TRUST EVALUATION IN SIoT ENVIRONMENT

A Thesis submitted to the
Babasaheb Bhimrao Ambedkar University, Lucknow
in fulfilment of Requirement for the Award of Degree of

Doctor of Philosophy

in Information Technology

BY

Sunil Singh

Enrollment No: 648/14

SUPERVISOR

Dr. P. K. Chaurasia

Assistant Professor

DEPARTMENT OF INFORMATION TECHNOLOGY SCHOOL
OF INFORMATION SCIENCE AND TECHNOLOGY

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY

(A CENTRAL UNIVERSITY)
LUCKNOW, UTTAR PRADESH-226025

2022

DECLARATION

I, Sunil Singh declare that this thesis of research on **„TRUST EVALUATION IN SIoT ENVIRONMENT"** is my original work. The study has been conducted under the guidance of Dr. Pawan Kumar Chaurasia, at Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow. It is further declare that to the best of my knowledge and belief it has not been submitted earlier for the award of any degree and also undertake that the thesis is essentially free from all kinds of plagiarism.

Dated: …..……

(Sunil Singh)

Research Scholar
Department of Information Technology
Babasaheb Bhimrao Ambedkar University,
(A Central University)
Lucknow-226025, India

CERTIFICATE

This is to certify that the thesis titled **"TRUST EVALUATION IN SIoT ENVIRONMENT"** submitted by **Mr. Sunil Singh** is an original research work and has not been previously submitted in part or full for the award of any other degree or diploma to this or any other University.

The thesis submitted to Babasaheb Bhimrao Ambedkar Univesrity Lucknow satisfies all the requirements as stipulated in the *Doctor of Philosophy (Ph.D.)* regulations-1999 as amended in 2017 and it is fit for submission and evaluation for the award of the degree of Doctor of Philosophy of the University.

Supervisor

Head of the Department

Date:

ACKNOWLEDGEMENT

Foremost, I would like to express my sincere gratitude to my guide and supervisor Dr. Pawan Kumar Chaurasia for the continuous support of my Ph.D. study and research for his patience, motivation, enthusiasm and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I am short of words to convey my real feelings for his invaluable help and concern together with 'scholarly, insight and critical' guidance. I could not have imagined having a better advisor and mentor for my Ph.D. study.

Besides my advisor, my sincere thanks goes to Prof. R. A. Khan and Head of the Department, Dr. Dhirendra Pandey for his encouragement, insightful comments and research questions. I am very thankful to faculty members Dr. Raj Shree, Dr. Alka, and Dr. Amit Singh for providing moral support, encouragement and consultation during the course of study. I am also thankful to all research scholars, colleagues and office staff of the Department for their assistance and support.

I would like to express my sincere gratitude for my parents Shri Birendra Singh and Rajeindri Singh, for giving birth to me at the first place and supporting me spiritually throughout my life.

I owe my loving thanks to my wife Arti Singh, She has lost a lot during my research. Without her encouragement and understanding it would have been impossible for me to finish this work.

Finally, I would grateful acknowledge to my Hon'ble Vice-Chancellor Pof. Sanjay Singh, Babasaheb Bhimrao Ambedkar Central University, Lucknow for his invaluable support, encouragement and inspired me.

Sunil Singh

ABSTRACT

In recent era, IoT technology is capable to integrate numerous heterogeneous and homogenous in the form of a device object. Such objects tend to integrate environmental components and produce various services associated with them. These objects transform into smart objects because they generate a tremendous amount of information related to the physical environment through sensors, actuators, and general multipurpose computers. Due to the exponential growth of RIFD devices, which ensures heavy growth in network traffic? Therefore available Search engines simultaneously receive a large number of queries that are unable to handle and manage them efficiently through the currently available system.

Through this vision, many algorithms are introduced for real-time systems. The common characteristics were found in these algorithms targeted on the centralized system which are unable to scale up appropriately several numbers of devices and a tremendous amount of queries received. So handling the problem of scalability associated with such a centralized system, the term came into existence called Social Internet of Things. Due to the introduction of SIoT social relationships among social objects established by smart objects came into existence. The SIoT environment provided the ability to configure social relationships between human to human, tangible objects to tangible objects, and tangible objects to humans, hence social networking is a place where people communicate with smart objects [9]. The construction of social structure so formed has a social relationship fetter which turns a smart object into a social object. .

Various researcher has analysed that due to specific rules and regulations set by the owner of devices and frequently changing behaviour (malicious or cooperativeness) of social node are unable to serve desired services in the SIoT environment. For the same trust among social nodes is the effective major that can be utilized to have healthy and secure communication. Keeping in mind, the importance of trust in SIoT the researcher tried to focus the problem of identifying malicious nodes present in the social networks through evaluation of trust. We have found the major issues concerns with the trust evaluation by conducting the literature survey thoroughly related to trust evaluation models, mechanism and application in the field of Social Internet of Things. We find very few articles which focuses on computation of trust. For the same we identify the effective parameter of trust while having collaboration of social nodes with in social networks in terms of of trustor and trustee. The major effective

factors are quality of service, quality of data, past reputation and recommendation. The researcher also tried to find the sub factors as depicted in chapter two and classify them in appropriate manner.

To achieve the aim of our study we have proposed the framework of for trust evaluation by focusing the need and importance during research and computation of results. We have categorize the tust in the form direct and indirect collaboration of social of social object In chapter three we have depicted the working flow of our framework through flow charts. The planning and preparation phase firstly deals with the the problem of the identifying malicious social nodes during collaboration in two scenario i.e service requestor to service provide and service provider to service requestor and perform the thr selection group of experts in relevant fied to collect the data samples. Further we have defined the scope and boundaries asocial with fuzzy AHP. Through relative scale of importance we have converted the linguistic terms into triangular fuzzy number. Based on expert opinion, a fuzzified pairwise comparison matrix is constructed as depicted in chapter three and the performed the defuzzification using the value integration method.We also perform the normalization process at get authentic eigenvectors. A test is conducted to check the consisitency of fuzzified pairwise matrix through utilizing the values consistency ratio and random index. We have integrated fuzzy AHP with synthetic extent analysis and degree of possibility to prioritize the weight in effective manner and introduced the mechanism for direct and indirect trust to determine trust value of social nodes in both scenarios. After that we have applied the sensitivity analysis to check appropriateness of results.

Following the research methodology shown in chapter we determine the trust trust for ten social nodes in a local adhoc network in SR to SP and SP to SR and computed change in percentage of trust value for direct and indirect trust in Scenario 1 and 2 respectively. We have analysed our results by performing validation process theoretically as well as statistically by incorporating the experts' advice and suggestion and compute the trust value for same set of nodes for reassessment and found negligible changes. Hence our computed results satisfy the need of validation appropriately. The detailed explanation of validation is depicted in chapter five.

On the basis of trust evaluation in SIoT platform, the proposed model may classify the trustee and un-trustee nodes and it may use as measurement tool for identification of malicious of the node in social networks. It also sets the benchmark value of trust computation in industrial based social environment.

ABBREVIATIONS

SIoT	:	Social Internet of Things
IoT	:	Internet of Things
SN	:	Social Networks
P2P	:	Peer-to-Peer
TAs	:	*Trustworthiness Attributes*
QoS	:	Quality of Service
QoD	:	Quality of Data
SR	:	Social Relationship
CPS	:	Cyber-Physical System
MANET	:	Mobile Ad-hoc Network
TM	:	Trust Management
API	:	Application Programming Interface
CDA	:	Community Detection Algorithm
SMSC	:	Social management through Spatial Crowdsourcing
RM	:	Relationship Management
P-NO	:	Probabilistic Neighborhood Overlap
AHP	:	Analytical Hierarchy Process
CoI	:	Community of Interest
MCDA	:	Multi-Criteria Decision Analysis
AHP	:	Analytical Hierarchy Process
TFN	:	Triangular Fuzzy Number
CPM	:	Combined Pairwise Matrix
SR	:	Service Requester
SP	:	Service Provider

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

Introduction

CHAPTER 1: INTRODUCTION

"If we do not trust one another, we are already defeated."

-- Alison Croggon --

1.1 Background

From last two decades, the trends of IoT have changed and enchanted a great deal of research. Scientists and researchers developed various smart devices, where a large number of distinct types of objects are connected to resolve critical problems. Data generates from various IoT device activities like information sharing, trust of nodes, security management, and privacy. These devices produced a huge data in different formats that can collect, integrate, treated, and analyzed to extract useful information. All these data are generated from heterogeneous devices and decentralized network environments[1]. Objectives of the IoT enabled devices are a high impact on the behavior and activities of the owners. The involvement of these IoT devices with society changes the nature and activities of human beings. To resolve some of the social issues, a new paradigm was involved, known as the Social Internet of Things (SIoT). Sample of data has represented the notion of everything, anything to access [2]. The notion of representation of data in various formats, change of time, and social networks change the behavior and activity of IoT devices. The sensitivity of visual devices makes things more sociable. It means, IoT gives social development and implements novel relationships between the social and objects as shown in figure 1.1 [3]. The combination of IoT and Social Networks (SN) leads to the SIoT, known as the Social Networks (SNs) of intelligent objects. The domains of the IoT environment expanded the novel integration. The domains of a social network within the current IoT models, reproduce additional novel frameworks for modern society.

It allows people and objects to interface with each other in a social network. The structure of the SIoT network depends on the requirement of navigability, performing objects, services innovation, and to make ensure the scalability of the objects in social networks[4]. However, the value of the trust may certify the strength of the degree of interaction among the objects. Further, these findings can extend the heterogeneous performance and diplomatic information, which is being shared with the connected objects. This dynamic behavior of the objects brings new challenges to developing a trustworthy environment between connected objects[5]. From various research papers, it is found that these dynamic challenges are communicated only by the security issues involved with the devices and users. But the social and individual issues among IoT objects and services are left. Therefore, the concept of trust

in SIoT environment can be observed as a key challenge[7]. Most of the researchers focused to establish trustworthy and reliable services between the connected objects.

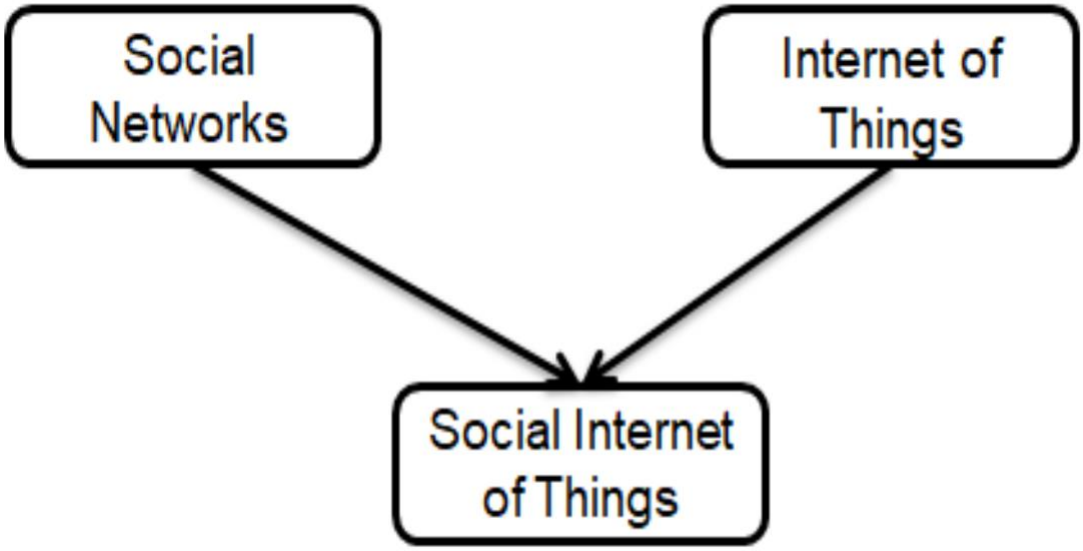

Figure 1. 1: Notion of Social Internet of Things

Various scientists and researchers defined trust in their own words as "*Trust is a belief between trustor and trustee that the trustee will provide or achieve a trusted goal as trustor's assumption*". The device that needs to depend on another device is known as the *trustor* (also known as the service consumer). The device that provides resources or services to trustors is known as a *trustee* (also known as a service provider) [8]. In the case of SIoT environment, the trustor may be a human being, devices, systems, applications, data, and services. It is a way of representation, with distinct meanings for both users and the framework, influenced by both determined and non-determined parameters. In extreme situations, trust can be elaborate as *"It is a qualitative or quantitative property of a trustee measured by the trustor for a particular objective in special conditions and a specific period*"[9]. It is an elementary decision that affects the requirement of an object to assess a particular service or device provided by a spare one. It is observed in day-to-day life that when we purchase any product, we generally buy a branded product due to trust in brands that provide quality products in comparison to unknown products[10]. It comes from our experience or with the *reputation* of the brands. It also comes from the opinion of different people who have experience and is *recommended* by family and friends about the product [11]. For some other trust issues, it is difficult to evaluate the accurate value of trustworthiness of an object or device. It is very difficult when distinct object performs isolated explanations and observations regarding trustworthiness. Therefore, it is very difficult to assign the trustworthiness value to the service provider and services [12]. Like, a customer assigns the "*very trustworthy*" to the provider for

a transaction from the same provider. Such types of distinction are to distinguish the accuracy of the trust of an object.

Still, there is not any comprehensive solution in respect of trust modeling, trust management, trust management framework, and trust quantification for assessing services and quality of data in a social environment. Therefore, the objective of the work is, to highlight reasonable research issues in the area of SIoT and view a plan of action, which can assist to establish trustworthy services, and data [13].

1.2 Social Internet of Things

Information Technology emerged as a new technology termed the Internet of Things (IoT). In the last two decades, there are drastic changes in the usage of IoT devices. Billions of people are connected with smart objects. On the base of usage, communities are developed in a heterogeneous environment on common needs and interests as well as the advantages of social relationships[14]. The first idea of *socialism of objects* was introduced by Holymquist et. al. Billions of IoT devices were developed and connected with the internet. These devices interface between the owners of devices and society. To take critical decisions and data transmission in society. It is important to make ensure the trustworthiness of the information and services. It is a collective measure of smart objects and the social relationships between them. As shown in figure 1.2**,** a number of the populations are connected with the objects [15].

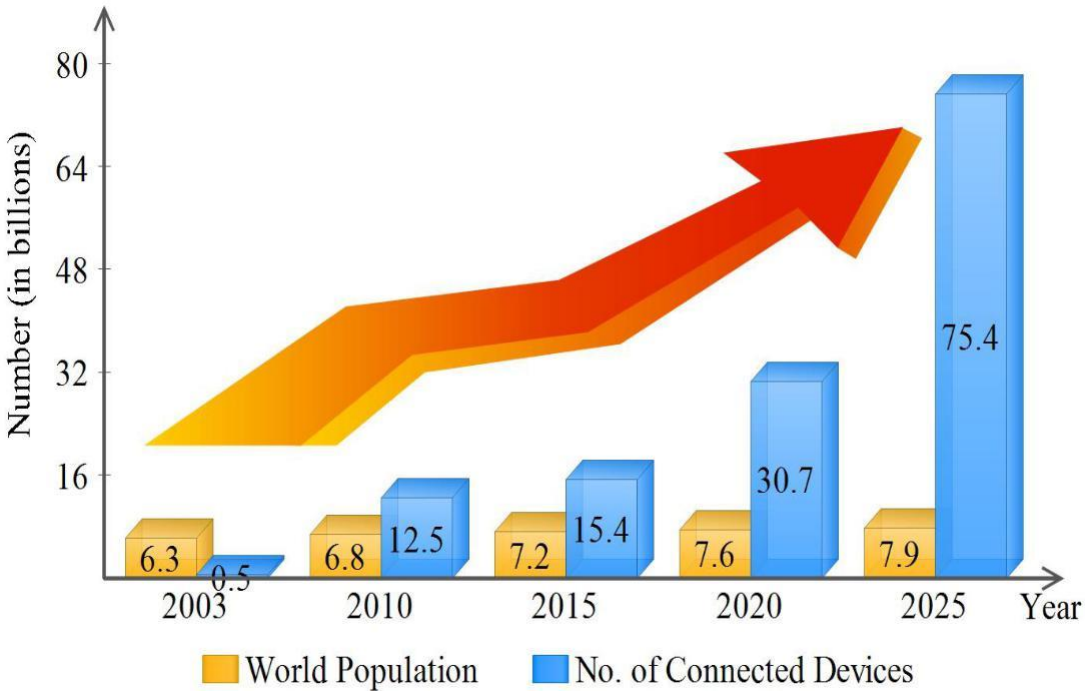

Figure 1. 2: Population connected with devices

In our daily life, the role of these internet-enabled objects is to solve the complexities of social relationships based on common interests. To solve these complexities, people interact with the communities and collaborate with the people of the society.[16] The progressive timeline of smart objects improves the performance of these smart objects as shown in figure 1.3.

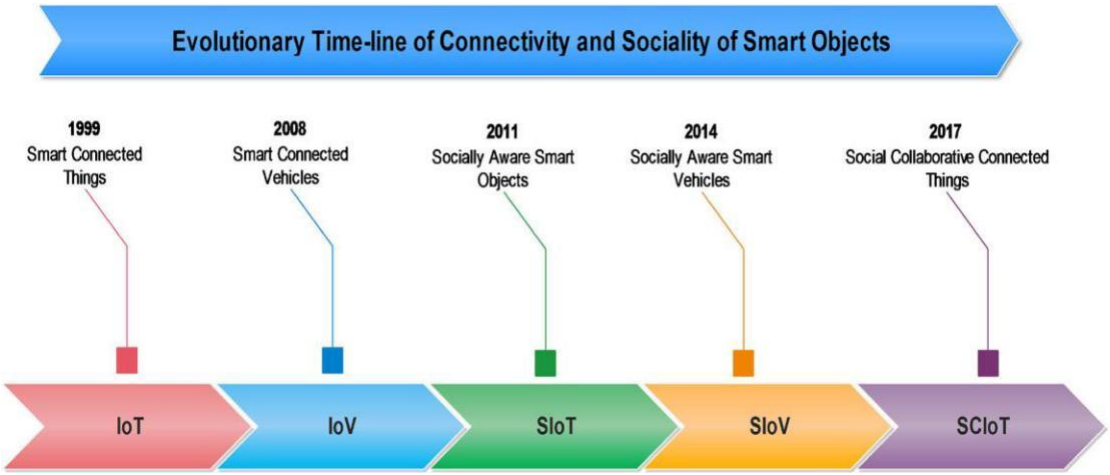

Figure 1. 3: Timeline of SIoT

These social object parameters allow them to interact between social networks and social communities and control the relationship without human intervention. It makes it different from other integrated devices [17]. Table 1.1, presents the comparison of two domains, IoT and SIoT. The social environment produced their relationship according to their interactions, and protocols acquire services within the network. Such malicious nodes are required to identify and restricted in the connected social network. Therefore, trust is the fundamental issue in the selection of the node.

Table 1. 1: Comparison of IoT and SIoT

Paradigms	Trust Attributes	Features Characteristics	Challenges	Disadvantages	Interactions
IoT	Temporal Trust, Reliability Trust, Dependence Trust, Fulfillment Trust Competence Trust	Intelligence, Connectivity, Sensing, Analyzing, Active Engagement	Scalability Security Privacy Maintenance Data management, Maintenance	Privacy issues, Technology over reliance, unemployment	H2H T2T
SIoT	Relationship Trust, Confidence Trust, Spatial Trust, Persistence Trust, Willingness Trust, Event Trust, Context Specific Trust	Social Interactions, Dynamic Nature, Social Role, Intelligence Object Discovery	Compatibility I/O Data Configuration Relationship Hardware Selection	Direct interaction, facilates laziness, ethical imlications	H2H T2T H2T

1.3 Trust Evaluation

With the increase of importance of trust in SIoT, mass research groups and agencies involved in trust-related domains in heterogeneous network environments like peer-to-peer (P2P) networks, wireless sensor networks, social networks, e-commerce, e-business, banking network, transport network, etc. in many applications and services to exchange or share the access control. To develop a proper trust platform, numerous domains of trust are taken into consideration like trust evaluation, trust management, and trust quantification. In this thesis, the researcher focuses on trust evaluation in the SIoT environment[18]. Besides these, the researcher also focuses on the mapping between trust attributes, the weight of trust attributes, and trust updates. Some of the researchers proposed trust evaluation techniques based on a set of information which is known as *Direct Trust*. It isolates the trustee's characteristics by observing trust behavior. These domains are used to describe the characteristics of trust attributes which are known as *Trustworthiness Attributes* (TAs) [19]. These trust attributes are combined to make overall trust represent the trustee's trustworthiness. By using the third part parameters like Quality of Service (QoS), Quality of Data (QoD), and Social Relationship (SR) have been used which is known as *Indirect Trust* [20]. The platform cooperates with applications, and services to secure activities and provide a better quality of services and information.

1.4 Trust Evaluation in SIoT

Trust is not related to a specific area. It is a very broad concept, over multiple applications, disciplines, and subject areas. There is not any common definition of trust. Studying the impact of trust is very important in our real world or digital world. The working of SIoT network performance is different from social networks [21]. It is a huge size and dynamic behavior with its limitations. Here, we consider two types of trust known as direct and indirect trust. Direct trust is associated with honesty, collaboration, and appreciation values[22]. The value of direct trust is assigned from one object to another object based on the experience and the communication between the two devices. If the two devices had never communicated with each other known as indirect trust. It depends on the monitoring and prior experiences of one device with another device. The domain of honesty and indirect trust is used to define the guidelines and mechanisms to implement trust-related attacks.

1.5 Relevant Issues

Human beings take decisions on a trust basis that we have to depend on a third party. These decisions are inherited and help us to investigate risk features to build a perception of trust.

With these features, humans may take necessary actions at the stated time to avoid any threats due to malicious nodes. Various trust-based solutions discussed in the review literature are based on distinct problems [3]. These issues take place as a common drawback in this area to reduce trust-related attacks in the SIoT. Incapacity of things to build up useful information like devices generate vulnerable data related to the environment. As a consequence, it is crucial to implement trust as a significant value to be used in a digital society[13]. To relieve risks and realize insight of trust for self-evaluation, which shows the research objective of the work. Therefore, the problem is used to quantify trust as a computational property in a digitized society. The available solutions provide a malicious free network and demonstrate a trustworthy SIoT environment for its users. It is used in many applications across various disciplines and research areas, but still, there is not any common consented definition. Various platforms exist for the SIoT implementation. The creation of groups and establishing the relation between objects is the main task of the SIoT network [23]. IoT devices established communication with peer nodes to access services using a set of protocols and heuristics [24]. The existing mechanism for trust evaluation is quite common in Cyber-Physical System (CPS) like Peer-to-Peer (P2P), Mobile Ad-hoc Network (MANET). There is not any pervasive evaluation model or platform to extract TMs from CPSS [25]. Physical devices are controlled by human beings and socially connected by physical-cyber social systems. Collaboration of objects is self-governing, which generates new challenges like security, privacy, trust, service, classification, behavioral classification, prediction, identity management, etc. Data management, data integration, and query processing are the major obstacles to the real-time deployment of SIoT networks[26]. In some circumstances, it is impossible to estimate the trust level of the services and data. There is not any guarantee for reliable communication among objects in SIoT environment. Therefore, the main requirement is to build trust and provide service invention in SIoT environment. The following issues should be considered for building a trusting and healthy SIoT network.

- What are the factors that assess the autonomous decision-making process among objects?
- What are the mechanisms to identify malicious objects in SIoT are vital?
- What are the factors that directly influence the social network?
- What are the factors affecting the trust of the objects or nodes?
- Is there any relationship between trust attributes?
- How can we relate one factor of trust to another factor?
- Is there any evaluation mechanism available for trust evaluation?
- Is it possible to evaluate the trust of the object at an early stage of collaboration?

- What is the quality of measures to evaluate the structure of SIoT network for assessing the information and collaborations?
- What are the methods required for easy and flexible assessment of resources/services inside and outside the SIoT communities?

From the above discussion, it can be concluded that the detection of malicious nodes in SIoT environment is a new challenge for the software industry and the social communities. Therefore, with the help of trust evaluation, the trust evaluation framework and evaluation mechanism improve the confidence level of the objects or nodes to collaborate with the network or the objects.

1.6 Problem Formulation

Trust evaluation is one of the emerging techniques in the computerized environment. It shows one of the important domains represents mitigating hazards concerned with privacy, security, and protection of the integrity of the interaction of the objects. The notion of trust develops a healthy and trustworthy environment for its users. Therefore, there is a requirement for a framework or technology to solve before executing in a physical world to avoid redundant issues which can take action within the system. Therefore, based on the above problems, and motivated by the researchers which are as follows:

- Regularize the concept of trust evaluation in SIoT environment:
- Design and development of trust evaluation mechanism for SIoT environment:
- Prioritize the trust attributes to evaluate the impact on trust in SIoT environment:

Keeping the above point in mind, the researcher has formulated a problem to develop a framework to evaluate trust in the social network.

"TRUST EVALUATION IN SIOT ENVIRONMENT"

1.7 Objectives of the Research

The investigation intends to recognize the benefits of organizing trust in a SIoT environment to measure the services, quality of data, and social relations. These domains defined the limitations of its interpretations and proposed a trust evaluation framework to decide the applications and services to objects independently to establish trust among them. Therefore the proposed solution should be able to fill the research gap between the existing techniques and propagated techniques. Therefore, to achieve the generic goal an approach for estimating the trust and identifying the untrusted nodes with the following objectives are as follows:

- To review and critically study the literature on the Internet of Things, Social Internet of Things, Trust evaluation mechanism, and to measure the untrusted nodes.
- To identify the new attributes of trust management.
- To identify the new sub-attributes of trust management.
- To identify the relation between trust attributes.
- To appreciate the need, importance, and significance of identifying the untrusted nodes and malicious nodes in the early stage in the SIoT environment.
- To develop a viable and perspective framework for Trust evaluation using its properties.
- To prioritize the weight of each attribute and assign the ranking using the Fuzzy approach.
- To validate the proposed framework.

1.8 Research Methodology

The proposed work includes the task to evaluate the trust of the nodes and measure the weight of each sub-domain. The proposed framework and its implementation is used to provide the malicious free network to the users and the connected devices. The methodology is supposed to incorporate various phases which are as follows:

- Conceptualize, review, and revision of the specification.
- Proposed Framework.
- Implementation of Framework.
- Implementation of Trust Evaluation Phases.
- Expert Review and Revision.
- Validation of framework.
- Documentation and finalization.

In this research, we will be focusing on the evaluation of trust in SIoT environment. The result will help in improving the social network. In addition, the results will also help in identifying the malicious nodes and improve the security of the network.

1.9 Significance of the Study

To capture the significance of quality of the service or quality of data related to information for trustworthy evaluation. Quality of service increased to improve the trust between the nodes. It is reasonable to assume that, the higher quality of service, and the quality of

information, the more trust is built up among the associated devices. If we decreased the quality of service, then trust automatically will be decreased.

1.10 Limitations

Everything has good and bad aspects. If we think research point of view, both have their importance. The good presence recommends new measurements for the novel study while the bad presence focuses on the failure of the work. Subsequently resolving the failure of the work, the redesign of the work discovers new features. There are various reasons for the adaption of the new approach, and its limitations also. In addition to the successful completion of the research work, the study was organized with the following limitations:

- The approach can be applied for trust evaluation by considering only three attributes.
- Due to the lack of industry data, the proposed framework is validated through a small set of data.
- To evaluate trust, quality of service and quality of data are chosen from various trust parameters.

1.11 Thesis Outline

A thesis of the research has been prepared to meditate on the detailed study of the research problem and previously mentioned research questions.

Chapter -1: Introduction

The first chapter is the introduction of the thesis. The chapter starts with the background of the internet of things and the social internet of things. some points are highlighted about the social internet of things, that need to identify the cause of malicious nodes. The second part is the trust of the nodes. The research question is generated to collect views to improve the value of the trust. Based on the incorporation of the suggestions, trust is improved. The objective of the research is framed. At last, the limitation of the research work is discussed.

