ENHANCED TRUST MANAGEMENT MODEL FOR IOT AND SOCIAL IOT

A Thesis submitted

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY
IN
COMPUTER APPLICATIONS

By

GEETHA V
17SCSE301037

Supervisor

Dr. AVADHESH KUMAR
Professor

SCHOOL OF COMPUTING SCIENCE & ENGINEERING
GALGOTIAS UNIVERSITY
Plot No 2, Sector 17-A Yamuna Expressway
Greater Noida, Uttar Pradesh
INDIA

JANUARY, 2022

CANDIDATE DECLARATION

I hereby certify that the work which is being presented in the thesis, entitled "**ENHANCED TRUST MANAGEMENT MODEL FOR IOT AND SOCIAL IOT**" in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Faculty of Computer Science and Engineering and submitted in Galgotias University, Uttar Pradesh is an authentic record of my own work carried out during a period from march 2018 under the supervision of **Dr. AVADHESH KUMAR**, Professor, School of Computing Science and Engineering, Galgotias University.

The matter embodied in this thesis has not been submitted by me for the award of any other degree or from any other University/Institute.

GEETHA V
17SCSE301037

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

Dr. AVADHESH KUMAR
Supervisor
SCSE

School of Computing Science & Engineering
Galgotias University

CERTIFICATE

This is to certify that **Ms. GEETHA V (Reg. No.17SCSE301037)** has presented her pre-submission seminar of the thesis entitled **"ENHANCED TRUST MANAGEMENT MODEL FOR IOT AND SOCIAL IOT"** before the committee and summary is approved and forwarded to School Research Committee of Computing Science & Engineering, in the Faculty of Engineering & Technology, Galgotias University, Uttar Pradesh.

Dean – SCSE Dean – PhD & PG

The Ph.D. Viva-Voice examination of **GEETHA V** Research Scholar, has been held on _____

Supervisor External Examiner

APPROVAL SHEET

This thesis/dissertation/report entitled "**ENHANCED TRUST MANAGEMENT MODEL FOR IOT AND SOCIAL IOT"** by **GEETHA V** is approved for the degree of Doctor of Philosophy.

Examiner Supervisor Chairman

ACKNOWLEDGEMENT

The author is very grateful to GOD ALMIGHTY for without His graces and blessings, this work would not have been possible.

Pursuing a Ph.D work is a both excruciating and pleasurable experience. It's just like mountaineering a high peak, gradually, accompanied with acrimony, destitutions, frustration, encouragement and trust and with so many people's kind help. When I found myself at the top enjoying the beautiful scenery, I realized that it was, in fact, teamwork that got me there. Though it will not be enough to express my gratitude in words to all those people who helped me, I would still like to give my many thanks to all these people.

I must owe a special debt of gratitude to Hon'ble Chancellor Mr. Suneel Galgtotia, Mr. Dhruv Galgotia, CEO and Hon'ble Vice-Chancellor Dr. Preeti Bajaj, Galgotias University for their valuable support throughout my research work.

I would first like to thank my thesis advisor Prof. (Dr.) Avadhesh Kumar, Pro Vice Chancellor, Galgotias University. Dr. Avadhesh was always there whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this thesis to be my own work, but steered me in the right the direction whenever he thought I needed it.

I express my sincere thanks to Dr. Munish Sabharwal, Dean School of Computing Science & Engineering and Dr. Naresh Kumar, Dean PG & PhD for their guidance and moral support during my research work and all faculties of School of Computing Science & Engineering who helped me a lot in my course of research work and all those who stood behind me.

I would like to thank the experts who were involved in the validation survey for this research work. Without their passionate participation and input, the validation survey would not have been successfully conducted. And I am grateful to Dr. K. Sampath Kumar for his very valuable comments on this thesis. I would like to thank Dr. Balamurugan for navigating my interest in to this research work at pre-registration stage.

I have been fortunate to have many friends who cherish me despite my eccentricities. I risk doing them a disservice by not mentioning all of them here, but plead paucity of space. I would like to thank all my friends and relatives who were supporting me unconditionally all these years for me to achieve whatever little I have done so far.

Words and sentences are not enough to thank the parents, but still I express my very profound gratitude to my parents Pramila and Venkatesan for all the unconditional love and the amazing chances they've given me over the years. I would like to thank my in-laws as well for their immense support,

Finally, yet importantly, I am greatly indebted to my devoted husband Jeevanandam and our responsible sons Ritvik and Mytresh. They form the backbone and origin of my happiness. Their love and support without any complaint or regret has enabled me to complete this Ph.D work. I owe my every achievement to them.

GEETHA V

ABSTRACT

The Internet of Things (IoT) is a system that allows things to detect and collect essential data from the surrounding world and then exchange that information via the internet; the collected information can be analyzed and used for a range of purposes. The IoT is an innovative way of thinking that has transformed traditional lifestyles into high-tech ones. Smart cities, smart homes, environmental management, energy conservation, smart transportation, and smart industries are examples of IoT-driven developments. Many interesting research works and studies have been conducted to improve technology via IoT.

IoT offers a consistent platform for people to engage with various physical andvirtual objects, with adapted medical fields. The difficulty of access to health services,the growing geriatric people with chronic illness and their need for surveillance, rising medical expenditures, and telemedicine in underdeveloped nations make the IoT is an interesting topic in healthcare. In terms of mobile health and clinical decision support, IoT technology offers a professional and disciplined method to handling service delivery components of healthcare. This research considers a patient monitoring service and proposes a trust level computation model based on trust properties.

In addition to the many advantages of the Internet of Things, its variability poses a new difficulty in creating a trusted environment between objects due to the lack of proper procedural safeguards. Furthermore, it is clear that these talks are frequently focused only on the security and privacy concern involved. Standard network safety precautions, on the other hand, are insufficient to verify the consistency of data transfers and online services. Thus, it remains vulnerable to threats ranging from the risk of data management in the cyber-physical components, to the potential discrimination in social structures. Trust in IoT can be considered as an important aspect to enforce trust among objects to ensure reliable services. Generally, trust revolves around assurance and confidence that individuals, data, organizations, information, or processes will operate in the expected ways. Furthermore, forcing trust in a society built on the IoT is challenging since things lack the authority of inherited risk evaluations and other characteristics that influence the dependability test

that people conduct. As a result, it's critical to balance the concept of trust in a way that artificial manufactures can understand. Trust is defined as a computerised description of the interaction between a supervisor and a trustee, defined in a specific context, quantified in trust metrics, and machine-tested in computer science.

The trust concept plays an important role in IoT that supports individuals and services to conquer the discernment of uncertainty and threat prior to making adecision. The value of confidence can be used to detect malicious, selfish, faulty and trustiness of nodes in IoT networks. In order to compute the trust value of each node in the IoT network, this research proposes a trust evaluation algorithm for finding node trustworthy. This algorithm uses a mathematical model to compute numeric trust value for each node based on the success, completeness, data quality and reward rate of sensed information.

The Social IoT (SIoT) is a network involving heterogeneous entities like a human, devices referred to as things that are connected with social relationships. Every individual thing has its own id, functional property, limited storage and capacity. Each one expects to establish trusted communication with other reliable entities in the IoT network, which cover the essential of Trust Management System (TMS). This research work proposes an adaptive trust management design that performs trust assessment considering both QoS and Social parameters for deciding the trustiness of a node in the IoT network. The design uses direct assessment and indirect recommendation, which are aggregated using a dynamic weighted method. The decay factor for the past experiences and dynamic updating of the trust profiles enhances the system performances. It compared with static, distributed, social and single trust types of systems with respect to resiliency and performance. The performance of the proposed work shows a very efficient trust assessment and increases the performance. The simulation testing is performed to assess the performance of the proposed trust level computation model. The simulation result indicates that the proposed trust computation model is an efficient model.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ANFIS	-	Adaptive Neuro-Fuzzy Inference System
AAL	-	Ambient Assisted Living
AATMS	-	Anti-Attack Trust Management System
CoI	-	Community-of-Interest
DIT	-	Decentralized Interoperable Trust
DST	-	Dempster–Shafer Theory
HMAC	-	Hash Message Authentication Code
ITIS	-	Indirect Trust Inference System
IoHT	-	Internet of Health Things
IoMT	-	Internet of Medical Things
IoT	-	Internet of Things
MANET	-	Mobile Ad Hoc Network
MSIoTs	-	Mobile Social Internet of Things
POR	-	Parental Object Relationship
PSO		Particle Swarm Optimization
P2P	-	Peer-to-Peer
RBAC	-	Role-based Access Control
SIoT	-	Social Internet of Things
SNS	-	Social Network Science
SDN	-	Software-Defined Networking

TMHC	-	Trust Management Hybrid Cryptography
TMM	-	Trust Management Model
QoS	-	Quality of Service
WSN	-	Wireless Sensor Network

LIST OF PUBLICATIONS

1. Geetha Venkatesan, Avadhesh Kumar (2021), "Trust level computational model for IoT enabled patient monitoring service using Trust properties", Journal of Design Engineering, vol-2021 Issue 07, pp 1299 – 1315. (SCOPUS)

2. Geetha Venkatesan, Avadhesh Kumar (2021), "Enhanced adaptive trust management system for socially related IoT", Journal of Inderscience, vol 11, issue 5-6, pp 584- 596 (SCOPUS)

3. Geetha Venkatesan, Avadhesh Kumar (2021) "Dynamic Trust Management System for Social IoT". In: Zhang YD., Senjyu T., So-In C., Joshi A. (eds) Smart Trends in Computing and Communications. Lecture Notes in Networks and Systems, vol 286. Springer, Singapore. https://doi.org/10.1007/978-981-16-4016-2_50. (SPRINGER CONFERENCE)

4. Geetha Venkatesan, Avadhesh Kumar (2021) "Reliable data acquisition by master slave approach in Marine-IoT environment for logistics" 3rd International Conference on mobile computing and sustainable informatics (ICMCSI 2022), Springer Conference. Got Acceptance. Yet to be present.

CHAPTER – I

INTRODUCTION

1.1 Overview

The Internet of Things (IoT) is a future innovation of communications systems and service architecture that allows the real world to be more integrated into computer-based methods. As a significant amount of devices get associated and things become smarter, a social strategy to the IoT interaction paradigm is required (Ortiz et al., 2014). The objects in a social IoT are able of forming a community relationship among others. Inter-object connections take place in the community network of things. During the IoT design process, the social interactions between owners and customers are considered (Chen et al., 2016a). In the social IoT, objects act as independent mediators, requesting and providing data and services while keeping their uniqueness.

The new "social" paradigm, incorporated into the IoT (Social IoT - SIoT) concept, entails applying a social hierarchy to factors by describing natural social ties to the digital world. Data analytics becomes critical for enabling trustworthy and secure data communication. SIoT is dependent on Social Network Science (SNS) views to improve system accessibility and knowledge discovery in the IoT. SIoT enables things to form community relations with one another depending on rules established by their owner. Scalability and effective network navigation are both possible with this paradigm. A friend of a node is a node with whom it has some type of social relationship. Friendships and friends-of-friends concepts are borrowed from a social network. SIoT reuses the communicative networking theories to solve issues correlated, including IoT. Figure 1.1 depicts a graphic representation of the SIoT.

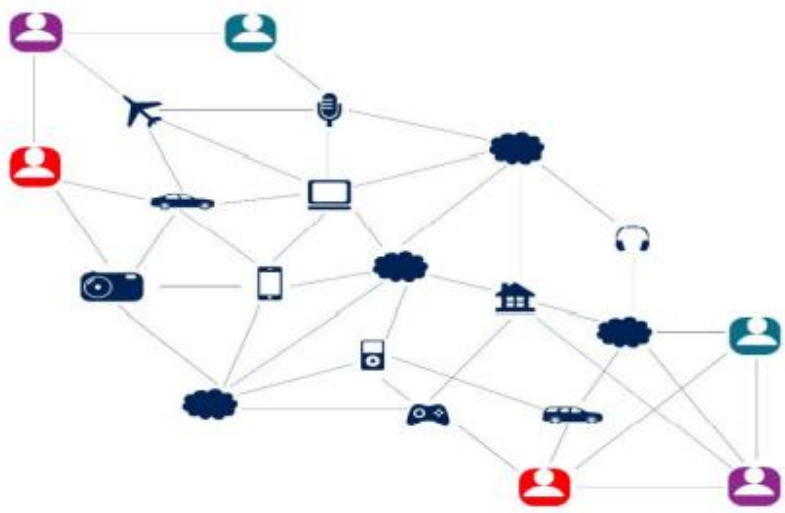

Figure 1. 1 Social Internet of Things (Aslam et al., 2020)

The social IoT is a developing paradigm that has drawn an extensive range of applications to operate on the top of it. As per the norms defined by the owners, social IoT apps are probable to be orient toward a service-oriented design. Each object can be a assistance provider, conversely requester, preferentially both at the same time. During the design process of social IoT apps, users'/owners' convivial relationships must be considered. IoT gadgets form social interaction with other gadgets on their own, based on social policy established by their administrators, and communicate through each other as they enter into communication. In social IoT contexts, assessing the reliability of service providers is critical to satisfying the service requester and enhance system performance.

Malicious devices may launch selective attacks based on their social interactions to benefit themselves at the costs of other IoT gadgets that offer related services. Furthermore, mischievous nodes with solid community relationships may band together and control a service category (Chen et al., 2016a). Because trust provisioning is directly linked to service provisioning in this environment, so trust-based service management is essential.

This research work proposes trust management for IoT and SIoT. The value of trust can be used to detect malicious, selfish, faulty and trustiness of nodes in the IoT network. The success rate, completeness rate, data quality and reward rate of sensed information are used to compute the trust level of each device. For SIoT, adaptive

trust management is designed. QoS and the social factor is used for finding the trustiness of a node in an IoT network.

1.2 Internet of Things

The Internet of Things is a comparably contemporary idea in the society today. However, as technology advances, it has become necessary for society, health care, universities, and homes to be linked to the Internet. According to a Cisco estimate (Cisco, 2019), around 500 billion gadgets will be equipped through sensors and linked to the Internet by 2030. IoT is described as a network that links these objects for the communication system. IoT services and apps collect, assess, and transfer information from these smart devices for further processing.

1.2.1 IoT Architecture

The IoT network transmits a variety of data types using various protocols for various applications utilizing multiple technologies. An IoT device collects hardware, software, network connectivity, and sensors that form a network of things. IoT Architecture Layers and Components are shown in Figure 1.2.

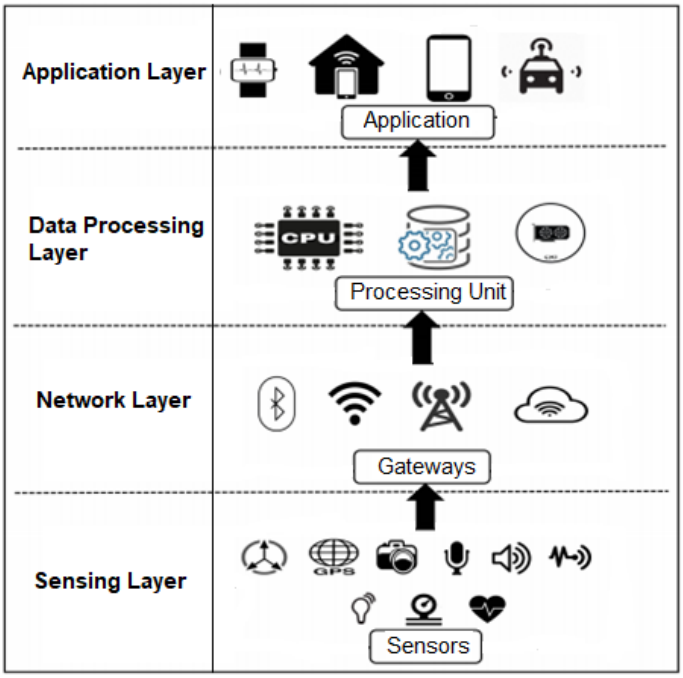

Figure 1. 2 IoT Architecture Layers and Components

Sensing, network, data processing, and application are the four IoT devices' architecture components. The sensing layer's primary goal is to collect information

and detect abnormality in the device's insignificant. It is made up of numerous sensors. Motion sensors, environmental sensors, and location sensors are examples of IoT sensors.

The network layer serves as a gateway for data acquired in the sensing layer to be sent to other linked devices. The network layer of IoT devices is accomplished utilizing various communication technologies to permit information to pass among devices on the same network. The core information processing layer concerning IoT gadgets makes up the knowledge processing zone. The information processing zone analyses the data acquired in the sensing layer and makes decisions based on the findings. The application layer executes and provides the data processing layer's results to achieve various IoT device applications. The application layer is a user-centric layer that performs a variety of tasks on behalf of the user. Intelligent transportation, smart homes, personal care, and healthcare are just a few IoT applications available.

1.2.2 IoT Application

Smart Cities: It uses enhanced computing and communication technologies to improve people's wellbeing. Smart houses, intelligent traffic control, intelligent emergency management, and smart services, and so on are all part of it. Cities are being pushed to become more innovative, and governments worldwide promote their growth via various incentives (Eckhoff and Wagner, 2018).

Smart Environment: Detecting fires in forest areas, tracking snow levels in high-altitude locations, avoiding landslides, earlier earthquake identification, pollution control, and other IoT applications are all part of the smart environment. These Internet of Things applications are related with the lives of people and animals in those places.

Smart grids: It works automatically and aids in allocating, effectiveness, and management of electricity waste in a more dependable manner. Security is a critical step because if control of the system falls into the hands of an attacker, it might inflict significant damage.

Health Care: One of the most practical and cost-effective applications of IoT is healthcare system. As the globe moves closer to a technological future, the health care

system has seen the most changes. The design shows that wireless sensors are implanted in the patient's body and connected to the cloud to relay medical data to the doctor. If the hackers modify the patient medicine details, the doctor gave invalid medicine to patient. It is highly risk to the patient health. So need a high secure system to protect the patient.

Safety and emergency: An additional central field where numerous IoT applications are being utilized is security and emergencies. It can be used for things like permitting only authorized persons into restricted locations. Another application in this field is detecting dangerous gas leaks in industrial regions or the surrounding area of chemical plants. Levels of radiation can also be monitored in nuclear plants and mobile access points, with alerts sent out if the level is too high. There is a variety of construction with sensitive data systems or that store sensitive items. To preserve privacy and items, security software might be used.

Smart Retail: IoT solutions are commonly used in retail stores. Plenty of apps have been developed to track the storability of things as they all pass within each supply chain. IoT is even utilized to track inventory in warehouses to be reloaded as quickly as feasible. Various intelligent e-commerce applications are also created to assist clients based on their interests, habits, sensitivities to specific ingredients, and other factors. The use of augmented reality techniques to give the experience of online purchasing to offline merchants has also been developed.

Smart Agriculture: Tracking soil moisture, maintaining microclimate conditions, selecting irrigation in dry regions, and regulating relative humidity are all part of smart agriculture. The application of such innovative characteristics in farming can assist farmers in achieving higher yields and avoiding financial losses. For example, fungal disease and other microbial pollutants can be prevented by controlling relative moisture intensity in a variety of grain and vegetable production. Maintaining the temperature can also aid in enhancing the quantity and quality of vegetables and crops.

Home Automation: It includes applications like those for remotely regulating electronic equipment to keep energy, intruder detection schemes installed on windows and doors, and so on. Power and water utilization are being tracked via monitoring systems, and consumers are being recommended to save money and resources.

1.2.3 Feature and challenges of IoT

IoT is characterized as an inter-networking model supported by a technology stack that allows for wireless communication among physical and virtual objects, allowing for the integration of advanced services and applications that can self-configure (Čolaković, and Hadžialić, 2018).

The common feature of IoT is,

- Innovative services are based on characteristics in recognizing, monitoring, communicating, and analyzing.
- Networks have a wide range of capabilities and the ability to communicate with one another.
- Anyone and everything can connect at anytime, anywhere.
- Infrastructure for global networks.
- A new technology stack that combines several technologies.
- Intelligent interfaces for self-configuring intelligent objects.

IoT-based systems are typically complicated due to their significant impact on all aspects of human life and the various technologies used to facilitate autonomous data transmission amongst embedded devices. As a result, the Internet of Things is affecting many elements of people's lives. Figure 1.3 shows some of the critical challenges.

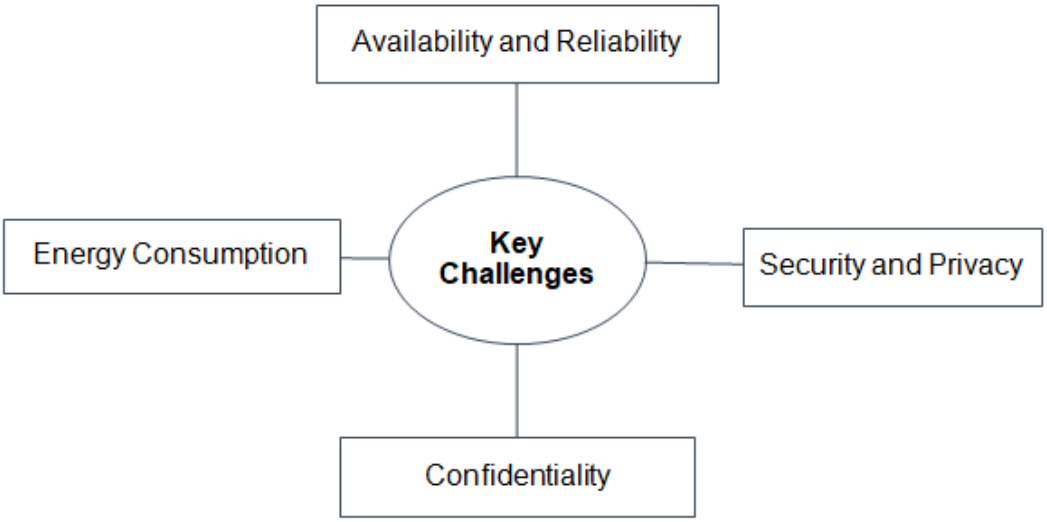

Figure 1. 3 IoT Key Challenges

Multiple concerns, weaknesses, risks, safety and confidentiality issues have been recognized as important challenges in deploying IoT systems. Verification, remote access, data integrity and confidentiality, cryptography, and other capabilities should be provided through security mechanisms, allowing for data processing depend on user-defined strategy and rules. To minimize complexity and increase accessibility, these mechanisms must function in the real world to be expensive and scalable. In IoT, trust management is critical for responsible data mining, authorized services with environmental awareness, and improved customer privacy and data safety.

1.3 Social Internet of Things

People are beginning to live in a cyber-physical-social hyperspace as IoT develops. The Internet of Things is revolutionizing what it means to be social. Mobile phones, tablets, laptops, and other wearable gadgets are examples of technologies connecting individuals directly or indirectly through various applications. The Social IoT is a social network that links everyday things and individuals to develop social ties and construct a social network (Atzori et al., 2012). IoT will create a new generation of online and offline social interactions. SIoT refers to the interconnection of various services, things, and people, with participants benefiting from their participation in the network. For instance, Smart transportations that include vehicle networks, drivers, mobile phones, and other gadgets may make road congestion as low as feasible where traffic information is quickly broadcast in real-time. In the evolutionary stage of the IoT, SIoT is projected to boost the effectiveness of object detection, service creation, and evaluation of the reliability of objects (Atzori et al., 2014).

1.3.1 SIoT Architecture

Traditional peer-to-peer and social networks are combined in the SIoT. Objects form social communications independently via IoT by exchanging interests, information, and services. Figure 1.4 shows the fundamental structural design of the SIoT.

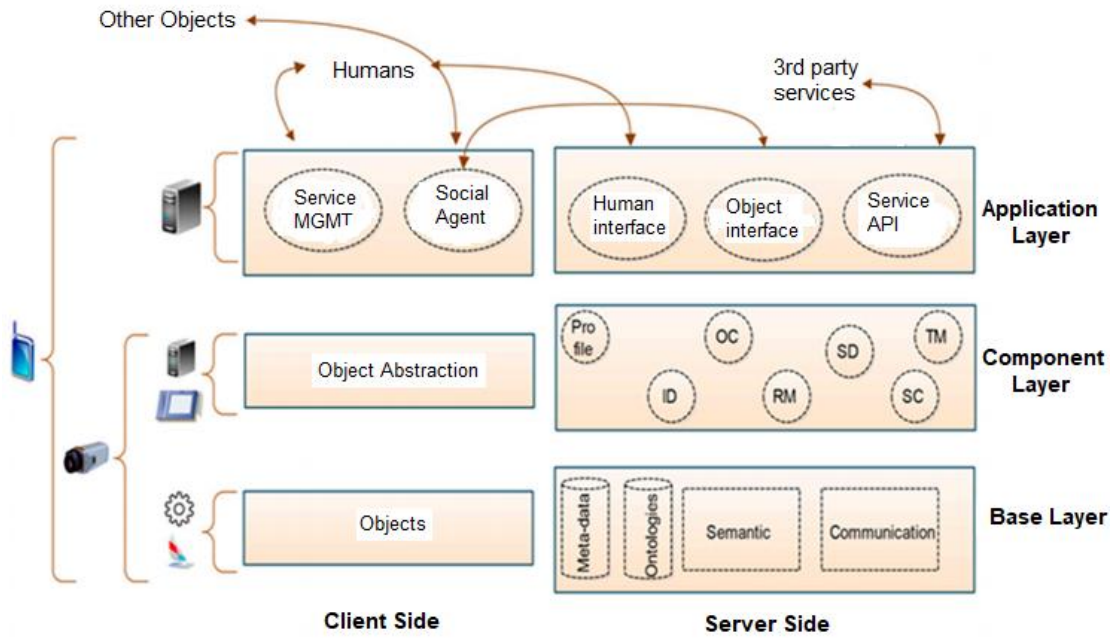

Figure 1. 4 Basic architecture for the SIoT (Amin et al., 2019a)

There are three layers in the SIoT model: base, component, and application. The first layer provides databases, wireless communications, semantic processing services, and other services. The component layer, in the middle, is utilized to implement satellite components. The application layer serves as a link between people and machines. It also establishes a connection to the services. The client-side component is separated into three layers on the left-hand side: objects, object abstractions, and a social agent. The objects layer is made up of a gathering of actual objects that act as a link among connected gadgets. Some specific programming languages are used to control the interface. The higher layer includes agents whose primary goal is to create new connections among the linked items and the social IoT. Finally, the service management level offers two kinds of services: an interface and a monitoring and control system for objects. This paradigm has the advantage of overcoming challenges such as service composition and detection.

In the SIoT architecture, there are five sorts of fundamental relationships between objects:

Parental Object Relationship (POR): establishes a link among items from the same production batch. The nature of such a partnership is usually homogeneous.

Co-location Object Relationship: is recognized among things in the exact position. These objects don't always share resources, but they need to form relationships to form short network links.

The Co-work Object Relationship is formed between things that work mutually to accomplish a general goal.

The Ownership Object Relationship is recognized between things that belong to the same person.

Social Object Relationship is formed between things that appear close to each other regularly or irregularly.

