process model (Van der Merwe et al., 2017)

Table 1 Design Science Research guidelines

Design Science Research Guidelines	Objectives	Chapters	Thesis Sections
Awareness problem	**Objective 1** To systematically investigate and analyse existing research in the fields of IoT, SIoT, and TM, identifying key challenges and gaps in multi-contextual trust evaluation mechanisms	Chapter 02	Literature Review
Suggestion	**Objective 2** To design and develop a MCTM-SIoT framework for SIoT, illustrating	Chapter 03	Context-Based Trust Management (MCTM-SIoT) Framework

	the interconnections between the foundational components of SIoT environments and TM, while integrating contextual factors that enhance decision-making in the selection of trustworthy service providers.		
Development	**Objective 2,3,4** To formulate a dynamic MCTM-SIoT model within the developed framework, utilising advanced computational techniques to effectively address the dynamic nature of SIoT environments. To design and develop an innovative SIoT simulator capable of generating realistic datasets, enabling the testing and validation of the MCTM-SIoT model under various scenarios	Chapter 03 Chapter 04 Chapter 05	Multi-Context-Awareness Trust Management (MCTM-SIoT) framework and model SIoT-Sim simulator SIoT dataset
Evaluation	**Objective 5** To conduct a comprehensive evaluation of the performance of the MCTM-SIoT framework and model through the SIoT simulator, employing machine learning algorithms, assessing their effectiveness and adaptability across diverse operational scenarios.	Chapter 06	Modelling Simulation Machine Learning
Conclusion		Chapter 07	Recommendation and Future Work

The design cycle for executing DSR includes the following five phases:

1) **Awareness problem**: This aspect is a crucial part of research design as it requires a comprehensive understanding of the state of the art in relevant research areas. This understanding helps to highlight any research gaps that require attention, as well as the successes and limitations of the field (Van der Merwe, Gerber and Smuts, 2017). To address the awareness problem, a systematic literature review was conducted covering multiple research areas such as IoT, SIoT, and TM in SIoT. The aim of this literature review aimed to offer a thorough examination of existing research and to identify any areas where knowledge may be lacking. A MCTM-SIoT framework is one of the research gaps that the literature review uncovered, highlighting the need for a novel artifact that can improve reliability in the highly diverse and dynamic SIoT environment. Additionally, the literature review revealed the need for a more complex TM framework that can take into account contextual

information to make informed decisions about trustworthiness (See chapter 02).

2) **Suggestion:** This is a creative phase in which the identified research gaps are addressed through the execution of an existing element or the creation of a new element (Van der Merwe, Gerber and Smuts., 2017) .The research gap identified in this particular research study is the need for MCTM-SIoT framework. To address this gap, the suggestion involves the development of a theoretical design phase with the aim of offering a general design for a context-based TM framework in SIoT. The theoretical design phase is crucial for the development of the proposed MCTM-SIoT framework. In order to make informed decisions about trustworthiness, this design phase requires the development of a conceptual model that describes the fundamental components of the SIoT environment and their relationship to TM. This also includes the development of a TM module that integrates contextual information (see Chapter 03).

3) **Development**: In order to achieve the research objectives, in this phase, the preliminary design is implemented with different implementation strategies based on the specific artifact to be developed (Van der Merwe, Gerber, and Smuts, 2017). This research study has designed a novel MCTM-SIoT framework and model, as well as a new simulator tool to generate an SIoT dataset.

   i. The development of a MCTM-SIoT (See chapter 03): Developing a MCTM-SIoT framework requires a systematic process that includes two fundamental steps. The first step is to build a comprehensive theoretical model that forms the basis for organising the TM framework. This phase describes the main components of the SIoT ecosystem and how TM fits into it. The next step is to identify the different types of contextual information that need to be considered in the final TM assessment. These scenarios cover a variety of features, such as tasks, user behaviour, device status, and environmental conditions. MCTM-SIoT framework is systematically built through these essential steps and provides a solid foundation for ensuring enhanced security and privacy in the SIoT environment.

ii. The development of the MCTM-SIoT (See chapter 04): In this phase, a comprehensive set of trust metrics and indicators is formulated. These metrics serve as evaluation tools to assess the reliability and credibility of IoT devices and services. By integrating a variety of contextual factors into the trust assessment process, the MCTM-SIoT model aims to improve the accuracy and relevance of trust assessments in SIoT environments.

iii. The development of a new SIoT simulator tool and SIoT dataset (See Chapter 05): The development process of the novel SIoT simulator tool includes a number of essential phases. The first step is to identify the key features and requirements for an effective SIoT simulator tool, such as the ability to simulate a wide range of IoT devices and various SIoT scenarios. Subsequently, the design phase focuses on developing a SIoT simulator tool that has the ability to generate realistic SIoT datasets.

4) **Evaluation**: Once the artifact is created, it is essential to evaluate its performance. This evaluation process is typically based on the requirements and criteria originally presented in the proposal phase (Van der Merwe, Gerber and Smuts, 2017). This phase in any research is crucial because it aims to show demonstrate that the proposed artifact or framework achieves its intended goals. The effectiveness of a MCTM-SIoT framework can be verified using a variety of techniques, such as focus groups, modelling, simulation, and systematic literature review. A systematic literature review requires a thorough analysis of the body of knowledge. This method can be used to find areas where the proposed framework can complement the existing body of knowledge, as well as gaps in the literature. Focus groups involve bringing together a group of interested parties typical of the artilect's target audience and holding discussions and feedback sessions. This method can provide insightful information about the effectiveness, acceptability, and

usability of the framework from the end user's perspective. The modelling process involves creating a computational or mathematical model for the artifact to analyses its functionality and behaviour. This method allows you to predict how the artifact will behave in different scenarios and identify potential problems before they become major problems. Using a simulation-based approach, to create a virtual environment and evaluate it in different scenarios. This method can provide insightful information about the advantages and disadvantages of the artifact and highlight areas in need of development. For this study, modelling, simulation and machine learning techniques are employed in the validation process to evaluate the performance of the model and the proposed TM framework in various scenarios (See chapter 06).

5) **Conclusion**: This is the final phase in which the conclusions and contributions of the research are presented. This includes not only the artifact itself but also the additional insights gained in the process of the study. The result of this phase is a recognised and satisfactory research contributions, a summary of the research results and suggestions for future research directions (Van der Merwe, Gerber and Smuts, 2017). The conclusion of the study provides a general assessment of the proposed framework and its effectiveness in managing trustworthiness in SIoT. It also examines how the stated research objectives were achieved and evaluates the overall effectiveness of the study. Additionally, the conclusion provides recommendations for future research directions. This may require identifying areas where additional studies are required to increase the effectiveness of the proposed framework. For example, future studies should focus on developing machine learning algorithms with higher complexity to increase the accuracy of the process. They may also explore how blockchain technology could be used to improve the security and openness of trust management in SIoT (See chapter 07).

Following the DSR presented in Figure 1, this research relies heavily on quantitative research methods that use numerical data and statistical analysis to measure and analyse phenomena (Cohen, Manion and Morrison, 2017). It involves collecting information through structured tools such as surveys, experiments, and observations and then using statistical techniques to analyse the information. The goal of quantitative research is to find relationships and trends in data. This includes collecting data that is representative of the broader population being studied and testing theories or hypotheses. This is achieved by selecting study participants or test subjects using random sampling methods. Among the many advantages of quantitative research is the ability to collect massive amounts of data for rapid and precise analysis (Punch and Oancea, 2014). Furthermore, quantitative research is based on quantifiable, verifiable numerical data which is considered more objective and trustworthy than qualitative research. However, this study used a mathematical model to validate its results using a quantitative research methodology, making various contextual parameters and SIoT aspects quantifiable. the development of the simulator, the generation of datasets, and the application of machine learning. all followed the same methodology.

The MCTM-SIoT framework and model employ quantitative research techniques to assess and confirm the efficiency of the proposed TM model in enhancing trust evaluations. This, in turn, enhances the security and dependability of the SIoT environment as a whole. For this research purpose, quantitative methods are used as follows:

1) The theoretical framework of the study centers on the establishment of quantitative metrics. Several context-aware-based TM models (Abderrahim, Elhedhili & Saidane, 2017; Khani *et al.,* 2018; Lin and Dong, 2018; Xia *et al.,* 2019; Wei *et al.,* 2021; Magdich, Jemal and Ayed, 2022) considered single or dual contexts in the final trust assessment. It is essential to develop an efficient TM model that incorporates multiple contextual factors, such as where including environmental condition, what including any services the objects can provide, and when (i.e., time). However, the MCTM-SIoT framework and model create a set of quantitative metrics (user context trust metrics, device context trust metrics, environmental context trust metrics, and task context trust metrics) to assess the trustworthiness of nodes in the SIoT network. These metrics include measurable factors such as user profile

information, device credibility, environmental conditions, and task reliability (see Chapter 04).

2) The practical framework is experimental validation: this is important to design a general simulator tool for an SIoT environment that takes into account the social structure of objects to validate the effectiveness of SIoT systems. While various simulation tools are available for the IoT environment OMNET++ (Varga and Hornig, 2008), NS-2 (Henderson *et al.,* 2003), and Cooja (Osterlind *et al.,*2006) not all of them are adequate for addressing the complexity of the social structure of objects in the SIoT environment. (Ojie and Pereira, 2017; Chernyshev *et al.,* 2018). In addition to those discussed previously, few other simulation tools are available and have been used by researchers (Kasnesis *et al., 2016*; Abderrahim, Elhedhili and Saidane, 2017a; Defiebre, Germanakos and Sacharidis, 2020; Gazi *et al.,* 2021) to simulate the SIoT environment. All these simulators are purpose-built simulators designed only for a specific study purpose. However, an SIoT simulator tool has been developed to simulate the behaviour of devices, sensors, and users in different SIoT contexts. It also includes the modelling of attacks and vulnerabilities that can be quantified in terms of their impact and frequency in the simulated SIoT environment (see chapter 05). This tool generates realistic data that is quantitatively analysed to evaluate the effectiveness of the MCTM SIoT framework and model.

1.9. Research contribution

The successful accomplishment of the research objectives will result in the following contributions:

1. A new MCTM-SIoT framework for demonstrating the relationship between the different SIoT components and TM as well as inferring trustworthiness within SIoT environments by incorporating various contextual information factors to select the most trustworthy SP.

2. A scalable MCTM-SIoT model in SIoT that takes into account the dynamic aspect such as contextual information.
3. A novel simulation tool (SIoT-Sim) that simulates various SIoT scenarios.
4. A realistic SIoT Dataset.
5. A proof of concept for a MCTM-SIoT framework and model using the generated SIoT datasets and ML techniques.

1.10. Research outline and relation of the thesis chapters

This section presents a brief summary of the remaining chapters and their relationships. Figure 2 demonstrates the correlation between the thesis structure and the individual chapters.

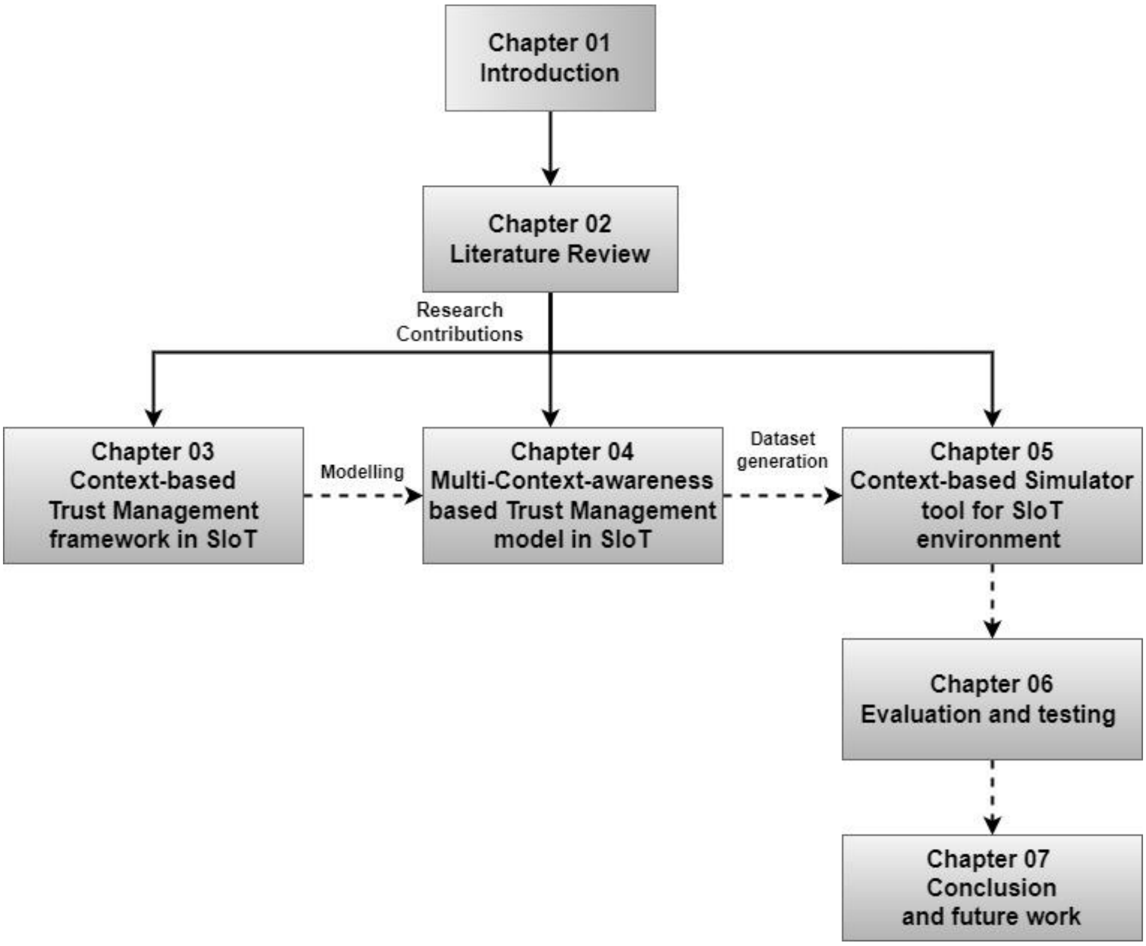

Chapter 01
Introduction
Chapter 02
Literature Review
Research Contributions
Chapter 03
Context-based Trust Management framework in SIoT
Modelling
Chapter 04
Multi-Context-awareness based Trust Management model in SIoT
Dataset generation
Chapter 05
Context-based Simulator tool for SIoT environment
Chapter 06
Evaluation and testing
Chapter 07
Conclusion and future work

Figure 2 Research outline and relation of the thesis chapters

1.11. Thesis structure

The thesis is structured in chapters to provide readers with a comprehensive breakdown of the research.

1. **Chapter One: Introduction**

The first chapter of the thesis introduces the background of the research. This chapter usually contains different key sections including:

- **Research Background**: This section presents the current research on SIoT, including a review of existing literature.
- **Research questions, aims, and objectives**: This section defines the main research questions to be addressed in the study. This also includes a presentation of the aims and objectives of the study, which should be specific, meaningful, and achievable.
- **Overview of the deliverables of the research**: This section presents a brief overview of the research findings, including the proposed frameworks, models, and methodologies developed as part of the research.

2. **Chapter two: literature review**

   The second chapter of a thesis usually consists of a literature review section in which the existing literature on SIoT and trust management are critically analysed. Therefore, this chapter is important because it helps set the research direction and identify any research gaps that need to be addressed. Additionally, the literature review chapter includes sections that provide an overview of existing SIoT research, including:

- **Introduction**: This section briefly introduces the literature review chapter and outlines its structure.
- **Overview of IoT, SIoT, Trust Management models and frameworks, and Context-awareness in SIoT**: This section discusses an overview of IoT, SIoT, TM models and frameworks, and context awareness in SIoT. To

provide a comprehensive overview of the SIoT TM concepts utilised throughout the thesis.

- **Existing SIoT architectures**: This section introduces various SIoT architectures, identifies their strengths and weaknesses, and suggests improvements.
- **Relevant TM attacks**: This section provides an overview of existing TM attacks. The goal is to provide an understanding of how these attacks impact SIoT trust.
- **Classification of existing framework and TM models**: This section classifies the existing TM framework and models based on their characteristics. The aim of this classification is to provide a comprehensive overview of the existing models and to highlight any gaps or limitations in the current state of the art.
- **Challenges related to the SIoT environment**: This section identifies and discusses the various challenges associated with the SIoT environment.

3. **Chapter three: MCTM-SIoT framework**

The following chapter is dedicated to presenting the proposed solution to the research problem. This chapter consists of sections that explain the proposed framework in detail. These sections include:

- **Introduction:** This section briefly introduces the proposed framework and outlines its structure.
- **SIoT environment and its main modules**: This section provides an overview of the SIoT environment and its main components, including SIoT object, relationship management, network navigability, resource discovery, service management, and TM. The purpose is to obtain a comprehensive understanding of the environment in which the proposed framework works.
- **MCTM-SIoT framework**: This section describes the proposed MCTM-SIoT framework that offers a comprehensive view of the SIoT ecosystem and places special emphasis on how different SIoT components link with one another and with TM. Additionally, the framework includes multiple contextual information into the final trust score to enable trustworthy

inference and improves the overall security and reliability of the system by helping to detect malicious behaviour.

- **MCTM-SIoT framework modules**: This section provides a detailed explanation of the modules of the proposed framework, including the relationship selection module, friendship selection module, service search module, and MCTM-SIoT model. It provides a comprehensive understanding of the framework and the role of each module in the TM process.
- **Validation of MCTM-SIoT**: In this section, the proposed framework is validated mathematically and experimentally. Mathematically, a series of contextual trust metrics are used to assess the trustworthiness of a device. A simulator tool is being experimentally developed to simulate the behaviour of SIoT systems and thus enable the generation of realistic SIoT data. The aim is to demonstrate the effectiveness of the proposed framework and its ability to assess the trustworthiness of SIoT devices and their interaction.

4. **Chapter four: MCTM-SIoT model**

This chapter focuses on the proposed MCTM-SIoT model in SIoT. The chapter consists of several sections intended to provide a detailed explanation of the proposed model.

- **Introduction:** This section briefly introduces the proposed MCTM-SIoT model and outlines its structure.
- **Problem statement**: This section describes the research gaps that the proposed MCTM-SIoT aims to address, particularly by incorporating various contextual information for the final trust assessment of each node in the SIoT network.
- **MCTM-SIoT model architecture**: This section presents the proposed MCTM-SIoT architecture, which considers various contextual information including device, user behaviour, environmental condition, and task type.
- **MCTM-SIoT Evaluation process phases**: This section describes all stages of the evaluation process of MCTM-SIoT.
- **Contextual trust metrics**: In this section, several contextual trust metrics are proposed and discussed for trustworthiness evaluation in MCTM-SIoT. The

aim of these contextual metrics is to provide a comprehensive understanding of the various contextual information considered in MCTM-SIoT.

- **Machine learning-driven (ML-driven) aggregation approach**: This section describes the proposed ML-driven aggregation approach to evaluate the performance of the proposed model by identify the influence of each contextual metric on the overall trust score and predict the trust score of each node in the network.

5. **Chapter Five: Simulator tool for SIoT environment**

This chapter focuses on the design and implementation of a simulator tool for SIoT environments. The aim is to explain in detail the development of the simulator tool to generate a realistic SIoT dataset. Some of the sections that are included in this chapter are:

- **Introduction:** This section briefly introduces the proposed SIoT simulator tool and outlines the chapter structure.
- **Design and implementation of the simulator tool**: This section outlines the design and implementation of the simulator tool for the SIoT environment. The simulator tool incorporates a range of functionalities, including the social structure of objects and modelling various attacks and vulnerabilities.
- **Generate a realistic SIoT dataset**: This section provides several generated SIoT datasets simulated in different scenarios context.

6. **Chapter six: Evaluation and testing MCTM-SIoT model and framework using ML techniques.**

This chapter provides a critical comparison between diverse SIoT datasets and MCTM-SIoT model to validate the performance of the proposed MCTM-SIoT model and framework in terms of inferring trustworthiness and ensuring the security and privacy of IoT devices. The MCTM-SIoT model aims to provide a comprehensive trust management mechanism for SIoT, that takes into account various contextual information that impacts the trustworthiness of IoT devices. The proposed model uses machine learning techniques to learn from the proposed model and improve their accuracy in predicting the trustworthiness of IoT devices.

7. **Chapter seven: Conclusion and future work**

   The final chapter provides an overall summary of the research and explains how the research objectives were achieved by conducting a critical analysis of the results obtained in the previous chapters. The chapter begins with a summary of the main contributions of the thesis, including the development of an MCTM-SIoT framework and model to ensure the security and privacy of IoT devices in SIoT environments and an SIoT simulator tool to generate SIoT datasets. It then highlights the importance of research in addressing the challenges and limitations of the current study. Finally, the chapter provides recommendations for future research directions such as developing new ML techniques that can effectively deal with the complexity of SIoT environment and improve the accuracy of trust management mechanisms.

1.12. Summary

This chapter provides an overview of research related to IoT and SIoT, including the research aims, objectives, contributions of the study, and research methodology that will be used throughout this thesis. Additionally, this chapter provides a summary of the entire thesis. The next chapter explores a literature review and analysis of research areas related to IoT, SIoT, TM, context-awareness, and existing TM frameworks and models in SIoT.

Chapter 2

landscape of Trust Management in the SIoT

2.1. Introduction

With the advancement of technology, the concept of the internet has evolved from merely connecting networks to advanced communication, referred to as IoT (Fortino *et al.,* 2020). According to Kashani *et al.* (2021), Real-world objects have been empowered to interact with the virtual realm through distinct identifiers, facilitating connectivity for items with ON and OFF functionalities regardless of location or time. IoT has established an ecosystem enabling data exchange among interconnected objects via a network. In recent years, technology has been widely embraced across diverse sectors, including healthcare, transportation, and remote-control systems (Elgazzar *et al.,* 2022). The idea of social networks has been applied to the IoT, where a node autonomously discovers other nodes and services and establishes social relationships. This integration has led to the concept of the SIoT. SIoT is an IoT in which objects communicate socially with one another. Smart social objects can work together to form their own network, manage social relationships, and make decisions without the intervention of humans. According to Nitti, Atzori and Cvijikj (2014) and Um *et al.* (2019) SIoT has the potential to address a number of research challenges such as Scalability, Management of social relationships between intelligent social objects and network navigability. The introduction of social features through SIoT has created opportunities for the advancement of the next generation of IoT. This makes it possible to find services by establishing social connections to nearby objects. However, the importance of SIoT is seriously exposed by security, privacy, and trust issues associated with these smart social objects (Cai *et al.,* 2016). When a SIoT object makes a service request, multiple service providers may offer to fulfil the request. In such situations, the credibility of the service provider is crucial as the requester chooses the most trustworthy provider. However, the significance of SIoT is potentially risked by security, privacy, and trust concerns associated with smart social objects. While conventional methods like cryptographic and non-cryptographic techniques have been suggested to mitigate these challenges, they may not offer adequate solutions (Hamad *et al.,* 2020; Nie *et al.,* 2022). It is challenging to address security issues related to trust and reputation using cryptographic or non-cryptographic solutions. In addition, there are malicious objects that, in order to pursue their own malicious goals, disrupt the basic functionality of the network. These malicious objects can affect the credibility of well-behaved objects or increase the legitimacy of those who misbehave (Fan *et al.,* 2019; Bahutair, Bouguettaya and Neiat, 2022). To prevent an unreliable object from sending malicious messages and compromising the quality and reliability of service, TM is crucial in SIoT (Rizwanullah *et al.,* 2022). Therefore, Given the dynamic nature of SIoT and the potential presence of misbehaving nodes capable of disrupting network functionalities, the implementation of an efficient TM system within SIoT becomes imperative. SIoT is an IoT in which objects communicate socially with one another. Smart social objects can work together to form their own network, manage social relationships, and make decisions without the intervention of humans.

This chapter is structured as follows: (Section 2.2) introduces the basics of IoT, SIoT, and trust concepts in SIoT followed by (section 2.3) which provides a comprehensive overview of the trust management process proposed in the literature for SIoT. (Section 2.4) describe context-awareness in SIoT, and (sections 2.5,2.6) conduct a comparison of the state-of-the-art TM systems developed for SIoT by conducting a comparative analysis in terms of the TM process. (Section 2.7) identifies and discusses the challenges and requirements of the emerging new wave of SIoT and highlights the challenges in developing trust and assessing trustworthiness between interacting social objects. Finally, (section 2.8) concludes the chapter.

2.2. From the IoT to the SIoT

Both IoT and SIoT technologies and architectures are discussed in this section

2.2.1. Overview of IoT

The rapid development of computer technology has given rise to an innovative idea that connects the real and the digital world. Computer technologies are embedded in the objects so that they can communicate with their surroundings and obtain a digital identity. This phenomenon gave rise to the IoT, a network of connected objects with unique identifiers that can collect, analyse and share data (Atzori, Iera and Morabito, 2010; Lin *et al.,* 2017). IoT consists of objects that provide unique services used to create compelling applications. The main goal is to improve human life by allowing surrounding objects to recognise users' needs and respond appropriately without explicit instructions. Services can be available to anyone, anywhere and at any time by connecting the real, virtual and digital worlds via IoT (Lin et al., 2017). IoT consists of five main components, as depicted in Figure 3. The most important component is called the device, which consists of an object or things such as sensors. These devices are constantly collecting information and transmitting it to the next level. However, due to low internal memory, low computing power and low performance, their functionality is limited, even some of these objects are modified to connect to the internet. Although they cannot support standard communication protocols or perform complex calculations without a gateway, these objects are still considered "smart" because they can send and receive data. As an intermediary between the devices and the cloud, the gateway is the second component. All data going to or coming from the cloud must pass through it, whether it is a software application or a hardware device. The third component is the cloud which consists of a network of powerful servers designed to handle traffic, process information quickly, and provide accurate analytics. The fourth component is analytics, which involves transforming the vast amounts of data collected by devices into insightful insights that are easy to interpret and further analyse. The fifth and final component is user interfaces, which allow users to visually view the results.

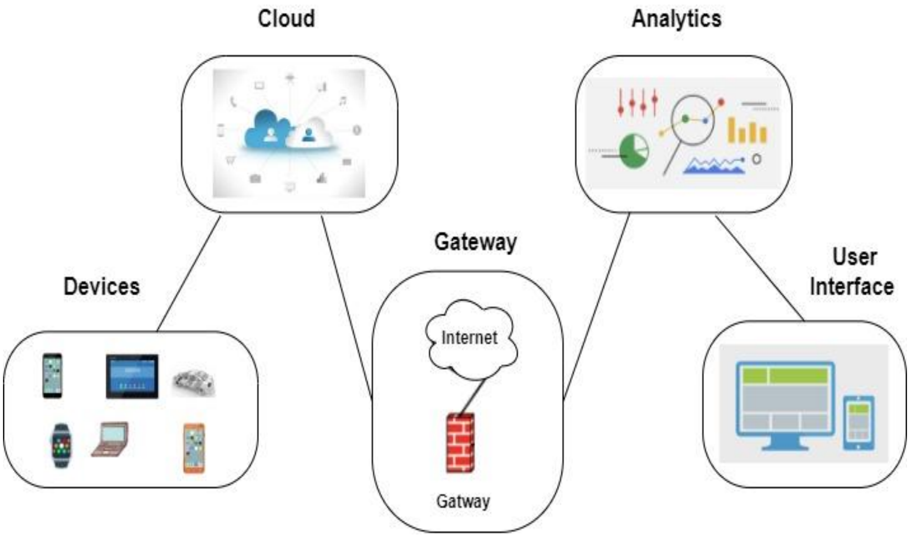


Figure 3 The main components of IoT

2.2.2. Overview of SIoT

The SIoT refers to a paradigm that integrates social networking principles into IoT, allowing objects to establish social relationships with one another and with humans. While IoT follows two interaction paradigms, human-to-human (H2H) and thing-to-thing (T2T), SIoT adds human-to-thing interactions (H2T). This concept extends the capabilities of traditional IoT by enabling devices to communicate and interact based on social dynamics. SIoT represents a significant evolution in how devices communicate and collaborate, leveraging social networking concepts to enhance the functionality of interconnected systems (Rad *et al., 2020)*.

Objects in SIoT are able to interact similarly to humans based on different types of relationships (Atzori *et al.,* 2012; Alam *et al.,* 2022; Khan et al., 2020). Initial socialisation is observed in the formation of a Parental Object Relationship (POR), which are objects made at the same time by the same manufacturer. Another form of relationship is the Co-Worker Object Relationship (CWOR), in which objects share public experiences, such as working to achieve common goals. Similarly, a Co-Location Object Relationship (CLOR) arises when objects share personal experiences such as location. Both co-location and Co-Worker object relationships can evolve over time and are affected by interaction frequency and reputation. Objects owned by the same person, such as a phone or laptop, create an Owner Object Relationship (OOR). Finally, the Social Object Relationship (SOR) refers to objects that come into contact occasionally or regularly, depending on the owner. This relationship is established through planned encounters arranged by their owners, potentially resulting in the objects forming friendships or remaining strangers (Amin, Ahmad and Choi, 2019; Nitti, Pilloni and Giusto, 2016). In SIoT, objects take away some capacity from humans and mimic their behaviours when looking for new friends. After an owner defines the rules, an object creates and manages different types of relationships and applies them to navigate the network in search of services (Nitti, Atzori and Cvijikj, 2015; Nitti, Pilloni and Giusto, 2016).

2.2.3. SIoT architecture structure

The architecture of SIoT includes the design and arrangement of the components that facilitate the integration of social networks with IoT devices and applications (Chahal, Kumar and Batra, 2020). It consists of four main components, shown in Figure 4, and explained as follows:

1. **Actors**: Within SIoT, owners and their devices are viewed as actors. The main goal of the IoT is to create an open environment that allows smooth interaction between owners and their devices. During these interactions, data exchange and control signals are received and used to manage the generated data.
2. **Intelligent System:** It includes essential subsystems such as application management, data management, and service discovery. These subsystems are essential for maintaining, organising, and coordinating the various interactions of the actors involved.
3. **Interface**: It facilitates communication between the different actors by acting as an intermediary. It allows generating outputs such as signals, commands and services and receiving inputs such as data and queries.
4. **Internet**: allows actors to interact with one another by acting as a communication link between them.

In addition, there are other fundamental aspects that form the basis of SIoT:

5. **Social Role**: Social structure is relevant to the SIoT, especially when it comes to shared smart objects. Trust within the social community is essential, and users can, for example, utilise their social network accounts for geolocation services.

6. **Socialised Devices**: Socialised devices play an important role in SIoT by enabling communication between people and various embedded devices and smart objects over the internet.

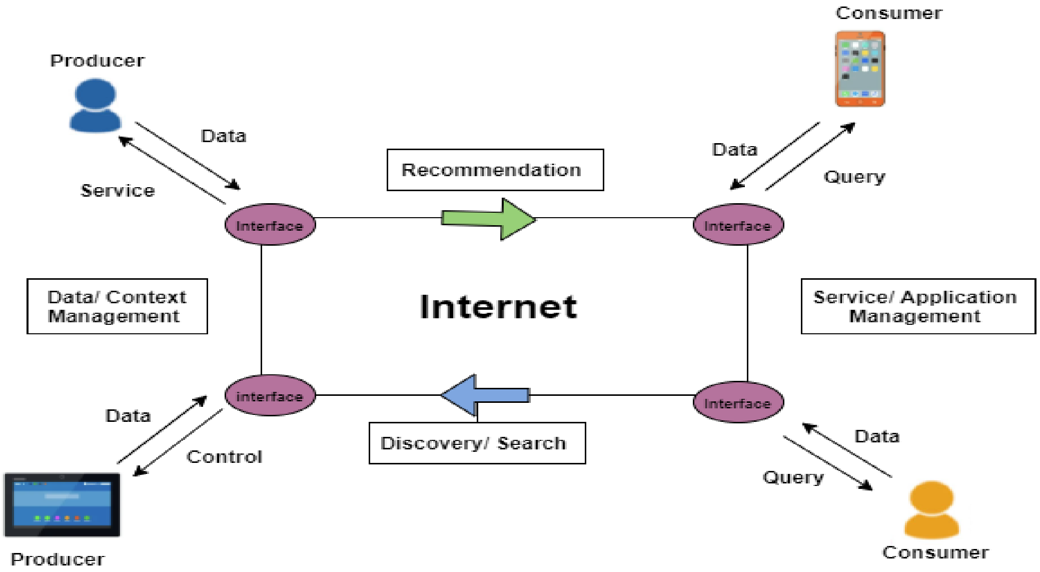


Figure 4 SIoT architecture

2.3. Trust management in SIoT

The evolution of TM is rapidly progressing and gaining widespread application across various fields. Hence, it is crucial to identify the optimal parameters for the SIoT ecosystem.

2.3.1. Trust as a concept

Trust is a foundational element of human existence, essential for establishing connections with others. With the swift progress of science, trust is now being incorporated and utilised across diverse fields, such as sociology, psychology, economics, and computer science. Trust is evaluated concerning its necessity, timing, and effectiveness in specific contexts. In computer science, the primary objective is to develop secure, functional systems that can be easily identified and promptly addressed in case of unforeseen weaknesses (Sagar *et al.,* 2023). The current computer systems deal with data communication and processing, which requires secure and trustworthy management. In the realm of SIoT, trust is a dynamic process through which one party, known as the trustor, delegates responsibilities to another party, the trustee, and relies on the trustee's actions to further its objectives. The trustor evaluates both the competency and willingness of the trustee, acknowledging the potential risks involved in placing trust in a specific environment. Mutual assessment of each other's trustworthiness occurs, influenced by environmental unpredictability, behavioural outcomes, and task Type. Both the trustor and trustee play pivotal roles in this trusting relationship, with the trustee evaluating the level of trust vested in them. In this dynamic, trustees act as service requesters while trustees function as service providers (Alam *et al.,* 2022). The concept of trust in SIoT is crucial for enabling secure and reliable interactions between various smart objects and users in the network. It helps in decision-making processes, service selection, and overall system security by allowing entities to judge the behaviour and reliability of other objects in the SIoT ecosystem (Rizwanullah et al., 2022).

2.3.2. Fundamental social trust aspects

The social trust aspect includes three categories: general trust properties, social trust properties, and social trust-related attacks.

2.3.2.1. General trust properties

To better understand and calculate trust in SIoT, it is important to examine the different properties of trust shown in Figure 5 including subjective, objective, direct, indirect, local, global, asymmetric, and context-specific (Rad *et al.,* 2020). The subjective trust property is viewed from a social perspective as an assessment of trust that uses the centrality of an object and calculates trust based on trust observations as well as the opinion of other objects. The objective trust property is evaluated based on the feedback of all objects in the network, with each object's trust information distributed and visible to everyone. Furthermore, accessing this information is achievable via distributed hash tables, with management overseen by pre-trusted social objects (Alghofaili and Rassam, 2022). The direct trust property asserts that trust should derive from interactions and firsthand observations between the trustee and the trustor. Moreover, it extends beyond experiences solely between these entities. On the other hand, the indirect trust property is established and developed through recommendations from other nodes, thus not reliant on any direct experiences or interactions, but rather on the evaluations of other nodes within the network. (Sagar, Mahmood, Sheng and Zhang, 2020). The local trust property implies that trust typically exists within individual pairs and can vary significantly. For instance, consider nodes (i,j) and (k,j). Node i might trust node j, while node k might distrust node j. On the other hand, the global trust property, often referred to as reputation, denotes that every node in the network possesses a distinct trust value that is universally recognised by neighbouring nodes. Asymmetric trust, another property, indicates that there can be differing levels of trustworthiness between connected entities. For instance, while X may trust Y, it doesn't necessarily imply that Y trusts X. (Abdelghani *et al.,* 2016). Finally, the context-specific trust property suggests that the trustworthiness of one object in another object varies depending on the context. The trust relationship among objects typically fluctuates and is influenced by various factors, including environmental conditions (Wei *et al.,* 2021).

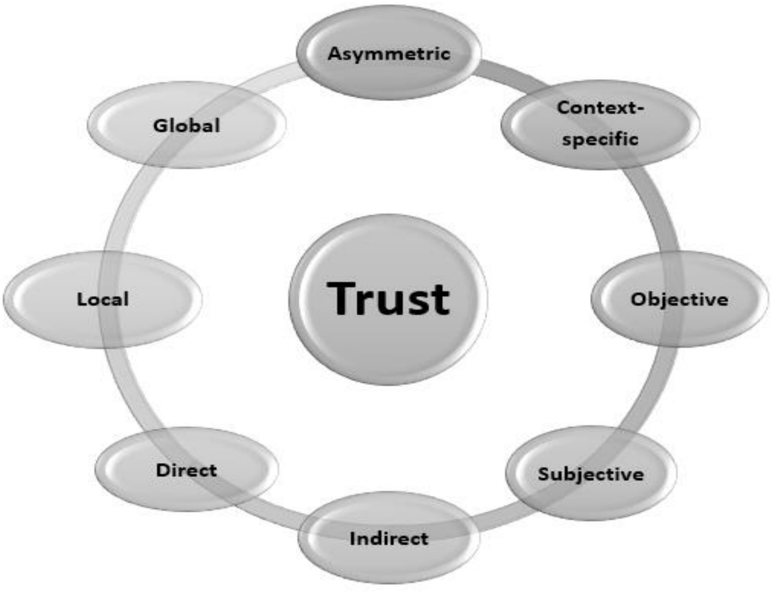


Figure 5 Type of trust properties

2.3.2.2. Social trust properties

The following list of social trust properties has been summarised.

1) **Community of interest**: this property indicates whether or not an object belongs to the same community as other objects in the network. Objects that belong to a community of interest not only share similar needs but are also more likely to interact with one another within the network and build trust. The effectiveness of the network and the trust relationships between objects that are part of the same community depend on this property (Kowshalya and Valarmathi, 2017).

2) **Honesty**: This characteristic, which refers to whether or not an object within the network can be considered trustworthy based on its behaviour and interactions with other objects, it is a crucial component of trust in SIoT networks. Distinguishing between dishonest and honest nodes is necessary because dishonest nodes can significantly damage the trust model (TM) in SIoT networks. Honest nodes are those that can act in a trustworthy manner and fulfil their obligations within the network. The level of honesty can be determined through both direct and indirect interactions between nodes in the network. By assessing the integrity of nodes, SIoT networks can establish and maintain reliable relationships which is a significant component in ensuring the security and integrity of the network (Muhammad *et al.,* 2023).

3) **Cooperativeness**: This attribute refers to whether an object within the network is socially cooperative or not. Cooperativeness is a key component in assessing the level of trust that can arise between nodes and is used to evaluate whether the trustee and trustor cooperate in achieving a common goal. Only objects that are considered friends or have strong social relationships with them can cooperate with other objects. SIoT networks can build and maintain relationships based on trust and collaboration by assessing the level of collaboration of nodes within the network. This can ensure the smooth operation of the network and the achievement of the common goals of its objects (Alam *et al.,* 2022).

4) **Centrality**: This attribute refers to the significance of nodes within the network, which can be assessed through various metrics. One such metric is

"degree centrality," which considers the number of direct connections a node has within the network. Nodes with higher centrality potentially have a greater influence on the overall behaviour of the network. However, centrality is critical for managing the flow of information within the network. SIoT networks can identify important nodes and ensure they are adequately protected from attacks by examining the centrality of nodes within the network. Additionally, understanding node centrality helps refine the structure of the network and increase overall performance (Guo and Chen, 2015).