Chapter-2: Literature Review

This chapter is related to the existing approaches to the Internet of Things and the Social Internet of Things. A detailed review of trust evaluation and the social internet of things over the last decade is presented. A detailed review of some significant existing models from the last decade is presented. Based on the review it is identified that the value of trust is increased by improving the quality of service and social relationships. Malicious node detection in a social environment is identified as a key factor in the network through literature surveys and

reviews. Therefore, there is a requirement of trust value to detect whether the node is a trustee or untrusted.

Chapter-3: Proposed Framework

This chapter presents a framework for trust evaluation in the social internet of things environment using a fuzzy approach. The chapter covers detecting the malicious nodes in the social environment at the time of the entry of nodes in the network. The assumption of the framework is presented. A framework for trust improvement of the network in SIoT environment is proposed. This framework consists of five phases, including the identification phase, categorization phase, evaluation phase, validation phase, and wrapping phase.

Chapter-4: Implementation of Framework

The objective of this chapter is to implement the proposed framework. The whole framework is divided into five phases. Identification phase, categorization phase, computation phase, validation phase, and wrapping phase. To evaluate trust, five factors are identified for evaluation of trust; quality of service, quality of data, and social relationship every four sub-factors, and the remaining two main factors are considered as reputation and recommendation. By using the fuzzy approach, multi-criteria decision analysis is used to evaluate the trust value of the node.

Chapter-5: Validation of the Framework

This chapter shows the theoretical and empirical validation of the proposed framework. As an experimental validation, pre-tryout is carried out of trust evaluation design. On the bases of the trust evaluation framework, metrics values of attributes are computed. On the base of expert‟s suggestions for the improvement of trust. Trust value is evaluated. It is then verified that the QoS, and Social relationships are maximized and QoD is minimized. After reevaluating of trust evaluation value is improved from the previous value. For the tryout purpose, ten nodes are connected. The same process is reproduced and is resolved that the approach performs well in this experiment. Various statistical studies and hypothesis tests were carried out for the acceptability of the framework.

Chapter-6: Conclusion and Future Scope

The last chapter of the thesis is the conclusion of the work. In this chapter, major research findings along with the other findings are presented. The research objectives of the first chapter are incorporated one by one in this chapter. The significance of the research is also discussed at the end. Plans for extending the study are also discussed.

Chapter 2

Literature Review

CHAPTER 2: LITERATURE REVIEW

"When the trust is high, communication is easy, instant, and effective."

-- Stephen Covey --

2.1 Background

With the rise of smart SIoT communication, several next-generation applications have been incepted providing large-scale services in education, health care, manufacturing remote area monitoring and control, and surveillance systems. Such services are provided by different social node devices using social relationships connected through existing ISP (trustee). Hence various trust-related issues, quality of service level, and quality of data are major areas to focus on.

Trust is explained as “The powerful and sustainable conviction of any entity to act securely, reliably and integrally within a specified context and an extent of subjective belief analyzing the behaviors of a particular entity". The anticipated behavior of any entity's actions can be observed by self-observation or by history-based calculations termed repudiation[27]. The idea of trust has its origin in social science literature to identify the specific stage where a member of a particular society called the trustor has faith and belief in a task executed by another member of a different society called the trustee. Security and trust are expletive to each other like security parameters in daily life such as fences, locks, and gates. The trust is needed to appropriate behavior of SIoT devices anywhere anytime like same we put these fences, locks, and gates in the SIoT platform to maintain various phases for inert process communication.[28] Trust-based models enhance the layers of SIoT integrity and architecture and provide a supporting role in data and service management and also boost social service in SIoT. Trust Evaluation is a prominent issue that prevailed in SIoT. It allows various users, devices, and entities to communicate their views about trustworthiness to nearby objects.[29] The data transfer and minimizing uncertainty among various nodes and objects, the factor of trust matters a lot in the SIoT environment. In the context of SIoT, the achievement of trustworthiness among social nodes operating multiple services can be very difficult[30]. The further section of this chapter has a

critical review of the literature regarding trust evaluation platforms, social node selection, and multi-criteria decision-making techniques utilized in SIoT environment.

2.2 Trust Evaluation and Node Selection

There are many trust evaluation common models, which can be evaluated in the literature review. Some papers considered reputation-based, knowledge-based, aggregation method, application purposed, and intelligent based. Trust evaluation methods have been investigated under various parameters including IoT with different objectives and goals. To evaluate the trust, some of the points are described here which are as follows:

Trust management plays an important role in the field of IoT for reliable data transmission and quality of service and enhancing user privacy. Quality of service refers to the belief that an IoT device can provide service to the service requester. It refers to performance and is measured by competence, cooperativeness, reliability, capability etc. to measure the QoS trust. In [31], define end-to-end connection, energy consumption, and packet delivery ratio to measure QoS trust. Some of the strong effort done by the researcher is discussed below:

- **In 2011, Aztori et. al**.; presented the first architecture for SIoT in 3 levels namely the physical layer, component layer, and application layer. The physical layer deals with smart tangible devices, communication protocols, and network technologies. The component layer is associated with service search, device identification, node selection, and semantic management. The application layer deals with a client, services, object interface, and application programming interface (APIs) [32].
- **In 2014, Bao et al.;** measured social trust by connectivity, intimacy, and honesty. It is especially common in social IoT systems where IoT devices should be evaluated not only based on QoS trust but also based on social trust. When considering a reputation and recommendation, an IoT device may trust its socially connected devices over unrelated devices [9].
- **In 2012, Tang et. al**.; proposed a network department technique based on the statistics diffusion version for communities falling under the SIoT environment. The two modules of the proposed technique comprise of

network fracturing module for the friend section and the network meeting module. The propagation of smart devices is quantified using these modules and bright parts include adaptability, and scalability in a large complex SIoT environment [33].

- **In 2015, Xiao et. al**.; proposed a SIoT-based domain guarantor and reputation to evaluate trust. To get access to the services from an object, it is categorized into parts. Perfect solutions service provider gets a higher rank while those who do not participate in any appropriate service by the objects with lower rank are known as malicious objects. Such a type of approach is used to determine the dishonesty of the objects. Such types of concepts perform in a social network and develop a social structure in IoT objects in SIoT environment. It defines as the social relationship between the device owners and is measured by intimacy, honesty, privacy, and connectivity [34].
- **In 2015, Chen et. al.;** proposed 3 types of relationships consisting of clients' communication through social friendship and social interrelation and CoI by utilizing the social trust parameter. The problem with this work is they have not considered various attack approaches to objects[35].
- **In 2016, Ruan et. al**.; proposed a trust management framework to support agents to evaluate their partners „trustworthiness". Trust cannot be fully measured. It is not possible to measure accurate trust due to a large domain from natural to physical connection of the trust relationship[36].
- **In 2016, Nitti et. al.**.; In this paper the author address issue of smart discovery of object through object detection algorithm-based similarity of structure in a distributed environment to provide a particular application-based service. Efficiently query solving by using the suggested algorithm major benefit of this article while scalability, cost, semantic-based length among services, and response time are out of focus [37].
- **In 2017, Kasnesis et. al.;** presented an amalgamation of cognitive IoT and SIoT using semantic-based web engineering and social agents. The social friendship among smart devices has a semantic synonym to make a complex decision using two ontologies for goal management. In conclusion, the scalability under decision-making boosts relationship management using machine learning algorithms [38].

- **In 2017, Truong et. al.;** proposed different scenarios for models where that include the triad of reputation, experience, and knowledge-based mobile crowd sensing through TMS to compute trust for several parameters. The SIoT services deal with reputation, recommendation, and knowledge. Car-sharing service is used as one of the best examples to consider their approach [39].

- **In 2018, Roopa et. al.;** analyzed 5 approaches to focus on the problem of friend selection within a social network of SIoT in terms of genetic algorithm to determine specific services by smart objects located in SIoT networks. The positive side of the article deals with SIoT performance regarding mean path length, means clustering, and mean node degree while the downside, the proposed methodology is latency and cost is out of the author‟s vision [40].

- **In 2018, Farhadi et .al.;** examine the problem module of relationship management through a brand new strategy able to control and management of friend requests in a SIoT environment. They used Naïve based methodology and weighted-based strategy for friendship creation and a random service model to test various relationship management algorithms. The advantageous part of the article presents gradual improvement in terms of, delay, throughput, path length, and friendship degree [41].

- **In 2019, Atzori et. al.;** handle social friendship among smart objects the authors depicted a novel architecture-based framework that can perceive information required to produce social relationships and make the SIoT environment updated by utilizing algorithms of determining. The relationship Management component presented under this mechanism can able to discover new social friendships. The building of social friendship among smart objects using relationship management improves mobility and dynamic linkage is the merits of this article. Handling incoming traffic through a recently added smart device under a detection algorithm didn‟t produce a better result[42].

- **In 2019 Yan et. al.;** understand the specification and informational parameter within the profile of socially smart devices having social

relationships perform appropriately service detection and friend selection utilizing the proposed novel framework. Achieving adaptability, scalability, and search time positive significance of the paper while they did not analyze the variation of friendship among smart physical objects through the presented algorithm shows the downside of this article[30].

- **In 2019, Chen et. al.;** proposed a newly Temporal Based End User methodology for smart social objects based on a recommendation system with social similarity which offers a selection of Friendships under a SIoT environment. The time-aware efficient recommendation that satisfies all primary rules is the most important advantage of this approach [43].

- **In 2019, et. al.;** proposed an ontology-driven recommendation-based system for friend selection and relationship management under the SIoT environment which perform recommendation according to user requirement and interest like opinion, motive, demographical information, and sequence of traveling. The merit of this strategy under recommendation is possible accurate outcomes utilizing user information implicitly and explicitly both [44].

- **In 2019, Xiao et. al**.; proposed a decentralized environment, desirable service discovery, and building social friendship relationship-based required services through a proposed novel social-like semantic technique. They utilize the ontology OWL tree to describe service. The outcome of the proposed methodology maximized the navigability under the SIoT environment based on features of a local network using social friendship relationships. The network traffic and energy consumption reduces using an adaptive forwarding approach [45].
- **In 2019 Rehmani 2019 et. al.;** depicted the improvement of SIoT community-based network navigability through a set of rules based on the proposed singular query primarily mechanism and try to improve scalability and friendship choice selection in a complex SIoT environment using small global residences [46].

- **In 2019, Aljubarney et, al.;** proposed a Bayesian-based prediction model and examine the physical object in the SIoT network under upcoming friendship. Here author considers two algorithms to identify the point of contact of the smart object and examine the relative position where and when the two objects meet. The outcome of a proposed model is more effective than other approaches analyzed.
- **In 2019, Halder et al.;** proposed a novel methodology for lifetime selection of a friend through clustered-based solutions in SIoT using Lifetime Based maximizing Optimal Clustering model they utilized Static CH-based clustering criteria but did not evaluate mobility[47].

- **In 2020, Lee et. al.;** proposed a knowledge Desire Intention model based on a recommendation approach to social friend selection SIoT environment. In the present article, the basic achievement of high accuracy through recall outcome is based on precision value while comparing the result with other solutions. The major weaknesses of this article depict an unscalable system and cost-effective criteria are missing [47].

- **In 2020, Kowshalaya et. al**.; proposed Community Detection Algorithm (CDA) to analyze SIoT environment service quality and its structure by using parameters of triangular participation ratio and modularity associated with it. Further, the author described effective service discovery to find social community through Inter and Intra community-based algorithms[48].
- **In 2020, Khanfor et. al.;** perform a spatial task in the SIoT environment through Spatial Crowdsourcing (SMCS) author proposed an Integer Linear program regarding spatial recruitment using SMCS for SIoT networks to extract smart objects finally. Lowest time complexity and community overlapping‟s merits and demerits respectively [49].
- **In 2020, Rajendran et al**.; use social relationships under the SIoT environment to enhance the relationship management process through recommendation-based techniques. The merits of this proposed model are searchability and high accuracy. However, termination and updation are losing factors governing relationship management are demerits[50].

- **In 2020, Marche et al.;** proposed a model based on Naïve Bayesian Classifier based Algorithm and Randomly allocation of services by utilizing a Proposed genetic-based Methodology for the creation of social friendship to locate an optimum solution. The network parameter is Average degree, average path, and mean clustered coefficients. The main disadvantage of this study is scalability factors were not taken into consideration [51].
- **In 2020, Rehman et. al.;** proposed a novel framework Utilizing a query-based information search strategy to enhance network navigability in the SIoT environment. The used Data searching model is based on a rule query mechanism for Social objects Prioritizing based on the service class criteria while the real world is missing[52].
- **In 2021, Mendoza et al.;** change the exposure of the client's nearby objects and QoS to evaluate the trust value between the trustor and the trustee. Each client may deposit the information of each trustee and store all the details of the nodes and their experiences. The proposed model detects the malicious nodes and stores the information in a form of a table for lightweight IoT devices [53].
- **In 2021, Narang et al.;** proposed the implementation of a SIoT-based service network in a multi-vendor environment of heterogeneous devices is the issue of trust. A hybrid trust management framework that makes use of Probabilistic Neighborhood Overlap (P-NO), a method for estimating tie-strengths between the nodes [54].
- **In 2021, Awan et. al.;** offered a model for TMS to manipulate trust deals with inter-domain communication during deploying services in IoT networks. The model presented concentrates on centralized controlling of client service requests and performs storage for data trust value and generates certificates that are not capable of ensuring scalability of the system. In addition to that, the objects with strong social friendships and spiteful clients that perform various types of attacks are not considered part of the system [55].

2.3 Multi-Criteria Decision-Making Techniques

In early 1970, Thomas L. Saaty introduced a multi-standard for performing reasonable decisions using the keyword analytical hierarchy process(AHP). It was introduced for structuring, measurement, and synthesis to perform the pairwise

comparison using a comparative significance fuzzy scale depicting the preference of decision-makers to select criteria and cost-effective parameters for a given problem. Such comparisons transform into matrices and are used to evaluate the weightage of specific criteria and metrics by following the intermediary of NFCM. There are two different methods are utilized for the formation of a pairwise comparison matrix namely scaling associated with a crisp digit (i.e. one to nine) and scaling on fuzzy digits. The methods given by Saaty utilize scaling (one to nine) for decision-makers through lingual terms like just equal, weakly important, etc.

The appropriate ideology related to fuzzy grouping given by Zadeh, 1965 is frequently utilized in literature to represent the ambiguity in human perception. It signifies the pertinence of an object in a range of 0-1 and has found many applications used in the last two-three decades. Some of the applications were fuzzy sets include are healthcare, traffic management, and control theory. The theory related to fuzzy sets depicts fuzzy values as integers and membership functions associated with boundary values as shown in figure 3.2. in the chapter. These values may be the same utilized by researchers to signify lingual terms to remove uncertainty and vagueness in personal perception. Hence fuzzy-AHP is the integration of fuzzy logic with AHP which utilizes arithmetic operation laws, random index, and consistency ratio to depict FPCM is consistent or not, to compute weight values.

To entertain these problems, numerous techniques have been proposed for many years to extract comparison matrices for better efficiency. Such techniques are admired by the various researcher in their work (Van Laarhoven and Pedrycz, 1983; Boender et al., 1989; Buckley, 1985; Deng, 1999)[56],[57]. Students and academicians are referred for critical literature analysis based on the F-AHP mechanism and platform applicable. Various academicians and researchers have frequently used the MCDM strategy for performing service selection and ranking of parameters. Hence, MCDM is a bunch of several techniques like AHP, TOPSIS (Technique for Order Preference by Similarity to Ideal Solutions), ANP (Analytic Network Process), ELECTRE (elimination and Choice Translating Reality), and many more ranking mechanisms utilized by academician to elucidate issues and major problems related to the physical world.

- **In 2020, Bharti et. al**.; to optimize the process of friend selection within the SIoT environment the author proposed a novel framework called Optimal Resource Discovery and Section (ORDS).To represent knowledge parameter author utilize the capability of Ontology-based on a semantic description. Further, they used a fuzzy-based set of rules to understand what knowledge has generated. The benefit of this approach suggested is more qualified than the existing results of other algorithms. On the other hand, the study shows a poor aspect of scalability [58].

- **In 2019, Cuka et. al.;** proposed a fuzzy-based mechanism for the smart selection of smart physical devices that are deployed in the SIoT environment by utilizing a fuzzy logic model. They used Device remaining energy, device inter Contact time, device inter distance, and device buffer occupancy as network parameters. The main demerit analyzed due to High Complexity due to numerous constraints associated with the existing system [59].
- **2018, Alshehri et. al**.; proposed a fuzzy logic-based protocol for detecting on-off attacks, contradicting behavior attacks, and other bad nodes. This protocol allowed nodes to transfer securely from one cluster to another. Additionally, the protocol utilized fuzzy logic to identify bad nodes and limit their untrusted role of making erroneous recommendations regarding nodes in the network[60].
- **In 2020, Baranwal et. al**.; proposed a framework that makes use of multi-criteria decision making (MCDM) as a combination of known approaches under the names Analytic Hierarchy Process (AHP) and Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) for conducting the selection process where QoS parameters of various component of IoT act as criteria. the effectiveness of the proposed approach along with the sensitivity analysis for showing the robustness of the proposed framework [20]
- **In 2018, Kowshalya et al.;** offered a fuzzy AHP hybrid model for community detection in SIoT networks for the management of trust among social objects. They depicted how to direct trust infers computation of trust before and after collaboration through utilizing centrality as well as dependability as the main factor for hierarchy. Through this work, they have tried to make communication among social objects reliable and secure. The results confirm

that the given model is highly reliable for establishing integrity among smart social objects to great extent[48].

- **In 2020, Talbi et al.;** described an interest-based model for the formation of social relationships among social IoT nodes autonomously regarding the virtual-based community. The presented model is sufficient in computing the trust of SIoT social nodes on the preference made by client users on an interest basis. Further, they have also depicted a new system based on recommendations signifying similarity associated with service requester and service provider to enhance the desired services [61]**.**

2.4 Relevant Findings

After careful study of the existing available approaches and techniques for the trust evaluation, various research papers of the following inferences are identified which are as follows:

- Existing trust evaluation and social relationship metrics have been reviewed exhaustively over the last ten years.
- Existing approaches to trust evaluation are based on the quality of service, recommendation, or reputation parameters. Most of the researchers used a single domain to measure trust. These trust evaluation models are based on internet devices known as IoT devices. None of the researchers have used multiple parameters to evaluate the trust.
- IoT devices are connected with society, then social internet of things-based devices are involved in society.
- Based on the literature review it is found that sharing information and avail the services from social devices is very risky. There is not any such framework; to evaluate the trust of internet-enabled social devices for multiple domains.
- There is a research gap between SIoT devices and the trust evaluation mechanism. Therefore the gap needs to be focused.

2.5 Conclusion

In conclusion, various approaches have been discussed in the literature to verify the trustee and untrusted nodes. Consequently, there exist substantial efforts to classify

them. In this chapter's classification of trust, models are described in an elaborated manner and adapted. This chapter consists of the latest applications of trust solutions for the SIoT through various types of references, publications, and articles.

After reviewing the various papers on IoT, SIoT, and trust evaluation methods of various models, we identify that the most effective and efficient trust computation models are applied and evaluated the trust values. Various trust computation techniques are used by the researchers. We further identify the research gaps in IoT and SIoT trust computation. Due to the relatively small amount directly related to work for trust evaluation. Therefore, we try to attempt to establish our work within the broader context related to the service provider, quality of data, and social relation of objects and present a critical review for the selection of trust evaluation models for our work.

Chapter 3

Proposed Framework

CHAPTER 3: PROPOSED FRAMEWORK

Whoever is careless with the truth in small matters cannot be trusted with important matters.

-- Albert Einstein--

3.1 Background

IoT is a new paradigm that depicts the interconnection of a large number of computing devices or electronic gadgets connected to the internet. Such devices can be categorized based on low and high computational capability associated with them. These IoT devices utilize meta information and unique identifiers to create their social objects in the IoT environment. Such social objects have enhanced capability to allow them to create their social network by utilizing specific social relationships like PLORand CLOR to provide desired services to client-user. They can initiate collaboration evolve, join different communities, and manage their relationship without the intervention of humans. Hence the enhancement taking place in the field of IoT systems produce new terminology called Social Internet of Things (SIoT) [62]. Therefore SIoT is an extension of IoT which is capable of establishing social relationships among several social objects concerning humans. Like humans these social objects as becoming part of social IoT networks that show suspicious behavior (malicious or cooperative)while collaborating with another social objects in SIoT networks. Users connected with these suspicious social networks are always worried and under threat while sharing their data and violation of their privacy [63].

Several applications have been introduced which utilize the concept of SIoT in various domains like education, medical field, telecommunication, transportation etc. Because SIoT devices are interconnected over the internet, the quality of service and quality of access by the user is most under threat in such SIoT networks. The services and data produced by SIoT device can be tampered with or intercepted during direct and indirect interactions between trustor and trustee. Hence the authenticity of the trustor and trustee is at great risk in terms of effective quality-based service and transmission of appropriate data. One effective solution to such issues prevailed in the SIoT environment is the trust evaluation of trustor and trustee. The impact of direct and indirect trust provides a better and safe environment for interaction with social

nodes very article have been covering the aspect of trust evaluation found by the researcher during the literature survey [64].

Trust has multi meanings in multi-environment so it can't be analyzed on a single metric. It is an integration of various properties like confidentiality, ability faith, and belief. Trust counts the degrees of closeness among its characteristic to make the environment healthy for reliable communication between trustor and trustee. In this chapter, the researcher has proposed the framework to overcome the problem of identifying the malicious nodes present in SIoT networks by following the same path a description of various trust-related mechanisms has been discussed in section 3.2 of this chapter and performed the categorization of trust in terms of the direct and indirect trust for quality based services accessed by client user[65]. Further the researcher has depicted the picture of the proposed framework for trust evaluation in SIoT environment by identifying various effective trust attributes through a literature survey and classifying them in a hierarchical structure. In section 3.8 of this chapter, we have depicted the mechanism associated with trust evaluation among social nodes in 2 scenarios i.e SR to SP and SP to SR by utilizing fuzzy AHP exten analysis and degree of possibility. At last, we have discussed the significance of the framework in terms of the identification of malicious nodes in SIoT networks.

3.2 Trust Evaluation Mechanisms

Over the last two decades, people have more attention to it. IoT device users regularly change the devices, therefore the trust value changes concerning the environment, scenario, and circumstances of users of the devices. [66] review such characteristics as well as offer an adaptability-based framework for aggregating trust in SIoT model. In 2017 [67], described the two approaches for computing the trust-based integrity of social nodes by using peer-to-peer scenarios in a social environment. Each social object evaluates the integrity of its neighbor nodes by utilizing the interaction and suggestions received. In this model, a particular social object utilizes its direct exposure to concerned nearby objects, to maintain the secrecy of the nodes. [43] offering a trust-based IoT mechanism for determining the trust value of a physical object through semantic-based analysis for social networks by utilizing authorization-based cross-layer protocol. Chen et. al. [68] described a set of procedures to determine the trust and reputation of IoT objects. The parameters used for the model

are similarity measures, social contract, and community of interest. Privacy was not part of the design of the model.

Moin et. al. [69], proposed a block-chain-based scheme utilized to protect and maintain the secrecy of various nodes. Here the author compared the existing blockchain applications dependency as well as essential issues associated with IoT devices. However, trust is a concern with users' previous knowledge, with the additional characteristics of the SIOT being personalization. Generally, two peoples have different opinions about a particular person. Therefore, trust may be asymmetric in that case. It means two people are attached in a relationship with a distinguished level of trustworthiness.

In [70] proposed IoT-based services model utilizing the concept of trust update. Here the proposed strategy shows dependency on collaboration and getting feedback from friends by applying social contacts, the similarity between node‟s centrality and honesty whereas the community is used like riddle parameter. In [71] advised a central model for management of trust by utilizing IoT to deliver trustworthy information among nearby smart devices. All the information related to trust value is kept for observation and stored in secondary storage through supernodes.

In [72], proposed a model based on trust evaluation to provide IoT service to the client by using machine learning techniques. The same model uses two techniques (i) to identify the number of clusters through k-means clustering (ii) to identify the boundaries of trusted and untrusted nodes by utilizing a support vector machine.

In [73], proposed a model to utilize various parameters to measure the level of trust associated with the device using the MCDM approach. The factor considered for computing trust values is security level, device security and ownership trust. The fuzzy-based approach is utilized to compute the impact of trust through ranking value. Similarly, a study conducted by [74], offered a mechanism to evaluate trust management in SIoT environment. The mechanism was based on 3 phases : (i) Several parameters are considered according to types of attacks in the trust evaluation phase The trustee node was selected based on the trust parameter. (ii)the trust value is determined by ANN in the trust aggregation phase. (iii)the time-driven based mechanism is used in the trust update phase. In [44], described a model shows dependency on the recommendation of dynamical management of trust in a network

of wireless sensing wireless sensor networks (WSNs). The value of trust depicts that node is evaluated in two manners: (i) The trust value in the case of direct trust is calculated by estimating its performance to interact with local data. (ii) The trust value of the device is updated timely to increase its reliability.

The study [75], gathered information about the distribution of power within IoT devices to provide solutions regarding communication. Initially, the mechanism estimates reputation based on exponential distribution through trust evaluation. Ambiguity may be possible in the case of direct trust assessed, and the indirect trust value was updated during the inaccuracies that arise from the direct trust. The results show accuracy improvements in both cases

3.3 Premises

A framework is a systematic representation of critical problems and processes. It provides a step-by-step process to perform a particular task. The proposed framework shows the actual documentation of the model and can be modified or updated from time to time as per the model requirement. It is a common approach to evaluating the trust of the nodes. To ensure the trustworthiness of the node, the framework has the following assumptions:

- The proposed framework improves the trust environment of the model.
- The trust score of the node may be changed by improving the quality of services and quality of data by using the sub-criteria during the process of framework implementation.
- Trust score may calculate with two techniques: direct or indirect trust.

By using the TMS framework is used to improve the quality of service, quality of data, and social relationships by evaluating the trust score of the end users/nodes.

3.4 Categorization of Trust

To understand trust, it is required to investigate and determine important facts regarding trust. To understand the information and its domain, it is required to categorize the trust which is as follows:

3.4.1 Direct Trust*:* The direct contact of two social nodes within SIoT networks is responsible for direct trust concerning one another. The direct trust value is more trustworthy when compared with indirect trust. Hence services accessed by the client on basis of direct trust are the most fruitful services

3.4.2 Indirect Trust*:* Indirect trust is also known as transitive trust because of the involvement of an intermediate node to determine the trust value of the respective node. There are more chances that a particular node is malicious in comparison to direct trust.

3.5 Proposed Framework

The classification of trust metrics is done based on how one parameter is dependent on the other. For example Quality of service highly shows dependency on latency, transaction time, scalability, and reliability. The rate of low latency time while completing the request of the client with minimum propagation delays like transmission and processing improves QoS. Hence trustworthiness of latency is responsible to deliver trustworthy services within social networks.

A framework is a schematic representation of a complex process. It provides a step-to-step guide to performing a task for research. This framework is a living document and can be updated and modified from time to time as per requirements. This framework is a common approach to computing the trust of the social object in SIoT. The framework has the following assumptions:

- The framework improves the life of social networks by considering individual nodes‟ trust as an effective measure to identify the malicious node.

- The list of trust metrics attributes is modifiable during the process of framework implementation. One can choose other factors which show strong dependency on certain parameters as per user requirements and can also add more security durability attributes.

- The levels of trust metrics hierarchy are not final. Due to the changes in the number of

  attributes it is changeable.