Characteristics for SIoT

- Create a social network between things and resembling human social networks in terms of interaction;
- Use IoT to achieve interaction between people and things;
- Use a combination of IoT and social networking services to demonstrate better internet service and user experience among people.

1.3.2 Smart to Social Things

Many intelligent gadgets with conventional routing protocols and distinct response systems make up the Internet of Things, which provides end-users with information and services. The emergence of IoT in telecommunications contexts was preceded by intelligence, which was the initial stage in an evolutionary custom that included transformed latest transmission facilities. The second step involves creating things with an assured level of intellectual property with fundamental public knowledge. These items can cooperate with the environment and incorporate the fake social status of "neighbours" or inside "loop" and "society". The third stage involves the origin of social objects operating in a community of objects and gadgets. These social media can establish relationships independently, join communities, and build a communication network that may differ from their owners. It has provided some structure for SIoT networks different from the standard social network configurations and brings about new relationships.

1.3.3 Challenges of SIoT

Heterogeneity: SIoT comprises many substances with different characteristics in terms of resources, devices and protocols, all of which must be achieved (Ray, 2016). These variations have resulted in the formation of a network of different factors that influence and direct interactions, increasing complexity, so that the order of things contributes to several significant issues such as interactions and compatibility that require solutions (Tripathy et al., 2016), such as:

- *POR material relationships are used*: parental things can be used in such programs to guarantee reliability because everything is consistent and the same.
- *Use of middleware (interface) for non-POR things*: unlike other alternatives, it can be used on suitable middleware as a visual connector to adapt and improve communication, applicability, feasibility and performance of devices regardless of models or manufacturers (Asghari et al., 2018)

Mobility and Dynamicity: Smart devices in environment frequently vary their location, leading to a lack of adequate search objects to select and provide services. Another critical problem is the dynamic behaviour of things and places that directs to a modify of circumstances. Therefore, things change their position in the network. Other clarifications suggested for these problems, including:

- *Generate object society*: to solve mobility, things can be created into region according to different mobility, social behaviour, social similarities (Girolami et al., 2013), and shared interests in collaboration (Kowshalya et al., 2019). When a thing alters its location, the social structure varies according to this removal
- *Manage flexible operations:* to resolve this issue; items need to provide specific fundamental rules and agreements with their holders to handle these transform to avoid varying network topology. However, flexibility is another problem from this tremendous power because something requirements to adapt to these expected changes.

Tracking items: one of the significant problems in SIoT and huge networks is uncommon tracking, communication, and operations. The solution to this problem:

- *Using a graph form:* A graph form is introduced as a smart thing based on social norms.
- *Decide rules:* some rules must define constructing, updating, predicting, or removing edges among two things. Each item is a work of art in its own right. Their edges are formed by their relationship. Their behaviour can append weight to it depending on the type and aspect of the relationship, such as the same interest, particular services, exact place, etc.
- Utilizing movement patterns: Zhiyuan et al. (2016) suggested resource utilization for detecting movement patterns via GPS and a three-dimensional positioning system based on preferences and motion similarities.

Security, Trust, and Privacy: due to the significant connected network of gadgets, opportunistic services, and SIoT consumers, safety is a necessary key to sharing data with caution. Thus, unlike many other types of research conducted within aforementioned area, it persists one of the important dispute including necessitates every system's durability in the face of different attacks to be safe, reliable, accessible, and robust in collaboration (Tripathy et al., 2016). So there are other clarifications to these issues, including

- *Access control method:* A control system is essential to avoid illegal access to information.
- *Effective Encryption Method:* Use an efficient cryptography method to encrypt information dependably or utilize inexpensive and adaptable models (Shen et al., 2017) to protect real identity from attack.
- *Trust Management Framework:* In addition, work with the SIoT management framework (Kowshalya and Valarmathi, 2017) to present new applications for building confidence among things and users.
- *Secure information distribution model:* generate easy use community that maintains privacy following the strategy to create a robust and secure information distribution model for greater safety and privacy.
- *Node behaviour prediction:* use other strategies such as machine learning (Yang et al., 2015) and a decision-making behavioural predictive tree (Meena and Valarmathi, 2016).

Devices with limited resources: despite the fact that SIoT is a resource-intensive system that has a direct impact on network life and information exchange, there is no longer a viable method to resolve this concern by taking power constraints into account in all design standards for effective communication.

A practical resource management system is required to handle the problem because of the flow of resources, which results in a lot of power and integration.

Active service explores and availability: the number of things in the SIoT has led to downgrading and navigation in the choice of friendships, search services, and the correct interaction between things. This problem spread all over the SIoT system. Thus one of the critical concerns is an active investigation and service availability, leading to lower system downtime, better service delivery, better response time, reduced transaction time, and increased network mobility and dispersion (Meena and Valarmathi, 2016). So there are other clarifications to this difficulty, including:

- *The control method is used:* it requires a way to control and efficiently explore resources, including creating communities of things according to significant factors including social connection (Kowshalya et al., 2019), providing similar services, resources, and other similarities (Abderrahim et al., 2017).
- *Using new search techniques*, Kowshalya et al. (2019) have efficiently used local and social status algorithms to find services between local and global communities.

1.4 Trust Management

The term "trust" refers to a connection between two parties (trustor and trustee) who rely on one another for mutual gain. Because of its multiple type of application, this phrase has several different definitions. It worth is strongly influenced by the environment in which it is employed. Depending on the contributors' perspectives and the context of trust, the notion of trust is described in various ways (Djedjig et al., 2018). The conventional definition of trust is shown in Table 1.1

Table 1. 1 Conventional Trust Definitions

Author and Year	Definition
Chang et al., 2005	The trusting agent's faith in the trusted mediator motivation and capacity to provide premium service in a specific environment and timeframe.
Buttyan and Hubaux, 2007	The facility to foresee another Party's actions.
Aljazzaf et al., 2010	The readiness of a trustor to rely on a trustee to accomplish what is assured in a specific setting, notwithstanding the trustor's inability to supervise or manage the trustee and the possibility of negative effect.
Daubert et al., 2015	Gadgets, entity, and information trust are all terms used in the IoT; trusted computing and computational trust could build device trust. The expected behaviour of participants, such as people or services, is referred to as entity trust. Trusted information can be acquired from untrustworthy sources through aggregation or formed from IoT services that require information to be assessed for trustworthiness.
Jayasinghe et al., 2017a	A trustor evaluates a trustee's descriptive property for an exacting task in a specific setting and period.

Trust has several significant traits. This section investigates some of the most important aspects of trust (Truong et al., 2017).

- Because it only applies for a limited time, *trust is dynamic*. The degree of faith in oneself may alter throughout time. For instance, 'X' has had a high confidence level in 'Y' for the past year. However, one day, 'X' discovered that 'Y' had lied to her, and as a result, 'X' no longer trusts 'Y.'
- *Trust is subjective:* Even when the trustee and trust are the same, trust amongst trustors may differ. To put it another way, confidence is based on the perspective of the trustor. For instance, 'X' has a lot of faith in 'Y,' whereas 'Z' does not (for satisfying a trusted objective).

- *Trust is asymmetric:* Trust is a non-mutual reciprocal; however, it can be symmetric in some rare instances. For instance, just because 'X' (very) trusts 'Y' (in achieving a trusted goal) doesn't indicate 'Y' will (extremely) trust 'X' (in satisfying a trusted objective).
- *The perspective of trust is essential:* Trust among a trustor and a trustee may vary depending on the context, which includes (i) the assignment objective, (ii) the time, and (iii) the surroundings. For example, (i) 'X' trusts 'Y' to offer a backup service but not a real-time streaming service; (ii) 'X' (extremely) trusted 'Y' two years past but not now; and (iii) 'X' (extremely) trusts 'Y' to supply a cloud storage service in the UK but not in the US.
- *Trust is not unavoidably transitive but propagative:* If 'X' (extremely) trusts 'Y' and 'Y' (extremely) trusts' Z,' it does not follow that 'X' will (positively) trust 'Z'. Nevertheless, evidence from the trust connection between 'Y' and 'Z' can be used by 'X' to assess 'Z's trustworthiness.

A trust management model is a accumulation concerning several steps, each of which delivers a different responsibility. The phases involved include data gathering, trust calculation, trust construction, update, and maintenance. A trust management method aims to make nodes more resilient and maintain trust in other devices. A system can only keep reviewing the information from the experience elements for a specific node density to include successfully. Trustors might build their trust by using earlier firsthand observations and suggestions.

Trust management is a significant factor contributing to any item that has to do with trust. In distributed systems, the confidence characteristic analytics, reputation modelling and transition, trust variation, credibility and confidence storage, applications decisions, and so on are all part of the trust management system. Acquisition, storing, modelling, communication, and decision are the five components of a trust management system (Fang et al., 2019).

1.5 Trust in IoT

"Trust" is a phrase that is used in a variety of contexts (Vasilomanolakis et al., 2015). Trust is a vital characteristic of digital interactions in data moreover communication technology, and it is expressed in a range of possible meanings by merging trust in people and machines (Levitt, 2015). The Internet of Things is no exception, as security is directly linked to consumers' capacity to trust their surroundings. As a result, trust in IoT can be described as the belief that a task will be completed without causing harm to the user. It contains the concepts of becoming secure and robust to threats, as well as the user's capacity to grasp the disparate services involved.

Direct trust and third-party trust are the two types of IoT trust (Yan and Prehofer, 2011). A circumstance in which two entities foster a trusting connection after performing transactions with each other is referred to as direct trust. On the other hand, a third-party trust connection is a trust association developed by a thing based on third-party suggestions, with no initial transaction among the two connected things. For instance, thing X trusts thing Y since entity Z trusts Y. In this case, entity X trusts entity Z, and X trusts that entity Z will not lie to him. Thus, there is a connection between risk and the trusting relationship between the entities, as there is any form of trust relationship.

1.6 Trust in SIoT

The trust paradigm has been applied in various areas, including psychology, sociology, and computer science. In the circumstances of SIoT, trust is described as a trustor's "belief" or "self-belief" in a trustee to do a particular task in a given situation within a given time frame to meet the trustor's perceptions (Amin et al., 2019b). Figure 1.5 shows the trust computation in a SIoT environment.

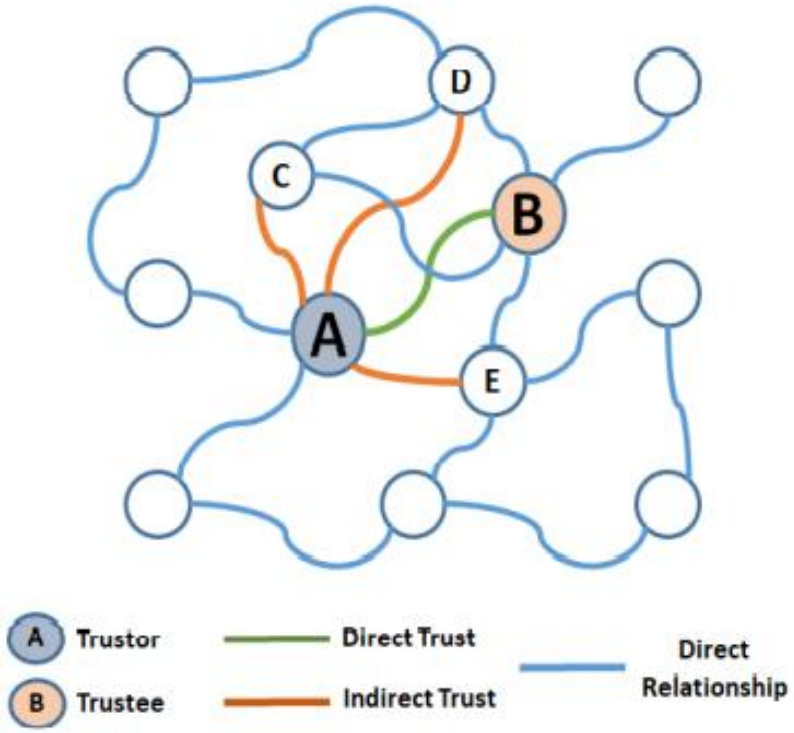

Figure 1. 5 Trust Computation in SIoT Environment

If node A wants to compute the confidence level for node B, it calculates the direct trust itself and then asks common nodes C, D, and E for their input. Then, a cumulative trust score is computed by merging direct and indirect trust. The primary motivation for developing a SIoT trust management system is that there are harmful nodes that could engage in various kinds of assault (including ballot stuffing, badmouthing, self-promotion, and whitewashing) depending on social interactions with other nodes to gain suspicious benefits at the cost of different IoT gadgets offered related SIoT services.

Figure 1.6 shows a suitable model based on trust social interaction. In this model, trust will be gained through the interaction among trustors (who perform in a certain way under natural circumstances) and trustees (Yu et al., 2013). Often, synchronization is achieved by accumulation, and trustors make recognition concerning trustees. Environmental circumstances among the two groups (either the caregiver or the trustee) are measured by the threat engaged throughout each transaction. The trustee's trust is not restricted to the trustee's interests and the trustee's confidence. In this case, environmental circumstances, including threats, are always of great concern. Friendship is a different property, and it is utilized to acquire neighbourly goods by forming community relations between them.

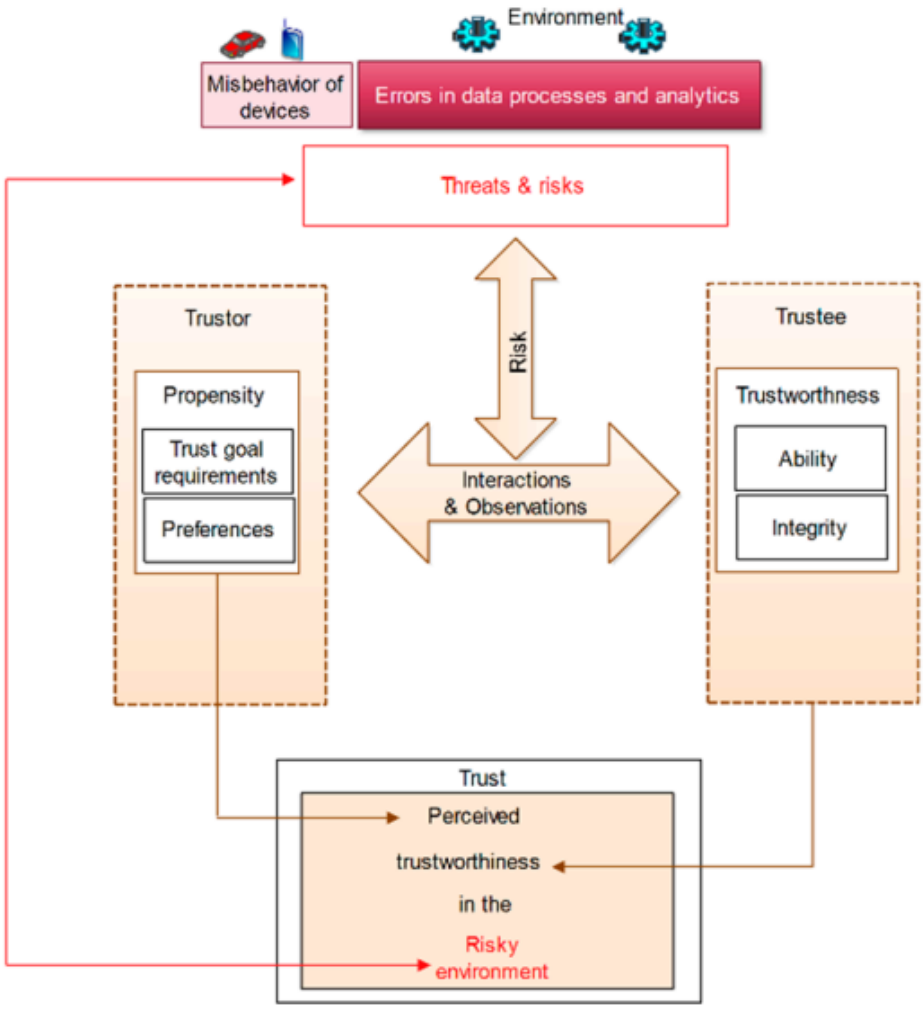

Figure 1. 6 Conceptual trust model in social IoT

The notion of trust construction is simple: it is an benefit of kindness, passed on to an individual termed a trustee. Typically, the trustee manages and manages the property. Trust creation can be used for similar reasons as before, or it can be used to assist.

Single trust is genuinely regarded as the one trustworthy asset that establishes a trust protocol. In this context, service feature is the primary significant metric for IoT service-based applications (Wang et al., 2016). Furthermore, QoS is often affected; therefore, trust between the applicant and the service provider. In this case, relying on the IoT community-based system always works collaboratively.

Multi-trust forever uses trust in a variety of ways. It means that many areas of faith have been measured for the construction of faith. For instance, Guo and Chen

(2015) looked at different structures of mutual trust, including loyalty, closeness, and selflessness. These facilities are used for MANET. In addition, there are many ways to use the formation of trust. Some of these are explained below.

- When a single individual uses the trust structures without having to merge them—a lower amount for each trusted asset based on application-specific criteria.
- One can use the scale of confidence through the process of confidence in the establishment of trust. First, this concept measures the most critical structures in the least essential areas, representing self-reliance. Then, as mentioned earlier, that amount of confidence is used to establish trust between many people.
- One can use a significant amount. It is a combination of the values of each hope. In addition, the given weight may reflect application-based requirements.

1.7 Problem Statement and Research Objectives

IoT is a rapidly growing paradigm that includes many technologies predicted to lead in the next technological revolution. Unfortunately, due to unsecured Web interfaces, inadequate transport encryption, insufficient permission, and inadequate software protection, IoT systems are highly vulnerable. All of these new potential hazards to data protection and security must be thoroughly considered.

Despite the hidden benefits of IoT based health monitoring solutions, the devices raise severe issues in data accuracy. For instance, malicious people or gadgets can provide inaccurate sensory data on purpose to benefit themselves. To assure the quality of the received data, it is therefore required to build trust maintenance and irregularity detection systems. For this reason, this research proposes a patient monitoring service, which computes the trust level of each device using trust properties. In addition, to calculate the trust level, it uses four metrics: success rate, completeness rate, data quality and reward rate of sensed information.

SIoT is a newly illustrated phrase in the research that stems from integrating social networks and IoT. It refers to the communication among objects moreover the Internet as a network layer, with functionality such as data sharing, behaviour, and

relationships independent of human interference. Furthermore, items can form social relationships independently, and their interaction can range from simple to complex. SIoT created a common system built on similar values and objectives to give more reliable assistance to end-users by combining all networked devices all across the universe.

To assure trustworthy information examination, competent services, and better user safety, trust management becomes a critical concern in SIoT. It assists people in confronting and overcoming their problems and uncertainties and encouraging user adoption and consumption of IoT services and apps.

Research Objectives:

- To develop the secure trust model for IoT and Social IoT
- To present a trust computation model that defines the formation of trust from sensed raw data to a final trust value.
- To examine each trust property and analyze the data
- To create an evolving trust management approach depending on QoS and Societal factors for Social IoT.

1.8 Thesis Outline

The thesis is planned into six chapters. The first chapter initiates IoT, social IoT, Trust model, problem statement, and research objectives. The remaining chapters are organized as follow.

Chapter 2 presents a review of the literature review relevant to the thesis. This literature review provided the understanding of the primary model of various topics and diverse viewpoints provided by different professionals and the research areas happening on the academic side.

Chapter 3 discusses in detail the trust model in IoT and the social IoT concept. This chapter explains a general trust model for the social IoT, which described six essential components of the trust model. It also explains the trust-based network classification of SIoT.

Chapter 4 provides the trust computation model for IoT. It explains the generic trust model with trust properties. This chapter considers a patient monitoring service

and proposes a trust level computation model based on trust properties. The statistical framework is used to calculate the trust degree for determining whether or not a node is trustworthy.

For determining the trustworthiness of a node in an IoT network, this trust approach incorporates both QoS and social variables. Static type trust handling is also covered in this chapter.

Chapter 6 concludes the thesis by summarising the key findings from the research work and providing the future direction for the research work.

CHAPTER – II

LITERATURE REVIEW

2.1 Introduction

The IoT is a network of heterogeneous objects that can exchange data and connected via distributed networks. Furthermore, it is a worldwide network created as a method for observing and regulating information about the physical environment (Lin et al., 2017b). IoT can connect everywhere and infrastructures through numerous communities to provide successful and secure services for any application, at any time and in any location. Future IoT schemes will use many intelligent things to connect the physical world to the Internet, and they are likely to be very profitable (Guo et al., 2017).

IoT devices might be hacked and misused; it is necessary to ensure secure communication across heterogeneous and trustworthy devices to complete IoT member authentication (Safkhani and Bagheri, 2017). As a result, trust management solutions are critical in the Internet of Things for reliable data and better user privacy (Sicari et al., 2015). Therefore, the primary aims of trust in the IoT include confidence between IoT layers, gadgets, and apps.

The notion of the IoT and social networks together usually known as SIoT. (Atzori et al., 2012). In particular, network node social and contextual data is viewed as a new and necessary feature in designing communication structure that utilizes nodes' social relationships (Chen et al., 2015b). The underlying idea is that gadgets in SIoT applications deliver various types of incorporated services to attain a general goal in a jointly advantageous manner. SIoT has created new opportunities for items to work together to achieve common goals that are mutually advantageous (Afzal et al., 2019). As a result, many new innovative products and services are being developed and made available to the public over the Internet.

The conventional privacy and safety of honesty, discretion, and accessibility face more difficulty than managing risk and safeguarding the SIoT (Sicari et al.,

2015). In this regard, trust is crucial in supporting individuals and services in overcoming risk and uncertainty in making the decisions.

In many domains of human life, trust is a multifaceted concept influenced by both participants and ambient factors. It's a basic emotional metric that can help a trustor decide whether or not to put himself in jeopardy if a trustee is found to be incompetent. Because the purpose of every SIoT service is to arrive conclusions externally requiring individual interference, confidence has been identified as a key circumstance in providing seamless communication, unharmed methods, and trustworthy assistance. By decreasing unexpected risks and enhancing predictability, a trusted policy can assist both SIoT support and assistance in working in a controlled mode.

This chapter reviews the related work of various topics related to IoT and SIoT. Then, it explains a related survey for the subject of IoT, trust management, Trust in IoT. Finally, it describes the detailed study of trust in SIoT.

2.2 Survey on IoT and SIoT

The increase of the IoT in recent has led to a concept move across all areas of human-machine communication. IoT has experienced widespread acceptance in industries ranging from industrial to medical, governance to infrastructure management, customer services to defence in just a few years. Customers may use IoT to access a wide range of intelligent apps. To a lesser extent, a ambulance or police vehicle may communicate with a robotic device to automatically turn a red or green light on in the event of an emergency. To a large extent, a homeowner can connect and interact with a surveillance camera installed in their home, to track the home located in another country (Lounis et al., 2020).

The cloud was used in previous IoT architectures to acquire and organize services; the current model uses the cloud with a fog node for analysis. In the future, the gadgets are expected to communicate directly with other gadgets and be associated with the Internet and other local gadgets (Hassija et al., 2019). As a result, SIoT and connected equipment are gaining popularity. SIoT will allow various social

networking clients to access gadgets, and users will exchange devices over the Internet (Frustaci et al., 2018).

Smart Healthcare: It is one of the most popular and exciting IoT apps. In recent years, remote health care services have grown in popularity. Remote health monitoring, elderly care, chronic health care, and fitness programs increase IoT applications (Baker et al., 2017). The Internet of Medical Things (IoMT) has become a professional initiative in the health care industry. It is used to collect and process information about the patient's body. To inspect health nodes embedded in the patient's body, for example. It can also use smart phones to decipher a patient's medical knowledge. To enable safe communication in health care systems, an anonymous secure user authentication approach (Deebak et al., 2019) is presented. It also shows that the rival cannot represent a verifiable user in order to gain unauthorised access to or retrieval of patient data.

Lu and Cheng (2020) have recommended a reliable information distribution system for IoMT. First, the scheme ensures the security and satisfaction of shared knowledge. Following, the method performs functional sincerity inspections unto the client opens the same information to counter a faulty application. Finally, the system offers a lightweight patient-to-userr process. The method eliminates the trouble of making encryption and decryption keys only on end devices.

Dilawar et al. (2019) use blockchain technology to secure patient health information. A blockchain-based integrated process can solve many of the difficulties associated with a central cloud solution. Farahat et al. (2018) present a information encryption method that captures initial data encoding and then encrypts that knowledge with a rounded key till transmitted beyond the system. Physicians can retrieve protected data using access keys and credentials. This work was implemented using the low-cost kit and dependable applications to guarantee the protection of the delivery of pharmaceutical data.

Aujla and Jindal (2021) introduced a blockchain-based approach to prevent data blocking and maintain patient privacy. This approach enables close by edge gadgets to generate separate blocks in the blockchain to transfer health care information from sensors to edge nodes securely. Tensor based method is used to

share and store data in the cloud. This assists in diminishing the replication of large amounts of information sent out over an extensive IoT health network.

Ming et al. (2020) introduce an anonymous certificate-based system with a comprehensive IoT healthcare signing scheme, which combines cryptography-based certificate and elliptic curve cryptography to make simpler certification managing issues, resolve significant sharing problems and guarantee confidentiality protection. The secure investigation recommends that this system is capable of privacy, malfunction, recipient name, sender anonymity and validity.

Xu et al. (2021) suggest an e-healthcare mobile social IoT (MSIoT) based on a targeted immunization program to accelerate the increase of a transmissible disease quickly. Exclusively, start by developing an e-healthcare MSIoT structure by incorporating the e-healthcare system with MSIoTs, where the infectious disease situation is collected on time. In addition, the graph colouring and spread-centrality-based optional candidate search algorithm are designed for candidates who have great potential to prevent infectious diseases.

Gulati, Kaur (2021) learns the importance of re-deploying IoT-enabled social systems in the AAL (Ambient Assisted Living) environment by proposing a robust AAL-based Social IoT program for older people (FriendCare-AAL). In addition, it presents a systematic approach to establishing partnerships between smart devices and introduces the concept of responsibility offloading between devices. This work can assist older persons living in a smart home environment. Furthermore, in an emergency, the system automatically generates proximity alerts to the organizations concerned.

Smart Home: The term "smart home" refers to a home automation system that is portion of the Internet of Things (IoT) model. Users can monitor and operate their household appliances and Internet connections from afar (Lee et al., 2016). This includes utilising a smartphone or voice command to turn lights on and off, thermostats that regulate indoor temperatures and produce power usage reports, or sprinkling practices that start at a specific time of day, on a regular monthly schedule, and so prevent water pollution.

It is essential to guard the connection among home IoT gadgets and mobile locations in an intelligent home. Sivaraman et al. (2018) focus on the impact of safety and confidentiality on smart home IoT gadgets. The associated attacks were highlighted at the level discussed in terms of secrecy, reliability, and access control. On the other hand, cloud-based platforms can serve as the backbone of a future smart home, providing reliable and efficient services.

Jabbar et al. (2019) introduce a low-cost and hybrid IoT-based home automation scheme with an easy-to-use interface for smartphones and laptops. IoT @ HoMe is developed with an algorithm that enables home supervising and easy control of household items over Internet anytime and everywhere. The method uses a node microcontroller unit as a Wi-Fi-enabled method to join various sensors and update their information on an Adafruit IO cloud server.