2.3.2.3. Social trust related attacks

A node might behave maliciously with the aim of disrupting the essential operations of the network and its services. Hence, attacks on trust management systems can be broadly categorised into collaborative and individual assaults.

2.3.2.3.1. Collaborative Attacks

Collaborative attacks represent the attack of a group of objects to give a specific object either a high or low rating. Collaborative attacks are briefly discussed below:

1) **Bad Mouthing Attack (BMA):** This is a type of attack in which a node in a network attempt to damage the reputation of another reliable node by making unfavourable feedback or recommendations. The aim of this attack is to reduce the likelihood of the target node being selected as a service provider, which ultimately affects the overall reliability and performance of the network (Li, Song and Zeng, 2018).

2) **Ballot Stuffing Attack (BSA)**: This type of attack aimed to improve the reputation of malicious nodes in a network. This attack aims to increase a faulty node's chances of being selected as a service provider by recommending it to other nodes. The attacker can influence the selection process, thereby damaging the overall security and reliability of the network (Chahal, Kumar and Batra, 2020).

2.3.2.3.2. Individual attacks

It refers to attacks launched from a single object. Individual attacks are briefly discussed below:

1) **Self-Promoting Attack (SPA):** In this type of attack, a node makes good recommendations about itself to increase the likelihood that a node will choose it as a service provider. However, the services offered by the node could be malicious or fake and could be used to launch further attacks or compromise the security and integrity of the network (Bao and Chen, 2012).

2) **Whitewashing Attack (WA):** In this type of attack, a node with a history of malicious behaviour aims to improve its reputation within a network by deleting its identity and joining a new application or service. Once connected, it provides legitimate services to gain the trust of other nodes and remain undetected, making this type of attack difficult to detect and prevent (Ferrag et al., 2019).

3) **Opportunistic Self-Attack (OSA):** In this type of attack, a malicious node provides legitimate services on the network to improve its reputation, which may have been harmed by previous malicious action. The node launches Bad Mouthing Attacks (BMA) and Ballot Stuffing Attacks (BSA) to damage the reputation of other nodes and improve its own chances of being selected as a service provider, once it has achieved a high level of reputation. This type of attack can be particularly dangerous because its seemingly legitimate behaviour allows the malicious node to manipulate the network without arousing suspicion (Abdelghani *et al.,* 2016).

4) **Discriminatory Attack (DA):** This attack targets malicious nodes in a network that are specifically connected to nodes that have weaker connections, such as fewer mutual friends or weaker connections. The idea behind this type of attack is that nodes in a network may be more inclined to interact with and trust those who have more connections or mutual friends, similar to human behaviour. Malicious nodes can exploit these trust

relationships to compromise the security and integrity of the network by targeting nodes with weaker connections (Marche and Nitti, 2021).

5) **On-Off Attack (OOA):** In this type of attack, malicious nodes within a network periodically turn their services on and off. This attack can be sudden and random and can be particularly difficult to stop or identify. The trust system may be unreliable in identifying or detecting ongoing attacks, making it difficult to prevent or mitigate their impact. This can significantly compromise the security and integrity of the network (Caminha, Perkusich and Perkusich, 2020).

2.3.3. TM process

TM is required in two scenarios: when the trustor node requests a specific service from the trustee node and when a trustor node receives information about the trustee node from other nodes and wants to check whether this information is trustworthy or not. Regardless of whether either scenario occurs, the TMS comes into play and helps the trustor node calculate the trust value of the trustee node (Chahal, Kumar and Batra, 2020; Kuseh *et al.,* 2022). TM includes five phases in any environment: information gathering, trust calculation, trust decision, trust update, reward and punishment.

2.3.3.1. Information gathering

The TMS collects information from all nodes within the system, which can be either transactional or opinion-based, and may vary in subjectivity and objectivity. The information-gathering process is characterised by two functions, Trust composition and trust formation as elaborated below:

2.3.3.1.1. Trust composition

Trust composition refers to the parameters used to determine the trust score. These parameters are based on either quality of service (QoS), which represents the quality of service offered by a node, or social behaviour, which represents the node's social interactions with others in the system. Therefore, there are two types of trust compositions: QoS trust and social trust. The parameters categorised under QoS trust include data delivery rate, risk, number of interactions and interacting peers, quality of service (positive or negative), time sensitivity, credibility, response time, throughput, availability, reliability and more. On the other hand, social trust parameters encompass attributes like honesty, intimacy, unselfishness, healthiness, cooperativeness, benevolence, integrity, and others (Aslam *et al.,* 2020) .

2.3.3.1.2. Trust formation

Trust formation involves establishing the trust value, which can be based on either a single factor or multiple factors. Certain TM systems compute the trust score using a single factor, like nodes' adherence to quality of service. Such trust values are categorised as a single trust. However, many trust management systems take into account multiple factors when calculating trust scores. These factors can be diverse and belong to either QoS or social dimensions. (Chahal, Kumar and Batra, 2020).

2.3.3.2. Trust calculation

Upon receiving information from the nodes within the system, the TM system assesses the reliability and trustworthiness of nodes that are offering a specific service. The method used to calculate this trust score depends on the system's policies. In general, this evaluation process consists of two main phases: trust aggregation and trust propagation (Chahal, Kumar and Batra, 2020) which are explained below.

2.3.3.2.1. Trust aggregation

Trust aggregation represents a vital phase in any trust calculation model, incorporating methods to combine trust observations into a single trust score. Numerous approaches have been explored in the literature, including weighted sum, belief theory, Bayesian systems, fuzzy logic, regression analysis, and machine learning.

1) **Weighted sum:** It stands as the most straightforward and frequently employed aggregation technique. This theory takes an average weighted mean of each metric, specifying a weight to each metric to arrive at a single value.
   Let M =$\{m_1, m_2, m_3, \ldots, m_n\}$ be the n trust metrics and
   W = $\{w_1, w_2, w_3, \ldots, w_n\}$ be the weights of n trust metrics, these weights can either be static (the weights remain the same for each metric) or dynamic (the weights may change over time) (Chen, Bao and Guo, 2016) .
   Weighted sum aggregation (WS) is calculated as follows:

$$WS = \sum_{i=1}^{n} W_i * M_i$$

2) **Bayesian system**: This theory aims to obtain a posterior probability about the data/nodes/interactions provided a prior probability and a probability function (Chen, Guo and Bao, 2016). It is based on Bayes' theorem, which is stated as:

$$p(A|B) = \frac{p(B|A)p(A)}{p(B)}$$

   Where: $p(A|B)$= posterior probability of A given B is true, $p(B|A)$= likelihood of B given A is true, $p(B)$= probability of B happening, and $p(A)$= prior probability of A.

3) **Fuzzy logic**: Uncertainty is the focus of fuzzy logic. Approximate values are supported. Real values are converted into fuzzy logic via the fuzzy controller. Unlike Boolean logic, which only accepts two values (0 and 1), fuzzy logic can easily describe complicated and unclear problems (Alam *et al.,* 2022).

4) **Blockchain**: This is essential for maintaining anonymity in SIoT. Therefore, the role that blockchain has played in securing shared information between different elements cannot be overstated. In general, in SIoT authentication and authorisation for data access can be done quickly, securely, and decentralised. While sharing and storing vehicle data in SIoV using smart contracts can be selective and limited to only certain vehicles (Kuseh *et al.,* 2022; (Wei, Wu and Long, 2020).

5) **Machine learning**: Machine learning-driven aggregation methods employ clustering (unsupervised algorithms) and prediction (supervised algorithms) to categorise nodes into trustworthy or untrustworthy categories *(Kuseh et al.,* 2022).

2.3.3.2.2. Trust propagation

Trust propagation is about how trust-related information is propagated across the network. Generally, it can be divided into three schemes: centralised, distributed and hybrid.

1) **Centralised**: In a centralised system, there exists an entity initially tasked with gathering trust-related data and computing trust scores, which are then disseminated across the network. Consequently, this setup carries the inherent risk of a single point of failure. Should such a failure occur, the entire trust management system might collapse (Sagar *et al.,* 2023).

2) **Distributed**: In a distributed scheme, both information gathering and trust computation are carried out by the nodes within the system. Each node collects data and computes trust scores independently, which can then be shared across the network for use by other nodes, either automatically or in response to requests. While this approach eliminates the vulnerability of a single point of failure, it introduces a fresh set of challenges. Each node must be honest when calculating trust and sharing information, as any bias or dishonesty can significantly impact the reliability of the system (Guo and Chen, 2015).

3) **Hybrid:** Hybrid systems are frequently used to manage the challenges encountered by both systems., i.e., centralised and distributed systems. In addition, hybrid systems are divided into two categories locally distributed/global centralised and locally centralised/global distributed (Sagar *et al.,* 2023).

2.3.3.3. Trust decision

Once the trust scores are calculated, the TM system shares this information with the requesting node. The TM system provides the trust scores of all these service providers when multiple nodes are willing to offer the same service. The requesting node then selects a service provider based on these trust scores. When the requesting node searches for the trust score of an information-providing node, it can evaluate whether or not to trust the received information based on the calculated trustworthiness value. This decision-making process can follow one of the approaches mentioned below:

2.3.3.3.1. Reputation-based decision

Decisions based on reputation involve assessing a node's reliability through evaluations from other nodes in the system or by the requesting node itself. Following the assessment of trustworthiness, the requesting node determines whether to trust the service provider. Several trust functions can be used to calculate trust, including complete and/or global, opinion-based and/or transaction-based, subjective and/or objective, and rank-based and/or threshold-based functions (Sagar *et al.,* 2023).

2.3.3.3.2. Context-based decision

Context-based decision techniques take contextual information into account to make decisions. This technique is particularly useful when the same object can be viewed as harmless or malicious depending on the context in which it is observed. In general, context-based decision techniques are useful for making decisions in complex and dynamic environments where decisions must be made quickly and accurately based on a variety of factors (Sagar *et al.,* 2023).

2.3.3.3.3. Policy-based decision

Policy-based decision-making is the making of decisions that depend on the exchange, storage, and maintenance of credentials between system nodes. These credentials are used according to specific policies to establish trust relationships between nodes. These systems operate based on access control that validates credentials and determines whether or not access is permitted based on policies associated with those credentials (Chahal, Kumar and Batra, 2020).

2.3.3.4. Trust update

After, the requesting node engages in a transaction with the selected service provider and observes the received service, noting predefined parameters or metrics as a reference for future decisions. Once the transaction is completed, the trust scores assigned to the service provider are updated according to its performance (Amin, Ahmad and Choi, 2019). Trust updating can occur through either event-driven time-driven or hybrid approaches, as explained below:

2.3.3.4.1. Event-driven approach

After every transaction or event in a distributed system, the event-driven approach updates the trust through an update mechanism. Trustworthiness depends on a number of variables, including the node's reputation, past actions, and relationships with other nodes. the node's trust level is adjusted depending on how the transaction ends and what information is received from other nodes. Since Trust updates occur frequently and deal with a large amount of data to calculate trust, the event-driven approach provides real-time updates and fast decision making but may result in increased network traffic (Amin, Ahmad and Choi, 2019; Alghofaili and Rassam, 2022).

2.3.3.4.2. Time-driven approach

The time-driven approach is a mechanism to update trust after a certain time interval. This approach is suitable for systems where real-time updates are not required and periodic trust updates are sufficient. Nevertheless, it can be difficult to select the correct time interval for trust updates, and systems may need to use adaptive time intervals to balance the impact on network traffic and the accuracy of trust scores (Amin, Ahmad and Choi, 2019) .

2.3.3.4.3. Hybrid approach

The hybrid approach is a flexible and adaptable mechanism that updates trust in distributed systems. By integrating both event-driven and time-driven approaches, the system can balance the need for real-time updates with the need for periodic updates. This approach enhances the overall performance of the system and ensures optimal results (Sagar *et al.,* 2023).

2.3.3.5. Reward and punish

The Reward and Punish approach is a method for updating trust in a distributed system. In this approach, the Trustor node rewards or penalises the Trustee node depending on how the transaction turns out and how well it has provided its services. The reputation and the trust score of the trusted node can be increased or decreased accordingly as a reward or penalty. Based on inputs and suggestions from neighbouring nodes, the trustor node chooses the reward or punishment. The Reward and Punish approach provide a direct feedback mechanism to update trust depending on the actual transaction result, which is one of its advantages. However, this approach can be vulnerable to collusion or manipulation if nodes collaborate to provide false feedback to increase their trust score or reputation. To address this challenge, some systems use reputation systems that combine multiple feedback techniques, including direct feedback, indirect feedback, and subjective feedback. This reduces the possibility of collusion and enables a more accurate assessment of the reliability of the nodes (Chahal, Kumar and Batra, 2020).

2.4. Context awareness in SIoT

Context-Awareness was first published by Schilit, Adams and Want (1994). It is the ability of a system, application, service, or actor to adapt to a specific context. The characteristics of context-aware systems include presentation, execution and tagging, which have been highlighted in various studies (Li *et al.,* 2015; Perera *et al.,* 2014). Context lifetime is defined as the period from context acquisition to its dissemination. In general, the context life cycle includes four phases: context acquisition, context modelling, context reasoning, and context distribution (Sezer, Doğdu and Özbayoğlu, 2018). A context-aware system has the capability to determine the information or services to offer to the user. By considering the context, such systems present pertinent information to the end user. Context plays a crucial role in shaping trust, as it reflects the circumstances under which trust is established. Context-based trust assessment involves using interactive queries to retrieve relevant information from remote devices. Moreover, it entails making distinct decisions contingent upon various contexts. Hence, an estimation or inference based on the prevailing context is adequate for making trust judgments.

Context awareness plays a crucial role in the SIoT, enhancing the capabilities and interactions of connected devices. In the SIoT paradigm, context awareness refers to the ability of devices to understand and adapt to their environment, user preferences, and the relationships they form with other objects (Khelloufi *et al.,* 2023) . Devices can establish trust among themselves based on various contextual factors. These factors may include different device statuses such as energy levels and the computing capacity to offer or request different services across diverse times and locations. Furthermore, in online social networks (OSN), device owners can trust one another in different types of tasks due to shared social relationships (Wang, Li and Liu, 2013). Taking into account diverse contextual factors among devices in IoT setups and their owners in online social networks, trust contexts within SIoT environments are grouped into four categories: device status, environmental conditions, user social profiles, and task types. In SIoT environments, trust contexts are described as follows:

- **User social profile**: This factor relates to the core aspects of the user's social profile including community of interests and friendship. User social profile is a crucial contextual factor to consider as it can help to identify common interests and social connections among various users within the network. This can be helpful in determining which users are more trustworthy or reliable based on their social interactions.
- **Device status**: This factor refers to the social connections including owners, social connection and services and capabilities such as smartphone, sensor or actor. This contextual factor can help identify security vulnerabilities and other issues that could impact the reliability of the device.
- **Environmental conditions**: This contextual factor refers to the various external factors that influence or can impact the behaviour of interconnected devices within the network. For example, a device located in a remote or unfriendly environment may be less reliable than a device located in a more controlled environment.
- **Type of task**: This factor applies to services performed by the devices on the network and may also affect trustworthiness. For example, devices collaborating on a critical task may need to be more trustworthy and reliable than devices performing less critical tasks.

2.5. TM framework in SIoT

In SIoT environments, some frameworks were reviewed and summarised as follow:

Ruggeri and Briante (2017) presented a combined EHealth and IoT social-aware framework with five planes: the object plane, the social object (S-Obj) plane, the network plane, the virtual environment (VEs) plane, and the user plane. The lowest plane called the object plane, where there are sensors and actuators that can interact with the physical world but are unable to establish social relationships. The social object plane includes smart objects (SOs), that can collaborate and communicate with one another to achieve common goals and build social links. Through middleware, the network plane allows S-Objs to communicate and send data from the real world to the upper planes. The virtual environment (Ves) plane includes the

VEs, which are in charge of processing raw data to create elaborated data and initiating actions in the real world. VEs include things like E-Butlers and virtual doctors. Lastly, all system users are able to communicate with both VEs and S-Objs form the user plane. Aljubairy *et al.* (2020) proposed a framework called SIoTPredict for predicting future relationships in SIoT. This framework includes three main phases. In the first phase, raw motion data is collected from both mobile and static IoT devices. In the second phase, time sequenced SIoT networks are generated based on the raw motion data of IoT devices observed in the first phase. This is done by identifying stays from the raw movement data, extracting locations, and labelling each stay based on the extracted locations. The number of meetings between IoT devices is then calculated using the Sweep Line Time Overlap (SLTO) algorithm. The third stage predicts future relationships between things using Bayesian non-parametric learning to build their predictive model. Narang and Kar (2021) presented a Hybrid Multi-Service Social Tie-Graph (HMST), a trust management system that integrates human and device intelligence. The social tie graph of the OSN platform's IoT nodes integrates human intelligence into HMST. The foundation of social ties and device intelligence in HMST is based on the opinions of IoT nodes. The reliability of each social bond is assessed by its probability. probabilistic neighbourhood overlap (P-NO) is used to evaluate the strength of nodal ties. The proposed framework has a victim node that detects any trustworthy behaviour directed against it by a malicious node in the SIoT network to counter OOA. Recently Khelloufi *et al.* (2023) introduces a contextual service recommendation framework for SIoT. The aim of the study is to improve the accuracy and relevance of service recommendations in SIoT. The proposed framework leverages factorisation engines and a latent feature combination technique to capture latent feature interactions within the SIoT. The framework also includes review aggregation and feature learning processes to improve the accuracy and relevance of service recommendations. The experimental evaluation demonstrates the effectiveness of the proposed framework in improving the accuracy and relevance of service recommendations.

2.6. TM models in SIoT

Trust management models in SIoT can be generally categorised as context-based or context-free, depending on whether or not context is included in trust composition, trust aggregation, and trust assessment.

2.6.1. Context-free TM systems

In this section, context-free TM models are reviewed and summarised in the comparative analysis Table 2

The author Abderrahim, Elhedhili and Saidane, (2017a) proposed a trust management system that predicts the trustworthiness of nodes using Kalman filters and community-based trust metrics. The suggested approach examines an on-off attack to assess the node's performance. Nevertheless, it's crucial to showcase the model's robustness against various trust attacks. In summary, the prediction-based method offers reliable trust aggregation, allowing for the differentiation of trust metrics and facilitating precise trust decisions. However, addressing the computational complexity of the prediction model, particularly for machine and deep learning, necessitates an optimal and cost-effective solution. The limitation of this model is that only the on-off attack considers the model validity evaluation. Therefore, it is important to determine how this model examines other trust-related attacks. The reputation, experience, and knowledge model (REK) is presented by Truong *et al.* (2017). This model uses experience and reputation as indicators of an object's trust. The experience is calculated based on three elements: intensity of interactions, interaction cores and current state of relationships. The trend of experience is then analysed based on experience development due to cooperative interaction, experience loss due to uncooperative interactions, and experience progression due to missing or neutral interactions. The Google PageRank algorithm, which considers both good and bad reputations to determine an item's overall reputation, is an example of the denial perspective of trust. At the end, the model is evaluated for convergence with minimal iterations. One of the limitations of this system is that there is no performance evaluation of trust computation and trust-related attacks. Azad *et al.* (2020) proposed a decentralised self-enforcement trust management model that determines the trustworthiness of an object based on its weighted reputation. This approach comprises three steps: initially, generating keys using homomorphic encryption to safeguard privacy and then publishing a public key on a bulletin board. Next, objects download the generated public key, and finally, object reputations are computed using weighted reputation. Self-enforcement is achieved through public verifiability by peers in the network, without requiring proof of knowledge. The evaluation of the model's performance is based on the bandwidth required for communication and the delivery of feedback. The disadvantage of this scheme is that the performance of the model does not take into account defence against trust-related attacks. In a research article by Sagar *et al.* (2020) a centralised social similarity-based trust calculation model uses reputation and direct trust to calculate the trust score of an object. K-means clustering, and random forest classification were used to examine the trust of nodes over time. The model also examined how each trust metric influences the final trust score. However, the proposed method lacks a defines mechanism against trust attacks. A bipartite graph-based trust management approach is proposed by Aalibagi *et al.* (2021). This model identifies the most dependable service provider for a requestor. However, Hellinger distance is used to create a social network of trustors, matrix factorisation technique is used for predicting the trust of trustees, and centrality and similarity metrics are used as feedback. The limitation of this model is the naive edges (in traditional graphs) present the social relationships and this may lose some information, there is no discussion of the advantages of bipartite graphs over other types of graphs. It is unknown how the trust model will perform under many other trust-related attacks. Marche and Nitti, (2021) present a trust-based attack detection model for SIoT. The trust calculation process in this proposed model is divided into two phases: the training phase and the steady-state phase. During the training phase, trust is calculated using three metrics: computational ability: The static property of an object is used to identify powerful devices, the relationship factor considers the relationships between objects, and external opinions gather recommendations from nearby friends. In addition, the training phase serves as an introduction to the steady state phase. However, the steady state uses the original dynamic information to continuously learn how an object behaves. An incremental Support Vector Machine (SVM) is employed alongside goodness, utility, and persistence scores to quantify trust in an object while continuously learning dynamic information. While this model exhibits improved performance in networks with diverse attacks, it experiences a decline in performance when addressing individual attacks. Moreover, there is a lack of information regarding the discussion of various simulation parameters considered in the performance evaluation. Recently, Alam, Zardari and Shamsi (2022) introduced a Blockchain-Based Trust and Reputation Management system tailored for the SIoT. Their design model encompasses a two-stage parameterised feedback-based framework, focusing on service-driven dynamics and resilience against attacks. Additionally, a punishment system is integrated to detect and eliminate fraudulent service receivers, enhancing the system's robustness and reliability. (SRs) and dishonest service providers (SPs) are "blacklisted," which has an impact on their trustworthiness, reputation, and service charges. By incorporating both "Social Trust" and "Quality of Service (QoS)" factors, the suggested model evaluated reputation, local and global trust of SP. This scheme incorporated Two Stage, stage-parameterised feedback to help better manage the "intention" and "ability" of SRs and to help identify suspect SRs early on. According to reputation values, the suggested paradigm divides SPs into three SP status lists including White List, Grey List, and Black List, each of which has a threshold for the highest service fee that may be charged. White List SPs have the highest per-service charges. There is a reduced selection probability for SPs in other lists. Every comment modifies the SP's reputation and trust value. Sorting SPs enhanced resistance against trust related attacks. The drawback of this scheme is that there is any protection against whitewashing attack or other types of external attacks.

2.6.2. Context-awareness systems

In this section, context-aware TM models are reviewed and summarised in the comparative analysis Table 3

A context-based trust management system for SIoT (CTMS-SIOT) was proposed by Abderrahim, Elhedhili and Saidane (2017). The proposed centralised Trust Management (TM) system comprises both a local TM system within each node and a central TM system hosted on a trust server. This TM system utilises a decision tree tool to identify the most trustworthy nodes in the network capable of providing the requested service for each specific context. Credibility is assessed using the Jaccard coefficient index to measure social similarity, coupled with object behaviour prediction through decision tree algorithms. The architecture of the proposed TM system comprises three main components: objects, service servers, and trust management servers. Various objects with diverse capabilities form the network, utilised exclusively by their respective owners and capable of establishing social connections. The service server facilitates object authentication, while the trust management server gathers feedback from network entities and computes contextual trust and reputation. It is divided into two modules: The trust module, where contextual trust and reputation are calculated. The learning module is used for behaviour classification. This scheme does not consider defence methods against trust-related attacks. As the number of nodes increases, the impact of energy consumption is also an important factor to consider. Khani *et al.* (2018) introduce a mutually contextual trust evaluation scheme that considers social trust metrics (social similarity in terms of friendship, community of interest, and relationships) and QoS metrics to evaluate the trust value of an object. For context detection, energy consumption, location, and task type are integrated to calculate trust metrics. The disadvantage of this scheme is that it does not take into account the dynamically changing environment. The work of (Lin and Dong, 2018) proposed a contextual trust management model based on six parameters: the trust giver, the trust taker, the goal, the trustworthiness assessment, the decision and its subsequent actions and its outcome, as well as the context (task type, environment). In this scheme, the trustworthiness is assessed bilaterally between the trustor and the trustee and is assessed based on the four factors of success rate, profit, damage, and costs. Finally, the trustworthiness calculation in the model takes the dynamic environment into account. It can help distinguish normal behaviour from malicious behaviour in a hostile environment. The limitation of this scheme is that the validity of the scheme is evaluated based on SPA attacks. However, it is important to examine behaviour in other trust-related attacks. Furthermore, Xia *et al.* (2019) outline a context-aware trustworthiness inference model using two trust metrics, namely similarity trust and familiarity trust. Similarity trust is calculated using centrality and community interest metrics. However, familiarity trust considers a kernel-based nonlinear multivariate gray prediction method to calculate direct trust and indirect trust (recommendations).

The trust score is aggregated based on fuzzy logic. This model could be valid considering its resilience to a variety of trust-related attacks. This model was limited because it did not provide enough information about contextual information and discussion of weights for different attributes. Wei *et al.,* (2021) introduced a context-aware socio-cognitive-based trust model tailored for service delegation within the service-oriented Social Internet of Things (SIoT). This proposed Trust Management System (TMS) hinges on two key factors: competence quantification and willingness quantification. Competence is assessed through two metrics: the Degree of Importance (DoI) and the Degree of Social Relations (DoSR). The DoI measures the service provider's competency, including their computational power, storage capacity, and communication abilities. On the other hand, willingness quantification combines the Degree of Contribution (DoC) with the DoSR. The DoC evaluates the service provider's willingness to contribute. The DoSR plays a pivotal role in weighing both competence and willingness, offering a balanced assessment of the service provider's capabilities and eagerness to contribute within the SIoT environment. The trustworthiness value is aggregated by using both the trust factors and the weighted sum technique. The drawback of this model is the integration of numerous trust attributes to calculate the trust value, though, the identification of the appropriate weight for each attribute is missing in the weighted sum. Recently, to prevent service providers from acting untrustworthy by providing poor services or spreading malicious behaviour that referred to as “Trust Related Attacks” (TRA), which damage the trust system, Magdich, Jemal and Ayed (2022) provides an efficient, trustworthy decision solution suitable for SIoT systems. In this research, three steps for attack detection were proposed: actor identification, feature extraction, and attack classification. In the actor identification step, there are three basic characteristics (transaction type, malicious node, and target node) for each TRA. The second step is the feature extraction step. In this step, various features are used to identify attacks and finally, in the attack classification step, the actions of malicious nodes can be evaluated to identify SPA, BSA, and OSA attacks using TAs such as reputation, social similarity, and honesty. This study considers social similarity and honesty in BMA seeking. The TAs (Honesty and Reputation) are evaluated to find OOA. A bad reputation and lack of social affinity are indicators of WA. Low honesty and reputation values help in finding the malicious node that launches DA. The proposed scheme uses ML approaches to classify interactions between nodes as benign or trustworthy based on social trust and service quality characteristics. The limitation of this model is that it only considers TRA and ignores the poor quality of the service provider when nodes are identified as malicious.

Table 2 Context-free TM models in SIoT

Studies	Trust Metrics	Trust Composition	Trust Formation	Trust Aggregation	Trust Propagation	Trust Decision	Trust Update	Trust-Related Attacks
Ben Abderrahim, Elhdhili and Saidane (2017)	Sociability Recommendation Direct observation	Social trust	Multi-trust	Machine Learning	Distributed	Threshold-based	Event-driven	OOA
Truong *et al.* (2017)	Reputation Knowledge Experience	Social trust QoS	Multi-trust	Fuzzy logic	Centralised	Threshold-based	Event-driven	No Attacks
Azad *et al.* (2020)	Reputation Experience	Social trust QoS	Multi-trust	Weighted Sum	Distributed	Threshold-based	Event-driven	No Attacks
Sagar *et al.* (2020)	Community of Interest Cooperativeness Friendship similarity Co-work similarity	Social trust	Multi-trust	Machine learning	Centralised	Threshold-based	Event-driven	No Attacks
Aalibagi *et al.* (2021)	Similarity Centrality	Social trust	Multi-trust	Filtering	Distributed	Threshold-based	Event-driven	OSA
Marche and Nitti (2021)	Goodness score Usefulness score Perseverance score	Social trust QoS	Multi-trust	Machine learning	Distributed	Threshold-based	Event-driven	SPA, WA, OSA, OOA, BMA, BSA, DA
Alam, Zardari and Shamsi (2022)	Availability Accuracy Cruciality Responsiveness cooperation	Social trust QoS	Multi-trust	Weighted Sum	Decentralised	Reputation-based	Event-driven	OOA, DA, OSA, SBA, BMA, BSA, GMA,SPA

Table 3 Context-awareness TM models

Studies	Trust Metrics	Context	Trust Composition	Trust Formation	Trust Aggregation	Trust Propagation	Trust Decision	Trust Update	Trust-Related Attacks
Abderrahim, Elhedhili and Saidane (2017)	Friendship Community-of-interest Object profile Credibility	Time	Social trust	Multi-trust	Weighted Sum	Centralized	Reputation-based	Time-driven	NA
Khani *et al.* (2018)	QoS metric Friendship Community-of-interest Recommendation	Environment Task type Energy consumption	Social trust QoS trust	Multi-trust	Weighted Sum	Distributed	Recommendation-based	Time-driven	SPA OOA, BMA, BSA
Lin and Dong (2018)	Friendship Community-of Interest Gain Damage Cost	Task Type Environment	Social trust QoS trust	Multi-trust	Weighted Sum	Distributed	Reputation-based	Event-driven	SAP
(Xia *et al.* (2019)	Centrality Recommendation Community-of-interest	Time, Location	Social trust QoS trust	Multi-trust	Fuzzy Logic	Distributed	Threshold-based	Event-driven	SPA, OSA, OOA, BMA, BSA
Wei et al. (2021)	Honesty experience	Task type Environment	Social trust QoS trust	Multi-trust	Weighted Sum	Distributed	Threshold-based	Event-driven	SPA, WA OSA, OOA, BMA, BSA, DA
Magdich, Jemal and Ayed (2022)	Honesty Recommendation Reputation Knowledge Cooperativeness COI	Environment Task Type	Social trust QoS trust	Multi-trust	Machine learning	Distributed	Reputation-based	Event-driven	SPA, WA OSA, BMA, BSA, DA

2.7. Challenges in TM in SIoT

While TM has received significant attention and significant insights have been gained in the SIoT, there are still numerous research areas that require further investigation. This section highlights the challenges faced in managing trustworthiness within SIoT given the scope of this study.

1) **The need for a comprehensive and holistic context-based TM framework in SIoT**: Current SIoT TM frameworks are not detailed enough and do not take into account different contextual information that includes a range of things such as: the status of the device, environmental conditions and user social profile. Therefore, there is a need for a TM framework that takes into account various contextual information to provide a more robust and effective system for TM. Such a framework should be able to analyse and assess the trustworthiness of the devices, users and the overall system. This would require collecting and processing data from various sources to assess the trustworthiness of the system in question. Furthermore, the framework should be able to adapt to the changing context and dynamically adjust the trust level based on the current situation.

2) **The need for TM models, which support more dynamic and multi-context problems in SIoT**: Various context-aware TM models have been proposed in the literature (Magdich, Jemal and Ayed, 2022; Xia *et al.,* 2019**;** Khani *et al.,* 2018). These models consider either a single or dual context in the trust calculation, aggregation, propagation, and evaluation processes. However, considering multiple contextual information, including the state of the environment, user behaviour, and device capabilities, could lead to a more accurate assessment of reliability in the SIoT environment and lead to a more comprehensive understanding of the trustworthiness of devices in the SIoT system. Furthermore, the use of multiple contextual information could enable a more flexible and adaptable TM model. A TM model that considers multiple contextual information could adjust trust levels based on dynamic adaptation to changes in the environment. This would enable a more effective response to emerging threats and vulnerabilities in the system.

3) **The need for a customised simulator to simulate real scenarios of SIoT as well as generate a realistic SIoT dataset:** Simulator tools are essential for simulating environments that mimic the SIoT environment and allow researchers to test and evaluate their systems in various scenarios. Datasets are also necessary for the development and testing of systems in the SIoT environment. The availability of datasets could help develop more robust and accurate systems. Therefore, there is a need to develop SIoT simulator tools that generate a realistic SIoT dataset that can be used for trust assessment and facilitate the development of effective and reliable systems. Furthermore, the availability of such a simulator could be helpful in benchmarking and comparing different TM models and identifying their strengths and limitations.

4) **The need for machine learning-based approaches for trust aggregation**: In TM systems for SIoT, the weighted sum mechanism is often used as the aggregation method. However, this method has drawbacks and there is a need for a more complex aggregation method to create a single trust score while taking into account a variety of trust indicators. To address these limitations, develop an intelligent trust aggregation process using machine learning techniques. According to Sagar *et al.* (2022); Sagar, Mahmood, Sheng and Zhang, (2020) machine learning algorithms have the ability to learn from data and create complex models that effectively represent the correlations between different trust indicators. This results in a more accurate trust score. SIoT TM systems can potentially overcome some of the drawbacks of traditional aggregation strategies and increase their accuracy and effectiveness by implementing machine learning-based trust aggregation techniques.

2.8. Summary

IoT has created an environment in which smart devices can communicate and exchange data without human intervention. An extension of IoT, SIoT, has emerged to address challenges such as scalability, trust, and resource discovery. In SIoT, social smart objects can establish social relationships based on their owners' online social networks, enabling better user services and better resource discovery. However, trust assessment in such an environment presents a significant challenge as trust-related attacks and dishonest behaviour can occur. This chapter examines trustworthiness management in SIoT in-depth and examines TM systems and assessment techniques developed for the SIoT environment. A comparative analysis of SIoT TM systems and techniques is presented. Furthermore, the current challenges faced by SIoT that require state-of-the-art solutions are identified.

Chapter 3

MCTM-SIoT Framework

3.1. Introduction

In recent years, the IoT has expanded to include the SIoT. Billion connected and addressable everyday objects are producing vast amounts of data that can be utilised to understand our daily needs (Rad et al., 2020). According to Liu *et al.,* (2013); Sezer, Doğdu and Özbayoğlu (2018) context-aware systems are intelligent systems that help users choose which services to consume based on contextual information and preferences. There are many different categories in which this contextual information can be placed, such as time, place, device, user, and task (De Matos, Amaral and Hessel, 2017). The SIoT is a vital platform for gathering information from a variety of objects that people interact with. This information can then be used to leverage contextual information to address the challenges associated with context-aware systems. Furthermore, it can transform contextual information by utilising the vast amounts of dynamic information produced by various SIoT devices to create more intelligent and dynamic systems. The vast amount of contextual information resulting from the range of services presents difficulties for SIoT because of its dynamic nature (Khan *et al.,* 2020). However, trust is essential to achieve a common goal of trusting collaboration between objects and providing system credibility and reliability. Through the delivery of malicious messages, an untrusted object in the SIoT can interfere with a service's basic functionality, thereby compromising its quality and reliability (Sagar *et al.,* 2023). Therefore, developing an MCTM-SIoT framework is extremely challenging because it lacks the functionality needed to provide dynamic and trustworthy contextual information based on the objects with which users interact with their surroundings. To address this challenge, it is suggested that contextual information gathered from IoT objects be used to develop a framework that incorporates contextual information like user, task, environmental condition, and device characteristics into TM to assess the reliability of devices. This framework seeks to improve device reliability and enhance trust among users.

The organisation of this chapter is as follows: In (section 3.2) sheds light on the key discoveries made during the investigation. (Section 3.3) introduces the MCTM-SIoT framework by going over the key components of SIoT and the modules of MCTM-

SIoT. Furthermore, it provides a validation of the proposed framework. Finally, (section 3.4) summarises the work of the whole chapter.

3.2. Synthesis

In SIoT environment, understanding the contexts of trust between devices appears to be crucial before evaluating and recommending devices as trustee devices. In reality, each object has a particular context in which it trusts another object. The challenges under consideration include the importance of contextual information within the dynamic landscape of SIoT, given the diverse array of applications and services. This dynamic nature necessitates that TM systems tailored for one application or service may not be suitable for others. To the best of the researcher's knowledge, there exist only a few frameworks that we could relate to SIoT, However, these frameworks are not comprehensive enough to represent the full spectrum of trust in SIoT. Also, the existing frameworks are not considered context awareness support trust in SIoT which is the core contribution of this study. Furthermore, the proposed context-aware-based TM models summarised in Table 3 consider single/dual context in trust computation, aggregation, propagation, and evaluation. Nevertheless, it could be crucial to create an efficient TM model that takes into account the multiple context information in terms of where such as environmental condition, what including task type provided by the device, and when (i.e., time).

On the other hand, trust aggregation is an important part of trust management, which determines a single trust score by aggregating the defined trust metrics. The traditional techniques of aggregation proposed in the literature (Table 2 and Table 3) use a linear weighted sum mechanism involves assigning weights randomly, which can either remain static or change dynamically for each trust metric. However, this approach presents certain limitations, such as the lack of ability to determine which trust metric holds the greatest influence on the overall trust level in a given context. Therefore, an intelligent trust aggregation mechanism is required to get around the limits of traditional aggregation methods using machine learning-based or blockchain technologies. Some Researchers have recently proposed the idea of machine learning-based aggregation to determine the weights of each metric in terms of its significance (Magdich, Jemal and Ayed, 2022a; Wei *et al.,* 2021; Marche and Nitti, 2021; Sagar *et* *al.,* 2022). Therefore, with the revolution of SIoT-based environments, it becomes crucial to create a new trust management prototype employing machine learning-based approaches for increased security and performance demands.

Based on the identified gaps, this study aims to create an MCTM-SIoT framework, that incorporates contextual information such as user, task, environmental condition, and device characteristics into trust assessment to select the most trustworthy SP in the SIoT network.

3.3. MCTM-SIoT framework

The SIoT has the potential to advance context awareness because it allows for the exploitation of vast and dynamic data from a variety of SIoT objects to create more dynamic and intelligent systems. The conventional systems take user preferences into account and presuppose that these preferences remain constant as users move from one location to another and engage in various activities. Due to the dynamic nature of SIoT and its wide range of applications and services, one of the challenges that have been taken into consideration is the significant contextual information. Nevertheless, the suggested framework employs contextual information, including task type, environmental conditions, and device attributes, in addition to user social profile, to provide an overall trustworthiness inference for SIoT environments. The framework offers trustworthiness inference for SIoT environments and attempts to illustrate the connection between TM and the fundamental components of a SIoT environment. The SIoT environment encompasses six main components: SIoT Object, Relationship Management, Network Navigability, Resource Discovery, Service Management, and TM. Several related works have addressed these modules, some of which have a relationship management focus (Chen, Bao and Guo, 2016; Atzori *et al.,* 2012). while some other research has focused on Navigability in SIoT networks (Nitti, Girau and Atzori, 2014; Amin, Ahmad and Choi, 2019). The issue of Resource Discovery in this kind of environment has been addressed in numerous related work environments (Hussein *et al.,* 2017; Li *et al.,* 2016). Other authors have addressed the TM issues (Azad *et al.,* 2020; Aalibagi *et al.,* 2021; Sagar *et al.,* 2020; Sagar *et al.,* 2022). Each of these modules has been examined separately in previous research, there lack of an existing framework that identifies the responsible modules, clarifies their connections, and allows trustworthiness inference for SIoT environments, as shown in Figure 6. On the other hand, the framework includes contextual information to address the issues of reliability and credibility challenges that arise in such environments. Therefore, the framework offers a comprehensive view of the SIoT ecosystem and places special emphasis on how different SIoT components interact with one another and with TM, ultimately enhancing trust and facilitating the effective functioning of SIoT systems. The following summarises the main aims of this framework:

1) To establish a connection between the foundational components of a SIoT environment and TM. This highlights how TM principles and mechanisms have been incorporated into the various SIoT infrastructure components.