Use of this trust evaluation framework Framework is the next step to determining the trust of a social object for enhancing the strength of social networks in terms of identifying malicious nodes, better QoS, and better network navigability. The proposed framework for trust evaluation comprises five phases as shown in figure 3.1 which are as follows:

- Identification Phase
- Categorization Phase
- Computation Phase
- Validation Phase
- Wrapping Phase

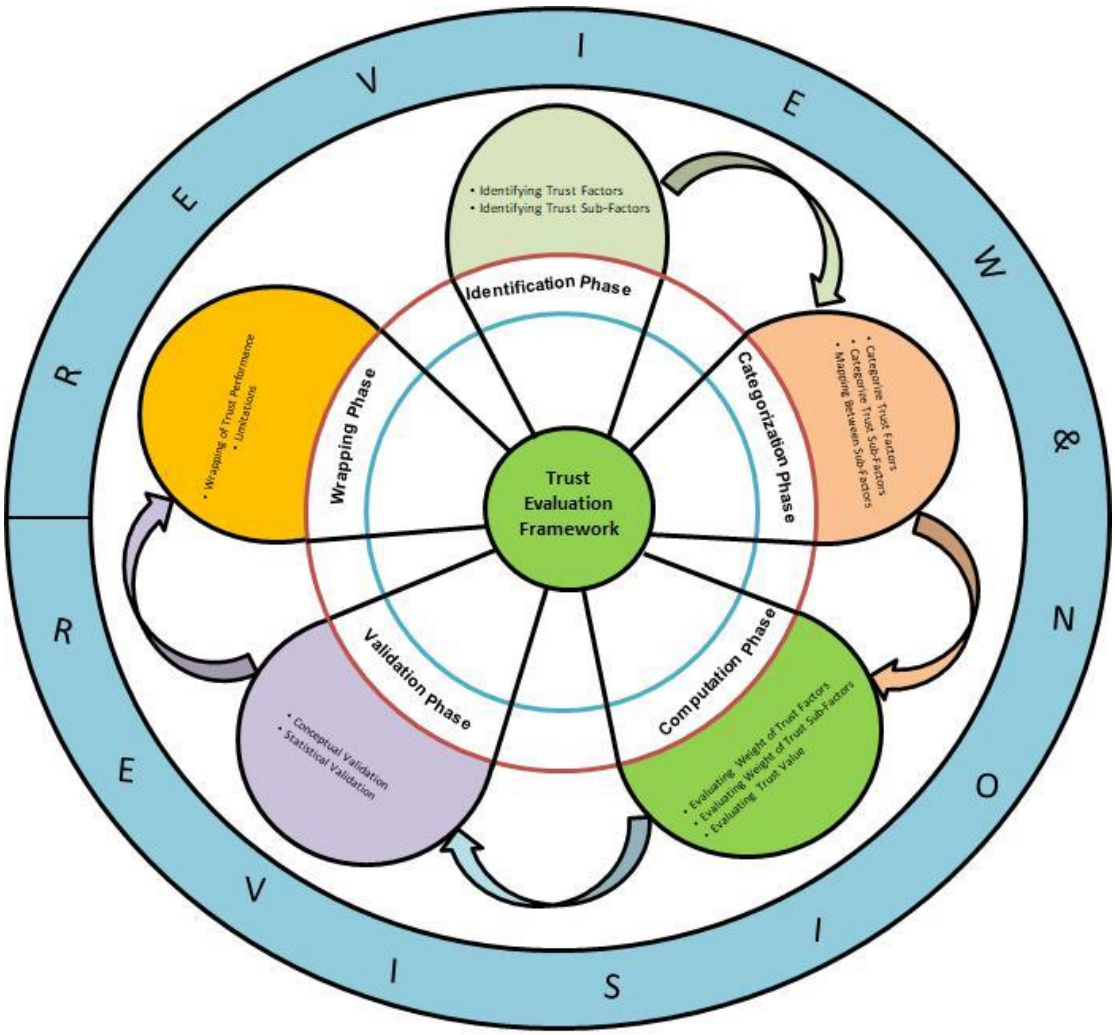

Figure 3. 1: Trust Evaluation Framework

In the first phase i.e., the relevant trust-based set of rules, relevant trust factors, and its different sub-categories are identified. In the next phase, i.e. the classification phase, for each identified trust factor, it is mapped whether the construct adheres to the identified set of rules to compute trust values. In the computation phase, prioritization of trust attributes is done to measure trust among social objects utilizing trust value in the case of the direct and indirect scenarios through that construct. The fourth phase involves the validation of the results or assessments that are developed. The fifth phase i.e.; the packaging phase evaluates performances based on validation. After this, Review and revision are common in all phases. In this phase, the whole approach is revisited for possible improvement and goes back to its last phase from the current one.

3.6 Identification of Trust Factors and Sub Factors

The proposed framework for trust evaluation is strongly designed by covering all necessary aspects of the social internet of things. As we come to know from the literature review the importance of various trust metrics' dependency on one another, we reviewed the most crucial factors which affect the trust among social objects within social networks. Frequently changing behaviors of the social object may deliver low-quality services, malicious data, and more transaction time are important risks that occur in SIoT networks. Therefore trust among such social objects is a key point to having quality based and secure data transmission.

Trust metrics or parameters associated with SIoT networks is a knowledgeable criterion in the fuzzy expert system to locate the truthfulness of social object. From the above review literature, it is found that trust can be evaluated on various metrics. In our work, the various trust metrics are taken under consideration including quality of data (QoD), transaction time, latency, reliability, scalability, quality of service (QoS), intrinsic, accessibility, recommendation, contextual representational, reputation from the reviewed articles as shown in figure 1.

3.6.1 Quality of Services (M1)

The QoS metric is utilized to determine the performance of a social IoT node successfully responding to an end-user request by following certain criteria of service

level agreement. The QoS metrics include sub-metrics are latency, transaction time scalability, and reliability.

a) ***Transaction Time (SM1):*** Transaction time signifies the minimal period associated with the SIoT server to complete a service request between the two SIoT nodes within a specified time frame. If the particular transaction doesn‟t completed in the given period, it has to be started again to achieve concurrency[76].

b) ***Latency (SM2):*** It is the time taken by the SIoT server to complete the client‟s request which experiences various propagation delays like transmission and processing while providing the desired service to end-users through utilizing the capability of social virtual object[22].

c) ***Scalability (SM3):*** Scalability signifies the capability of handling workload within the SIoT system. According to our scenario scalability in terms of trust metric depicts network throughput surpassing as the number of clients increases gradually. The bulkiness of the SIoT network is observed in terms of service requests receives by the server and the number of data streams produced. Hence, the scalability is responsible for a scalable system for reinforcement of QoS to produce maximum throughput under heavy workload in a SIoT-based environment[20].

d) ***Reliability (SM4):*** It is responsible for measuring the manner, in which services complete successfully without failure within a particular timeframe and under certain conditions. It can be analyzed in SIoT systems, that the number of client request decline by SP at peak time following certain conditions. Hence, reliability is the possibility that an SP provides desired services to its client under a specific set of rules without failure for a particular period[27][78].

3.6.2 Quality of Data (M2)

It determines the level of accuracy, and completeness offered by a smart social object while providing a service to a client or during collaboration with other nodes. It is the level of intrinsic, contextual, accessibility, and representational format of data provided by the smart social object.

a) ***Intrinsic (SM5):*** The intrinsic data deals with the functionality of data quality which includes accuracy, objectivity, believability, and reputation dimensions during transmitting information among nodes (SP to SR and SR to SP) to perform an integral transaction in SIoT-based services. The accuracy and objectivity alone are not sufficient to be a reliable quality of data; it must have ensured effective dimension (source of data) and believability.

b) ***Accessibility (SM6):*** Accessibility of data quality depends on what extent of availability and obtainability of data by the client while accessing desired services from the SIOT server. Hence the role of the SIoT system is to make the platform secure and accessible.

c) ***Contextual (SM7):*** The contextual data signifies the specific context of the task considering timeliness and completeness up to which extent data are applicable in delivering services in SIOT using different social relationships among different smart devices. The client accessing services focused on contextual data quality (value-added, relevancy, and amount of data) rather than representation.

d) ***Representational (SM8):*** The representational data quality during sharing of information between client and service provider maintains the format of data that must be concise and consistent to interpret data appropriately and easy to understand.

3.6.3 Social Relationship (M3)

The social relationship responsible for social trust between owners and SIoT devices is measured by honesty, centrality, cooperativeness, the community of interest, and connectivity. The social relationship like POR and CLOR represent the nature of bonding among social objects due to continuous interaction between the client (trustor) and SP (trustee). Hence it allows the trustor to monitor the inappropriate (dishonest) nature of the trustee for a particular time frame during successful interaction in the SIoT network.

a) ***Honesty (SM9):*** The social relationship property named honesty signifies whether a particular social object is honest or not. In SIoT, a malicious node can act dishonestly during providing services as well as recommendations.

The selection of honesty as a trust sub-metric because of the dishonest social object may interrupt trust management and continuity of desired services of SIoT-based application. In SIoT based application scenario a social object relies on direct interaction and indirect evidence (using past reputation and recommendation) to determine honesty as a trust metric of the connected node through social relationship[79].

b) ***Cooperativeness (SM10):*** The cooperativeness trust metric characteristic depicts the extent of social objects' socially interactive behavior towards the trustor. The social object may have the possibility to follow some set of rules while interacting with a trusted social object or friends with whom having strong social tie-up, but simultaneously become uncooperative while interacting with another social object. In SIoT application, a social object can compute the cooperativeness characteristic of the different social nodes by utilizing social tie-up and performing a selection of the socially active cooperative social objects to achieve high performance of application[16].

c) ***Community of Interest (CoI) (SM11)****:* The CoI trust metric signifies the property of the SIoT network whether the trusted social object belongs to a socially similar group/community (same community, co-location, and co-work) or not. The two social objects having a greater level of trust-based CoI can produce various interactions and positive experiences among other nodes which can result in better performance of application[21].

3.6.4 ***Centrality (SM12):*** The centrality of a social object, trust sub-metric of social relationship among other social objects represents its geographical position in the SIoT network. It signifies the importance of a particular social object „i" concerning social object j but declining other social nodes within the SIoT network. Hence the prime objective of centrality is to stop spiteful social objects to form more relationships [5].

3.6.5 Past Reputation (M4)

The client"s (trustor) previous trust value signifies the trust of SP"s (trustee) depends on earlier communication for a specific time frame between the client and SP. There is a significant impact of past interaction between trustee and trustor to compute the

trustee‟s trustworthiness. If the trustor had direct interaction in the past results in a positive impact otherwise it may produce a negative impact using the present trust score [68][69].

3.6.6 Recommendation (M5)

Trust score from the trustworthy social object can be utilized to compute the trust of the SP specifically when the client doesn‟t have any past interaction with the trustee. Recommendations from the nearby social object are utilized for evaluation when a particular trustor cannot able to locate a trust score through direct observation. Further, the recommendation must be honest and strong enough to prevent trust-related attacks [71].

3.7 Categorization of Trust Factors and Sub-Factors

The classification of trust metrics is done based on how one parameter depends on the others. For example Quality of service highly shows dependency on latency, transaction time, scalability, and reliability. The rate of low latency time while completing the request of the client with minimum propagation delays like transmission and processing improves QoS. Hence trustworthiness of latency is responsible to deliver trustworthy services within social networks.

Figure 3.2 shows the hierarchy-based classification of trust factors and their sub-factors which categorize into two levels. The main category and sub-category depict different factors association, the trust factors and trust sub-factors are shown in terms of direct and indirect trust. For example, latency and transaction time has different impact values on QoS as well but their effects are not the same. Moreover the classification of trust factors helps to identify weight vectors to determine the contribution of each parameter. QoS, QoD, and social relations affect the direct trust value of social nodes while past reputation and recommendation affect the trustworthiness of nodes indirectly. For the computation of trust, metrics at level 1 are denoted as M1, M2, M3, M4, M5, and at level 2 are denoted as SM1, SM2, SM3, SM4, SM5, SM6, SM7, SM8, SM9, SM10, SM11, SM12.

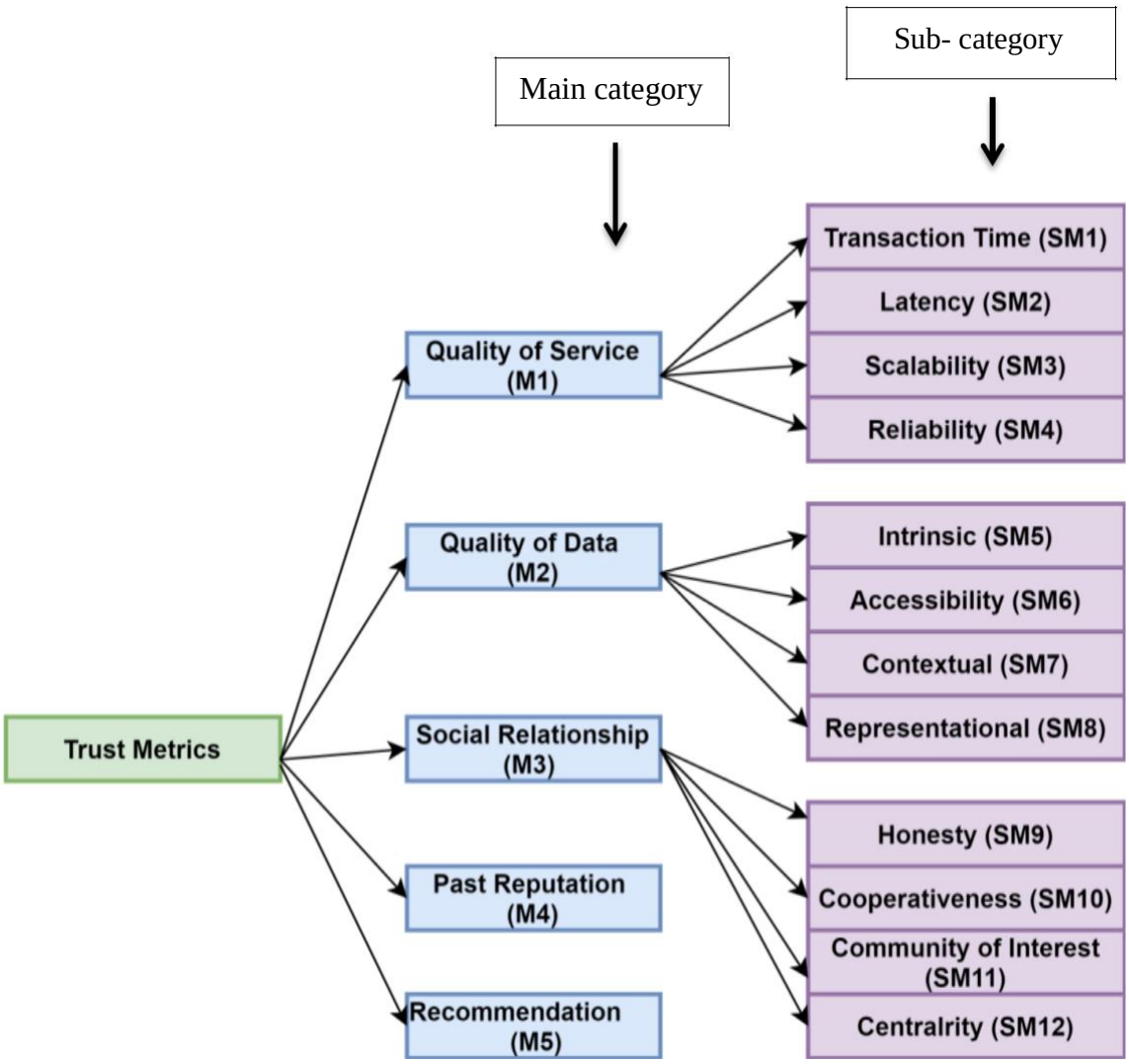

Figure 3. 2: Categorization of Trust Factors and Sub-Factors

3.8 Trust Evaluation Mechanism using Fuzzy AHP

Trust is the most promising characteristic among social objects which is related to service providers and service requesters. Trust computations play a key role to improve the quality of services, quality data sharing, malicious node-free social networks and minimizing attacks etc. Therefore, trustworthy nodes provide desired services to their client through social objects efficiently in a specific time frame with certain rules set by the owner of the device. Here, the computation of trust comprises two steps including mechanism selection and description & implementation.

3.8.1 Mechanism and its Interpretation

After evaluating the problem of trust computation, it is found that this is a decision-making problem which is having multiple criteria in the form of trust metrics

associated with social objects. Thus, in technical terms, trust computation relates to multiple criteria decision-making problems. There are multiple methods and techniques to solve the problem of decision-making. After a literature review of previous work, researchers have found that there are so many techniques to solve this type of problem. Further, Multi-Criteria Decision Analysis (MCDA) strategy is responsible for supporting the respondent to provide a path in case of conflict occurred. The approach defined above differs in their decision, objective or subjective. This work is using the Fuzzy AHP for trust e computation for two scenarios i.e SR to SP and SP to SR. Further, the results help to identify malicious nodes present in the social network of SIoT.

3.8.2 Implementation

In early 1970, Thomas L. Saaty introduced a multi-standard for performing reasonable decisions using the keyword analytical hierarchy process(AHP). It was introduced for structuring, measurement, and synthesis to perform the pairwise comparison using a comparative significance fuzzy scale depicting the preference of decision-makers to select criteria and cost-effective parameters for a given problem. Although AHP seems to be better while analyzing decision groups but various academicians accept that a hybrid form of AHP produces better results by utilizing fuzzy set theory with AHP strategy to compute trust value. The inclusion of methodology is shown in Figure 3.3, in the form of a flowchart. It depicts the design process for evaluating trust in SIoT environment. The computation of trust using a flowchart is breakdown into 5 steps which includes planning and preparation, fuzzification, fuzzy operation, analysis, confirmation, and estimation. The problem analysis, selection of trust factors, and sub-factors that determine the scope of AHP are the major concern related to the planning and preparation phase. The application of fuzzy AHP has been carried out to compute the weight vector in the most prioritized form by utilizing fuzzy extent analysis and degree of possibility..Such weight metrics are utilized to compute the trust for 2 scenarios i.e SR to SP and S to SR.

a) Planning and Preparation Phase

The problem of computing trust is recognized and depicted in previous chapters and closely related factors that affect trust are identified and categorized in the

previous section of this chapter. The AHP act as a mathematical tool for decision-making to prioritize and produce weight vectors by using a hierarchical structure of multi attributes. According to our work, AHP is the most suited technique to compute the trust of the social object in SIoT-based networks. That is why we have used fuzzy in our work to produce more refined results.

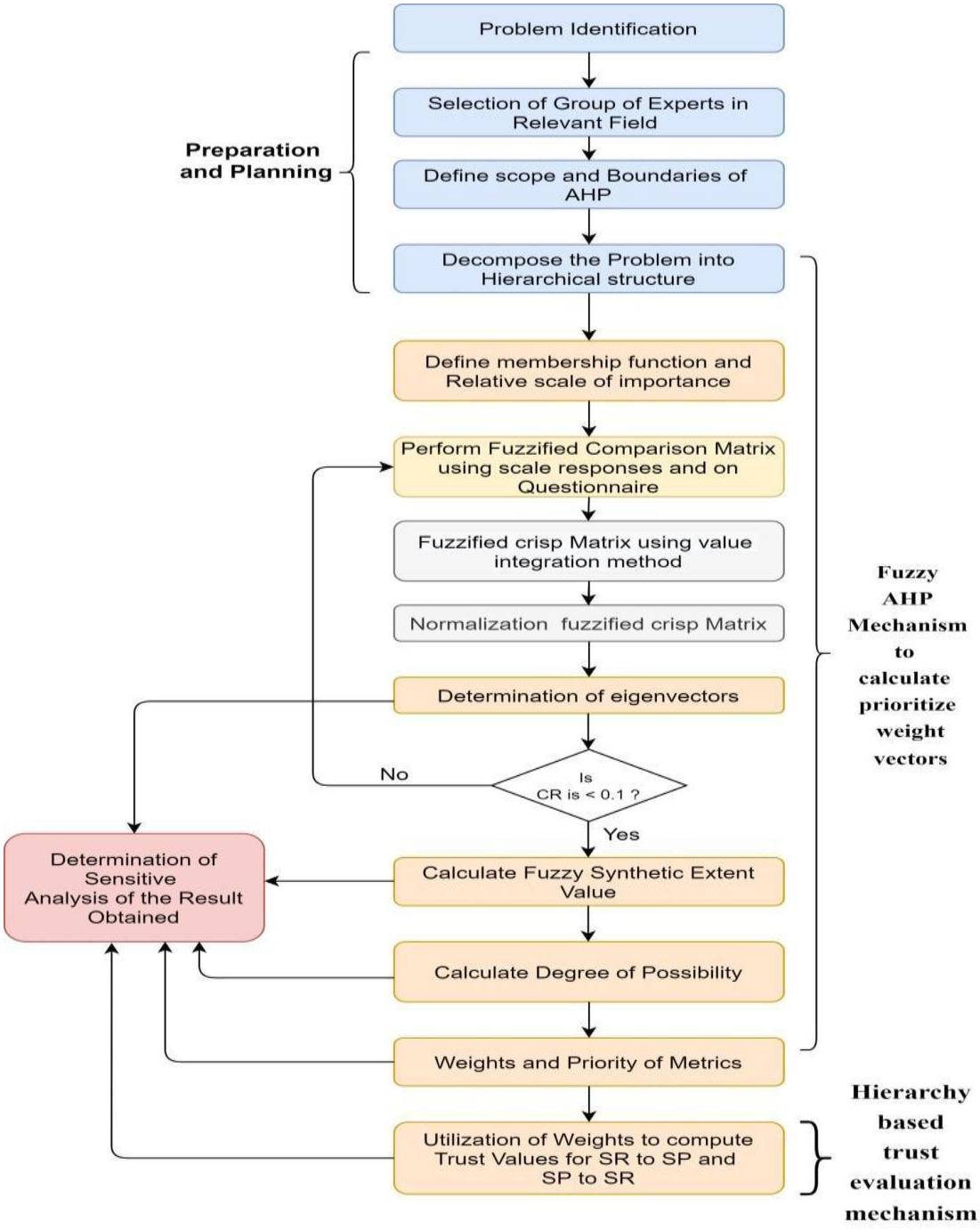

Figure 3. 3: Flow chart for implementation of Fuzzy AHP Method

b) Fuzzy AHP Mechanism to calculate the prioritized Weight Vectors

AHP (Saaty)is observed as the finest MCDM technique to provide levels (hierarchy) to criteria or factors suitable for decision-based problems while considering appropriate constraints by minimizing complexity. Further balancing the metric associated with it, AHP performs Pairwise comparison matric for a certain number of criteria and parameters which is beneficial for verdict-makers. AHP is distinct from ANP, which considers the interrelationships and feedback from the networks between alternatives and criteria [81].

From previous research, it is found that the F-AHP mechanism has been utilized in various studies and resultant depicts its usage in various applications and adequate for various situations. From various journals, it is found that the best result for criteria plays an important role [31]. By utilizing Fuzzy -AHP mechanisms verdict-makers are much capable to take realistic decisions efficiently through investigating the prominent parameters. That is why the authors tried to appertain the Fuzzy-AHP to compute the trustee nodes in a social network. After performing the planning phase, the basic procedure for hybrid fuzzy AHP starts to perform fuzzification, defuzzification, construction of normalized matrix consistency, fuzzy extent analysis, and degree of possibility are utilized to compute the weight vectors. Before discussing all such terms let's understand what fuzzy set theory is. The possible definition related to the fuzzy set theory that has been discussed here understand the concept of fuzzy AHP [82].

In a fuzzy system, the triangular fuzzy number (TFN) is depicted by 3 keywords lower (l), middle (m), and upper (u) as signified in Figure. 2. The membership function μN( ) is defined in equation (2).

$$\mu_N(\quad) \begin{cases} \quad \\ \quad \end{cases} \qquad (2)$$

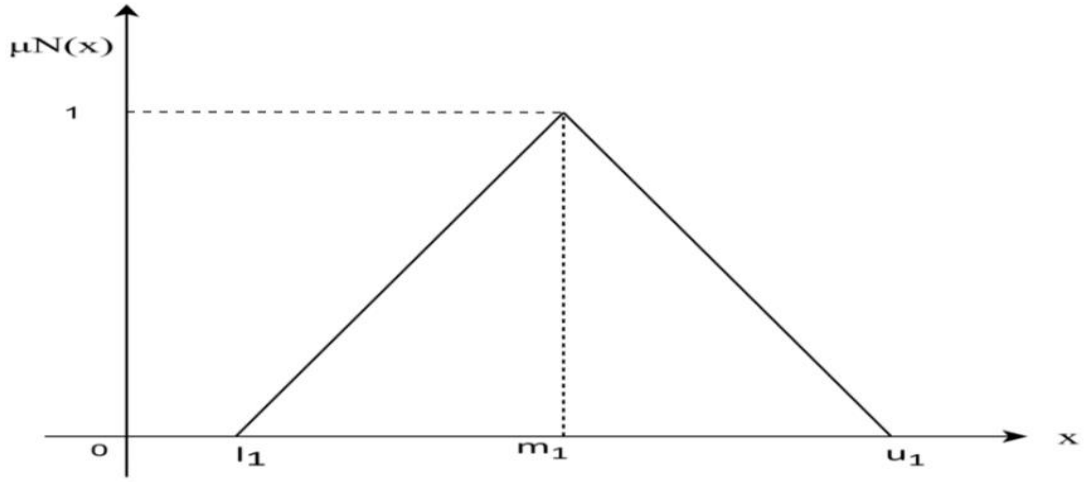

Figure 3. 4: Triangular Fuzzy numbers

Statement 1:

Consider Ŷ and Ž are the 2 TFNs Ŷ = (Yl, Ym, Yu) and Ž = (Zl, Zm, Zu). The vertex approach is utilized to compute the distance between Ŷ and Ž as given by Eq. (3). Table 3.1

$$D(\hat{Y},\check{Z}) = \sqrt{\frac{1}{3}\left[(\quad)(\quad)+(\quad)(\quad)+(\quad)(\quad)\right]} \qquad ()$$

Table3. 1: Fuzzy Operations

OPERATION	ALGEBRAIC EXPRESSION
$Y \oplus Z$	$(Y_l + Z_l , Y_m + Z_m , Y_u + Z_u)$
$Y \ominus Z$	$(Y_l - Z_l, Y_m - Z_m, Y_u - Z_u)$
$\hat{Y} \otimes Z$	$(Y_l \times Z_l , Y_m \times Z_m , Y_u \times Z_u)$
$Y \oslash Z$	$(Y_l/Z_u, Y_m/Z_m, Y_u/Z_l)$
$\hat{Y}^{-1}$	$(1/Y_l ,1/ Y_m ,1/ Y_u)$
kY	(kY_l , kY_m , kY_u)

In this work, the researcher uses an extent analysis mechanism to produce an accurate and consistent result. The procedure followed regarding the fuzzy AHP strategy in eight phases is given below:

Table3. 2: Satty Scaling

Linguistic Value	TFN	TFN Reciprocal	Trust Value
Not Trusty	(1,1,1)	(1,1,1)	0.0
Very Less Trusty	(0.5,1,1.5)	(0.6,1,2)	0.2
Less Trusty	(1,1.5,2)	(0.5,0.6,1)	0.4
Strongly Trusty	(1.5,2,2.5)	(0.4,0.5,0.6)	0.6
Very Strongly Trusty	(2,2.5,3)	(0.3,0.4,0.5)	0.8
Absolute Trusty	(2.5,3,3.5)	(0.2,0.3,0.4)	1.0

Phase 1: The computation of data value deals with the issue identified based on the trust metric in the SIoT network shown in fig 1. The fuzzy scale of comparative significance between every element put together in the same pecking order defined in **Table 3.1** signifies linguistic variables (Not Trusty, Very Less Trusty, Less Trusty, Strongly Trusty, Very Strongly Trusty, and Absolute Trusty)

Phase 2: Based on expert opinion, an FPCM is constructed by transforming linguistic variables into a fuzzy number using TFN[83]. We used a trust-based fuzzy scale to convert lingual elements into a set depicting fuzzy values shown in table 1. An example of FPCM can be depicted as.

$$T_{ij} = [\quad\quad] \tag{4}$$

where $b_{ij}=1$, for i=j and $T_{ij}= (tij^{l}, tij^{m}, tij^{u})$

Phase 3: In this phase, we construct a single decision matrix (SDM) using an FPCM based on expert opinion about the trust metric for a social object in SIoT by utilizing equation 5.

$$T_{ij} = (P_{ij}, Q_{ij}, R_{ij})$$

$$P_{ij} = \min \{Pij^{k}\} \quad (5)$$
$$Q_{ij} = -_{\Sigma}$$

$$R_{ij} = \max\{Rij^{k}\}$$

Where n represents the size of metrics and k signifies each member in SDM.