Song et al. (2017) propose a communication process that saves energy, secure and maintains the privacy of a smart home system. A symmetric encryption protects data transfer with secret keys created by random. This scheme use message verification codes to ensure data authenticity and integrity.

Smart City: Montori et al. (2017) suggested a SenSquare architecture that is focused in looking at the customer current data flow of the smart city using a crowded mobile sensor. This architecture used a data-sharing method to assess the feasibility of the proposed method. Still, information authority and user confidentiality are not considered; therefore, distribution may not be permitted.

Cheng et al. (2018) proposes a standardized approach to building and implementing a new fog-based framework, namely FogFlow, for innovative city platforms. The FogFlow editing model allows IoT service developers to design easy-to-expand IoT resources over the cloud and edges. In addition, it supports common ways to share and reuse content data across services. Finally, Hu and Ni (2018) suggest a new scheme of finding urban monitoring systems. This new approach is used to determine and select the highest frequencies of imaging waves found in digital camera sensors, choosing license plates for cars.

Rahman et al. (2019) propose Blockchain-based infrastructure support secure and private contracting services designed for Internet of Things-enabled economic

sharing in significant mega cities. The infrastructure incorporates fog nodes at the edge of hosting and processing multimedia downloads of geo and communications from the mobile edge and IoT nodes, utilized AI to develop and derive important incident data, generate semiotic analytics digital, and store outcomes in Blockchain plus disseminated cloud depots to assist the sharing of financial services.

Table 2.1 shows the IoT application comparison.

Table 2. 1 IoT Application

Author	Domain	Application	Device
Kim et al., 2018	Healthcare	IoT medical service contributors	autonomous hand-held devices and smartphones
Subrahmanyam et al., 2018	Healthcare	Healthcare Framework	Wearable devices
Islam et al., 2018	Healthcare	Human body data collection	Bio-sensor attached to the body
Naranjo et al., 2019	Smart City	Fog based Smart city	WSN devices
Akbar et al., 2018	Smart City	Weather System	Smart devices
Lin et al., 2017a	Smart Home	Monitoring indoor condition	Sensor devices
Sun et al., 2017	Smart City	Street parking system	WSN Devices
Kwon et al., 2016	Healthcare	Medical industry	Medical sensor
Luvisotto et al., 2018	Industry	Indoor monitoring system	Industrial sensor

2.3 Survey on Trust Management

Trust management is projected based on distributed and intermediate methods. In the shared organization of the trust, all trustee is in charge for accounting. The distributed machine is subject to multiple failures (Truong et al., 2016). In central trust management, the foremost influence is in charge of managing the confidence of all nodes. An important issue for the centralized method is the crash of central authorities. If the main authority does not succeed, then no backup security method is accessible to handle the confidence.

Trust is a complex concept driven by a variety of factors that are measurable and non measurable. It is inseparably linked to security, as maintaining the device's security is essential to gaining confidence. Another important principle of confidentiality is privacy, which refers to the business's right to decide whether or not information will be published or disclosed. It can be used on various network domains such as WSN, MANET, VANET, cloud, and social networks.

Trust in WSN

Wireless Sensor Networks (WSNs) are often installed in remote, unprotected and open spaces. As a result, nodes can be attacked and interrupted. The attacker may use disturbing sensors node to interrupt communication or inject ambiguous sensor values. Misleading data can ruin an entire decision-making process. A different robust security system is required to protect WSNs from internal and external attacks. Reliability measurement methods are used to measure the reliability, validity, and reliability of sensor nodes by analyzing their behaviours to protect them from malicious node.

Khan et al. (2019) propose a novel and comprehensive approach to measuring the trust of a WSN that use to enhance collaboration, reliability, and safety by identifying faulty or self-centred links with lessened memory and energy usage. Sequentially, the system is managed at two stages: the intra-cluster and the inter-cluster and the distributed and centralized method to obtain a reliable and proper conclusion of the sensor connections. It contains distinctive features, such as measuring resistance to attack, and the integration of active trust in the collection,

head to determine the value of the global response. Data trust and communication trust plays a significant role in dealing with hostile environments.

Busi Reddy et al. (2017) proposes a trusted approach that analysis WSN's communication and data trust. Connection trust is measured by the immediate and secondary perception of the transmission behaviour of a neighbour. Direct confidence is based on the forwarding behavior. Indirect trust is taken from a neighbour's perception translated into recommendations—Dempster-Shaffer (DS) weight theory is used to calculate indirect trust. Data reliability is calculated using sensor data median.

For the evaluation of node trust and reputation in WSNs, an exponential system based on the definition of information and reputation is advocated (Zhao et al., 2019). It is used to monitor node behaviour, and explicit sharing is used to characterise the sharing of nodes' trusts. Within wireless sensor networks, node expectation is used to detect dependable data transmission and to weaken harmful assaults. Most crucially, entropy theory is used to determine the ambiguity of direct trust ratings. When the ambiguity of direct confidence is great enough, indirect trust is begun to support interaction specifics. It may not only cut node computing power but also extend network life.

Trust in MANET

Managing trust on the Mobile Ad Hoc Network (MANET) is a challenge where collaboration or cooperation is essential to achieving the goals of node reliability, availability, disability, and restructuring. Shabut et al. (2015) propose a trust model that depends on a defensive scheme, which uses a clustering to strictly filter out attacks related to dishonesty recommendations over time regarding the amount of communication, information compatibility and closeness between nodes.

Cai et al. (2019) propose a system of evolutionary commitment that mimics the human process of understanding and relies on knowledge of the level of reliance to prevent various attacks. In this program, mobile nodes swap reliability data and process trusted data obtained based on their understanding. Ultimately, each node drastically changes its cognition to keep out malicious entities. The most interesting feature is that they cannot damage the system even if the internal attackers know how the security system works.

Cho et al. (2019) propose a work-sharing protocol using a concept of multiple trusts, which aims to increase the completion rate of standard machines that contain numerous tasks by measuring reliability and performance risk. In the light of the basic notion of confidence, defined as the motivation to acquire on a task, selecting suitable sites for a known job while meeting the satisfactory level of risk of performing multiple tasks contributes to the success of a mission.

Lwin et al. (2020) created a lightweight consensus algorithm and a blockchain-based trust management system for ad-hoc networks. For MANET routing nodes, the approach provides a distributed confidence architecture that does not interact with Blockchain. In addition, the optimised link channel protocol is employed in MANET to reflect the blockchain concept.

Trust in VANET

The vehicular ad-hoc network (VANET) presents a unique platform for automotive exchanges with sensitive information, such as messages, to avoid collisions. VANETs are used to enhance traffic management and decrease the number of highway accidents by given that safety applications. Still, the VANETs were affected by several security attacks from malicious organizations. Tangade et al. (2020) suggest a trust management system based on hybrid cryptography to protect VANET on a large scale. Since verification is essential for building trust and secure communication between vehicles, this work incorporates hybrid cryptography to validate an effective and efficient trustworthiness management system. Hybrid cryptography contains asymmetric identity-based digital signature and symmetric hash message authentication code (HMAC). The roadside unit of trust assesses the value of trust, and a reliable agent measures the value of a vehicle based on its rewards.

Ahmad et al. (2018) provided a novel framework for analysing trust and management that can be used to design, manage, and evaluate trust under diverse scenarios and in the presence of aggressive cars. To identify harmful threats, this approach uses an asset-based threat model and an ISO-based risk assessment.

A attack-resistant trust management is proposed for VANETs to detect and respond to malicious attacks and check the reliability of both data and mobile nodes

on VANETs. (Li et al., 2016). Specifically, data reliability has been tested based on information obtained and collected on multiple vehicles; a node trust is tested in two dimensions, confidence and trust recommendations, which show how well the node can perform its function and how reliable the suggestions from other nodes are.

Zhang et al. (2020) suggest an anti-attack trust management method called AATMS to assess vehicle reliability. With the help of AATMS, vehicles on VANET can avoid dangerous vehicles and cooperate with reliable vehicles. The concept of AATMS is mainly inspired by the TrustRank algorithm, which is used to combat web spam. First, the Bayes theory is accepted to calculate the local reliability of vehicles based on historical interactions. Then choose a small set of seed trucks according to local trust and other community features. Once a reputable seed vehicle is identified, use the regional structure that connects the vehicle trust to assess the global reliability of all vehicles.

Trust in Cloud

Trust management becomes an vital need in the cloud space and requires a trusting association among the service user and the service provider. Thus, relying on the capabilities of cloud resources to complete the work is based on alternatives such as availability, reliability, and processing power.

Zhang et al. (2018) present a novel trust model based on domain divisions that includes a compatible technique for reducing trust management and improving the capacity to detect rogue nodes. First, by preserving reliability and accountability, the separation of nodes on domains helps to reduce trust management. The latest dependability values are then stored by raising domain and cross-domain sliding windows. After that, a node's domain values and cross-domain trust are calculated using an algorithm. Finally, to remove malicious trust and malicious nodes from the domain, a filtering method is used.

Wang et al. (2019) offer a cloud service selection method based on user preference integration and reliability. This method does a comprehensive dependability test, which is then used to evaluate and choose cloud services. In addition, the suggested integrated collection of positions is based on user preferences, which will increase the accuracy of the recommendations even more.

Hassan et al. (2020) provide a well-known QoS model for evaluating a cloud provider's reliability. This model calculates the total collection amount, which is constantly updated on each sale, and displays the provider's current or recent transaction in the cloud. Furthermore, the cloud device's reliability is determined using the covariance calculation procedure to determine the reliability of the user's response, as well as the provider's reputation history from user response ratings. Finally, the cloud device's dependability is assessed by estimating the computational power of resources used during implementation.

Han (2021) proposes a dynamic access control model based on trust and privacy protection to solve privacy disclosure and the use of cloud services. First, add a sense of responsibility and purpose in managing access and establish a privacy policy and privacy policy tree. Second, set a new hope test and provide a consistent weight algorithm. Third, prepare the privacy information for the common space and the measurement system. In addition, propose a tradeoff relationship model between mutual trust and privacy protection; each participant can choose related parameters depending on your actual requirement and preferences.

Trust in Social Networks

A social network can be considered a group of people (or groups of people) who share various information for friendship, marketing or business exchange. Social networking modelling refers to analyzing the multiple components of a network to understand the basic pattern that can help or disrupt the formation of information in this type of connected community. (Ureña et al., 2019)

Nasir, and Kim (2020), offer a way to measure the ongoing level of trust/mistrust among offline users. This approach is based on consultation and conveys the spread of trust. It determines, on average, how two users trust differently authorized by other users and how the difference a user trusts the other user in how much that user is authorized. Using this difference, they rated four partial reliance rates and calculated the final trust value from a trustee to a trustee as the estimated value of these partial values.

Xu et al. (2019a) suggest a way to maintain the confidentiality of trust that shares such combined images. The basic idea is to produce an actual image so that

users who may lose the top-secret in photo sharing will not be seen from an unknown image. The loss of privacy on the user depends on how much you trust the recipient of the picture. And the user's reliance on the publisher is affected by the loss of privacy. The limit specified by the publisher controls the anonymity effect of the image. A greedy approach is suggested for the publisher to open a limit to balance confidentiality with information shared with others.

Ding et al. (2020), a novel trust model based on a public discovery algorithm. By improving the calculation of traditional hope through the power of inter-node interaction and similarity in social interaction, it finds communities through K-Mediods integration. Xu et al. (2019b) propose trust based approach to access to integrated privacy management. The user decides whether or not to send the data item based on the combined view of all the users involved. Users' reliability rates are used for weight users 'opinions, and the values are renewed according to users' privacy loss.

2.4 Survey on IoT Trust

This section discusses the basic features and their differences, advantages, and disadvantages of IoT trust management.

Chen et al. developed a flexible trust management solution for active and social IoT systems (2016a). The supply of dependency principles between IoT devices is a critical factor to consider. Each device stores the level of trust between users and devices. For trust value assessments, object suggestions, transaction history, and direct recognition are used. In addition, based on social interactions between IoT devices, particular metrics such as dependability, quality of service (QoS), and collaboration are assessed. Although the machine protects user privacy, it has a low density.

The QoS-based service purchase framework was proposed by Li et al (2017). The ontological model is built to show and match the service to context and QoS data. Furthermore, an effective system for distributing trust is linked with the service availability process without the inclusion of extra infrastructure. In this study,

customer service retrieval is utilised as QoS-based information to aid customers in picking trustworthy services. The accuracy and quality of the results are not checked.

A sequencing strategy based on the trust management blockchain with mobility assistance was proposed by Kouicem et al. (2018). This method is scalable, and it allows smart devices to spread service provider confidence as it is deployed. The proposed method protects user anonymity in the Blockchain, however it ignores critical measures like confidence, accuracy, and integrity.

The data reliability and business reliability of Jayasinghe et alproposed .'s reliability and predictive data test methodology have been evaluated. Data matrix output, data integration reliability, testing, and prediction are all layers in the proposed approach. A collaborative filtering method predicts trust values between users and specific data sources based on numerous parameters such as completeness, uniqueness, timeliness, correctness, accuracy, and consistency after collecting trust values. Furthermore, the integrity and quality of the outcomes produced are maintained, but the density is minimal.

Al-Hamadi and Chen (2017) developed an IoT-based decision-making strategy based on a health system that considers reliability, risk, and potential health loss. This computer accurately analyses data and evidence to make trustworthy decisions, and it modifies the performance of sites by lowering their dependability value on a regular basis. Furthermore, it raises the likelihood of making the best decision possible and eliminates people who give inaccurate information. The device, on the other hand, considers that the IoT environment consists solely of sensor nodes capable of achieving the goals of IoT services.

Chen (2018a) developed a trust management strategy that included techniques like Selection Combining (SC) and Maximum Ratio Combining (MRC). Before integrating with control information, the prescribed parameters are retrieved and measured with a single measurement value. The data obtained in the MRC is then passed to SC to calculate the amount of trust. The value of the faith made in the previous stage determines the QoS rate. They did, however, assess the proposed process with a restricted number of nodes, which did not guarantee power interruptions.

An honest and ethical policy-based hearing process was proposed by Li et al. (2018). Contextual data and unfavourable IoT data are used to analyze data reliability and IoT node features. The rules outlined above are used to test loyalty in a variety of situations. Imitation results have shown that the proposed method can determine the reliability of information and IoT nodes accurately and effectively. However, what's worse in this way is that new devices or new common sight can be considered a node with a malicious expiration rule.

Maddar et al. (2018) presented a new IoT access model, focusing on WSNs. The location checking methodology was used to ensure that users interacted with the correct node for each transaction. In addition, to update trust node values and eliminate malicious nodes, a mathematical calculation of the trust calculation was developed.

Fernandez-Gago et al. (2017) proposed a methodology to assist IoT developers in incorporating confidence into IoT scenarios. This framework addresses issues such as trust, privacy, and ownership, as well as other operational needs that should support IoT trust in order to deliver various services that enable the inclusion of confidence in IoT contexts.

How to manage smart trust was proposed by Caminha et al. (2018a). This approach was based on machine learning and the performance of the sliding window to automatically check the reliability of the IoT device and the service provider's features. With the data generated, this method has detected attackers and outsiders with 96% accuracy with minimal use of time in the real world.Dependability of nodes is determined by TMM utilising both node ethical integrity and data reliability, which are estimated using ANFIS and weighted add-ons, respectively.

Alshehri et al. (2018) propose an innovative IoT trust management system based on integration. IoT applications, super-node, cluster, and master node are all part of it. Cluster nodes are responsible for ensuring that the data provided by the master node is successfully transferred. The master node connects the nodes within the collection, while the super-node maintains the natural IoT confidence.

Awan (2019a) proposes a high-quality, high-quality multilevel computer management model. This approach divides domains into communities based on

similarities and interests in providing multilevel protection. All teams have their dedicated server for calculating and managing confidence levels. The trust server manages domain management, calculates domain trust, manages trust values, and distributes standard trust certificates on domains based on trust standards. The calculation of faith is based on direct and indirect trust frameworks. For example, if the trustee deals with the partnership, the public server considers the trustee's public trust when the trust is tested.

In IoT, Adewuyi et al. (2019) propose a complex confidence model for collaborative applications. Although recommendations are evaluated using responsible practices, trust is used with accuracy. In the process of trust testing, the effects of faith and maturity were investigated. Appropriate mathematical operations are used to illustrate each variability of hope. Rani et al. (2019) propose a power-saving reliability test model using a high-reliability test model to reduce the destructive effects of unauthorized sensor areas and limit network distribution of integrated trust-sensor IoT-enabled power applications.

Awan et al. (2019b) propose a domain-based trust management framework that allows a computer to measure the reliability of various devices in a location. The confidence of this framework is divided into three security components that help IoT nodes cope with compromising devices/nodes.

In a monitoring service study, Shayesteh et al. (2018) propose a computerized hybrid entity/data trust system that uses Bayesian learning to measure users (such as data reporters) and Dempster - Shafer theory (DST) for data integration and data reliability calculations. The magnitude of the opportunities used in the DST is drastically altered using the newly calculated user scores and contextual structures associated with recorded data to provide resilience to behavioural changes.

Chen (2019) proposes to use IoT-based RBAC (Role-based Access Control) in conjunction with a test algorithm testing model to reduce the risk of internal security in the intra-server and inter-server for large integrated IoT applications. Three trust test algorithms are developed and introduced in the proposed IoT-based RBAC collaboration model to reduce internal security threats to compatible IoT servers. These include a trusted location algorithm, a reliance test algorithm, and a collaborative algorithm to test trust.

Hameed et al. (2021) proposed that identification, i.e., public keys and trust indicators for IoT devices, might be maintained in the Blockchain to assure consistency and resistance in a software-defined networking (SDN) based IoT network. With an adequate conceptual framework that proves the intensity of the suggested solution, an emerging unique approach for key management and trust of IoT devices in IoT networks is provided. Simulations that can store the public keys of IoT devices in the Blockchain and efficiently streamline network traffic via SDN effectively illustrate the convergence of IoT network and Blockchain technology with SDN.

Abou-Nassar et al. (2020) propose a Blockchain Decentralized Interoperable Trust (DIT) framework for IoT sites where an intelligent contract ensures budget assurance and the Indirect Trust Inference System (ITIS) reduces semantic spaces and improves reliable object measurement with network locations and edges. DIT IoHT (Internet of Health Things) uses the Blockchain ripple secret chain to establish reliable connections by securing nodes based on their collaborative architecture. Furthermore, the controlled connections needed to resolve integration and integration issues are facilitated through various IoHT infrastructures.

Hussain et al. (2020) propose a reliability test model to test user loyalty to Fog based IoT. This approach utilizes the reliability of multiple sources and a reputation-based testing program that helps to assess user reliability effectively. In addition, use a well-informed feedback-response system and feedback that helps make confidence testing fair, effective and reliable. Finally, it introduces a monitoring mode for corrupt/dishonest users, monitoring user performance and reliability.

Park et al. (2021) suggest TruSense, a reliable novel sensor framework for IoT environments that incorporates end-to-end performance from an IoT device to cloud service. The TruSense framework includes a small sensor board, a communication protocol, and a reliable cloud sensing service in the IoT environment.

Altaf et al. (2021) propose a fidelity testing program based on the content of intelligent architectural applications. Reliability of service rating is calculated based on previous client interactions and recommendations from similar customer contexts. The client selects the best service provider based on previous and current schools relying on subsequent collaboration. The model also helps to filter out malicious

nodes with a reliable indirect calculation process. This process strongly provides weights based on direct interaction with reliable recommendations for detecting and avoiding aggressive interactions.

2.5 Survey on SIoT Trust

Internet of Things is a network of connected computer devices capable of transferring valuable data to each other via the Internet without the need for human intervention. Social IoT (SIoT) has become an emerging trend in a connected environment where many IoT user devices support communication within a social circle. Trust management on the SIoT network is essential because trusting data from compromised devices can lead to severe reductions within the network. Therefore, it is necessary to have a system in which devices and their users check the reliability of other devices and users before relying on the information submitted by them.

Azad et al., 2020 introduces a novel framework for computing and restoring participants' loyalty in the SIoT network in a self-imposed manner without relying on any trusted third party. Instead, participants' privacy in SIoT is protected by using homomorphic encryption in a power-enabled system. Furthermore, to implement compulsory structures, each device's reliability rating is automatically updated based on its previous trust scores and the peer-to-peer rating in the zero-knowledge proofs (ZKPs) to ensure that everyone involved adheres to the law faithfully.

Wei et al. (2021) incorporates the public trust theory and includes different features of IoT devices to address confidence in the SIoT. They developed a standard model of trust that fully captures the skills, determination, and social relationships of the SIoT. Specifically, describe the two functions according to the Degree of Importance and the Degree of Contribution to calculate strength and determination. Then, present a reliable model of substantial equilibrium in a dynamic environment and combat common aggressive attacks.

A complete reliability model developed for social IoT (Lin and Dong, 2018) is proposed. The model includes trustee, goal, loyalty test, decision, action, outcome, and context. Building on this model of trust, we define the concepts of trust in social IoT in five aspects such as 1) manager-to-manager agreement; 2) the transmission of

complete trust; 3) flexibility of trust; 4) renewal of trust, and 5) fidelity influenced by a active setting.

The SIoT Access Service Recommendation Scheme is presented with an understanding of the environmental issues and factors affecting the security and stability of IoT networks (Chen et al., 2015a). SIoT service/device reliability tests include vulnerability, robust performance, and resource restriction. In addition, they offer compelling metrics that include transaction time structures and social interactions between devices in testing an effective environment access service. The performance-oriented approach is also based on the measurement of workload and network durability. This approach allows you to avoid self-promotion and negative self-expression, including Ballot.

Nitti et al. (2014) focused on honesty management in social IoT by promoting independent approaches and objectives. Modesty has a slow, noticeable response, especially when dealing with powerful behaviours. On the contrary, the intentional approach suffers from this type of behaviour because the reliability of the notes is pervasive throughout the network and includes both perceptions from areas of misconduct and perceptions from areas of misconduct. Direct service quality monitoring and response dissemination are used to avoid self-motivating attacks. Loyalty is used to prevent unwarranted attacks on Bad-mouthing and ballots, and quality assurance tests are used to correct attacks on Opportunistic service. A distributed hash table is used to strengthen the durability and expansion capacity.

Xiao et al. (2015) recommends a reliability model built on the assurance and standing of SIoT sites. It all has a reputation rating attached to it, which is recorded in the object and can only be modified by the reputation server. Agents are founded on a history of rehabilitation. Items are linked to their owners. If the owner purchases and integrates a new item, the base's relevance will be comparable to other SIoT goods owned by the same individual. Credits are used by nodes to get access to services. If a node offers the right service, it is compensated with extra credits as a commission. If he responds rudely, he should acknowledge other nodes as a loss of money. The commission and lost prices serve as a guarantee of good conduct. Because the information on the objects is divided down in a widespread manner, this strategy assures an increase. However, it simply considers social interpersonal relationships

and offers the same level of trust for all objects possessed by the same individual. Objects' finite limit and computing power, as well as their energy usage, are ignored.

Chen et al. (2016a) proposed a TM-based rule based on TM critical criteria to assess trust response: Reliability (according to direct or indirect evidence, whether an item is trustworthy), Partnership (related to the level of social interaction in a community with friends such as social media) and Community Of interest (based on shared interests and aspirations or other similar skills that existed among the objects placed in a collaborative group or community (e.g. a place of cooperation or collaboration), but the lack of this study is that they do not look at solid environmental issues.

Chen et al. (2016b) introduced three types of social interventions based on proprietary interaction, including Friendship, Social Networking, and Community of Interest relationships, based on shared interests. In addition, the strengthening of the anti-bullying service plan was considered. However, the limit of this work is that they do not look for ways to attack.

Chen et al. (2019) propose a hierarchical trust management scheme for IoT cloud applications. It has a three-dimensional cloud-based gadgets configuration that enables the IoT device to share its service information and social interactions with another IoT device and question the reliability of the IoT device using a local cloud from the cloud. This function prioritizes the "subjective" reliability test design that allows the designated IoT device to rely on another IoT device by incorporating the device's visibility and other IoT device recommendations. Furthermore, recommendations are rated based on the IoT device's public relations with its compliments.

2.6 Summary

This chapter provides a systematic overview of the literature on IoT, SIoT, and Trust. It intended to examine trust management strategies in the IoT in a systematic way. It describes IoT based application of smart home, city and healthcare. Furthermore, the method for describing and categorizing the trust management method is offered. It explains how the trust is used in other domains like WSN, MANET, VANET and cloud. This chapter describes, different techniques of trust based IoT and SIoT system.

CHAPTER – III

TRUST MODEL IN IOT AND SIOT

3.1 Introduction

The basic characteristic of IoT devices is that they may be found anywhere, at any time, making communication and computing in the information and communication sector omnipresent. IoT is the interconnection of physical objects, such as smartphones, tablets, electronic items, automobiles that include software, sensors, controllers, and network connections, allowing them to gather and share data across a network. Because of the high heterogeneity in IoT communication, the messages being sent among the devices are vulnerable. This vulnerability involves the heterogeneous devices' lack of trustworthiness, integrity, and reliability. In addition, multiple security concerns arise due to the IoT network's various devices, multiple channels, and lack of standards and supporting protocols.

In a distributed context like the IoT network, identification, authorization, remote access, and non-repudiation are required to enable safe interaction. These devices must first create a secure communication connection before commencing interaction. These safe connections are generated when the communication devices have established confidence. To assure that the risks in these devices are remedied, and that continued communication is secure, trust must be established.

The SIoT concept is gradually established in various ways. The main premise is that IoT items belong to individuals in the network, and individuals provide services via their things. As a result, SIoT is a social network in which any device can form social interactions with others based on its owner's preferences. These entities, not only through themselves but also through the actions of their owners, expose their qualities to the public. The feature of SIoT is that it separates the two stages of individuals and things, permit gadgets to have their community networks and enable people to put restrictions on their gadgets to preserve their confidentiality, safety and maximise confidence through object interactions.

Trust can be described as a trustor's "guarantee" or "belief" in a trustee to accomplish a duty in a method that meets the trustor's expectations. In this view, when the trustee completes the work, the trustor partially understands the vulnerabilities and potential hazards. So it indicates the trustor's desire to be susceptible in the face of difficulties and dependencies. Trust interactions between social sciences and computer science in the SIoT environment are impacted by objective and subjective elements from both participants and ambient features. When considering trust in the SIoT environment, consider it from the standpoint of a trustor about society. Social connections, an individual's subjective perception, and the surroundings should not be overlooked.

3.2 Trust Classification Model in IoT

The enhanced security level designed to assure that all connected gadgets are secured is one of the essential requirements of the IoT system. The importance of security, privacy, and security when using IoT technologies is crucial (Mosenia and Jha, 2016). The Internet of Things system connects a variety of devices and generates a vast amount of data. Where IoT devices must interface with other gadgets for information security reasons, assurance that the device is dependable is necessary. As a remedy to these issues, researchers have devised a variety of solutions (Ammar et al., 2018). Many properties, on the other hand, can have both quantitative and non-measurable consistency and effect. As a result, trust is a very difficult notion to grasp. It has to do with other aspects of the object, such as its durability, beauty, dependability, availability, ability, or other characteristics. As a result, trust management is a greater challenge than defence. The actions of establishing, validating, and maintaining trust are referred to as trust management. Furthermore, Yan et al. (2014) said that confidence, safety, and anonymity are critical challenges in the burgeoning technological field of IoT.