2) To illustrate how contextual information can be added to trust assessment to enable trustworthy inference in SIoT environments.

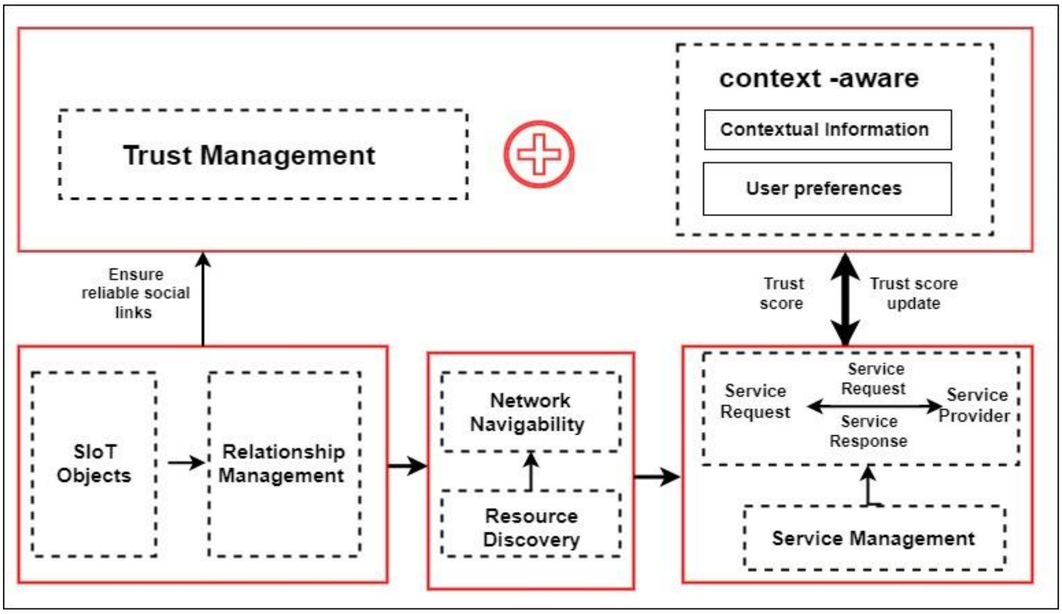


Figure 6 High-level architecture of the MCTM-SIoT framework

3.3.1. SIoT components

The SIoT environment contains six main components: SIoT Object, Relationship Management, Network Navigability, Resource Discovery, Service Management, and TM.

3.3.1.1. SIoT object

SIoT objects, such as sensors, actuators, and smartphones, transmit and receive data (Zhang *et al.,* 2023). These objects use a variety of protocols to establish connections within a network and communicate with other users and objects. The ability of SIoT objects to sense, act, process, and transmit data demonstrates their intelligence. Social networks and proximity-based discovery are two methods by which SIoT objects communicate with other entities (Atzori, Iera and Morabito, 2014). One of the key features of SIoT objects is their interoperability, which enables seamless communication and cooperation between multiple objects. They can be separated into service providers and requesters, which enables efficient interaction and communication within the SIoT ecosystem. According to (Sagar *et al.,* 2023) a service request is an entity that sends service requests to other entities, and a service provider is an entity that provides services to other entities in the SIoT environment.

3.3.1.2. Relationship management

In SIoT environments, diverse relationships and social interactions link various types of objects. According to Chen, Bao, and Guo (2016), three distinct relationship types emerge among object owners: the friendship relationship, signifying a level of intimacy, the community of interest relationship, fostering shared experiences among owners with common interests and the social contract relationship, representing agreements or understandings regarding social responsibilities or obligations. Atzori *et al.* (2012) delineate various forms of social interactions among objects, illustrated in Figure 7. A parental relationship is established for objects originating from the same manufacturer. Objects owned by the same user are defined within an ownership relationship. Objects located in close proximity to one another form a co-location relationship, while objects collaborating on common tasks are classified under a co-worker relationship. Additionally, Ali *et al.* (2018) introduces the Stranger Object Relationship (STGOR) for objects encountering each other in public spaces or while on the move, and the Service Object Relationship (SVOR) for objects managing similar service requests within the same service composition. According to previous related studies (Eddy and Oussama, 2018; Wei *et al.,* 2018) relationships in a SIoT system are classified into four categories: User to User (UU), User to Object (UO), Object to Object (OO), and Object to Service (OS) Relationships. The first function of the Relationship Management module is the definition of different types of relationships. The next function will be to establish rules for determining such relationships. For example, how can two objects be considered co-located based on proximity? In addition, this module is tasked with establishing and updating these relationships, which are typically dynamic and subject to change over time.

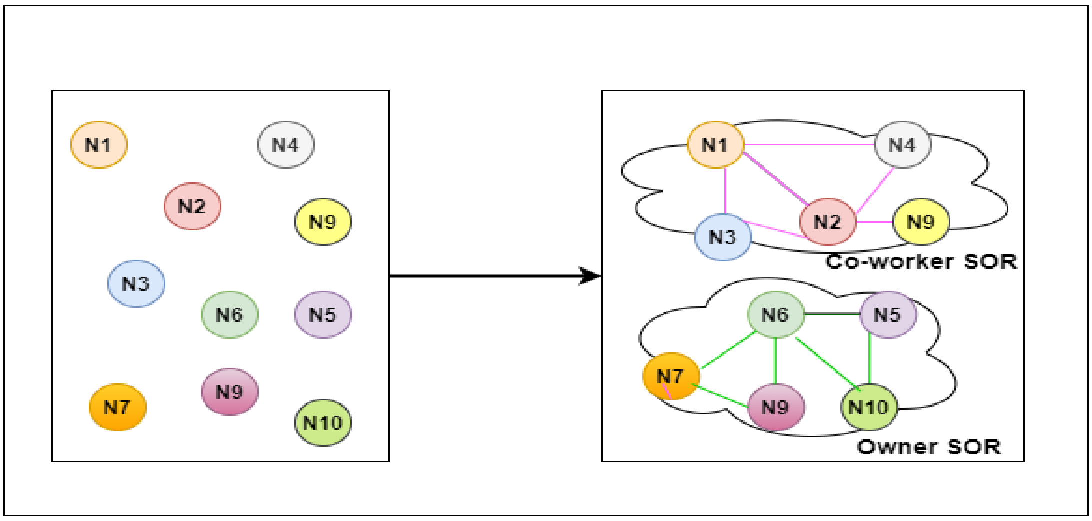


Figure 7 Relationship management

3.3.1.3. Network navigability

An SIoT network is based on the notion that enables objects to navigate through the network of other objects to find the most efficient path to provide a service to the user. This is important in SIoT because it allows objects to collaborate and share resources to provide better services to users (Nitti, Atzori and Cvijikj, 2014; Rad *et al.,* 2020). Each object has the capability to search for the desired service by leveraging relationships, querying friends, friends of friends, and so forth in a distributed manner, ensuring an efficient and scalable discovery of objects and services. This approach mirrors the principles observed in social networks among humans. The sociologist Stanley Milgram's theory on the small-world phenomenon underpins the assumption that an SIoT network will possess navigability akin to that found in human social networks (Nitti, Atzori and Cvijikj, 2014). This paradigm requires each object to implement search functions, store and manage friendship-related information, and eventually make use of additional tools like the trustworthiness relationship module to assess each friend's dependability. According to Kowshalya and Valarmathi (2015), the quantity of relationships influences memory usage, the use of computational resources, and battery life, as well as the effectiveness of service search operations. Accordingly, choosing the right friendships is essential for deploying the SIoT successfully.

3.3.1.4. Resource discovery

In SIoT, resource discovery is the process of locating and gaining access to resources that are available within the network of interconnected IoT devices, such as devices, services, data, or sensors (Khalil *et al.,* 2020; Kamel *et al.,* 2021). Resource discovery is essential to the SIoT because it allows users to access and make use of the network's resources. It can be challenging due to the large number of IoT devices, the variety of resources, and the dynamic nature of the network. Numerous strategies, such as machine learning algorithms, social networking principles, and semantic technologies, have been put forward to address these issues (Khanfor *et al.,* 2020). Resource discovery involves the services discovery and the objects discovery. Service discovery is the process of locating and deciding which services are available within the network (Khanfor *et al.,* 2020). Service discovery is an essential component since it allows objects to cooperate and share resources to give users better services (Hamrouni, Ghazzai and Massoud, 2022; Rad *et al.,* 2023). On the other hand, object discovery is the process of discovering and identifying physical objects that are linked to SIoT (Nitti, Pilloni and Giusto, 2016). Object discovery is crucial because it enables users to find the particular devices that are gathering information or carrying out tasks in an SIoT environment (Hassan *et al.,* 2020). Service and object discovery are closely related to one another. While object discovery can assist in identifying the identified devices that are providing those services, service discovery is frequently utilised to find devices that are providing specific services. In light of this, service and object discovery are crucial components of the SIoT that let users find and engage with connected devices and services. Together, they offer an effective and scalable means for objects to cooperate and share resources in order to offer users improved services.

3.3.1.5. Service management

In SIoT, service management ensures that users not only find individual services but can also combine useful services as needed. The two main attributes of this component are service composition and service selection (Chen, Bao and Guo, 2016). Service composition is a method for combining different services to meet user needs. Service composition is crucial in the SIoT environment to handle complex user requests (Aoudia *et al.,* 2019). Social IoT devices are virtually connected via social networks, the system breaks down the request and finds appropriate services and service providers to compose a comprehensive service that satisfies the user's needs (Ahmed *et al.,* 2023). Service selection is one of the most important processes in the SIoT, which is finding and choosing the right services to suit users' needs in a particular context as demonstrated in Figure 8 (Khanfor *et al.,* 2020).

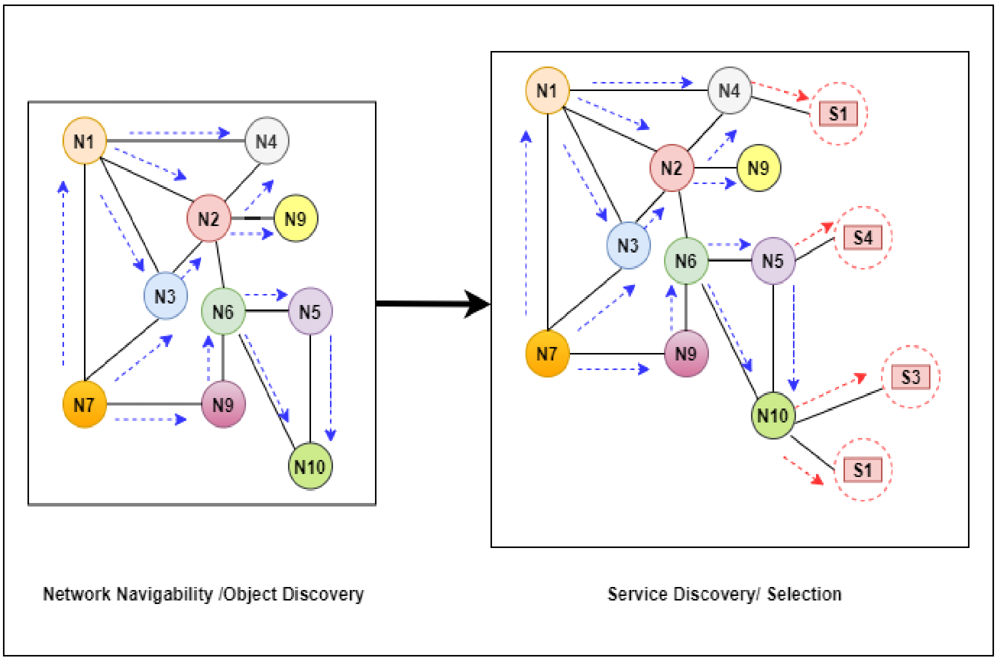

N1
N4
N2
N9
N3
N6
N5
N7
N9
N10
Network Navigability /Object Discovery
N1
N4
S1
N2
N9
N3
N6
N5
S4
N7
N9
N10
S3
S1
Service Discovery/ Selection

Figure 8 Service management in SIoT

3.3.1.6. Trust management

An entity's trust is a multifaceted concept that cannot be adequately captured using a single parameter (Sagar *et al.,* 2023). It encompasses a blend of diverse characteristics within an entity, such as integrity, reliability, safety, and capability. It represents the extent or level of confidence, belief, and expectation regarding these attributes (Truong *et al.,* 2017a). Another concept closely related to trust is reputation. An entity's reputation is established through direct or indirect knowledge and information derived from past interactions with other entities. The social trust aspect encompasses three main categories: general trust characteristics, social trust characteristics, and social trust-related attacks. These categories are thoroughly explored in the literature review and are summarised in Figure 9. The TM systems comes into play and help the trustor node in calculating the trust value of the trustee node. TM includes five phases in each environment, namely information gathering, trust calculation, trust decision, trust update, reward and punishment, which are discussed in the literature review and summarised in Figure 10. The overall trust management process comprises three steps: In Step 01, the service requester solicits the trust score of the objects offering the desired service from the trust management system. Subsequently, in Step 02, the object can procure the service from the service provider boasting the highest trust score. Lastly, in Step 03, upon receiving the service response from the service provider, the service requester updates the trust value within the trust management system.

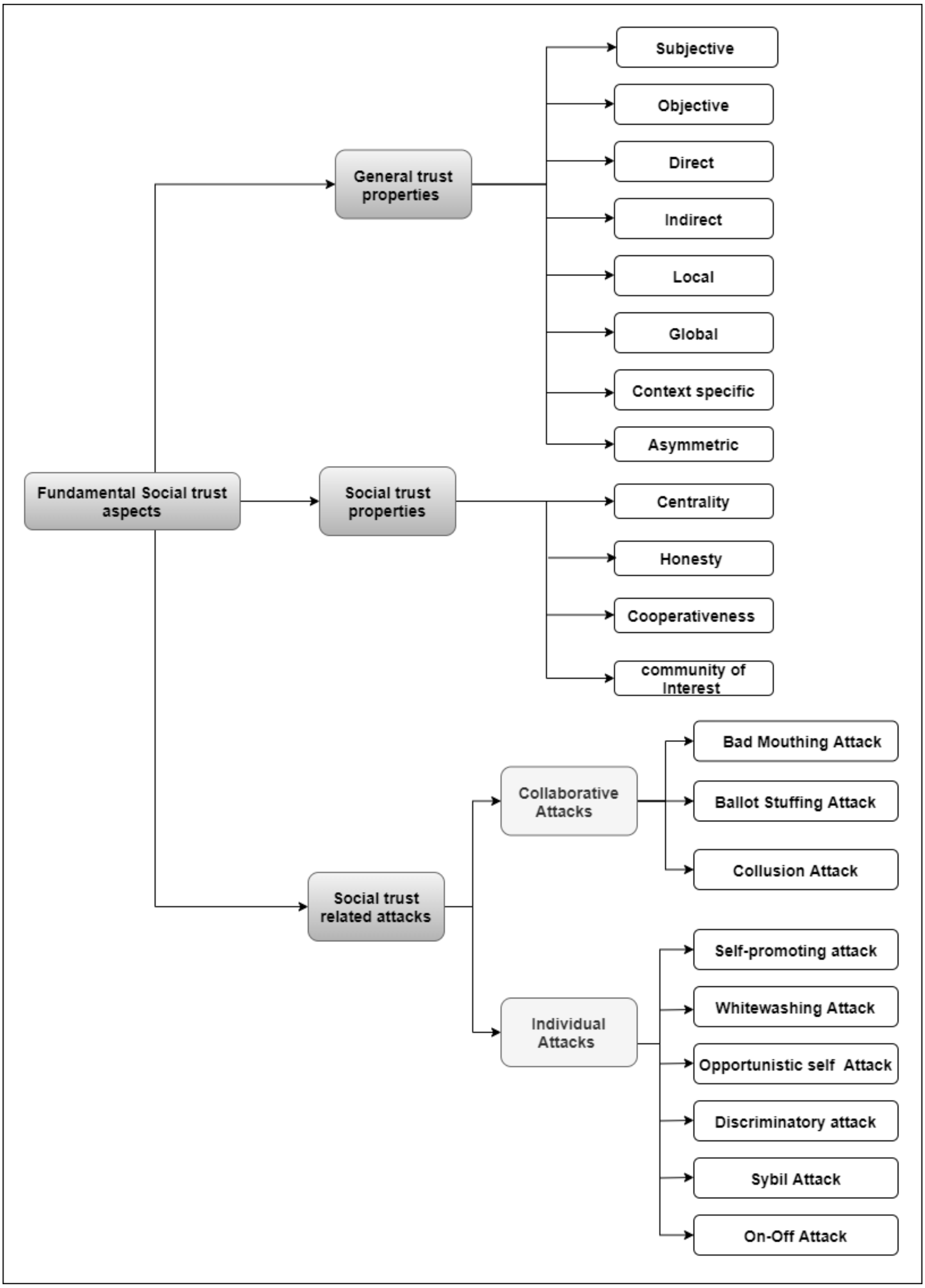


Figure 9 Fundamental social trust aspects

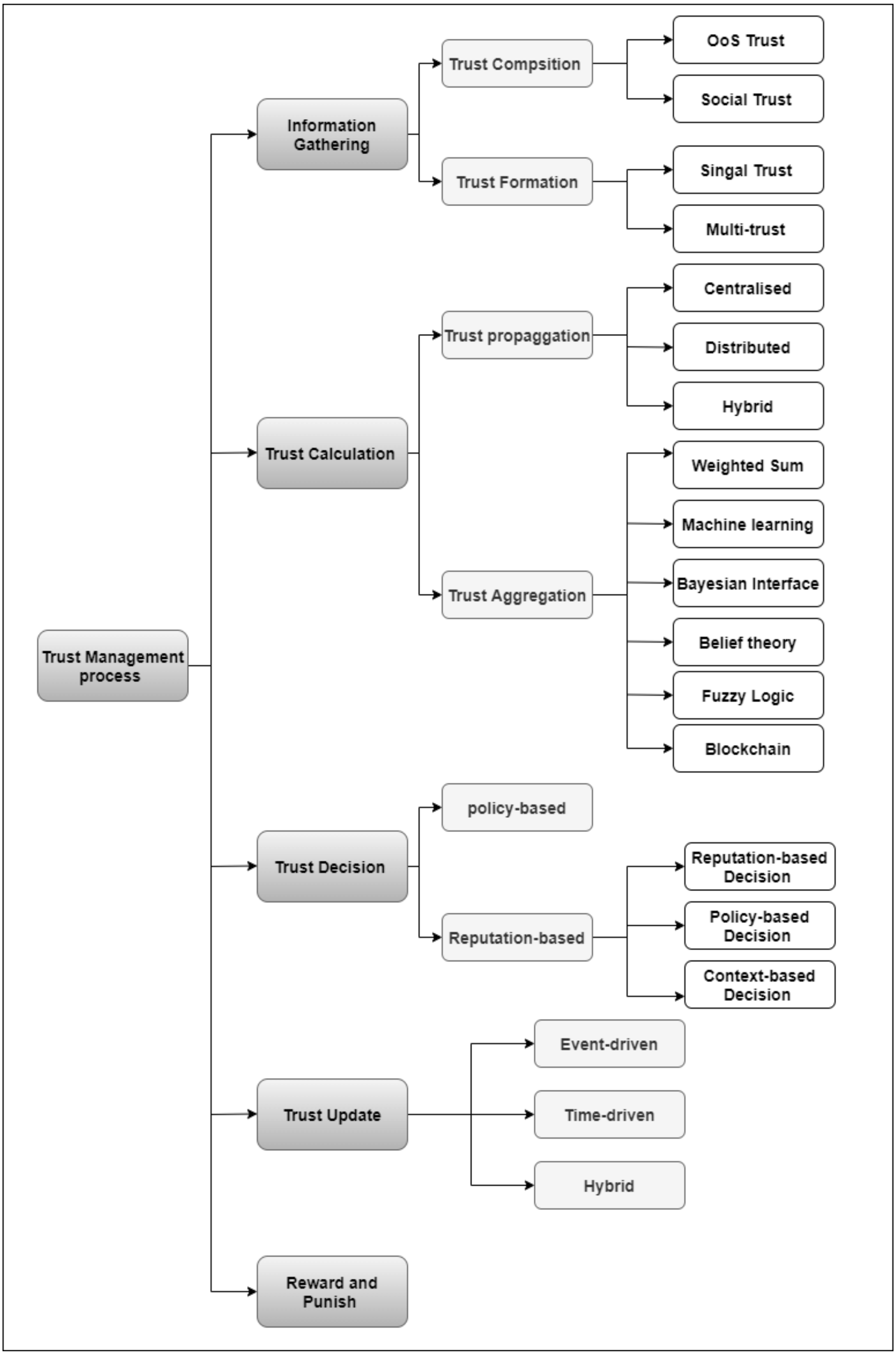


Figure 10 Trust management process

3.3.2. MCTM-SIoT framework modules

The MCTM-SIoT framework consists of four key modules: social relationship selection, friendship selection and management, service search, and context-aware TM. The basic functionality of the framework is guaranteed by the fact that each module consists of at least two SIoT components.

3.3.2.1. Social relationship selection module

Social relationship selection is essential to SIoT as it involves creating and maintaining social connections between users and devices. building these social connections between users and devices involves various elements such as interests, preferences, location, context, and social networks (de Matos *et al.,* 2015). In SIoT, the selection of social relationships requires careful consideration of user data security and privacy. Therefore, building social relationships should include clear consent procedures and give users authority over the information they share with other users or devices (Wei *et al.,* 2018). Another crucial factor is promoting device and network interoperability. To enable seamless connections and interactions between users and various devices and networks, furthermore, device compatibility allows users to connect and communicate with various networks and devices without technical difficulties (Wei *et al.,* 2018). Two essential SIoT components support the social relationship selection module including SIoT object and relationship management as shown in Figure 11. These components enable the selection of social relationship ties between smart objects, creating a social structure of smart nodes within the SIoT network. The concept of social relationships in SIoT involves various types of relationships among IoT entities, such as OOR, Co-WOR, Co-LOR, POR, SOR to enhance services and content delivery within the SIoT ecosystem.

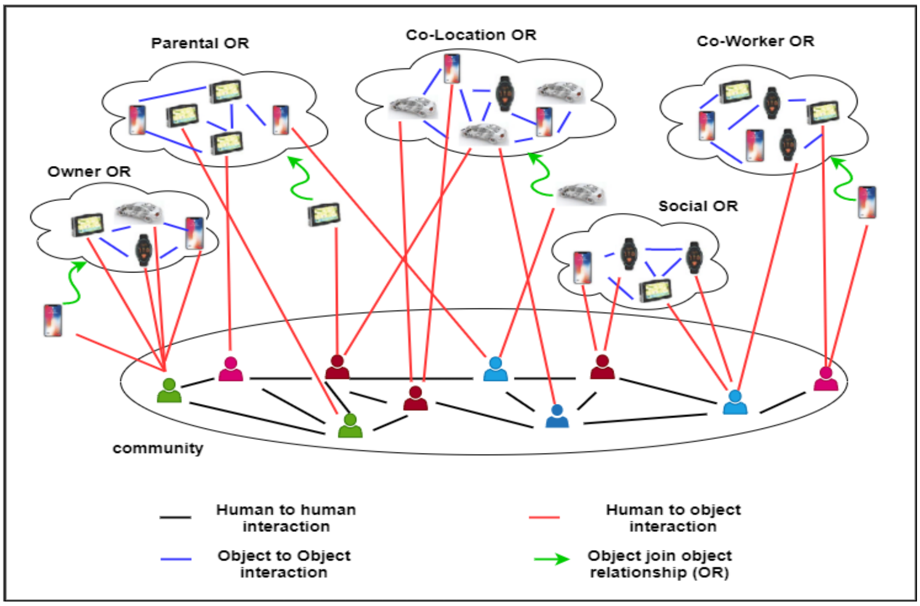

Parental OR
Co-Location OR
Co-Worker OR
Owner OR
Social OR
community
Human to human interaction
Human to object interaction
Object to Object interaction
Object join object relationship (OR)

Figure 11 Social relationship selection

3.3.2.2. Friendship selection and management module

Friendship selection plays an important role in SIoT, it consists of a network of intelligent devices connected to one another to perform various tasks and communicate with users and other devices (Farhadi *et al.,* 2021). The process of selecting and forming friendships between these entities is a crucial factor in the SIoT environment (Nitti, Atzori, and Cvijikj, 2015). The friendship selection process consists of three steps: friendship initiation, friendship update, and friendship termination. A device can initiate a friendship by sending a request to another device based on predetermined parameters, such as Proximity. The level of friendship between two devices may change during the update phase depending on a number of factors (Farhadi et al., 2021). For example, if Device D2 becomes unresponsive, the reciprocity factor could decrease, causing Device D1 to lower its friendship level and ask higher-us friends for help. Finally, the two devices have the option to end their friendship if they wish. Friendship selection in SIoT is critical to improving service discovery and enabling effective resource discovery, including object and service discovery. Building social relationships within the SIoT framework leverages the navigation capability of the network to facilitate the navigation of nodes within the network, ensuring scalability and efficient resource utilisation (Amin, Ahmad and Choi, 2019). This process includes various SIoT components such as resource discovery, network navigability, and relationship management. The complexity of the friendship selection process in SIoT highlights the importance of considering factors such as scalability, interoperability, and trustworthiness when establishing friendships between devices to improve interaction and service delivery within the network (Rad *et al.,* 2020).

3.3.2.3. Service search module

In SIoT, service search is the process of finding appropriate services that meet user needs while reducing search time and effort. Quality of Service (QoS), cost, reliability, compatibility, and user preferences are just some of the factors that need to be considered when selecting an SIoT service. These factors are crucial to ensure that the selected service meets the user's needs and expectations within the SIoT ecosystem (Nitti, Pilloni and Giusto, 2016). Once friendships are made and maintained, users can connect and access a variety of services on the SIoT's social network. The social component of SIoT leverages the combined resources of their social network and allows users to find and use services that their trusted friends have either used or recommended. Additionally, by integrating social connections, users can benefit from trust-based service selection and personalised recommendations. In SIoT, service discovery is based on two fundamental elements: service management and service discovery. These elements work together to help users find the most relevant services and combine them according to their individual needs. Within the SIoT network, service discovery is responsible for identifying the available services and providing users with a list of relevant services to choose from. It is also important to reduce the time and effort required for searching (Khanfor *et al.,* 2020). Service management and service discovery work hand in hand to help users find the most relevant services and combine them according to their individual needs.

3.3.2.4. Contextual TM module

In SIoT, the contextual trust management module is becoming increasingly important. This module evaluates the reliability of services, devices, and users, taking into account the dynamic and diverse nature of the SIoT environment (De Matos, Amaral and Hessel, 2017). The SIoT context is taken into account in the trust assessment by the context-aware TM module. Contextual information is crucial in SIoT. It describes the ability of a device to understand the situation and environment in which it operates. Devices that want to communicate more intelligently and individually with users and other devices must have contextual information to be able to choose which services or information they want to offer to the user (Atzori *et al.,* 2011). By highlighting the specification of the situation in which the trust exists, context is a crucial component that influences trust. Interactive queries were used in context-based trust assessment to retrieve relevant data from remote devices. Devices in SIoT environments can generally trust each other based on various contextual factors, which enable them to request or provide different services at different times and contexts. To provide relevant information or services to the user, various contextual information is taken into account, including user's social profile, device status, environmental condition, and service requirements. Contextual information can be integrated into TM (see Figure 12) to improve decision-making and service selection by improving the precision and personalisation of trust assessments.

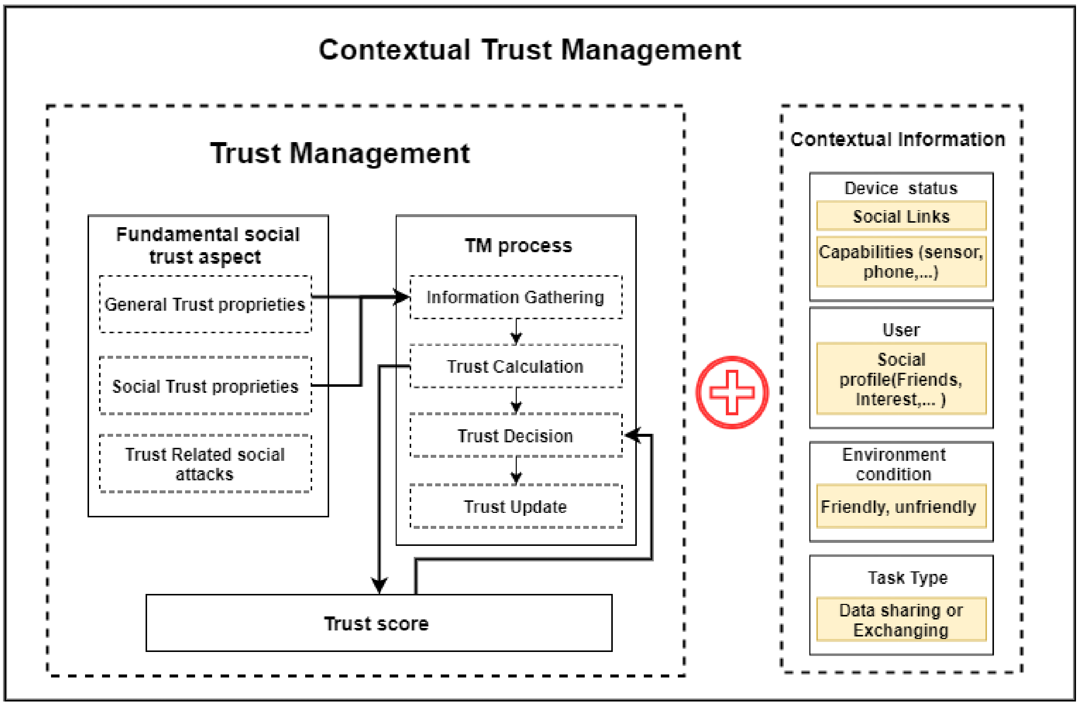


Figure 12 Contextual Trust Management

The Figure 13 shows a MCTM-SIoT framework where the contextual TM module works horizontally across the various modules mentioned, as the contextual TM module is closely linked to the service search, friendship selection, and management and social relationship selection modules in the SIoT ecosystem. It provides mechanisms for assessing the trustworthiness of services and social relationships. by integrating these modules with the contextual trust management module: The contextual TM module helps users evaluate the trustworthiness and credibility of services offered on the SIoT network and allows users to include a trustworthy service as one of the selection criteria when searching services. This allows users to choose services with a higher level of reliability and trust. To evaluate the trustworthiness of a potential friend, the friendship selection module and the contextual trust management module can be combined. Before adding another user as a friend, the contextual TM module allows users to assess the reliability and credibility of that user. Similarly, contextual TM and social relationship selection modules can support this process by assessing the level of trustworthiness of possible social relationships. They help users make informed decisions about building and maintaining relationships with others in the SIoT network based on their trustworthiness.

The MCTM-SIoT framework addresses a notable gap in existing SIoT systems by supporting multiple contexts in trust computation rather than the single or dual contexts found in other frameworks. This multi-context approach is critical because SIoT environments are inherently dynamic, with devices and users constantly interacting in different settings. The framework's unique multi-context mechanism, which incorporates user, device, environmental, and task context into the TM system, enhances the accuracy and relevance of trust assessments, thereby facilitating safer and more reliable device interactions.

Additionally, the use of machine learning-based techniques to weigh trust metrics introduces a more intelligent approach to trust aggregation. This flexibility makes the framework adaptable to various applications within SIoT environments, where different devices and contexts may require unique trust profiles.

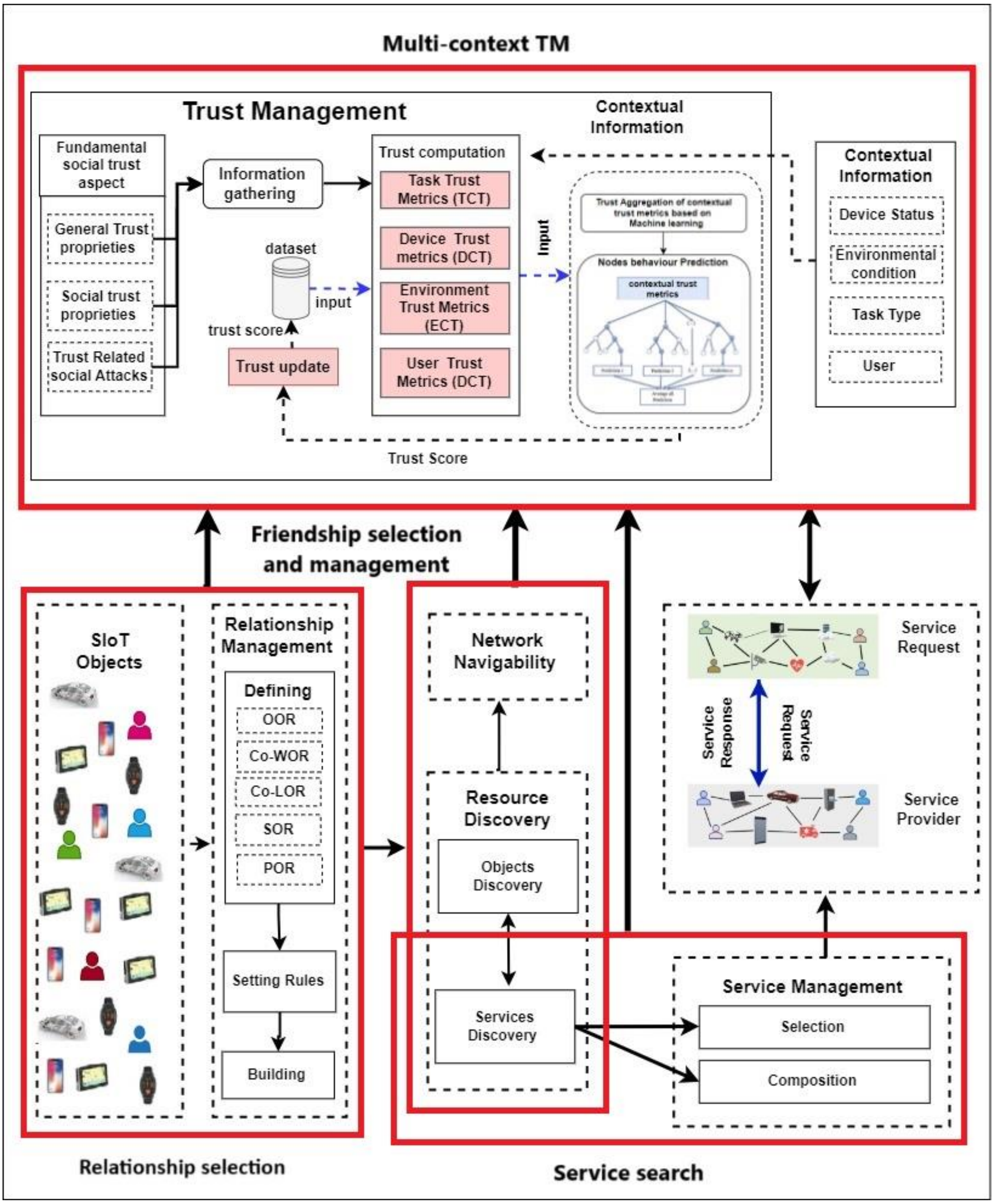


Figure 13 MCTM-SIoT framework

3.4. MCTM-SIoT framework validation

The MCTM-SIoT framework aims to improve the security and reliability of SIoT networks by incorporating contextual information such as user social profile, device status, environment condition, and task type in trustworthiness evaluation to ensure trustworthy communication between any two nodes in the network. To guarantee that the framework effectively meets user needs, the validation of the framework is carried out using both mathematical and experimental techniques.

Mathematically, a set of trust contextual metrics, namely user context trust metrics, device context trust metrics, environmental context trust metrics, and task context trust metrics, served as the basis for MCTM-SIoT model. These metrics used to assess the trustworthiness of a device are defined as follows:

1. User context Trust Metrics (UCT) consider the user's ability to provide services based on the information collected about the user, including profile information and interest lists, social network.

2. Device context Trust Metrics (DCT) measure the honesty of a device in accurately reflecting its opinions on a specific task. The DCT metric is evaluated based on two key factors: the credibility of the object and the social object relationship. The credibility of an object takes into account the accuracy, completeness and timeliness of the information provided by the device. The relationship between social objects evaluates the relationship between the device and other devices on the network.

3. Environmental condition context Trust Metrics (ECT) evaluate the trustworthiness of the environment. Unfriendly environmental conditions such as a node with many connections can reduce the effectiveness of SIoT systems. Therefore, the ECT metric can be used to evaluate the level of trustworthiness in a particular environment.

4. Task context trust metrics (TCT) evaluate the reliability of the recommendation and service provided by the provider node in a particular task. The TCT metric can be calculated based on various factors, including the provider's recommendation or past performance.

Experimentally, SIoT simulator tool is developed to simulate and analyses the behaviour of SIoT systems such as devices, sensors, and users in different SIoT contexts, enabling the generation of realistic SIoT data to evaluate the effectiveness of the elaborated MCTM-SIoT framework and model. The simulator tool incorporates a range of functionalities, involving the modelling of various attacks and vulnerabilities.

3.5. Summary

Developing an MCTM-SIoT framework for trustworthiness inference in SIoT environments is critical to address the security challenges posed by the proliferation of interconnected devices. The proposed framework is modular, flexible, and new modules and algorithms can be added as needed. This guarantees that the framework adapts to changing SIoT environments and remains effective over time. Implementing a trustworthy SIoT environment is critical to protecting sensitive data and ensuring the continued expansion and success of SIoT. To maintain the security of SIoT environments and give users confidence in the SIoT systems and devices they rely on. The next chapter evaluates the proposed framework by proposing and modelling a MCTM-SIoT model considering various contextual factors. This model can provide users with a reliable and transparent method for assessing the trustworthiness of SIoT devices and their communications.

Chapter 4

MCTM-SIoT Model

4.1. Introduction

The study of the SIoT paradigm and TM systems has not only offered insights into the advantages of SIoT and its practical applicability but has shed light on its limitations and unique characteristics. Moreover, it has facilitated the recognition of various challenges encountered in TM systems. Context awareness is one of the biggest problems encountered by TM systems in SIoT environments. Additionally, an intelligent trust aggregation process is required to combine the selected trust indicators and produce a single trust score for the SIoT nodes. However, machine learning-based approaches could be a way to overcome these limitations. The TM process consists of four main steps. “Trust composition”, "Trust aggregation”, “Trust propagation” and “Trust update”. The trust composition step consists of selecting the contextual trust metrics. The second step which is trust aggregation, focuses on attack detection, node classification, or node behaviour prediction. The proposed model centers on node behaviour prediction. The propagation steps used in this study are based on a distributed scheme in which each IoT device autonomously shares trust observations with other IoT devices that come into contact without the help of a central entity. Finally, the event-driven update approach is chosen to ensure scalability, dynamism, and resource efficiency.

This chapter is organised as follows: (Section 4.2) classifies the existing context-based TM models in SIoT based on their trust calculation methods. (Section 4.3) contains a description of the research problem. (Section 4.4) provides a representation of the architecture and process of the MCTM-SIoT Model, which deals with the contextual information contained in the SIoT environment, namely device status, task type, user social profile, and environmental conditions. Finally, (section 4.5) summarises the work in this chapter.

