TRUST EVALUATION IN SIoT ENVIRONMENT

A Summary 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

SUMMARY

1. INTRODUCTION

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.

From last two decades, there are drastic changes in the usage of IoT devices. Billions of people connected with the 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. The first idea of socialism of objects was introduced by Holymquist et. al. Billions of IoT devices developed and connected with the internet.

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. The construction of social structure so formed has a social relationship fetter which turns a smart object into a social object.

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. 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). 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.

2. RELEVANT ISSUES

Various researcher has analyzed that due to specific rules and regulations set by the owner of devices and frequently changing behavior (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. 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?

3. 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"

4. OBJECTIVES OF THE RESEARCH

The intention of the investigation is 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, proposed a trust evaluation framework 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 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.

5. 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.

6. RELEVANT FINDINGS

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

- After thorough study on trust evaluation models has been done of one decade.
- Existing trust evaluation and social relationship metrics has been reviewed exhaustively of last ten years

- Existing approaches of trust evaluation is based on quality of service, recommendation or reputation parameters. Most of the researchers used a single domain to measure the 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 the society, then social internet of things based devices are involved in the society.
- On the basis of literature review it is found that, during sharing the information and avail the services from the 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 trust evaluation mechanism. Therefore the gap needs to be focused.

7. PROPOSED FRAMEWORK

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 proposed framework for trust evaluation comprises five phases as shown in figure 1 which are as follows:

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

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.

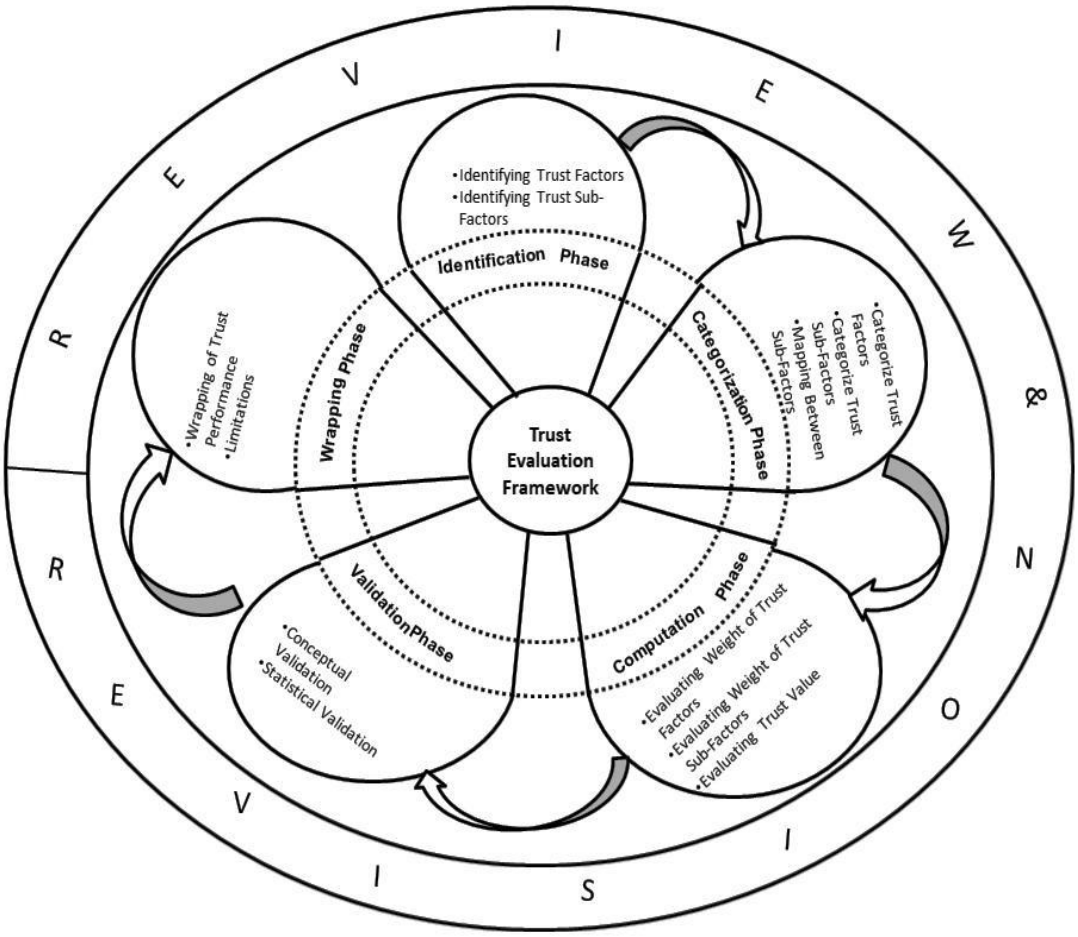

Figure 1: Trust Evaluation Framework

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.