Najib et al. (2019) divided the trust model into five categories, trust metric, trust source, trust algorithm, trust architecture, and trust distribution.

Trust Metric

The IoT system integrates multiple gadgets and generates a large quantity of information. Where IoT devices must interface with other gadgets for information security reasons, assurance that the gadget is dependable is essential. As a remedy to these issues, researchers have devised a variety of solutions. Quality of service (QoS) and social trust is the most commonly employed parameters in the trusted combo.

QoS Based Trust: Device trust testing uses metrics based on the QoS supplied to IoT gadgets, e.g., the device's ability to perform the requested service. Nitti et al. (2012) employ QoS trust metrics in the transactional process to assess the value of the trust. They also used another QoS metric related to the IoT device's calculation capabilities.

Social Trust: The Social IoT design can be considered of as a bridge among a conventional peer network and a social network, in which devices create social ties depending on the network of their owners. The social IoT system is inextricably tied to social dependency. Friendship, centrality, similarity, and community-of-interest (CoI) are only a few of metrics that have been utlitized in social trust. Nitti et al. (2014) presented a trust model based on centrality. One researcher proposes access control based on trust and centrality degree, which can be used in wireless sensor networks (Duan et al., 2019). A collection of community (thing) who distribute a frequent interest is characterised as a CoI. The CoI trust indicates whether a trustor and trustee device are members of the same social community or group. For instance, spatial relationships or co-operative spatial relationships (Chen et al., 2016a).

Trust Source

Investigators have hypothesised two primary sources of trust: direct trust and indirect trust. The communication of the IoT device with other gadgets is used to calculate direct trustworthiness. Based on the communication records between two devices, direct trust indicates the estimated value in the device's capacity to accomplish the required task. The degree of trust an object acquires from another item identified in earlier sense of engagement is known as indirect trust. Some academics use terms like reputation, recommendations, ranking, and review to describe indirect trust (Guo et al., 2017). The most widely used source of trust is the hybrid trust, a

mixture of direct and indirect confidence. Figure 3.1 shows the three types of reliability used by previous investigators to model the reliability of the IoT system.

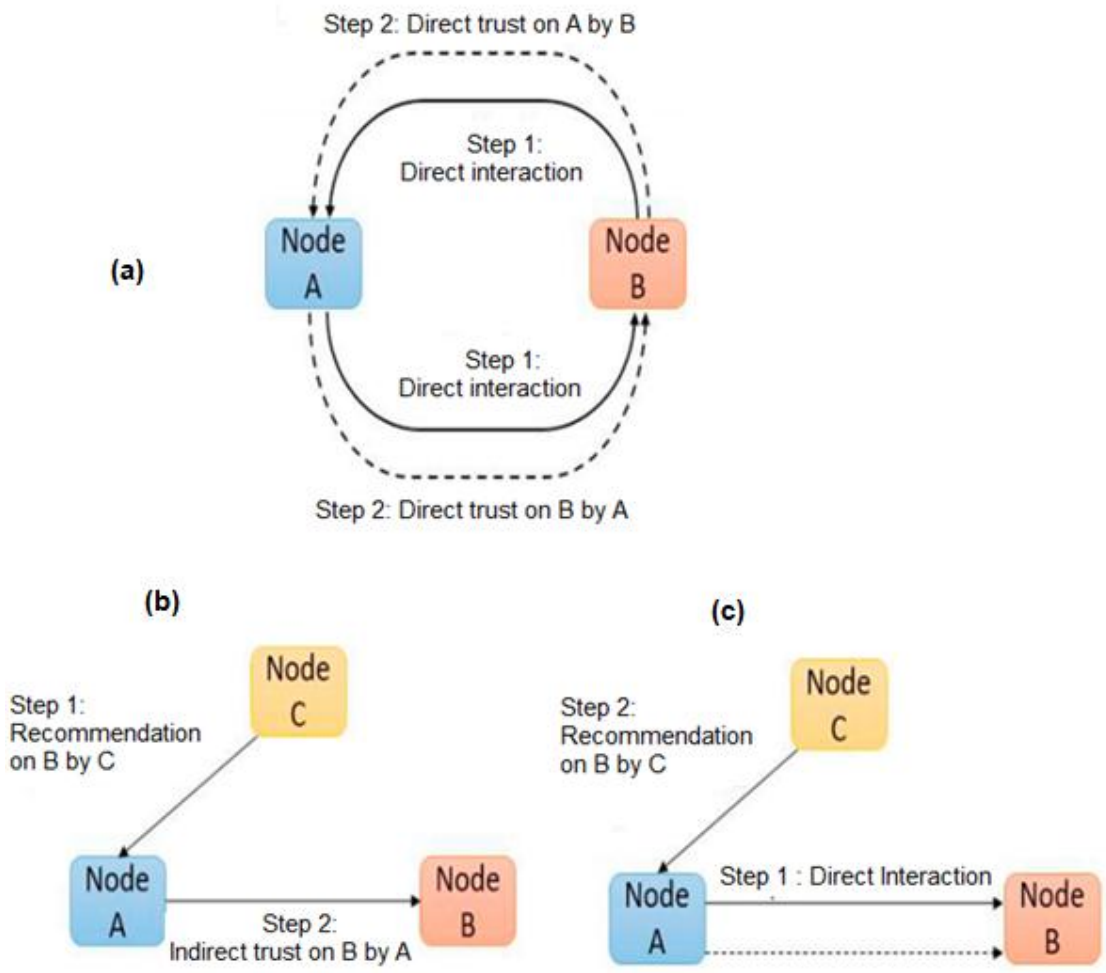

Figure 3. 1 (a) Direct Trust (b) Indirect Trust (c) Hybrid

Trust Algorithm

A trust algorithm is a self-examination or repute response from another IoT device that generates a trust-based confidence test. Algorithms and methods utilized to test trust include Bayesian considerations (Bao et al., 2013), fuzzy logic (Nitti et al., 2014), particle swarm (Chakraborty and Datta, 2017), etc. optimization algorithms such as ant colony (Sun et al., 2018) and multi-particle processing (PSO). Recently, a new algorithm has been developed to measure trust in IoT, based on machine learning (Jayasinghe et al., 2019).

Trust Architecture

When considering trust, one of the most significant aspects to examine is architecture. Because of the variety of IoT devices and their dynamic capabilities, there is no comprehensive measurement method for establishing IoT trust. Many trustworthy structures have been proposed by investigators, with central (Saied et al., 2014), power-allocation (Yuan et al., 2018), and cloud (Ammar et al., 2018)

Trust Distribution

The distribution of trust is linked to how an IoT node shares the results of its reliability tests to other nodes. Distribution may be managed at either the node or cluster level.

Node Level: In this distribution model, IoT gadgets independently broadcast reliability points to other IoT gadgets without using a connector or group header. Numerous investigators have employed a node-level method in their reliability distribution model, with Chen et al. (2016b)

Cluster Level: The hopeful spread of a system based on the IoT collection is compiled by the cluster's head. Yuan and Li (2018) proposed lightweight trust computing using this distribution model.

Table 3.1 shows the comparability trust model based on architecture, computation, metrics and performance measures.

Table 3. 1 Comparison of the trust-based model

Author	**Architecture Model**	**Computation Method**	**Trust Metric**	**Performance Measures**
Joshi and Mishra, 2016	Cluster-based model	Direct and Indirect	community trust, collaboration index, selfish index	Trusted and untrusted routing table
Chen et al., 2016b	Hierarchical, SIoT	SOA-based IoT, Direct, indirect	Companionship, community contact, CoI	Scalability, convergence point in time
Yuan and Li,	Hierarchical	Direct, indirect	QoS trust, success rate,	Convergence time, task

2018	model		information entropy	collapse ratio, computational effectiveness
Caminha et al., 2018b	Node level, decentralized	Direct trust	Direct trust	Percentage of discovered resources.
Bhargava et al., 2017	Node level, decentralized	Direct and indirect trust	Trust and distrust level	vagueness of trust due to malevolent vehicle
Jayasinghe et al., 2018b	Social IoT	Machine learning-based method	Cooperativeness, occurrence, centrality	Distribution of trustworthiness
Ammar et al., 2018	Cloud-based IoT	-	Architecture, application design, hardware	-
Wang et al., 2017	Node level trust, decentralized	Attribute-based access control	Access control strategy	The relation among rule and decision time

3.3 General Model of Trust in SIoT

This section describes a typical model of reliance on social IoT. Trust is a trustee method in the social IoT evaluate the level and assumption of the trustee's capacity and decisions, including purpose, opting to delegate tasks to a trustee, and manipulating the trustee's conduct to reach a goal. The supervisor allow the threat of being in danger by entrusting the trustee to a particular context. Loyalty testing is the same between trustee and supervisor. However, it based on the work environment and is influenced by the penalty of behaviour and environmental vagueness (Lin and Dong, 2018).

Trustor and Trustee

Trustor, Tr in IoT is a purposeful mediator who has a objective, his require, and other mediator attitude and events. Depending on its viewpoint to other mediators

and their perception of the circumstances and the surroundings, the trustee may issue and transmit the services and assess the outcomes. The administrator, Te, is an IoT mediator equipped with gadgets which create a specific effect resulting from their behaviour. Trustee Te is another independent agency recognized by Trustor Tr and is away from the direct control of Tr. Both the trustee and the trustor should act in a manner that is compatible with their trust relationship.

Target

The trustee relies on the trustee's action to attain the purpose and convene their necessitate. The trustee is motivated to give responsibilities to the trustee and is optimistic about the outcome. Waiting is a good thing if a trustee can produce the desired results consistent with achieving that goal. Expectations are wrong if the outcome puts dissatisfaction and risk against the objective. The trustee aim to use the positive effects of the trustee's action and make appropriate resolution.

In the case of SIoT, trustor Tr does not have complete control over trustee Te. The Trustor (Tr) puts itself at risk by assigning services to a trustee (Te) and is at risk. The loyalist is in danger of becoming a victim of failure. The trustee may not act, or the action may not have the preferred effect. There is vagueness in the information of the trustee. Further, based on the trustee, the trustee is showing to the probable harm caused by the trustee.

Evaluation of Trustworthiness:

The trustor tests the trustee's loyalty to perform his task of accomplishing a particular purpose. Traditionally, honesty is the property of a trustworthy trustee.

In SIoT, both the trustee and the trustee can understand, and consequently the integrity test is consistent. Trustor Tr examines trustee Te and symbols in Te attitude and expected action to achieve the purpose of Tr. At the same time, the trustee Te can check the trustee Tr and say to Tr the amount of trust in the interest of Tr. There are two types of social IoT loyalty tests, namely, pre-test and post-test. The trustee and the trustee assess first before the transfer action according to context and previous experience. The trustee attempts to recognize the most powerful trustee, and the trustee makes an effort to identify the malevolent intent. After the designation, the trustee and the trustee conduct a post-test evaluation of results and environment.

Testing is based not only on success but also on profitability, harm, cost, and environment.

The decision, Action, and Result

In the SIoT, confidence is a fundamental method that involves decisions, actions, and outcomes. Trust is more than just an opinion or attitude by a different mediator. It has its ethical characteristics in management verdict making and the next course of the manager. The trustee assesses probable trustees, evaluates the probable results, estimates the threats and costs, and sets the referral momentum. After its verdict, the trustee submits and relies on its action to create the preferred outcome. If the conductor's behaviour predicts, the result of the trust results from an predictable action that can be used to achieve the trustee's purpose. In practice, the outcome may depart from what is probable, affecting the relationship among the trustee and the supervisor.

Assume that trustor Tr can estimate trustee Te of performing job ₸. The predictable gain attained by Tr is $Gain_{Tr \leftarrow Te}(₸)$ if Te achieves job ₸. The predictable damage caused by Tr is $Damage_{Tr \leftarrow Te}(₸)$ if Te fails to perform the job. The predictable cost of Tr is $Cost_{Tr \leftarrow Te}(₸)$ despite Te's success or failure. The predictable outcome of Te executing task ₸ that Tr can exploit is $Result_{Tr \leftarrow Te}(₸)$ which is a function of $Gain_{Tr \leftarrow Te}(₸)$, $Damage_{Tr \leftarrow Te}(₸)$ and $Cost_{Tr \leftarrow Te}(₸)$. The predictable gain, damage and cost can be expressed in terms of QoS/QoE constraints, such as delay, jitter, bandwidth, packet loss, procurement cost, dependability, effectiveness, users' perspective of the overall value of the service provided, etc.

Trustor Tr has its goal $Goal_{Tr}$. If the predictable outcome is associated with the goal, e.g., $Result_{Tr \leftarrow Te}(₸) \subseteq Goal_{Tr}$ Meaning the predictable outcome is a detachment of the goal, trustor Tr assigns trustee Te to do the task. The result of Te's action that can attain Tr is the real outcome $Result_{Tr \leftarrow Te}(₸)$. The concrete outcome may be dissimilar from the predictable consequence. Due to the need of a predictable result or the addition of side effects, the real outcome may not be a subset of the goal, i.e., $Result_{Tr \leftarrow Te}(₸) \not\subseteq Goal_{Tr}$The expected gain $Gain_{Tr \leftarrow Te}(₸)$, damage $damage_{Tr \leftarrow Te}(₸)$ and cost $Cost_{Tr \leftarrow Te}(₸)$ need to be adapted accordingly.

Context

Trust depends on the content. That is, the trustee trusts the trustee in a particular circumstance for their conduct. If the context changes, the loyalist's verdict may vary. The context consists of two elements, namely, the kind of activity and the environment. For example, in social IoT, Trustor Tr can trust Trustee Te for one job but not another. As a result, the agent's loyalty to one action may differ from that of another. Therefore, the reliability test requirements to be applied to that particular assignment.

The setting is an external entity. In the method of trust, there is a significant threat to the vagueness of private agents' actions and environmental uncertainty. The Trustor Tr examines the trustees and makes a decision somewhere. The environment affects the inspection process of trust Tr. Nature also affects how the Te-bearer acts, whether purposely or not, and how they produce the outcome. Te's honesty varies from place to place. In IoT, the setting can be a supportive communications or an external disruption. The process of confidence lies in both the type of work and the setting. The process of trust and all the components are shown in Figure 3.2

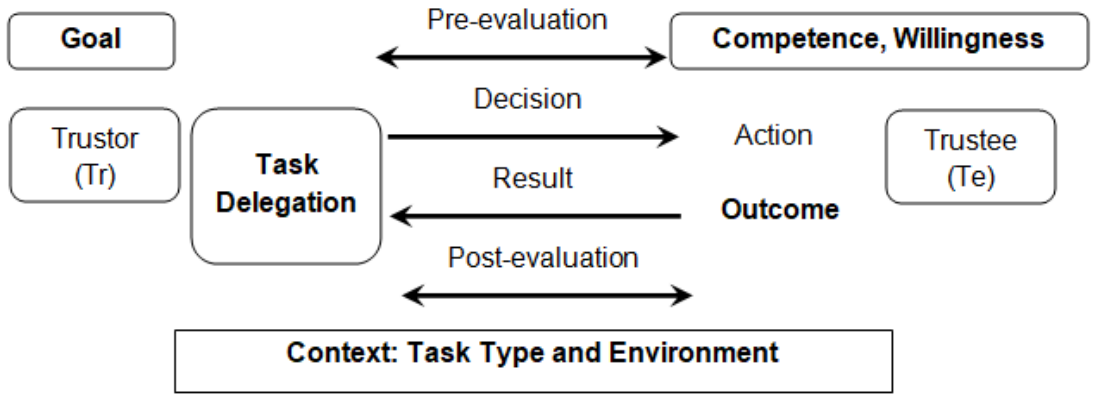

Figure 3. 2 Trust Process (Lin and Dong, 2018)

The concept of trust is more than one value as trust. It is a dynamic method that engages trust, and flexibility rather than a fixed perspective. Trust is an attitude, a test, and a decision and an action full of unexpected risks.

3.4 Trust Classification in SIoT

A trust is a trustee's trust that a trustee will offer or fulfil a confidence policy as per the trustee's expectations within a particular time frame. In the SIoT setting, trustor and trustees can be individuals, gadgets, method, apps and services. The rate of confidence as a faith can be complete or degree of trust. The purpose of the trust is in broader thoughtful. It could be a trust for action or information provided by a trustee. The Trustor's potential are intentionally considered to contain certain needs for a well-to-do (to some extent) goal of trust.

Figure 3.3 shows the division of trust in the SIoT (Amin et al., 2019a). The trust is divided into the consolidation of trust, the renewal of hope, and the formation of trust. The consolidation of Trust consists of three groups: Bayesian systems, superstition, and weight-bearing power. The Trust update is divided into event-based and timely processes. Ultimately, the formation of trust is divided into one trust and one trust.

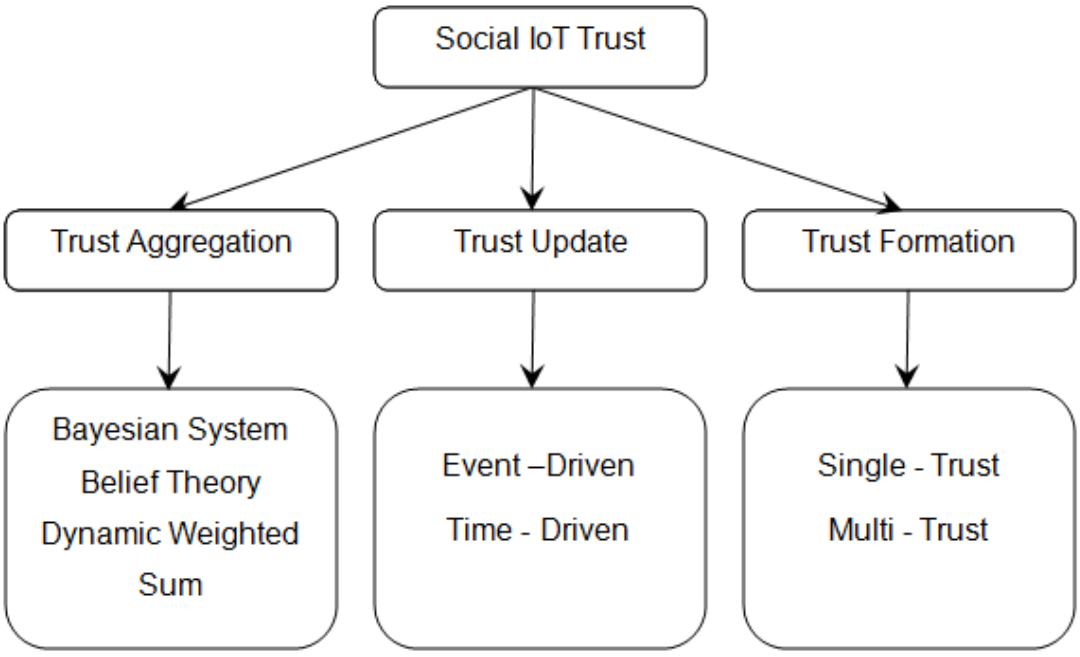

Figure 3. 3 SIoT Trust Classification

3.4.1 Trust Aggregation

The collection of valuables based on purchases through testing is known as trust aggregation (Abdelghani et al., 2016). It is depends on comment or observations.

The model of confidence integration was consider concurrently with Bayesian programs, statistical weights, and belief theory (Goo et al., 2017).

Bayesian Systems

In terms of opportunity definition, a random amount is considered the dependency value followed by the distribution of opportunities. when an incident occurs, its constraint is modernized consequently. Since Bayesian programs are based entirely on mathematical information, they are accepted in computer science and other fields (Abdelghani et al., 2016).

Jøsang (2001) introduced a system based on random values and calculated the reliability value between (0, 1). Then, a beta distribution scheme was followed, in which the sum of all the results was mapped to parameters (0, 1). The purpose of this study was to calculate the value of the dependency scale. Ganeriwal et al. (2008) introduced a similar type of study, who used the Basis system to represent the reputation model. This model has been applied to the wireless sensor network. Their purpose was to calculate the sensor node value by taking binary values (0, 1), including positive/negative inputs. Their approach works on two types of attacks: voting and improper placement.

Belief Theory:

The theological category is the most popular method of gathering evidence (Abdelghani et al., 2016). This scheme is used to compute thinking and vagueness in the idea of opportunity.

Jøsang (2001) proposed a consistent logic model. This is a vision-based model. Yu and Singh (2002) suggested an independent system of agents based on the concept of Dempster-Shafer (Beynon et al., 2000). The major scheme in this work was to create a complete model based on confidence, distrust, and ambiguity. Opinion about a particular node a is displayed (b, d, u, a).

Other studies by Suryani (2016) argue a variety of variable, such as b, d, and u, representing belief, disbelief, and uncertainty, respectively. Weight, b + d + u = 1, and weights given is sometimes called the minimum. The basic level is estimated based on proof. In this case, general trust is identified as an predictable likelihood and is

estimated using a mathematical formula, such as b + au. At last, subjective parameters can be used disjointedly to merge option, such as reduction and compliance value.

Dynamically-Weighted Sums:

Calculating compiled proof using weighted amounts is currently a trendy practice. Many reputable programs include ranking/opinion using weighted statistics. However, characters with a improved reputation (e.g., trade-offs) have a maximum weight. Many schemes can be used openly to capture the combined response using powerful weight calculations. In such cases, those with a enhanced repute are given higher weights. Nitti et al. (2014) presented a response solution to estimate the inconsistency of indirect trust by providing fidelity as a measure. Chen et al. (2019b) used similarity as the weight of a reliable indirect combination. In addition, reliable direct and indirect structures were leased. The given weights can be adjusted vigorously through the first design stage.

Trust Update

If the value of the trust is reviewed, it will be pretentious. There are two categories: event-driven and time-driven.

Event-Driven Approaches

In this way, behind the occasion takes place, the reliable node information is updated accordingly. In addition, whenever a service is requested, the cloud trust manager sends a response regarding service quality. It is called a meeting-based setting since suggestion can be sent upon receipt of the application.

Ben Saied et al. (2013) has presented a centralized trust manager. This confidence manager can keep a record of trusted data on IoT devices. Their system is smart because it automatically selects an IoT gadgets to respond to a service request. Xiao et al., 2015 argued a model generally based on fame. It has a reputation for reliance on something. The repute constraint is considered a SIoT guarantee. In the first case, the request is made to one of the other items in the network. Their goal is to discover a guarantor. The task of the guarantor is to offer a wide range of services. Later, it uses repute to determine confidence. Researchers Chen et al. (2016) mimicked a model in the real world and accomplished that their confidence model

could be used in various IoT public spaces. First, their model is used to identify malevolent nodes, after which it will also force certain punishments.

Time-Driven Approaches

Evidence is collected from time to time based on recommendations made by friends and in person. Then, the Trust is reviewed using the trust merger method. At this point, if no proof is gathered, then the decay of trust is used over time. The motive is that someone can trust current information. The decay work was based on the interpretation of things. This activity can adjust the level of self-reliance over some time (Nitti et al., 2016). This function is built with observance in mind particular application necessities.

Chen et al. (2014) proposedd a reliable communication society through MANET. A powerful model which can be used to find out from previous experiences has been introduced. This approach can adapt to changes in environmental setting and thus, guarantee increased efficiency. Their suggestion is practical in node failure and cannot take events in termination cases. It has been proven to help improve app performance by reducing the false positive and inaccurate rate on mobile nodes. Finally, it was said that QoS was developed through this program.

Trust Formation

The notion of hope building is easy: it is an asset of compassion, passed on to a individual called a trustee. generally, the trustee manages and manages (or simply does) own this property. Occasionally, hope formation is used for the same benefits, or sometimes it is used to help. The formation of trust is divided by one trust or multiple trusts.

Single Trust

Single trust is truly regarded as the one trustworthy asset that is considered a confidence protocol. In this context, service quality is supposed to be the most important metrics for IoT service-based applications (Wang et al., 2016). Furthermore, in SIoT, QoS is often pretentious. Therefore, confidence is the association among the applicant and the service provider. In this case, easily assume that relying on a community-based IoT system always works collaboratively.

Multi-Trust

It uses trust in a variety of ways. It means that there are many areas of confidence that have been considered for the construction of trust. For instances, Guo and Chen (2015) looked at a variety of structures of mutual confidence, such as loyalty, closeness, and selflessness.

3.5 Trust Computation Model in SIoT

The SIoT proposes several trust management programs. For example, Nitti et al. (2014) described a system of trust and independence to gain trust in the SIoT setting. The confidence of every exacting place was assessed by combining three key factors: size, opinions, mutual friends, and shortest experience. However, the impact of every of these aspects of the merger method was confirmed by assured aspects of the measurement that are very difficult to detect, mainly because dependence based on many difficult constraint, namely, circumstance, occasion, resources, and situation.

Chen et al. (2016a) proposed a series of trustworthy SIoT system rules. To gain complete trust, it uses direct observing and indirect recognition from user with metrics for the same social function, i.e., community links, truthfulness, and interested community. In addition, the same combination, a flexible filtering system is considered to combine direct and indirect visualization with the constraints of each view. On the other hand, the author did not apply the expected procedure to a wide range of dynamic environmental conditions, where allocating survival parameters is a difficult task.

Abderrahim et al. (2017) employed public interest as a metaphor for public trust to find a way to manage objectives for IoT purposes, in which the Kalman filter was utilized as a tool to measure the confidence value of a node prior to communication. Yet, the amount of combined confidence is estimated using a straightforward formula with direct and indirect reliability characteristics.

Truong et al. (2017) presented a reliability model that uses the same social characteristics regarding common interests, reliability, and cooperation in assessing trust points for a same node. To gain direct trust, a weight-bearing measurement was utilized to combine both present and history. However, the form did not consider the indirect recognition or suggestions from other nodes in the system that are important in the delivery of IoT services.

The content-based community support model (Rafey et al., 2016) is designed for IoT reasons by allowing for social interactions between communities. Using a node trust rating, a direct and indirect view is used with the transaction context. To acquire a particular measure of reliability, a weight-bearing measurement was utilized for the combination. Jayasinghe et al. (2019) suggested a trust model based on the node public profile, in which various social factors were collected to acquire a node confidence value. Further, the machine learning algorithm is used to compile only a reliable and insufficient metric to determine whether a node is reliable or not.

This section describes the computer model details of an effective and efficient trust management system in the SIoT proposed by Sagar et al. (2021).

This trust model has two measures, Direct Trust and Indirect Trust Measure, shown in Figure. 3.4. Direct trust gives the impression of direct attention, while indirect trust gives the repute of the nodes in the network. The trustor node trust (trustee) in respect of n j (trustee) is indicated by T_X (i, j), where X indicates social features such as friendship, CoI, reward and cooperation. The sort of T_X (i, j) varies from [0, 1], where value closest to 0 designate infidelity while values around 1 specify reliability. After combining every T_X (i, j) features from direct communication with the machine learning algorithm, the outcome is stored in a storage area and employed as a direct confidence point. With indirect confidence, trustor needs direct confidence from other nodes.