4.2. Classification of existing context-based TM models in SIoT

Through the literature review, various context-aware TM models, as listed in Table 3, took into account either single or dual contextual information when aggregating, propagating, and evaluating trust. These models enable more precise and efficient trustworthy assessment in the SIoT environment by calculating the trust of SIoT nodes using probabilistic models or machine learning techniques.

4.2.1. Trust calculation based probabilistic models

Probabilistic models are widely used in SIoT to represent the uncertainty in the reliability of IoT devices when calculating trust. To calculate trust in SIoT, trust values from different sources must be combined. These sources depend on previous interactions, the characteristics of the device, and the social connections between devices. The combination of these data sources enables the calculation of an overall trust score for a device using probabilistic models. Bayesian network is a popular probabilistic model type used in SIoT trust management models (Khani *et al.,* 2018; Lin and Dong 2018; Xia *et al.,* 2019; Wei *et al.,* 2021). The probability of a variable can be updated based on the occurrence of another variable using Bayesian networks, which show the probabilistic relationships between different variables. To update a device's trust score based on new information, such as how the device behaves in a particular situation.

4.2.2. Trust calculation-based ML algorithms

Based on related literature review, several context-aware TM models utilising machine learning to calculate trust have been proposed (Abderrahim, Elhedhili and Saidane, 2017; Magdich, Jemal and Ayed, 2022). ML is a useful technique for trust calculations for several reasons. First, since complex and dynamic data often occurs in SIoT applications, ML algorithms are well suited for processing it. The use of patterns and relationships that ML algorithms discover in the data to make predictions and decisions based on new data. Second, calculating trust manually can be difficult and time-consuming, ML can help automate it. To increase the scalability and effectiveness of TM in SIoT applications, therefore, ML algorithms possess the capability to swiftly and accurately process vast volumes of data. Third, ML in TM can help address the problem of uncertainty and incomplete information. Information about device and user reputation and behaviour may be limited or untrustworthy in

SIoT applications. However, using the limited data available, ML algorithms can probabilistically predict the trustworthiness of users and devices. These predictions can then be updated as new data becomes available. Finally, TM in SIoT applications can become more accurate and effective using ML, As ML algorithms can detect patterns and anomalies in user and device behaviour that may be difficult for humans to detect by learning from past data. This can improve the overall security and reliability of the system by helping to detect and contain malicious behaviour.

Typically, probabilistic models are used to calculate trust scores of the SIoT nodes, which take into account a variety of variables, including device behaviour, communication patterns, and historical data. However, these models can generate a significant computational load, which can be difficult for SIoT devices with low computational capabilities. Additionally, ML-based solutions are becoming increasingly popular in the SIoT space due to their ability to generate accurate predictions and detect anomalies in the network. Nevertheless, these solutions have certain drawbacks, including their high computational cost, which may lead to higher resource consumption and higher computational latency. One potential solution to address these limitations is to develop an optimised ML-based aggregation method. Rather than utilising individual objects in the network to train the models, this approach aggregates the trust metrics of groups of objects. Using a prediction approach, the ML algorithms can be trained on a smaller subset of the network data. This reduces the computational effort and latency associated with training and inference and increases the effectiveness and precision of the trust assessment process. Additionally, it is important to consider that the reliability of the TM model results may be affected by the lack of a real SIoT dataset or SIoT simulator. Accurately assessing and validating the effectiveness of these models could be challenging without sufficient data. To ensure the validity of research in this area, it is crucial to use the right SIoT datasets.

4.3. Problem Statement

In SIoT modelling, a set of users U= $\{u_1 ,\dots, u_n \}$ with cardinality N and a set of devices D= $\{d_1 ,.. d_i ., d_r \}$ with cardinality R. Where: each user own one or more devices, and each device belongs to its user (owner). Each device in the system can provide and request services S from different devices in the network, presented by S= $\{s_1, \dots, s_i\}$ which all considered in user centric architecture (Figure 14). In the SIoT environment, the service provider (SP) might be service request (SR) in any device's connection. Moreover, both SP and SR are defined by a vector containing multi-context attributes: Device $(\boldsymbol{C_D})$**,** Environmental condition $(\boldsymbol{C_E})$**,** User $(\boldsymbol{C_U})$ and task $(\boldsymbol{C_T})$**.**

Denote by equations (1) and (2):

$$SP_i = \begin{bmatrix} \boldsymbol{C_{Di}} \\ \boldsymbol{C_{Ei}} \\ \boldsymbol{C_{Ti}} \\ \boldsymbol{C_{Ui}} \end{bmatrix} \qquad (1)$$

$$SR_j = \begin{bmatrix} \boldsymbol{C_{Dj}} \\ \boldsymbol{C_{Ej}} \\ \boldsymbol{C_{Tj}} \\ \boldsymbol{C_{Uj}} \end{bmatrix} \qquad (2)$$

Devices, users and services are three main components of the proposed user-centric SIoT architecture, where each device keeps a record of its trust score, transaction history between nodes, its profile (capacity, location, etc.), and the profiles of its owners. Devices can retrieve information about user relationships. The proposed model can be represented as a social graph consisting of interactions between recommendations and social relationships. The interactions include the services that are exchanged between the devices as part of data processing. For example, if a device provides a particular service, it will be recommended to other devices that have a strong social connection to that device. In addition, these devices are socially connected and consist of communities that have the same friends and usually interact socially with each other through their owners' social networks, establishing a variety of social interactions, including:

1) Human-to-human interaction: In SIoT environments the basic task is to detect users' behaviour and their relationships to evaluate the trust in the devices. Users with similar relationships and interests are viewed as more trustworthy than others because of their social relationships. Therefore, if the user acts maliciously, their device cannot be classified as an honest device. Some

characteristics such as friendship and community of interest (CoI) could be taken into account in this type of interaction.

2) Object-to-object interaction: SIoT devices exchange services with each other through communication. Therefore, each device assesses the other, considering their social interactions as part of the evaluation process. All devices are maintained based on their profile information such as manufacturer, location, conditions, and owner. Additionally, equivalent devices from the same person can work together on demanding tasks. Therefore, in our proposed TM model, both social trust and QoS are used to evaluate this type of interaction.

3) Human-to-object relationship: in the SIoT system, users must evaluate both their own devices and those on the network to uphold secure communication. Typically, in the SIoT environment, each user is responsible for assessing their personal devices as well as those belonging to others on the network to ensure effective communication. Moreover, when establishing interactions, ownership relationships should be considered. Integrating QoS into the TM process enhances user satisfaction by considering constraints and user preferences for specific tasks.

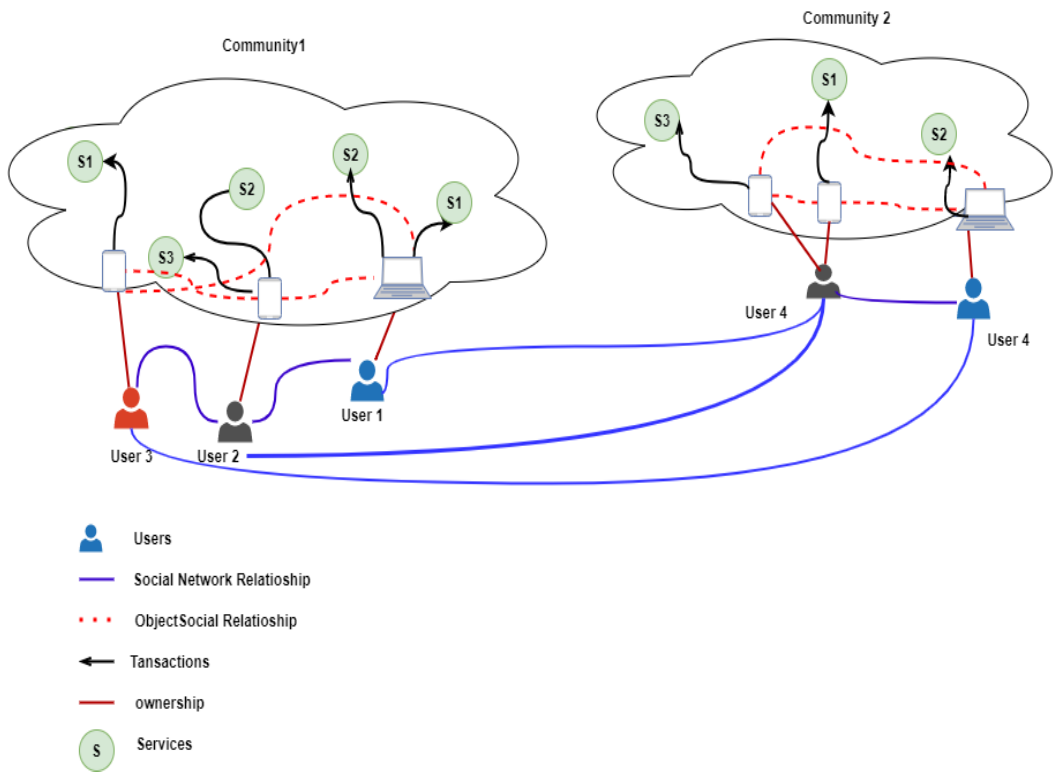


Figure 14 SIoT user centric architecture

4.4. MCTM-SIoT model

This section proposes the MCTM-SIoT model architecture and discusses the TM process including trust composition, trust aggregation, trust propagation and trust update for the proposed TM model.

4.4.1. MCTM-SIoT model architecture

In this section, an overview of the proposed model architecture entitled “MCTM-SIoT model” is provided. It conveys the previously addressed issue of the influence of contextual information on the trust assessment process of each node presented in the SIoT network. In fact, MCTM-SIoT helps the end user to select the best service provider in the absence of node behaviour history. This model integrates contextual information features into the trust assessment of SIoT nodes. The trustee node acting as a service provider (SP) can be connected to a trustor node acting as a service request (SR) to receive services (Sagar *et al.,* 2023). Therefore, SP would collect information and send a service to the SR. In a specific SIoT context. To ensure trustworthy communication between any two nodes in the network, a trust assessment is required before every transaction. The evaluation process includes three phases: the initial communication phase, the service request phase, and the trust assessment phase, as shown in Figure 15.

1) **Initial communication phase**: At the beginning of the network, each node has an initial trust value for new neighbour based on the social relationship between two nodes. The object relationship (OR) represents the type of relationship between two objects (Nitti, Girau and Atzori, 2014). It is used to enhance the information provided by friends. Where the high value leads to higher trust between two nodes that belong to the same object relationship. Therefore, it is rare to detect a malicious node between two nodes owned by the same owner or workplace. Therefore, the highest relationship factor value is assigned to OOR, CWOR and CLOR. The SOR is assigned a smaller relationship factor value when the object comes into contact sporadically or continuously. Finally, the riskiest social relationship since objects that were made at the same time by the same manufacturer but never met (Nitti *et al.,* 2012). Therefore, the initial value of node "A" from the perspective of another node "B" is defined as defined in Table 4. When two nodes are linked by multiple relationships, the strongest relationship is prioritised, given its highest level of influence or significance (Nitti, Girau and Atzori, 2014). All of these evaluations are stored in a module embedded in the nodes.

2) **Service request phase**: When a user requests service S, the user object needs to send a request to all user objects in the community. The detection mechanism is then triggered and the objects that can provide the requested service S are returned. Therefore, the service request checks its local trust table to determine its trust interaction. If no history is found about them, a trust assessment is required before this transaction.

3) **Trust evaluation phase**: This phase requires several steps. If no history of the provided service is initially available, contextual trust metrics are calculated to determine the node's trust score. ML techniques are then used to predict the obtained trust value based on the calculated metrics. In addition, if the called

node refuses to perform service to the SR node, the task request is forwarded to the next trusted SP in the list, ensuring continuous service delivery and task fulfilment within the network.

Figure 16 shows the architecture of the proposed MCTM-SIoT model. In the trust composition step, four contextual trust metrics with their respective functions are defined. The contextual trust metrics include device context trust metrics, user context trust metrics, task context trust metrics, and environmental context trust metrics which are based on the contextual information about user behaviours, device status, task type, and environmental conditions discussed in chapter 02. Each metric is calculated based on some basic trust metrics. The UCT are based on social similarity (Friendships and communities of interest). The DCT are based on object relationship and object credibility. The TCT are based on recommendations. Finally, the ECT are based on an unfriendly environment. The trust aggregation step takes as input these different contextual trust values to identify the influence of each contextual metric on the overall trust score of each node and predict the node behaviours to select the best service provider using a ML-based approach.

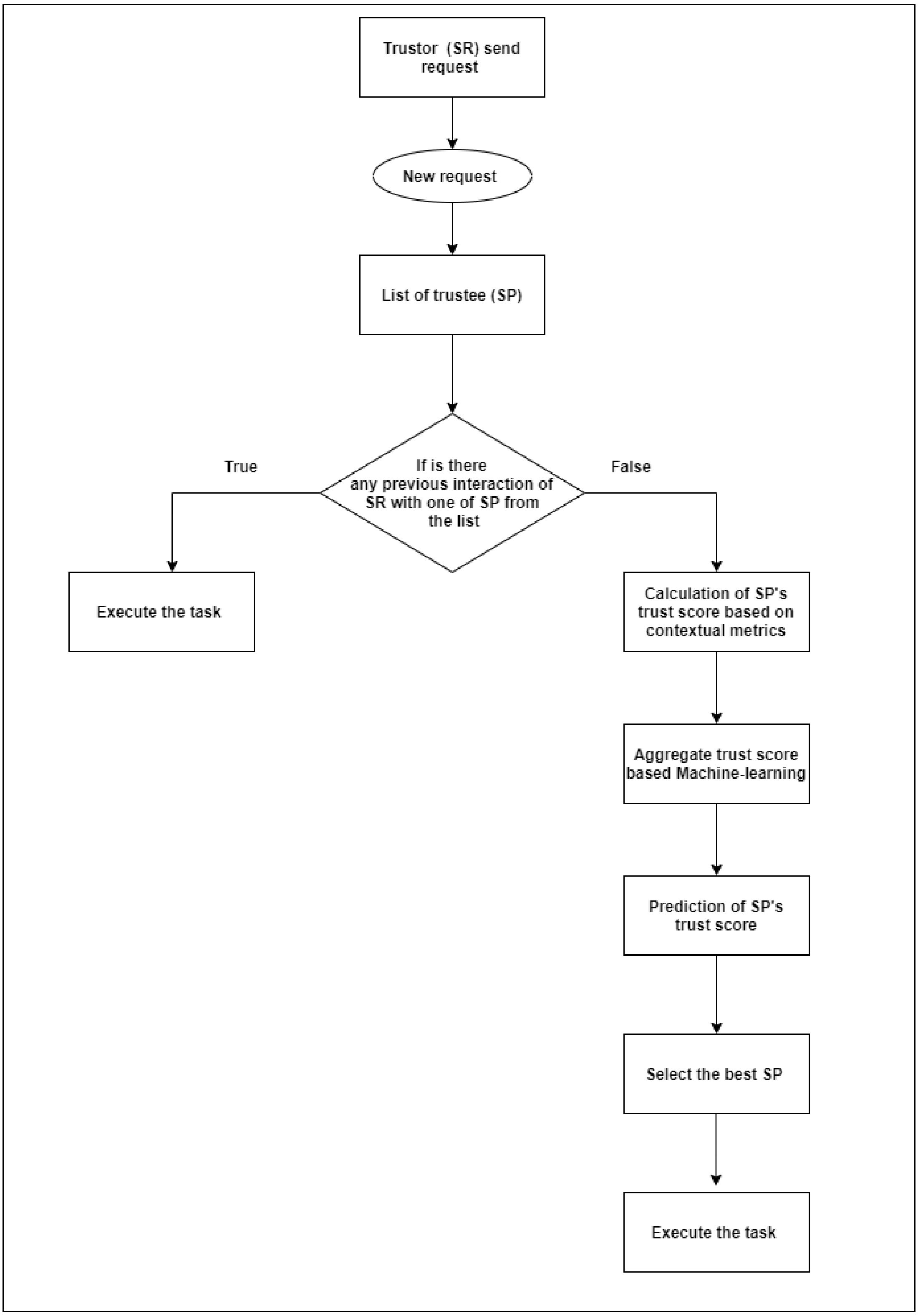

Trustor (SR) send request
New request
List of trustee (SP)
If is there any previous interaction of SR with one of SP from the list
True
False
Execute the task
Calculation of SP's trust score based on contextual metrics
Aggregate trust score based Machine-learning
Prediction of SP's trust score
Select the best SP
Execute the task

Figure 15 The trust evaluation process

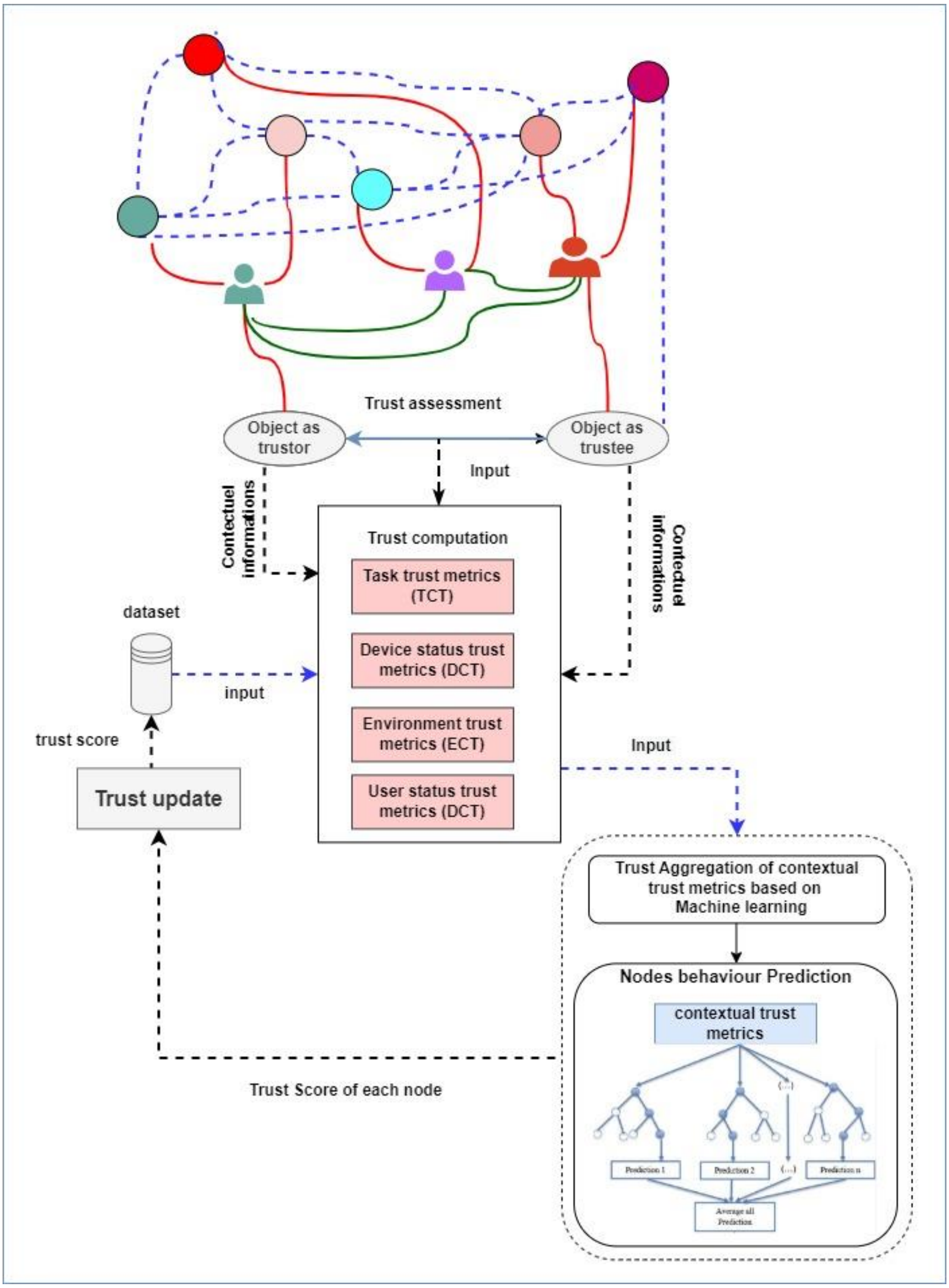


Figure 16 MCTM-SIoT model architecture

4.4.2. Basic elements in trust evaluation

The following elements are used to compute the trust:

- **The total number of transactions** occurring between two nodes. is defined by N_T This metric helps identify any abnormal or unusually high number of transactions between node D and other nodes p_i .

- **Successful number of transactions W_T:** is used to identify the successful transactions between node D and other nodes' p_i friends.

- **Unsuccessful number of transactions Z_T:** is used to identify the unsuccessful transactions between node D and other nodes' p_i friends.

- **Contextual information (DC), (UC), (TC), (EC):** defines the significance of contextual information: a high level of interaction within a specific context signifies its importance, resulting in a higher weight assigned to it in the trust evolution process.

- **The relationship factor (OR):** OR presents the relationship type between two objects. It is used to improve the information given by friends p_i.

Table 4 displays the relationship factor values for each relationship type. A higher value indicates stronger trust between two nodes sharing the same social relationship.

Table 4 The Relationship factor value (Nitti *et al.,* 2012)

Social relationships	Transaction factor
Ownership Object Relationship (OOR)	0.9
Co-Worker Object Relationship (CWOR)	0.8
Co-Location Object Relationship (CLOR)	0.8
Social Object Relationship (SOR)	0.6
Parental Object Relationship (POR)	0.5

4.4.3. MCTM-SIoT model process

The process of the MCTM-SIoT model consists of four main steps. Trust composition step, trust aggregation step, trust propagation step and trust update step. These are explained as follows:

4.4.3.1. Trust composition

The main focus of this section is the selection of trust metrics based on contextual information, i.e. Device status, user social profile, task type, and environmental condition to assess the trust of SIoT nodes and to determine the impact of each feature on the final trust decision.

1. **User context Trust Metrics (UCT)**: A user should possess both the capability to offer quality services and demonstrate good intentions when providing feedback. If a user delivers subpar services, it's not indicative of their abilities but rather suggests ill intentions. This could stem from two potential scenarios: either the user intends to launch an attack, or they are new to the system and thus lack adequate ratings. Social similarity is leveraged to evaluate the resemblance between two users, thereby quantifying each user's ability. Based on data gathered from a user's profile, interests list, social networks, and other sources, this metric calculates their overall usage. If there is a similar link between these two users, the trust between them increases by 1 as complete similarity and 0 as no similarity (Chen, Guo and Bao, 2016). Social similarity can reveal user similarities, but its primary purpose is to show that they are the same user hiding behind a different identity. For some attacks, such as the BMA or BSA attack, this metric is not interesting. However, it makes it possible to identify SPA attacks in which the user hides behind a fake profile to improve their own reputation. The Jaccard similarity coefficient serves as a statistical measure for assessing the similarity and dissimilarity between sample sets (Abderrahim, Elhedhili and Saidane, 2017). It describes the size of the intersection between two sample sets relative to the size of their union. MCTM-SIoT uses the friendship list and community list as example sets. User trust metrics are calculated as follows in equation (3).

$$T_{UT}^{t}(d_i, d_j) = T_F^t(d_i, d_j) + T_{CoI}^t(d_i, d_j) \tag{3}$$

Where: $T_F^t(d_i, d_j)$ is Friendship list similarity and $T_{CoI}^t(d_i, d_j)$ is Community list similarity.

a) **Friendship-list similarity:** this attribute refers to the significance of an object d_i with respect to the social relationships of the object d_j locally between its neighbours at any time t. Additionally, friendship similarity prevents the malevolent nodes from forming fake social connections to benefit from greater similarity. Objects that exhibit high similarity may be chosen for service discovery and provision or for collaborating on common tasks, as it is commonly assumed that friends are inclined to cooperate. It is computed in formulation (4):

Friendship-list $(\boldsymbol{d_i}, \boldsymbol{d_j})$:

$$T_F^t(d_i, d_j) = \frac{\left|F_{d_i} \cap F_{d_j}\right|}{\left|F_{d_i} \cup F_{d_j}\right|} \tag{4}$$

Where: F_{d_i} and F_{d_j} denote, respectively, a set of friends of objects trustor d_i and trustee d_j.

b) **Community of interest- list (CoI-list) similarity**: This feature facilitates the assessment of the community-based trust attribute of a trustee d_j relative to the trustor d_i at any time t, when both objects share similar interest groups such as social groups, etc. In an SIoT environment, objects interact with at least one interest group, and when two objects have a high level of interest community, they are more likely to make frequent contact with each other. The community of interests introduced in objects, unlike friendship similarity, does not change regularly. Therefore, each object must store a list of its owner's interest, which is calculated mathematically (5) as follows:

CoI-list $(\boldsymbol{d_i}, \boldsymbol{d_j})$:

$$T^{t}_{CoI}(d_i, d_j) = \frac{\left|CoI_{d_i} \cap CoI_{d_j}\right|}{\left|CoI_{d_i} \cup CoI_{d_j}\right|} \tag{5}$$

Where, CoI_{d_i} and CoI_{d_j} represent the corresponding interest groups of objects d_i and d_j. The more obvious the degree of similarity between objects, the stronger the degree of similar interests.

2. **Device context Trust Metrics (DCT)**: The device is defined as honest when it reflects its actual opinion about the task (Muhammad *et al.,* 2023) and is assessed based on object credibility and social object relationships.

a) **Object credibility**: The term "credibility" is often associated with "trust" in literature, although it lacks a universally agreed-upon definition and is assessed diversely in various works. In this study, a device is deemed trustworthy if its ratings authentically represent its opinions, without any attempt to submit false ratings to enhance or undermine the reputation of other devices. Credibility is deemed essential as it can identify various types of attacks. For instance, the Bad-Mouthing Attack (BMA) involves a malicious device submitting negative reviews for another device offering high-quality services to tarnish its reputation. The malware device in the BSA attack promotes another malicious device to boost its reputation. The hostile device in the SPA attack attempts to strengthen its own reputation by giving itself good reviews even when the quality of its services is low. Equation (6) is used to calculate the credibility of the object.

$$Cre^{T}(D, d_i) = \sum_{t=1}^{T-1} \sum\nolimits_{i=1}^{r} \frac{W_T(D, d_{i,})}{N_T(D, d_{i,})} \tag{6}$$

Where: N_T is total number of transactions among two nodes and W_T Successful number of transactions between node D and other nodes' d_i friend.

b) **Object relationships factor (OR)**: It focuses on the relationships between devices to identify colluding attacks. In fact, devices working together to launch an attack could have the potential for a close relationship. In addition, two devices can be connected to each other through different relationships. For example, if two nodes are linked by multiple relationships, the strongest relationship is prioritised, with the highest factor being assigned to it (Nitti, Girau and Atzori, 2014). The weights assigned to each type of relationship between social objects are provided in Table 4. The parent relationship is regarded as the weakest because it solely connects objects from the same manufacturer, whereas the ownership relationship between two devices owned by the same owner is considered the strongest. During the initial communication phase, each node is assigned an initial trust score toward its new neighbour based on the social relationship ties between the two nodes at the network's outset, as there may have been few or no transactions between individual nodes during the early stages of trust assessment. The DT metrics can be used to predict the trust of the devices using Equation (7).

$$T_{DT}^{t}(d_i, d_j) = Cre^{T}(D, d_i) - OR(d_i, d_j) \tag{7}$$

Where: N_T is the total number of transactions between two nodes and W_T successful number of transactions between node D and other nodes d_i and OR object relation weight factors.

3. **Task context Trust Metrics (TCT):** The task in the SIoT includes concrete properties or detailed requirements that are essential for the success of the task execution and the achievement of the SR goal. An object is considered trustworthy for a specific task if it provides good recommendations and qualified services. Therefore, a trust service provider is a node that provides good service and does not provide false information to mislead the trust

system. The information provided by the friends of the service request helped to evaluate the reliability of the service provider in this particular task. Considering that the concept of friendship influences one another's decisions to a significant way. The more interested someone is in another for a particular task, the more likely they are to trust each other to do that task. To evaluate the reliability of the recommendations and services provided by the provider node in the task type. Jaccard similarity is used to compare the similarity between the service provider's recommendation for itself and its friends' recommendation in terms of specific task, as shown in the following formulation (8).

$$T_{TT}^{t}\left(d_i, d_j\right) = \mathrm{Rec}\left(d_i, d_j\right) = \frac{\left|d_i \cap\ d_j\right|}{\left|d_i \cup\ d_j\right|} \tag{8}$$

Where: $\mathrm{Rec}\left(d_i, d_j\right)$ is the node's recommendation d_i regarding a specific task and the recommendation d_j of its friends regarding the same task.

4. **Environmental context Trust Metrics (ECT):** In this metric, it is important to consider environmental conditions when evaluating the node's trust score. Because every distributed system must have a trust-based environment, it is particularly significate that nodes work together securely on demanding tasks. Therefore, the focus is on evaluating an unfriendly environment that reduces the effectiveness of an SIoT system. For example, a node with many social connections and interactions in an unfriendly environment generally cannot be trusted and is also at risk of launching vulnerable attacks such as denial-of-service attacks (DoS), etc. The environmental context encompasses situations where certain users attempt to execute various trust-related attacks, posing a potential threat to the security of the trust system. Moreover, it can influence the trust score and thus should not be overlooked, as it provides supplementary information to other trust metrics when assessing the trustworthiness of SIoT nodes. The calculation of the environmental trust metrics is defined in Equation (9).

$$T_{ET}^{t}(d_i, d_j) = \sum_{t=1}^{T-1} \sum\nolimits_{i=1}^{r} \frac{Z_T(d_{i,}, D)}{N_T(d_{i,}, D)} \tag{9}$$

Where N_T is the total number of transactions between two nodes and Z_T unsuccessful number of transactions between node D and other nodes d_i.

4.4.3.2. Trust aggregation

The trust aggregation step involves choosing the best approach to aggregating the values of the trust into a trust value of each device that allows the user to decide whether to trust or not. This section summarises the different steps of the trust aggregation method to identify the influence of each contextual metric on the overall trust score of each node and predict the node behaviour using the static approach weighted sum and the machine learning-based approach.

4.4.3.2.1. Trust aggregation using the static approach Weighted sum

The most popular method according to the literature review mentioned above, is based on the static weighted sum approach, which refers to an average weighted mean of each metric, with a weight given for each metric to arrive at a single value (Chen, Bao and Guo, 2016). Therefore, the resulting trust metrics need to be aggregated using a weighted sum approach and then selected at which threshold a node is considered harmless to ensure the effectiveness of the TM model. The calculation of the estimated trust values is defined in Equation (10).

$$T_t(d_i, d_j) = \sum_{i=1}^{n} W_i \, T_X^t(d_i, d_j) \tag{10}$$

Where X denotes the contextual trust features (UT, DT, TT, and ET), w defines the weight of each trust feature, and n is the number of trust factors that were used in total.

However, the weighted sum technique has many drawbacks, including the inability to determine which trust metrics have the greatest impact on trust in a given context and the unlimited number of possible outcomes when determining a weighting factor for each feature. To address these issues, a ML-based approach is used to integrate all trust features, identify the influence of each contextual metric on the overall trust score of each node, and determine the most appropriate prediction for the nodes currently present in the SIoT network.

4.4.3.2.2. Trust aggregation using the ML based approach

ML refers to intelligent techniques that use sample data or previous experience to maximise performance criteria. More specifically, ML algorithms use mathematical approaches on large amounts of data to create behavioural models. For smart devices, ML also enables learning without explicit programming. Based on the recently added data, future projections are made using these models as a foundation (Hussain *et al.,* 2020). There are two categories of ML algorithms supervised, and unsupervised.

A. **Supervised ML Algorithms**: These supervised algorithms are a subset of ML algorithms that use labelled training data to learn how to predict or classify new or unseen data. The basic principle of supervised learning is to use a model trained on a set of inputs and their corresponding outputs or labels to predict the output for new inputs. In supervised learning, the algorithm is provided by a data set with inputs (also called features) and the corresponding outputs (also called labels or goals). The algorithm then creates a mapping between the inputs and outputs to predict new data (Hussain *et al.,* 2020). There are various supervised ML algorithms including linear regression, logistic regression, decision trees, random forests, support vector machines (SVM), and neural networks. In addition, supervised ML algorithms come in different types: regression, classification, and multiclass classification. Regression algorithms predict continuous values such as room temperatures. The algorithm learns an output value that maps the inputs to a continuous value. Classification algorithms predict a discrete class label for each input. These algorithms are trained with a function that maps an input to a class label. and the multi-class classification algorithms predict a class label from a set of more than two possible classes. The algorithm learns a function that transforms the inputs of different possible label classes (Saranya *et al.,* 2020).

B. **Unsupervised ML Algorithms**: These algorithms are a subset of ML algorithms that can make predictions or classifications without the need for labelled data. The basic idea of unsupervised learning is to find relationships in the data without first knowing the outputs or labels. The dataset used in unsupervised learning provides the algorithm's inputs (also called features). The algorithm then discovers a structure in the data that it can use to better understand the data, such as clusters. Popular unsupervised ML algorithms such as K-means clustering and hierarchical clustering, include principal component analysis (PCA) and association rule mining. There are different types of unsupervised ML algorithms: clustering and dimensionality reduction. Clustering algorithms group similar data points together in the dataset. Without first understanding what these groups must be, the algorithm learns to recognise the patterns in the data that characterise these groups. Dimensionality reduction algorithms minimise the number of features in a data set without losing crucial information. The most relevant relationships are captured in a lower-dimensional representation of the data that the algorithm learns (Saranya *et al.,* 2020).

This study uses an ML-based aggregation approach based on supervised ML algorithms called Random Forest. Random Forest is a flexible algorithm that can be used for both regression and classification tasks, where the output is a continuous numerical value in regression and a binary value (0, 1) in classification. The algorithm is well suited for this study because it can handle both types of outputs (Jaiswal and Samikannu, 2017). Furthermore, Random Forest reduces overfitting by using multiple random decision trees for a single dataset. The Random Forest regressor is used to evaluate the performance of the proposed MCTM-SIoT model in selecting the best service provider without prior behavioural history of nodes by assessing the final trust score of each node present in the SIoT network obtained from the contextual metrics (UCT, TCT, DCT, ECT). It also allows to identify the influence of each context metric on the final trust decision of each node presented in the SIoT network.

1. Performance evaluation of MCTM-SIoT for the best Service Provider Selection

Contextual trust metrics (UCT, ECT, TCT, and DCT) are aggregated to predict node behaviour based on each node's calculated trust score using the Random Forest Regressor. This process involves several critical steps (Liu *et al.,* 2014). First, pre-processing of the data includes dealing with missing values, encoding categorical variables, and splitting the data into sets for testing and training. Next, the number of trees and other relevant hyperparameters should be used as initialisation parameters for the random forest regressor model. Using the training data, the initialised model is trained to learn and make predictions using the contextual trust metrics as input features and the trust values as target values. By building multiple decision trees, the random forest regressor develops predictions from the training dataset and outputs the average of these predictions. The model can now predict results for new or unseen data, capturing the relationships between the input features (contextual trust metrics) and the target values (trust scores). To understand how each feature contributes to the overall prediction, the importance of the feature is then evaluated. After training and evaluation, the model can be applied to new and unobserved data to generate predictions.

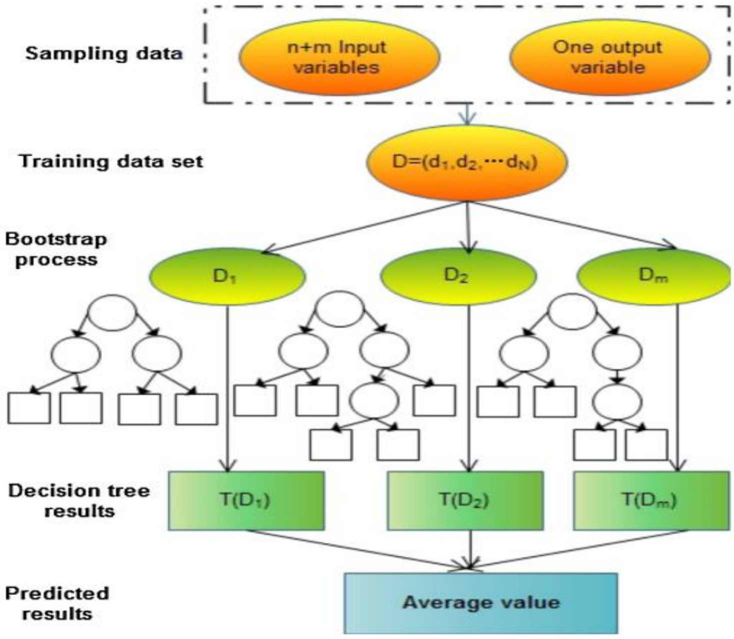


Figure 17 The flow chart of random forests (Liu et al., 2014)

2. Identifying the impact of each context metric on the final trust score for each node

MCTM-SIoT is trained using a random forest regressor, which is an effective tool for modelling the relationship between input features and the target variable. Understanding how each contextual metric contributes to the overall trust score of each node present in the SIoT network, becomes easier with the help of the feature importance analysis that this algorithm provides. This analysis evaluates each input feature (contextual trust metric) based on how well it predicts the target variable (trust score). The final trust score of each node can be determined by calculating feature importance and determining which context metrics have more influence. The data gathered is utilised to acquire a deeper understanding of the trust evaluation procedure by assessing the significance of various contextual metrics. This analysis helps to gain a knowledgeable perception of the factors that influence the trust scores of each node.

4.4.3.3. Trust propagation

Trust propagation is the process of how trust evidence is propagated on to peers in a network (Ureña *et al.,* 2019). In a limited environment such as SIoT, where there are many nodes, high dynamics, limited computing and storage capacity of devices, the propagation phase is considered crucial. To build an efficient trust system, it is recommended to use a propagation method that ensures the scalability and efficiency of the sources (Magdich, Jemal and Ayed, 2022). In general, there are two types of trust propagation schemes: centralised and distributed (Guo and Chen, 2015)

1) Distributed trust propagation: This scheme involves the autonomous dissemination of trust observations by IoT nodes to other IoT nodes without relying on a centralised entity. While it addresses the issue of a single point of failure, it introduces a fresh set of challenges, as each node must be transparent and provide impartial information during trust calculation (Guo and Chen, 2015).

2) Centralised trust propagation: In this scheme, there exists an entity tasked initially with gathering trust-related information and calculating trust scores, which are subsequently disseminated across the network. Consequently, this approach is vulnerable to a single point of failure, as the failure of this central entity could result in the collapse of the entire trust management system (Guo and Chen, 2015). In addition, this method allows scalability but is extremely resource-intensive, especially when the proposed framework is complicated. Therefore, the centralised approach is undesirable because most IoT devices have low computing and storage capabilities.

Researchers often use one of two strategies to propagate trust. While the distributed approach manages information differently than the centralised approach in SIoT environments to improve the scalability of the system in the face of an increasing number of large nodes, several works choose a distributed approach. The propagation trust used in this study is based on a distributed approach, where each node is responsible for storing and updating trust data, which may lead to security vulnerabilities.

4.4.3.4. Trust update

The trust update step allows the service provider's trust score to be updated based on one of three main schemes, either after a set period of time using the time update approach, or after each new transaction is entered into the system using the event update approach, or as a hybrid. TM models often focus on calculating a trust score. This could be applied to classify the nodes in the network and identify trustworthy nodes. Furthermore, a node that was previously trusted remains so for the following transaction, and this rating is only changed after some time or after another transaction. However, for a TM model to be effective, it must determine which malicious nodes should be removed based on their behaviours.