8. 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.

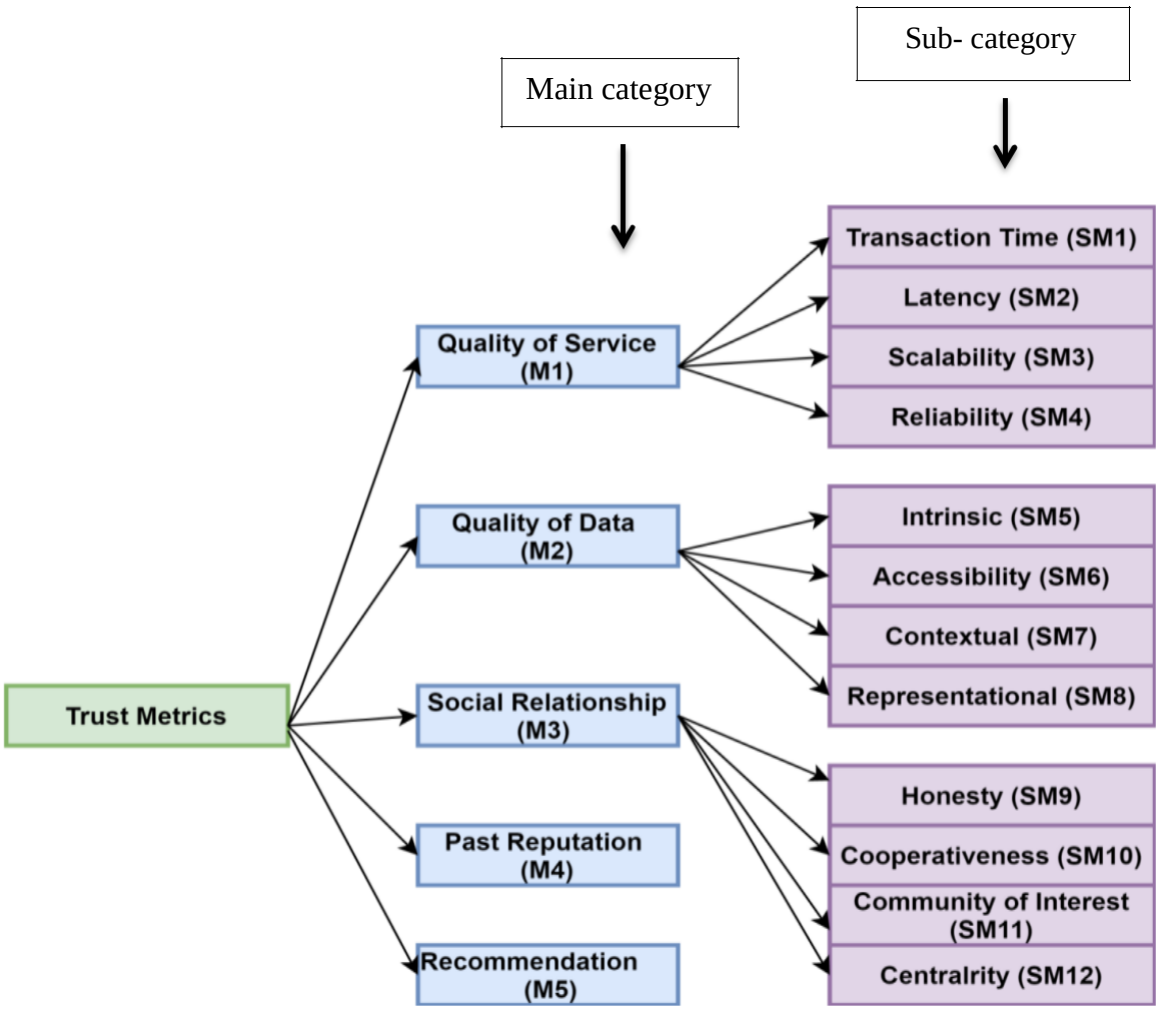

Figure 3. 2: Categorization of Trust Factors and Sub-Factors

Figure 3.2 shows the hierarchy based classification of trust factors and its sub factors which categorize into two levels. The main category and sub-category depict different factors association, the trust factors and trust sub-factors is shown in terms of the 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.