Phase 4: The combined pairwise matrix (CPM) acquired through phase 3 is supposed to check for consistency to acknowledge the expert opinion regarding the trust metric of the SIoT system is consistent or not. First, defuzzification of CPM is done in crisp format[84]. For example, suppose V= (a,b,c) is a TFN, its defuzzification into crisp format is depicted by the formula.

$$T_{crisp} = \quad \text{———} \quad (6)$$

Further, the pairwise matrix is supposed to check for consistency after defuzzification and the matrix must be normalized by performing a division of each element in a column by adding all the elements in a column.

$$T_{ij} = \Sigma \ \text{———} \quad \text{for all } (i,j \in t) \quad (7)$$

Where n represents the size of metrics

The eigen-vector (EV) signifies the weight value of every trust metric depicted by

$$W_i = \frac{\Sigma}{\text{———}} \quad (8)$$

Where Wi represents the EV in row i, and Σ is the addition of every term in the row of the normalized pairwise matrix(NPM)[85]. The highest value of EV λmax of the fuzzy crisp matrix is calculated by the multiplication of every term of the crisp matrix and EV. Therefore, λmax is given by

$\lambda_{max} = \Sigma * (\Sigma$) (9)

Where ∑ represents the addition of all column terms of the crisp non-normalized values, Wi depicts the EV and n is the size of metrics.

The consistency ratio (CR) and consistency index are computed through eq. 10 and 11 respectively.

CI = —— (10)

CR = — (11)

Table3. 3: Random Index

Matrix size	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

In Table 3.3 RI depicted matrix sizes up to 10 metrics. To compute the consistency of the PCM, CR must be less than 0.10 otherwise the procedure for the PCM has to be repeated. In other words, the expert's opinion about identified trust metric for social object selection is acceptable if CR<0.10 otherwise their judgment is incoherent.

Phase 5: In this phase, we have to compute the fuzzy synthetic extent value (FSE) using an FPCM through eq. 12. The FSE for the ith value is expressed by:

$S_i = \Sigma \otimes [\Sigma \Sigma]^{-1}$ (12)

Where Si signifies FSE and ∑ is calculated by using fuzzy addition operational law, is given by eq. 13

$\Sigma = (\Sigma \Sigma .\Sigma)$ for all (I ϵ [1, 2, 3…n]) (13)

The expression is ∑ ∑ evaluated by using fuzzy addition law on Σ

. Further, each column element perform addition to compute ∑ ∑ through eq. 14 That is,

Σ Σ = (Σ Σ ,Σ) for all (j ϵ [1, 2, 3…n]) (14)

The expression [Σ Σ]-1 is calculated by taking the transpose of the outcome (eq. 15). which is given by

[Σ Σ]$^{-1}$=(, ,) (15)

Finally, the expression Σ ⊗ [Σ Σ]-1 is computed by applying fuzzy multiplication operation law using eq. 13 and 15 and is given by Eq. 16

S_i = (Σ , Σ , Σ) (16)

For all (i,j ϵ [1,2,3…n])

Phase 6: The degree of possibility (DP) has to be calculated in this phase because there may a exist TFN value between the 2 fuzzy numbers[86]. Consider, there exist two triangular fuzzy numbers say H1 = (l1,m1, u1) and H2 = (l2,m2, u2), then their DP must be H1 ≥ H2 is given by

$$V(H1 \geq H2) = \sup [\min (\mu H1(y), \mu H2(z))] \quad (17)$$

The above expression can also be defined as given in eq. 17

$$V(H1 \geq H2) = hgt(H1 \cap H2) = \mu_{H1}(d)$$

N() { ( ) (18)

Where, ordinate d is the highest point of intersection between μH1, μH2, and DP as depicted in figure 3.4.

Phase 7: Further, evaluate the degree of possibility (DP) using eq. 19 and 20 for convex fuzzy number i.e, greater than r CFNs.

$$V(H \geq H_1, H_2. H_r) = \min V(H \geq H_k)_{\forall k \in [1, 2, \ldots r]} \quad (19)$$

$$d'(Gk) = \min V(H_k \geq H_j) \quad \forall j, k \in [1, 2, \ldots n], j \neq k \quad (20)$$

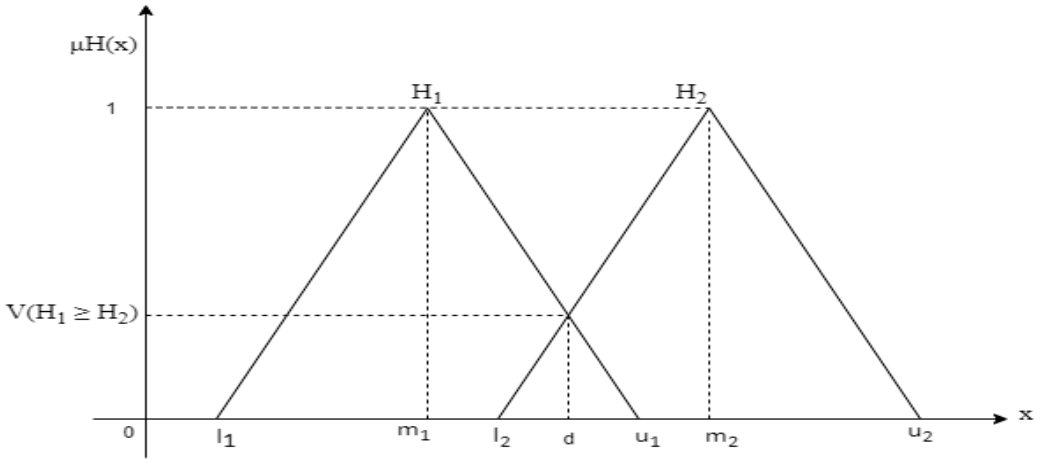

Figure 3. 5 : Degree of the possibility of the Two TFN

Phase 8: Compute the weight value and normalized it to again evaluate the non-fuzzy weight vector using eq. 19 and 20.

$$\acute{W} = (d'(G_1), d'(G_2) \ldots, d'(G_n))^T \quad (21)$$

Finally, we obtain the weight computed through eq. 21 and further normalized to evaluate the non-fuzzy weight vector depicted by:

$$W = (d(G_1), d(G_2), \ldots, d(Gn))^T \quad (22)$$

Where $d(G_k)$, $\forall\ k \in [1, 2, 3\ldots.., n]$ represent the weight of metric k.

c) Hierarchy-based trust evaluation mechanism

After finding the prioritize weight metric using fuzzy AHP by applying fuzzy extent analysis we follow a hierarchical based trust computation model to determine the level of trust in both the scenario i.e SR to SP and SP to SR[87]. The hierarchical model for scenario 1 and 2 consist of 3 levels, at level 1 we place the goal to determine the level of trust, at the second level we placed the affecting parameter of the main category which deals with direct and indirect trust and its sub-category at a level as shown in figure 4 and figure 3.5. The author considered main category factors to compute trust value in both scenarios.

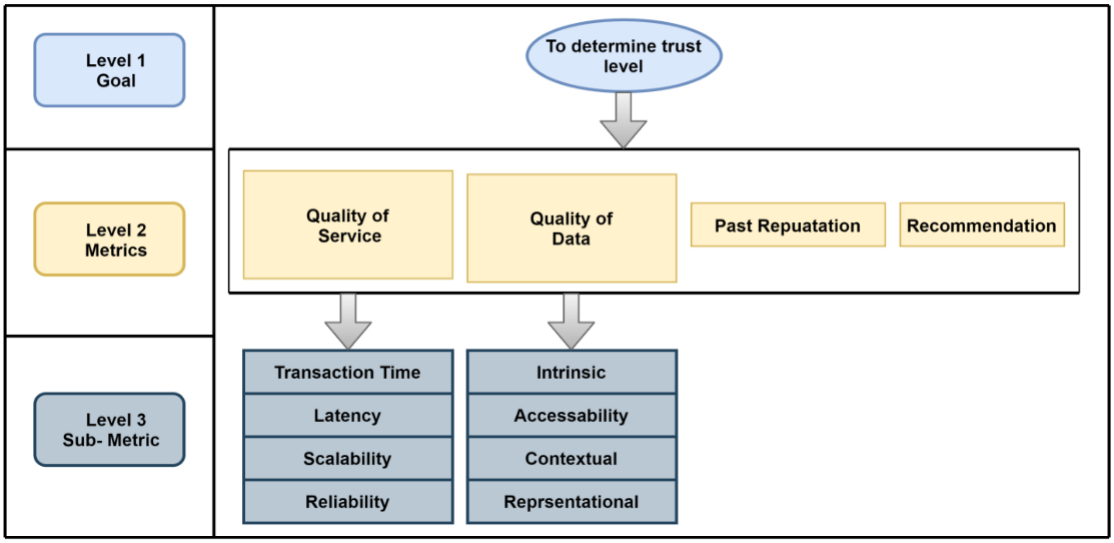

Figure 3. 6: Trust-based computation hierarchy model (SR to SP) using fuzzy-AHP

Evaluation of trust is computed through a social object‟s trust score by following criteria of profitability to assign a task, interact and collaborate with other social objects. The trust in the trustee acts as a function of the interaction data value (present and Past) obtained from the different social objects[88].

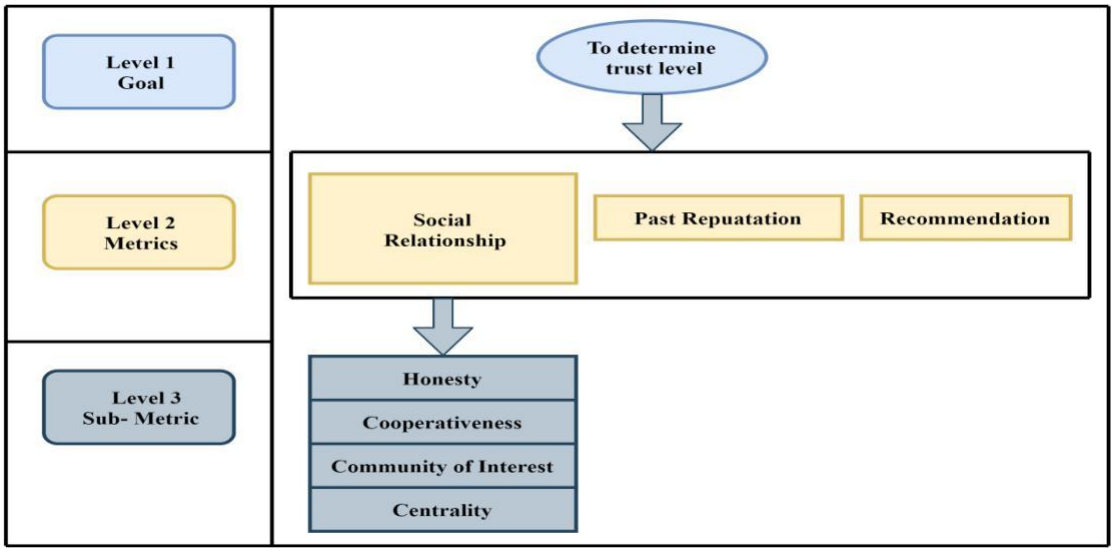

Figure 3. 7: Trust-based computation hierarchy model (SP to SR) using fuzzy-AHP

The computation of trust depends on trust metrics to assign a particular weightage to every parameter by the trustor. The social object's truthfulness is based on the direct trust value received from the direct communication of a client and previous reputation data value with the SP along with suggestions obtained from the social object.

Notably, TMS working efficiently follows two-way communication SR to SP and SP to SR in SIoT computing.

So, utilizing capabilities of trust management here we considered the two scenarios SR to SP and SP to SR where SP provides services to the end-user while SR requests social object collaboration with others of the same community or groups. Hence the trust management system (TMS) is split into 2 streams namely direct trust (DT) and indirect trust (IDT) as given below:

- **Direct Trust:** The direct trust evaluation of social object node SONi by end-user j depends on QoS and QoD in terms of SR to SP, it also computes the DT value of j utilizing social relationship (centrality, community of interest, and cooperativeness) among social object in SIoT network.

  Trust Value Tij in case of direct interaction is given by

  $$T_{ij}= \alpha D_{ij}+ (1-\alpha-\beta)\, X_{ij} + \lambda\, Y_{ij} \quad (23)$$

  where Dij = $\frac{\Sigma}{\Sigma}$ is direct trust of node i with respect node j during direct contact.

  Transactional factor (Tf) and Fbk both ϵ (0, 1)

  X_{ij} and Y_{ij} are the weights of Trust metrics.

  $0<(\alpha,\beta,\lambda,\gamma)<1$ \1, $0<Tij<1$

  α, β, λ, are trust adjusting value to maintain the trust value between 0 and 1.

- **Indirect Trust:** It computes the subjective trust value of the SP on basis of suggestions and prior knowledge received by the client. In other words, the Indirect trust data value is the integration of recommendations and earlier experience of social objects in SIoT networks.

  Trust Value Tij in case of direct interaction is given by

  $$T_{ij} = T_{ij}\,(t)\,(t-\Delta t) + \beta \text{Rec}\, kj + \alpha Dik \quad (24)$$

  where $0<(\alpha,\beta)<1$, $0<Tij<1$

α and β are the trust adjusting value to maintain the trust value between 0 and 1.

D_{ik} signifies direct trust of node k concerning node i.

Tij(t) (t - Δt) is past reputation value , Reckj depicts recommendation of of socil object k regarding socil object j.

3.9 Significance of the Framework

In the SIoT environment, the changing behaviors of the social object may produce a suspicious environment for the end user. In such cases Users connected with these suspicious social networks are worried while sharing the data and violating their privacy. Hence, the concept of trust in SIoT can be considered as a treatment for malicious or dishonest nodes. Through literature, we come across various problems associated with the evaluation of trust. Answering those problem show path to producing trust based frame for social IoT nodes. The above-discussed framework has the following significance

- It may help to find dishonest or untrusty nodes by computing the trust values of social objects
- It may help to provide quality-based service to the client with intrinsic data quality.
- It may help to assess the impact of various trust factors during the collaboration of social objects in SIoT environment
- It may help to find the impact of direct and indirect trust on particular social object

3.10 Conclusion

In this chapter, the researcher tries to full fill the needs, and importance required to perform trust evaluation for the identification of malicious nodes within the social node. The same researcher has proposed a framework for trust evaluation.to follow the requirement of the framework, we have found out from the literature major affecting trust factors of social networks like QoS, QoD, social relationships, etc. Further, the classification of trust factors has been done using a hierarchical structure. To achieve the goal we have to provide the full description of a flow chart for trust

evaluation where we have firstly depicted the planning and preparation phase and then the mechanism utilized by the researcher to calculate the weight vectors of different factors. After that, a simple mechanism for the evaluation of trust by utilizing a weight vector has been depicted based on the hierarchical structure of trust factors. At last, we presented the major significance of the framework.

Chapter 4
Implementation of Framework

CHAPTER 4: IMPLEMENTATION OF FRAMEWORK

The people when rightly and fully trusted will return the trust.

--Abraham Lincoln--

4.1 Background

In the last two decades, the Internet of Things (IoT) emerges as a revolution in the field of computer science and a progressive face of challenge for academic researchers. The transformation of IoT to the Social Internet of Things (SIoT) currently gaining much popularity as well as attracting the research community because of the spacious and flexible nature associated with it. In the SIoT environment, the smart objects are capable of locating appropriate services for client users by using social networks, such a network consists of a social node that may show malicious or falsie nature to provide bad services[89]. Therefore evaluation of trust for the same social nodes provides a path to better network navigability and detection of malicious nodes. A trust may be expressed as a function of reliable service through social networks.

Trusty and malicious nodes are dependent on various effective direct and indirect metrics. Direct metrics at level 1 consist of QoS, QoD, and social relationships while indirect metrics are past reputation and recommendation. The direct factors at level 2 include latency, transaction time, scalability, reliability, Intrinsic, accessibility contextual, representation, honesty, cooperativeness, a community of interest, and centrality. No indirect metric exists at level 2. The QoS and QoD is directly responsible for quality-based services in SIoT network, so they are categorized as direct metrics while reputation and recommendation need metrics are measured in terms of other nodes as an intermediary so they are depicted as indirect metrics. Hence trust value at an early stage through reputation and recommendation may improve the performance of social networks but it‟s very hard to implement [90]. Therefore evaluation of trust is necessary for the detection of malicious social nodes. The computation mechanism involves not only quantifying trust factors but also identifying the most crucial metrics among them. In a nutshell, identification, categorization Ranking, and evaluation of trust metrics is a critical task.

Unfortunately, we find none of the authors in the literature performs trust evaluation for such factors. Hence in this chapter, we attempt to perform ranking and computation of trust based on direct and indirect metrics using real-time examples of local ad-hoc networks.

The mechanism process for trust computation for the detection of malicious nodes is already discussed in chapter 3. According to the mechanism firstly, the author calculates the local and global weights of each metric and sub-metrics and performs a ranking of the final weights. To compute the trust value, we use two scenarios of the fuzzy-based hierarchy model as discussed in chapter 3, to determine direct and indirect trust. Based on direct and indirect trust, evaluated through fuzzy methods the overall trustworthiness of the social node (malicious or not) is estimated. The step-by-step process of trust computation is depicted in the next portion of the chapter.

4.2 Framework Implementation

In this chapter the researcher, presented the mathematical solution for the given problem to find the malicious nodes in a social network of SIoT.For the implementation, we have taken a social ad-hoc network of 10 to compute the trust values and tried to identify the no of malicious or dishonest nodes on the basis fuzzy trust value taken in chapter 3.

4.2.1 Identification Phase

Trust metrics or parameters associated with SIoT networks are a knowledgeable criterion in the fuzzy expert system to locate the truthfulness of social objects. From the above review literature, it is found that trust can be evaluated on various metrics. In our article, the various trust metrics are taken under consideration including quality of data (QoD), transaction time, latency, reliability, scalability, quality of service (QoS), intrinsic, accessibility, recommendation, contextual representational, reputation from the reviewed articles as shown in the previous chapter. To compute the value of trust for a social object, we adhere to the flow chart depicted in the previous chapter and follow the procedure step by step.

4.2.2 Computation Phase

The computation phase deals with the fuzzy AHP mechanism used as a tool to compute weight vectors of trust factors by following the given procedure in the previous chapter using fuzzy synthetic extent analysis and degree of possibility. These weights are further utilized for the computation of trust using the hierarchical-based model for 2 scenarios i.e. SR to SP and SP to SR.

4.3 Estimating Weights of Trust Factors using Fuzzy Method

The Analytical hierarchy process has been utilized to perform a ranking of factors in different environments. We have used a novel fuzzy-AHP strategy to compute ranking to perform to compute weights in the SIoT network. To obtain the trust value of a social node in SIoT, firstly we have to perform a selection of trust base metrics and sub-metrics. For the same, various metrics were identified from literature in the SIoT environment. Further, the opinion of 15 experts belonging to academics and industry was used to collect data based on discovered factors. Hence, five metrics and twelve sub-metrics were selected as depicted in chapter3. Afterward, the hierarchy-based framework is constructed to compute the trust of a social object which includes our goal, metrics, and sub metrics as shown in fig 5 and 6. In our constructed framework, there are three levels where first-level signifies our main goal while the metric and sub-metric are taken into level 2 and level 3 as depicted in chapter 3. The ultimate aim of the present study is to perform a ranking of metrics and sub-metrics to evaluate the trust value of trustees through direct trust and indirect trust in SIoT.

4.3.1 Formation of Pairwise Comparison Matrix

By using the technique fuzzy-AHP, we have surveyed fifteen experts, and the formation of pairwise comparisons of trust metrics is done. The sample size obtained from survey experts is quite small but the fuzzy AHP is very subjective.. Various other researchers have also taken such a small dataset and produces effective results. Therefore utilizing fifteen experts‟ suggestions to collect a dataset for fuzzy-AHP in our work is quite justifiable. Now, we have performed the formation of a pairwise comparison matrix through the data collected. The linguistic variables signify their corresponding triangular fuzzy number (TFN) is depicted in chapter 3 for the conversion to be done. Thereafter, we obtained an aggregate fuzzified comparison

matrix by combining fifteen matrixes through equation 5. Finally, the obtained FPCM for scenario 1 and scenario 2 is depicted in Tables 4 and 8. For example, how the value of Tij = (Pij, Qij, Rij) is calculated and sample data collected from the experts for the trust metric and sub metric for levels 2 and 3 is given below:

(1,1.5,2), (0.4,0.6,0.5), (1.5,2,2.5), (1,1.5,2), (1,1.5,2), (0.4,0.6,0.5), (1,1.5,2), (1,1.5,2), (0.4,0.6,0.5), (1,1.5,2), (1.5,2,2.5), (1,1.5,2), (1.5,2,2.5), (1,1.5,2), (1.5,2,2.5)

$P_{ij} = \min \{Pij^k\}$

$= \min\{1, 0.4, 1.5, 1, 1, 0.4, 1, 1, 0.4, 1, 1.5, 1,1, 1, 1.5\}$

$=0.4$

$Q_{ij} = -_{\Sigma}$

$= — (1.5+0.6 +2 +1.5 +1.5+0.6 +1.5+1.5\ 0.6+1.5+2+1.5+2+1.5+2)$

$= 1.45$

$R_{ij} = \max\{Rij^k\}$

$= \max\{2, 0.5, 2.5, 2, 2, 0.5, 2, 2, 0.5, 2, 2.5, 2, 2.5, 2, 2.5\}$

$= 2$

Hence, $T_{ij} = (0.4, 1.45, 2)$

Table 4. 1: Fuzzified Pairwise Comparison Matrix for Main category (Scenario 1)

	QoS	QoD	Reputation	Recommendation
QoS	1,1,1	0.4,1.45,2.5	1,1.89,2.5	1.5,2.16,3.5
QoD	0.4,0.97,2.5	1,1,1	1.5,2.29,3.5	1.5,2.42,3.5
Past Reputation	0.4,0.59,1.5	0.3,0.42,0.6	1,1,1	0.4,1.54,2.5
Recommendation	0.3,0.59,1.5	0.3,0.49,0.6	0.4,0.88,2.5	1,1,1

Table 4.1 depicts the fuzzified pairwise comparison matrix (FPCM) for main category factors like QoS, QoD, past reputation, and recommendation. Using equation (4), we have calculated the values of each cell. The example for the same has been discussed in the previous portion of this chapter. Hence all the values of each cell have been determine by following the procedure discussed above for FPCM for SR to SP.

Table 4. 2: Fuzzified Crisp Matrix for Scenario 1

	QoS	**QoD**	**Reputation**	**Recommendation**
QoS	1	1.45	1.85	2.27
QoD	1.13	1	2.36	2.44
Past Reputation	0.71	0.43	1	1.51
Recommendation	0.68	0.47	1.07	1

Table 4.2 Shows the defuzzification of TFN value into crisp value using the value integration method as depicted by equation (6) for the trust factors in chapter3. Hence the value of the crisp matrix depends on the lower, middle, and upper value of FPCM.

Table 4. 3: Normalized Fuzzified crisp Matrix for Scenario 1

	QoS	**QoD**	**Reputation**	**Recommendation**
QoS	0.284	0.432	0.295	0.375
QoD	0.321	0.296	0.376	0.377
Past Reputation	0.201	0.128	0.159	0.209
Recommendation	0.193	0.14	0.171	0.138

λ_{max} = 4.165, CI= 0.06, CR=0.06

Table 4.3 depicts the normalization of fuzzified crisp value by dividing each element in a column by the sum of all elements in the column by using equation 6 for all the trust factors of the scenario1. The value of λmax is calculated by multiplying each element of the fuzzy crisp matrix corresponding eigenvector by equation 8. The value of CR and CI is calculated by equations 9 and 10.

Table 4. 4: Eigen Vectors of trust metrics for Scenario 1

TRUST METRIC	EIGEN VECTOR
QoS	0.345
QoD	0.343
Past Reputation	0.174
Recommendation	0.161

Table 4.4: Shows the final value of the eigen-vector. It can be calculated by the sum of all elements in a row of the normalized pairwise matrix and divided by the number of trust factors. It represents the weight of trust factors

4.3.2 Validate the consistency of the pairwise comparison matrix

After the formation of PCM, the consistency ratio is computed. For example, we have evaluated the greatest EV for scenarios 1 and 2 of PCM. For the same, the TFN of a PCM is defuzzified corresponding to crisp format through equation 6 and the obtained FCM is depicted in Tables 4.2 and Table 4.3. The fuzzified crisp matrix is further normalized through eq. 7 and the outcomes obtained are shown in Tables 4.3 and --.

The eigen-vector (EVS) of the fuzzified crisp matrix is computed through eq. 8. The outcomes of the EVs for 2 scenarios are depicted in Tables 4.4 and --. We have computed the highest EV (λmax) of the fuzzified crisp matrix through eq. 9. Therefore scenario 1

λmax=
(1+1.13+0.171+0.68)*0.345+(1.45+1+0.43+0.47)*0.343+(1.85+2.36+1+1.07)*0.174
+ (2.27+2.44+1.51+1)*0.161= 4.165

Since we have considered 4 factors, so the corresponding value of the Random Index is 0.90as depicted in chapter 3. Hence CI is calculated using equation 10.

CI = ——— = 0.06

Therefore, the consistency ratio (CR) is computed as using equation 11.

CR = — = 0.05

Now, the CR value is 0.05 which is less than 0.10 so the Table 4.1 representing fuzzified pairwise comparison matrix is acceptable and consistent.

4.3.3 Performing prioritization of weights of trust metric

We have computed the local weight (LW) of the trust metric and sub-metric and shown the description of our evaluation based on Table 4.1 for scenario 1 of the main category. we have utilized the extent analysis strategy and the procedure for the same is given below:

Table 4. 5: ∑_(j=1)^n Tij Value for each metric

Trust Metrics	Σ
QoS	3.9,6.5,9.5
QoD	4.4,6.68,10.5
Past Reputation	2.1,3.55,5.6
Recommendation	2,2.94,5.6

Table 4.5 depicts the sum of all T_{ij} by performing fuzzy addition operations using equation 13.

Table 4. 6: Fuzzy synthetic extent (Si) value for trust metrics

Trust Metrics	S_i
QoS	0.125,0.382,0.779
QoD	0.141,0.341,0.861
Past Reputation	0.064,0.181,0.459
Recommendation	0.054,0.152,0,289

Table 4.6 show the Fuzzy synthetic extent value of trust metrics for comparison of fuzzy numbers, which is calculated by using equation 12. It depicts the "extent" to which a metric satisfies a goal by performing comparison of fuzzy values.