In the MCTM-SIoT model, the event-driven approach updated approach is selected. Where trust is updated after every transaction. The trust update is calculated by Equation (11):

$$T_{up}^{t}(d_i, d_j) = (1-\alpha)T^{t}(1-\Delta t) + \alpha L_s(d_i, d_j) \tag{11}$$

Where:

Δt represents the time difference elapsed between the last trust rating and the completion of the services. $L_s(d_i, d_j)$ describes how the trustor d_j's rated the trustee d_i's attributes based on how the expected trustworthiness and the actual action were compared.

T_{up}^{t} and T^{t} are the trust score of d_j, d_i respectively. After each transaction both of $T_{up}^{t}(d_i, d_j)$ and $T_{up}^{t}(d_j, d_i)$ are the updated trust score of d_j, d_i.

The predicted SP trust information (trustee) is recommended autonomously between nodes. Each node maintains its own trust information, which it passes on to or communicates with other nodes in its environment.

4.5. Summary

In this chapter, a novel model called "MCTM-SIoT" is proposed. MCTM-SIoT considered various contextual information related to the place in terms of environmental conditions, the task type provided by objects, and the timing (i.e., time) when assessing trust. A set of trust metrics, namely UCT, DCT, ECT, and TCT, for the trustworthiness of a device evaluation in the proposed model. Furthermore, an ML-driven aggregation approach is used to determine the influence of each contextual metric on the overall trust score of each node and predict node behaviour to address the aforementioned shortcomings of the weighted sum method. The main goal of MCTM-SIoT is to select the best SP without prior node behaviour history to improve the security and reliability of the SIoT network. Therefore, in order to evaluate the effectiveness and performance of MCTM-SIoT, a robust SIoT simulator is developed in the next chapter to generate an SIoT dataset.

Chapter 5

SIoT-SIM: Simulator for SIoT and SIoT Dataset

5.1. Introduction

Rapid advances in computing and communications have led to a range of technologies that support a network of connected and intelligent objects. Many terms, including machine-to-machine (M2M), IoT, and SIoT, can be used to characterise this ecosystem. Therefore, the integration of intelligent features, whether built into the devices themselves or made available through cloud-based processing and storage, has made the long-standing concept of machine intelligence a reality. Depending on the type of relationship, objects in SIoT can interact similarly to human relationships (Atzori *et al.,* 2012; Alam *et al.,* 2022; Khan *et al.*, 2021). The nature of this relationship determines the planned interactions arranged by the owners (Amin, Ahmad and Choi, 2019). When it comes to making new friends, objects in SIoT somewhat mimic human behaviour. An object creates and manages a variety of relationships after an owner sets the rules, and then uses these relationships to navigate the network and search for services (Nitti, Atzori and Cvijikj, 2015). Users benefit from SIoT through improved navigation, service discovery, reliability, and other features. However, due to the complexity of these systems, it is difficult to verify their effectiveness and performance in various real-world scenarios. To overcome this difficulty, the proposed framework is validated using an SIoT simulation tool called SIoT-Sim. The main goal of SIoT-Sim is to simulate and analyse the behaviour of users, sensors, and other SIoT systems in various SIoT contexts. This enables the creation of accurate SIoT data for testing and evaluation. SIoT-Sim also allows the adjustment of various simulation parameters to generate tailored synthetic data, increasing flexibility and adaptability. Numerous functions are included, such as modelling various attacks and vulnerabilities as well as simulating various devices. Researchers and developers can use this tool to optimise the design and extend the functionality of their SIoT systems to gain insights into their system's performance in different scenarios. This can accelerate the development of more reliable and efficient SIoT systems.

The remaining sections of the chapter are organised as follows: (Section 5.2) provides a summary of the current status of SIoT simulators and available datasets. (Section 5.3) introduces the requirements and capabilities to design a simulator tool for SIoT.

(Section 5.4) provides a detailed explanation of SIoT-Sim. (Section 5.5) discusses the generated SIoT dataset in more detail, and (section 5.6) concludes this chapter.

5.2. Existing SIoT Simulators and Datasets

5.2.1. Existing SIoT Simulators

As the SIoT paradigm receives increasing attention in research, it is crucial to identify appropriate simulation tools for designing a specific SIoT environment that takes into account the social structure of objects. Although OMNET++, NS-2 and Cooja are some of the available simulation tools for the Internet of Things, not all of them are suitable for dealing with the complexity of the social structure of objects in the SIoT environment (Ojie and Pereira, 2017; Chernyshev *et al.,* 2018). The simulation tools used specifically for SIoT are the main focus of this section. In particular, these tools are used to simulate and analyse trust management systems in SIoT through experiments. The literature commonly uses a number of simulation tools, which are summarised in Table 5 and discussed below:

Osterlind *et al.* (2006) developed a simulator called COOJA specifically designed for cross-level simulation using the Contiki sensor node operating system. This simulator allows simultaneous simulations at different levels, including the network level, the operating system level, and the machine code instruction set level. Cooja enables researchers to simulate and analyse the performance and behaviour of their WSN designs before real-world deployment.

Varga and Hornig (2008) presented OMNeT++, a simulator for low-level peer-to-peer networks with emphasis on stored networks and optical switches. In sensor network research, OMNET++ is a popular tool for discrete event simulation. It is an established and comprehensive tool that integrates external elements to meet specific environmental requirements. For example, to improve application capabilities, OMNET++ can integrate social profiles of objects and mobility for vehicular networks (Deshpande *et al.,* 2015). In general, OMNET++ can be used in a variety of domains and applications due to its flexibility. Several studies have recently evaluated the effectiveness of their proposed trust management systems in SIoT using the

OMNET++ simulator and Small World in Motion called SWIM. Originally intended as a mobility model for ad hoc networks, SWIM can generate artificial traces of mobility patterns to build a small world. In addition, SWIM is intended to take into account social behaviour that is comparable to human behaviour in everyday situations. Furthermore, statistical analysis shows that the synthetic tracks generated by SWIM are very similar to human tracks (Mei and Stefa, 2009).

Henderson *et al.* (2003) introduced the NS3 simulator framework. This framework is designed to consume network packets using VLANs or actual device drivers. The open-source discrete event simulator NS-3 is considered a replacement for NS-2. This adaptable tool can be used to create simulation scenarios that closely resemble actual hardware and protocols. NS-3 is a popular option for network simulation in a variety of areas and applications due to its versatility and flexibility (Campanile *et al.,* 2020). Numerous studies in the literature (Chen, Bao and Guo, 2016; Hamadi and Chen, 2017) have validated their proposed trust management models using the NS-3 simulator.

To simulate the SIoT environment, researchers have used a variety of other simulation tools in addition to those previously discussed. These include Microsoft Visual Studio and Python. Python has been used by researchers as a simulation environment, particularly for studies that involved prediction. It has been widely used by researchers to assess performance evaluations of various SIoT trust management systems. Kasnesis *et al.* (2016) presented ASSIST, a simulator focused on agent-based semantic rules and services specifically designed for SIoT applications. Abderrahim, Elhedhili and Saidane (2017a) introduced TMCoT-SIoT which stands for trust management system that leverages community of interest to moderate on-off attacks. Defiebre Defiebre, Germanakos and Sacharidis (2020) designed the DANOS simulator, which adds intelligent features similar to human friendships to improve object profiles and their interaction behaviour. Recently, Gazi *et al*. (2021) developed an SIoT simulator that would address the problem of traffic congestion in urban areas using a supervisory traffic control system.

Table 5 Existing simulators tool

Authors	Simulator	Scope	Mobility	Cyber-attacks simulation	Overall practical
Osterlind *et al.* (2006)	Cooja	Network	Yes	Incorporated custom Extensions	Significant
Varga and Hornig (2008)	OMNeT++	Network	Yes	Incorporated custom Extensions	Average significance
Henderson *et al.* (2003)	NS-3	Network	Yes	No	Significant
Kasnesis *et al.* (2016)	ASSIST	SIoT	No	No	Low significance
Abderrahim, Elhedhili and Saidane (2017a)	TMCoT-SIoT	SIoT	No	No	Low significance
Defiebre, Germanakos and Sacharidis (2020)	DANOS	SIoT	No	No	Low significance
Gazi *et al.* (2021)	Traffic simulator	SIoT	No	NA	Low significance

Current simulation tools like OMNET++, NS-3, and Cooja, though robust for network and sensor-level simulations, are primarily designed for low-level network operations and lack native support for simulating the intricate social structures and trust relationships between devices that are central to SIoT. While they can be extended through external modules or plugins to simulate some aspects of SIoT, such modifications are not only labour-intensive but also often fail to capture the dynamic and evolving nature of SIoT environments in a realistic manner.

On the other hand, specialised tools like ASSIST and DANOS are better aligned with SIoT-specific needs, focusing on aspects like agent-based modelling, trust management, and social interactions between objects. However, these tools still present limitations when it comes to scalability, handling large-scale real-world deployments, and integration with advanced techniques like machine learning, which is becoming increasingly crucial for predictive analytics, behaviour modelling, and decision-making in SIoT systems. Additionally, existing tools often fall short in simulating the stochastic nature of malware propagation, real-time device management, and dynamic network adjustments that reflect real-world SIoT scenarios.

Furthermore, certain key areas like user behaviour modelling, forming user-device communities of interest (CoIs), and advanced trust mechanisms remain underexplored in the current toolset. For example, DANOS supports friendship-like relationships between devices but lacks robust support for modelling malicious behaviours like on-off attacks or for managing large-scale device addition and removal in real-time, which are vital for the robustness of SIoT networks.

The creation of a new simulation tool would enable researchers and developers to simulate these SIoT-specific behaviours more accurately and efficiently, providing an integrated environment that includes not only the basic functionality of network simulation but also the essential features for modelling social interactions, dynamic trust, user behaviours, and scalable real-world deployment scenarios. By filling these gaps, the new tool would serve as a crucial platform for advancing SIoT research, particularly in areas like predictive modelling, security, TM, and large-scale deployment, where current solutions are either insufficient or overly complex to customise.

Table 6 shows a comparison of the capabilities of existing tools, highlighting their strengths and weaknesses:

Table 6 Comparison of capabilities in existing simulation tools for SIoT

Capabilities	**Osterlind *et al.* (2006)** **Cooja**	**Varga and Hornig (2008)** **OMNET++**	**Henderson *et al.* (2003) NS3**	**Kasnesis *et al.* (2016) ASSIST**	**Abderrahim, Elhedhili and Saidane (2017a) TMCOIT-SIoT**	**Defiebre, Germanakos and Sacharidis (2020) *DAMOS***	**Gazi *et al.* (2021)** **Traffic**
User behaviour modelling	✗	✗	✗	✗	✗	✗	✗
Managing network dynamics	✗	✗	✗	✗	✗	✗	✗
Friendship between users	✗	✗	✗	✗	✗	✗	✗
Forming social relationship between devices	✗	✗	✗	✗	✗	✓	✗
Real world Scenarios	✗	✗	✗	✗	✗	✗	✗
Stochastic malware propagation	✗	✗	✗	✗	✗	✗	✗

5.2.2. Existing SIoT datasets

This section provides information about the datasets currently available for evaluating trustworthiness management systems in the SIoT. Datasets are essential when evaluating and validating systems in an environment that closely resembles real-world scenarios. There are many IoT and social network datasets available, but they cannot be directly applied to SIoT architecture. In the following discussion, we will examine some of the datasets used in the literature to evaluate the trust management model in SIoT.

The dataset introduced by (Marche *et al.,* 2020) is especially proposed for building the SIoT network. It includes 16,216 IoT devices deployed in the city of Santander, Spain, belonging to both private users and public service providers. The dataset provides various details including device ID, owner ID, device type (public or private), brand (represented as a number between 1 and 12), and model (represented as a number between 1 and 24). Furthermore, the dataset comprises information about the applications and services offered by each device, as well as an adjacency matrix indicating the object relationship categorised as OOR, POR, CLOR, CWOR, or SOR. While this dataset can be used to build the SIoT network, it cannot be used to validate the trust model as it lacks information about device interactions and ratings. In addition, researchers have used the SIoT dataset reported in (Marche *et al.,* 2020) in combination with well-known datasets such as Yelp2 and Epinions ((Richardson, Agrawal and Domingos, 2003) to take the social structure into account and check how well their trust models work. Epinions is a consumer review online social network and has more than 75,000 nodes and over 500,000 edges showing the connections between users and their reviews. Yelp, another social media platform with 1.6 million users, 6 million reviews, and 192,000 businesses, is another place where people can rate and review businesses. Researchers often use the SIGCOMM-2009 dataset to evaluate trust models in the SIoT domain because it can be tailored to emulate the SIoT environment (Sagar *et al.,* 2020). This dataset includes information about 76 objects, their social profiles (friends, community affiliations, and other details), and interactions (15,776 total interactions). The dataset also shows how the objects' social profiles have changed over time.

Researchers have been forced to create their own datasets using the SIoT structure described in (Atzori *et al.,* 2012) because there are few real-world datasets suitable for evaluating trust models in the SIoT paradigm. This highlights the requirement for more real-world datasets that are specifically designed for SIoT trust management system evaluation.

5.2.3. The need for a new dataset for SIoT

Evaluating trust management systems in the SIoT requires datasets that accurately reflect the unique social and technical dynamics of the SIoT environment. While several datasets have been used in research to simulate SIoT scenarios, they often lack the necessary attributes to fully capture the complexity of trust relationships and device interactions in real-world SIoT applications. This section outlines the limitations of existing datasets and justifies the need for a new dataset tailored specifically to the demands of SIoT TM.

5.2.3.1.Limitations of existing datasets

Many existing datasets, such as those used in IoT and social network research, cannot be directly applied to the SIoT architecture due to their lack of focus on device-to-device interactions and trust evolution. For example, the Santander dataset includes real-world IoT device data but lacks information on trust ratings and device interactions, which are essential for evaluating trust models. Similarly, social network datasets like Yelp and Epinions provide a wealth of data on user relationships and reviews but are centered on human-to-human interaction rather than device-to-device communication.

Another frequently used dataset is SIGCOMM-2009, which offers interaction data and some social relationship structures, but its small scale (76 objects) and the lack of trust ratings limit its utility for evaluating large-scale, dynamic trust management systems in SIoT. Furthermore, these datasets generally lack features to simulate malicious behaviour, which are crucial for assessing the resilience of trust systems in adversarial environments. While custom-generated datasets based on the SIoT structure have been proposed by researchers, these datasets often focus on specific use cases and lack generalisability or real-world scalability.

A new dataset is necessary to overcome these limitations and provide a more robust framework for evaluating SIoT trust management systems. This dataset should incorporate the following key features:

- Scale: The dataset must represent a large number of devices (potentially tens of thousands) to accurately simulate the scalability of TM systems.
- Interaction Data: It should include detailed records of device-to-device, Human to human and human to device interactions to allow for the modelling of dynamic trust relationships.
- Trust Ratings: The dataset must provide trust ratings derived from interactions between devices, allowing researchers to simulate the evolution of trust over time.
- Malicious Behaviour Simulation: The inclusion of simulated malicious activities is crucial for evaluating the security and resilience of trust models.
- ML Integration: The dataset should be structured to support the use of ML techniques for predictive analytics and dynamic TM.

5.2.3.2. Comparative analysis of existing datasets

The proposed new dataset would resolve the limitations of existing solutions by providing large-scale, device interaction data combined with simulated malicious behaviours. This will allow for comprehensive testing of SIoT TM models, including predictive trust analytics, and scalability under real-world conditions. Moreover, by integrating support for ML, the dataset would enable advanced research into dynamic trust prediction.

The creation of such a dataset would fill a critical gap in current research and provide a robust platform for testing and validating TM systems in the complex, evolving environments of the SIoT.

To clearly demonstrate the need for a new dataset, Table 7 shows a comparison between existing datasets, and the proposed solution is presented below:

Table 7 A comparison between existing datasets

Dataset	Scale (Number of Devices)	Interaction Data	Trust Ratings	Malicious Behaviour Simulation	Social Structure (OOR, POR, etc.)	ML Support	Limitations
Santander Dataset	16216	✗	✗	✗	✓	✗	Lacks interaction and trust data, no malicious behaviour simulation, no dynamic trust tracking.
Yelp	1.6 million users	✓	✓	✗	✗	✗	Human interaction data, not device-oriented, no dynamic trust or malicious behaviour.
Epinions	75,000 nodes	✓	✓	✗	✗	✗	Human interaction data, lacks context for device-to-device relationships.
SIGCOMM-2009	76 objects	✓	✗	✗	✗	✓	Small-scale, limited to object interactions, lacks real-world scale and malicious behaviour simulation.
Generated SIoT Datasets	Varies	✓	✓	✗	✓	✗	Custom-generated datasets often lack scalability, real-world deployment scenarios, and integration with ML techniques.

5.3. Key requirements and capabilities to design simulator tool for SIoT

Designing a simulator for SIoT requires a multidisciplinary approach that combines knowledge of IoT technology, social contexts, user social profile and visualisation. Below are some important specifications for designing such a tool:

- **Understanding of SIoT technology**: Creating a simulator tool that effectively visualises the behaviour and profiling of objects in an environment requires a detailed understanding of the SIoT paradigm. This includes being familiar with the communication protocols of SIoT technology.
- **Understanding of social contexts**: It is critical to develop a simulator tool that takes into account the specific social contexts in which the devices will be used. It could also have significant implications for the development and application of IoT devices.
- **Knowledge of user behaviour:** It is important to understand user behavior, preferences, and requirements. This knowledge will be useful in developing a tool that simulates interactions between users and IoT devices.
- **Ability to simulate multiple scenarios**: To evaluate the performance of the simulator in different scenarios, it is important to simulate a variety of scenarios. This includes creating different network conditions to understand how the devices perform in various environments. It is also important to simulate different user interactions. Developers can verify the effectiveness and reliability of the simulator by testing SIoT devices against a series of simulated scenarios.
- **Data analysis and visualisation capabilities**: This is a crucial aspect of simulation tools as it supports users' understanding and interpretation of simulation results. Therefore, the simulator tool should be able to gather and evaluate the data generated during the simulation process and present the results in a meaningful way. This includes the ability to visualise data using charts and graphs.
- **Customisation options**: The ability to customise simulations to individual requirements is a crucial feature of a simulator tool. Therefore, it should be customisable to adapt the simulator tool to different simulation parameters like device settings and network configurations.
- Scalability: The ability of the simulator tool to perform large-scale simulations is one of the most important features of simulation tools for evaluating the performance of SIoT devices in real-world scenarios.

The following capabilities should be included in an SIoT network simulation:

- **Device emulation**: To develop a virtual device that mimics the actions of a real device that can communicate with one another, such as environmental sensors and smart home devices.
- **Network topology modelling**: It describes the process of assembling a visual representation of the arrangement of nodes, devices, and connections within a network. It is used to evaluate the functionality, performance, and connectivity of a network and can be either physical or logical. Network topology modelling is essential for designing and maintaining a network. It makes it easier to predict network functionality.
- **User behaviour modelling**: the ability to mimic users' behaviour and interactions with IoT services and devices in social context. Modelling various usage scenarios, such as adding or removing users, changing settings, and sharing data.
- **Data analytics**: the ability to gather, store, and analyse data produced by users and IoT devices. This might involve user preferences, data security, and network performance in real time.
- **Security and privacy**: To maintain the volume of data generated and used by these networks, SIoT must implement additional security measures. In addition, evaluating and assessing various security protocols to stop threats like unauthorised access and data breaches.
- **Integration with ML**: ML plays a crucial role in uncovering the hidden patterns in SIoT data by analysing vast amounts of data using advanced algorithms. SIoT devices can extract valuable insights or knowledge from the data generated by IoT with the aid of ML.

Based on these capabilities, simulating an SIoT environment tests network performance and behaviour under different conditions with different network scenarios.

- **Adding or removing devices from the SIoT**: Adding or removing devices could be a useful simulated scenario to test the scalability and capacity of the SIoT network to handle varying numbers of devices. For example, the performance of an SIoT network may be affected as it expands in a smart city as more data is transferred and processed. Evaluating network performance under these conditions can improve the architecture of the network and identify potential bottlenecks.

- **Changing network parameters**: It is an essential additional simulation scenario. For example, the performance and behaviour of the network may change when certain network parameters are changed. By determining the correct network parameters for the SIoT context through simulation, the effectiveness and stability of the network could then be improved.
- **Real-world scenarios**: The network is modelled to mimic real-world scenarios, such as smart city applications or traffic tracking systems. This can help identify potential areas for development and evaluate how well the SIoT network manages real-world use cases

5.4. SIoT-Sim tool

SIoT is a collection of different IoT devices that work together to create a social, intelligent environment and support users in their tasks. These devices interact with one another based on predefined relationships, mimicking the structures of social networks, such as building user friendships and user registration in communities of interest (CoIs, social groups), as well as the formation of social object relationships, including POR, OOR, CWOR, SOR, and CLOR, disconnecting and leaving devices from the network and a stochastic propagation of malware on the network. To the best of our knowledge, there is no real dataset presented in such an environment. The SIoT simulator called "SIoT-Sim" is designed to illustrate the capabilities of such a system in facilitating autonomous relationships between SIoT objects. These SIoT objects can exchange recommendations with each other and with their owners. Additionally, SIoT-Sim models user and device behaviour in various SIoT scenarios, enabling the creation of an accurate SIoT dataset for SIoT systems assessments and testing. To achieve this purpose, a series of actions that can be performed in SIoT-Sim are built, such as:

1. **Friendships between users**: SIoT users can make friendships with each other and share information, collaborate, and control connected devices together. In addition, users can grant access to their devices and enjoy shared benefits within the SIoT network through friendships.

2. **Communities of Interest (CoI)**: To mimic the SIoT environment, two communities of interest are implemented, including users joining CoI and devices forming social object relationships:

   - Users joining CoI: Joining a community is an option available to users. By participating in these communities, users can exchange ideas, information, and experiences on specific topics or passions (sports, music, etc.). This user's CoI is based purely on real-world user-user interactions. While user-device interaction can improve the overall SIoT experience for users and their devices, participation in these communities allows users to find new devices that match their interests and preferences.
   - Forming social object relationships: The device can form relationships with other devices based on predefined object relationships, or devices can find new friends based on the user's CoI because devices can access the user's CoI. POR is a pure device-device relationship where two devices from the same batch can exchange information and trust each other because they come from the same factory. OOR, SOR, and C-WOR can be viewed as hybrid CoI that includes both device-device interactions and user-device interactions.

3. **Devices disconnect and leave the network**: Sometimes devices lose connection for various reasons, such as low battery life or technical difficulties. When devices lose their connection, data loss and reduced functionality can occur.

4. **Probabilistically communicating**: It occurs between users and devices. Depending on the situation and requirements, they can choose to broadcast messages to all their connections, multicast within CoI, or interact individually.

5. **Stochastic malware propagation over the network**: This refers to the random and unpredictable spread of malware over the network, which poses a significant security challenge for interconnected devices.

5.4.1. SIoT-Sim architecture

Figure 18 provides an overview of the proposed SIoT-Sim architecture and highlights the essential modules and their respective processes. The architecture consists of four layers including the IoT environment layer, the interaction layer, the social interaction layer, and the simulation layer.

1. **IoT Environment layer**: Every SIoT object connected to the SIoT network is included in this layer. These SIoT objects can be users or devices. This layer consists of three components: network topology modelling, device emulation, and user modelling. In SIoT network, it is the responsibility of user modelling to accurately represent user's behaviour. It has attributes such as user's preferences, location data and user's profiles. The network topology modelling component simulates the communication between the physical devices and the SIoT network, while the device emulation component mimics the physical devices and sensors connected to the SIoT network.

2. **Interaction layer**: This layer facilitates connections and communication and includes different types of interactions. These include human-to-human interactions, where people interact with each other, object-to-object interactions, which allow devices to communicate and collaborate, and human-to-object interactions, where objects and people communicate with one another. This layer plays an important role in shaping the dynamics of the IoT environment, which also improves the overall user experience.

3. **Social interaction layer**: This layer serves as an interface to form social networks and facilitates social communication between IoT objects. The IoT devices create a network of friendships, build a social structure, and create CoI, which are virtual groups within the network that have similar interests.

4. **Simulation layer**: The two main components of this layer are data collection and event-based simulation. By considering user's interactions, device behaviour, and network conditions, event-based simulation creates events that manage the simulation. On the other hand, data collection is the process of obtaining information for reporting and analysis while the simulation is running.

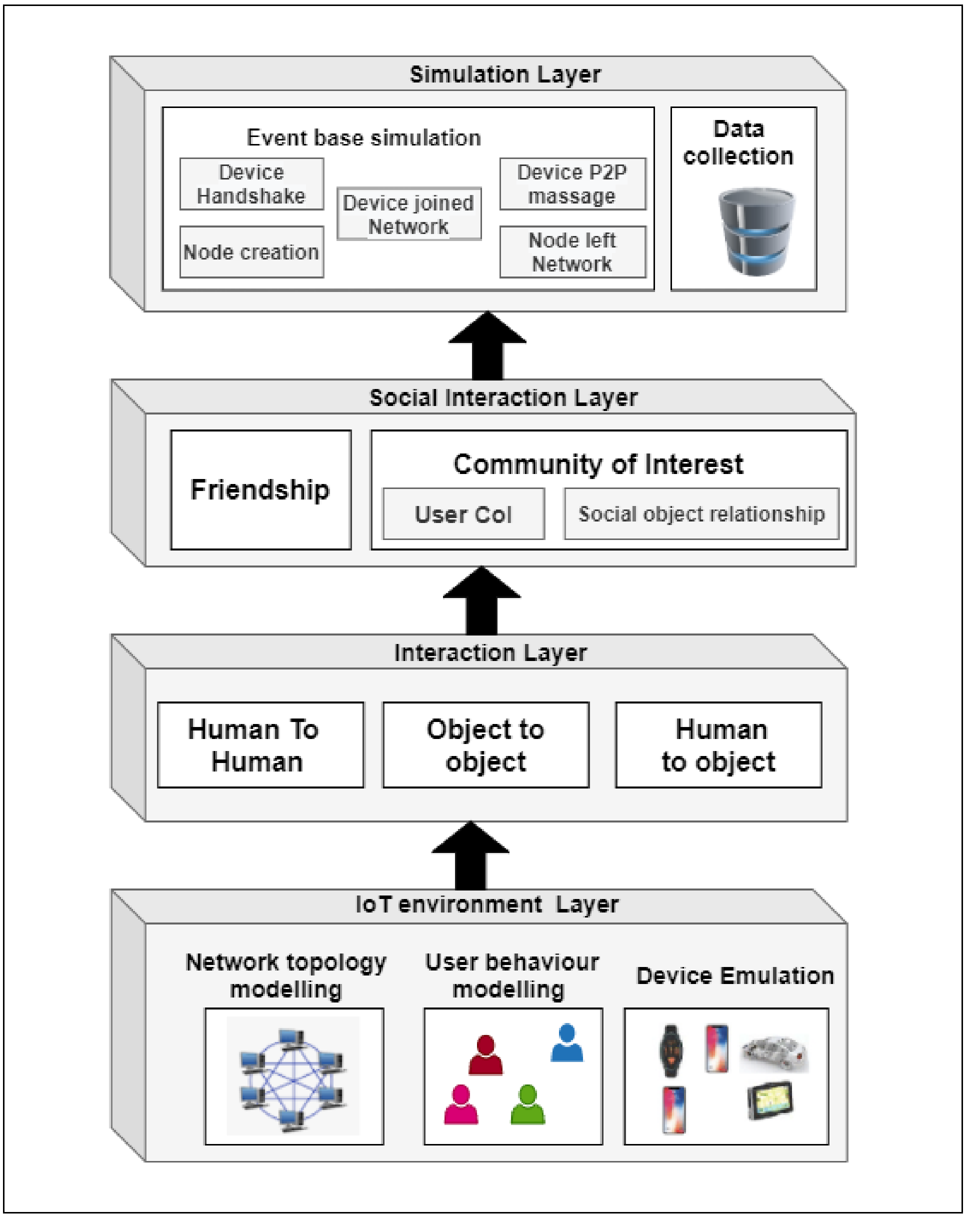


Figure 18 SIoT-Sim architecture

5.4.2. SIoT-Sim design

The simulated network is represented as a NetworkX Multi-Directed Graph (Multi-DiGraph) to capture bilateral relationships between entities (Figure 19). SIoT-Sim consists of two important high-level modules including nodes and events.

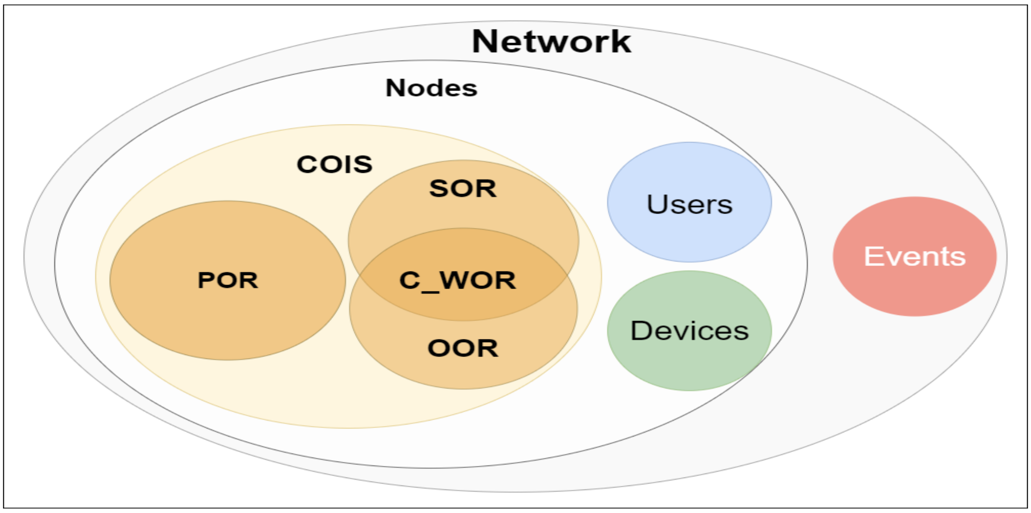


Figure 19 Main components of SIoT-Sim

1) **Node module**: The nodes are modelled as an abstract class that represents each entity (namely users, devices, and CoI) within the simulation graph. It does not directly represent a specific node in the graph but rather provides a common set of attributes and behaviours for all entities in the diagram. Each node in the simulation graph has the following attributes:

- Trust value: This property indicates the degree of trust that other nodes in the graph have in this specific node. It is likely used to determine the interactions and relationships with other nodes.
- Connection status: This property indicates how connected the node is to the network. If a user has at least one device connected to the network, this attribute is automatically set to true for the user node. This determines which nodes can communicate with each other.

- Node ID: This property gives the node a special identification. It can be automatically generated sequentially or assigned manually at instantiation. the ID attribute is an important factor in identifying nodes in the simulation graph.

The node module consists of three submodules including Users and Devices and CoI:

A. **The users' submodule**: This submodule is used to represent users in the social network. When a user is created, a device list is also created. The global parameters set in the settings can determine whether these devices are pre-activated or not and whether they are movable or not. Typically, devices are not pre-activated to simulate users' connection with their devices at random intervals over time, rather than having all devices already present on the network from the start (at t=0). Since most social network users join the network gradually rather than all at once, this method attempts to recreate a more realistic real-world scenario.

B. **Device submodule**: This submodule is used to represent devices within the social network. These devices serve as representations of the different types of devices used to connect to the social network. There are two types of devices as shown in Figure 20 movable devices such as smartphones and laptops and non-movable devices such as smart lights, security cameras, servers and desktop computers. To simplify the simulation, all movable devices belong to any users, while non-movable devices belong to any CoI type. These devices have specific attributes and behaviours tailored to their device characteristics. In addition, they can track whether they are working autonomously or being used by their owner, track their friendship connections to enable direct exchange without CoI, or emulate an expiring battery life that leads to a connection interruption.

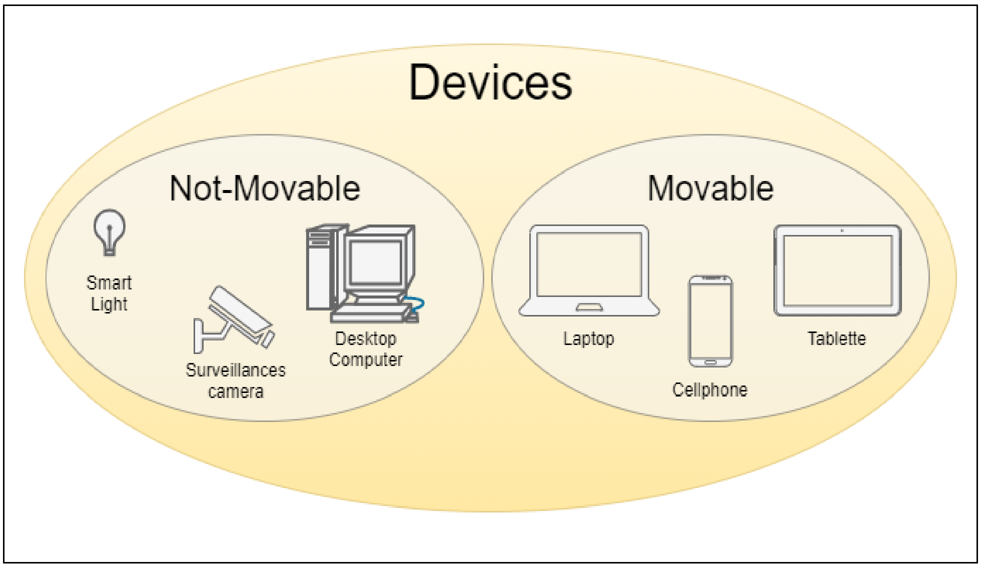


Figure 20 Device type in SIoT-Sim

C. **CoI submodule**: This submodule enables the representation of different types of CoI to give devices and users access to different groups that share the same interests. Each CoI has a different implemented function called “can_access” that evaluates whether a user or device can join the CoI and has a different pattern of open/close time frame to emulate the different CoI. To join a CoI, some space must be available, modelled by a capacity and a list of currently connected devices. In addition, In SIoT-Sim, there are shady accesses to allow users to access a CoI that they do not belong to such as customers can access the C-WOR group. The probability of shady access can be adjusted in the setting to mimic strong or weak CoI management. devices can find new friends based on the user CoI because devices can access the user CoI or devices can establish relationships with other devices based on predefined object relationships (OOR/ POR/ WOR/ SOR):

- OOR: The OOR represents the social group of an owner's device. Devices in an OOR can freely exchange interactions and choose to join the OOR frequently (by default, the OOR is always accessible, and devices can join at any time).
- POR: Like the OOR, the POR is a social group that is considered always open but does not allow user access, only autonomous devices from the same batch can access it outside of shady access.

- SOR: SOR tries to mimic physical locations such as coffee shops, user meetings in a park, etc. It can be a one-time or recurring event that any user/device can participate.
- C-WOR: C-WOR limits connections to a list of authorised users/devices. An authorised user can add any of their devices to the authorised devices list to mimic work-related circles. Shady Access also allowed new users to access this CoI.

2) **Event module**: To keep track of the actions that took place during the simulation, an event class is used to store the various actions of users (offline/online), devices, CoI opening and closing, and friendship creation and suppression as a short log. The basic structure of an event is abstracted from a Pandas row, where each row contains: (i) the time step of emission, (ii) the time step of reception, (iii) the ID corresponding to the event type, (iv) source device ID, (vi) owner ID of the source device, (vii) the circle of relationships involved in the exchange, if any, otherwise None or Friendship is displayed depending on the action, (viii) destination device ID, (ix) the owner ID of the destination device and finally (x) the payload content of the event. In SIoT-Sim, there are five high-level event types that capture all transaction types shown in Table 8. Some repeated events within a single time step indicate certain forms of functionality. For example, multicast and broadcast messages are modelled as concurrent P2P messages, where a multicast results in a series of broadcasts from the same sender to all CoI members or all friends in the list. Figure 21 and Figure 22 depict a user communication process within a specific online platform, likely designed for communities with shared interests. The process commences with a user entering which can be understood as a group focused on a particular topic or activity. Once within the CoI, the user possesses several communication options. They can exit the CoI entirely or choose to join a different one aligned with their evolving interests. In terms of message dissemination, the user can broadcast a message, effectively announcing the entire CoI. Alternatively, they can multicast a message, targeting a specific subgroup within the community. Finally, the user can engage in private messaging with individual friends within the platform. It essentially illustrates a user decision-making process for communication

purposes. Based on their intent, users can choose the most appropriate communication channel, ranging from broadcasting to the entire community to private conversations with specific individuals.