9. TRUST EVALUATION MECHANISM USING FUZZY AHP

Trust is most promising caharacteristic of among social objects which is related to service providers and service requester. 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.

FUZZY AHP MECHANISM

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).

() [ ] ()

N( ) { (2)

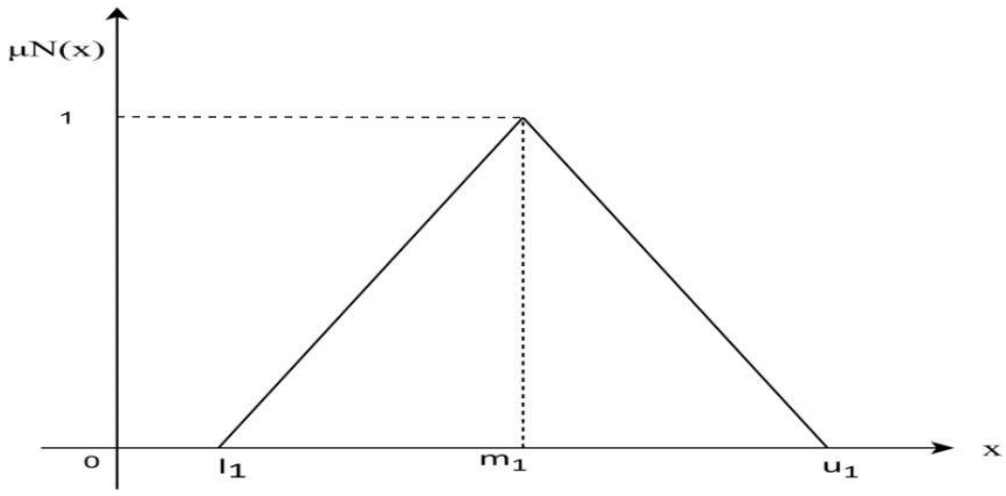

Figure 3. 3: Triangular Fuzzy numbers

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. 1 : ∑_(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 sum of all T_{ij} by performing by performing fuzzy addition operation using equation 13.