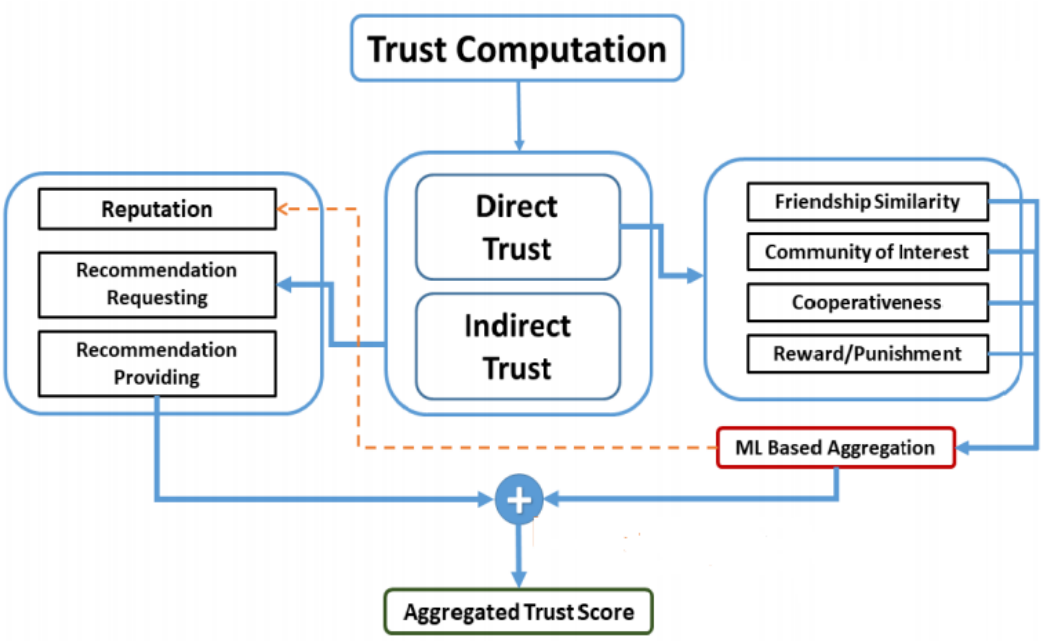

Figure 3. 4 Trust Computation (Sagar et al., 2021)

3.5.1 Direct Trust Metric

It is used to give an immediate impression of a trustee before a partnership. Although a trustee may not be tested for a wide variety of characteristics, in this work, four main attributes of each trustees' assessment concerning the trustee have been identified and described as follows:

***Friendship Similarity*:** Friendship equality symbolizes social relations concerning the interdependence of the elements. It measures the value of an object, among other things, in terms of a particular function and specific content. This item of property is considered as:

$$T_{F_{sim}}(i,j) = \frac{\left|F_i \cap F_j\right|}{|F_i| - 1}$$

When F_i and F_j refer to a number of friends of node i and j.

Community-of-Interest: This type of feature represents the relationship of places about communities or groups of public interest. Therefore, nodes with a higher social value have more opportunities to communicate to build a trusting relationship. The community-based trust of the two areas counts as:

$$T_{Comm_{Int}}(i,j) = \frac{\left|C_i \cap C_j\right|}{|C_i|}$$

Where C_i and C_j represent a group of node i and j communities.

Cooperativeness: Indicates whether the trustee is working with the community or not. Refers to the degree of stability in the communication among nodes. Cooperativeness based trust is listed as:

$$T_{cop}(i,j) = T_p \log\left(T_p\right) - (1 - T_p)\log(1 - T_p)$$

When Tp represents a fraction of messages during interaction

Reward / Punishment: To maintain both trustworthy relationships and to punish areas of misconduct, the applicable reduction formula is used to provide incentives to trusted nodes and fines for misconduct such as:

$$T_{Reward}(i,j) = \frac{|Int - Int_U|}{|Int|} e^{-(\frac{Int_U}{Int})}$$

Int indicated the overall amount of communications, and IntU calculates the number of failed connections among node i and j.

The final direct confidence computed as,

$$T_{Direct}(i,j) = w_1 T_{F_{sim}}(i,j) + w_2 T_{comm_{Int}}(i,j) + w_3 T_{cop}(i,j) + w_4 T_{Reward}(i,j)$$

Where w_1, w_2, w_3, w_4 are weighting factors.

3.5.2 Indirect Trust Metric

It is used to find trust depends on the views of other nodes in the network. However, the items' repute varies from node to node; consequently, it is not advisable to look at every nodes in the network to use the administrator's repute. Therefore, a repute assessment is requested from at slightest one node with the same partner between trustee and administrator.

The algorithm for estimating points of reliability is highly dependent on direct reliability. If a direct confidence is 0 or unreliable and most suggestions are unreliable (|U|) or neutral (|N|), the node is unreliable. where, neutrality indicates that the node is unreliable and unreliable. In addition, if the direct trust is 0 or unreliable and the amount of reliable suggestions (|T|) is greater than the unreliable suggestions, i.e., (|T|> |U|), then it does not mark the node as immediate. As an alternative, a proportion of reliable recommendations (PT) is calculated ($P_T = \frac{|T|}{Total\ Recommendations+1}$) and if PT is > threshold (θ) (0.7), then the node is noticeable as reliable. If PT exceeds the limit (θ) (0.7), the node is marked as reliable. The amount depends entirely on each application, and the cause for such a high case value, in this case, is to give advanced influence to the fund node than to suggestions from other nodes in the network to deal with the problem of good word and voting attacks.

If the direct trust is one or trusted, check if the node is trustworthy or based on the following status (| T | ≥ | U |) || (| N | ≥ | T | && | N | ≥ | U |). If the node is not trusted, then count the unreliable recommendations ($P_U = \frac{|U|}{Total\ Recommendations+1}$). PU value is large or equal - the node is not reliable; otherwise, the node is reliable.

Finally, if the direct trust rate is two or neutral, it means that the trustee node does not have a trustee and that the reliability of the node is determined based on recommendations. Finally, if | T | > | U |, the node is noticeable as trusted; or else, it is not trusted.

3.6 Summary

This chapter presents a breakdown of reliance technique for relying on IoT systems. Divisions are based on confidence factors, including confidence metric, trust structure, resource, algorithm, and trust distribution. Reliance on SIoT is shown as a vibrant method. It consists of the relationship of the six basic ingredients, namely, trustee, trustee, purpose, loyalty test, verdict and its following action outcome, and environment. It also describes a computer-assisted reliability model expected to deliver key reliability features concerning the SIoT domain. Next, to combine trust, data was labelled using k-means integration to identify reliable and unreliable interactions.

CHAPTER – IV

TRUST LEVEL COMPUTATION MODEL FOR IOT

4.1 Introduction

The Internet of Things (IoT) is a model which describes an ecosystem in which various physical things connect and collaborate over the Internet to create new services (Gubbi et al., 2013). By saving energy, time, and cost, the Internet of Things strives to create a more creative environment and a simpler living. Expenses in various sectors can be lowered using this technology. IoT has become a major trend in recent decades of massive investments and numerous studies (Mahdavinejad et al., 2018). Industry estimates predict that by 2020, the IoT will have a total installed base of around 212 billion gadgets (Dorodchi et al., 2016). The IoT expansion take a amazing outcome to a variety of fields, such as smart cities (Memos et al., 2018), smart healthcare (Catarinucci et al., 2015), intelligent transportation, cellular communications (Elsaadany et al., 2017), data mining, industrialized, and environmental observing (Din et al., 2019). This high degree of variability, along with the IoT system, is seen to pose a security risk to the present Internet, which allows humans to connect with machines (Yan et al., 2014). Because of its inadequate computing capacity, traditional privacy and security approaches and provisions fail to meet user needs.

Trust is a abstract concept having varying meanings depending on participants and settings, as well as measurable and non-measurable aspects. Because there are so many different types of trust definitions, it's hard to come up with a universal symbol that works regardless of individual preferences or circumstances. In practice, trust is viewed as a quantitative value represented by a trustor-trustee relationship, articulated in a exact circumstance, assessed by trust metrics, and analyzed by a technique (Truong et al., 2016).

The emerging IoT is highly challengeable in construction trust and trust management in an surroundings with heterogenous gadgets with limited storage and capacity and may fail due to this limitation. Trust management help the system to

overcome user dissatisfaction, uncertainty, and risk in consuming IoT services. It supports reliable data mining and enhances information privacy and security (Truong et al., 2016). Trust management includes forming information for decision, criteria evaluation based on a trust relationship, evaluating existing trust, monitoring dynamic change in trust relation, active context study (Bello and Zeadally, 2016).

These fields include applications such as surveillance of health data, smart health care services, personalized well-being, and binding site and rescue (Borgia, 2014). Additionally, IoT devices for environmental health are rather inexpensive. They can give significant assessments for numerous environmental factors, such as CO levels, temperature, hydrocarbons, pollution, noise, chemical smells, perfumes, and so on, when integrated with a smartphone application. Medical IoT devices are predicted to play a key role in providing outstanding assistance in day-to-day treatment since environmental assessment is directly related to the healthcare of specific disorders and overall health.

Despite the potential benefits of IoT based health monitoring solutions, these devices raise severe issues in data accuracy. For instance, fraudsters or equipment, may purposefully submit incorrect sensed information for their own gain. As a result, trust conservation and abnormality detection technologies must be designed to support the data quality acquired. For this reason, this chapter explains a patient monitoring service, which computes the trust level of each device using trust properties. In addition, to calculate the trust level, this chapter uses four metrics: success rate, completeness rate, data quality and reward rate of sensed information.

4.2 Trust Computation Model

Guo et al. (2017) propose five architecture dimensions for IoT confidence computation models: trust composition, trust dissemination, trust accumulation, trust modification, and trust creation. Figure 4.1 shows the classification of trust computation models.

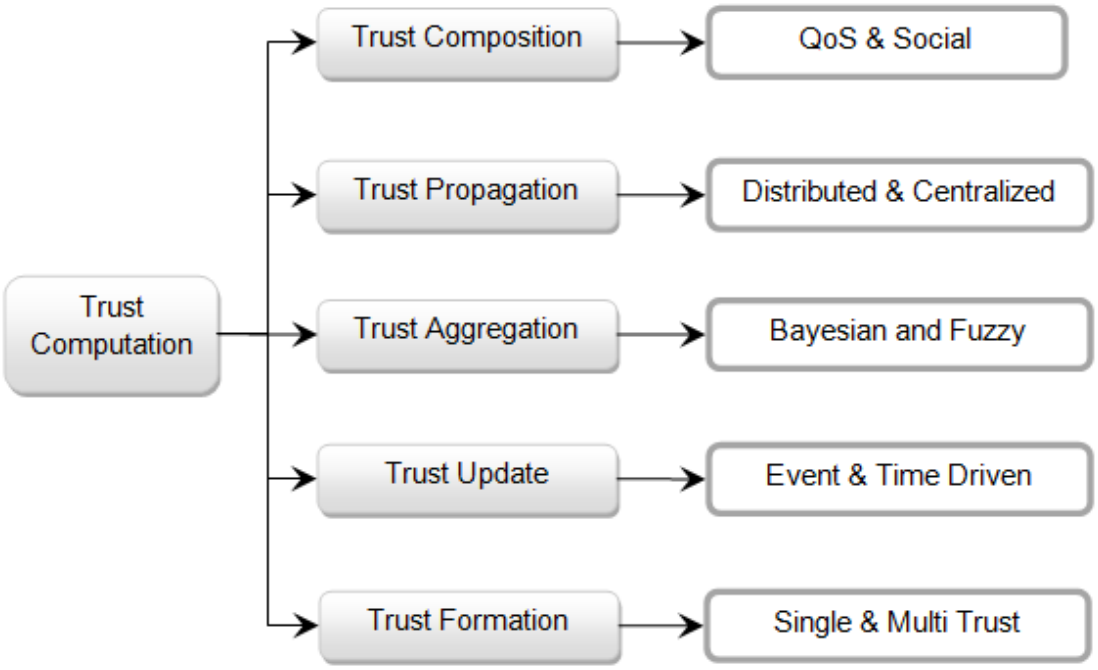

Figure 4. 1 Trust Computation Model

Trust Composition:

The kinds of parameters, whether QoS (Nitti et al., 2014) or Social (Chen et al., 2016b) type's (quality) connected to the efficiency of the node, and the interaction among nodes, is determined by trust composition. Energy usage, load balance, and packet ratio are only a few instances of QoS. Friendship, colleague, and community of interest, are instances of social parameters.

Trust Propagation:

Data packet, transaction details, profile, friend list, and other data must be forwarded by network nodes. There are two types of confidence dissemination schemes: distributed (Chen et al., 2011) and centralized (Saied et al., 2013). The information is delivered to all nodes without the oversight of the central authority during distribution. In contrast, centralised propagation occurs exclusively with requestors and is controlled by centralised administration.

Trust Aggregation:

Trust information gathered via self-observation or comments from others is combined in trust aggregation. Weighted sum, belief theory, Bayesian inference

(including belief discounting), fuzzy logic, and regression analysis are some of the most common trust aggregation techniques (Jsang et al., 2007).

Trust Updation:

The value of recent trust reports is higher than that of earlier reports. The majority of the time, trust reports are updated on a time or event basis. Reports created a long time ago are updated when a period of time has elapsed, and in event-driven systems, the update occurs when an interaction event occurs.

Trust Formation:

The overall degree of confidence is determined by a single or a combination of elements (Chen and Guo, 2014). A single trust is formed when just one trust property is utilised to assess absolute trust, while a multi trust formation is formed when many trust properties are used to assess absolute trust.

4.3 Trust Properties

A trustee's qualitative or quantitative value estimated by a trustor for a particular task in a given context during a certain time is referred to as trust (Jayasinghe et al., 2017a). Figure 4.2 depicts a standardized confidence model. Centred on three trust metrics: expertise, experience, and credibility, this generic model illustrates the trust acquisition and assessment process.

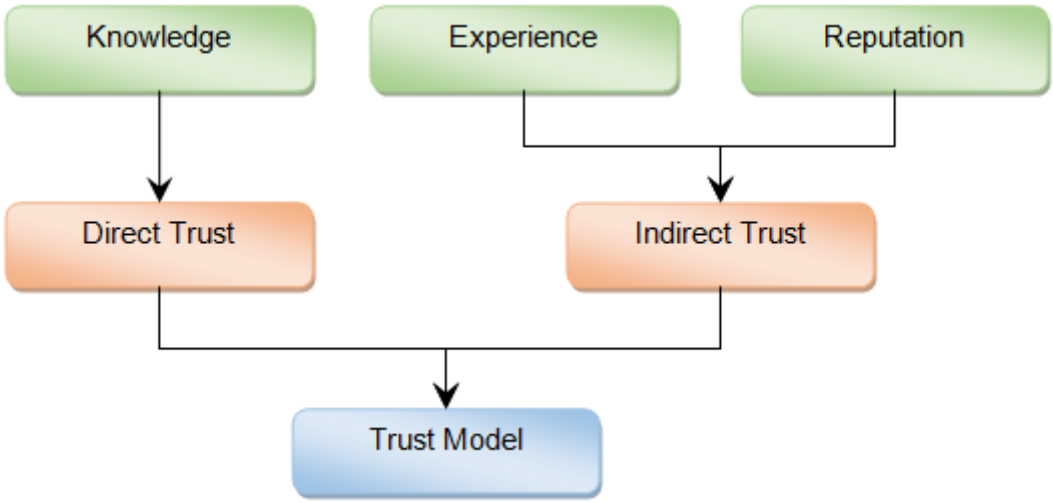

Figure 4. 2 Generic Trust Model

The information metric encompasses all facets of direct trust assessments, including trustees' impressions before a meeting. Relationship, Willingness, Spatial, Persistence, and Trust are social traits, while Disposition, Competence, Fulfillment, Temporal, and Dependence are non-social qualities. The experience measure is based on personal observation of only relations between a trustor and a trustee, including creditability and feedback. The credibility metric, on the other hand, represents the trustee's overall view. The two qualities of credibility are recommendation and ratings. The information metric, on the other hand, is the foundation of both practice and credibility.

The analytical strategy to determining the confidence value trustor i and trustee j can be depicted as below (Jayasinghe, 2018a)

$$K_{ij} = \alpha_1 K_1 + \alpha_2 K_2 + \cdots + \alpha_n K_n \qquad (4.\ 1)$$

$$E_{ij} = \beta_1 E_1 + \beta_2 E_2 + \cdots + \beta_n E_n \qquad (4.\ 2)$$

$$R_{ij} = \gamma_1 R_1 + \gamma_2 R_2 + \cdots + \gamma_n R_n \qquad (4.\ 3)$$

$$Trust_{ij} = \theta_1 K_{ij} + \theta_2 E_{ij} + \theta_3 R_{ij} \qquad (4.\ 4)$$

α, β, γ and θ are weighting parameters that standardize each metric among 0 and 1. K_n, E_n, and R_n stand for the knowledge, experience and reputation attributes, correspondingly.

Different players participated in trust management, each of whom acts individual or more roles. As a result, an player may be a trustor or a trustee or a third person who believes in another actor. Service requesters, providers, and responsible third parties are examples of such actors. A trustor should trust a trustee in a particular situation to create a trust relationship. When developing a rigorous trust management system, many trust assets linked to the various actors must be considered, as previously mentioned. The trust properties are described as follow:

Context properties: A confidence association is depend on the circumstances, which symbolizes every data which explains the condition of associated players. In different terms, the idea of the confidence, the requirements of trust (e.g., occasion and place), the part of the grown players, and the danger of belief are determined a priori. In some

cases, a trustor might trust a trustee to provide a sensed data; yet, the linked trustor cannot allow a trustee to perform various obligations in another situation.

Subjectivity Properties: Confidence factors that are challenging to scale and proctor. These characteristics are further included in cognitive or social confidence.

- *Trustor:* belief, (personal) desires or hope, subjective possibility, readiness, faith, disposition, character, feeling, purpose, belief, expect, trustor's confidence and dependence.
- *Trustee:* truthfulness, confidence, morality, motives and kindness.

Objectivity Properties: Confidence factors that can be estimated and observed. These properties are more interested in computational trust.

- *Trustor:* evaluation, principles or methods particular by the trustor to build a trust assessment.
- *Trustee:* proficiency, capability, safety, reliability, honesty, unavoidability, consistency, appropriateness, reputation (observed behaviour), power, accessibility.

Subjective, asymmetric, context-dependent, non-transitive, propagative, self-reinforcing are the critical characteristics of trust. Trust is a measure to SOA IoT as it is entities that can be malicious for selfish purposes. If trustworthy nodes are not identified, these malicious users may dominate the whole network. IoT supports many applications like healthcare, product management, innovative home application, etc. It collects and shares entity information on a context base as the trust differs according to context, i.e. separate trust value for each context.

4.4 IoT Healthcare

IoT is extensively accepted in several programs that its significantly increases in our every day lives. IoT technology is advancing in the health care examining scheme by offering efficient urgent situation services to patients (Rahmani et al., 2018). It is also used as an E-health program for a variety of purposes including early recognition of health problems, crisis information and computer-assisted treatment. Smartphones have become a very important part of everyday human life and these are

connected by a sensory health monitor (Wu et al., 2017). This diagnostic-based diagnostic program incorporates a variety of information into wards and diagnostic components, and enables this information to be properly and systematically managed by health care providers (Chen et al., 2018b). The IoT health care system provides effective scrutinize and monitoring that assists improve human resource management (Subramaniyaswamy et al., 2018). A wearable sensor installed in patients in an IoT-based health care scheme has a very restricted battery supply. Regular charging of these devices can be stressful for patients and require the involvement of a nurse, affecting the user experience (Yang et al., 2018) Another problem in recognizing health care is that information can be without difficulty damaged by invader or hijackers. Therefore, it is essential to enlarge a health care system that supports IoT privacy and should be integrated with patients in order to effectively transfer data (Elhoseny, et al., 2018).

Kumar and Gandhi(2018) includes 3-D formats to collect sensory data from portable devices, cloud storage and a predictor model based on the retreat of cardiovascular disease. Parthsarathy and Vivekandan (2018) are designed to monitor patients who have arthritis and to diagnose early. The proposed framework consists of three stages, the first stage is information collection from sensors. The second stage stores information in the cloud. The final stage is utilized to improve the information gathered, which includes inflammation and uric acid.

Kim and Chung (2015) designed and organized sensory tools in a typical living space and other places where patients with chronic illnesses lead every day life as a whole. This test does not process essential information, and it is a very expensive procedure. To lower the cost of the entire process, the method's architecture can be evaluated, and the sensor can be utilised rather than a camera. An outline of the IoT health architecture is displayed in Figure 4.3

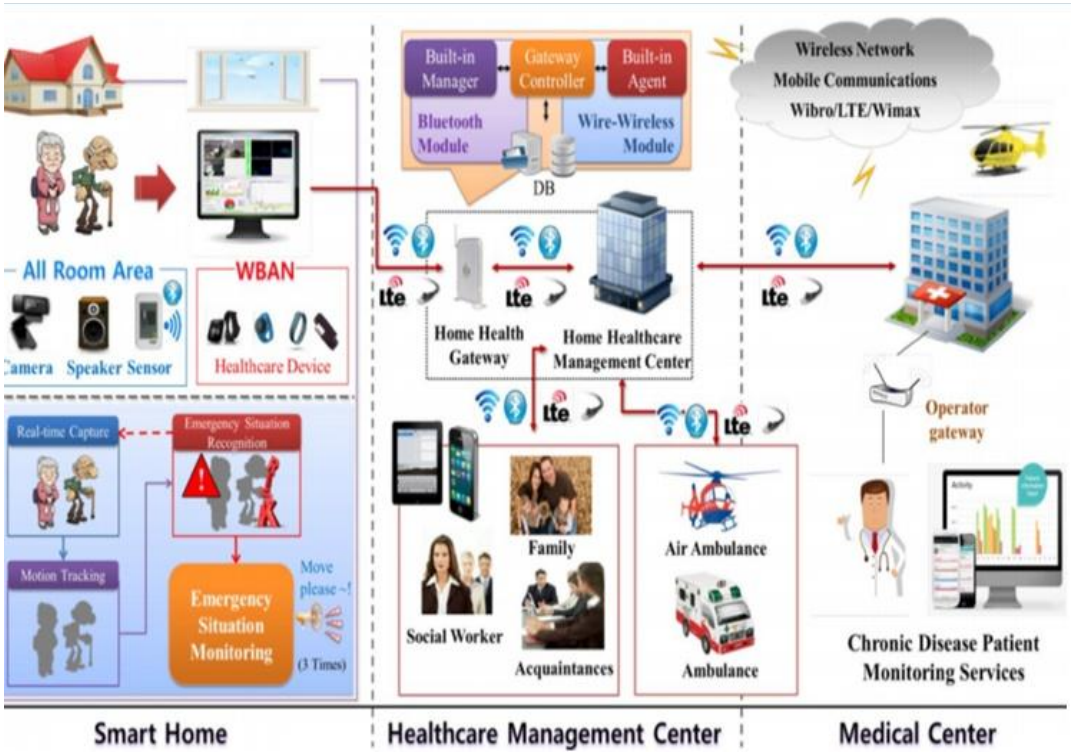

Figure 4. 3 IoT Healthcare Architecture

IoT is widely accepted for a variety of applications and offers a variety of health care system support including patient health checking, a diabetic household care system. The following are the major issues that arise in the health-care system.

- IoT allows for greater flexibility, for example, if a patient requires constant care, they can remain at home rather then going to hospital and be examined on a frequent basis using IoT technology. Some gadgets include nerves, are make feel uneasy in the patient's body.
- Data is transported from the sensor to the remote controller and then to the central controller, where distortion will degrade the data integrity. Better design aids in the transmission of data while minimising the impact on the environment. The data stream can also benefit from the audio reduction technique.
- The majority of ECG monitoring methods contain carefully controlled signal analysis. This raises prices and raises the chances of an acquisition mistake. Signal investigation can benefit from machine learning, which improves productivity and lowers costs.

- As the number of devices and applications grows, so does the need for more computational power, resulting in increased energy wastage and utilization. The optimal solution can be used to cut down on energy usage.
- Monitoring large numbers of users on IoT requires a lot of storage and a main frame, which can be conquer by store information in the Cloud. On the other hand, cloud-based IoT enlarge the difficulty.
- Another major issue with IoT is anonymity, as gadgets are prone to hacking. These are limited resources, and applying cryptography to them is challenging.

4.5 Proposed Trust Level Computation

This explains the proposed trust level computation model for patient health monitoring services. Figure 4.4 shows the system model. Each sensor node in the IoT network periodically senses patient health information like body temperature, BP, Heart rate, room temperature, air quality and noise level etc., The Gateway collects data from all the sensor nodes and sends it to trust evaluator for further processing. Trust evaluator receives and preprocesses the patient data and computes the trust value for each sensor node.

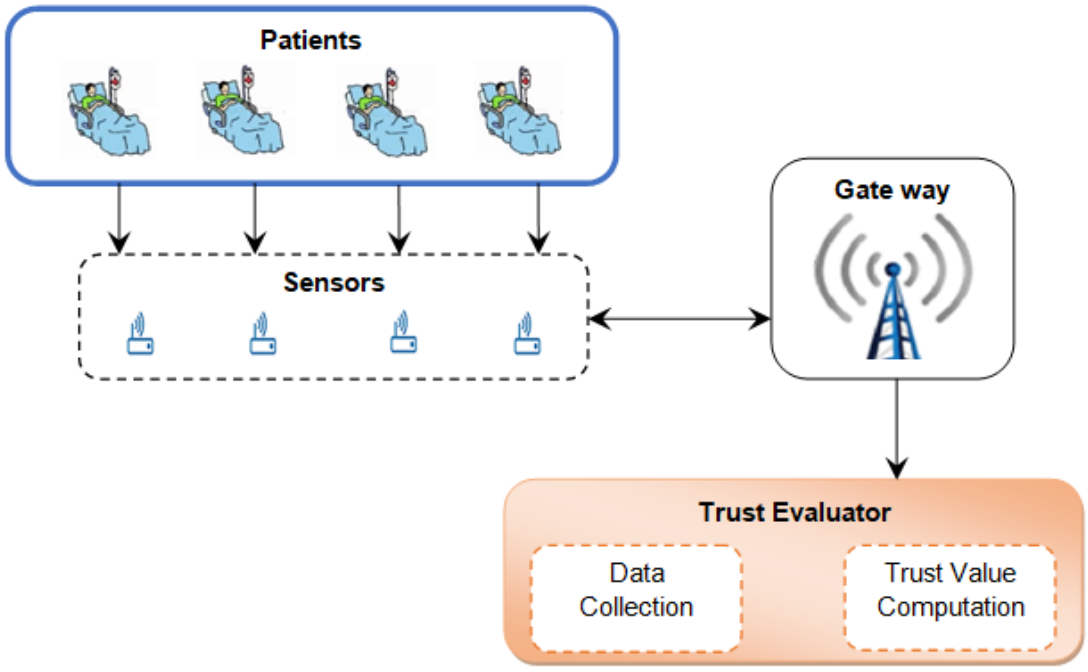

Figure 4. 4 Proposed System Model

The followings are the assumptions:

- Each patient has a sensor to examine medical data like heart rate, body and room heat.
- Only one Gateway is used to collect patient health information.
- The trust evaluator computes the trust value for each senor node for every time slot.