Table 8 SIoT event types

Event Type	Description
DEVICE JOINED_NETWORK	Indicates when a device has joined the network
DEVICE_ HANDSHAKE	Triggered when 2 devices connect
DEVICE _P2P _MESSAGE	Triggered when transmission occurs between 2 devices
Node_Creation	Indicates when user, device or CoI has been created
Node_left_Network	Indicates when a device, user or CoI has been removed from the network

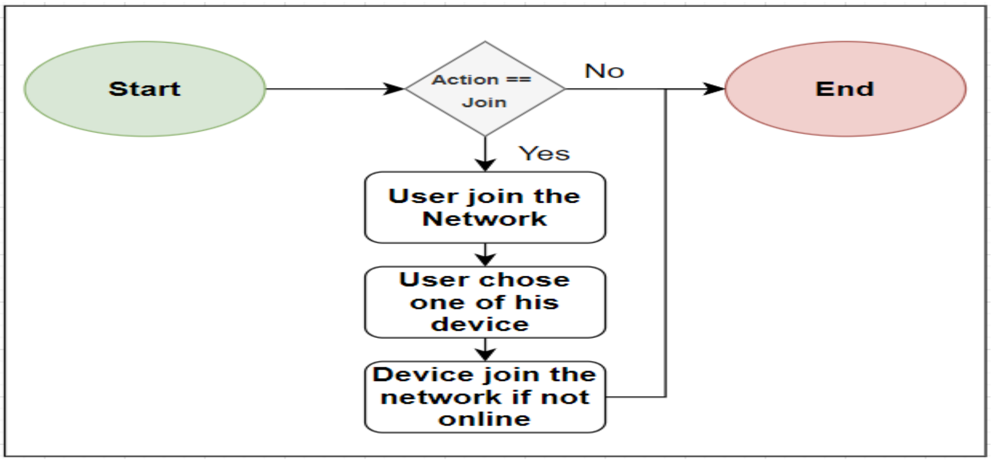

Start
Action == Join
No
End
Yes
User join the Network
User chose one of his device
Device join the network if not online

Figure 21 Offline event process

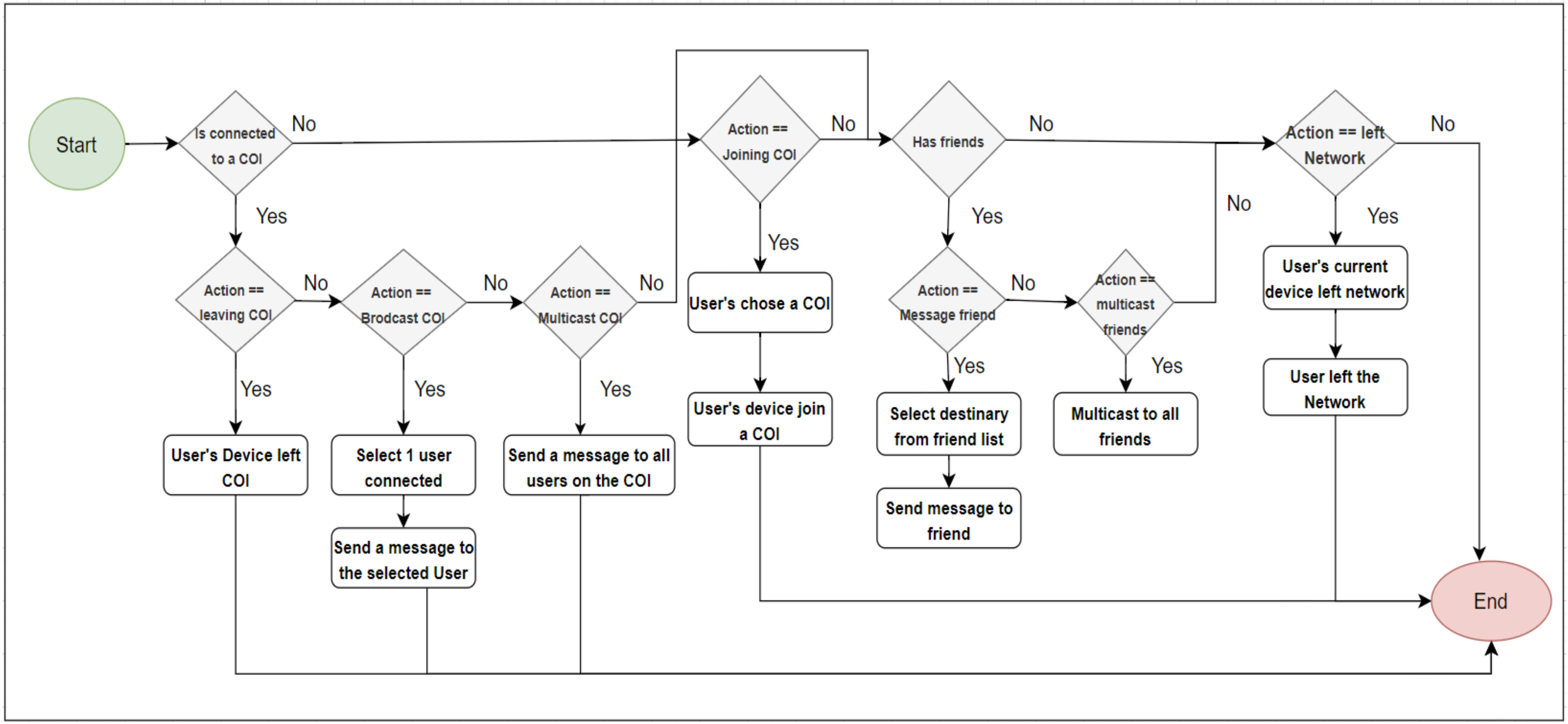


Figure 22 Online event process

In SIoT-Sim, all events are triggered probabilistically, based on a custom probability defined in the settings, along with the use of a Numpy random selection that follows the normal distribution and allows the observation of different action sets that are not predefined. The action selection also takes into account the state of the device. For example, a device can only join a CoI if it has not already joined. Otherwise, the available action includes sending, multicast over the CoI, and terminating the CoI. To prevent the device from switching from one CoI to another, each device also has time to ensure that it spends a minimum amount of time connected to the CoI and enables message exchange. Similarly, a probabilistic selection of a recipient from a list of users is defined using the following Equations (12), (13):

$$f(x)\begin{cases} 0, & if\ \alpha = -1 \\ \dfrac{1}{1+\Delta}, & if\ \alpha = 0 \\ 1, & if\ \alpha = 1 \end{cases} \tag{12}$$

$$f(y) = \frac{f(x)}{\sum_{i=0}^{N} f(i)} \tag{13}$$

Where Δ is the number of interactions between the sender (service provider) and the receiver (service requester), $f(x)$ the probability of choosing x as a receiver for the broadcast, α the state of the friendship:

$$\begin{aligned} &\alpha = -1, \quad Receiver\ and\ Sender\ broke\ their\ friendship \\ &\alpha = 0, \quad Receiver\ and\ Sender\ are\ not\ friends \\ &\alpha = 1, \quad Receiver\ and\ Sender\ are\ friends \end{aligned}$$

The probabilities are then normalised based on the number of potential receiver and the sum of their probabilities using $f(y)$. This way, the spread of messages is encouraged to be broadcast between friends to give a chance for two users to make a connection and avoiding two users/devices to keep interactions if they decided for any reason to break their friendship.

By incorporating realistic timing and probability distributions for different event types, the simulation aims to replicate real-world behaviours. Regarding device initialisation, a deliberate effort is made to interleave malicious and trusted devices instead of concatenating them sequentially. This design choice ensures that the initial network topology reflects a real-world scenario in which malicious and trusted devices are randomly distributed across the network rather than grouped. The simulation environment closely resembles real-world dynamics and improves the accuracy of the simulation results in a simplified representation.

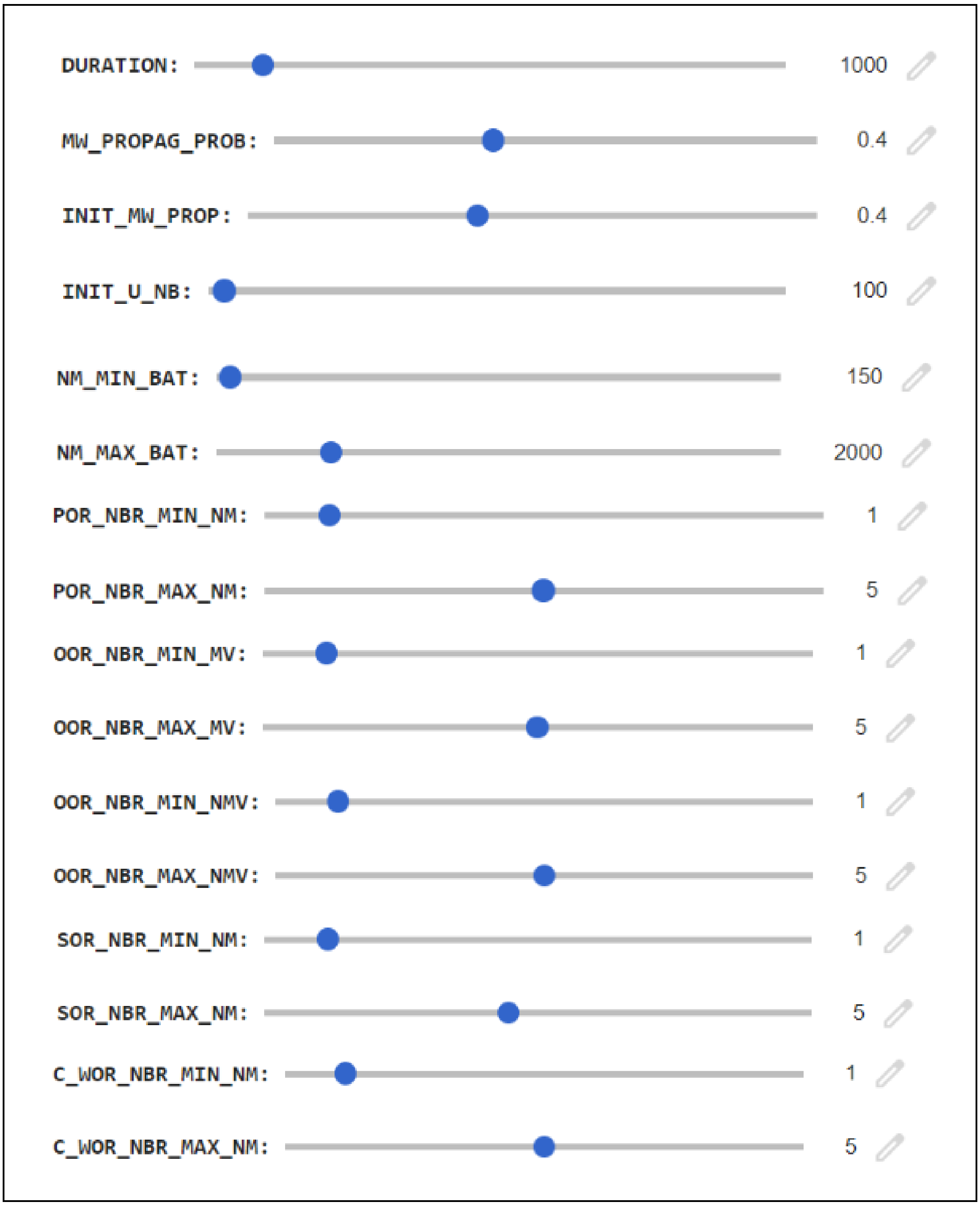
5.4.3. SIoT-Sim Parameters

SIoT-Sim is a valuable tool for simulating device actions and behaviours in diverse SIoT environments. To guarantee an accurate emulation of these nodes, SIoT-Sim typically uses predefined parameters including Simulation parameters (see Table 9). These parameters are crucial in defining the specific characteristics and qualities of the simulated system. Through precise parameter configuration and adjustment as shown in Figure 23, SIoT-Sim can simulate various SIoT scenarios and allows researchers and programmers to evaluate and improve their system's functionality, behaviour, and communication within the SIoT network.

Table 9 SIoT-Sim parameters

Simulation parameters	Definitions
DURATION	The simulation time is determined by the clock, users/devices perform one action per clock.
MW_PROPAG_PROB	The chance of a corrupted device to propagate corruption in messaging.
INIT_MW_PROP	Probability of device compromise when starting the simulation.
INIT_U_NB	The number of existing users at the start of the simulation, who can be online or offline.
NM_MIN_BAT	The minimum battery life with which a no-moving device can start when it joins the network.
NM_MAX_BAT	The maximum battery life with which a no-moving device can start when it joins the network.
POR/OOR/SOR/C_WOR NBR_MIN_NMV	The minimum number of no-moving devices in POR/OOR/SOR/C_WOR

POR/OOR/SOR/C_WOR_NBR_MAX_NMV	The maximum number of no-moving devices in POR/OOR/SOR/C_WOR
OOR NBR_MIN_MV	The minimum number of moving devices in OOR
OOR _NBR_MAX_MV	The maximum number of moving devices in OOR



DURATION: 1000

MW_PROPAG_PROB: 0.4

INIT_MW_PROP: 0.4

INIT_U_NB: 100

NM_MIN_BAT: 150

NM_MAX_BAT: 2000

POR_NBR_MIN_NM: 1

POR_NBR_MAX_NM: 5

OOR_NBR_MIN_MV: 1

OOR_NBR_MAX_MV: 5

OOR_NBR_MIN_NMV: 1

OOR_NBR_MAX_NMV: 5

SOR_NBR_MIN_NM: 1

SOR_NBR_MAX_NM: 5

C_WOR_NBR_MIN_NM: 1

C_WOR_NBR_MAX_NM: 5

Figure 23 SIoT-Sim control panel

5.4.4. SIoT-Sim Scenarios

SIoT-Sim was specifically designed to replicate complex SIoT environments. Is has the ability to model a wide range of different scenarios, including single device, disconnected device, and multi-user scenarios. These scenarios, which act as comprehensive templates, enable accurate modelling of various SIoT environments. It provides a solid framework for conducting large-scale SIoT simulations as each scenario captures different configurations, interactions, and device ownership patterns. Therefore, these different scenarios can be used to create SIoT datasets that can be used to customise the simulation to take into account various aspects such as the number of devices owned by users and the complex behaviour of these devices within the SIoT ecosystem. This flexibility allows researchers to precisely tailor their simulations to the intended context, allowing them to learn more about how SIoT systems behave and function in different scenarios. Figure 24 carefully presents a spectrum of simulation scenarios, each comprising different features and attributes. These variations serve as clear examples of the flexible possibilities that SIoT-Sim offers when simulating a wide variety of scenarios within the SIoT environment:

A. **Single-device scenario**: In this scenario, each user only has one IoT device that is part of the SIoT network. This is a user-friendly method for collecting information about SIoT devices. During the early stages of development, researchers use it to understand the behaviour of a single device. The dataset created in this scenario would focus primarily on the performance and connectivity of a single device. In addition, the data collected can be leveraged to enhance device performance and reliability.

B. **Multi-devices scenario**: In this scenario, each user has multiple IoT devices connected to the SIoT network. Although the interactions between devices in this scenario are more complicated than in the single-device scenario, the systems require an understanding of these interactions to design reliable SIoT. The dataset created in this scenario focuses on the behaviour of different devices, including how they communicate with each other, how users use them, and how well they perform. The aim is also to improve the reliability and performance of the system.

C. **Faulty device scenario**: The focus of this scenario is sporadic malfunctions of the IoT devices or inaccurate data delivery within the SIoT system. An important use of the dataset generated in this scenario is to evaluate how well the network can detect and resolve device errors. Additionally, this dataset provides important insights into the system's ability to maintain data integrity, ensuring accurate and high-quality information in the SIoT.

D. **New device scenario**: In this scenario, users add new IoT devices to the SIoT network. This scenario would produce a dataset primarily concerned with the process of adding new devices to the network, including how often they are added, and how these additions affect the behaviour and overall performance of the network. It is also important to remember that this dataset helps make SIoT systems more scalable by providing insightful information about how well the network can support and adapt to new devices that users add to it.

E. **Multi-user scenario**: This scenario simulates a situation where multiple users either connect their own devices to the SIoT network or share the same IoT devices. The dataset generated by this scenario can be used to evaluate how well the network can manage numerous users and their interactions with it and to identify potential privacy and security issues. Additionally, this dataset provides a comprehensive understanding of the resilience and scalability of the SIoT environment across a variety of collaborative user activities.

F. **Disconnected device scenario**: In this scenario, IoT devices regularly lose connection to the network for various reasons, including low battery life, network disruptions, or other technical issues. The following dataset contains important information about how frequently and for how long these device interruptions occur, as well as details about how these interruptions impact user’s behaviour and network performance. When intermittent device connectivity issues occur, this scenario provides important insight into the robustness and reliability of SIoT systems.

G. **Mobility scenario**: This scenario includes the movable devices within the network. The generated SIoT dataset serves as a valuable resource for assessing the performance of the SIoT system when dealing with movable devices and ensuring smooth communication when navigating the network. It allows evaluation of the network's adaptability to changes in device locations and tests its efficiency in maintaining connectivity and data transmission reliability.

H. **Attacks propagation scenario**: This scenario helps understand how malicious activities spread throughout the SIoT network. the generated SIoT dataset is essential for evaluating resilience to security threats and its ability to detect and stop the spread of attacks across different SIoT systems.

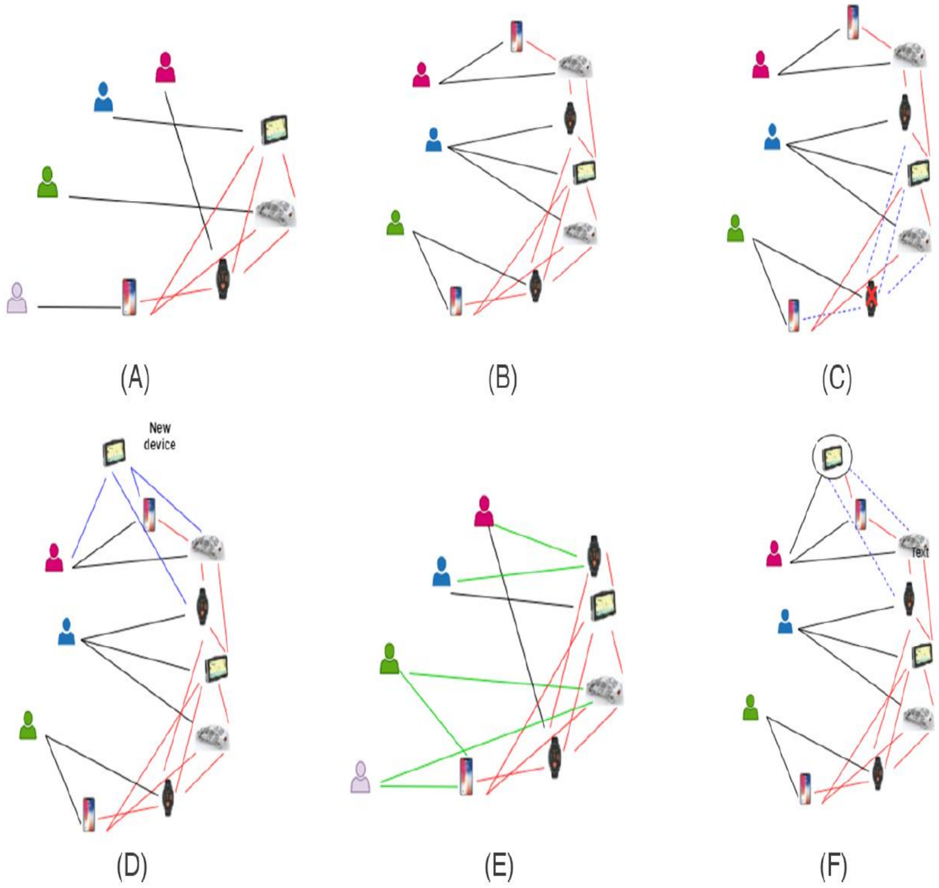


Figure 24 SIoT-Sim various custom scenarios

5.5. Generated SIoT Dataset Description

The biggest problems with SIoT are the lack of available datasets and the low quality of the data. To address this challenge, the main goal of SIoT-Sim is to provide invaluable datasets that can be tailored to different research needs to evaluate and test a range of trust management models or any SIoT systems. This created SIoT dataset contains a variety of features such as social interactions between devices and users (friendships and communities of interest, social relationship), data transfers and transactions, and various event types. The trustworthiness of each object in the SIoT network depends on several factors, including packet delivery ratio (PDR) and social similarity based on friendships and communities of interest. After addressing these issues in detail, the resulting SIoT dataset becomes an invaluable tool for researchers, giving them the opportunity to explore trust management models in SIoT in more detail.

The generated SIoT dataset includes six trace sets: Friends_progress, CoIs_progress, Transmission_progress, Friend_list_progress, Event_progress, and Users_CoIs_list.

1. Friends_progress trace: This trace provides details about the friends that users and devices have made on the IoT network. Table 10 records various events related to friendships, including COI, devices, and users. friendship events involve nodes making new friends or ending a friendship. The dataset presents a chronological record of events, indicating the involved nodes, timestamps, and actions, such as becoming or terminating a friendship.

Table 8 Friends_progress trace elements description

Sending Time	Receiving Time	Id. Sender	Sender. Own	Receiver.Id	Receiver. Own	Payload
t	t	Device.id,	User.id	Device.id	User.id	Two nodes became friend
t	t	Device.id,	Coi.id	Device.id,	Coi.id,	Two nodes became friend
t1	t2	User.id	User.id,	User.id	User.id,	Two nodes became friend
t1	t2	Device.id,	None	Device.id,	None	Two nodes became friend
t1	t2	Device.id,	User.id	Device.id	User.id	Two nodes stop being friends

t2	t3	User.id	User.id,	User.id	User.id,	Two nodes stop being friends
t2	t3	Device.id,	None	Device.id,	None	Two nodes stop being friends

2. CoIs_progress trace: This trace provides details about the social relationships between IoT devices and the interest groups that users have formed in the SIoT network. It represents groups of users and devices who are more likely to interact with one another and share interests, preferences, or goals. Table 11 captures records of all COI-related events, such as: creating, opening, closing, and deleting the COI**.**

Table 9 CoIs_progress trace elements description

Sending Time	**Receiving Time**	**Sender.Id**	**Sender. Own**	**CoI**	**Receiver. Id**	**Receiver. Own**	**Payload**
t	t	Coi.id	None	None	None	None	CoI Has Been Created
t	t	Coi.id	None	Coi.id	None	None	CoI Is Now Open
t	t1	Device.id	User.id	Coi.id	Coi.id	None	Joined CoI
t1	t2	Device.id	None	Coi.id	Coi.id	None	Joined COI
t1	t2	Device.id	Coi.id	Coi.id	Coi.id	None	Joined CoI
t1	t2	Device.id	User.id	Coi.id	Coi.id	None	Left CoI
t1	t2	Device.id	None	Coi.id	Coi.id	None	Left CoI
t2	t3	Device.id	Coi.id	Coi.id	Coi.id	None	Left CoI
t	t	Coi.id	None	Coi.id	None	None	CoI Is Now Close
t2	t3	Coi.id	None	None	None	None	CoI Has Been Deleted

3. Event_progress trace: This trace contains information about different types of events that can occur in the SIoT network. Table 12 captures records of all events involving users, devices, and CoI, including devices joining the network, devices, users, and CoI creation.

Table 10 Event_progress trace description

Sending Time	Receiving Time	Event_ Type	Sender. Id	Sender . Own	CoI	Receiver . Id	Receiver . Own	Payload
t	t	Event1	Coi.id	None	None	None	None	CoI Has Been Created
t	t	Event2	Coi.id	None	Coi.id	None	None	CoI Has Been Created
t	t1	Event1	Device.id	User.id	Coi.id	Coi.id	None	User Joined Network
t1	t2	Event3	Device.id	None	Coi.id	Coi.id	None	Device Joined Network
t1	t2	Event5	Device.id	Coi.id	Coi.id	Coi.id	None	Device Joined Network
t1	t2	Event1	Device.id	User.id	Coi.id	Coi.id	None	User Joined Network
t1	t2	Event0	Device.id	None	Coi.id	Coi.id	None	Device Has Been Created
t2	t3	Event6	Device.id	Coi.id	Coi.id	Coi.id	None	Device Has Been Created
t	t	Event3	Coi.id	None	Coi.id	None	None	CoI Has Been Created
t2	t3	Event2	Coi.id	None	None	None	None	CoI Has Been Created

4. Transmission_progress trace: This trace contains details about data transmissions and transactions that take place within the SIoT network. It shows how data is exchanged between different nodes or devices. Table 13 tracks various transmission events involving users, devices, and CoI. Each entry contains information about devices, users, CoI, timestamps and payload including a trusted transmission and a malicious transmission between two devices.

Table 11 Transmission_progress trace description

Sending Time	Receiving Time	Sender.Id	Sender. Own	CoI	Receiver. Id	Receiver. Own	Payload
t	t	Device.id	None	None	Device.id	None	Transmission (Trusted) or (Malicious)
t	t	Device.id	Coi.id	None	Device.id	Coi.id	Transmission (Trusted) or (Malicious)
t	t	Device.id	User.id	None	Device.id	User.id	Transmission (Trusted) or (Malicious)
t	t	Device.id	None	Coi.id	Device.id	None	Transmission (Trusted) or (Malicious)
t	t	Device.id	Coi.id	Coi.id	Device.id	Coi.id	Transmission (Trusted) or (Malicious)
t	t	Device.id	User.id,	Coi.id	Device.id	User.id,	Transmission (Trusted) or (Malicious)

5. Friend_list_progress Trace: The dataset captures the dynamics of friendships within an IoT network over time, with each row representing a specific timestamp indicating the chronological order of events, as shown in Table 14. Users are identified by unique IDs, and for each timestamp, the dataset records each user's friends as well as any enmities they may have formed. This structured recording enables the analysis of social interactions and the identification of developing friendships or enmities across the networks.

Table 12 Friends_list_progress trace description

Timestep	User_ID	Friends_ID	Enemies_ID
t	U1	[U1, U5]	[]
t	U2	[U2, U7, U9]	[]
T1	U3	[U9, U3, U16, U1]	[]
t	U4	[U8, U3, U4]	[]
T3	U5	[U1, U5, U20, U8, U7]	[U13]

6. **Users_CoIs_list:** The dataset captures the dynamics of CoIs by users within an IoT network over time, with each row representing a specific timestamp indicating the chronological order of events, as shown in Table 15. Users are identified by unique IDs and for each timestamp, the dataset records each user's CoIs.

Table 13 Users_CoIs_list trace description

Timestep	User_ID	CoIs_ID
t	U1	[CoI1]
t	U2	[CoI2, CoI 8,]
T1	U3	[CoI 9]
t	U4	[CoI 8, CoI 3, CoI 4]
T3	U5	[CoI 1]

The generated SIoT dataset is a comprehensive and representative feature set that captures the complexity of real-world SIoT interactions. This dataset covers a wide range of aspects including social interactions (human-to-human, object-to-object and human-to-object relationships), transactions, data transmission, social object relationships (OOR, POR, WOR, SOR), and different event types. It stands out for its similarity to real-world scenarios and highlights the SIoT-Sim's ability to capture the dynamics and complexity of interactions within the SIoT ecosystem. Therefore, one of the main advantages of the dataset is that its wide feature set makes it serve as a perfect benchmark for evaluating trust management models in an SIoT environment, providing a comprehensive testing ground for evaluating the effectiveness of various trust management models and simple approaches to sophisticated machine learning algorithms.

5.6. Summary

The lack of a SIoT simulator tool has been identified as a major obstacle for researchers in the area of SIoT. This is due to the dynamic and complex nature of SIoT systems, whose effectiveness depends heavily on the environment in which they are deployed.

To address this problem, this chapter introduces a novel SIoT simulator tool “SIoT-Sim” that aims to identify essential properties and specifications for such a tool, as well as to generate realistic SIoT data that can be used for tests and evaluations by simulating different contexts and SIoT scenarios. Due to its adaptability and flexibility, SIoT-Sim can be adapted to various SIoT applications and environments. SIoT-Sim provides numerous features, such as the ability to model various attacks and vulnerabilities and simulate different types of sensors and networks. The ability to test and evaluate SIoT systems in a repeatable and controlled environment is one of the key benefits of SIoT-Sim for researchers and practitioners. This not only improves the performance of the SIoT systems but can also help identify and resolve potential security and privacy concerns.

Chapter 6

Evaluation and testing of MCTM-SIoT Framework and model in SIoT

6.1. Introduction

In the previous chapters, a novel MCTM-SIoT framework was proposed. It provides a comprehensive overview of the SIoT ecosystem and pays particular attention to how different SIoT components are linked to one another and to TM. In addition, the framework incorporates multiple contextual information into the final trust assessment to enable trustworthy inference and improve the overall security and reliability of the system by helping to select the most trustworthy SP in the absence of prior node behavioural history. The framework is validated using both mathematical and experimental techniques. Mathematically, by proposing a MCTM-SIoT approach to identify the most trustworthy SP based on a set of trust context metrics, namely UCT, DCT, ECT, TCT. On the other hand, experimentally, by using the design SIoT simulator, which simulates and analyses the behaviour of SIoT systems and enables the generation of realistic SIoT data to evaluate the effectiveness of the MCTM-SIoT framework and model in SIoT.

In this chapter, a series of experiments are presented to validate the above framework and model at the level of composition and aggregation steps. To this end, (section 6.2) summarises a different scenarios of simulation settings. (Section 6.3) presents a comparative analysis of the generated SIoT datasets and MCTM-SIoT model in various scenarios using a ML-driven aggregation approach to evaluate the performance of MCTM-SIoT model. (Section 6.4) determines the influence of each contextual metric on the overall trust score of each node in different scenarios. In (section 6.5) discusses the experimental results and (section 6.6) summarises the content of the whole chapter.

6.2. Simulation settings in different SIoT scenarios

Due to the unavailability of real SIoT datasets, many studies rely on simulations for experimentation. In this study, the experimental environment for evaluating the effectiveness of the elaborated MCTM-SIoT framework utilised the SIoT-Sim simulator on the Google Colab platform, simulating three distinct scenarios, each taking between 4 to 6 hours depending on the number of devices involved and different network dynamics and user-device interactions. Table 13 provides a comprehensive summary of the simulation settings for each scenario and describes three different scenarios with varying degrees of network dynamics and user-device interactions.

Scenario 1 featured moderate interaction frequency and low dynamics, which closely resembles settings such as a smart conference or restaurant. In this scenario, users typically engage with a limited number of devices, resulting in stable and predictable interactions. The environment is characterised by a consistent flow of information exchange and controlled device usage, making it ideal for evaluating how the MCTM-SIoT framework performs under relatively stable conditions.

Scenario 2 represented medium interaction frequency and moderate dynamics, akin to smart health centre. In this scenario, user-device interactions are more varied, with users frequently interacting with multiple devices across different applications, such as medical monitoring equipment, patient information systems, and mobile health applications. The dynamics in this environment are influenced by factors such as patient movement, varying device availability, and the need for real-time data sharing among healthcare professionals, thus providing a more complex setting for testing the framework's adaptability and robustness.

Scenario 3 depicted a highly dynamic and interactive network environment, similar to smart campus. This scenario is marked by a high volume of interactions and frequent changes in device availability and user mobility. Users in a smart campus setting engage with numerous devices across different platforms such as smart classrooms, IoT-enabled libraries, and campus-wide communication tools leading to unpredictable patterns of device interactions. The framework's effectiveness is critically assessed in this scenario to understand its ability to manage and optimise resources in a fast-paced and ever-changing environment.

Each scenario was configured with specific parameters, including network dynamics ranging from 30% to 60%, a consistent malicious interaction rate of 30%, and battery levels with a minimum of 150 and a maximum of 2000. These configurations allowed for a comprehensive assessment of user-device interactions involving between 1 to 5 devices per scenario and a total of 300 users participating in the simulations. By simulating these varying contexts, the study aims to evaluate the MCTM-SIoT framework's effectiveness in adapting to diverse interaction patterns and network conditions, ultimately providing valuable insights for the deployment of SIoT systems in real-world applications.

Table 13 Simulation setting for different SIoT scenarios

Scenarios	Network Dynamics	Malicious rates	Min batterie level	Min batterie level	Devices Number	Users number	Simulation time
Scenario 01	30%	30%	150	2000	[1,5]	100	3h
						200	3h 40
						300	4h 10
Scenario 02	50%	30%	150	2000	[1,5]	100	4h 05
						200	5h00
						300	5h 40
Scenario 03	60%	30%	150	2000	[1,5]	100	5h 20
						200	5h 55
						300	6h 30

The dataset generated from different scenarios by SIoT-Sim described in chapter 6, used to evaluate the Multi-Context Trust Management in SIoT (MCTM-SIoT) framework, includes between 100 and 1500 devices and captures a variety of device and user interactions in different scenarios such as smart campuses and smart care center. It records social interactions, including friendships, CoIs, and SOR, along with POR, OOR and COR. The dataset tracks event types like devices joining or leaving the network, data transmissions (trusted and malicious), and network handshakes. Additionally, it monitors malware propagation across the network for security testing and logs user and device actions such as joining or leaving CoIs, sending messages, and experiencing network disconnections.

6.3. Evaluating SIoT datasets against MCTM-SIoT model across diverse scenarios

The comparative analysis between SIoT datasets and MCTM-SIoT model in different scenarios consists of three procedures. The first procedure is performed to evaluate the generated SIoT dataset by classifying the node as harmless and malicious. The second procedure is performed to evaluate the proposed MCTM-SIoT model based on various contextual metrics. These contextual metrics are used to determine the final trust score of each node and help users select the most trustworthy SP by predicting the final trust score of each node in the network. The last procedure is performed to compare the results obtained from both models.

To achieve this, a series of experiments are conducted on two types of datasets including the generated SIoT dataset and the context-based SIoT dataset based on different contextual metrics.

6.3.1. Evaluation of SIoT dataset

In this section, we mainly use a random forest classifier to classify the nodes in the SIoT network as either harmless or malicious. Preparing the dataset for learning is an important step that must be completed before starting the process. In particular, the dataset contains simulation results, which means that careful preprocessing is required to ensure that it is suitable for training the random forest classifier. This step is critical for eliminating redundant or irrelevant rows of data that could lead to noise or overfitting. In order to improve the quality and relevance of the dataset and enable more reliable and accurate classification results (Zelaya, 2019).

As part of the preprocessing step, I first removed all rows that had missing values since incomplete data cannot be used to train the model to prevent classifier bias. I then looked for features that were highly correlated and eliminated duplicates. In order for the random forest algorithm to accurately determine the importance of each feature. I also normalised the feature values to bring them to a common scale.

After cleaning the dataset, I split it into test and training sets and saved some of the data for the final evaluation. By using cross-validation to adjust hyperparameters such as tree depth and number of trees, I was able to train a random forest classifier using the training data. To objectively determine the performance of the tuned model, it was evaluated on the test set.

To evaluate the performance of the random forest model, accuracy, precision, recall, FPR, F-measure, and other information retrieval metrics are commonly used (Zheng, 2015).

1. **Accuracy**: This measure represents the percentage of accurate predictions out of all predictions made. It is determined by dividing the total number of correct predictions by the total number of predictions made, as depicted in Equation 14. When there is a class imbalance, the accuracy may not be sufficient to measure the performance of a model.

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{FN} + \mathrm{TN}} \tag{14}$$

2. **Precision:** It is calculated by dividing the number of true positives by the sum of true positives and false positives, as shown in Equation 15. A higher precision score suggests that the model makes fewer false positive predictions, indicating a greater likelihood of correctness when predicting a positive outcome.

$$Precision = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \tag{15}$$

3. **Recall:** Sometimes referred to as the true positive rate or sensitivity, it represents the proportion of true positive cases correctly identified by the model. This is calculated by dividing the total number of true positives by the sum of true positives and false negatives (Equation 16). The recall is particularly important when false negative results are associated with high costs.

$$Recall = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{16}$$

4. **False Positive Rate (FPR):** FPR indicates the percentage of actual negative cases that the model incorrectly classified as positive. It is crucial When false positive results are associated with high costs. FPR is calculated by the ratio of false positive results to the total number of false positive and true negative results (Equation 17).

$$FPR = \frac{\mathrm{FP}}{\mathrm{FP} + \mathrm{TN}} \tag{17}$$

5. **F-measure**: The harmonic mean of recall and precision is called the F1 score or F-measure. It offers a single score that balances recall and precision. The F-measure, which accounts for both false positives and false negatives (Equation 18), is particularly useful in cases where the class distribution is unbalanced.

$$\mathrm{F} - \mathrm{measure} = 2 * \frac{\mathrm{Precision} * \mathrm{Recall}}{\mathrm{Precision} + \mathrm{Recal}} \tag{18}$$

The random forest achieved different accuracies in classifying the SIoT node as malicious and harmless based on the above scenarios, as shown in Figure 25, and the obtained recall, precision and F-measure are reported in Table 14.

Table 14 Evaluation metrics in different scenarios

Series		**Evaluation Metrics**				
Scenarios	**Users number**	**Precision**	**Recall**	**F1 score**	**False positive rate**	**True positive rate**
Scenario 01	**100**	0.86	0.88	0.87	0.12	0.89
	200	0.84	0.85	0.84	0.16	0.86
	300	0.82	0.83	0.82	0.18	0.84
Scenario 02	**100**	0.83	0.85	0.84	0.16	0.86
	200	0.81	0.80	0.81	0.27	0.87
	300	0.77	0.78	0.77	0.23	0.79
Scenario 03	**100**	0.78	0.80	0.79	0.24	0.83
	200	0.77	0.77	0.77	0.23	0.77
	300	0.71	0.72	0.71	0.32	0.76

Figure 25 and Figure 26 show the performance metrics of a random forest classifier evaluated on a raw SIoT dataset in three scenarios with increasing network dynamics and user numbers.

The results show that model performance, measured in terms of accuracy, precision, recall, F1 score, false positive rate, and true positive rate, decreases significantly when moving from low dynamic situations such as scenario 01 to highly dynamic environments such as scenario 03. Moreover, metrics continue to deteriorate as the dataset size increases from 100 to 300 users.

1. Accuracy remains highest in scenario 01, where network dynamics are low. For 100 users, accuracy starts at 0.88, indicating that in less dynamic networks, the classifier has strong predictive accuracy. As network dynamics rise to scenario 03 and the user count increases to 300, accuracy declines to 0.73, emphasising the classifier's challenge in adapting to the complexities of highly dynamic environments.
2. Precision: initially high in scenario 01 at 0.86 (100 users), precision represents the model's reliability in making positive identifications. However, it falls significantly to 0.71 in scenario 03 with 300 users, suggesting that in complex environments, the model is more prone to false positives, struggling to confidently classify malicious nodes.
3. Recall reflecting the classifier's sensitivity to true positives, declines from 0.88 to 0.72 between scenarios 01 and 03. This trend points to a rise in false negatives, where the model fails to detect malicious nodes in more dynamic networks with increased interaction variability.
4. The F1 score, balancing precision and recall, follows a steady downward trend from 0.87 to 0.71, mirroring the decline in both core metrics and underscoring the combined impact of lower precision and recall under higher dynamics.
5. The FPR increases from 0.12 in scenario 01 to 0.32 in scenario 03, indicating a rise in false alarms as network complexity escalates. In high-dynamic environments, the classifier is more likely to misclassify benign nodes as malicious, showing its limitations in managing high rates of benign-malicious interaction
6. TPR experiences a decline from 0.89 to 0.76 across the scenarios, highlighting the model's decreasing ability to identify true positive cases as dynamics grow. This trend confirms the classifier's struggle to maintain robust detection capabilities under high complexity.

The decline across these metrics, especially precision, recall, and F1 score, shows the classifier's difficulty in managing high dynamicity and large user scales. High network dynamics imply frequent changes in relationships, user-device interactions, and data transmission patterns, leading to increased false positives and false negatives. Additionally, as benign nodes interact in a highly dynamic manner, the classifier increasingly struggles to differentiate between benign and malicious behaviours without added contextual cues. This analysis reinforces the need for models capable of handling dynamic SIoT environments, ensuring effective machine learning applications across evolving network conditions.