The Si of the PCM in Table 4 was calculated using eq. 12

Si = Σ ⊗ [Σ Σ]-1

Σ is computed using eq.13 and results depicted in Table 15 and the value of

Σ Σcalculated by eq.14 is given by

Σ Σ= (12.4, 19.67, 31.21)

Further the inverse value of Σ Σ computed using eq.15 which is given below

[Σ Σ]-1 = [(—— ,—— ,—)]

Therefore, the FSE value (Si) is computed as

[Si] = [ ] ⊗ [0.032, 0.051, 0.082]

The result obtained for each value of Si is depicted in Table 4.6.The degree of possibility (DP) for one TFN is highest than other is computed through eq 17 and 18. Further, the DP associated with convex fuzzy values (CFV) highest than the three is evaluated through equation. 19 and 20. as given by

$$d'(S1) = least \{WV(S1 \geq S2, S3, S4)\}$$

$$= least \{ WV(1, 1, 1)\} = 1$$

$$d'(S2) = least \{WV(S2 \geq S1, S3, S4)\}$$

$$= least \{WV(0.937, 1, 1)\} = 0.947$$

$$d'(S3) = least \{W V(S3 \geq S1, S2, S4)\}$$

$$= least \{WV(0.529, 0.537, 1)\} = 0.585$$

$$d'(S4) = least \{WV(S4 \geq S1, S1, S3)\}$$

$$= least \{WV(0.358, 0.322, 0.853)\} = 0.416$$

The weight vector is computed through utilizing eq. 21

$$W' = (1, 0.947, 0.585, 0.416)T$$

Now, we can compute the normalized weight vector W by taking the transpose of W′ utilizing eq. 21

W = (——— ——— ——— ———)T = 0.342 ,0.321,0.198,0.141

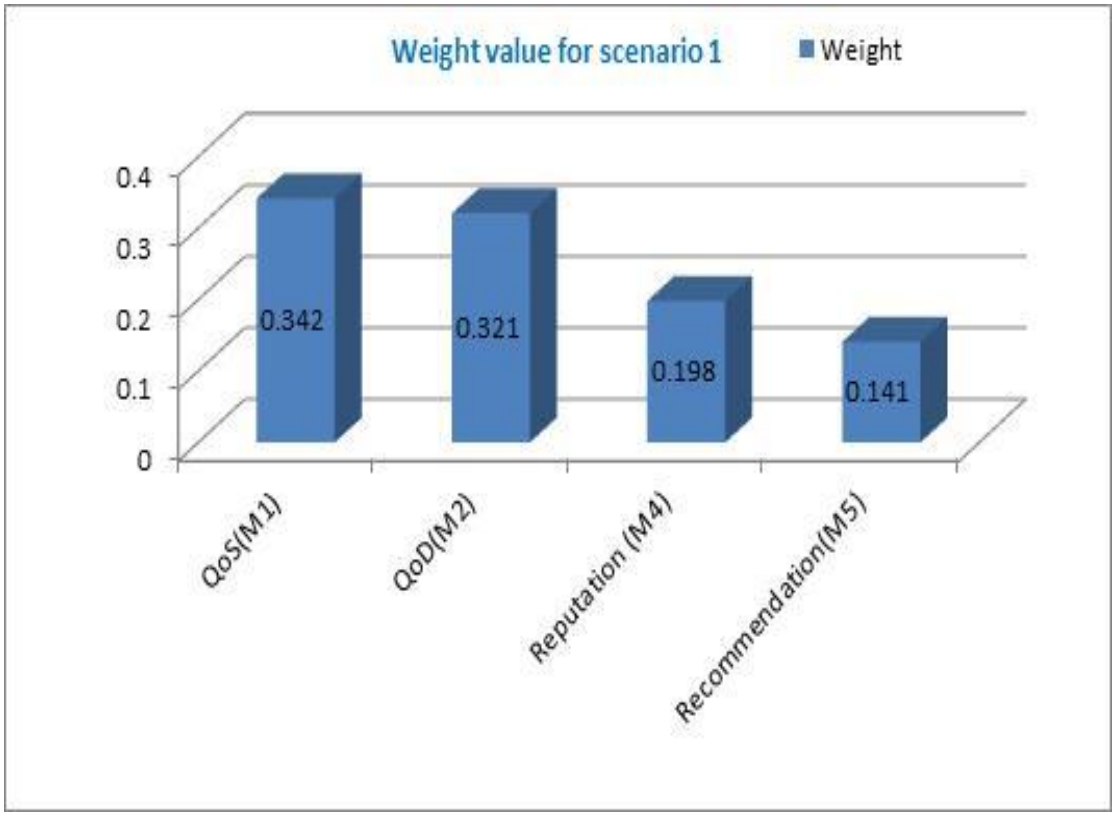

Figure 4. 1: Graphical Representation of Weight obtained in scenario 1

Figure 4.1 shows the prioritize weights of QoS, QoD Reputation, and recommendation. The most prioritized factor is QoS. The QoS and QoD show a very close impact.

For scenario 2 (SP to SR), In the same manner, we can calculate the weight vectors for social relationships, past reputation, and recommendation.

Table 4. 7: Fuzzified pairwise comparison matrix for scenario 2

	Social Relationship	Reputation	Recommendation
Social Relationship	1,1,1	1.5,2.234,3	1,2.26,3
Past Reputation	0.3,0.42,0.6	1,1,1	0.5,1.2,2
Recommendation	0.3,0.44,1	0.5,0.94,1	1,1,1

Table 4. 8: Fuzzified crisp matrix for scenario 1

	Social Relationship	Reputation	Recommendation
Social Relationship	1	2.31	2.17
Past Reputation	0.444	1	1.21
Recommendation	0.514	0.89	1

Table 4. 9: Normalized FCM for scenario 2

	Social Relationship	**Reputation**	**Recommendation**
Social Relationship	0.511	0.549	0.499
Past Reputation	0.226	0.228	0.264
Recommendation	0.263	0.235	0.232

λ_{max} = 3.104, CI= 0.05, CR=0.086

The calculation of eigenvector λmax for scenario 2 is given by equation 9

$$\lambda max = (1+0.444+0.514)*0.522 + (2.31+1+0.89)*0.239+ (2.17+1.21+1)*0.234 = 3.104$$

Since we have considered 3 metrics so the corresponding value of RI is 0.058 using Table 3. Hence the CI is calculated using equation 10.

$$CI = \frac{\quad}{\quad} = 0.05$$

Therefore, the consistency ratio (CR) is computed using equation 11.

$$CR = \frac{\quad}{\quad} = 0.086$$

Now, the CR value is 0.05 which is less than 0.10 so the Table 8 representing PCM is acceptable and consistent. Using the same procedure, we have validated the CR for every metric and sub-metric, and the outcomes are depicted in Tables 12, 13, and 14.

Table 4. 10: Eigen on trust metrics for scenario 2

Trust Metrics	Eigen Vector
Social Relationship	0.522
Past Reputation	0.239
Recommendation	0.234

Table 4. 11 : Fuzzy Synthetic Extent value (Si) value

Trust Metrics	Si
Social Relationship	0.256,0.526,0.995
Past Reputation	0.131,0.246,0.511
Recommendation	0.133,0.224,0.433

The result obtained for each value of S_i is depicted in Table 16. The degree of possibility (DP) for one TFN is highest than the other is computed through eq 17 and 18. Further, the DP associated with convex fuzzy values (CFV) highest than the three is evaluated through an equation. 19 and 20. as given by

$d'(S1) = \text{least } \{ WV(S1 \geq S2, S3)\} = \text{least } (1,1,1)=1$

$d'(S2) = \text{least } \{ WV (S2 \geq S1, S3)\} = \text{least } (0.376,1)=0.376$

$d'(S3) = \text{least } \{ WV (S3 \geq S1, S2)\} = \text{least } (0.474,0.932)=0.474$

$d'(S3) = \text{least } \{ WV (S3 \geq S1, S2)\} = \text{least } (0.474,0.932)=0.474$

$W' = (1, 0.376, 0.0.474)T$

$W= (1/1.85),(0.376/1,85),(0.474/1.85)$

W= (0.540),(0.204),(0.256)

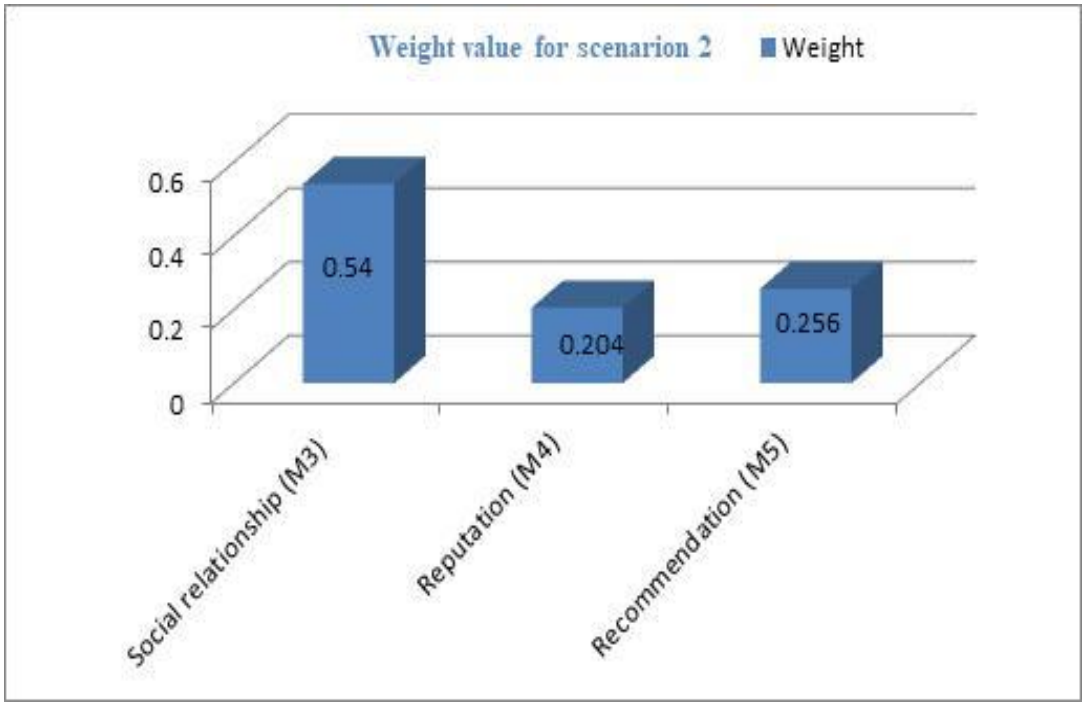

Figure 4. 2 : Graphical Representation of Weight obtained in scenario 2

4.1 Figure shows the social relationship metric gains the highest weight while reputation at the lowest position which shows the social relationship is the most important factor for the collaboration of nodes.

4.4 Estimating Weights of sub-Attributes using the Fuzzy Method

Similarly, we have calculated the weights of sub-metric criteria of QoS, QoD, and Social relationship sub-metrics to determine the weight values**.**

Table 4. 12: FPCM for Quality of Service for Sub metric

	Transaction Time (SM1)	**Latency (SM2)**	**Scalability (SM3)**	**Reliability (SM4)**
Transaction Time (SM1)	1,1,1	1,1.64,2.5	0.5,1.42,2.5	0.5,1.4,2
Latency (SM2)	0.4,0.55,1	1,1,1	0.5,1.07,2	0.4,0.7,2
Scalability (SM3)	0.4,0.73,2	0.5,0.95,2	1,1,1	0.4,0.9,2
Reliability (SM4)	0.5,0.71,2	0.5,1.17,2.5	0.1,1.17,2.5	1,1,1

λ_{max} = 4.109, CI= 0.03, CR=0.04

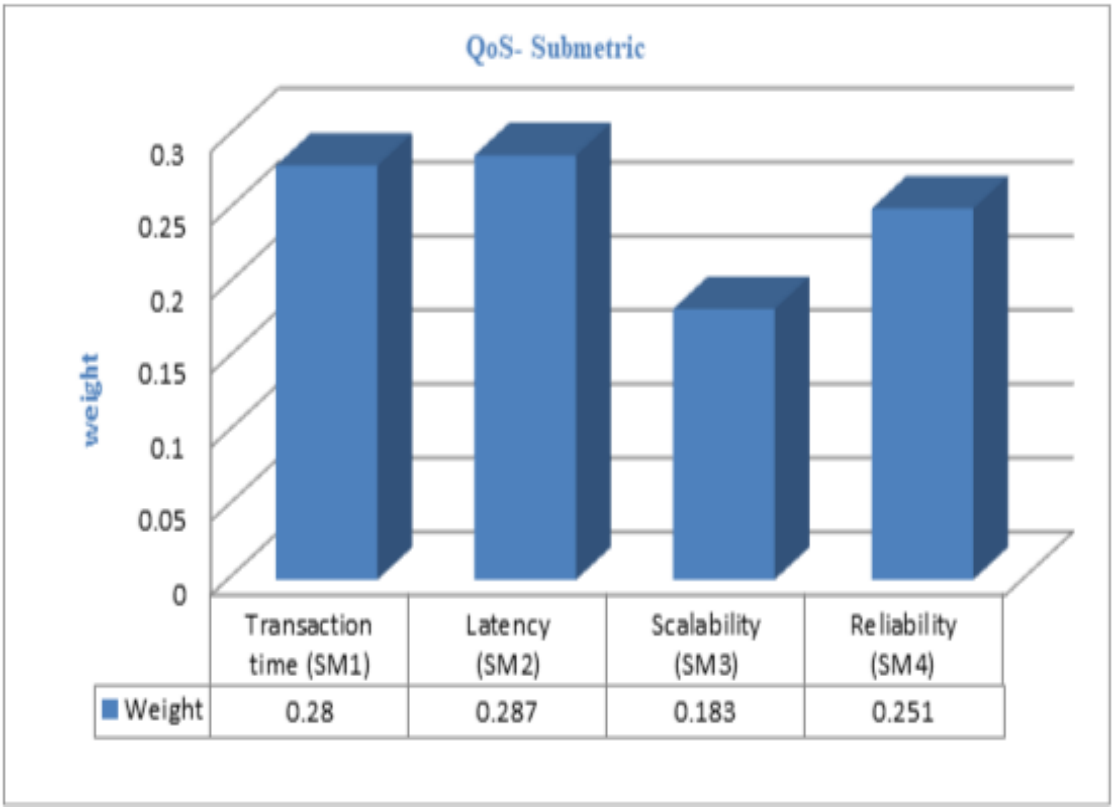

Figure 4. 3: Graphical Representation of Weight obtained QoS- Sub-metric

Figure 3 shows the graphical representation of transaction time, latency scalability, and reliability with a weight of 0.280,0.287,0.183, and 0.251 respectively where latency is the most prioritized one while scalability is at least position.

Table 4. 13: FPCM for Quality of Data-Sub metric

	Intrinsic (SM5)	**Accessibility (SM6)**	**Contextual (SM7)**	**Representational (SM8)**
Intrinsic (SM5)	1,1,1	0.5,1.39,2	0.5,1.19,2	1,1.69,2.5
Accessibility (SM6)	0.5,0.67,2	1,1,1	0.5,1.04,2	0.5,1.39,2.5
Contextual (SM7)	0.5,0.85,2	0.5,1.03,2	1,1,1	0.5,1.3,2
Representational (SM8)	0.4,0.55,1	0.4,0.73,2	0.5,0.77,2	1,1,1

λ_{max} = 4.106, CI= 0.035, CR=0.038

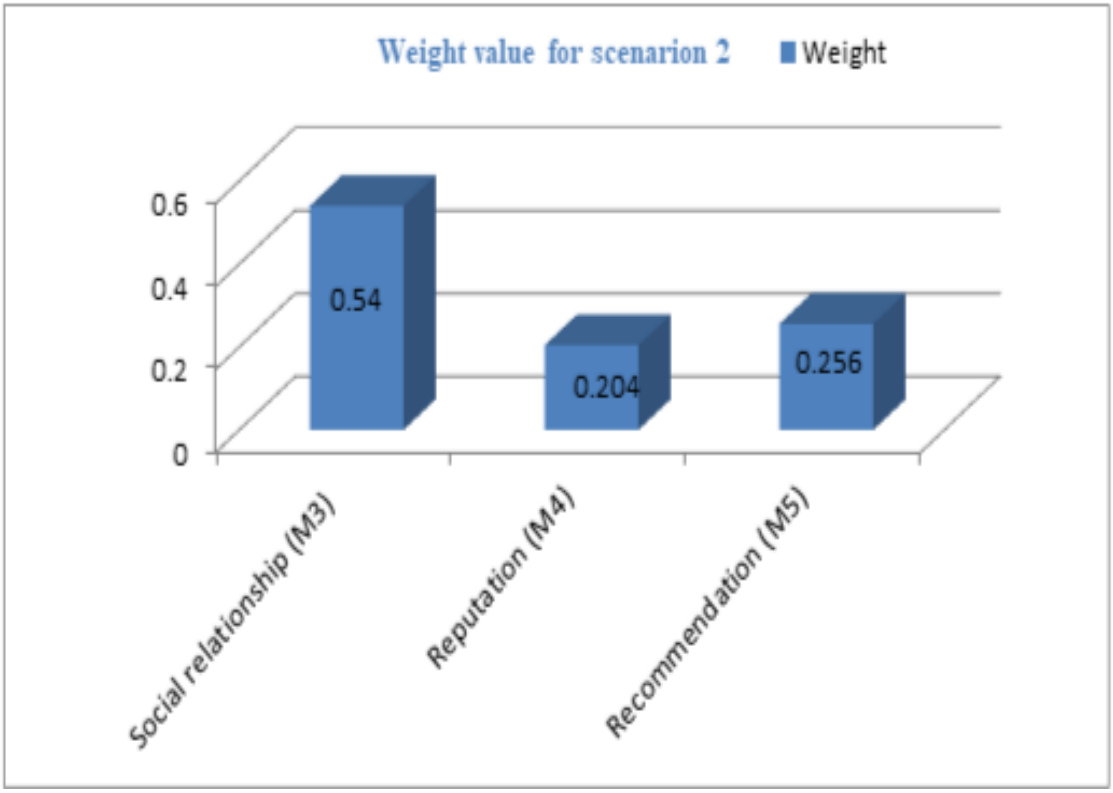

Figure 4. 4: Graphical Representation of Weight obtained-QoD sub-metric

Figure 4.4 depicts the sub-metric of quality of data where intrinsic achieve more weight as compared to other while representation gains very weight.

Table 4. 14: FPCM for Social relationships- Sub metric

	Honesty (SM9)	**Cooperativeness (SM10)**	**Community of Interest (SM11)**	**Centrality (SM12)**
Honesty (SM9)	1,1,1	0.5,1.32,2	1,1.44,2	0.5,1.34,2.5
Cooperativeness (SM10)	0.5,0.72,2	1,1,1	0.5,1.09,2	1,1.05,2
Community of Interest (SM11)	0.50.84,2	0.4,0.56,0.6	1,1,1	0.5,1.3,2
Centrality (SM12)	0.4,0.58,1	0.4,0.72,2	0.4,0.47,2	1,1,1

λ_{max} = 4.175, CI= 0.058, CR=0.064

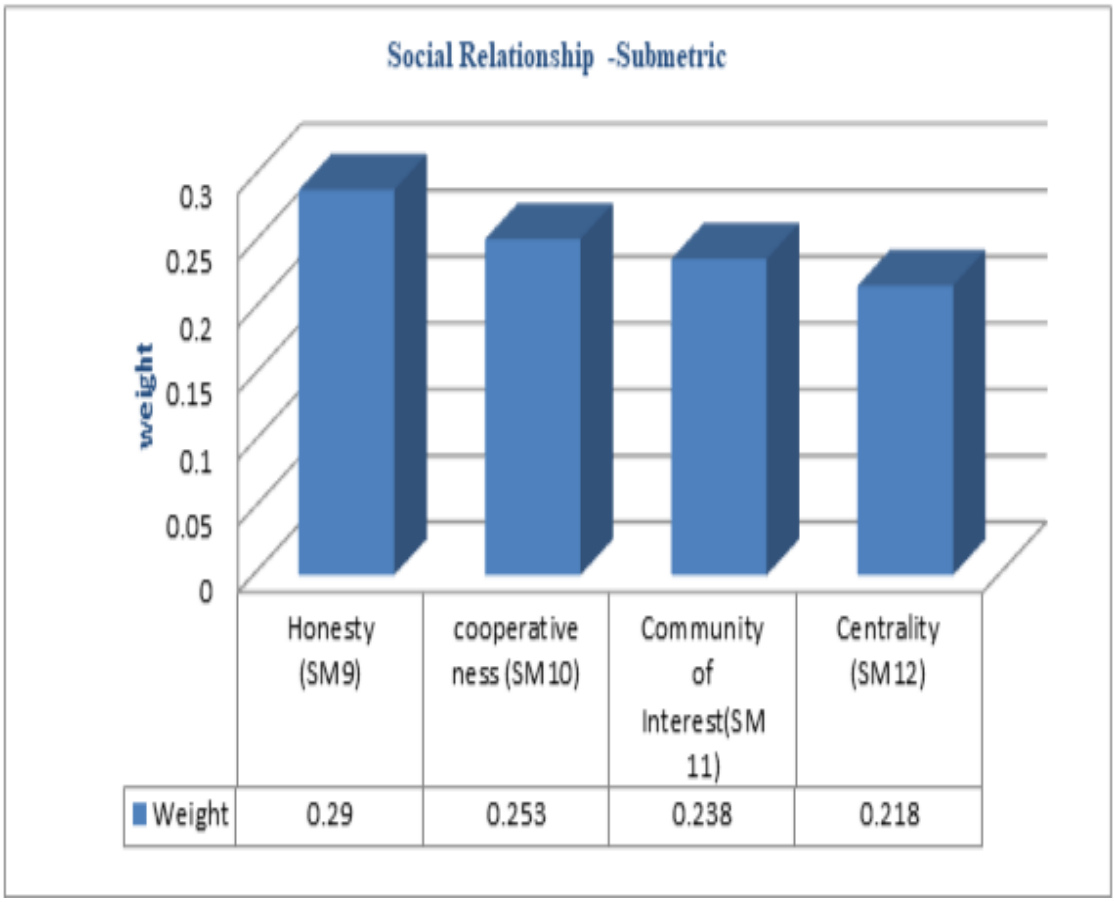

Figure 4. 5: Graphical Representation of Weight obtained- Social relationship-sub-metric

Figure 4.5 depicts the weight obtained by the social relations sub-parameter where honesty is the most prioritized one while centrality is at least positioned**.**

4.5 Estimation of Weights of Metrics and sub metric through Fuzzy Method

The trust metric weight for Scenario 1 and scenario 2 are shown in Tables 4.14, and depict local and global weights respectively. The computed global weight (GW) using fuzzy AHP of each trust metric reflects its priority over other metrics. The GW of every metric is the product of its local weight (LW) and level 1 metric weightage. The LW depicts each metrics' impact on one another metric in the same category[91]. For instance, the LW of SM2 is 0.287 and it is the top graded metric in the class of QoS because of its weight when inspect with others at the same level.

From the previous discussion, it is clear that recommendation and past reputation signifies indirect trust whereas QoD and QoS signify direct for scenario 1 and social

relationship for scenario 2. Therefore, it can be observed that SM2 is the high-rank global metric for scenario 1 while past reputation gains the highest rank among all[92]. In scenario 2, honesty (SM9) achieved the highest rank globally for the direct trust metric while recommendation overall ranked high. Within level 1 for scenario 1, QoS is the top rated metric whereas recommendation achieves the lowest rank In level 1 for the scenario, 2 social relationships emerged as the highest prioritized metric because of their maximum weight by examining other metrics whereas reputation seems to be the lowest one. Based on the result depicted in figure 4.5, latency is the top graded metric locally and it is the rated higher metric globally and achieving the third rank overall.

Table 4. 15: Final Weight of each metric local and Global and ranking for Scenario 1

Metric	Weight	Sub-metric	Native weight	Native ranking	Universal weight	Universal ranking
QoS(M1)	0.342	SM1	0.280	2	0.0957	4
		SM2	0.287	1	0.0981	3
		SM3	0.183	4	0.0625	10
		SM4	0.251	3	0.0878	6
QoD(M2)	0.321	SM5	0.284	1	0.0911	5
		SM6	0.259	2	0.0831	7
		SM7	0.231	3	0.0741	8
		SM8	0.223	4	0.0715	9
Past Reputation (M4)	0.198	-	-	-	0.198	1
Recommendation(M5)	0.141	-	-	-	0.141	2

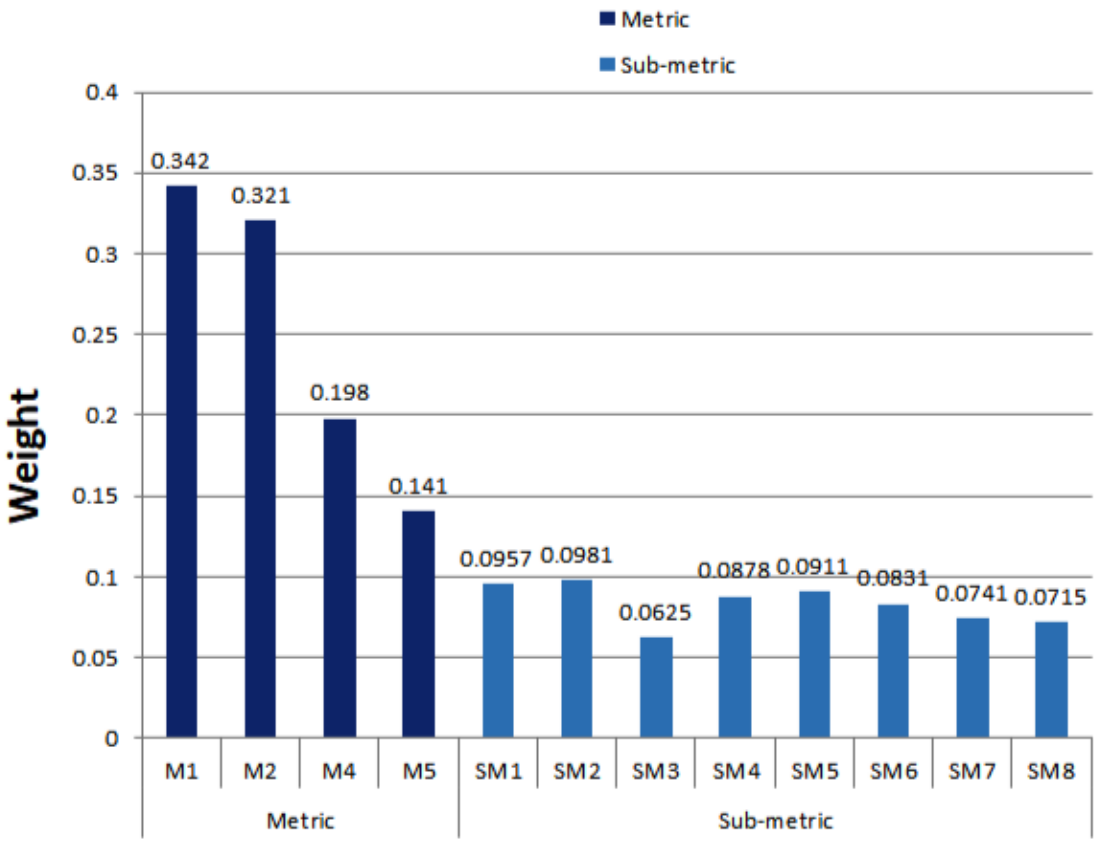

Figure 4. 6: Ranking of Metric for scenario 1

It signifies that experts have taken latency as an important metric while computing direct trust. The other highest-ranked metric is transaction time, intrinsic data, accessibility, and reliability with native weights of 0.280, 0.284, 0.259, and 0.251.

Moreover, in the case of indirect trust past reputation performs better than the recommendation. This scenario points out experts considered the significance of past reputation over recommendation while receiving inputs from nearby nodes. In addition, recommendation and past reputation have no further sub metric so they obtained higher rank among sub-metrics. So, reputation based on past communication obtained the topmost rank overall.