Table 4. 2 : 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

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

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

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

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

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

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

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

= 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

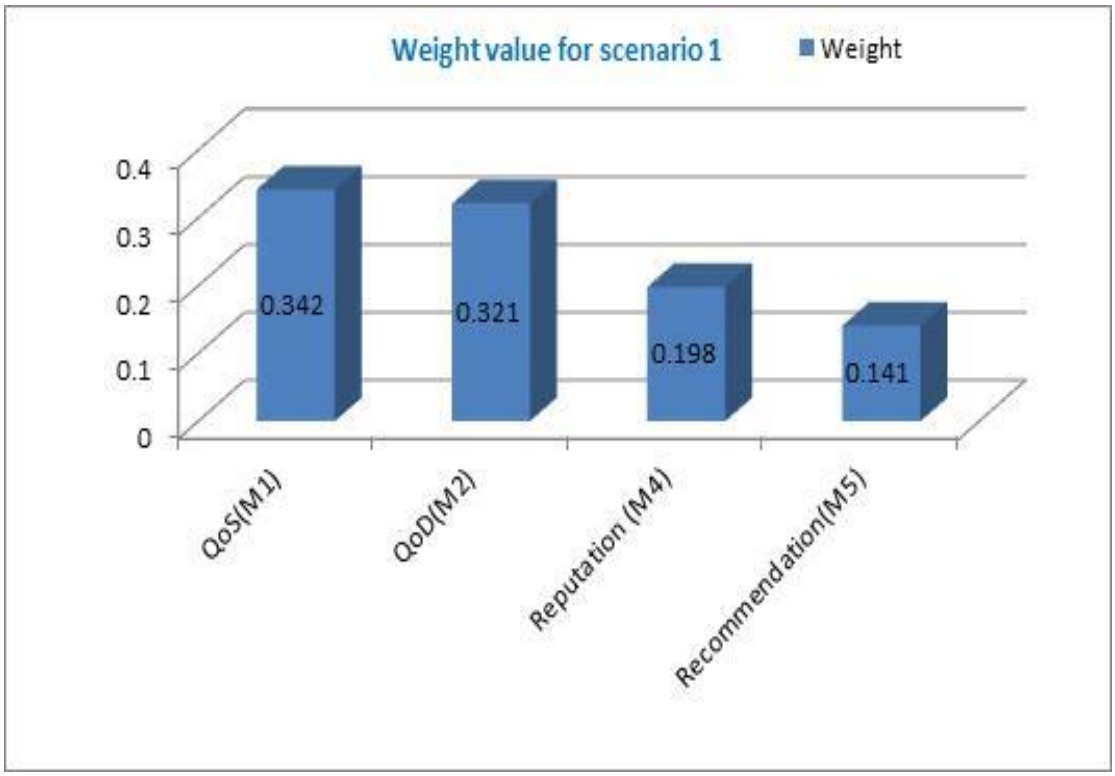

Figure 4. 1 : Graphical Representation of Weight obtained in scenario 1

Figure 4.1 shows the prioritize weights of QoS, QoD, Reputation and recommendation. The most prioritize factor is QoS among. The QoS and QoD are shows 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. 3 : 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. 4 : 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. 5 : 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 as using equation 11.

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

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. 6 : Eigen on trust metrics for scenario 2

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

Table 4. 7 : 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 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