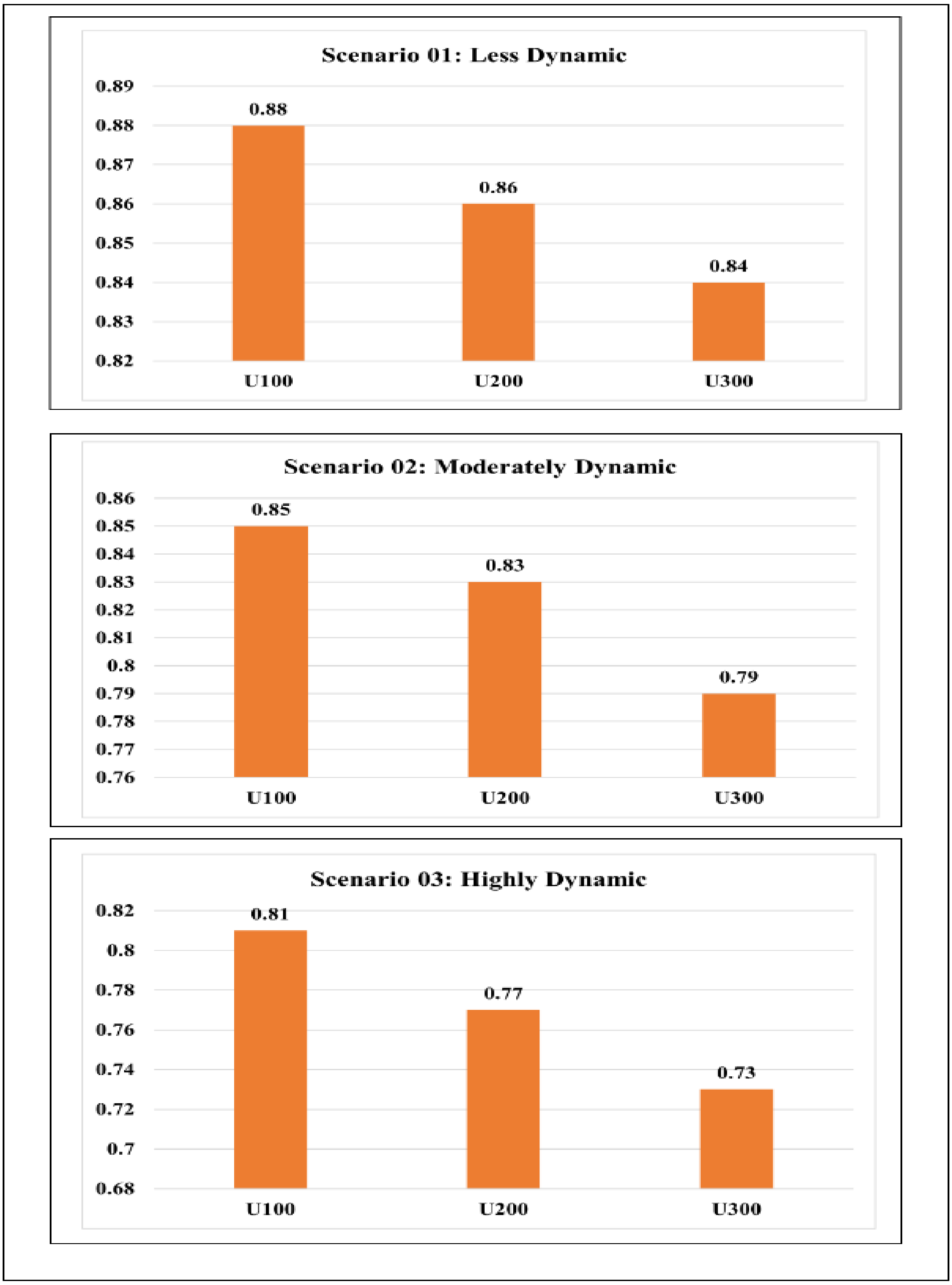
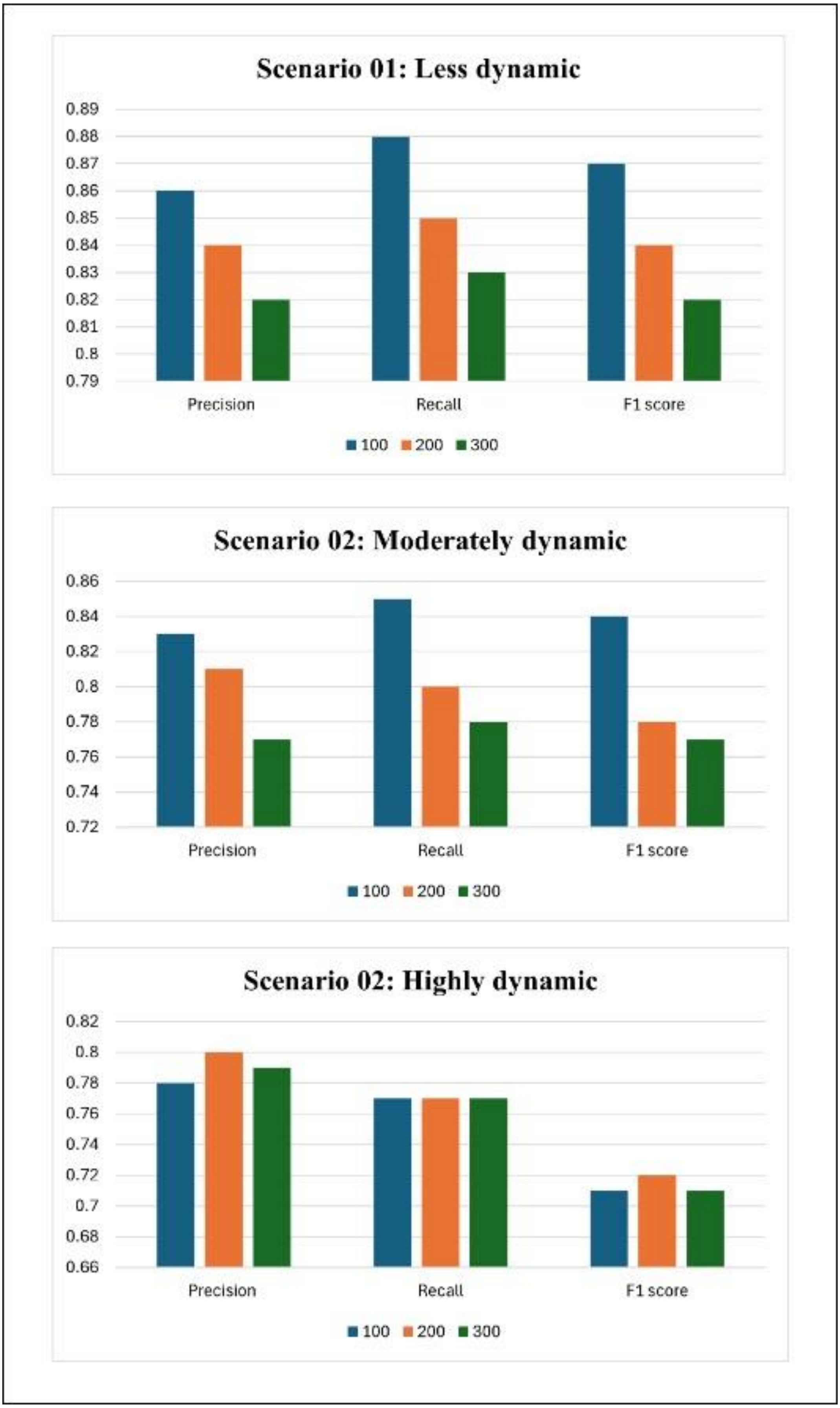


Figure 25 SIoT datasets Accuracies in Different SIoT Scenarios



Scenario 01: Less dynamic

Scenario 02: Moderately dynamic

Scenario 02: Highly dynamic

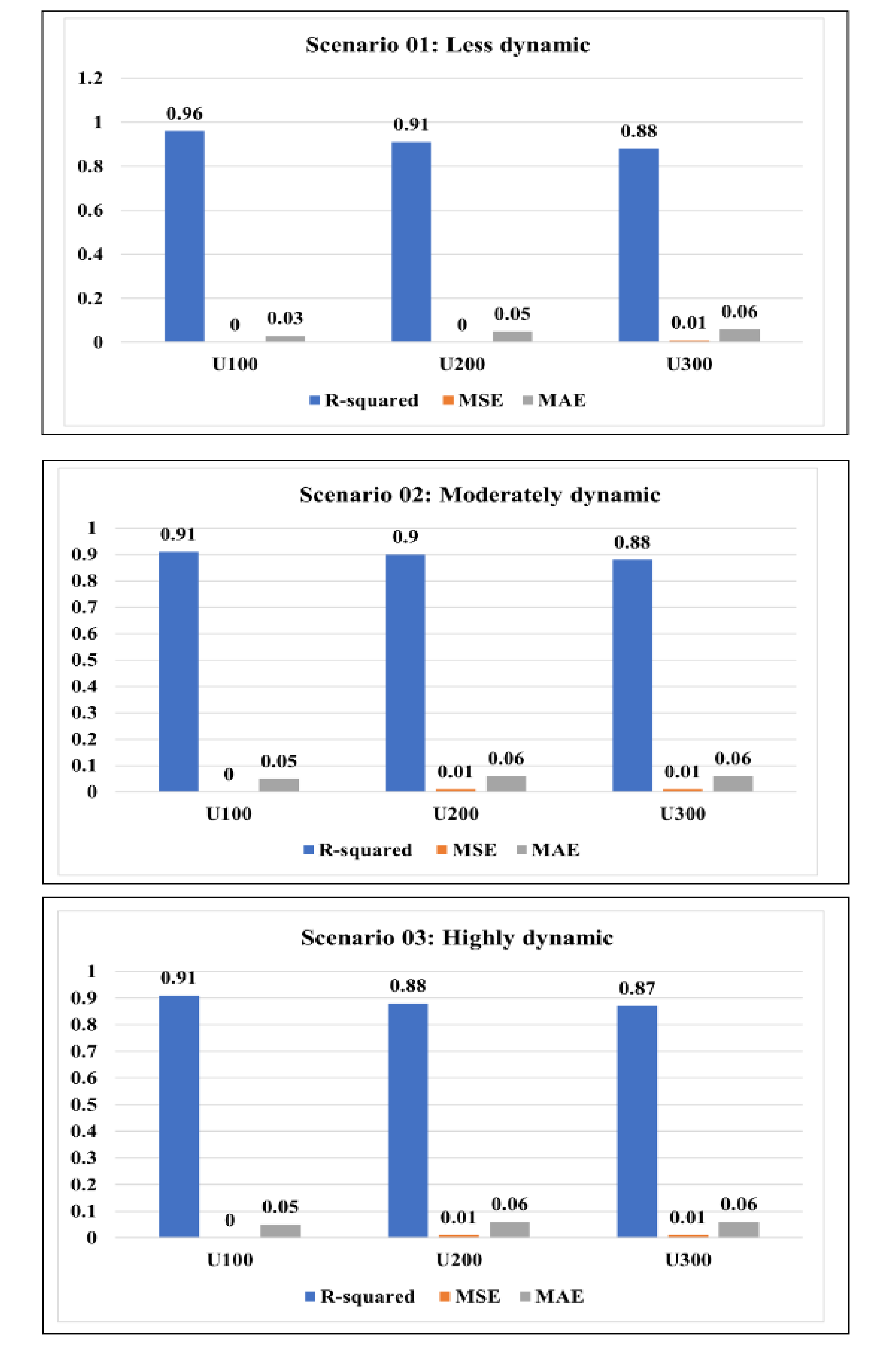
Figure 26 Evaluation metrics results for different scenarios

6.3.2. Evaluation of MCTM-SIoT model

This section focuses on predicting the trust value of each node in the SIoT network to select the most trustworthy service provider in the absence of prior node behaviours history by using supervision ML algorithm maned random forest regressor to predict the continuous numeric value of the SIoT entity's trust scores obtained from the aggregation of the contextual trust metrics DCT, UCT, ECT, TCT. To evaluate the performance of the random forest regressor model, the Mean Absolute Error (MAE), Mean Squared Error (MSE), and R-squared (R2) metrics are commonly used (Durap, 2023).

1. **Mean Absolute Error (MAE)** is a metric used to measure the average absolute differences between predicted values and actual values in a regression problem. It is computed by averaging the absolute differences between predicted and actual values across all data points. A lower MAE signifies better model performance.
2. **Mean Squared Error (MSE)** is a metric utilised to measure the average of the squares of errors or deviations between predicted values and actual values in a regression problem. It is obtained by averaging the squared differences between predicted and actual values across all data points. A lower MSE also signifies better model performance.
3. **R-squared (R2)** which is also is known as the coefficient of determination, denotes the portion of the variance in a dependent variable that can be elucidated by one or more independent variables within a regression model. It ranges from 0 to 1, with 0 indicating that the model fails to account for any variability in the response data around its mean, and 1 indicating that the model captures all variability. This metric serves as a gauge of how accurately the regression model aligns with the actual data, with higher R-squared values indicating superior fit.

The Random Forest Regressor achieved different accuracies in predicting the trust score of each node in the SIoT network based on the above scenarios, shown in Figure 27.



Scenario 01: Less dynamic

Scenario 02: Moderately dynamic

Scenario 03: Highly dynamic

Figure 27 MCTM-SIoT model accuracies in Different SIoT Scenarios

Figure 27 shows a comprehensive analysis of the performance metrics obtained from evaluating a Random Forest Regressor model on the MCTM-SIoT framework. The evaluation is carried out in three different scenarios characterised by different network dynamics and user numbers, with the aim of evaluating the robustness and adaptability of the model in different SIoT environments. Evaluating model performance includes three key metrics: R^2, MSE, and MAE, which provide insight into the accuracy and reliability of the model predictions.

1. R^2 values, consistently ranging from 0.87 to 0.96, underscore the model's capacity to capture the variance in actual trust values across all test scenarios. This high R^2 score confirms the model's ability to explain the majority of variability in trust scores, indicating that it effectively models node behaviour under various network dynamics. This is particularly crucial in SIoT, where trust prediction accuracy affects reliable network interactions and service provision.
2. MSE metric, remains notably low across scenarios, with values between 0 and 0.01. Such low MSE scores demonstrate the model's precision in minimising prediction errors even as the complexity and dynamics of the network increase. This stability indicates that the random forest regressor can handle fluctuations in trust levels due to varied environmental and network factors without significantly deviating from actual values.
3. MAE values ranging from 0.03 to 0.06, the random forest regressor achieves a low average error, reflecting its consistency in accurately predicting trust values with minimal deviations across different SIoT configurations. The low MAE complements the MSE results, underscoring that the error size remains small even in demanding conditions, such as high user counts (e.g., U300 in highly dynamic networks).

In scenarios marked by high network dynamics and user counts, the model maintains reliable accuracy and minimal error rates, with metrics such as $R^2 = 0.87$, MSE = 0.01, and MAE = 0.06 in the U300 Highly Dynamic case. These results illustrate that the random forest regressor is resilient in capturing trust scores even when SIoT networks undergo substantial changes, including increased user interactions and node mobility.

The stable performance of the model across these metrics indicates that the MCTM-SIoT framework effectively integrates contextual factors such as user, device, environmental, and task conditions into its trust evaluations. This integration allows the model to handle the diverse scenarios typical in SIoT, where trustworthiness assessment plays a critical role in maintaining reliable, secure network interactions. High R^2 scores and low error metrics (MSE, MAE) ensure that the framework is suitable for real-world applications requiring dependable trust-based service selection.

The results collectively confirm that the random forest regressor within the MCTM-SIoT framework not only provides accurate trust score predictions but also proves resilient to network dynamics and scalable with user growth. This makes the MCTM-SIoT model a robust approach for trust assessment in SIoT, facilitating efficient SP selection and enhancing secure, trustworthy communication across the network

6.3.3. Comparative analysis between SIoT datasets and MCTM-SIoT model in various scenarios

In this section, we conduct a comparative analysis between the accuracy of the generated SIoT datasets and the performance of the MCTM-SIoT model. The evaluation is conducted across different levels of network dynamics and user numbers to evaluate the robustness and reliability of the MCTM-SIoT. Figure 28 shows two primary metrics used for the evaluation accuracy of the generated SIoT datasets and the R^2 for the MCTM SIoT model.

In less dynamic environment, the accuracy of the generated SIoT dataset is between 0.84 and 0.88, indicating a relatively high level of predictive ability. However, the accuracy decreases slightly as the number of users increases from U100 to U300. In contrast, the MCTM-SIoT model consistently achieves high R^2 values ranging from 0.88 to 0.96, indicating its ability to explain significant prediction in trust scores of each SIoT node. This suggests that the model effectively captures the underlying patterns of trust dynamics despite changes in user numbers.

In moderately dynamic environment, the environment becomes more dynamic, and the accuracy of the generated SIoT dataset further decreases and is between 0.79 and

0.85. This decline suggests that the generated dataset may have difficulty in accurately representing trust dynamics in scenarios with moderate dynamics and varying user counts. However, the MCTM-SIoT model maintains consistently high R² values, ranging between 0.88 and 0.91. This demonstrates the model's ability to adapt to changing environmental conditions and provide reliable predictions of trust scores of each SIoT node across different user scales.

In highly dynamic environments, the accuracy of the generated dataset decreases significantly and ranges from 0.73 to 0.81. This significant drop in accuracy suggests that based solely on analysis of the generated SIoT datasets may face difficulties in accurately predicting trust scores in highly dynamic SIoT environments. Despite the challenges presented by highly dynamic conditions, the MCTM-SIoT model shows remarkable stability with R² values between 0.87 and 0.91. This demonstrates the model's robustness and effectiveness in capturing trust dynamics and providing accurate predictions even under significant environmental conditions.

The comparative analysis highlights the effectiveness of the MCTM-SIoT model in improving the accuracy of each node's trust value represented in SIoT network predictions across different levels of network dynamics in SIoT environments. The MCTM-SIoT model delivers consistently superior performance. This consistency demonstrates the model's strength and reliability in adapting to various SIoT scenarios, where it effectively captures and interprets different contextual information to provide accurate predictions. Consequently, the results underscore the MCTM-SIoT model as a promising solution for trust management in dynamic SIoT ecosystems, providing improved predictive capabilities and promoting decision-making processes in service provider selection.

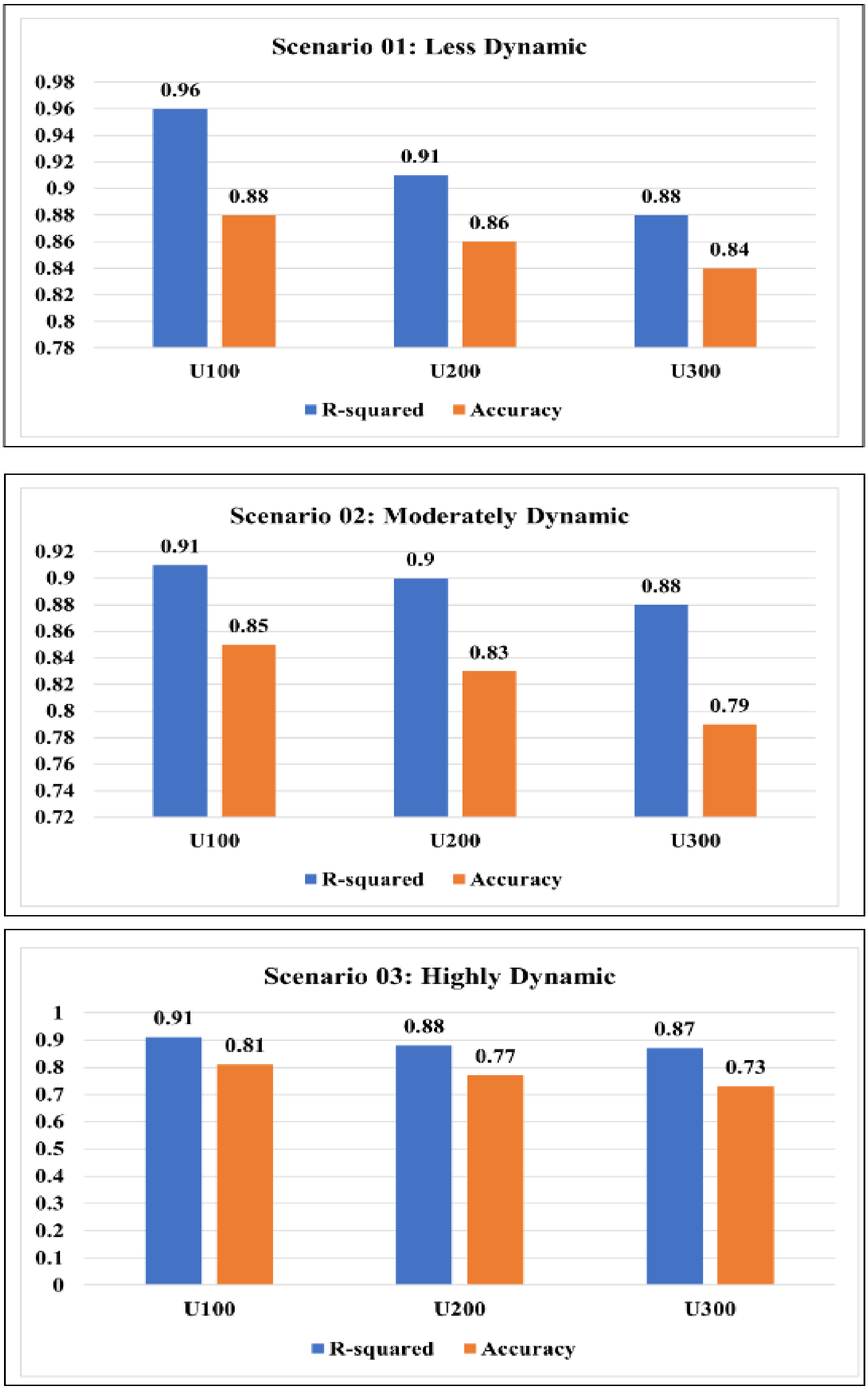


Figure 28 SIoT Dataset vs. MCTM-SIoT Model performance comparison in Different Scenarios

6.4. Comparative analysis against existing works

Our proposed model stands apart from existing works due to the absence of any directly comparable data or approaches that capture the unique characteristics of the SIoT. To date, no model or dataset fully aligns with the specific SIoT scenarios were simulated, marking a significant distinction in our research. While numerous studies focus on IoT or SN, they often fail to represent the complex interplay of social relationships and IoT devices that defines SIoT.

One of the major limitations of relevant studies is their reliance on datasets that do not accurately reflect SIoT environments. For instance, many works utilise SN data from platforms like Facebook or traditional IoT simulations, but these lack the contextual factors critical to SIoT simulation. As such, a direct comparison between our model and these previous approaches is not feasible. Additionally, previous research typically employs limited or manipulated datasets, as seen in the works of (Xia et al., 2019; Wei et al., 2021), which constrains the scale and diversity of their simulations. In contrast, our model leverages an automated simulator, SIoT-Sim, that generates a broader range of scenarios reflective of real-world dynamics. This allows us to simulate varying network conditions, device types, and user interactions, creating a more robust and comprehensive analysis. In terms of robustness, our model outperforms existing works. As seen in the Table 15, the accuracy metrics in studies like (Magdich, Jemal, and Ayed, 2022; Abderrahim, Elhedhili, and Saidane, 2017) are comparable to ours (0.96 and 0.91 respectively), but these studies do not simulate the SIoT scenarios that our model does. Our model achieves similar or superior performance (0.96/0.91/0.88) while incorporating a broader array of factors, making it superior in robustness and scope. Ultimately, our model offers a more comprehensive, scalable, and contextually accurate approach to SIoT simulation, standing in contrast to the limitations of prior studies. It outperforms existing models by combining a broader dataset, a more diverse simulation environment, and enhanced evaluation methods, making it a pioneering contribution to the field of SIoT research.

Therefore, there is no direct comparison between our model and existing models, as our approach goes beyond the limitations of prior work by simulating more diverse and realistic SIoT scenarios. This is reflected in both the scale and the robustness of our simulations, which are not matched by the datasets or methods used in earlier studies.

Table 15 Comparative analysis against existing work

Works	**Datasets**	**Evaluation methods**	**Accuracy**
Abderrahim, Elhedhili and Saidane (2017)	Simulated dataset	ML (Decision Tree)	0.91
Khani et al. (2018)	Simulated IoT + dataset online social network Facebook obtained from the Stanford Large Network Dataset Collection	Simulation-based	Not mentioned
Lin and Dong (2018)	online social network Facebook, Google+, and Twitter	Simulation-based	Not mentioned
Xia et al. (2019)	Simulated IoT dataset (Swim)	Simulation-based	Not mentioned
Wei et al. (2021)	Simulated IoT dataset (Netlogo)	Simulation-based	Not mentioned
Magdich, Jemal and Ayed (2022)	Simulated IoT (cooja) dataset + online social network dataset sigcomm2009	ML (Artificial Neural Network)	0.96
Our model	SIoT-Sim	ML (Random Forest)	0.96/ 0.91/ 0.88

6.5. Quantifying the impact of contextual metrics on trust score of each node in diverse scenarios

The foundation of the MCTM-SIoT framework and model consists of various trust context metrics, including ECT, TCT, DCT, and UCT. These metrics are combined to calculate a final trust score for each node presented in the SIoT network. However, gaining insight into the factors that influence trust requires an understanding of the specific impact of each contextual metric on each node's overall trust score. An effective approach for quantifying these impacts involves leveraging the feature importance of random forest regressor. The attached feature importance graphs in Figures 29, 30, and 31 visualise the relative impacts of the metrics under low, moderate, and high dynamics scenarios. Several illuminating observations can be observed from examining the graphs:

Above all, UCT clearly has the highest importance of all metrics in every scenario tested. It is consistently the predominant factor determining trust scores. Its characteristics are related to the user's ability to provide good intentions while providing feedback to friends and communities of interest. Following UCT, DCT is the second largest trust factor in all scenarios. The reliability of the devices themselves has a big impact on the trust in the nodes. Device attributes, including device credibility and social relationships, are important drivers of trust. The third most important trust metric is TCT. The specifics of tasks and requests moderately impact the trust calculation. The type of interactions and transactions impacts trust in the nodes. Finally, ECT has the lowest impact compared to the other metrics in all scenarios. Environmental conditions have some measurable weight but are much less important than user, device, and task context.

The relative importance varies somewhat across different levels of dynamics, but the order remains consistent. UCT and DCT consistently dominate as primary factors for node trust scores, with an average of 70% and 50%, respectively, while TCT and especially ECT play a secondary and tertiary role, with an average of 25% and 10%, respectively.

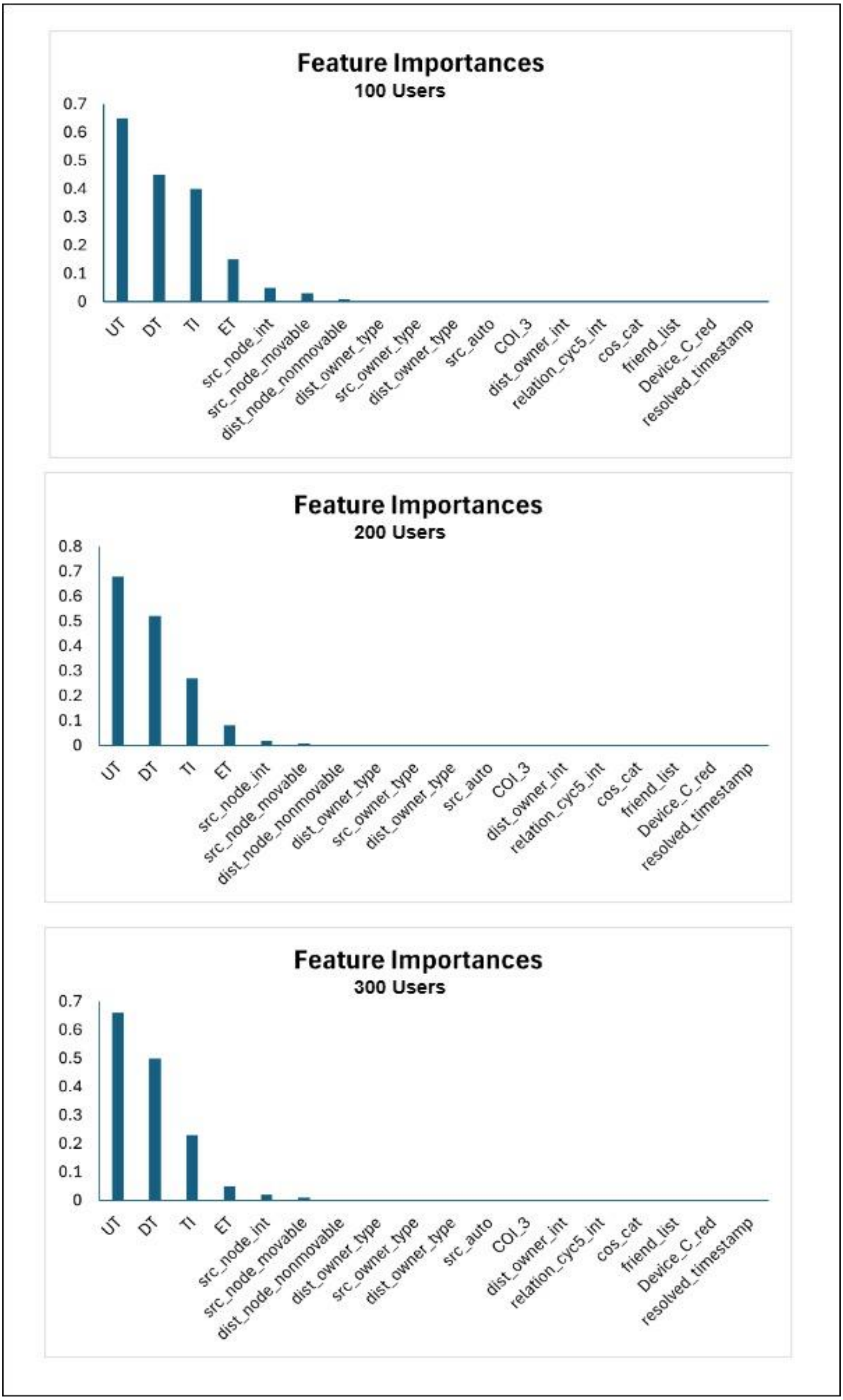


Figure 29 Feature importance in scenario 01 (low dynamic)

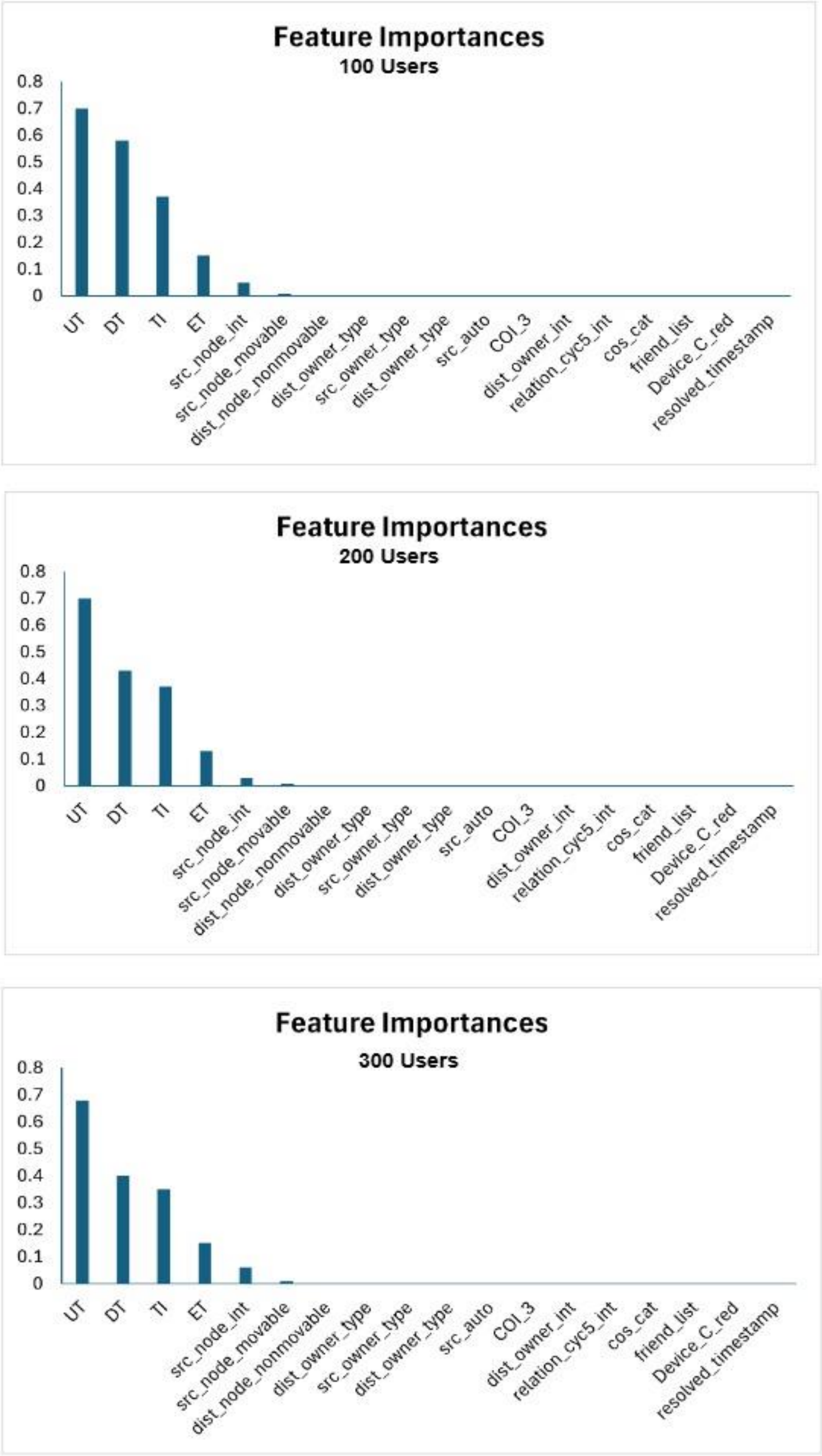


Figure 30 Feature importance in scenario 02 (Moderately dynamic)

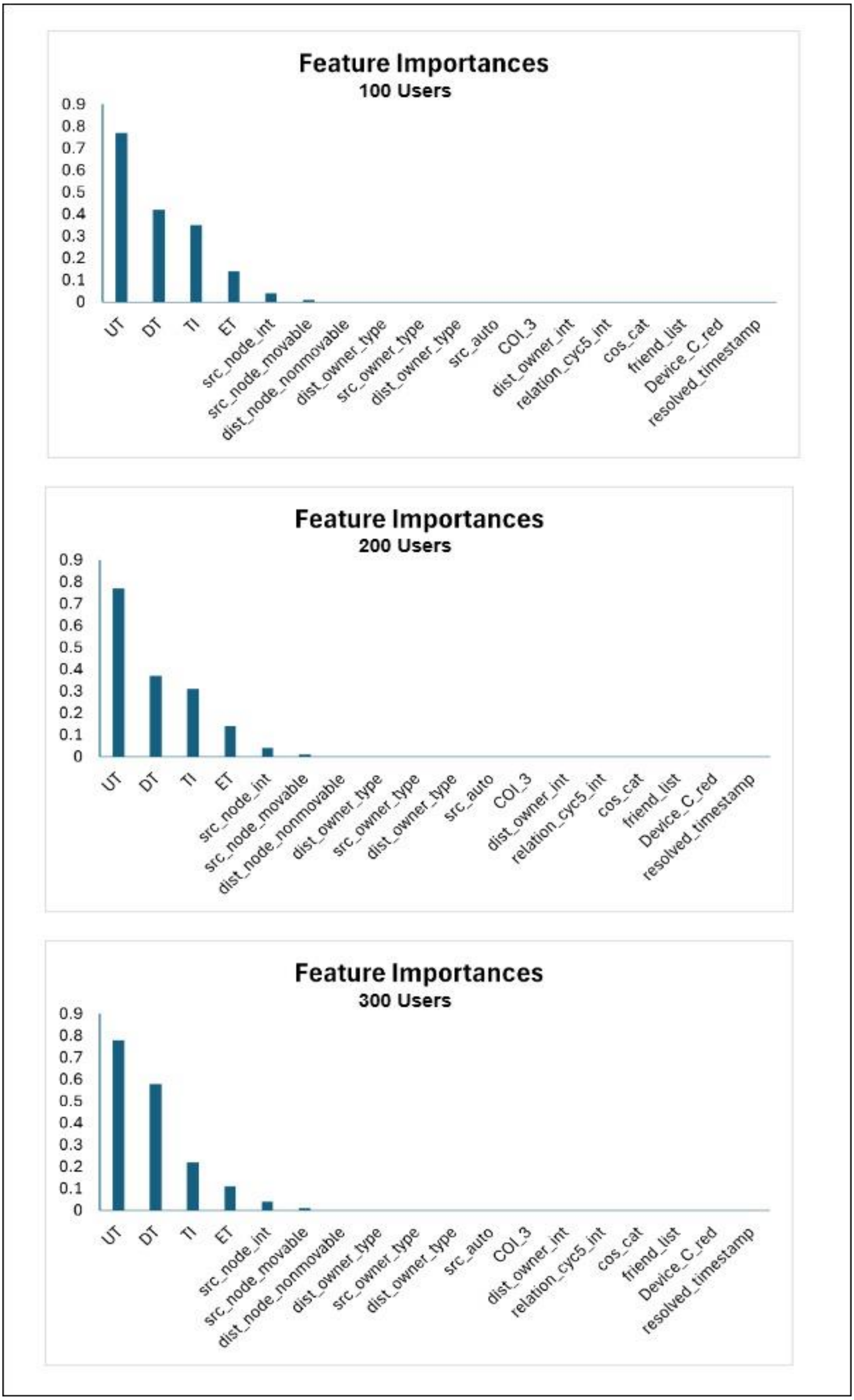


Figure 31 Feature importance in scenario 03 (Highly dynamic)

6.6. MCTM-SIoT framework performance analysis

The main goal of the MCTM-SIoT framework is to facilitate the user's decision-making in selecting the optimal service provider when there is no prior behaviour history for nodes. This selection process is based on predicting the trust scores of SIoT nodes that will be used to provide the desired service. By incorporating contextual trust metrics, we examine different dimensions of SIoT contextual trust relationships when assessing node trust.

To validate this approach, we conducted several comparative experiments. First, we developed four contextual SIoT trust metrics, namely UCT, TCT, DCT, and ECT to ensure the assessment of trust in specific contexts. We then aggregated these contextual trust metrics to calculate the trust score for each node present in the network. In the second step, we used supervised machine learning algorithms, specifically random forest, to compare the performance of the generated SIoT datasets, which do not take context information into account, with the MCTM-SIoT model.

Based on the experimental results in the previous section, we highlight the effectiveness of the MCTM-SIoT model in improving the accuracy of trust score predictions across different levels of network dynamics in SIoT environments.

The MCTM-SIoT model has higher accuracy in predicting trust scores and exceeds the accuracy of the generated SIoT dataset using the same ML algorithm, which represents a significant difference, especially in a crucial area such as security since the model is able to effectively predict trust levels between SIoT nodes and directly help to identify the trustworthy nodes for strong security measures within IoT networks. This might be explained by the manner in which the MCTM SIoT model examines contextual SIoT trust metrics, which could influence the trustworthiness of an SIoT node during network communication. This is particularly important because, in such a situation, each node may pose an increased risk compared to another. The MCTM-SIoT model proves to be a valuable tool for improving trust management and decision-making processes within the dynamic SIoT landscape. The MCTM-SIoT model proves to be a valuable tool for improving trust management and decision-making processes within the dynamic SIoT landscape.

On the other hand, using of the features importance of random forest regressor is important to quantify the specific impact of each contextual trust metric on the trust calculations of each node in all tested network dynamics scenarios. UCT is by far the most dominant factor, with node user characteristics related to providing good intentions and feedback to friends and communities of interest being highly influential drivers of trust score. DCT emerges as the second most important factor, with device credibility and social relationships having a major impact on trust. TCT moderately influences trust as the third most important characteristic, while ECT has only a small influence compared to the other metrics. Therefore, user and device context always prove to be primary determinants of node trustworthiness, while task and environmental context play secondary and tertiary roles. This feature importance analysis provides important insights into the contextual factors behind trust calculations in SIoT networks.

At this level of synthesis, we conclude that the developed framework stands out as a benchmark for all upcoming efforts in the field of trust management in SIoT. The MCTM-SIoT framework shows promise in improving trust scores and predicting the trustworthiness of each SIoT node within the network. Its objective is to allow users to select the best SP even without prior knowledge of node behaviour history, thereby ensuring reliable communication within the SIoT network.

6.7. Summary

This chapter provides a comprehensive overview of the validation of the MCTM-SIoT framework. The framework was evaluated by comparing generated SIoT datasets and MCTM-SIoT model in different SIoT scenarios using ML algorithm specifically random forest. The results showed the effectiveness of the MCTM-SIoT model in predicting the trust value of each SIoT node in the SIoT network to help users select the best SP even without the node's previous behavioural history. This research contributes to the development of TM solutions for SIoT and addresses the need for reliable and secure systems in SIoT. The theoretical and simulation-based analysis of the framework further supports its potential to improve TM in SIoT environments.