Table 4. 16: Final Weight of each metric local and Global and ranking for Scenario 2

Metric	Weight	Sub-Metric	Local Weight	Local Ranking	Global Weight	Global Ranking
Social Relationship(M3)	0.540	SM9	0.290	1	0.1566	3
		SM10	0.253	2	0.1366	4
		SM11	0.238	3	0.1285	5
		SM12	0.218	4	0.1177	6
Past Reputation (M4)	0.204	-	-	-	0.204	1
Recommendation (M5)	0.256	-	-	-	0.256	2

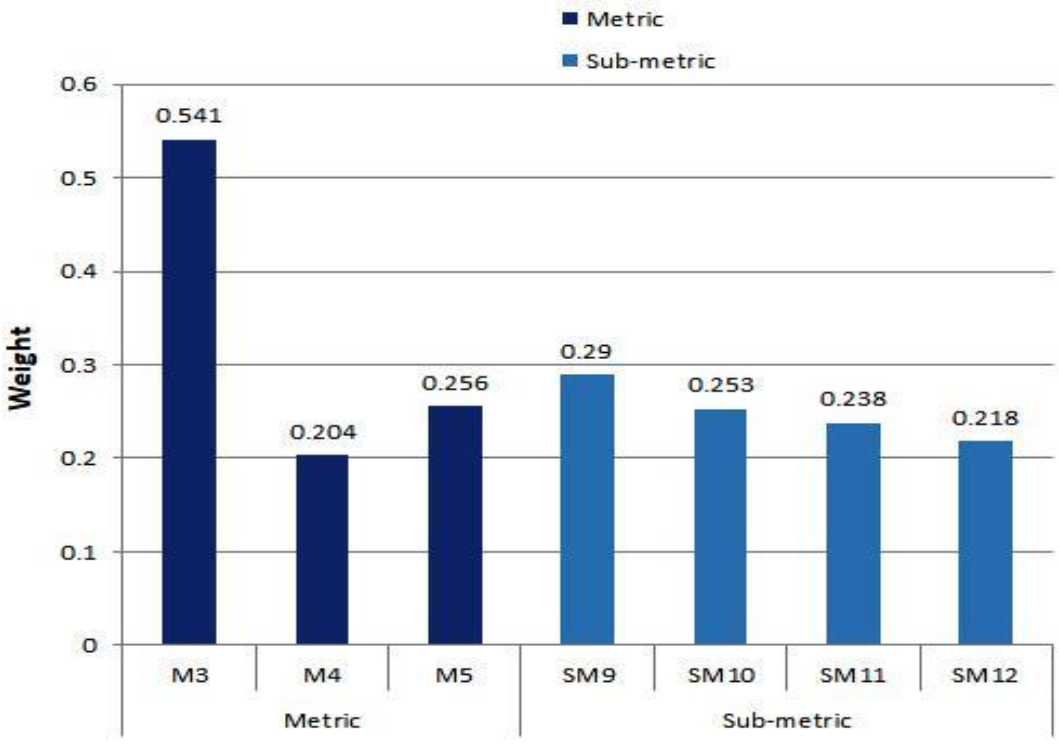

Figure 4. 7: Ranking of Metric for scenario 2

As depicted in figure 8, locally honest has gained the highest rank and highest top-rated sub-metric for DT evaluation. This implies that experts acknowledge the fact associated with honesty prominently to compute trustee's trust about the social object to social object collaboration. Again, honesty is the highest-ranked sub-metric as compared to all with a global weight of 0.1566. In the case of an IDT, the recommendation obtained a higher rank than the past reputation. This means that the respondent acknowledges recommendation is extra effective than reputation achieve through past communication from social object to social object colluding[93]. Since recommendation and reputation do not have further factors, therefore these are top graded in GW where recommendation gained the highest rank.

4.6 Estimation of trust using the hierarchy-based model for scenarios 1 and 2

After computing the weight vectors value, hierarchical-based models are utilized for trust computation for both scenarios which are depicted in chapter 3. The computation of the trust value for ten nodes computed on the local ad-hoc network for SR to SP and SP to SR is shown below in Table 4.17. Further, the direct and indirect trust is calculated by using equations 23 and 23. In our, we have taken only level for computation trust of social objects to identify the malicious ones. The trust value of all social nodes can be utilized to depict whether a particular node is trusty or not by referring the table 3.2 of chapter 3.

Table 4.6.1 shows the comparison trust value obtain in both scenarios i.e SR to SP and SP to SR where direct trust value gained more weightage in comparison to indirect trust value at level 1. The sensitivity analysis has been done to check the variation of trust values in both scenario by changing the trust adjusting factor to maintain the trust value.

Table 4. 17: Depicts the trust value of 10 nodes obtained from local ad-hoc network

Nodes	Level -1 Scenario 1			Level-1 Scenario 2		
	Direct Trust (M1+M2)	Indirect Trust (M4+M5)	Change in Trust value in %	Direct Trust (M3)	Indirect Trust (M4+M5)	Change in Trust value in %
Node 1	0.6422	0.6089	5.18 %	0.7082	0.6379	9.92 %
Node 2	0.7584	0.6953	8.32 %	0.8625	0.7571	12.22%
Node 3	0.9599	0.8374	12.76 %	0.9749	0.8189	16.00%
Node 4	0.6563	0.6149	6.30 %	0.4795	0.4267	11.01%
Node 5	0.7805	0.6947	10.99 %	0.6984	0.6095	12.72%
Node 6	0.8347	0.7275	12.84 %	0.7679	0.6476	15.66%
Node 7	0.4658	0.4079	12.43 %	0.9532	0.8121	14.80%
Node 8	0.8963	0.7944	11.36 %	0.6084	0.5372	11.70%
Node 9	0.6995	0.6462	7.619 %	0.8463	0.7268	14.12%
Node 10	0.2621	0.2267	13.50 %	0.4847	0.3956	18.38%

4.7 Assessment of Social objects using trust values

The trust value depicted in the previous table shows the decrease in trust of social nodes while performing collaboration using an indirect trust (transitive trust). It signifies that direct trust computes more trust among social objects while indirect collaboration minimizes its trust among social objects in SIoT networks. The value of trust adjust factors α, β and γ have taken by the researcher 0.6,0.3 and 0..3 respectively to measure trust value which reflects balancing behavior to main the trust of the social object in both the scenario i.e SR to SP and SP to SR.

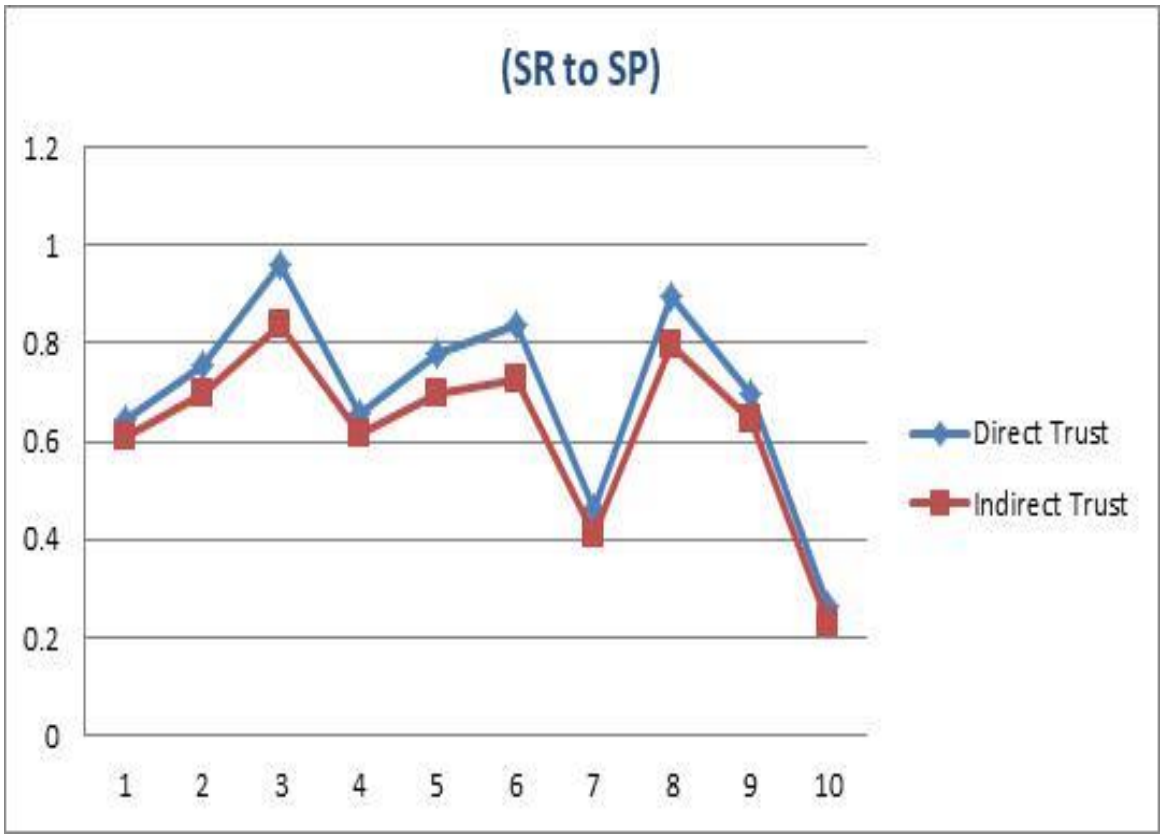

Figure 4. 8: Comparison of trust values for scenario 1

The comparison of direct trust and indirect trust for the same node is shown in figure 4.8 and figure 4.9. The average change in trust observed in case of scenario 1 (SR to SP) 7.10 % while in another case i.e SP to SR is 11.74 %. which signifies that the client accesses better services and quality of data is based on QoS and QoD metrics while past reputation and recommendations responsible for poor or false services

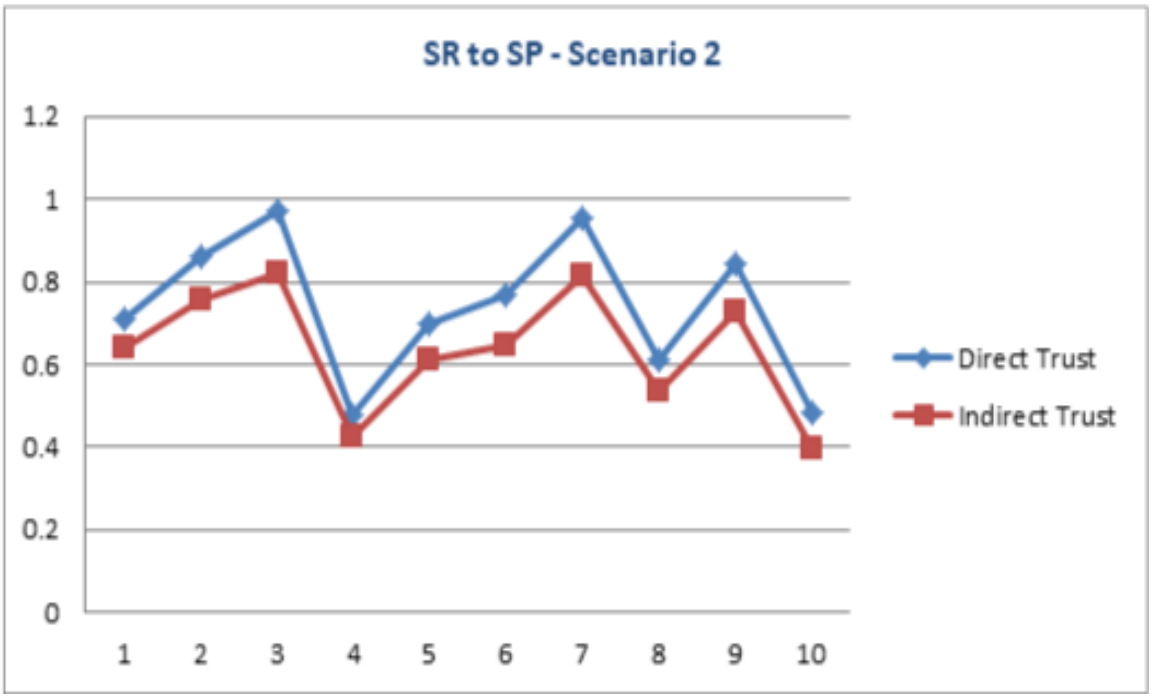

Figure 4. 9: Comparison of Trust values for scenario2

The range of trust value for various linguistic term like no trusty ,very less trust, trust, strong ly trust and absolute trusty is depicted in previous chapter is applied to check consistency of our local adhoc network. We find 80 % nodes are comes in range of trust while 20 % nodes show malicious behavior or untrusty. The validation of trust values computed for assessment has been done in chapter 5 Since without theoretical and statistical validation for trust evaluation framework does not certify to be applicable all scenario.

4.8 Validation Phase

The validation of trust values computed for assessment has been done in chapter 5 Since without theoretical and statistical validation for trust evaluation framework doesn‟t certify to apply to all scenarios. The theoretical validation is performed by a selection of experts of same from the same industry who have a strong background in social IoT networks.15 experts have given their valuable suggestions and comment .most of them praised the usage of a fuzzy environment integrated with the social internet of things due to the high reliability of results[94]. Therefore the implemented framework passes the test of theoretical validation successfully. The detailed description of theoretical validation is given in chapter 5The statistical validation only makes sense when the current framework qualifies the theoretical framework. It is a

mathematical tool for collecting, organizing, analyzing, and interpreting numerical data in a structured way to represent the statistical significance or validation of the proposed framework, statistical analysis is performed on the ten nodes by incorporating suggestions for a reassessment of the local ad-hoc network in terms of SR to SP and SP to SR. The trust value calculated for assessment of trust in both scenarios and after considering the suggestion and comment show s negligible changes. A detailed description of statistical validation is depicted in the upcoming chapter.

4.9 Wrapping Phase

Every study is limited by some facts that need to be discussed. The present strategy is based on experts‟ opinions they may create vagueness and inconsistency at the time of trust evaluation of social nodes in SIoT. The present work only considers the 5 trust metrics among a range of other Metrics. With the help of different trust metrics, security trust among social nodes can be increased. Using Small data set of 10 nodes is a major limitation of our work We consider the direct and indirect trust while other aspects can also be analyzed like local Vs Global, subjective Vs objective, and Rank Vs Threshold

4.10 Conclusion

In this chapter, the researcher has depicted the conceptual working of the trust evaluation frame by following the theory and principle disused in chapter 3. They determined the weighted vectors associated with trust factors using fuzzy AHP mechanism. We have also computed the local as well as the global impact of trust factors on social networks and perform an overall ranking utilizing weight metrics. And then further computed the trust value for two scenarios SR to SP and SP to SR for the social object for 10 nodes on a local ad-hoc network and analyze the change in trust between a direct and indirect trust for both scenarios. Further, we have also pointed out the importance of validation and a few limitations associated with our work

Chapter 5
Validation of Framework

CHAPTER 5: VALIDATION OF FRAMEWORK

"When the trust is high, communication is easy, instant, and effective."

-- Stephen Covey --

5.1 Background

With the development of the digital world, various physical devices are enabled by the internet known as the Internet of Things (IoT). These IoT devices connected with the digital world in cyberspace through various instruments like sensors, smart objects, and RFID are used in society. Smart objects like electronic gadgets and electronic consumers are connected to compute the resources and share information to access billions of new services connecting everyone with everything. An IoT device needs to connect to the network and provide services in the network that are trustworthy[95]. The motivation of the trust system for SIoT environment is very sensitive to sharing information. Miscellaneous devices and owners are connected with the objects. Misbehaving owners and devices or attackers activated on the network may perform attacks to destroy the reputation of other IoT devices or owners. These IoT devices may perform homogeneous or heterogeneous services on the network[96]. In addition to this, users of IoT devices are likely to be socially connected through social networks like Facebook, Twitter, Google, etc. as a consequence, misbehaving nodes are socially connected to share and access the ownership of the services.

Trust of the social object plays a vital role while having interaction with one another in SIoT network. The number of increasing untrusty nodes significantly decreases the performance of the system to a great extent[97]. It‟s difficult to identify the trust of social nodes at an early stage due to various attacks like bad mouthing, whitewashing attacks, self-promoting attack etc. Hence untrusty social object is responsible to influence the QoS and QoD level in a social IoT environment[98]. Thus researchers are always looking for novel methods and techniques for computing the trust of the social system to provide fruitful service through these social objects to their clients and assure them of safe and secure communication. In the designing phase, the evaluation of trust is more efficient while considering the improvement by utilizing

the MCDM approach[99]. Therefore the validation accomplished in this chapter was utilized to validate the overall trust score of the newly joined Social IoT node to be detected as malicious or not.

Due to the unavailability of fixed and standard values regarding trust evaluation, it is difficult to validate the outcomes obtained. Because of the involvement of α, β, and γ, result analysis has been discussed in this chapter. By considering the importance of validation, the outcomes obtained on trust evaluation are utilized for both theoretical as well as empirical respectively. The expert working in the field of Social Internet of Things finds the methodology and framework for trust evaluation appropriate. The experts also provided a questionnaire related to the goal and methodology along with adequate questions dealing with the objective. For determining the effectiveness of the results obtained the researcher compared their results with other existing techniques evaluated in the chapter and found them more improved. Further, the evaluation of validation through statistically improved suggestion; the methodology is again implemented on social vehicle networks based on suggestion and weightage of metrics.

5.2 Sensitivity Analysis

Analyzing the impact of an independent variable over the dependent variable under a certain set of assumptions is termed sensitivity analysis. Sensitive analysis not only analyzes the effect due to key metric of a network but also check consistency for input variables according to a range of boundaries as defined. In chapter 3, the researcher considered the values of α, β, and γ as 0.6, 0.3, and 0.3 during trust evaluation. The values of α, β, and γ lies in the range of 0 to 1 depicting that a smaller value signifies the highest imprecision in decision making. The α = 0.6, β=0.3 and γ=0.3 shows a balanced environment because of the uncertainty associated with dependent variables. Hence such value strongly affects the weight of each metric, ranking and overall trust evaluation.

The integrity of Fuzzy-AHP can be further enhanced by determining the impact α, β, and γ values in the final results, and analysis is required to compute the value of α, β, and γ truthfully. Hence to verify the variation involved within the result, researcher has used 15 combination of α, β and γ values for direct and indirect trust on social

local ad-hoc network as experiment consist of N1(0.6,0.3,0.1), N2(0.6,03,0.4), N3(0.6,03,0.7), N4(0.6,0.3,0.9), N5(0.6,0.1,0.3), N6(0.6,0.4,0.3), N7(0.6,0.6,0.3), N8(0.6,0.8,0.3), N9(0.6,0.9,0.3), N10(0.2,0.3,0.3), with N0 (0.6,0.3,0,3).

Table 5. 1: Sensitivity analysis for Scenario 1

	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust
Exp No	N1		N2		N3		N4		N5		N0		N6		N7		N8		N9		N10	
α	0.6		0.6		0.6		0.2		0.5		0.7		0.8		0.3		0.9		0.7		0.2	
β	0.2		0.5		0.3		0.3		0.3		0.3		0.1		0.5		0.2		0.7		0.9	
γ	0.7		0.2		0.6		0.9		0.7		0.5		0.2		0.3		0.3		0.3		0.3	
Trust Comp	0.8563	0.7399	0.6322	0.6089	0.7584	0.6953	0.6599	0.6374	0.6563	0.6149	0.7805	0.6786	0.8347	0.7275	0.4658	0.4079	0.8963	0.6944	0.6995	0.6052	0.2621	0.2237

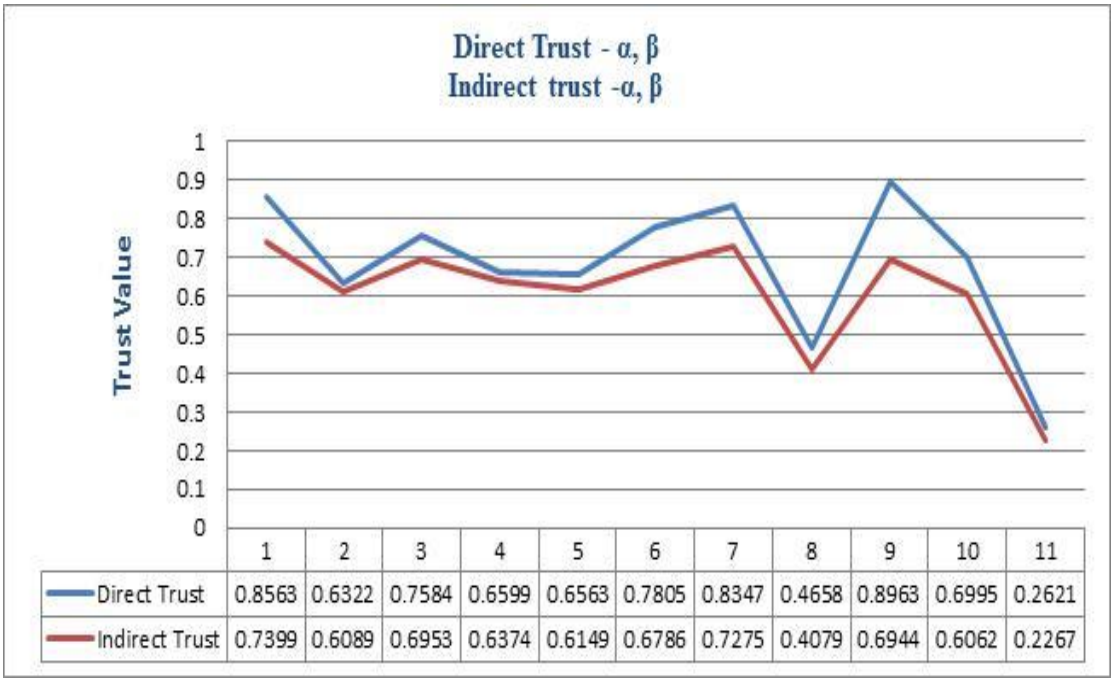

Figure 5. 1: Sensitive Analysis of direct and indirect trust for scenario 1

Here the value of α, and β is constant while γ is in variation for N1, N2, N3, and N4. For N5, N6, N7, N8, N9, α, and γ are constant while β is in variation and further for N10, N11, N12, N13, N14, β, and γ are constant while α is in variation. The results are depicted in table 5.1.

Table 5. 2:: Sensitivity analysis for Scenario 2

	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust	Direct Trust	Indirect trust
ExpNo	N1		N2		N3		N4		N5		N0		N6		N7		N8		N9		N10	
α	0.6		0.6		0.6		0.2		0.5		0.7		0.8		0.3		0.9		0.7		0.9	
β	0.2		0.1		0.3		0.3		0.3		0.3		0.1		0.5		0.2		0.7		0.1	
Trust Comp	0.7082	0.6081	0.7625	0.6871	0.6549	0.6089	0.4795	0.3767	0.6847	0.6295	0.7024	0.6876	0.8532	0.9121	0.6084	0.5372	0.8463	0.7268	0.4847	0.9056	0.7308	0.6912

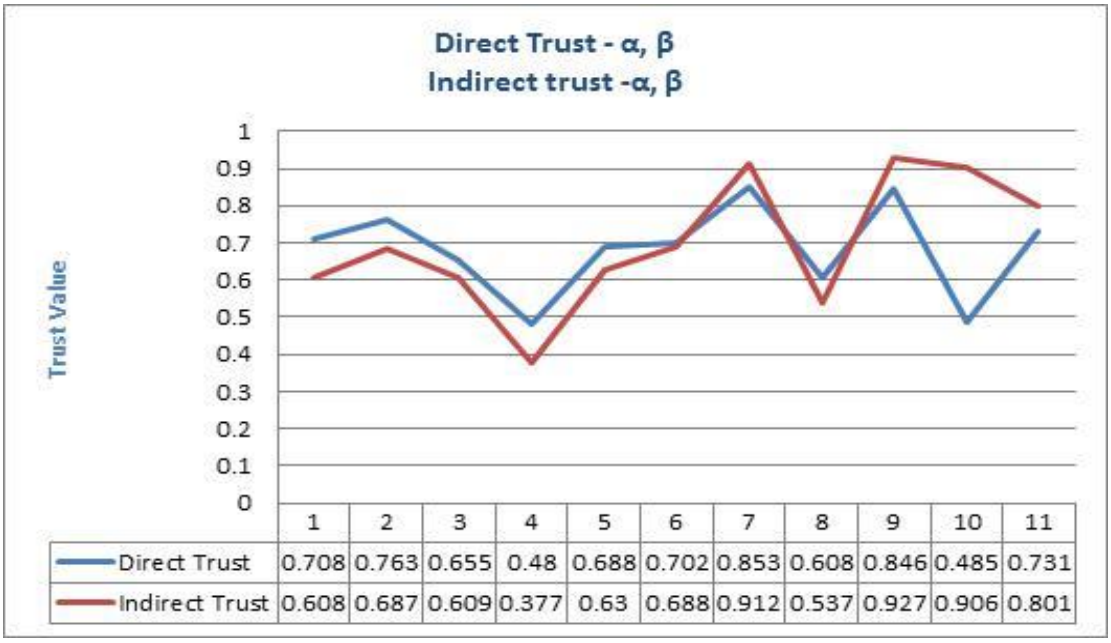

Figure 5. 2 : Sensitivity analysis for scenario 2

5.3 Validation

Validation methods are the heart to test any research. It is a way of theoretical validation that explains the scope and nature of the work. It is the process of developing and evaluating proof of work, validation, and use. How the validity is to visualize mentally the scope and nature of validity investigation as well as the method of gathering information. The acceptance of any result depends upon its validation and makes the people accept the result of any method. Generally, two types of techniques are used for validation known as theoretical validation and statistical validation. Theoretical validation is used to address the question, according to the evaluation of the methods and what it is supposed to measure. On the other hand, empirical validation is used to address the question, of whether the evaluation of the method is experimental and it defines the different variables in the methodology in various ways. Malvin V. Zelkowitz said "without anything is confirmed, why should industry select new tools or methods?

The statistics of the data provide a method to collect the data. It is used to process and analyze the data in an experimental environment. Interpretation of the result of an experiment is one of the methods to accept or reject the consequences of any research. The statistical validation involves the Null hypothesis in a sequence of data collection, data presentation, data experiment, and inference drawn from the result. Based on some set of statistical rules provided by the statisticians, the Null hypothesis is either accepted or rejected. Rejection of the Null hypothesis shows the acceptance of the research or vice versa.

5.3.1 Theoretical Validation

It is the fundamental technique of validation. It serves as the precondition to illustrate the importance of a measure or empirical validation. Theoretical validation requires that an analyst has a deep understanding of the concept being measured. Researchers had identified 35 experts from India and abroad working in the area and discussed with them the proposed framework. Out of the 24 experts give their valuable comments and suggestions. Most experts are of the view that a proper structure of trust evaluation enhances the performance of the network and provides an opportunity to improve the services and quality of data to participate in the network. Most of the experts gave their views and agreed that the trust of the nodes is impressed by the three attributes including quality of service, quality of data, and social relationship. Service providers can directly trust the nodes, after evaluating the trust in the

nodes[100]. It is also suggested by most of the experts that quality of service may be affected by the other direct or indirect attributes and sub-attributes inclusive latency, scalability, reliability, and other attributes with the positive or negative impression[101]. Hence, the proposed trust management framework, may confidentially improve the quality of service and apply the transactions on the network. Some of the critical comments and remarks made by experts are as follows:

- Without the implementation of the framework, the proposed framework evaluation is useless.
- Validation of the framework will deliberate its actual use.
- The proposed framework may be implemented in industrial software projects also.

All the given comments and suggestions are incorporated by the researcher. The proposed framework is implemented and validated also.

5.3.2 Statistical Validation

It is the process by which it can be established that an assessment is useful in the imagination and that it is related to the other variables as expected in the theory. It is performed in two ways: pre-tryout and tryout. Pre-tryout involves a small set of data. If the result of the analysis is satisfactory, the tryout will be applied to a large set of data.

5.4 Design of an Experiment process

Experiments are organized for testing and investigating a given theory. With the help of experiments, theoretical predictions are tested against reality. Theories are validated by using experimentation and data collection tools[102]. The objective of the experiment is to collect adequate data to acquire a statistical result. The proposed framework for the evaluation of trust in SIoT environment performed experiments for validation purposes. In pre-tryout, Local ad-hoc network design is used as input.

With the help of defining the precedency of the trust attributes, the researcher evaluates the trust of the nodes. After receiving suggestions from the expert and then incorporating them on the nodes, the updated trust value is increased from the previous trust value. After analyzing the result of the pre-tryout, hence no significant changes are received. Therefore, a tryout is performed on a larger set of data. 10

nodes are considered as input. The same may be repeated for the 10 nodes. Based on the result, statistical interpretations are done.

5.4.1 Pre Tryout

The pre-tryout has been conducted on the local ad-hoc network. Trusts of nodes are evaluated on direct interaction as well as indirect interaction among nodes of the local ad-hoc network. Indirect interaction means trust calculated based on recommendation and reputation and direct interaction means, direct trust calculated based on the quality of service and quality of data in the social environment which is shown in table 5.3.