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

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

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

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

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

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

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

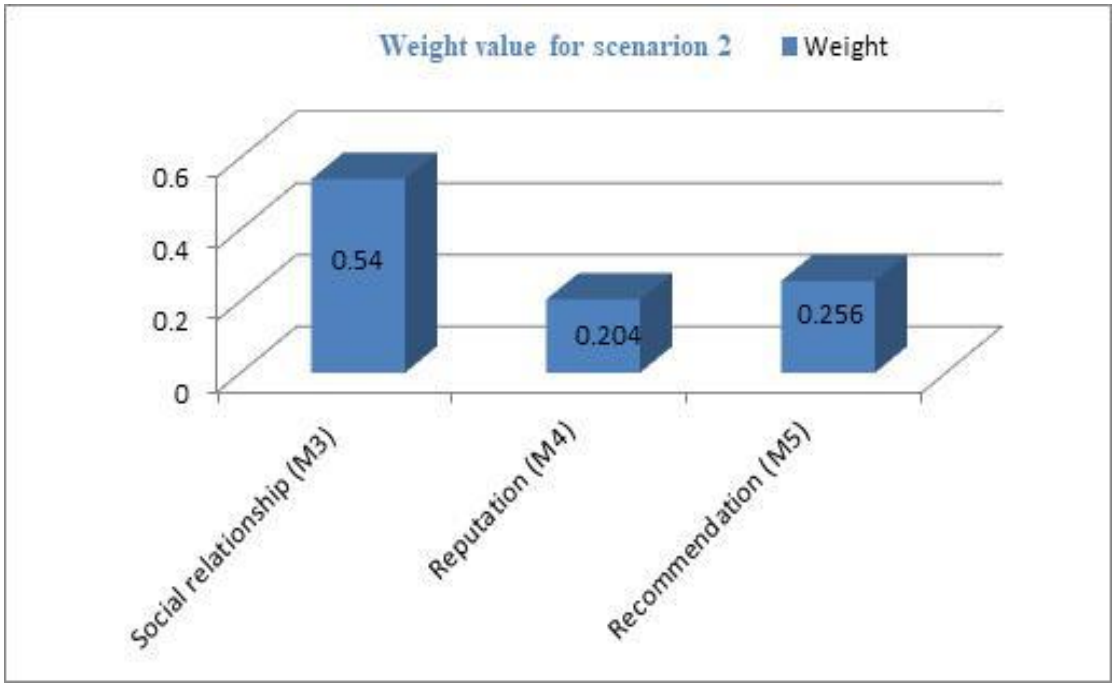

Figure 4. 2 : Graphical Representation of Weight obtained in scenario 2

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

10. ESTIMATING WEIGHTS OF SUB-ATTRIBUTES USING FUZZY METHOD

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

Table 4. 8 : 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

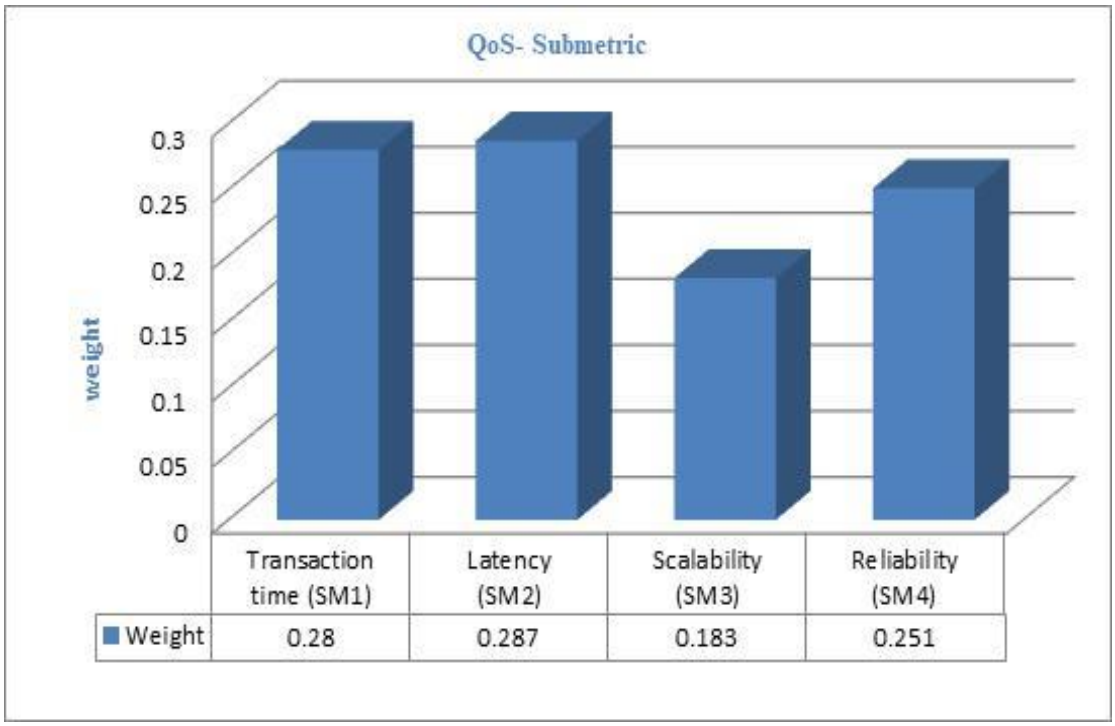

Figure 4. 3 : Graphical Representation of Weight obtained QoS- Sub-metric

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

Table 4. 9 : 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