System Model

IoT enabled patient health monitoring system consists of M number of patients $P = \{p_1, p_2, \cdots, p_M\}$ with N number of sensors $S = \{s_1, s_2, \cdots, s_N\}$ who can sense a set of K attributes A= $\{a_1, a_2, \cdots, a_K\}$ for each patient. Table 4.1 shows the attributes list used in this chapter.

Table 4. 1 Patient Health Attributes

Attributes	Description
Room Temperature	Patient room temperature
Fever	Body temperature in degree Celsius
Heart Rate	Heartbeat readings
Respiratory Rate	Respiratory readings
Blood Pressure	Blood Pressure readings
Glucose Level	Glucometer adapter readings

Each attribute has its specified ranges. Table 4.2 shows the attributes of normal range values

Table 4. 2 Normal Ranges of Health Attributes

Attributes	Units	Normal Range
Room Temperature	Degrees Celsius	20 - 25
Fever	Degree Celsius	35-38
Heart Rate	Beats per minute	60-90
Respiratory Rate	Breaths per minute	12-20
Blood Pressure (Systolic)	mm Hg	80-120
Glucose Level (Fasting)	Mg/dl	70-140

For a particular time interval, these attributes are sensed using IoT devices and send to Gateway. Then, the trust evaluator collects all the sensed information from the Gateway and uses the mathematical model to compute numeric trust value (TV). The confidence value of each sensor is within the range of [0, 1].

Figure 4.5 illustrates the interaction sequence of the sensor and confidence evaluator. At time t, the sensor starts to sense information about patient health attributes. Then, the trust evaluator collects sensed information through the Gateway, computes trust value, and finally updates the sensor node's trust value.

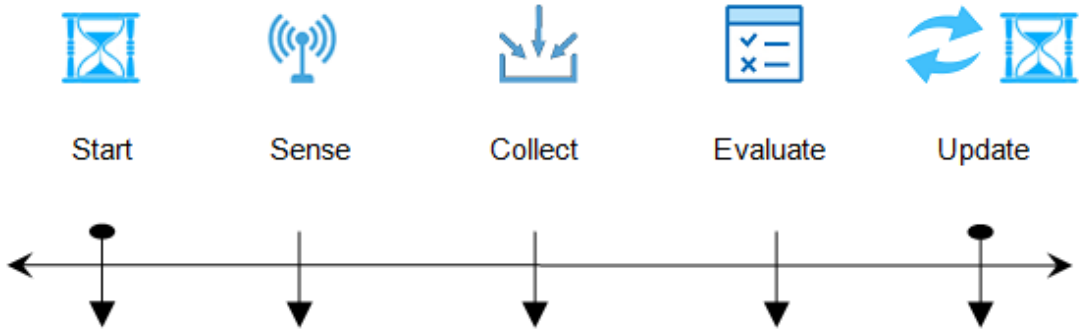

Figure 4. 5 Interaction Sequence of Sensor and Trust Evaluator at time t

Algorithm-1 explains trust computation for each sensor.

Algorithm-1 Trust Computation
1. Collect data from the Gateway
2. For each t in the timeslot
3. For each node, repeat steps 4 to 8
4. Compute Success Rate (SR) using equation (formula) (4.5)
5. Compute Completeness Rate (CR) using equation (4.6)
6. Compute Data Quality Rate (DQR) using equation(4.7)
7. Compute Reward Rate (RR) using equation (4.8)
8. Trust=SR+CR+DQR+RR/4
9. End For
10. End For
11. Get the Trust Value of each node

The algorithm uses four trust metrics to compute each sensor node's trust value in the IoT network. The metrics are success rate, completeness rate, data quality and reward rate. Each metric returns the numeric value within the range of [0, 1]. All the metrics are computed based on the sensed patient health information.

Success Rate (SR)

It is the primary factor to examine the credibility of the node in trust computation. The success rate of the node is used to predict the node behavior.

The success rate can be determined as,

$$SR(s) = \frac{\sum_{i=1}^{t}\left({}^{RP_i}/_{SP_i}\right)}{t} \qquad (4.5)$$

Where SR(s) = Success Rate of Sensor

t = Total Number of Time Slot

SP_i = Number of packets send to gateway for particular time slot

RP_i = Number of packets received in gateway for particular time slot

Completeness Rate (CR)

The completeness is nothing but to check whether the sensor node sense and send all the attributes to the Gateway or not.

The completeness rate can be estimated as,

$$CR(s) = \frac{\sum_{i=1}^{t}\left({}^{CP_i}/_{RP_i}\right)}{t} \qquad (4.6)$$

Where CR(s) = Completeness Rate of Sensor

CP_i = Number of complete packets received in the Gateway for the particular time slot.

Data Quality Rate (DQR)

It checks the accuracy of the sensed information. Sometimes the malicious nodes can send abnormal range values.

Data quality rate can be estimated as,

$$DQR(s) = \frac{\sum_{i=1}^{t}\left(\sum_{j=1}^{att}(checkAtt(j))/att\right)}{t} \qquad (4.\ 7)$$

Where DQR(s) = Data Quality Rate of Sensor

att = Total Number of attributes

checkAtt() returns 1 if the attribute value is correct, otherwise return 0.

Reward Rate (RR)

In order to examine the previous service experiences between a trustor and a trustee, every service provisioning system must incorporate a reward and punishing mechanism or a feed-back model. Here the reward rate is calculated as,

$$RR(s) = \frac{\sum_{i=1}^{t}(SP_i - CP_i/SP_i)}{t} \qquad (4.\ 8)$$

4.6 Experimental Result

This segment confers the simulation outcomes, including the study of statistical conclusions achieved in the preceding division. The simulation was carried with the aid of Java (version 1.8). The tests are conducted on a PC consisting of Intel(R) Pentium with a speed of 1.60 GHz and 4.0 GB RAM using Windows 7, 64-bit Operating System. The simulation difficulty is based on the amount of communications within the timeslots (set as 15) and the number of nodes (vary from 10 to 50). Initially, a network with ten sensor nodes is randomly generated using Java. Then the algorithm-1 is executed to find the SR, CR, DQR, RR and final trust value for the various time slot.

Two experiments are conducted for trust evaluation, one for regular nodes and another for malicious nodes. It is assumed that the normal nodes always send original and correct sensed information. On the other hand, the malicious node sends invalid data and sends null values to the Gateway.

Figure 4.6 illustrates the confidence value for every time slot. The average trust value for each sensor node is taken to plot the graph. The overall trust value is increased for normal nodes.

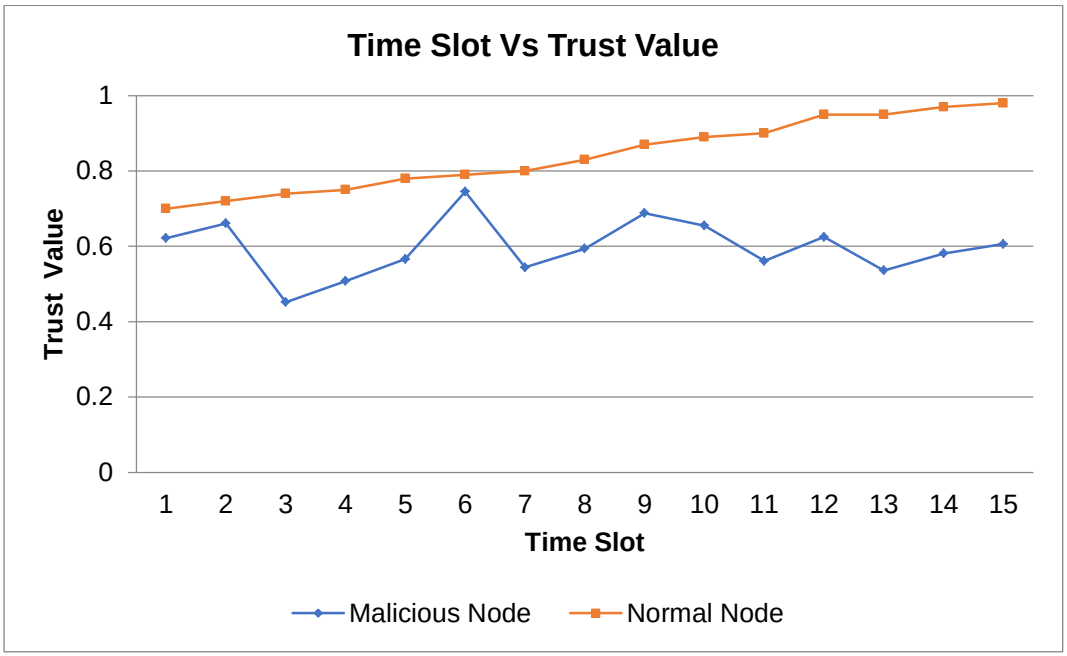

Figure 4. 6 Time Slot Vs Trust Value

Table 4.3 shows the four trust metrics with different time intervals.

Table 4. 3 Trust Metrics for different time intervals

Time Interval	SR	CR	DQR	RR
1	1	0.7	0.4	0.85
2	1	0.7	0.52	0.85
3	1	0.6	0.5	0.8
4	1	0.6	0.33	0.8
5	1	0.3	0.33	0.65
6	0.8	0.5	0.43	0.65
7	0.75	0.4	0.67	0.57
8	0.75	0.4	0.46	0.57
9	0.75	0.4	0.71	0.57
10	0.67	0.6	0.58	0.63
11	0.67	0.3	0.44	0.48
12	0.67	0.6	0.58	0.63
13	0.5	0.4	0.67	0.45
14	0.33	0.6	0.58	0.47
15	0.29	0.7	0.5	0.49

Figure 4.7 illustrates the four confidence metrics value for every time slot. Again, the SR and RR are gradually reduced from starting time interval to the ending time interval.

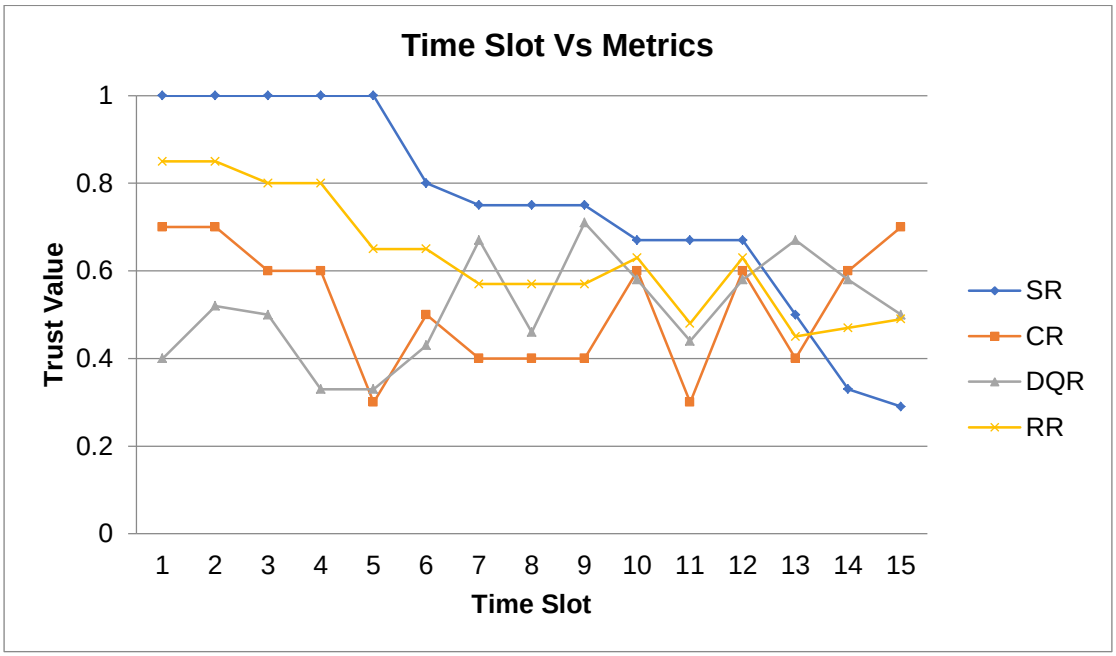

Figure 4. 7 Trust value for each time slot

Table 4.4 shows the trust metrics for sample sensor nodes.

Table 4. 4 Trust Metrics for 10 Sensor nodes

Sensor	SR	CR	DQR	RR
1	1	0.33	0.5	0.67
2	1	0.67	0.4	0.83
3	0.25	0.53	0.65	0.39
4	0.25	0.53	0.46	0.39
5	0.71	0.47	0.69	0.59
6	0.91	0.73	0.55	0.82
7	1	0.4	0.25	0.7
8	0.83	0.4	0.61	0.62
9	0.86	0.47	0.57	0.66
10	0.9	0.67	0.68	0.78

Figure 4.8 shows the trust metrics for each sensor. The SR and RR are interrelated metrics. When SR is increased, the RR also gradually increased.

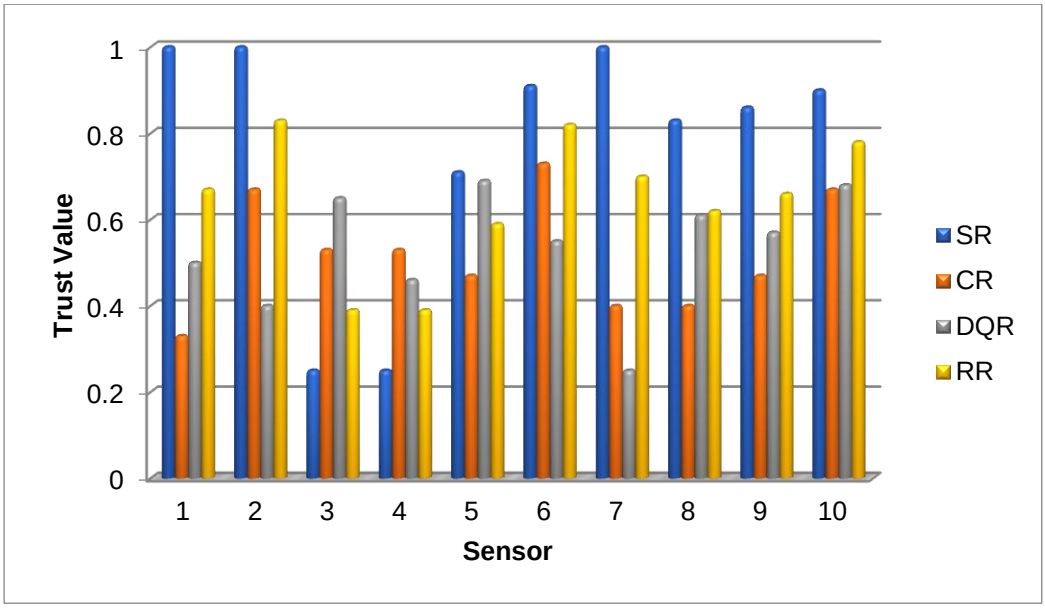

Figure 4. 8 Trust Metrics for Sensors

Table 4.5 shows the four trust metrics values for normal and malicious nodes. From that table, the CR is always higher trust value (1) for normal node. Because normal send all sensed information completely.

Table 4. 5 Trust Metrics for Normal and Malicious Node

Time Interval	Normal Node				Malicious Node			
	SR	CR	DQR	RR	SR	CR	DQR	RR
1	0.73	1	0.8	0.75	0.7	0.65	0.62	0.5
2	1	1	0.75	0.71	0.61	0.5	0.6	0.61
3	1	1	0.65	0.8	0.47	0.4	0.56	0.47
4	0.71	1	0.7	0.78	0.5	0.35	0.38	0.5
5	0.78	1	0.82	0.63	0.3	0.6	0.56	0.3
6	0.67	1	1	0.6	0.29	0.3	0.61	0.7
7	0.86	1	0.86	0.7	0.67	0.35	0.45	0.62
8	1	1	0.75	0.71	0.5	0.3	0.44	0.57
9	0.75	1	1	0.7	0.3	0.4	0.6	0.3
10	0.86	1	0.8	0.6	0.6	0.45	0.33	0.5
11	1	1	0.85	0.68	0.8	0.4	0.58	0.27
12	0.92	1	0.9	0.74	0.33	0.65	0.54	0.33
13	0.97	1	1	0.67	0.6	0.65	0.44	0.57
14	1	1	0.74	0.6	0.47	0.35	0.62	0.68
15	0.85	1	0.86	0.74	0.69	0.55	0.61	0.62

Figure 4.9 depicts the trust metrics value for normal and malicious nodes. Again, the normal node gives a higher trust value compare to malicious nodes.

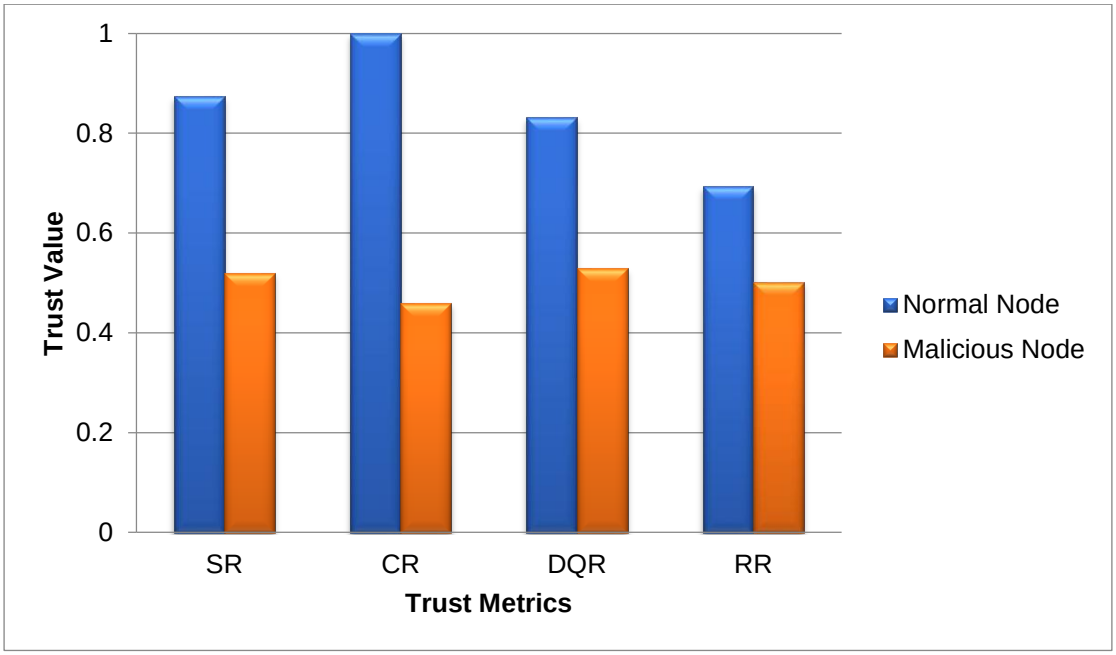

Figure 4. 9 Trust Metrics Analysis

4.7 Summary

IoT refers to the notion of connecting billions of tiny gadgets to acquire and swap information in a variety of fields, namely medical, surroundings, and industry, between others. In comparison, IoT has unverified stability, confidentiality, and confidence attributes critical in specific environments. This chapter explains a trust level computation model of IoT enabled patient health monitoring services. First, the Gateway collects all the patient attributes from sensors and sends them to the trust evaluator to evaluate the trust level. Then, the four trust metrics, success rate, completeness rate, data quality, and reward rate, are used to estimate each sensor's trust value.

CHAPTER – V

ENHANCED ADAPTIVE TRUST MANAGEMENT SYSTEM FOR SIOT

5.1 Introduction

IoT is the new generations developing model. It's used in a variety of fields, including health, smart homes, smart cities, promising markets, and transportation. However, because IoT networks are scattered, they are vulnerable to malicious assaults. In addition, IoT devices are vulnerable to assaults because they are heterogeneous and have limited capacity and storage. As a result, safety, confidentiality, and trust are critical for IoT networks.

As a result, the IoT system is vulnerable to the features of IoT contexts that need trust. To begin with, the IoT contains a vast amount of hybrid entities, each with its own set of standards. Second, because many nodes might connect or leave the network simultaneously, the trust system must examine the network in real-time. Third, while the IoT entails gadgets, the devices are handled by humans. In addition, the social relationship is taken into description while evaluating the system's performance. Finally, the system is susceptible to trust attacks, which the IoT ecosystem should be able to sustain (Abderrahim et al., 2017)

SIoT paradigm was created by incorporating community networking models into the IoT, allowing people and linked things to converse, distribute data, and enable numerous exciting purposes. In the IoT, things or items are controlled by humans and are subject to their work. As a result, social interactions among clients and owners must be considered while developing the system. The social association is based on community policy that their owners can define. For example, when two nodes begin interacting, one uses the services of the other. Trust rating based on community relationships has gained popularity, and this capability allows devices to build social relationships with others automatically. Many studies have employed social IoT to manage the trust, with nodes' historical behaviour gauge confidence (Atzori et al., 2012). Figure 5.1 depicts a social IoT perspective.

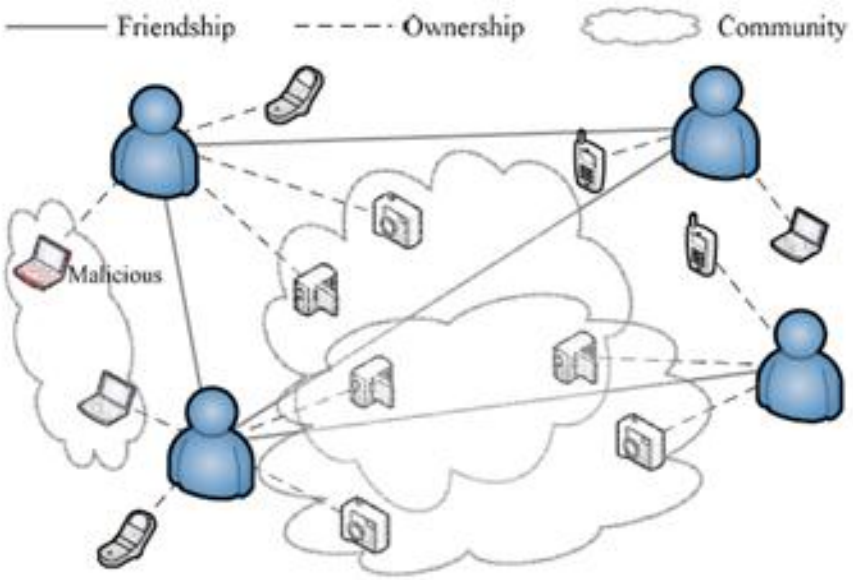

Figure 5. 1 Social IoT structure (Bao & Chen, 2012)

Trust management is required to provide trusted message among IoT devices and to identify malicious nodes. The trust management system is responsible for not only safety but also consistency and confidentiality protection. Methods for determining the trustworthiness of interacting nodes are included in a trust management system (TMS). The mechanism determines the level of trust in a particular situation. The trust management system allows nodes to collaborate and share their services. Based on its previous experience, each node performs a trustworthy relation.

The nodes involved are incredibly diverse and belong to distinct communities. As a result, the nodes purposefully compromise themselves and provide misleading reports to gain attention. The trust mechanism is critical to the Internet of Things. This chapter describes an dynamic trust management methodology for SIoT based on QoS and social characteristics. The trust assessment is done in concurrent, and the outcomes are disseminated. The delay in trust is calculated in order to lessen the importance of earlier trust values. Filtering the trustworthy recommenders only affects the trust ratings on a node that are based on a 3rd party. This is made possible by the node's mutuality and centrality properties.

5.2 Trust management in SIoT

The notion of confidence has been researched in a variety of areas, together with psychology and computer science. Because of its comprehensive, transdisciplinary, and numerous features, it is difficult to describe the phrase "trust accurately." A trust connection consists of minimum two parties: a trustor and a trustee who are completely dependent on one another for common gain, as well as the interpretation where the confidence affiliation exists, including the intention of the trust, the trust situation (e.g., duration, place, behaviour, gadgets used, type of operation, etc.), and the hazard of trust. In addition, it defines some data that can be utilized to describe the surroundings or status of the entities involved. In networking systems such as SIoT, trust management is critical. This section discusses some general trust features that are dependent on the author's vision and premise. Then, in a SIoT setting, explain the particular issues and restrictions of trust management.

Several methods for calculating trust were used, depending on the attributes that were examined.

Direct Trust: The trustor and the trustee have direct encounters, activities, or observations, according to this property.

Indirect Trust: In this instance, the trustor and the trustee have no past experience or relationship. The trust is built on the suggestions and opinions of other nodes.

Local Trust: It is determined by the pair trustor/trustee in question and varies from couple to couple, implying that a node i can confide a node j while a different node k can disbelieve the similar node j.

Global Trust: It is also known as reputation, which derive from the fact that every node in the network has a distinct trust value that all other nodes can see.

Asymmetric: When a connection binds two persons together, their degree of credibility may differ. The truth that X has faith in Y does not mean that Y should have confidence in X.

Subjective: Trust is naturally a individual judgment based on a variety of elements or facts, which may be more important than others.

Objective: In specific scenarios, including when trust is calculated depending on a device's QoS attributes.

Context-dependent: When a node i's trust in a node j differs depending on the framework.

Composite Property: Trust is a composite quality made up of several attributes such as reliability, integrity, faithfulness, safety, competency, and punctuality, all of which must be addressed based on the context in which trust is defined.

Depends on history: This feature implies that previous experiences may have an impact on current trust levels.

Dynamic Trust: Trust changes over time in a dynamic way. It must respond to environmental changes in the context in which the trust decision was taken, and it may be refreshed or revoked regularly.

A malicious node seeks to disrupt the IoT's essential functions (for example, service composition). It can also carry out the following trust-related attacks: (Abdelghani et al., 2016)

Self-promotional attacks can exaggerate their significance (by making positive suggestions for themselves) to be chosen as a service contributor but later cease offering services or providing defective services.

Bad-mouthing attacks: They can tarnish the identities of dutiful nodes (by making negative suggestions about them) to reduce the likelihood of superior nodes being chosen as service providers.

Ballot stuffing attacks: it can improve the reputation of misbehaving nodes (by making positive suggestions) to enhance the likelihood of being chosen as service providers.

Whitewashing attack: a compromised actor might vanish and reappearance in the programme to erase its poor reputation.

Discriminatory attacks: A compromised node can discriminate against non-friends or nodes exclusive of strong social links in SIoT systems due to human nature or a propensity for mates (without many familiar friends).

Opportunistic service attacks: a compromised actor might give superior service to opportunistically earn a maximum reputation, particularly if it believes its reputation is deteriorating due to poor service. It can successfully collaborate with other rogue nodes to conduct badmouthing and ballot-stuffing attacks if it has a good reputation.