Table 5. 3: Observed change in Trust (SR to SP)

	Trust of Node's on Direct Interaction	Trust of Node on Indirect Interaction	Change in Trust (%)
Node's Trust Value	0.7305	0.6786	07.10 %

Table 5. 4: Observed change in Trust (SP to SR)

	Trust of Node's 0n Direct Interaction	Trust of Node 0n Indirect Interaction	Change in Trust (%)
Node's Trust Value	0.7628	0.6732	11.74 %

Therefore, we can say that the expert‟s suggestion and the implemented framework established for direct interaction as well as indirect interaction among nodes of the local adhoc network regarding SR to SP and SP to SR changed by 07.10 % and 11.74 % as shown in table 5.4.

5.4.2 Review and Revision

Results received from pre-tryout are investigated**.** A critical review of the result reinforced the acceptability of the proposed framework. For the alteration of the

evaluation, the classical method is used for correlation between fuzzy and classical methods. Therefore, the researcher adopted the same framework for a further tryout with a large set of data.

5.4.3 Tryout

Statistical validation is a continuous process and hence these are the degrees of validity, more testimonials are there, the more valid an approach. Collecting more and more testimonials is required for the proposed framework[103]. A tryout is carried out with the following pre-tryout. The tryout contains 10 nodes of the same network. These are the nodes selected by the administrator of the local ad-hoc network and assess the impact of direct trust on indirect trust with the same trust metrics

Table 5. 5: Reassessment of the trust for a social object using ten nodes (SR to SP)

Nodes of Local adhoc Network	Trust of Node's on Direct Interaction	Trust of Node on Indirect Interaction	Change in Trust (%)
Node 1	0.6436	0.6101	5.20 %
Node 2	0.7587	0.6956	8.31 %
Node 3	0.9595	0.8376	12.70 %
Node 4	0.6561	0.6147	6.31%
Node 5	0.7809	0.6945	11.06%
Node 6	0.8343	0.7282	12.71 %
Node 7	0.4662	0.4081	12.46 %
Node 8	0.8969	0.7941	11.46%
Node 9	0.6998	0.6461	7.67 %
Node 10	0.2625	0.2269	13.56 %

Due to the unavailability of a relevant model for comparison of results regarding local ad-hoc networks for the same set of metrics like QoS, QoD, Social relationship, Reputation, and Recommendation in case of scenarios 1 and 2. We asked experts for review and suggestions for our results to validate our work. Further, we analyze the expert's opinions and suggestions provided by them and perform reassessment for both the scenario (SR to SP and SP to SR) and computed the trust values. After performing the reassessment of both scenarios for the same set of nodes by utilizing the expert‟s opinion and suggestion, we found negligible changes while computing the trust values for SR to SP and SP to SP for the local ad-hoc network utilized by the researcher

Table 5. 6: Reassessment the trust for a social object using ten nodes (SP to SR)

Nodes of Local adhoc Network	Trust of Node's on Direct Interaction	Trust of Node on Indirect Interaction	Change in Trust Value (%)
Node 1	0.7088	0.6382	9.96 %
Node 2	0.8627	0.7569	12.26 %
Node 3	0.9752	0.8187	16.04%
Node 4	0.4799	0.4269	11.04%
Node 5	0.6987	0.6092	12.80 %
Node 6	0.7684	0.6464	15.87 %
Node 7	0.9539	0.8114	14.93 %
Node 8	0.6087	0.5367	11.82 %
Node 9	0.8465	0.7263	14.19 %
Node 10	0.4854	0.3958	18.45 %

5.5 Statistical Analysis

It is a mathematical tool for collecting, arranging, investigating, and demonstrating numerical data. It is used to represent the statistical consequence or validation of the proposed framework. To perform the validation, statistical analysis is executed on the ten nodes[104]. The collection of sample size from the ad-hoc network is small. The two-tailed t-test is employed for finding out the level of the significance, like acceptance and rejection of the null hypothesis. Therefore, the acceptance and rejection of a Null hypothesis is based on a level of significance for one-tailed and two-tailed tests. Alpha (α) level of significance may be considered on (0.05) or (0.01) for a one-tailed test is taken for rejection of the Null hypothesis[105]. The performance of statistical analysis is performed with the formulation of the null hypothesis and alternate hypothesis. The trust values are calculated firstly based on data collected and secondly based on experts' opinions and suggestions for both scenarios (SR to SP and SP to SR). Hence the pre and post-trust evaluation for social nodes is taken under consideration to determine the conclusion that whether there is a drastic change observed or not by utilizing before execution and after execution of the data[106]. After performing the hypothesis, the computed values „t" is decision making, either to accept or reject the hypothesis.

5.6 Hypothesis Testing

The hypothesis is used to conduct quantitative research to make an effort to answer research questions. The null hypothesis considers that there is no significant difference between two or more variables. However, the alternate hypothesis rejects the relationship. Therefore, the rejection of the hypothesis provides a stronger base to accept the alternate hypothesis. Hence, the presented hypotheses were used for validation of the proposed framework which is as follows:

Null Hypothesis (H_{01}) There is no significant difference between trusty ad untrusty nodes in the SIoT environment.

Alternative Hypothesis (H_{11}) There i[9]s a significant difference between trusty and un-trusty nodes in the SIoT environment.

5.7 Statistical Interpretation

The observation values of trust evaluation as shown in table 5.7, it can be decided very easily that all the suggestions provided by the experts for all the nodes perform well. The value of trust evaluation for both scenarios after experts' opinions depicts no change (negligible) as compared to the previous one. By examination, it appears that all the suggestions are incorporated and work correctly. The values showed that the trust of the nodes in all the ten nodes are estimated and found it was the same approximately. A comparative study and change in trust evaluation for the scenario are shown in figure 5.3 for a comparison of nodes.

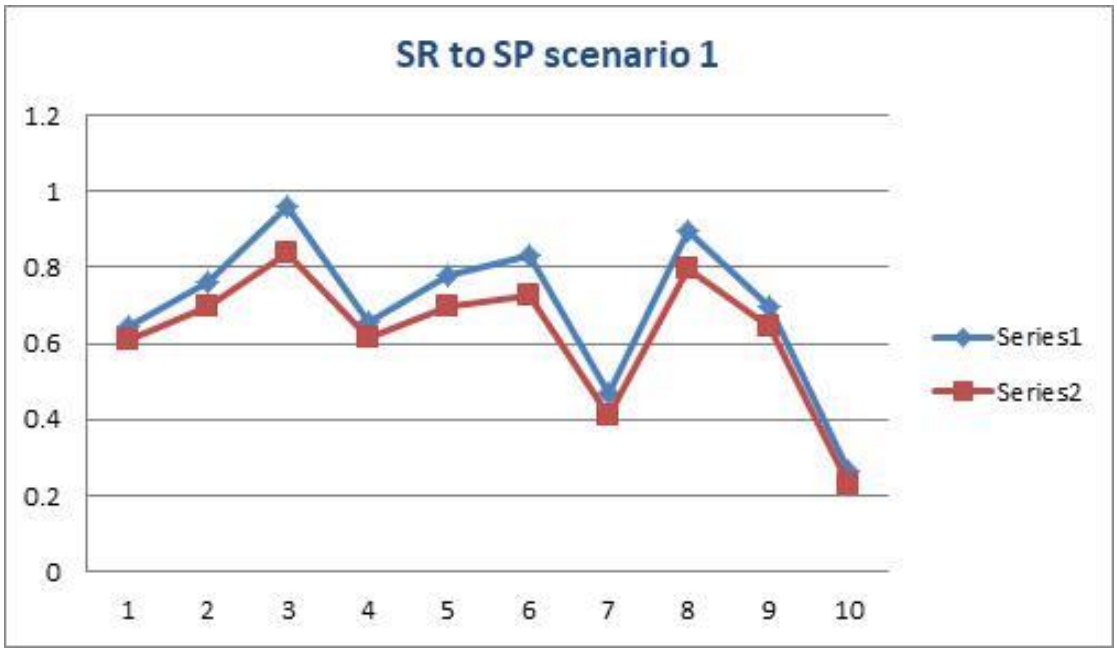

Figure 5. 3: Graphical Representation of Trust values using expert suggestions for scenario 1

To make the evaluation derived from it, acceptable or validate the approach, it should be verified, therefore the difference in the evaluated values is due to the given suggestions from the experts or it is just a sampling error. Therefore, the level of the proposed framework should be evaluated. By using the imaginary data analysis, the t-test is appropriate for the current situation for a small set of data. When the homogeneous groups of individuals participate in a pre-test then the group demonstrates for the treatment. The tested group again participated for retested after treatment to evaluate the impact of the treatment has been significantly accepted. The t-test was performed to verify the level of significance approach is acceptable or not.

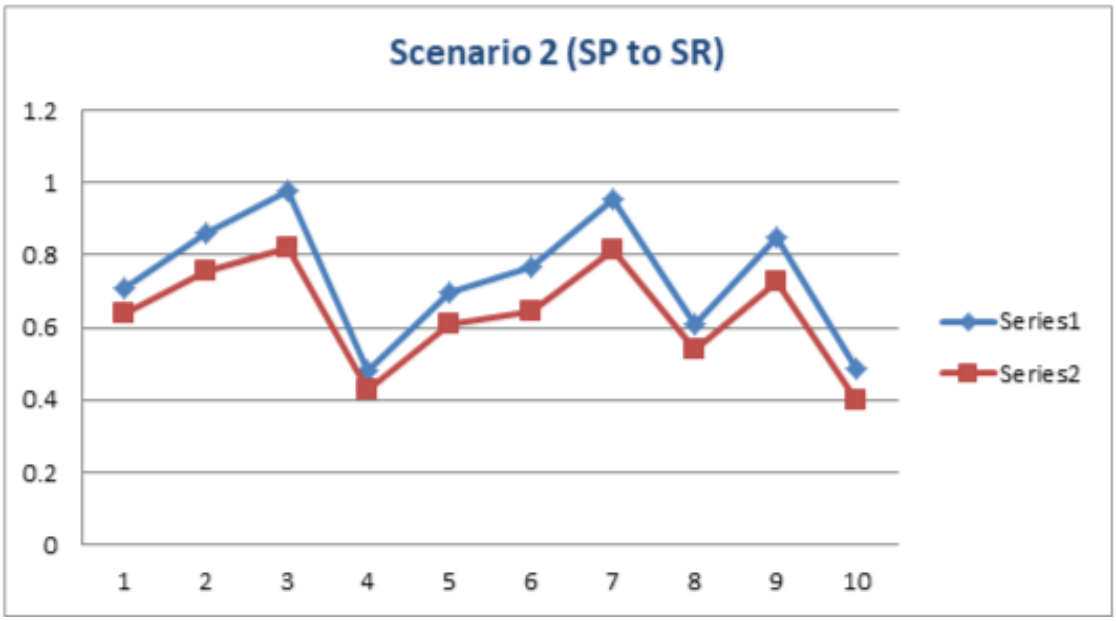

Figure 5. 4: Graphical Representation of Trust values using expert suggestion for scenario 2

5.8 Level of Significance

To measure the significant difference between the means of trust before connection and trust after connection as shown in table 5.7. The value of the Pearson coefficient correlation is 0.8873. The coefficient value shows the relationship between the trust value calculated before the nodes connected in the network and after incorporating the expert suggestions, the trust value is improved, this shows that the suggestions are highly correlated. The degree of freedom is 9 for both the trust values before connected and after being connected. For the application of the t-test in the structural homogeneity of the variance i.e the value of F should be tested. The value of homogeneity is obtained by dividing the larger variance from the smaller variance. The value of the larger variance is 0.00182 for the before-connected trust value and the smaller variance is 0.00112 for the trust value. The ratio of the F value is obtained as 0.89. Therefore, the value of F is less than 1.83 (the critical value of F for 2 variances of a degree of freedom 9), and it can be concluded that the variance is homogeneous. By applying the test to give support for the acceptance of the t-test. The computed value of „t" is 2.26. If the calculated value is increased from the „t" critical value of 1.83 for a one-tailed test at the 0.05 level for 09 degrees of freedom, the null hypothesis H_{01} is highly rejected. While the value of „t" is less, the alternate hypothesis H_{11} is accepted. Therefore, it is validated that the trust management

framework is validated and after the expert suggestion is incorporated trust value of the node can be improved.

Table 5. 7: T-test Level of Significance

T-test for Level of Significance								
Statistical Value **Metric Values**	**Mean**	**Std. deviation**	**Std. error**	**No of samples (N)**	**Pearson Coefficient**	**Degree of Freedom**	**H01**	**t-value**
New Trust	0.6958	0.264	0.034	10	0.485	9	Rejected	2.264
Old Trust	0.6957	0.263	0.032	10				

Any model or framework is acceptable only by the society or industry depending on the validation of the model or the framework. Validation is the process that proves the usefulness of the methodology in society or industry. All the calculations of models are done with the help of MATLAB software. For testing the usefulness of the trust management framework, a systematic validation is performed. Initially, for the purpose the theoretical validation, an expert review was conducted. The framework was evaluated by numerous experts in the area and was found to be satisfactory. As a second step, statistical validation is performed. Statistical validation performs both

pre-tryout and tryout. Pre-tryout applies to a small set of data whereas tryout applies to a large set of data. The pre-tryout is performed on a local adhoc network.

Later, a successful pre-tryout shows the researcher to the next step i.e tryout. The tryout is carried out on ten modules. All the nodes are analyzed and the values before and after are computed. The trust values of nodes before and after have to go through statistical analysis. The complete process shows that the framework has been successfully evaluated. The values for trust value and after trust value have to experience statistical analysis to establish the fact that the framework has successfully estimated the trust and has enhanced it. The t-test is performed and it is found that the t-values obtain by computation performed on the after and before trust nodes exceed the t-critical values. Therefore, the null hypothesis composed at the beginning of the statistical analysis, are rejected one by one and alternate hypotheses are accepted. Researchers declare that the proposed trust management framework can assess the trust and suggestions can improve the performance of the network.

Chapter 6
Conclusion and Future Work

CHAPTER 6: CONCLUSION AND FUTURE WORK

"Trust yourself, you will start to trust others."

-- Santosh Kalwar--

6.1 Background

The Internet of Things has empowered many heterogeneous technologies and communication devices. This paradigm has taken to the notion of everything, anything, and any time to access. These various perceptions and visualization of IoT make things useful for the sociable. The combination of IoT and Social Networks (SNs) extends the concept of the social internet of things (SIoT). Trust management is one of the important networks that can be made up of trustworthy nodes, to make communication will be reliable. SIoT uses a decentralized approach where objects are independent of each other. Trust evaluation is computed based on the behavior of objects.

These objects are controlled by their owners and the various types of relationships with the objects. SIoT can be considered as a collection of these smart objects having social relationships among them with their owners.

6.2 Significance of the Findings

Therefore, a study was carried out to identify to evaluate the trust value of the nodes. This trust value is used to quantify whether the connected node is trustee or un-trustee. The above study helps in identifying the trustee network in reference of service requester to the service provider (SR-SP) or service provider to service requester (SP-SR) which is directly or indirectly significant in terms of the following:

- It may help in the selection of the domain for the trust evaluation.
- It may help to identify the quality of service provided by the node in the SIoT environment.
- The proposed framework may also help to identify the quality of the information provided by the node in the SIoT network.

- It may encourage identifying the trustworthy node.

- It may support identifying the trusty service provider to the service requester.

Further, it is observed that the contribution of this successful proposal may provide to specifically significant in the manner:

- The proposed model may help to provide to classify the trustee and un-trustee nodes.
- The proposed model may be helpful to evaluate the trust value of the node.

- The proposed approach may be used as a measurement tool for trust evaluation of the node in the development of the trustee service providers.

- The proposed approach may encourage other researchers to undertake the development of other new models based on these approaches.

- The proposed approach may be used to set the benchmark value for trust evaluation by the organization.

6.3 Answers to Research Questions

Various research questions may place at the beginning of the research work and are answered separately by the research findings in the following section:

Research Question: What are the factors that directly influence the trustee network?

Research Findings: Quality of service and quality of data directly influence the trust of the network.

Research Question: How to detect whether the connected node is a trustee or an un-trustee?

Research Findings: By using the trust scaling value to detect whether the connected node is trustee or un-trustee.

Research Question: Is there any method or technique to evaluate the trust of the node?

Research Findings: Yes, the researcher has identified the three factors; quality of service, quality of data, and social relationship are the key parameters for evaluation of trust of the node.

Research Question: Is there any standard framework available to evaluate the trust of the node?

Research Findings: There is not any standard framework to evaluate the trust of the node with multiple domains.

Research Question: Is the quality of service metric are used to measure the trustworthiness of the nodes or objects?

Research Findings: Yes, researchers have measured the weight of each domain and identified the quality of service as the key factor to evaluate the quality of service.

Research Question: Can we identify the un-trustee node in the network?

Research Findings: Yes, we can identify the un-trustee node in the network by using the trust score.

Research Question: Is the trust evaluation method applicable for the entire network?

Research Findings: Yes, the researcher has proposed a framework for trust evaluation to measure the trust of the network.

Research Question: Is the quality of service contributes evaluation of trust of the node?

Research Findings: Yes, the quality of service contributes evaluation of trust of the node.

Research Question: Is there any guidelines available for the selection of the node or object to collaborate with the network?

Research Findings: No, there are not any such guidelines for the selection of the node or object to collaborate with the network.

6.4 Future Direction

Research is an ongoing process. Reaching one milestone may promote the way to the next. As a future research plan, there may be the tasks to be performed which are as follows:

- Researchers can plan to conduct more experiments on industry data to draw more accurate trust values.
- The trust evaluation framework for classifying the trustee and un-trustee node may be changed. So that it can help to help to identify easily the un-trustee nodes.
- Researchers can increase the data set, to evaluate the more accurate trust value.
- Researchers can develop a dynamic trust evaluation framework to measure the trust value of the framework.

6.5 Conclusion

The existing approaches for the trust evaluation are quite specific for the domain of the physical object and display less interest in SIoT environment. From the literature review, it is found that there is no model to evaluate the trust of the node with multi-criteria in SIoT environment. Therefore, it is the key issue to investigate the trust evaluation methods when accessing various service requests or services provided to the user. During service requests or services provided, there may be possibilities of threats, attacks by the malicious nodes, or un-trustee nodes. Protecting from these threats, it is also important to review the methodology to enhance the trustworthiness among objects and improve the services. Therefore, the objective of this research is to propose a framework to evaluate the trust of the node in SIoT environment that provide trustworthy services in various applications.

To evaluate the trust in the SIoT environment is finalized, which can be used as a standard value for any system, to avoid any conflict due to the existing definitions of trust. Though, the value of trust is used as the main parameter for decision-making to access the services from the node or to receive the services from the nodes, should be

modeled quantitatively. To overcome this issue, a comprehensive trust evaluation framework is proposed that can be used to measure the trust evaluation on three domains; quality of service, quality of data, and social. These domains represent direct trust while reputation and recommendation are used for indirect trust evaluation. To validate the work opinions collected from the global experts, who had previous experience in this field and incorporate the suggestions to improve the services of the nodes.

References

REFERENCES

[1] W. Abdelghani, C. A. Zayani, I. Amous, and F. S. ` Edes, "Open Archive TOULOUSE Archive Ouverte (OATAO) Trust Management in Social Internet of Things: A Survey," vol. 2016, no. September, 2016, doi: 10.1007/978-3-319-45234-0.

[2] A. I. A. Ahmed, S. H. Ab Hamid, A. Gani, S. khan, and M. K. Khan, "Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges," *Journal of Network and Computer Applications*, vol. 145, Nov. 2019, doi: 10.1016/j.jnca.2019.102409.

[3] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the internet of things (ctm-iot)," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 12, pp. 533–543, 2018, doi: 10.1007/978-3-319-69811-3_48.

[4] M. Amiri-Zarandi and R. A. Dara, "Blockchain-based Trust Management in Social Internet of Things," in *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2020, pp. 49–54. doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00024.

[5] A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, [. MacDermott, and X. Wang, "CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5432–5445, Jun. 2019, doi: 10.1109/JIOT.2019.2902022.

[6] J. Guo, "Trust-based Service Management of Internet of Things Systems and Its Applications," pp. 1–151, 2018.

[7] R. K. Chahal, N. Kumar, and S. Batra, "Trust management in social Internet of Things: A taxonomy, open issues, and challenges," *Computer Communications*, vol. 150, pp. 13–46, Jan. 2020, doi: 10.1016/j.comcom.2019.10.034.

[8] G. Bachi, M. Coscia, A. Monreale, and F. Giannotti, "Classifying trust/distrust relationships in online social networks," in *Proceedings - 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Conference on Social Computing, SocialCom/PASSAT 2012*, 2012, pp. 552–557. doi: 10.1109/SocialCom-PASSAT.2012.115.

[9] F. Bao, I.-R. Chen, and J. Guo, "Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems."

[10] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management."

[11] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Computers and Security*, vol. 39, no. PART B, pp. 351–365, 2013, doi: 10.1016/j.cose.2013.09.001.

[12] B. Jafarian, N. Yazdani, and M. Sayad Haghighi, "Discrimination-aware trust management for social internet of things," *Computer Networks*, vol. 178, p. 107254, 2020, doi: 10.1016/j.comnet.2020.107254.

[13] J. Byun, S. H. Kim, and D. Kim, "Lilliput: Ontology-based platform for IoT social networks: Towards socialized people, objects, and places," in *Proceedings - 2014 IEEE International Conference on Services Computing, SCC 2014*, Oct. 2014, pp. 139–146. doi: 10.1109/SCC.2014.27.

[14] R. N. Chakravartula and N. L. V, "Trust Management Framework for IOT Based P2P Objects," *International Journal of Peer to Peer Networks*, vol. 8, no. 2/3, pp. 17–24, 2017, doi: 10.5121/ijp2p.2017.8302.

[15] E. W. L. Cheng and H. Li, "Construction Partnering Process and Associated Critical Success Factors: Quantitative Investigation," *Journal of Management in Engineering*, vol. 18, no. 4, pp. 194–202, Oct. 2002, doi: 10.1061/(ASCE)0742-597X(2002)18:4(194).

[16] I.-R. Chen, F. Bao, and J. Guo, "Trust-Based Service Management for Social Internet of Things Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 6, pp. 684–696, Nov. 2016, doi: 10.1109/TDSC.2015.2420552.

[17] F. Azzedin and M. Ghaleb, "Internet-of-Things and Information Fusion: Trust Perspective Survey," *Sensors*, vol. 19, no. 8, Art. no. 8, Jan. 2019, doi: 10.3390/s19081929.

[18] A. M. T. Ali-Eldin, "A CLOUD-BASED TRUST COMPUTING MODEL For The SOCIAL INTERNET OF THINGS," 2021, doi: 10.1109/M.

[19] W. KUN, Q. XIN, S. LEI, D. DER-JIUNN, and R. JOEL J. P. C., "Toward Trustworthy Crowdsourcing in the Social Internet of Things," *Ieee Wireless Communications*, no. December, pp. 2–10, 2010.

[20] M. Singh, G. Baranwal, and A. K. Tripathi, "QoS-Aware Selection of IoT-Based Service," *Arab J Sci Eng*, vol. 45, no. 12, pp. 10033–10050, Dec. 2020, doi: 10.1007/s13369-020-04601-8.

[21] A. M. Kowshalya and M. L. Valarmathi, "Trust Management in the Social Internet of Things," *Wireless Pers Commun*, vol. 96, no. 2, pp. 2681–2691, Sep. 2017, doi: 10.1007/s11277-017-4319-8.

[22] P. Ferrari, E. Sisinni, D. Brandão, and M. Rocha, "Evaluation of communication latency in industrial IoT applications," in *2017 IEEE International Workshop on Measurement and Networking (M&N)*, Sep. 2017, pp. 1–6. doi: 10.1109/IWMN.2017.8078359.

[23] L. Atzori, D. Carboni, and A. Iera, "Smart things in the social loop: Paradigms, technologies, and potentials," *Ad Hoc Networks*, vol. 18, pp. 121–132, Jul. 2014, doi: 10.1016/j.adhoc.2013.03.012.

[24] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (SIoT) - When social networks meet the internet of things: Concept, architecture and network characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, 2012, doi: 10.1016/j.comnet.2012.07.010.

[25] H. Xia, Z. Jia, L. Ju, X. Li, and Y. Zhu, "A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules," *Proceedings - 2011 IEEE/ACM International Conference on Green Computing and Communications, GreenCom 2011*, vol. 2, pp. 124–130, 2011, doi: 10.1109/GreenCom.2011.30.

[26] M. N. Ba-hutair, A. Bouguettaya, and A. Ghari Neiat, "Multi-Perspective Trust Management Framework for Crowdsourced IoT Services," *IEEE Transactions on Services Computing*, pp. 1–14, 2021, doi: 10.1109/TSC.2021.3052219.

[27] S. Ruohomaa and L. Kutvonen, "LNCS 3477 - Trust Management Survey." *Online+. Available: http://www.cs.helsinki.fi/group/tube/

[28] S. Sagar, A. Mahmood, J. Kumar, and Q. Z. Sheng, "A Time-Aware Similarity-Based Trust Computational Model for Social Internet of Things," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, Dec. 2020, pp. 1–6. doi: 10.1109/GLOBECOM42002.2020.9322540.

[29] A. Sharma, E. S. Pilli, A. P. Mazumdar, and P. Gera, "Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes," *Computer Communications*, vol. 160, pp. 475–493, Jul. 2020, doi: 10.1016/j.comcom.2020.06.030.

[30] B. Yan, J. Yu, M. Yang, H. Jiang, Z. Wan, and L. Ni, "A novel distributed Social Internet of Things service recommendation scheme based on LSH forest," *Pers Ubiquit Comput*, vol. 25, no. 6, pp. 1013–1026, Dec. 2021, doi: 10.1007/s00779-019-01283-4.

[31] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things," *Computer Science and Information Systems*, vol. 8, no. 4, pp. 1207–1228, 2011, doi: 10.2298/csis110303056c.

[32] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, Nov. 2012, doi: 10.1016/j.comnet.2012.07.010.

[33] P. He and T. Tang, "Community-Oriented Multimedia Content Maximization Mechanism in Social Internet of Things," *IEEE Access*, vol. 8, pp. 22826–22833, 2020, doi: 10.1109/ACCESS.2020.2970453.

[34] H. Xiao, N. Sidhu, and B. Christianson, "Guarantor and reputation based trust model for Social Internet of Things," in *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug. 2015, pp. 600–605. doi: 10.1109/IWCMC.2015.7289151.

[35] R. Chen, F. Bao, and J. Guo, "Trust-based service management for social internet of things systems," *IEEE transactions on dependable and secure computing*, vol. 13, no. 6, pp. 684–696, 2015.

[36] Y. Ruan, A. Durresi, and L. Alfantoukh, "Trust management framework for internet of things," in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, May 2016, vol. 2016-May, pp. 1013–1019. doi: 10.1109/AINA.2016.136.

[37] M. Nitti, L. Atzori, and I. P. Cvijikj, "Friendship Selection in the Social Internet of Things: Challenges and Possible Strategies," *IEEE Internet of Things Journal*, vol. 2, no. 3, pp. 240–247, Jun. 2015, doi: 10.1109/JIOT.2014.2384734.

[38] P. Kasnesis, C. Z. Patrikakis, D. Kogias, L. Toumanidis, and I. S. Venieris, "Cognitive friendship and goal management for the social IoT," *Computers and Electrical Engineering*, vol. 58, pp. 412–428, 2017, doi: 10.1016/j.compeleceng.2016.09.024.

[39] N. B. Truong, H. Lee, B. Askwith, and G. M. Lee, "Toward a Trust Evaluation Mechanism in the Social Internet of Things," *Sensors*, vol. 17, no. 6, Art. no. 6, Jun. 2017, doi: 10.3390/s17061346.

[40] H. Agarwal, F. Husain, and P. Saini, "Advances in Computing and Data Sciences," vol. 1046, no. July, pp. 655–665, 2019, doi: 10.1007/978-981-13-9942-8.

[41] B. Farhadi, A. Masoud Rahmani, P. Asghari, and M. Hosseinzadeh, "Friendship selection and management in social internet of things: A systematic review," *Computer Networks*, vol. 201, Dec. 2021, doi: 10.1016/j.comnet.2021.108568.