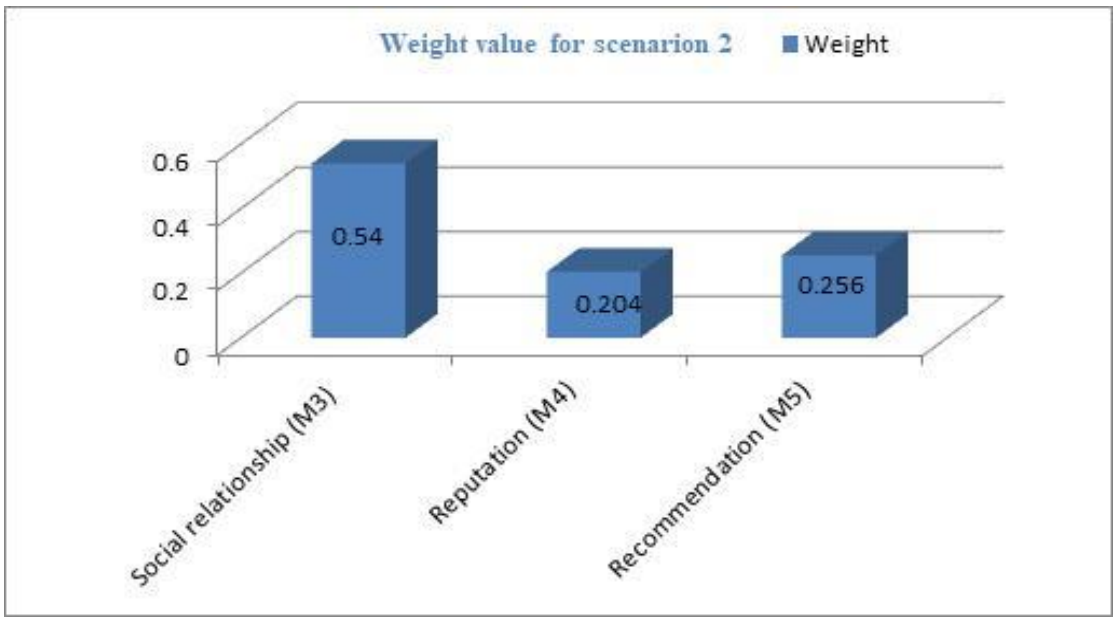

Figure 4. 4 : Graphical Representation of Weight obtained-QoD sub-metric

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

Table 4. 10 : 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

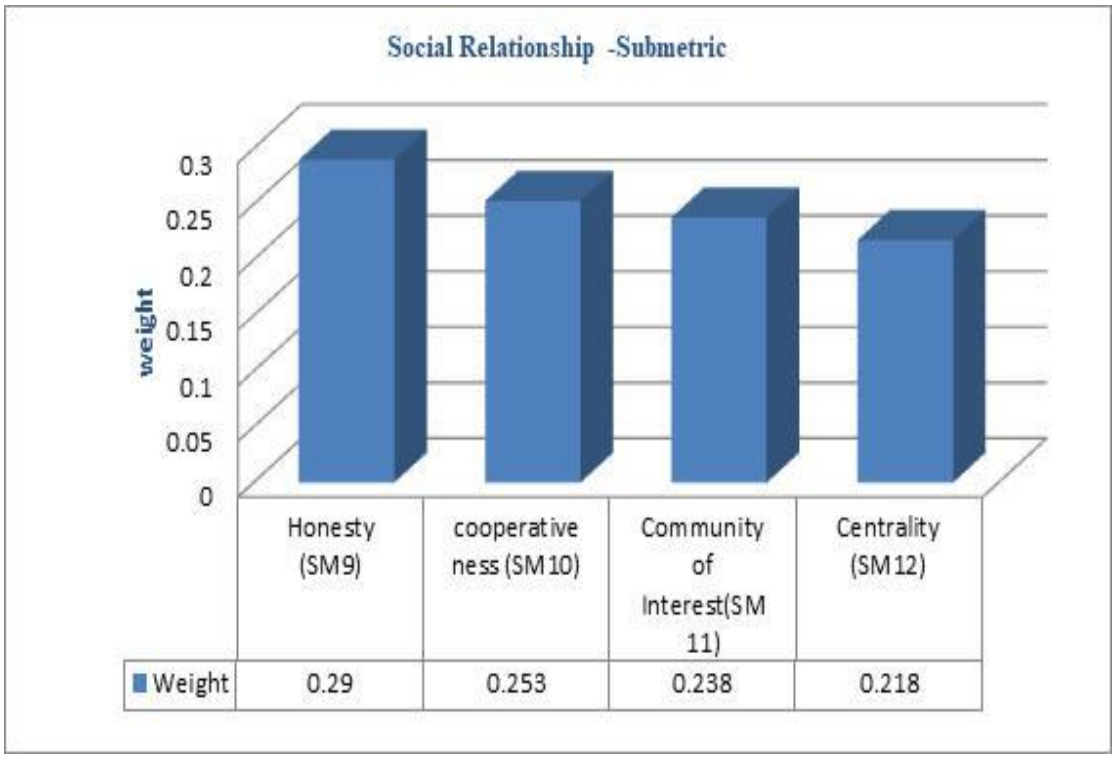

Figure 4. 5 : Graphical Representation of Weight obtained- Social relationship-sub-metric

Figure depicts the weight obtained by social relations sub parameter where honesty is most priotize one while centrality is at least position**.**

11. 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 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. 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. 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. On the basis of the result depicted in figure, latency is the top graded metric locally and it is the rated higher metric globally and achieving the third rank overall.