SIoT networks distinguish from social networks in that they have a significant series of criteria and limits, such as:

- A large number of entities and devices are engaged.
- Things and gadgets have restricted storage space.
- Things and gadgets have restricted computing resources.
- High dynamism results from the high number of nodes that connect and disconnect networks at any time.
- Energy utilization is one of the most significant challenges facing entities and devices recharged using a battery.
- Because they interact with the real world, used apps and services are critical and sensitive.
- To accommodate tiny things restrictions, energy efficiency means making trust management algorithms and procedures quicker and fewer power-consumption.

Accessibility, flexibility, durability, power consumption, and resiliency of the SIoT network are all key characteristics that must be accommodated and ensured through trust management protocols.

5.3 Static Type Trust Management

The social IoT system is made up of independent moving parts, the trust mechanism must be dispersed rather than centralized. Every node keeps track of other nodes' trustworthiness. The repeated apprise of trust value is dependent on both interactions and activities. During the direct communication of more than one node, exchange their recommendations for another trustee and change their confidence measurement is possible. The following is a description of each component's construction.

5.3.1 Trust Composition

The social interactions that characterise the system include honesty, collaboration, and common interest. Honesty is an important part of trust management, and it is evaluated by obtaining both direct and indirect data, such as a suggestion from some other node. A node that has an increased group link to another trustor is very cooperative. Closely compatible nodes do well in the Internet of Things. The same community includes nodes with comparable interests and skills. When the trustor and trustee have the greatest amount of commonality of interest, they interact more.

5.3.2 Trust Propagation and Aggregation

It combines previous and current data. They combine both direct and indirect recommendations from the new observations. Consider the node *x* be trustor and node *y* be trustee, and *z* is suggestion node to provide an outlook on node *y* to node *x*. Let $V_{xy}^{p}(t)$ Where p = sincerity of interest. The rate of $V_{xy}^{p}(t)$ vary from zero to one with zero as distrust, 0.5 as obliviousness and one as complete trust. $V_{xy}^{p}(t)$ is rationalized while node x and node y develops into straight interface. The renew is given as

$$V_{xy}^{p}(t) = (1-\alpha)V_{xy}^{p}(t-\Delta t) + \alpha D_{xy}^{p}(t) \qquad (5.1)$$

Where $D_{xy}^{p}(t)$ is direct examination of *x* node on *y* node and $V_{xy}^{p}(t-\Delta t)$ is it past trust value. The constraint α obtain the value in the vary zero, and one and is used to weight the values.

The thorough examination of node *x* on node *y* for the three associations (*integrity*, *cooperativeness*, and *community-interest)* is as follows

To check the *sincerity* of *y*, evaluate the *x* suggestion and *y* suggestion for a different node, say *q*

$D_{yq}^{honesty}(t-\Delta t)$ is the trust of *y* on *q* and is zero when *y* is fraudulent.

$D_{xq}^{honesty}(t-\Delta t)$ is trust of *x* on *q* and is 0 when *x* is fraudulent

The comparative dissimilarity among *x* measurement and *y* measurement is greater than the threshold, then *y* is distrustful. To ensure the level of cooperativeness

of *y* by *x* depend on direct interpretation. The bond among nodes as well decides the cooperativeness.

The friendly nodes are very mutual. Each node preserves a friend list and $D_{xy}^{cooperativeness}(t)$ is the ratio of familiar friends among x and y $D_{xy}^{cooperativeness}(t) = \frac{|friends(x) \cap friends(y)|}{|frinends(x) \cup friends(y)|}$ Where friends(x) are friends of node x owner, and friends(y) are contacts of y owner. When node x and node y are in direct communication, they share their friend list and filter familiar friends. Thus, an truthful node present a valid list while a untruthful node provide the counterfeit list and self-prompt itself to be selected by x (trustor).

This stuff estimates the general concern and ability of x and y. each node upholds a list of groups of their owners, and this record may modify vigorously. the direct CoI is given as $D_{xy}^{community-interest}(t) = \frac{|community(x) \cap community(y)|}{|community(x) \cup community(y)|}$ where $community(x)$ is a set of groups of owners. When *x* and y unswervingly communicate, they share the profiles.

5.3.3 Decay and Update

While *x* node meet *z* node and z ≠ y, *z* has prior knowledge with node y, then node *z* is a influencer of *y* to node *x*. The suggestion is given as $R_{zy}^{p}(t)$. This influence alters the trust evaluation $V_{xy}^{p}(t)$ on come upon and is assumed as

$$V_{xy}^{p}(t) = (1-\gamma)V_{xy}^{p}(t-\Delta t) + \gamma R_{zy}^{p}(t) \qquad (5.2)$$

- γ is the limit for new suggestion and knowledge of *x with y*.

If z is good, then the estimation of BMA is also good. Else BSA is terrible. To decide this,

$$\gamma = \frac{\beta D_{xz}^{p}(t)}{1+\beta D_{xz}^{p}(t)} \qquad (5.3)$$

5.3.4 Trust Formation

$\boldsymbol{V_{xy}^{p}(t)}$ where p = *truthfulness*, *compliancy*, and *community-interest* are independently evaluated by x. The general trust value based on possessions depends

on the IoT apps used. When sincerity is rationalized, the scheme can identify malevolent clients. In contrast, cooperativeness and community-interest are justified, detecting trustees with good community ties. The subsequent is trust configuration when truthful is taken as decide property with an sincerity threshold of 0.5.

$$V_{xy}(t) = \begin{cases} 0, & if V_{xy}^{honesty}(t) \leq 0.5 \\ min\begin{pmatrix} V_{xy}^{cooperativeness}(t) \\ V_{xy}^{community-interest}(t) \end{pmatrix}, & if\ V_{xy}^{honesty}(t) > 0.5 \end{cases} \quad (5.4)$$

5.4 Suggested Adaptive Dynamic Trust Management Model

A large portion of the research focuses on direct evaluation, recommendation, and trust acquisition. The context-based trust criteria evaluate whether a node can deliver a trustworthy service. Trust values are developed through time, and a new value is assigned.Previous interactions are considered for node recommendations, or it can sometimes assist in the selection of a node with no previous interactions. When a node is called for a suggestion, the recommendation method can sometimes result in badmouthing and ballot stuffing attacks.

The suggested framework is useful for the following research.

- Parameters that are weighted and set at runtime
- Trust deteriorates over time and in response to events
- Endorsement role and decision depending on recommender's reliability
- A dynamic weighted approach for combining direct and indirect evaluations

Many TMs (Trust Managers) are located at various geographical areas in the centralized method. The servers are in which all of the nodes are registered. Another common entity is in charge of the servers. The social interaction between the nodes must be taken into consideration in trust management in social IoT. This could lead to a slew of attacks from misbehaving nodes. Trust is a human-decidable detail that must be resolved in a variety of situations. Since it has delicate data, it shall sometimes be done in an invasive manner that insulates non-relevant data (Yan et al., 2014).

In the cooperative IoT with decentralization, there really is no single way to determine a device's reputation. The most of trust models are built on the foundation

of suggestions. It focuses on parameter-based decision-making, with recommendation as a first step. The degradation process is also modeled in the system. Because dynamic changes in IoT are reflected in decisions, past experiences gathered over a lengthy period of time are not recognized for decision-making.

Believe is built on a combination of criteria that are particular to the circumstance. On a hub, there are two sorts of certainty evaluations: objective (QoS) and subjective (social). The trustor gives the parameter weight based on its significance, and the weighted parameter scores as halfway believe evaluations. The believe values are broadly dispersed and have no centralised specialist. Each hub keeps its certainty esteem whereas moreover permitting get to to others. Certainty scores debase over time and are upgraded based on the interaction of time and occasions. A suggestion is chosen depending on the trustor's relationship. A weighted whole approach is utilized for conglomeration. The taking after could be a depiction of the show:

Let C be collaborate nodes, □ xy be theself-belief value of y calculated by x

P= {p_1, p_2,…..p_n }are trust constraint,

W_x = {$w_x(p_1)$, w_x (p_2), w_x (p_3),……. w_x (p_n) } is weighted parameter by node x

V_{xy} = {$V_{xy}(p_1)$, $V_{xy}(p_2)$, …… $V_{xy}(p_n)$ is node x evaluation on node y for each parameter

F= f(W, V) $\square_{xy}$ aggregation function of total trust value.

half(x) partial trust score node x half-life period

Trust criteria:

Trust factors are both subjective & objectives. Rate, speediness, dependability, and work are all relevant parameters. Honesty, friendliness, and cooperation, coworker, and co-located that result in the social tie-up are subjective. The parameters that are irrelevant to the context are set to zero.

Weighted parameter:

The weighted parameter is stated as

$$w_x(p) \quad [0,1] \quad x \quad C, p \quad P \text{ and } \sum \square x = 1 \qquad (5.5)$$

When the trustor node interacts, the weights are dynamically modified.

Trust aggregation evaluation method and Partial trust:

As V_{ex} is a incomplete evaluation of x on y for each constraint, each comprise a total trust value. The fractional scores are cumulated using the dynamic weighted technique and is given by F= W˙ × V

$$\square_{xy} = \sum_{i=1}^{n} w_x(p_i) \times V_{xy}(p_i) \forall x, y \in C,\ p_i \in P \quad (5.6)$$

Trust Decay:

During communication among nodes increases, the evaluation decreases to decay. The decay time depends upon the trustor. half (x) is given as

$$\left(V_{xy}(p)\right)_{0 \to t} = (\emptyset_x)_t \times \left(V_{xy}(p)\right)_0 \forall x, y \in C, p \in P \quad (5.7)$$

Trust Recommendations and the notion of mutuality-centrality

Node x can assess node y's trustworthiness by consulting other nodes z which interacted with y. This is known as indirect valuation or a suggestion from node x to node z on node y.

The concept of criticality provides information about a node's centrality in the network. The network's primary node is one that has numerous relationships and transactions. A node's centrality reveals how satisfied it is with others through contact and involvement. The mutuality tells the trustor node x where the trustee node y is. Nodes which are relatively close will share similar profiles. However, a node with a large number of mutual friends cannot be compared to a newly joined trustworthy node with a small number of friends at first. Mutual friends are compared to familiar friends to overcome this problem.

Let M_{xy} is familiar friends of x and y

Nx is a set of trustee's friends. stated as

$$C_{xy}^{MC}(t) = \left|M_{xy}\right||N_x| \quad (5.8)$$

The two nodes with many friends in general are true friends and suggest mutual honestly.

5.5 Experimental Result

The simulation is conducted among 50 independent agents dispersed to 20 users. The simulation time is for 200hrs. There were ten communities. The social IoT system is established with friendly relations. The efficacy of the proposed scheme is appraised by merging, and resiliency performance to the intervention is investigated. The constraint is set as $\alpha = 0.5$, $\beta = 0.2$ from previous research.

Figure 5.2 shows the convergence study of different malicious percentages. The test is repetitive on changeable malicious ratios such as P_m = 20%, 30%, 40% and 50%

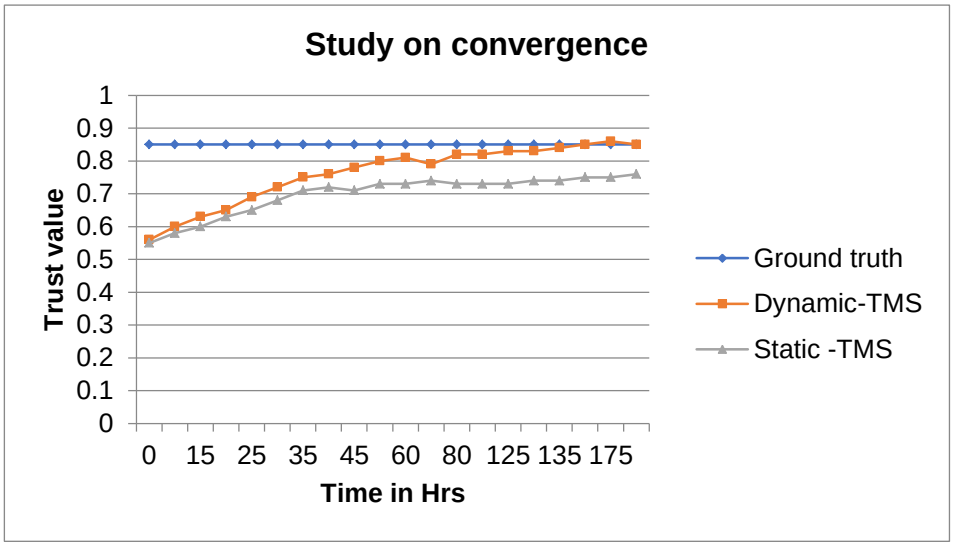

Figure 5. 2 Study on convergence at Pm = 20%, 30%, 40% and 50%

Figure 5.2 shows that both the system and the malicious node take some time to unite at the beginning rise. The graph shows that later some point, the confluence towards ground level has occurred. This is because the rogue node's direct trust value is initially lower.

For a lesser percentage of malicious nodes and a larger rate of malicious nodes, the Static –TMS and Dynamic –TMS resiliency behaviour. When a malicious node is present, resiliency refers to the ability to adjust the system to improve its performance. The malicious node may make poor suggestions in two circumstances, leading in a bad mouth attack and a ballot stuffing assault.

The bend of the Energetic Versatile framework meets very rapidly, with exceptionally little inclination hole between the ground truth levels, as appeared in Figure 5.3. This is often too due to the common and centrality properties sifting out the untrustworthy recommender. As a result, they don't consider voting great when a hub is off base and voting terrible when it is performing well. The static TMS meets closer to ground level, as seen within the chart, in spite of the fact that the believe predisposition crevice is more noteworthy for inactive TMS than for energetic TMS.

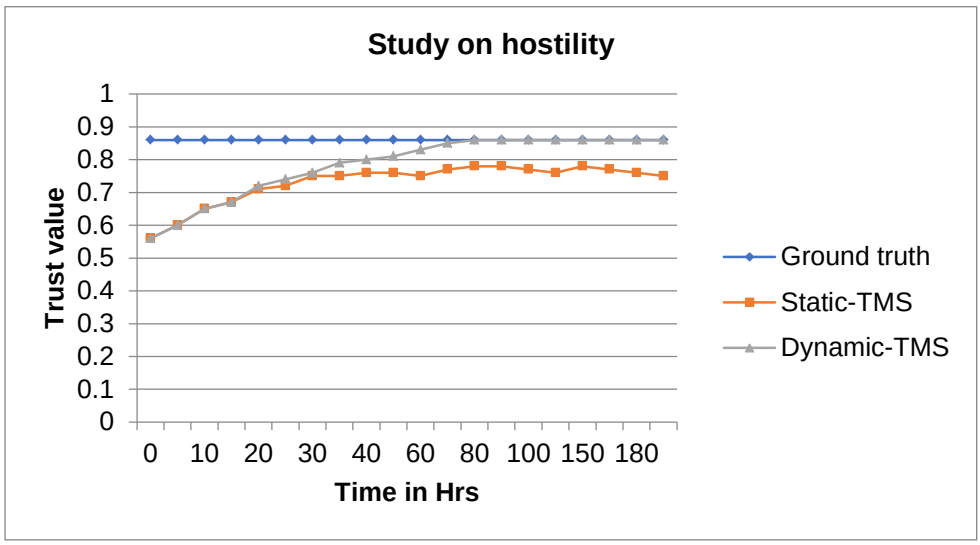

Figure 5. 3 Effect of low hostile (Pm = 20%) and high hostile (Pm = 50%) environment

Figure 5.4 shows the effect of decay parameters. It takes $\emptyset = 0.1, 0.01, 0.001$

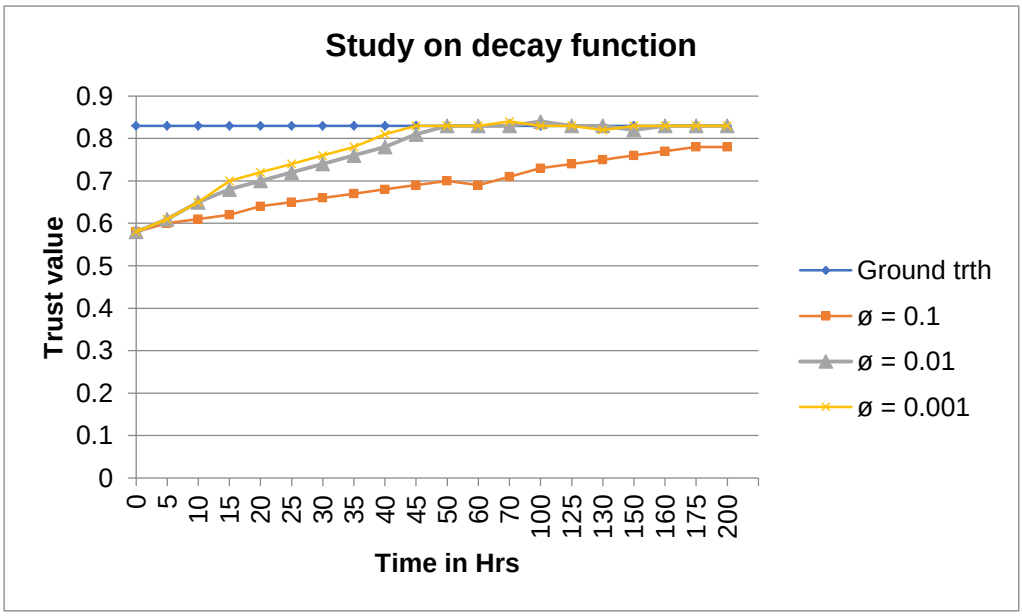

Figure 5. 4 Effect of decay parameter

The results illustrates that the certainty rot parameter reach the territory truth level. If the rot variable is set to or near to 0, it demands a long time to reach ground truth, in any case when it is set to ∅ >0, it merges rapidly. The great hubs are suited for a long time, subsequently they effectively take an interest in benefit, as seen by this result. When the fabulous hub is hurt, usually not the case.

5.6 Summary

Controlling and observing Social IoT is made simpler with believe. In any case, the current approaches for assessing certainty within the cipher-digital world are inadequately. Whereas planning the framework to ensure against dangers, it is basic to ensure question dependability, which can make strides benefit conveyance. The investigate presents a Believe Administration Framework (TMS) as a arrangement to the issues, which encourages protest communication and sets up dependable administrations. The taking after are the different plan components of this framework:

Utilizing a dynamic weighted sum aggregation methodology and an unique trust strategy, the suggested method is categorized as disseminated, QoS, and social factor construction, decentralized variety of trust transmission, including primary and secondary evaluation, and a ultimate number based on a individual trust system. A proposed dynamic IoT model is compared to a static IoT model in this study. The findings show that these recommended versatile framework cumulates through the spot precision level in a clear and productive style, and that the trust aggregation component applies novel approaches, such as more detailed social information of entities.

CHAPTER – VI

CONCLUSION AND FUTURE RESEARCH

6.1 Conclusion

IoT is a model which defines a group of connected things and gadgets that can be wired or wirelessly connected to the Internet. IoT, has gained prominence as these innovations are employed for a variety of reasons such as communication, navigation, educational, and commercial development.

A trust level computation model of an IoT enabled patient health monitoring services is proposed. The gateway collects all the patient attributes from sensors and send to trust evaluator for evaluate the trust level. The four trust metrics success rate, completeness rate, data quality and reward rate is used to estimate the trust value for each sensors.

Trust is a powerful tool for managing and monitoring Social IoT. However, the previous methods of gauging digital world belief are insufficient. It is critical to ensure the integrity of the material while organising the system to protect against assault, consequently increasing the provision of services. This research proposes a trust management system that encourages interdisciplinary collaboration and establishes trustworthy services. The following is a list of the components of the proposed system:

This method is based on the distribution of distribution parameters, QoS, and Social, a dispersed sort of faith, which is tested directly and indirectly before a dynamic process of combining weight and final points based on a single trust process. The study compared the recommended adaptive framework to a static Internet of Things paradigm. The simulation demonstrates that the suggested dynamic system transforms world-class reality into a clear and efficient system and applies new techniques to the trust integration object, which incorporates correct business social information.

The major focus of the thesis is as follows:

- To monitoring patient health using IoT devices and collect sensed information like patient heart rate, BP, glucose level and body temperature etc.,
- Defines the construction of trust from sensed raw input to a final trust value using a trust computation model.
- To examine the facts and each particular trust property
- To provide an adaptive trust control system that assesses a node's trustworthiness in an IoT network while taking into account both QoS and social parameters.
- Evaluate the effectiveness of the findings through simulations.

6.2 Future Research

There is still a lot of potential for more research on IoT and SIoT application-based trust computation limitations. The solutions on offer improve the sustainability and deployment of dependable IoT solutions. The solutions will be tested and deployed in a real-world setting in the future.

The followings are the some future research direction:

- Use machine learning or deep learning algorithm to detect malicious nodes in IoT network based on trust level.
- Dynamically modify the trustworthiness factor to impove system performance.
- To investigate statistical strategies for excluding suggestion anomalies in dynamic trust management protocol in order to minimize confidence variation and improve trust convergence.

REFERENCES

1. Abdelghani, W., Zayani, C.A., Amous, I., Sèdes, F., (2016), "Trust Management in Social Internet of Things: A Survey", In: Dwivedi Y. et al. (eds) Social Media: The Good, the Bad, and the Ugly. I3E 2016. Lecture Notes in Computer Science, vol 9844. Springer, pp. 430-441
2. Abderrahim, O.B., Elhdhili M.H., and Saidane, L.,(2017), "TMCoI-SIOT: A trust management system based on communities of interest for the social Internet of Things," 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 747-752
3. Abou-Nassar, E.M., Iliyasu, A. M., El-Kafrawy, P. M., Song, O., Bashir, A. K., and El-Latif, A. A. A., (2020), "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems," in IEEE Access, 8, pp. 111223-111238
4. Adewuyi, A.A., Cheng, H.,Shi, Q., Cao, J., MacDermott, Á., and Wang, X., (2019), "CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things," in IEEE Internet of Things Journal, 6(3), pp. 5432-5445
5. Afzal, B., Umair, M., Asadullah Shah, G., and Ahmed, E., (2019), "Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges," Futur. Gener. Comput. Syst., 92, pp. 718–731.
6. Ahmad, F., Franqueira, V.N.L., and Adnane,A., (2018), "TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks," in IEEE Access,6, pp. 28643-28660
7. Akbar, A., Kousiouris, G., Pervaiz, H., Sancho, J., Ta-Shma, P., Carrez, F., and Moessner, K., (2018), "Real-time probabilistic data fusion for large-scale IoT applications", IEEE Access, 6, pp. 10015–10027.
8. Al-Hamadi, H., and Chen, R., (2017), "Trust-based decision making for health IoT systems," IEEE Internet of Things Journal, 4(5), pp. 1408-1419
9. Aljazzaf, Z.M., Perry, M., and Capretz, M.A.M., (2010) "Online Trust: Definition and Principles," 2010 Fifth International Multi-conference on Computing in the Global Information Technology, Valencia, pp. 163-168

10. Alshehri, M.D., Hussain,F.K., and Hussain, O.K., (2018), "Clustering driven intelligent trust management methodology for the Internet of Things (CITM-IoT)," Mobile Netw. Appl., 23(3), pp. 419–431
11. Altaf, A., Abbas, H., Iqbal, F., Khan, M.M.Z.M., and Daneshmand, M., (2021), "Robust, Secure, and Adaptive Trust-Oriented Service Selection in IoT-Based Smart Buildings," in IEEE Internet of Things Journal, 8(9), pp. 7497-7509
12. Amin F, Abbasi R, Rehman A, Choi GS. (2019a) "An Advanced Algorithm for Higher Network Navigation in Social Internet of Things Using Small-World Networks", Sensors, 19(9)
13. Amin, F., Ahmad, A., and Sang Choi, G., (2019b), "Towards Trust and Friendliness Approaches in the Social Internet of Things", Applied Sciences, 9(1)
14. Ammar, M., Russello, G., and Crispo, B., (2018), "Internet of Things: A survey on the security of IoT frameworks", J. Information Security Appl., 38, pp. 8–27.
15. Asghari, P., Rahmani, A.M., Javadi, H.H.S, (2018) "Service composition approaches in IoT: a systematic review", Netw Comput Appl., 120, pp. 61–77
16. Aslam, M.J., Din, S., Rodrigues, J.J.P.C., Ahmad, A., and Choi, G.S., (2020), "Defining Service-Oriented Trust Assessment for Social Internet of Things," in IEEE Access, 8, pp. 206459-206473
17. Atzori, L., Iera, A., and Morabito. G., (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
18. Atzori, L., Iera, A., and Morabito, G., (2014), "From smart objects to social objects: The next evolutionary step of the internet of things", Communications Magazine, IEEE, 52(1), pp. 97–105
19. Aujla, G.S., and Jindal,A., (2021), "A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring," in IEEE Journal on Selected Areas in Communications, 39(2), pp. 491-499
20. Awan, K.A., Din, I.U., Zareei, M., Talha, M., Guizani, M., and Jadoon, S.U., (2019a), "HoliTrust-A Holistic Cross-Domain Trust Management Mechanism for Service-Centric Internet of Things," in IEEE Access, 7, pp. 52191-52201

21. Awan, K.A., Din, I.U, Almogren, A., Guizani, M., Altameem, A., and Jadoon, S.U., (2019b) "RobustTrust – A Pro-Privacy Robust Distributed Trust Management Mechanism for Internet of Things," in IEEE Access, 7, pp. 62095-62106
22. Azad, M.A., Bag, S., Hao, F., and Shalaginov, A., (2020) "Decentralized Self-Enforcing Trust Management System for Social Internet of Things," in IEEE Internet of Things Journal, 7(4), pp. 2690-2703, April 2020
23. Baker, S.B., Xiang, W., and Atkinson, I., (2017) "Internet of Things for smart healthcare: Technologies, challenges, and opportunities," IEEE Access, 5, pp. 26521–26544
24. Bao, F., and Chen, I.R., (2012), "Dynamic trust management for internet of things", Proceedings of the 2012 international workshop on Self-aware internet of things. ACM, pp. 1-6.
25. Bao, F., Chen, I.R., and Guo, J., (2013), "Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems", in 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS). pp. 1–7.
26. Bello, O., and Zeadally, S., (2016), "Intelligent Device-to-Device Communication in the Internet of Things," in IEEE Systems Journal, 10(3), pp. 1172-1182
27. Ben Saied, Y., Olivereau, A., Zeghlache, D., and Laurent,M., (2013), "Trust management system design for the Internet of Things: A contextaware and multi-service approach," Computers & Security, 39, pp. 351–365
28. Beynon, M., Curry, B., Morgan, P., (2000), "The Dempster-Shafer theory of evidence: An alternative approach to multicriteria decision modelling. Omega 2000, 28, pp. 37–50.
29. Bhargava, A., Verma, S., Chaurasia, B.K., and Tomar, G.S., (2017) "Computational Trust Model for Internet of Vehicles", 2017 Conf. Inf. Commun. Technol. CICT 2017 Apr. 1–5.
30. Borgia, E., (2014), "The Internet of Things vision: Key features, applications and open issues", Computer Communications, 54, pp. 1-31
31. Busi Reddy, V., Venkataraman, S., and Negi,A., (2017), "Communication and Data Trust for Wireless Sensor Networks Using D–S Theory," in IEEE Sensors Journal, 17(12), pp. 3921-3929