[42] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, Nov. 2012, doi: 10.1016/j.comnet.2012.07.010.

[43] S. Rho and Y. Chen, "Social Internet of Things: Applications, architectures and protocols," *Future Generation Computer Systems*, vol. 82, pp. 667–668, 2018, doi: 10.1016/j.future.2018.01.035.

[44] G. Zheng, B. Gong, and Y. Zhang, "Dynamic Network Security Mechanism Based on Trust Management in Wireless Sensor Networks," vol. 2021, 2021.

[45] G. Xiao *et al.*, "Multimodality Sentiment Analysis in Social Internet of Things Based on Hierarchical Attentions and CSAT-TCN With MBM Network," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12748–12757, Aug. 2021, doi: 10.1109/JIOT.2020.3015381.

[46] S. Aljawarneh, M. Maraoui, International Association of Researchers, Institute of Electrical and Electronics Engineers, and University of Monastir, *Proceedings, 2017 International Conference on Engineering & MIS (ICEMIS), (ICEMIS'2017) : University of Monastir, Monastir, Tunisia, 08-10 May, 2017*.

[47] G. Lee, N. B. Truong, and G. M. Lee, "A Reputation and Knowledge Based Trust Service Platform For Trustworthy Social Internet of Things."

[48] A. M. Kowshalya and M. L. Valarmathi, "Trust Management in the Social Internet of Things," *Wireless Personal Communications*, vol. 96, no. 2, pp. 2681–2691, 2017, doi: 10.1007/s11277-017-4319-8.

[49] A. Khanfor, H. Ghazzai, Y. Yang, M. R. Haider, and Y. Massoud, "Automated Service Discovery for Social Internet-of-Things Systems," in *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, Oct. 2020, pp. 1–5. doi: 10.1109/ISCAS45731.2020.9181080.

[50] S. Rajendran and R. Jebakumar, "Friendliness Based Trustworthy Relationship Management (F-TRM) in Social Internet of Things," *Wireless Pers Commun*, vol. 123, no. 3, pp. 2625–2647, Apr. 2022, doi: 10.1007/s11277-021-09256-8.

[51] C. Marche and M. Nitti, "Trust-Related Attacks and Their Detection: A Trust Management Model for the Social IoT," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3297–3308, Sep. 2021, doi: 10.1109/TNSM.2020.3046906.

[52] A. Rehman, A. Paul, and A. Ahmad, "A Query based Information search in an Individual's Small World of Social Internet of Things," *Computer Communications*, vol. 163, pp. 176–185, Nov. 2020, doi: 10.1016/j.comcom.2020.08.027.

[53] C. V. L. Mendoza and J. H. Kleinschmidt, "A Distributed Trust Management Mechanism for the Internet of Things Using a Multi-Service Approach," *Wireless Pers Commun*, vol. 103, no. 3, pp. 2501–2513, Dec. 2018, doi: 10.1007/s11277-018-5942-8.

[54] N. Narang and S. Kar, "A hybrid trust management framework for a multi-service social IoT network," *Computer Communications*, vol. 171, no. June 2020, pp. 61–79, 2021, doi: 10.1016/j.comcom.2021.02.015.

[55] K. A. Awan, I. U. Din, M. Zareei, M. Talha, M. Guizani, and S. U. Jadoon, "HoliTrust-A Holistic Cross-Domain Trust Management Mechanism for Service-Centric Internet of Things," *IEEE Access*, vol. 7, pp. 52191–52201, 2019, doi: 10.1109/ACCESS.2019.2912469.

[56] C. G. E. Boender, J. G. de Graan, and F. A. Lootsma, "Multi-criteria decision analysis with fuzzy pairwise comparisons," *Fuzzy Sets and Systems*, vol. 29, no. 2, pp. 133–143, Jan. 1989, doi: 10.1016/0165-0114(89)90187-5.

[57] J. J. Buckley, "Fuzzy hierarchical analysis," *Fuzzy Sets and Systems*, vol. 17, no. 3, pp. 233–247, Dec. 1985, doi: 10.1016/0165-0114(85)90090-9.

[58] M. Bharti and H. Jindal, "Optimized clustering-based discovery framework on Internet of Things," *J Supercomput*, vol. 77, no. 2, pp. 1739–1778, Feb. 2021, doi: 10.1007/s11227-020-03315-w.

[59] M. Cuka, D. Elmazi, R. Obukata, K. Ozera, T. Oda, and L. Barolli, "An Integrated Intelligent System for IoT Device Selection and Placement in Opportunistic Networks Using Fuzzy Logic and Genetic Algorithm," in *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Mar. 2017, pp. 201–207. doi: 10.1109/WAINA.2017.178.

[60] M. D. Alshehri, F. K. Hussain, and O. K. Hussain, "Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM-IoT)," *Mobile Networks and Applications*, vol. 23, no. 3, pp. 419–431, 2018, doi: 10.1007/s11036-018-1017-z.

[61] S. Talbi and A. Bouabdallah, "Interest-based trust management scheme for social internet of things," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1129–1140, Mar. 2020, doi: 10.1007/s12652-019-01256-8.

[62] D. Dutta, S. Das, and B. K. Tripathy, "Social Internet of Things (SIoT): Transforming smart object to social object Decision making and Interval Valued Intuitionistic Fuzzy Soft Set View project Social Internet of Things (SIoT): Transforming smart object to social object," 2015. *Online+. Available: https://www.researchgate.net/publication/287216756

[63] J. Abed, "A NOVEL FRAMEWORK FOR SOCIAL INTERNET OF THINGS: A NOVEL FRAMEWORK FOR SOCIAL INTERNET OF THINGS: LEVERAGING THE FRIENDSHIPS AND THE SERVICES LEVERAGING THE FRIENDSHIPS AND THE SERVICES EXCHANGED BETWEEN SMART DEVICES EXCHANGED BETWEEN SMART DEVICES Downloaded from Downloaded from." *Online+. Available: https://scholarscompass.vcu.edu/etd

[64] M. Chiregi and N. J. Navimipour, "A comprehensive study of the trust evaluation mechanisms in the cloud computing," *Journal of Service Science Research*, vol. 9, no. 1, pp. 1–30, Jun. 2017, doi: 10.1007/s12927-017-0001-7.

[65] F. Cicirelli *et al.*, "Edge computing and social internet of things for large-scale smart environments development," *IEEE Internet of Things Journal*, vol. 5, no. 4, Nov. 2017, doi: 10.1109/JIOT.2017.2775739.

[66] I. R. Chen, F. Bao, and J. Guo, "Trust-Based Service Management for Social Internet of Things Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 6, pp. 684–696, 2016, doi: 10.1109/TDSC.2015.2420552.

[67] A. M. Kowshalya and M. L. Valarmathi, "Trust Management in the Social Internet of Things," *Wireless Personal Communications*, vol. 96, no. 2, pp. 2681–2691, 2017, doi: 10.1007/s11277-017-4319-8.

[68] Z. Chen, L. Tian, and C. Lin, "Trust evaluation model of cloud user based on behavior data," *International Journal of Distributed Sensor Networks*, vol. 14, no. 5, 2018, doi: 10.1177/1550147718776924.

[69] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain: Analysis, requirements and open issues," *Future Generation Computer Systems*, vol. 100, pp. 325–343, 2019, doi: 10.1016/j.future.2019.05.023.

[70] I. R. Chen, J. Guo, and F. Bao, "Trust Management for SOA-Based IoT and Its Application to Service Composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482–495, 2016, doi: 10.1109/TSC.2014.2365797.

[71] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the internet of things (ctm-iot)," *Lecture Notes on Data Engineering and Communications Technologies*, vol. 12, pp. 533–543, 2018, doi: 10.1007/978-3-319-69811-3_48.

[72] U. Jayasinghe, G. M. Lee, T. W. Um, and Q. Shi, "Machine Learning Based Trust Computational Model for IoT Services," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 1, pp. 39–52, 2019, doi: 10.1109/TSUSC.2018.2839623.

[73] A. Khalil, N. Mbarek, and O. Togni, "Fuzzy logic based security trust evaluation for IoT environments," *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, vol. 2019-November, 2019, doi: 10.1109/AICCSA47632.2019.9035294.

[74] M. N. Ba-hutair, A. Bouguettaya, and A. Ghari Neiat, "Multi-Perspective Trust Management Framework for Crowdsourced IoT Services," *IEEE Transactions on Services Computing*, pp. 1–14, 2021, doi: 10.1109/TSC.2021.3052219.

[75] K. Lingda, Z. Feng, Z. Yingjie, Q. Nan, L. Dashuai, and C. Shaotang, "Evaluation method of trust degree of distribution IoT terminal equipment based on information entropy Evaluation method of trust degree of distribution IoT terminal equipment based on information entropy," 2021, doi: 10.1088/1742-6596/1754/1/012108.

[76] K. Vidyasankar, "A Transaction Model for Executions of Compositions of Internet of Things Services," *Procedia Computer Science*, vol. 83, pp. 195–202, Jan. 2016, doi: 10.1016/j.procs.2016.04.116.

[77] D. Domingos, A. Respício, and R. Martinho, "Reliability of IoT-Aware BPMN Healthcare Processes," *Virtual and Mobile Healthcare: Breakthroughs in Research and Practice*, 2020. https://www.igi-global.com/chapter/reliability-of-iot-aware-bpmn-healthcare-processes/www.igi-global.com/chapter/reliability-of-iot-aware-bpmn-healthcare-processes/235345 (accessed Jul. 05, 2022).

[78] Y. Wang, Y.-C. Lu, I.-R. Chen, J.-H. Cho, A. Swami, and C.-T. Lu, "LogitTrust: A logit regression-based trust model for mobile ad hoc networks," in *6th ASE International Conference on Privacy, Security, Risk and Trust, Boston, MA*, 2014, pp. 1–10.

[79] U. Jayasinghe, "Trust Evaluation in the IoT Environment," 2018.

[80] G. Fortino, L. Fotia, F. Messina, D. Rosaci, and G. M. L. Sarné, "Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges," *IEEE Access*, vol. 8, pp. 60117–60125, 2020, doi: 10.1109/ACCESS.2020.2982318.

[81] T. L. Saaty, "How to Make a Decision: The Analytic Hierarchy Process," *Interfaces*, vol. 24, no. 6, pp. 19–43, Dec. 1994, doi: 10.1287/inte.24.6.19.

[82] L. A. Zadeh, "Fuzzy sets as a basis for a theory of possibility," *Fuzzy Sets and Systems*, vol. 1, no. 1, pp. 3–28, Jan. 1978, doi: 10.1016/0165-0114(78)90029-5.

[83] H. Deng, "Multicriteria analysis with fuzzy pairwise comparison," *International Journal of Approximate Reasoning*, vol. 21, no. 3, pp. 215–231, Aug. 1999, doi: 10.1016/S0888-613X(99)00025-0.

[84] T. R. Ayodele, A. S. O. Ogunjuyigbe, O. Odigie, and J. L. Munda, "A multi-criteria GIS based model for wind farm site selection using interval type-2 fuzzy analytic hierarchy process: The case study of Nigeria," *Applied Energy*, vol. 228, pp. 1853–1869, Oct. 2018, doi: 10.1016/j.apenergy.2018.07.051.

[85] M. Rajak and K. Shaw, "Evaluation and selection of mobile health (mHealth) applications using AHP and fuzzy TOPSIS," *Technology in Society*, vol. 59, p. 101186, Nov. 2019, doi: 10.1016/j.techsoc.2019.101186.

[86] S. O. Ogundoyin and I. A. Kamil, "A Fuzzy-AHP based prioritization of trust criteria in fog computing services," *Applied Soft Computing*, vol. 97, p. 106789, Dec. 2020, doi: 10.1016/j.asoc.2020.106789.

[87] W. Z. Khan, Q. U. A. Arshad, S. Hakak, M. K. Khan, and Saeed-Ur-Rehman, "Trust Management in Social Internet of Things: Architectures, Recent Advancements, and Future Challenges," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7768–7788, May 2021, doi: 10.1109/JIOT.2020.3039296.

[88] E. Alemneh, S.-M. Senouci, P. Brunet, and T. Tegegne, "A two-way trust management system for fog computing," *Future Generation Computer Systems*, vol. 106, pp. 206–220, May 2020, doi: 10.1016/j.future.2019.12.045.

[89] S. Sagar, A. Mahmood, Q. Z. Sheng, J. K. Pabani, and W. E. Zhang, "Understanding the Trustworthiness Management in the Social Internet of Things: A Survey," pp. 1–29, 2022, [Online]. Available: http://arxiv.org/abs/2202.03624

[90] S. Adali *et al.*, "Measuring behavioral trust in social networks," in *2010 IEEE International Conference on Intelligence and Security Informatics*, May 2010, pp. 150–152. doi: 10.1109/ISI.2010.5484757.

[91] J. R. Figueira, S. Greco, B. Roy, and R. Słowiński, "An Overview of ELECTRE Methods and their Recent Extensions," *Journal of Multi-Criteria Decision Analysis*, vol. 20, no. 1–2, pp. 61–85, 2013, doi: 10.1002/mcda.1482.

[92] M. M. Tahernejad, M. Ataei, and R. Khalokakaie, "Selection of the best strategy for Iran's quarries: SWOT-FAHP method," *Journal of Mining and Environment*, vol. 3, no. 1, pp. 1–13, Sep. 2012, doi: 10.22044/jme.2012.71.

[93] C. Kahraman, U. Cebeci, and D. Ruan, "Multi-attribute comparison of catering service companies using fuzzy AHP: The case of Turkey," *International Journal of Production Economics*, vol. 87, no. 2, pp. 171–184, Jan. 2004, doi: 10.1016/S0925-5273(03)00099-9.

[94] J. K. W. Wong and H. Li, "Application of the analytic hierarchy process (AHP) in multi-criteria analysis of the selection of intelligent building systems," *Building and Environment*, vol. 43, no. 1, pp. 108–125, Jan. 2008, doi: 10.1016/j.buildenv.2006.11.019.

[95] F. Amin, R. Abbasi, A. Rehman, and G. S. Choi, "An Advanced Algorithm for Higher Network Navigation in Social Internet of Things Using Small-World Networks," *Sensors*, vol. 19, no. 9, Art. no. 9, Jan. 2019, doi: 10.3390/s19092007.

[96] R. Casadei, G. Fortino, D. Pianini, W. Russo, C. Savaglio, and M. Viroli, "Modelling and simulation of Opportunistic IoT Services with Aggregate Computing," *Future Generation Computer Systems*, vol. 91, pp. 252–262, Feb. 2019, doi: 10.1016/j.future.2018.09.005.

[97] K. C. Chung and S. W.-J. Liang, "An Empirical Study of Social Network Activities via Social Internet of Things (SIoT)," *IEEE Access*, vol. 8, pp. 48652–48659, 2020, doi: 10.1109/ACCESS.2020.2978151.

[98] G. Xu *et al.*, "TT-SVD: An Efficient Sparse Decision-Making Model With Two-Way Trust Recommendation in the AI-Enabled IoT Systems," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9559–9567, Jun. 2021, doi: 10.1109/JIOT.2020.3006066.

[99] D.-Y. Chang, "Applications of the extent analysis method on fuzzy AHP," *European Journal of Operational Research*, vol. 95, no. 3, pp. 649–655, Dec. 1996, doi: 10.1016/0377-2217(95)00300-2.

[100] P. B. Velloso, R. P. Laufer, D. de O. Cunha, O. C. M. B. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Transactions on Network and Service Management*, vol. 7, no. 3, pp. 172–185, Sep. 2010, doi: 10.1109/TNSM.2010.1009.I9P0339.

[101] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Computers & Security*, vol. 39, pp. 351–365, Nov. 2013, doi: 10.1016/j.cose.2013.09.001.

[102] J. Byabazaire, G. O'Hare, and D. Delaney, "Data Quality and Trust : A Perception from Shared Data in IoT," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, Jun. 2020, pp. 1–6. doi: 10.1109/ICCWorkshops49005.2020.9145071.

[103] M. B. Javanbarg, C. Scawthorn, J. Kiyono, and B. Shahbodaghkhan, "Fuzzy AHP-based multicriteria decision making systems using particle swarm optimization," *Expert systems with applications*, vol. 39, no. 1, pp. 960–966, 2012.

[104] G. Lizet, W. JingpeP, and S. Bin, "Trust Management Mechanism for Internet of Things."

[105] I. Ud Din, M. Guizani, B. S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the internet of things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2019, doi: 10.1109/ACCESS.2018.2880838.

[106] L. Wei, J. Wu, C. Long, and B. Li, "On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4775–4787, Mar. 2021, doi: 10.1109/JIOT.2020.3028380.

APPENDIX A

COMPILED COMMENTS FROM RESPONDENTS

"…This work proposes a quantitative methodology for computing trust among social object in SIoT environment by utilizing social relationship. The depict two scenario (SR to SP and SP to SR).The collaboration of social object required any specific kind of social relation. The practicality of the proposal needs to be justified with real-world with large dataset cases. It seems that the author utilizes weights to to computes trust in terms of SR to SP and SP to SR ……..*Prof. Kasnesis Ambel < Kasnesis @termido.edu>*
"……..The AHP was a known algorithm; no improvement of the algorithm was done. Another dimension depict about and process/method performed well . the result need to be more explained throughly. …..…….." Dr. Cuka Garnek, < Garnek_cuka@NMFU.edu.sa>
"……This work is blend of fuzzy AHP and concept of trust. Such combination is good part of contribution in research field of SIoT.But this work signifies certain factors level effect trust, on the other hand role of social relation regarding computation need to focused.The mechanism of trust evaluation having trust adjusting factor alpha, beta, gama with value 0.6,0.3 and 0.8 bright part of the work ……..." *Prof.Maniish Pandey, <@srms.edu.ac.in>*

Details and Description: Due to the heavy cost incurred on trust evaluation since quality of service and quality of data in large amount are basic demand of each client user. This property of SIoT makes it more trustworthy while accessing services. During computation of trust various effective metric are required to compute the weight of each trust metric. To help developers, the researcher has proposed a methodology to evaluate the trust of social object in two scenarios (SR to SP and SP to SR).

The methodology is based upon Multi Criteria Decision Analysis Methods. Your suggestions will surely help to improve the methodology. So you are requested to kindly give your pinion for the given set of questionnaire. The scale for answers has been given in the table X. The responses are to be given in numeric form.

Table 1: Fuzzy scale of relative importance of Trust

Linguistic Value	TFN	TFN Reciprocal	Trust Value
Not Trusty	(1,1,1)	(1,1,1)	0.0
Very Less Trusty	(0.5,1,1.5)	(0.6,1,2)	0.2
Less Trusty	(1,1.5,2)	(0.5,0.6,1)	0.4
Strongly Trusty	(1.5,2,2.5)	(0.4,0.5,0.6)	0.6
Very Strongly Trusty	(2,2.5,3)	(0.3,0.4,0.5)	0.8
Absolute Trusty	(2.5,3,3.5)	(0.2,0.3,0.4)	1.0

Please read the following questions and put check marks on the pair wise comparison matrices. If criteria on the left is trusty than the matching one on the right, put your check mark to the left of the trusty „not trusty"" under the importance level you prefer. If a criteria on the left is less important than the matching one on the right, put your check mark to the right of the trusty „not trusty" under the trust level you. Reciprocal value means the opposite effect of the factor of assigned value. Here, total 5 groups are available. Please put your mark for each group. Here, total 5 groups are available. Please put your mark for each group.

A. With respect to weight vector to compute trust in SR to SP (Scenario 1)

(1) How much trusty is quality of service (M1) compared with quality of Data (M2)?

(2) How much trusty is quality of service (M1) compared with past reputation (M4)?

(3) How important is quality of service (M1) compared with recommendations (M5)?

(4) How important is quality of Data (M2) compared with M4?

(5) How much trusty is quality of QoD compared M5?

(6) How much trusty is past reputation compared with M5?

Ques No.	Trust factors	Not Trusty	Very Less Trusty	Less Trusty	Strongly Trusty	Very Strongly Trusty	Absolute Trusty	Trust factors
1	M1							M2
2	M1							M4
3	M1							M5
4	M2							M4
5	M2							M5
6	M4							M5

B. With respect to weight vector to compute trust in SP to SR (Scenario 2)

(1) How much trusty is Social relationships (M3) compared with M4?

(2) How much trusty is M3 compared with past M5?

(3) How much trusty is Past reputation compared with M5?

Ques No.	**Trust factors**	**Not Trusty**	**Very Less Trusty**	**Less Trusty**	**Strongly Trusty**	**Very Strongly Trusty**	**Absolute Trusty**	**Trust factors**
1	M3							M4
2	M3							M5
3	M4							M5

C. With respect to weight vector (QoS- Sub Metrics)

1) How much trusty is Transaction time (SM1) compared with quality of latency (SM2)?
2) How much trusty is Transaction time (SM1) compared with quality of scalability (SM3)?
3) How much trusty is Transaction time (SM1) compared with quality of Reliability (SM4)?
4) How much trusty is quality of latency (SM2) compared with scalability (SM3)?
5) How much trusty is quality of latency (SM2) compared with of Reliability (SM4)?
6) How much trusty is scalability (SM3)? Compared with of Reliability (SM4)?

Ques No.	**Trust factors**	**Not Trusty**	**Very Less Trusty**	**Less Trusty**	**Strongly Trusty**	**Very Strongly Trusty**	**Absolute Trusty**	**Trust factors**
1	SM1							SM2
2	SM1							SM3
3	SM1							SM4
4	SM2							SM3
5	SM2							SM4
6	SM3							SM4

D. With respect to weight vector (QoD- Sub Metrics)

1) How much trusty is Intrinsic (SM5) compared with quality of Accessibility (SM6)?
2) How much trusty is Intrinsic (SM5) compared with quality of contextual (SM7)?
3) How much trusty is Intrinsic (SM5) compared with quality of Representational (SM8)?
4) How much trusty is Accessibility (SM6) compared with contextual (SM7)?
5) How much trusty is Accessibility (SM6) compared with of Representational (SM8)?
6) How much trusty is contextual (SM7)? Compared with of Representational (SM4)?

Ques No.	**Trust factors**	**Not Trusty**	**Very Less Trusty**	**Less Trusty**	**Strongly Trusty**	**Very Strongly Trusty**	**Absolute Trusty**	**Trust factors**
1	SM5							SM6
2	SM5							SM7
3	SM5							SM8
4	SM6							SM7
5	SM6							SM8
6	SM7							SM8

E. With respect to weight vector (Social Relationship)

1) How much trusty is Honesty (SM9) compared with cooperativeness (SM10)?
2) How much trusty is Honesty (SM9) compared with Community of Interest (SM11)?
3) How much trusty is Honesty (SM9) compared with Centrality (SM12)?
4) How much trusty is quality of cooperativeness (SM10) compared with Community of Interest (SM11)?
5) How much trusty is quality of cooperativeness (SM10) compared with of Centrality (SM12)?
6) How much trusty is scalability (SM11) compared with of Centrality (SM12)?

Ques No.	**Trust factors**	**Not Trusty**	**Very Less Trusty**	**Less Trusty**	**Strongly Trusty**	**Very Strongly Trusty**	**Absolute Trusty**	**Trust factors**
1	SM1							SM2
2	SM1							SM3
3	SM1							SM4
4	SM2							SM3
5	SM2							SM4
6	SM3							SM4

Your Comments (Please mark corrections as and where required): Please find details in E-Mail:

Expert‟s Name and Signature:
(Please return this to: Sunil Singh (8cts.sunil@gmail.com), D/O Information Technology,
SIST, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India)

LIST OF PUBLICATIONS

1) Singh, Sunil, Pawan K. Chaurasia. "A Review on Trust Management in the Social Internet of Things: Issues and Challenges." ***Technix International Journal for Engineering Research***".9.6 (2022): 1-8.
2) Singh, Sunil, Pawan K. Chaurasia." A Review of Trust Management Techniques in the Internet of Things (IoT). "***International Journalof Research and Analytical Reviews (IJRAR)****." 2022,*volume 9,Issue 3,
3) Singh, S., Chuarasia, P.K.,Upadhyay,S.P,. "Friend Selection in Social Internet of Things: A Novel Approach", ***In International Conference on Advances in Data Science Challenges with Big Data Analysis (ICADSC2022)****,* February 16 -17, 2022.
4) Singh, S., Chuarasia, P.K.,Upadhyay,S.P, Trust Management in Social Internet of Things: A Road Map., ***In International Conference on Smart Computing Technologies and Business Management Strategies (ICCTBM 2022),***Feb, 2022.
5) Singh, S., Yadav, N. and Chuarasia, P.K., 2020, July. A Review on Cyber Physical System Attacks: Issues and Challenges. In 2020 ***International Conference on Communication and Signal Processing (ICCSP)*** (pp. 1133-1138). IEEE.
6) Singh, S., Chuarasia, P.K.,Upadhyay,S.P, Future Challenges of Trust Management in the Social Internet of Things:A Survey, ***In 45 Indian Social Science congress****,* S09145, March , 2022.
7) Singh, S., Yadav, N. and Chuarasia ,A Comprehensive Study of Trust Management: Internet of Things (IoT) in Edited Book "***Emerging Trends in Information Technology***" published by Sapatrishi Publishers, ,Chandigarh, ETIT06, June 10, 2022
8) Singh, Sunil, Pawan K. Chaurasia. "Critical Review of Truthful friend Selection in Social Internet of Things". ***Harbin Gongye Daxue Xuebao/ Journal of Harbin Institute of Technology***. **(ACCEPTED)**
9) Singh, Sunil, Pawan K. Chaurasia, ***A Rule-Based Ranking of Trust Metrics in the social Internet of Things (Communicated)***

Document Information

Analyzed document	Merge Chapter.docx (D142701830)
Submitted	8/6/2022 2:01:00 PM
Submitted by	O. P. Saini
Submitter email	gbl.bbau@gmail.com
Similarity	1%
Analysis address	gbl.bbau.bbau@analysis.urkund.com

Sources included in the report

W	URL: https://vtechworks.lib.vt.edu/bitstream/handle/10919/82854/Guo_J_D_2018.pdf?sequence=1Jafarian, **10** Fetched: 8/6/2022 2:01:00 PM	
W	URL: https://link.springer.com/chapter/10.1007/978-3-319-45234-0_39 Fetched: 11/6/2020 10:33:34 AM	6
W	URL: https://link.springer.com/article/10.1007/s00500-019-04319-2 Fetched: 11/5/2021 9:23:15 AM	1

Entire Document

CHAPTER 1: INTRODUCTION
CHAPTER 1: INTRODUCTION
“If we do not trust one another, we are already defeated.” -- Alison Croggon --
1.1 Background From last two decades, the trends of IoT have changed and enchanted a great deal of research. Scientists and researchers developed various smart devices, where a large number of distinct types of objects are connected to resolve the critical problems. Data generates from various IoT device activities like information sharing, trust of nodes, security management, and privacy. These devices produced a huge data in different formats that can collect, integrate, treated, and analyzed to extract useful information. All these data are generated from heterogeneous devices and decentralized network environments (Atzori et al., 2012). Objectives of the IoT enabled devices are the high impact on the behavior and activities of the owners. Involvement of these IoT devices with the society, change the nature and activities of the human beings. To resolve some of the social issues, a new paradigm was involved, known as the Social Internet of Things (SIoT). Sample of data has represented the notion of everything, anything to access (Atzori, Luigi, Antonio Iera, 2011). The notion of representation of data in various formats, change of time, social networks change the behavior and activity of IoT devices. The sensitivity of visual devices, make things more sociable. It means, IoT gives a social development and implement novel relationships between the social and objects as shown in figure 1.1. The combination of IoT and Social Networks (SN) leads to the SIoT, known as the Social Networks (SNs) of intelligent objects (Bao & Chen, 2012). The domains of the IoT environment expanded the novel integration. The domains of a social network within the current IoT models, reproduce additional novel frameworks for the modern society (Malekshahi Rad et al., 2020).
Figure 1. 1: Notion of Social Internet of Things