Table 4. 11 : 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

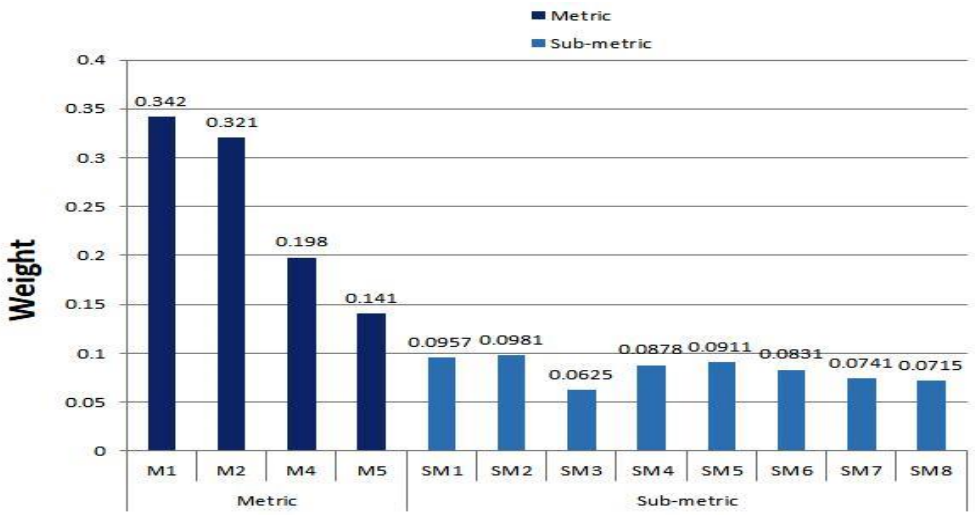

Figure 4. 6 : Ranking of Metric for scenario 1

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. 12 : 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

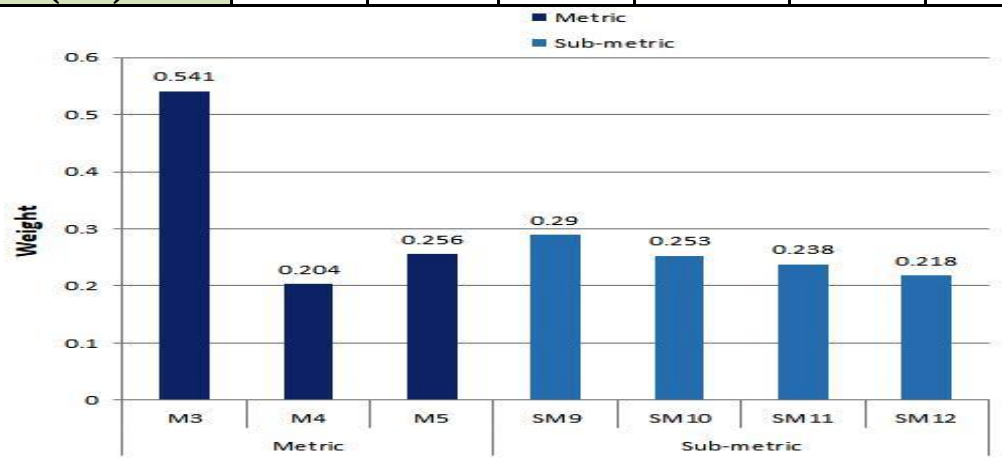

Figure 4. 7 : Ranking of Metric for scenario 2

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. Since recommendation and reputation do not have further factors, therefore these are top graded in GW where recommendation gained the highest rank.

The table 4.6.1 shows the comparison trust value obtain in both the scenario 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 the scenario by changing the trust adjusting factor to maintain the trust value.

Table 4. 13 : Depicts trust value of 10 nodes obtained from local adhoc 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%

12. 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.

HYPOTHESIS TESTING

Hypothesis is used to conduct a quantitative research to make an effort for answer a research questions. Null hypothesis consider that there is no significant difference between two or more variables. However, the alternate hypothesis, reject the relationship. Therefore, rejection of hypothesis provides a stronger base to accept the alternate hypothesis. Hence, the presented hypotheses were used for validation of the proposed framework which are 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 is a significant difference between trusty and un-trusty nodes in the SIoT environment.

LEVEL OF SIGNIFICANCE

To measure the significance difference between the means of trust before connection and trust after connection as shown in table . Value of 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 incorporate 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 connected. For application of the t-test in the structure homogeneity of the variance i.e the value of F should be tested. The value of homogeneity is obtained from by dividing the larger variance from the smaller variance. The value of larger variance is 0.00182 for before connected trust value and the smaller variance is 0.00112 of 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 variance of degree of freedom 9), it can be concluded that the variance are homogeneous.

Table 5. 1: 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				

13. 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.

14. 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.

15. 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.

16. 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: Present approaches

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 one 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: Framework Implementation

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 has 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.