32. Buttyan, L., and Hubaux, J.P., (2007), "Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing, Cambridge University Press
33. Cai, R.J., Li, X.J., and Chong, P.H.J., (2019), "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," in IEEE Transactions on Mobile Computing, 18(1), pp. 42-55
34. Caminha, J., Perkusich, A., Perkusich, M., (2018a), "A smart trust management method to detect on-off attacks in the internet of things", Secur. Commun. Netw., 2018
35. Caminha, J., Perkusich, A., and Perkusich, M., (2018b) "A Smart Middleware to Perform Semantic Discovery and Trust Evaluation for the Internet of Things" in CCNC 2018 - 2018 15th IEEE Annu. Consum. Commun. Netw. Conf. Jan. pp. 1–2.
36. Catarinucci, L., DeDonno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M.L., and Tarricone, L., (2015), "An IoT-Aware Architecture for Smart Healthcare Systems", in IEEE Internet of Things Journal, 2(6), pp. 515-526
37. Chakraborty, T., and Datta,S.K., (2017), "Application of swarm intelligence in Internet of Things," 2017 IEEE International Symposium on Consumer Electronics (ISCE), pp. 67-68
38. Chang, E., Dillon, T.S. and Hussain, F.K, (2005) "Trust and reputation relationships in service-oriented environments," Third International Conference on Information Technology and Applications (ICITA'05), 1, pp. 4-14
39. Chen, H.-C., (2019) "Collaboration IoT Based RBAC with Trust Evaluation Algorithm Model for Massive IoT Integrated Application", 24(3), pp. 839-852
40. Chen, J.I.-Z., (2018a), "Embedding the MRC and SC Schemes into Trust Management Algorithm Applied to IoT Security Protection," Wireless Personal Communications, 99(1), pp. 461-477
41. Chen, X., Ma, M., Liu, A., (2018b), "Dynamic power management and adaptive packet size selection for IoT in e-Healthcare", Comput Electr Eng, 65, pp. 357–375
42. Chen, D., Chang, G., Sun, D., Li, J., Jia, J., and Wang, X., (2011), "TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things", Computer Science and Information Systems, 8(4), pp. 1207-1228

43. Chen, I.R., Bao, F., and Guo, J., (2016a), "Trust-based service management for social Internet of Things systems", IEEE Trans. Depend. Sec. Computing, 13(6), pp. 684–696
44. Chen, I.R., Guo, J., and Bao, F., (2016b), "Trust Management for SOA-based IoT and Its Application to Service Composition", IEEE Transactions on Service Computing, 9(3), pp. 482-495
45. Chen, I., and Guo, J., (2014), "Dynamic Hierarchical Trust Management of Mobile Groups and Its Application to Misbehaving Node Detection", 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, Victoria, BC, pp. 49-56
46. Chen, I.R., Guo,J., Wang,D.C., Tsai,J.J.P., Al-Hamadi, H., and You, I., (2019), "Trust-Based Service Management for Mobile Cloud IoT Systems", IEEE Trans. Netw. Serv. Manag., 16, pp. 246–263.
47. Chen, Z., Ling, R., Huang, C.M., Zhu, X. (2015a), "A scheme of access service recommendation for the social internet of things", Int. J. Commun. Syst.
48. Chen, X., Proulx, B., Gong, X., and Zhang, J., (2015b), "Exploiting Social Ties for Cooperative D2D Communications", IEEE/ACM Trans. Netw., 23, pp. 1471–1484
49. Cheng, B., Solmaz, G., Cirillo, F., Kovacs, E., Terasawa, K., and Kitazawa, A., (2018) "FogFlow: Easy Programming of IoT Services Over Cloud and Edges for Smart Cities," in IEEE Internet of Things Journal, 5(2), pp. 696-707
50. Cho, J., Al-Hamadi, H., and Chen, I., (2019), "COSTA: Composite Trust-Based Asset-Task Assignment in Mobile Ad Hoc Networks," in IEEE Access, 7, pp. 92296-92313
51. Cisco White Paper,(2019), "Visual Networking Index: Forecast and Trends, 2017–2022"
52. Čolaković, A., and Hadžialić,M., (2018), "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues", Computer Networks, 144, pp. 17-39
53. Daubert, J., Wiesmaier, A., and Kikiras, P., (2015), "A view on privacy & trust in IoT," 2015 IEEE International Conference on Communication Workshop (ICCW), London, pp. 2665-2670

54. Deebak, B.D., Al-Turjman, F., Aloqaily, M., and Alfandi,O., (2019), "An Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT," in IEEE Access, 7, pp. 135632-135649
55. Dilawar, N., Rizwan, M., Ahmad, F., and Akram,S., (2019), "Blockchain: Securing Internet of medical things (IoMT)", Int. J. Adv. Comput. Sci. Appl., 10(1), pp. 82-89
56. Din, I.U., Guizani, M., Kim, B.S., Hassan, S., and Khan, M.K., (2019), "Trust management techniques for the Internet of Things: A survey", IEEE Access, 7, pp. 29763–29787
57. Ding, S., Yue, Z., Yang, S., Niu, F., and Zhang,Y., (2020), "A Novel Trust Model Based Overlapping Community Detection Algorithm for Social Networks," in IEEE Transactions on Knowledge and Data Engineering, 32(11), pp. 2101-2114
58. Djedjig, N., Tandjaoui, D., Romdhani, I., and Medjek, F.,(2018), "Trust Management in the Internet of Things", Security and Privacy in Smart Sensor Networks, pp. 122-146
59. Dorodchi, M., Abedi, M., and Cukic, B., (2016), "Trust-based development framework for distributed systems and IoT", inProc. IEEE 40th Annual Computer Software Application Conference (COMPSAC), 2, pp. 437–442
60. Duan, J., Gao, D., Foh, C.H. and Zhang, H., (2013) "TC-BAC: A Trust and Centrality Degree Based Access Control Model in Wireless Sensor Networks", Ad Hoc Networks, 11(8): pp. 2675–2692.
61. Eckhoff, D., and Wagner, I., (2018), "Privacy in the smart city—applications, technologies, challenges, and solutions", IEEE Communications Surveys & Tutorials, 20(1), pp. 489–516
62. Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N., Farouk, A., (2018) Secure medical data transmission model for IoT-based healthcare systems", IEEE Access 6, pp. 20596–20608
63. Elsaadany, M., Ali, A., and Hamouda, W., (2017), "Cellular LTE-A Technologies for the Future Internet-of-Things: Physical Layer Features and Challenges," in IEEE Communications Surveys and Tutorials, 19(4), pp. 2544-2572
64. Fang, W., Xu, M., Zhu, C., Han, W., Zhang, W., and Rodrigues, J.J.P.C., (2019), "FETMS: Fast and Efficient Trust Management Scheme for

Information-Centric Networking in Internet of Things," in IEEE Access, 7, pp. 13476-13485

65. Farahat, I.S., Tolba, A.S., Elhoseny, M., and Eladrosy,W., (2018), "A secure real-time Internet of medical smart things (IOMST)", Comput. Electr. Eng., 72, pp. 455-467
66. Fernandez-Gago, C., Moyano, F., and Lopez, J., (2017), "Modelling trust dynamics in the internet of things", Inf. Sci., 396, pp. 72–82
67. Frustaci, M., Pace, P., Aloi, G., and Fortino, G., (2018), "Evaluating critical security issues of the IoT world: Present and future challenges", IEEE Internet Things J., 5(4), pp. 2483–2495
68. Ganeriwal, S., Balzano, L.K., Srivastava, M.B., (2008) "Reputation-based framework for high integrity sensor networks", ACM Trans. Sen. Netw., 4, pp. 1–37
69. Girolami, M., Barsocchi, P., Chessa, S., et al (2013) A social- based service discovery protocol for mobile ad hoc networks. 12th Annual Mediterranean Ad Hoc Networking Workshop, pp 103–110
70. Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M., (2013), "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions", Future Generation Computer Systems, 29(7), pp 1645-1660
71. Gulati, N., Kaur, P.D., (2021), "FriendCare-AAL: a robust social IoT based alert generation system for ambient assisted living", J Ambient Intell Human Comput.
72. Guo, J., Chen, I.R., (2015) "A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems", In Proceedings of the 2015 IEEE International Conference on Services Computing, New York, NY, USA, 27, pp. 324–331.
73. Guo, J., Chen, R., and Tsai, J.J., (2017), "A survey of trust computation models for service management in internet of things systems", Computer Communications, 97, pp. 1–14
74. Hameed, S., et al., (2021) "A Scalable Key and Trust Management Solution for IoT Sensors Using SDN and Blockchain Technology," in IEEE Sensors Journal, 21(6), pp. 8716-8733
75. Han, H., (2021), "Research on Adaptive Relationship Between Trust and Privacy in Cloud Service," in IEEE Access, 9, pp. 43214-43227

76. Hassan, H., El-Desouky, A.I., Ibrahim, A., El-Kenawy, E.M., and Arnous, R., (2020), "Enhanced QoS-Based Model for Trust Assessment in Cloud Computing Environment," in IEEE Access, 8, pp. 43752-43763
77. Hu, L., and Ni, Q., (2018), "IoT-Driven Automated Object Detection Algorithm for Urban Surveillance Systems in Smart Cities," in IEEE Internet of Things Journal, 5(2), pp. 747-754
78. Hussain, Y., et al., (2020), "Context-Aware Trust and Reputation Model for Fog-Based IoT," in IEEE Access, 8, pp. 31622-31632
79. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., and Sikdar, B., (2019), "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, 7, pp. 82721-82743
80. Islam, M.S, Islam, M.T., Almutairi, A.F., Beng, G.K., Misran, N., and Amin, N., (2019), "Monitoring of the human body signal through the Internet of Things (IoT) based LoRa wireless network system", Appl. Sci., 9.
81. Jabbar, W.A., et al., (2019), "Design and Fabrication of Smart Home With Internet of Things Enabled Automation System," in IEEE Access, 7, pp. 144059-144074
82. Jayasinghe, U., (2018a) "Trust Evaluation in the IoT Environment", Doctoral thesis, Liverpool John Moores University
83. Jayasinghe, U., Lee, G.M., Um, T.-W., and Shi., Q., (2018b), "Machine Learning based Trust Computational Model for IoT Services", IEEE Trans. Sustain. Comput, pp. 1–10.
84. Jayasinghe, U., Lee, H.W., and Lee, G.M., (2017a), "A computational modelto evaluate honesty in social internet of things", in Proceedings of the 32nd ACM Symposium on Applied Computing, pp. 1830–1835
85. Jayasinghe, U., Lee, G.M., Um, T., and Shi, Q., (2019), "Machine Learning based Trust Computational Model for IoT Services", IEEE Transactions on Sustainable Computing, 4(1), pp. 39–52
86. Jayasinghe, U., Otebolaku, A., Um, T.W., and Lee, G.M., (2017b), "Data centric trust evaluation and prediction framework for IoT," in ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), IEEE, pp. 1-7.
87. Jøsang, A., (2001) "A logic for uncertain probabilities", Int. J. Uncertain. Fuzziness Knowl.-Based Syst, 9, pp. 279–311.

88. Jøsang, A., Ismail, R., and Boyd, C., (2007), "A survey of trust and reputation systems for online service provision", Decision Support Systems, 43(2), pp. 618-644
89. Joshi, S., and Mishra, D.K., (2016), "A Roadmap Towards Trust Management And Privacy Preservation In Mobile Ad Hoc Networks", in 2016 International Conference on ICT in Business Industry & Government (ICTBIG). pp. 1–6.
90. Khan, T., et al., (2019), "A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks," in IEEE Access, 7, pp. 58221-58240
91. Kim, S., Kim, S., (2018), "User preference for an IoT healthcare application for lifestyle disease management", Telecommun. Policy, 42, pp. 304–314.
92. Kim, S.H., Chung, K., (2015), "Emergency situation monitoring service using context motion tracking of chronic disease patients", Clust Comput, 18(2), pp.747–759
93. Kouicem, D.E., Bouabdallah, A., and Lakhlef, H., (2018), "An Efficient Architecture for Trust Management in IoE Based Systems of Systems," in 2018 13th Annual Conference on System of Systems Engineering (SoSE), IEEE, pp. 138-143.
94. Kowshalya, A.M., Gao, X.Z., Valarmathi, M.L., (2019) "Efcient service search among Social Internet of Things through construction of communities", Cyber-Physical Systems, 6(1), pp. 33-48
95. Kowshalya, A.M., and Valarmathi, M.L., (2017), "Trust management for reliable decision making among social objects in the Social Internet of Things", IET Netw, 6(4), pp.75–80
96. Kumar, P.M., Gandhi, U.D, (2018), "A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases", Comput Electr Eng 65, pp. 222–235
97. Kwon, D., Hodkiewicz, M.R., Fan, J., and Shibutani, T., Pecht, M.G., (2016), IoT-based prognostics and systems health management for industrial applications", IEEE Access, 4, pp. 3659–3670.
98. Lee, K.-M.; Teng, W.-G.; Hou, T.-W., (2016), "Point-n-Press: An Intelligent Universal Remote Control System for Home Appliances", IEEE Trans. Autom. Sci. Eng., 13, 1308–1317

99. Levitt, T., (2015), "Internet of Things: IoT Governance, Privacy and Security Issues"
100. Li, J., Bai, Y., Zaman, N., and Leung, V.C., (2017), "A Decentralized Trustworthy Context and QoS-Aware Service Discovery Framework for the Internet of Things," IEEE Access, 5, pp. 19154-19166
101. Li, W., and Song, H., (2016), "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," in IEEE Transactions on Intelligent Transportation Systems, 17(4), pp. 960-969
102. 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
103. Lin, Z., and Dong, L., (2018), "Clarifying Trust in Social Internet of Things," in IEEE Transactions on Knowledge and Data Engineering, 30(2), pp. 234-248
104. Lin, Y.B., Lin, Y.W., Hsiao, C.Y., and Wang, S.Y., (2017a), "Location-based IoT applications on campus: The IoTtalk approach", Pervasive Mob. Comput., 40, pp. 660–673.
105. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., and Zhao, W., (2017b), "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, 4(5), pp. 1125-1142
106. Lounis, K., and Zulkernine, M., (2020), "Attacks and Defenses in Short-Range Wireless Technologies for IoT," in IEEE Access, 8, pp. 88892-88932
107. Lu, X., and Cheng, X., (2020), "A secure and lightweight data sharing scheme for Internet of medical things", IEEE Access, 8, pp. 5022-5030
108. Luvisotto, M., Tramarin, F., Vangelista, L., and Vitturi, S., (2018), "On the use of LoRaWAN for indoor industrial IoT applications" Wirel. Commun. Mob. Comput., pp. 1–11.
109. Lwin, M.T., Yim, J., Ko Y.-B., (2020), "Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks", Sensors, 20(3)
110. Maddar, H., Kammoun, W., and Youssef, H., (2018), "Effective distributed trust management model for internet of things", Procedia Comput. Sci., 126, pp. 321–334

111. Mahdavinejad, M.S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P., and Sheth, A.P., (2018), "Machine learning for internet of things data analysis: a survey", Digital Communications and Networks, 4(3), pp. 161-175
112. Mahmud, M., et al., (2018), "A brain-inspired trust management model to assure security in a cloud based iot framework for neuroscience applications", Cogn. Comput., 10(5), pp. 864–873
113. Meena, K.A., and Valarmathi, M.L., (2016), "Community detection in the social internet of things based on movement, preference and social similarity", Stud Inf Control, 25(4), pp.499–506
114. Memos, V.A., Psannis, K.E., Ishibashi, Y., Kim, B.-G., and Gupta, B.B., (2018), "An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework", Future Generation Computer Systems, 83, pp. 619-628
115. Ming, Y., Yu, X., and Shen,X., (2020), "Efficient Anonymous Certificate-Based Multi- Message and Multi-Receiver Signcryption Scheme for Healthcare Internet of Things," in IEEE Access, 8, pp. 153561-153576
116. Montori, F., Bedogni, L., Bononi, L., (2017), "A collaborative internet of things architecture for smart cities and environmental monitoring", IEEE Internet Things J., 5, 592–605
117. Mosenia, A., and Jha, N.K., (2016), "A Comprehensive Study of Security of Internet-of-Things", IEEE Trans. Emerg. Top. Comput., 5(4)
118. Najib, W., Sulistyo, S., Widyawan, (2019), "Survey on Trust Calculation Methods in Internet of Things", Procedia Computer Science, 161, pp. 1300-1307
119. Naranjo, P.G.V., Pooranian, Z., Shojafar, M., Conti, M., and Buyya, R., (2019), "FOCAN: A Fog-supported smart city network architecture for management of applications in the Internet of Everything environments", J. Parallel Distrib. Comput., 132, pp. 274–283
120. Nasir, S.U., and Kim, T., (2020), "Trust Computation in Online Social Networks Using Co-Citation and Transpose Trust Propagation," in IEEE Access, 8, pp. 41362-41371
121. Nitti, M., Girau, R., and Atzori, L., (2014), "Trustworthiness Management in the Social Internet of Things", IEEE Transactions on Knowledge and Data Management, 26(5), pp. 1253-1266

122. Nitti, M., Girau, R., Atzori, L., Iera, A., and Morabito, G., (2012), "A Subjective Model for Trustworthiness Evaluation in The Social Internet Of Things", in 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Comm. - (PIMRC). pp. 18–23.
123. Nitti, M., Pilloni, V., Colistra, G., and Atzori, L., (2016) "The Virtual Object as a Major Element of the Internet of Things: A Survey", IEEE Commun. Surv. Tutor., 18, pp. 1228–1240
124. Ortiz, A.M., Hussein, D., Park, S., Han, S.N., and Crespi, N., (2014), "The cluster between Internet of Things and social networks: Review and research challenges", IEEE Internet Things Journal, 1(3), pp. 206–215
125. Park, S., Park, J., and Oh, J., (2021), "Design and implementation of trusted sensing framework for IoT environment," in Journal of Communications and Networks, 23(1), pp. 43-52
126. Parthasarathy, P., Vivekanandan, S., (2018), "A typical IoT architecture-based regular monitoring of arthritis disease using time wrapping algorithm", Int J Comput Appl. https://doi.org/10.1080/1206212X.2018.1457471
127. Rahman, M.A., Rashid, M.M., Hossain, M.S., Hassanain, E., Alhamid, M.F., and Guizani, M., (2019), "Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City," in IEEE Access, 7, pp. 18611-18621
128. Rahmani, A.M., Gia, T.N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., and Liljeberg, P., (2018), "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: a fog computing approach", Future Gener Comput Syst 78, pp. 641–658
129. Rani, R., Kumar, S., and Dohare, U., (2019), "Trust Evaluation for Light Weight Security in Sensor Enabled Internet of Things: Game Theory Oriented Approach," in IEEE Internet of Things Journal, 6(5), pp. 8421-8432
130. Ray, P.P., (2016), A Survey on Internet of Things Architectures, Journal of King Saud University - Computer and Information Sciences
131. Roman, R., Najera, P., and Lopez, J., (2011) "Securing the internet of things", Computer, 44(9), pp. 51-58.
132. Safkhani, M., and Bagheri, N., (2017), "Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things," The Journal of Supercomputing, 73(8), pp. 3579-3585

133. 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," ICC 2020 - 2020 IEEE International Conference on Communications (ICC),pp. 1-6
134. Saied, Y.B., Olivereau, A., Zeghlache, D., and Laurent, M., (2013), "Trust management system design for the Internet of Things: A context-aware and multi-service approach", Computers and Security, 39, pp. 351–365
135. Saied, Y.B., Olivereau, A., Zeghlache, D., and Laurent, M., (2014), "Lightweight Collaborative Key Establishment Scheme for the Internet of Things", Comput. Networks 64: 273–295
136. Shabut, A.M., Dahal, K.P., Bista, S.K., and Awan, I.U. (2015), "Recommendation Based Trust Model with an Effective Defence Scheme for MANETs," in IEEE Transactions on Mobile Computing, 14(10), pp. 2101-2115
137. Shayesteh, B., Hakami, V., and Akbari, A., (2018), "A trust management scheme for IoT-enabled environmental health/accessibility monitoring services", International Journal of Information Security, pp. 1-18
138. Shen, J., Tianqi, Z., Fushan, W., Xingming, S., Yang, X., (2017), "Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things", IEEE Internet Things Journal, 5(4), pp.2526–2536
139. Sicari, S., Rizzardi, A., Grieco, L.A., and Coen-Porisini, A., (2015), "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, 76, pp. 146-164
140. Sivaraman, V., Gharakheili, H., Fernandes, C., Clark, N., and Karliychuk, T., (2018), "Smart IoT devices in the home: Security and privacy implications", IEEE Technol. Soc. Mag., 37(2), pp. 71-79
141. Song,T., Li,R., Mei,B., Yu, J., Xing, X., and Cheng, X., (2017), "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," in IEEE Internet of Things Journal, 4(6), pp. 1844-1852
142. Subrahmanyam, V., Zubair, M.A., Kumar, A., Rajalakshmi, P., (2018), "A low power minimal error IEEE 802.15. 4 Transceiver for heart monitoring in IoT applications", Wirel. Pers. Commun., 100, pp. 611–629.
143. Subramaniyaswamy, V., Manogaran, G., Logesh, R., Vijayakumar, V., Chilamkurti, N., Malathi, D., Senthilselvan, N., (2018), "An ontology-driven

personalized food recommendation in IoT-based healthcare system", J Supercomput, 75, pp. 3184–3216

144. Sun, X., and Ansari, N., (2017), "Dynamic resource caching in the IoT application layer for smart cities", IEEE Internet Things J., 5, pp. 606–613.
145. Sun, Z., Zhang, Z., Xiao, C., and Qu, G.,(2018), "D-S Evidence Theory Based Trust Ant Colony Routing in WSN", China Commun. 15(3): 27–41.
146. Suryani, V., (2016), "A survey on trust in Internet of Things", In Proceedings of the 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, Indonesia, pp. 1–6.
147. Tangade, S., Manvi, S.S., and Lorenz,P., (2020), "Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs," in IEEE Transactions on Vehicular Technology, 69(5), pp. 5232-5243
148. Tripathy, B.K., Dutt, D., Tazivazvino, C., (2016), "On the Research and development of Social Internet of Things", Internet of Things (IoT) in 5G Mobile Technologies, 8, pp 153–173
149. Truong, N.B., Jayasinghe, U., Um, T.W., and Lee, G.M., (2016), "A Survey on Trust Computation in the Internet of Things", The Journal of Korean Institute of Communications and Information Sciences (J-KICS), 33(2), pp. 10-27
150. Truong, N.B., Lee, H., Askwith, B., and Lee, G.M., (2017), "Toward a trust evaluation mechanism in the social Internet of Things", Sensors, 17(6)
151. Ureña, R., Kou, G., Dong, Y., Chiclana, F., and Herrera-Viedma,E., (2019),"A review on trust propagation and opinion dynamics in social networks and group decision making frameworks",Information Sciences, 478, pp. 461-475
152. Vasilomanolakis, E., et al. (2015), "On the security and privacy of internet of things architectures and systems", In: 2015 International Workshop on Secure Internet of Things (SIoT). IEEE
153. Wang, K., Qi, X., Shu, L., Deng, D.j., Rodrigues, J.J.P.C., (2016), "Toward trustworthy crowdsourcing in the social internet of things", IEEE Wirel. Commun, 23, pp. 30–36
154. Wang, J., Wang, H., Zhang, H., and Cao, N., (2017), "Trust and Attribute-Based Dynamic Access Control Model for Internet of Things", Proc. - 2017 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2017 Jan. pp. 342–345.

155. Wang, Y., Wen, J., Zhou, W., Tao, B., Wu, Q., and Tao, Z., (2019), "A Cloud Service Selection Method Based on Trust and User Preference Clustering," in IEEE Access, 7, pp. 110279-110292
156. Wei, L., Wu, J., Long, C., and Li, B., (2021) "On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things," in IEEE Internet of Things Journal, 8(6), pp. 4775-4787
157. Wu, T., Wu, F., Redoute, J.M., Yuce, M.R., (2017) "An autonomous wireless body area network implementation towards IoT connected healthcare applications", IEEE Access 5, pp. 11413–11422
158. Xiao, H., Sidhu, N., Christianson, B., (2015), "Guarantor and reputation based trust model for social internet of things", In: 2015 International Wireless Communications and Mobile Computing Conference (IWCMC),IEEE, pp. 600–605
159. Xu, L., Bao, T., Zhu, L., and Zhang, Y., (2019a), "Trust-Based Privacy-Preserving Photo Sharing in Online Social Networks," in IEEE Transactions on Multimedia, 21(3), pp. 591-602
160. Xu, L., Jiang, C., He, N., Han, Z., and Benslimane, A., (2019b), "Trust-Based Collaborative Privacy Management in Online Social Networks," in IEEE Transactions on Information Forensics and Security, 14(1), pp. 48-60
161. Xu, Q., Su, Z., Zhang, K., and Yu, S., (2021), "Fast Containment of Infectious Diseases with E-healthcare Mobile Social Internet of Things," in IEEE Internet of Things Journal,
162. Yan, Z., and Prehofer, C., (2011), "Autonomic Trust Management for a Component Based Software System," in IEEE Transactions on Dependable and Secure Computing, 8, no. 6, pp. 810-823
163. Yan, Z., Zhang, P., and Vasilakos, A.V., (2014), "A survey on trust managementfor Internet of Things", Journal of Network and Computer Application, 42, pp. 120–134
164. Yang, Y., Lichtenwalter, R.N., Chawla, N.V, (2015), "Evaluating link prediction methods", Knowledge and Information Systems, 45(3), pp.751–782
165. Yang, Y., Liu, X., Deng, R.H., (2018), "Lightweight break-glass access control system for healthcare Internet-of-Things", IEEE Trans Ind Inf 14(8), pp. 3610–3617

166. Yu, H., Shen, Z., Leung, C., Miao, C., Lesser, V.R., (2013), "A Survey of Multi-Agent Trust Management Systems", IEEE Access, 1, pp. 35–50
167. Yu, B., Singh, M.P., (2002) "An evidential model of distributed reputation management", In Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1; ACM: Bologna, Italy, 2002; pp. 294–301
168. Yuan, J., and Li, X., (2018), "A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion", IEEE Access, 6: 23626–23638.
169. Zhao, J., Huang, J., and Xiong,N., (2019), "An Effective Exponential-Based Trust and Reputation Evaluation System in Wireless Sensor Networks," in IEEE Access, 7, pp. 33859-33869
170. Zhang, P., Kong, Y., and Zhou,M., (2018), "A Domain Partition-Based Trust Model for Unreliable Clouds," in IEEE Transactions on Information Forensics and Security, 13(9), pp. 2167-2178
171. Zhang, J., Zheng, K., Zhang, D., and Yan,B., (2020), "AATMS: An Anti-Attack Trust Management Scheme in VANET," in IEEE Access, 8, pp. 21077-21090
172. Zhiyuan, L., Chen, R., Liu, L., et al (2016), "Dynamic resource discovery based on preference and movement pattern similarity for large-scale social internet of things", IEEE Internet Things, 3(4), pp.581–589