Chapter 7

Conclusion and Future Work

7.1. Conclusion

Rapid advances in computer science have made it possible to integrate physical objects with computer technologies, giving them a digital identity and enabling them to communicate with their surroundings. This gave rise to the IoT paradigm, which has many positive impacts on society. However, the rise of IoT also presents some daunting challenges for researchers. One of the main challenges is heterogeneity which is a large variety of types and degrees of variation between IoT devices. Additionally, with the rapid increase in the number of devices connected to IoT networks, scalability is another important concern. Both challenges hinder autonomous communication and object-to-object interaction, limit people's access to a wide range of services of services anytime and anywhere, and impact how easily resources can be found and navigated in IoT networks.

SIoT extends the capabilities of IoT by incorporating a SN component. Within SIoT, smart objects transition into social objects capable of independently establishing relationships with other objects, participating in communities, and forming social networks, which may differ from those of their owners. In the SIoT landscape, various entities vie to promote their services, with some resorting to malicious behaviour through different types of attacks aimed at propagating low-quality services. These trust attacks pose significant risks in SIoT environments, where services can impact the physical world. TM assumes a pivotal role in furnishing automated mechanisms for determining trust among entities. Through the literature review, several frameworks emerge as relevant to SIoT. However, these frameworks are not comprehensive enough to represent the full spectrum of trust in SIoT. In addition, the existing frameworks are not considered as context awareness support trust in SIoT, which is the core contribution of this work. On the other hand, TM models in SIoT can be broadly categorised as context-based or context-free depending on whether or not the context information is included in trust calculation, trust aggregation and trust assessment. The proposed context-based TM models consider single/dual contexts in trust calculation, aggregation, sharing, and evaluation. Incorporating contextual information into TM models can significantly improve the accuracy and effectiveness of trust decisions. In addition, SIoT networks are complex and involve a significant number of nodes that interact dynamically in real-time. It is important to note that the lack of a SIoT simulator or a real SIoT dataset may limit the reliability of the TM model results. Without access to sufficient data, it may be difficult to accurately evaluate and validate the effectiveness of proposed TM frameworks or models.

Therefore, these limitations were the challenges addressed by this study and offer the following contributions:

7.1.1. Contribution 1 – MCTM-SIoT framework

In order to provide a thorough overview of SIoT, the study has looked into a variety of SIoT components, including SIoT objects (smart devices and humans), Relationship management (where objects can update a relationship status and terminate the relationship), Network navigation (where each object in the network autonomously establishes different types of relationships and uses the resulting links to navigate the network), Resource discovery (where objects interact with one another and find out what services are available on the network, similar to people searching for services in the SN), Service management (i.e., managing the services provided by the IoT Devices), and Trust management (an important aspect in providing methods for determining trust between entities based on an automated mechanism). The study aims to provide a comprehensive overview of the SIoT ecosystem and places particular attention on how different SIoT components are interconnected with one another and with TM. This is achieved by proposing a novel TM in SIoT called "MCTM-SIoT", which groups the above components into four modules: relationship selection, friendship selection and management, service search, and context-aware TM. In addition, the framework incorporates multiple contextual information into the final trust score to enable a trustworthy interface and improve the overall security and reliability of the system by helping to detect malicious behaviour. The proposed framework was evaluated mathematically, where a set of contextual trust metrics, namely UCT, DCT, ECT, and TCT, served as the basis for the MCTM-SIoT framework and experimentally, the SIoT simulator tool was designed to simulate the behaviour of SIoT systems in different SIoT contexts, thus enabling the generation of realistic SIoT data to evaluate the effectiveness of the MCTM-SIoT framework and model.

7.1.2. Contribution 2 – MCTM-SIoT model

The mathematical validation of the framework is based on the development of MCTM-SIoT model, which incorporates multiple contextual information into the final trust assessment to identify the most trustworthy service provider. This includes device status to identify security vulnerabilities and other issues that impact device reliability, environmental conditions to identify the various external factors that affect the behaviour of interconnected devices on the network, and users to use their Behaviour to determine which users are more trustworthy, and task type, to determine the reliability of the services performed by devices on the network. The proposed MCTM-SIoT model process consists of several steps including trust composition, trust aggregation, trust propagation, and trust updating. The first step is the trust composition, which consists of selecting the contextual trust metrics (UCT, TCT, DCT, ECT) based on the above contextual. The second step is trust aggregation, which focuses on node prediction by proposing an intelligent trust aggregation process that combines the selected trust indicators to produce a single trust score. Therefore, in order to achieve the goal of node prediction and intelligent trust aggregation, this study employed an ML-driven aggregation approach, particularly utilising Random Forest. This method enables the prediction of trust scores for each node within the network, while also assessing the impact of various context metrics on the final trust decision of each node. The third step is the trust propagation is based on a distributed scheme where each IoT device autonomously shares trust observations with other IoT devices that come into contact without the help of a central entity. Finally, the event-driven update trust is chosen to ensure scalability, dynamics, and resource efficiency.

7.1.3. Contribution 3 – SIoT-Sim and the generated SIoT dataset

For the experimental validation part of the framework, SIoT-Sim is designed to mimic the structures of SIoT networks, such as establishing user friendships and user registration in communities of interest (CoIs, social groups), as well as their formation of social object relationships, including POR, OOR, CWOR, SOR, and CLOR, the disconnection and abandonment of devices from the network, and the stochastic spread of malware across the network. SIoT-Sim consists of two important high-level modules including nodes and events. The node module represents each entity namely users, devices, and CoI within the simulation graph. It does not directly represent a specific node in the graph but rather provides a common set of attributes and behaviours for all entities in the diagram. The event module tracks the actions that took place during the simulation, an event class is used to store the various actions of both offline and online users, devices, CoI opening and closing, and friendship creation and suppression as a short log. In addition, SIoT-Sim is a flexible and adaptable simulator that can be adapted to various SIoT environments and applications. It includes a variety of features such as the ability to simulate different types of SIoT scenarios, as well as the ability to model different types of attacks and vulnerabilities. On the other hand, SIoT-Sim addresses the challenge of the lack of available data sets and the low quality of the data in SIoT by generating realistic SIoT data that can be used for testing and evaluation purposes. The generated SIoT dataset contains a variety of features such as social interactions between devices and users (friendships and communities of interest, social relationships), data transfers and transactions, and various event types to enable researchers to test and evaluate SIoT systems in a controlled and repeatable environment. This helps identify and remediate potential security and privacy issues as well as optimise the performance of SIoT systems. Furthermore, the performance of both the MCTM-SIoT framework and the model are evaluated.

7.1.4. Contribution 4 – Evaluation and testing MCTM-SIoT framework and model using ML techniques

To validate this approach, we conducted several comparative experiments based on three scenarios, including a low-dynamics scenario, a medium-dynamics scenario, and a high-dynamics scenario, to test the consistency of the MCTM-SIoT model in improving the accuracy of trust score predictions at different levels of network dynamics.

The experimental results show that the MCTM-SIoT model outperforms the generated SIoT dataset using the same ML algorithm called “Random Forest” in predicting the trust score. This is a notable difference, especially in a critical area such as security, where the model's ability to accurately predict trust levels between SIoT nodes directly helps identify reliable nodes for robust security measures in IoT networks. This could be supported by the way the MCTM SIoT model examines contextual SIoT trust metrics that impact an SIoT node's credibility in network communication.

On the other side, the use of features importance of the Random Forest Regressor measured the specific impact of each contextual trust metric on the trust assessment of each node in all tested network dynamics scenarios. Since node user characteristics are associated with giving feedback to friends and communities of interest and providing good intentions, UCT is by far the most important factor that ultimately influences the trust score. The device's credibility and social relationships have a significant impact on trust, making DCT the second most important factor. As the third most important factor, trust is moderately influenced by TCT, while ECT has minimal impact relative to the other metrics. Therefore, this feature importance analysis provides important insights into the contextual metrics that influence trust calculations in SIoT networks.

In summary, the MCTM-SIoT framework offers the potential to improve trust scores and predict the reliability of each SIoT node in the network. Its goal is to ensure credible communication within the SIoT network by allowing users to select the most trustworthy SP even in the absence of the prior behaviour history of the node. Therefore, the proposed framework serves as a standard for all future work in the area of TM in SIoT.

7.2. Limitations of study

This study has the potential to improve the security of SIoT systems, but there are several limitations that need to be addressed. These restrictions include: The unique use of SIoT-Sim requires further validation for generalisation and limited scalability in experimentation due to computational limitation of Google Colab Pro.

1) **The unique use of the SIoT-Sim simulator requires further validation for generalisation**: The SIoT-Sim simulation tool plays a crucial role in simulating and analysing users' and devices' behaviour in various SIoT scenarios. Its main goal is to facilitate the generation of accurate SIoT data for testing and evaluation purposes. SIoT-Sim offers the flexibility to adjust simulation parameters, enabling the creation of tailored synthetic data for specific research needs. In addition, the tool includes various functions including attack and vulnerability modelling and simulation of different device types. However, it is important to note that a limitation of the study is the unique use of the SIoT-Sim simulator to generate experimental datasets. This limitation highlights the need for further testing and validation by other researchers in the SIoT field to ensure the generalisability and robustness of the simulator. Collaborative efforts by researchers can help refine and improve the capabilities of SIoT-Sim, thereby strengthening its applicability and utility within the broader SIoT research community.

2) **Limited scalability in experimentation due to computation limitations of Google Colab Pro**: In this study, the SIoT-Sim simulator has commendable scalability and is capable of simulating a large number of users and devices. However, the maximum capacity of the experiment is limited to 300 users with 1 to 5 devices each, as aggregating contextual trust metrics proved time-consuming. This limitation arises from the computational limitations imposed by the Google Colab Pro platform, which impact the ability to calculate the trust values of each node within the SIoT network. Despite the inherent scalability of the simulator, the experimental design of the study is limited by these computational resource limitations, potentially limiting the scope and depth of analysis achievable in the simulated SIoT environment.

3) **Foundational assumptions of the MCTM-SIoT Framework:** The MCTM-SIoT framework relies on specific contextual metrics, bounding its trust assessments within these predefined indicators. If additional metrics become relevant in evolving scenarios or if security conditions change significantly, recalibration of the framework may be necessary to preserve accuracy. Furthermore, the framework's reliance on a distributed trust propagation

approach assumes devices have sufficient processing power and connectivity, limiting its applicability to environments that meet these technical conditions; in resource-constrained settings, performance may be affected. Lastly, the framework's validation on simulated data means its outcomes are generalized based on these specific scenarios, and real-world configurations that differ from the simulation may produce results that deviate from the framework's predicted performance.

7.3. Future work

MCTM-SIoT framework offers several potential directions for future research, all of which should focus on creating solutions that can successfully address the complex issues associated with TM in dynamic and heterogeneous environments. Future research could focus on the following areas:

1) **Enhancing simulation experience by designing a GUI for SIoT-Sim simulator:** The graphical user interface (GUI) of the SIoT simulator facilitates effective simulation design, increases usability, and improves the user experience. Ultimately, a well-designed GUI will improve productivity and user experience by providing simple controls, real-time data visualisation, and smooth interaction with the simulation environment. The GUI will allow users to easily configure and monitor simulations, interpret results, and make defensible decisions by integrating features such as drag-and-drop functionality, configurable dashboards, and interactive visualisation tools. In addition, a user-friendly GUI will be created to meet the unique needs of SIoT simulation, including displaying social interactions, IoT device behaviour, and network dynamics. To optimise accessibility and flexibility for users, GUI development will also focus on ensuring compatibility with different screen sizes, input devices, and operating systems. To ensure that the SIoT-Sim will work well on various devices, it is important to follow responsive design principles and conduct extensive testing across multiple platforms.

2) **addressing time constraints in aggregating contextual trust metrics:** The study found that the process of aggregating contextual trust metrics to determine the final trust score for each node in the network was excessively time-consuming. This finding indicates that the algorithms used to calculate the trust metric may have high computational complexity, resulting in longer calculation times. Therefore, it is crucial to conduct a comprehensive study of the computational properties of these algorithms to account for the observed time constraints. By gaining insights into the complexity of the algorithms and identifying areas for improvement, researchers can develop more efficient and scalable solutions for trust management within the network.

3) **Improving node trust score prediction accuracy through deep learning techniques:** While the study primarily used machine learning, it is worth considering deep learning to improve the prediction accuracy of node trust scores, as deep learning is great at automatically finding complex patterns in data. By using techniques such as deep neural networks, the complicated trust relationships within networks can be better understood, and more accurate prediction results can be achieved. So, adding deep learning could help make trust management in networks more effective and make decision-making easier.

4) **Enhancing MCTM-SIoT framework through hybrid centralised-distributed paradigm:** Improving the MCTM-SIoT framework through a hybrid centralised-distributed paradigm: To maintain a hybrid trust paradigm in SIoT networks, a centralised entity such as a cloud server can monitor nodes and distribute trust values to reduce resource consumption. In this approach, the cloud server collects and aggregates trust data from nodes, calculates trust scores, and distributes them back to the network. By centralising trust management, nodes can make informed decisions without extensive local processing, benefiting from both the reliability of centralised systems and the distributed nature of SIoT networks. This hybrid model optimises resource utilisation while ensuring robust trust relationships, improving network stability and performance.

References

Aalibagi, S. et al. (2021) 'A matrix factorization model for Hellinger-Based trust management in social internet of things,' IEEE Transactions on Dependable and Secure Computing, 19(4), pp. 2274–2285. https://doi.org/10.1109/tdsc.2021.3052953.

Abdelghani, W. et al. (2016) 'Trust Management in Social Internet of Things: A survey,' in Lecture Notes in Computer Science, pp. 430–441. https://doi.org/10.1007/978-3-319-45234-0_39.

Abderrahim, O.B., Elhdhili, M.H. and Saïdane, L.A. (2017a) TMCOI-SIOT: A trust management system based on communities of interest for the social internet of things, 13th international wireless communications and mobile computing conference. https://doi.org/10.1109/iwcmc.2017.7986378.

Abderrahim, O.B., Elhedhili, M.H. and Saïdane, L.A. (2017) 'CTMS-SIOT: A context-based trust management system for the social Internet of Things,' 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1903–1908. https://doi.org/10.1109/iwcmc.2017.7986574.

Ahmed, A.I.A. et al. (2023) 'Formal analysis of trust and reputation for service composition in IoT,' Sensors, 23(6), p. 3192. https://doi.org/10.3390/s23063192.

Alam, S. et al. (2022) 'Trust Management in Social Internet of Things (SIOT): a survey,' IEEE Access, 10, pp. 108924–108954. https://doi.org/10.1109/access.2022.3213699.

Alam, S., Zardari, S. and Shamsi, J.A. (2022) 'Blockchain-Based trust and reputation Management in SIoT,' Electronics, 11(23), p. 3871. https://doi.org/10.3390/electronics11233871.

Alghofaili, Y. and Rassam, M.A. (2022) 'A trust management model for IoT devices and services based on the Multi-Criteria Decision-Making approach and Deep Long

Short-Term memory technique,' Sensors, 22(2), p. 634. https://doi.org/10.3390/s22020634.

Ali, S. et al. (2018) 'A model of socially connected web objects for IoT applications,' Wireless Communications and Mobile Computing, 2018, pp. 1–20. https://doi.org/10.1155/2018/6309509.

Aljubairy, A. et al. (2020) 'SIoTPredict: A framework for predicting relationships in the social internet of Things,' in Lecture Notes in Computer Science, pp. 101–116. https://doi.org/10.1007/978-3-030-49435-3_7.

Amin, F., Ahmad, A. and Choi, G.S. (2019) 'Towards trust and friendliness approaches in the social internet of things,' Applied Sciences, 9(1), p. 166. https://doi.org/10.3390/app9010166.

Aoudia, I. et al. (2019) 'Service composition approaches for Internet of Things: a review,' International Journal of Communication Networks and Distributed Systems, 23(1), p. 1. https://doi.org/10.1504/ijcnds.2019.10017271.

Aslam, M.J. et al. (2020) 'Defining Service-Oriented trust assessment for social internet of things,' IEEE Access, 8, pp. 206459–206473. https://doi.org/10.1109/access.2020.3037372.

Atzori, L. et al. (2012) 'The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization,' Computer Networks, 56(16), pp. 3594–3608. https://doi.org/10.1016/j.comnet.2012.07.010.

Atzori, L., Iera, A. and Morabito, G. (2010) 'The Internet of Things: A survey,' Computer Networks, 54(15), pp. 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010.

Atzori, L., Iera, A. and Morabito, G. (2011) 'SIOT: giving a social structure to the internet of things,' IEEE Communications Letters, 15(11), pp. 1193–1195. https://doi.org/10.1109/lcomm.2011.090911.111340.

Atzori, L., Iera, A. and Morabito, G. (2014) 'From ‘smart objects’ to ‘social objects’: The next evolutionary step of the internet of things,' IEEE Communications Magazine, 52(1), pp. 97–105. https://doi.org/10.1109/mcom.2014.6710070.

Azad, M.A. et al. (2020) 'Decentralized Self-Enforcing Trust Management System for social Internet of things,' IEEE Internet of Things Journal, 7(4), pp. 2690–2703. https://doi.org/10.1109/jiot.2019.2962282.

Bahutair, M., Bouguettaya, A. and Neiat, A.G. (2022) 'Multi-Perspective Trust Management framework for crowdsourced IoT services,' IEEE Transactions on Services Computing, 15(4), pp. 2396–2409. https://doi.org/10.1109/tsc.2021.3052219.

Bao, F. and Chen, I.-R. (2012) Trust management for the internet of things and its application to service composition, IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM). https://doi.org/10.1109/wowmom.2012.6263792.

Cai, Z. et al. (2016) 'Collective Data-Sanitization for preventing sensitive information inference attacks in social networks,' IEEE Transactions on Dependable and Secure Computing, p. 1. https://doi.org/10.1109/tdsc.2016.2613521.

Caminha, J., Perkusich, A. and Perkusich, M. (2018) 'A smart trust management method to detect On-Off attacks in the internet of things,' Security and Communication Networks, 2018, pp. 1–10. https://doi.org/10.1155/2018/6063456.

Campanile, L. et al. (2020) 'Computer Network Simulation with ns-3: A Systematic Literature Review,' Electronics, 9(2), p. 272. https://doi.org/10.3390/electronics9020272.

Chahal, R.K., Kumar, N. and Batra, S. (2020) 'Trust management in social Internet of Things: A taxonomy, open issues, and challenges,' Computer Communications, 150, pp. 13–46. https://doi.org/10.1016/j.comcom.2019.10.034.

Chen, I.-R., Bao, F. and Guo, J. (2016) 'Trust-Based service management for social internet of things systems,' IEEE Transactions on Dependable and Secure Computing, 13(6), pp. 684–696. https://doi.org/10.1109/tdsc.2015.2420552.

Chen, I.-R., Guo, J. and Bao, F. (2016) 'Trust Management for SOA-Based IoT and its application to service composition,' IEEE Transactions on Services Computing, 9(3), pp. 482–495. https://doi.org/10.1109/tsc.2014.2365797.

Chernyshev, M. et al. (2018) 'Internet of Things (IoT): research, simulators, and testbeds,' IEEE Internet of Things Journal, 5(3), pp. 1637–1647. https://doi.org/10.1109/jiot.2017.2786639.

Cohen, L., Manion, L. and Morrison, K. (2017) Research methods in education. Routledge.

Da Xu, L., He, W. and Li, S. (2014) 'Internet of Things in Industries: A survey,' IEEE Transactions on Industrial Informatics, 10(4), pp. 2233–2243. https://doi.org/10.1109/tii.2014.2300753.

De Matos, É. et al. (2015) Context-aware system for information services provision in the Internet of Things. 20th ed, IEEE Conference on Emerging Technologies & Factory Automation (ETFA). https://doi.org/10.1109/etfa.2015.7301624.

De Matos, É., Amaral, L.A. and Hessel, F. (2017) 'Context-Aware Systems: Technologies and challenges in Internet of everything environments,' in Internet of things, pp. 1–25. https://doi.org/10.1007/978-3-319-50758-3_1.

Defiebre, D., Germanakos, P. and Sacharidis, D. (2020) DANOS: A Human-Centered Decentralized Simulator in SIOT. 28th ed, ACM Conference on User Modeling, Adaptation and Personalization. https://doi.org/10.1145/3386392.3399292.

Deshpande, P. et al. (2015) M4M: A model for enabling social network-based sharing in the Internet of Things. 7th ed, International Conference on Communication Systems and Networks (COMSNETS). https://doi.org/10.1109/comsnets.2015.7098685.

Domingo, M.C. (2012a) 'An overview of the Internet of Things for people with disabilities,' Journal of Network and Computer Applications, 35(2), pp. 584–596. https://doi.org/10.1016/j.jnca.2011.10.015.

Durap, A. (2023). A comparative analysis of machine learning algorithms for predicting wave runup. Anthropocene Coasts, 6(1). https://doi.org/10.1007/s44218-023-00033-7

Eddy, B and Oussama, H (eds) (2018) Social Relationship Paradigm applied to object interactions in industrial IoT, IFAC-PapersOnLine, 51(11).

Elgazzar, K. et al. (2022) 'Revisiting the internet of things: New trends, opportunities and grand challenges,' Frontiers in the Internet of Things, 1. https://doi.org/10.3389/friot.2022.1073780.

Fan, X. et al. (2019) 'Decentralized Trust Management: risk analysis and trust aggregation,' arXiv (Cornell University) [Preprint]. https://doi.org/10.48550/arxiv.1909.11355.

Farhadi, B. et al. (2021) 'Friendship selection and management in social internet of things: A systematic review,' Computer Networks, 201, p. 108568. https://doi.org/10.1016/j.comnet.2021.108568.

Ferrag, M.A. et al. (2019) 'Blockchain Technologies for the Internet of Things: Research issues and challenges,' IEEE Internet of Things Journal, 6(2), pp. 2188–2204. https://doi.org/10.1109/jiot.2018.2882794.

Fortino, G. et al. (2020) 'Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges,' IEEE Access, 8, pp. 60117–60125. https://doi.org/10.1109/access.2020.2982318.

Gazi, S.M., Arko, S.R., Gomes, E.L. and Bin Shahid, A (2021) Developing a SIOT compatible novel traffic simulator to evaluate and execute complex SIOT based algorithms in typical road traffic scenarios. Doctoral dissertation. Brac University.

Guinard, D., Fischer, M. and Trifa, V. (2010) Sharing using social networks in a composable web of things. 8th ed, IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). https://doi.org/10.1109/percomw.2010.5470524.

Guo, J. and Chen, I.-R. (2015) A classification of trust computation models for Service-Oriented Internet of Things Systems, IEEE International Conference on Services Computing. https://doi.org/10.1109/scc.2015.52.

Hamad, S.A. et al. (2020) 'Realizing an Internet of Secure Things: A survey on issues and enabling technologies,' IEEE Communications Surveys and Tutorials, 22(2), pp. 1372–1391. https://doi.org/10.1109/comst.2020.2976075.

Hamadi, H.A. and Chen, I.R. (2017) 'Trust-Based decision making for health IoT systems,' IEEE Internet of Things Journal, 4(5), pp. 1408–1419. https://doi.org/10.1109/jiot.2017.2736446.

Hamrouni, A., Ghazzai, H. and Massoud, Y. (2022) 'Service Discovery in Social Internet of Things using Graph Neural Networks,' 2022 IEEE 65th International Midwest Symposium on Circuits and Systems (MWSCAS) [Preprint]. https://doi.org/10.1109/mwscas54063.2022.9859333.

Hassan, R. et al. (2020) 'Internet of Things and its Applications: A Comprehensive survey,' Symmetry, 12(10), p. 1674. https://doi.org/10.3390/sym12101674.

Henderson, T.R., Lacage, M., Riley, G.F., Dowell, C. and Kopena, J (2003) Network simulations with the NS-3 simulator, SIGCOMM demonstration, 14(14).

Holmquist, L.E. et al. (2001) 'Smart-Its Friends: A Technique for Users to Easily Establish Connections between Smart Artefacts,' in Lecture Notes in Computer Science, pp. 116–122. https://doi.org/10.1007/3-540-45427-6_10.

Hussain, F. et al. (2020) 'Machine learning in IoT Security: current solutions and future challenges,' IEEE Communications Surveys and Tutorials, 22(3), pp. 1686–1721. https://doi.org/10.1109/comst.2020.2986444.

Hussein, D. et al. (2017) 'Towards a dynamic discovery of smart services in the social internet of things,' Computers & Electrical Engineering, 58, pp. 429–443. https://doi.org/10.1016/j.compeleceng.2016.12.008.

Jaiswal, J. and Samikannu, R. (2017) Application of Random Forest Algorithm on Feature Subset Selection and Classification and Regression, world congress on computing and communication technologies (WCCCT). https://doi.org/10.1109/wccct.2016.25.

Kashani, M.H. et al. (2021) 'A systematic review of IoT in healthcare: Applications, techniques, and trends,' Journal of Network and Computer Applications, 192, p. 103164. https://doi.org/10.1016/j.jnca.2021.103164.

Kasnesis, P. et al. (2016) ASSIST: An agent-based SIoT simulator. 3rd ed, World Forum on Internet of Things (WF-IoT). https://doi.org/10.1109/wf-iot.2016.7845409.

Khalil, K. et al. (2020) 'Resource discovery techniques in the internet of things: A review,' Internet of Things, 12, p. 100293. https://doi.org/10.1016/j.iot.2020.100293.

Khan, W.Z. et al. (2020) 'Trust management in social Internet of Things: architectures, recent advancements, and future challenges,' IEEE Internet of Things Journal, 8(10), pp. 7768–7788. https://doi.org/10.1109/jiot.2020.3039296.

Khanfor, A. et al. (2020) Automated Service Discovery for Social Internet-of-Things Systems, IEEE International Symposium on Circuits and Systems (ISCAS). https://doi.org/10.1109/iscas45731.2020.9181080.

Khani, M. et al. (2018) 'Context-Aware trustworthy service evaluation in social internet of things,' in Lecture Notes in Computer Science, pp. 129–145. https://doi.org/10.1007/978-3-030-03596-9_9.

Kamel, M. B. M., Yan, Y., Ligeti, P., & Reich, C. (2021). ATTRED: Attribute Based Resource Discovery for IoT. Sensors, 21(14), 4721. https://doi.org/10.3390/s21144721

Khelloufi, A. et al. (2023) 'Context-Aware Service recommendation system for the social internet of things,' arXiv (Cornell University) [Preprint]. https://doi.org/10.48550/arxiv.2308.08499.

Kleinberg, J. (2000) The small-world phenomenon, In Proceedings of the thirty-second annual ACM symposium on Theory of computing. https://doi.org/10.1145/335305.335325.

Kowshalya, A.M. and Valarmathi, M.L. (2015) Improved network navigability and service search in social internet of things (SIoT), International Journal of Research and Scientific Innovation, 2(9).

Muhammad Kowshalya, A.M. and Valarmathi, M.L. (2017) 'Trust management for reliable decision making among social objects in the Social Internet of Things,' IET Networks, 6(4), pp. 75–80. https://doi.org/10.1049/iet-net.2017.0021.

Kuseh, S.W. et al. (2022) 'A survey of trust management schemes for social internet of things,' Journal Inform, 7(1), pp. 48–58. https://doi.org/10.25139/inform.v7i1.4567.

Li, W., Song, H. and Zeng, F. (2018) 'Policy-Based secure and trustworthy sensing for internet of things in smart cities,' IEEE Internet of Things Journal, 5(2), pp. 716–723. https://doi.org/10.1109/jiot.2017.2720635.

Li, X. et al. (2015) 'Context Aware Middleware Architectures: Survey and challenges,' Sensors, 15(8), pp. 20570–20607. https://doi.org/10.3390/s150820570.

Li, Z. et al. (2016) 'Dynamic resource discovery based on preference and movement pattern similarity for Large-Scale Social Internet of Things,' IEEE Internet of Things Journal, 3(4), pp. 581–589. https://doi.org/10.1109/jiot.2015.2451138.

Lin, J. et al. (2017) 'A survey on Internet of things: architecture, enabling technologies, security and privacy, and applications,' IEEE Internet of Things Journal, 4(5), pp. 1125–1142. https://doi.org/10.1109/jiot.2017.2683200.

Lin, Z. and Dong, L. (2018) 'Clarifying trust in social internet of things,' IEEE Transactions on Knowledge and Data Engineering, 30(2), pp. 234–248. https://doi.org/10.1109/tkde.2017.2762678.

Liu, M. et al. (2014) 'Evaluating total inorganic nitrogen in coastal waters through fusion of multi-temporal RADARSAT-2 and optical imagery using random forest algorithm,' International Journal of Applied Earth Observation and Geoinformation, 33 ed, pp. 192–202. https://doi.org/10.1016/j.jag.2014.05.009.

Liu, Q. et al. (2013) 'A SURVEY OF CONTEXT-AWARE MOBILE RECOMMENDATIONS,' International Journal of Information Technology and Decision Making, 12(01), pp. 139–172. https://doi.org/10.1142/s0219622013500077.

Magdich, R., Jemal, H. and Ayed, M.B. (2022) 'A resilient Trust Management framework towards trust related attacks in the Social Internet of Things,' Computer Communications, 191, pp. 92–107. https://doi.org/10.1016/j.comcom.2022.04.019.

Magdich, R., Jemal, H. and Ayed, M.B. (2022a) 'Context-awareness trust management model for trustworthy communications in the social Internet of Things,' Neural Computing and Applications, 34(24), pp. 21961–21986. https://doi.org/10.1007/s00521-022-07656-w.

Marche, C. et al. (2020) 'How to exploit the Social Internet of Things: Query Generation Model and Device Profiles' Dataset,' Computer Networks, 174, p. 107248. https://doi.org/10.1016/j.comnet.2020.107248.

Marche, C. and Nitti, M. (2021) 'Trust-Related Attacks and their Detection: A trust management model for the social IoT,' IEEE Transactions on Network and Service Management, 18(3), pp. 3297–3308. https://doi.org/10.1109/tnsm.2020.3046906.

Mei, A. and Stefa, J. (2009) SWIM: A Simple Model to Generate Small Mobile Worlds, IEEE INFOCOM 2009. https://doi.org/10.1109/infcom.2009.5062134.

Muhammad, S. et al. (2023) 'Honesty-Based social technique to enhance cooperation in social internet of things,' Applied Sciences, 13(5), p. 2778. https://doi.org/10.3390/app13052778.

Narang, N.K. and Kar, S. (2021) 'A hybrid trust management framework for a multi-service social IoT network,' Computer Communications, 171, pp. 61–79. https://doi.org/10.1016/j.comcom.2021.02.015.

Nie, L. et al. (2022) 'Intrusion detection for secure social internet of things based on collaborative edge computing: a generative adversarial Network-Based approach,' IEEE Transactions on Computational Social Systems, 9(1), pp. 134–145. https://doi.org/10.1109/tcss.2021.3063538.

Ning, H. and Wang, Z. (2011) 'Future internet of things architecture: like mankind neural system or social organization framework? IEEE Communications Letters, 15(4), pp. 461–463. https://doi.org/10.1109/lcomm.2011.022411.110120.

Nitti, M. et al. (2012) A subjective model for trustworthiness evaluation in the social Internet of Things. 23rd ed, IEEE international symposium on personal, indoor and mobile radio communications-(PIMRC). https://doi.org/10.1109/pimrc.2012.6362662.

Nitti, M. et al. (2016) 'Exploiting social internet of things features in cognitive radio,' IEEE Access, 4, pp. 9204–9212. https://doi.org/10.1109/access.2016.2645979.

Nitti, M., Atzori, L. and Cvijikj, I.P. (2014) Network navigability in the social Internet of Things, 2014 IEEE world forum on internet of things (WF-IoT). https://doi.org/10.1109/wf-iot.2014.6803200.

Nitti, M., Atzori, L. and Cvijikj, I.P. (2015) 'Friendship selection in the social Internet of Things: Challenges and possible strategies,' IEEE Internet of Things Journal, 2(3), pp. 240–247. https://doi.org/10.1109/jiot.2014.2384734.

Nitti, M., Girau, R. and Atzori, L. (2014) 'Trustworthiness management in the social internet of things,' IEEE Transactions on Knowledge and Data Engineering, 26(5), pp. 1253–1266. https://doi.org/10.1109/tkde.2013.105.

Nitti, M., Pilloni, V. and Giusto, D.D. (2016) Searching the social internet of things by exploiting object similarity. 3rd ed, IEEE World Forum on Internet of Things (WF-IoT). https://doi.org/10.1109/wf-iot.2016.7845506.

Ojie, E. and Pereira, E (ed.) (2017) Simulation Tools in Internet of Things: a review. 1st ed, In Proceedings of the international conference on internet of things and machine learning.

Österlind, F. (2006) A Sensor Network Simulator for the Contiki OS, Swedish Institute of Computer Science. https://eprints.sics.se/2296/.

Perera, C. et al. (2014) 'Context Aware Computing for the Internet of Things: A survey,' IEEE Communications Surveys and Tutorials, 16(1), pp. 414–454. https://doi.org/10.1109/surv.2013.042313.00197.

Punch, K.F. and Oancea, A. (2014) Introduction to research methods in education. SAGE.

Rad, M.M. et al. (2020) 'Social Internet of Things: vision, challenges, and trends,' Human-centric Computing and Information Sciences, 10(1). https://doi.org/10.1186/s13673-020-00254-6.

Rad, M.M. et al. (2023) 'Community detection and service discovery on Social Internet of Things,' International Journal of Communication Systems, 36(11). https://doi.org/10.1002/dac.5501.

Richardson, M., Agrawal, R. and Domingos, P. (2003) 'Trust management for the semantic web,' in Lecture Notes in Computer Science, pp. 351–368. https://doi.org/10.1007/978-3-540-39718-2_23.

Rizwanullah, M. et al. (2022) 'Development of a model for trust management in the social internet of things,' Electronics, 12(1), p. 41. https://doi.org/10.3390/electronics12010041.

Ruggeri, G. and Briante, O. (2017) A framework for IoT and E-Health systems integration based on the social Internet of Things paradigm, In 2017 international symposium on wireless communication systems (ISWCS). https://doi.org/10.1109/iswcs.2017.8108152.

Sagar, S., Mahmood, A., Sheng, Q.Z., Zaib, M., et al. (2020) Towards a Machine Learning-driven Trust Evaluation Model for Social Internet of Things: A Time-aware Approach, In MobiQuitous 2020-17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. https://doi.org/10.1145/3448891.3448927.

Sagar, S., Mahmood, A., Sheng, Q.Z. and Zhang, W.E. (2020) Trust Computational Heuristic for Social Internet of Things: A Machine Learning-based Approach, In ICC 2020-2020 IEEE International Conference on Communications (ICC). https://doi.org/10.1109/icc40277.2020.9148767.

Sagar, S. et al. (2022) 'Trust-SIOT: towards trustworthy object classification in the social internet of things,' arXiv (Cornell University) [Preprint]. https://doi.org/10.48550/arxiv.2205.03226.

Sagar, S. et al. (2023) 'Understanding the trustworthiness management in the social internet of Things: a survey,' arXiv Preprint arXiv:2202.03624 [Preprint]. https://doi.org/10.2139/ssrn.4629067.

Saranya, T. et al. (2020) 'Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: a review,' Procedia Computer Science, 171, pp. 1251–1260. https://doi.org/10.1016/j.procs.2020.04.133.

Schilit, B.N., Adams, N.I. and Want, R. (1994) Context-Aware computing applications. 1st ed, first workshop on mobile computing systems and applications IEEE. https://doi.org/10.1109/wmcsa.1994.16.

Shammar, E.A. and Zahary, A. (2020) 'The Internet of Things (IoT): a survey of techniques, operating systems, and trends,' Library Hi Tech, 38(1), pp. 5–66. https://doi.org/10.1108/lht-12-2018-0200.

Sezer, Ö.B., Doğdu, E. and Özbayoğlu, A.M. (2018) 'Context-Aware Computing, Learning, and Big Data in Internet of Things: A survey,' IEEE Internet of Things Journal, 5(1), pp. 1–27. https://doi.org/10.1109/jiot.2017.2773600.

Sisinni, E. et al. (2018) 'Industrial Internet of Things: challenges, opportunities, and directions,' IEEE Transactions on Industrial Informatics, 14(11), pp. 4724–4734. https://doi.org/10.1109/tii.2018.2852491.

Truong, N.B., Um, T.-W., et al. (2017a) From Personal Experience to Global Reputation for Trust Evaluation in the Social Internet of Things, In GLOBECOM 2017-2017 IEEE Global Communications Conference. https://doi.org/10.1109/glocom.2017.8254523.

Truong, N.B., Lee, H., et al. (2017) 'Toward a trust evaluation mechanism in the social internet of things,' Sensors, 17(6), p. 1346. https://doi.org/10.3390/s17061346.

Um, T.-W. et al. (2019) 'Design and implementation of a trust Information Management Platform for social Internet of things environments,' Sensors, 19(21), p. 4707. https://doi.org/10.3390/s19214707.

Ureña, R. et al. (2019) 'A review on trust propagation and opinion dynamics in social networks and group decision making frameworks,' Information Sciences, 478, pp. 461–475. https://doi.org/10.1016/j.ins.2018.11.037.

Van Der Merwe, A., Gerber, A. and Smuts, H. (2017) 'Mapping a design science research cycle to the postgraduate research report,' in Communications in computer and information science, pp. 293–308. https://doi.org/10.1007/978-3-319-69670-6_21.

Varga, A. and Hornig, R. (2008) AN OVERVIEW OF THE OMNeT++ SIMULATION ENVIRONMENT. 1st ed, In International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems. https://doi.org/10.4108/icst.simutools2008.3027.

Wang, Y., Li, L. and Liu, G. (2013) 'Social context-aware trust inference for trust enhancement in social network-based recommendations on service providers,' World Wide Web, 18(1), pp. 159–184. https://doi.org/10.1007/s11280-013-0241-5.

Wei, D. et al. (2018) 'Social relationship for physical objects,' International Journal of Distributed Sensor Networks, 14(1), p. 155014771875496. https://doi.org/10.1177/1550147718754968.

Wei, L. et al. (2021) 'On designing Context-Aware Trust model and service delegation for social Internet of things,' IEEE Internet of Things Journal, 8(6), pp. 4775–4787. https://doi.org/10.1109/jiot.2020.3028380.

Wei, L., Wu, J. and Long, C. (2020) 'Enhancing Trust Management via Blockchain in Social Internet of Things,' In 2020 Chinese Automation Congress (CAC), 159–164. https://doi.org/10.1109/cac51589.2020.9326856.

Xia, H. et al. (2019) Trustworthiness Inference Framework in the Social Internet of Things: A Context-Aware Approach, In IEEE INFOCOM 2019-IEEE Conference on Computer Communications. https://doi.org/10.1109/infocom.2019.8737491.

Zhang, H. et al. (2023) 'Smart object recommendation based on topic learning and joint features in the social internet of things,' Digital Communications and Networks, 9(1), pp. 22–32. https://doi.org/10.1016/j.dcan.2022.04.025.

Zhang, Y., Wen, J. and Fan, M. (2014) The application of internet of things in social network. 38th, In 2014 IEEE International Computer Software and Applications Conference Workshops. https://doi.org/10.1109/compsacw.2014.41.

Zheng, A. (2015) Evaluating machine learning models: A Beginner's Guide to Key Concepts and Pitfalls.

Zelaya, C.V.G. (2019) Towards explaining the effects of data preprocessing on machine learning. 35th ed, IEEE international conference on data engineering (ICDE). https://doi.org/10.1109/icde.2019.00245.