A Review on Trust Management in the Social Internet of Things: Issues and Challenges

Pawan K. Chaurasia[#], Sunil K Singh[*], Manohar Lal[*]

[#] Department of IT, BBAU, Lucknow, India
[*]Department of IT, BBAU, Lucknow, India
[#]IGNOU, New Delhi
[1] pkc.gkp@gmail.com
[2] 8cts.sunil@gmail.com
[2] prof.manohar.lal@gmail.com

Abstract— *In today's era, every electrical and electronic device is connected very intelligently. These electronic devices like sensors, RFIDs, actuators are becoming an important part of the structure. It is required to connect to the internet. Internet is used in every aspect of daily life. There are drastic changes in the usage of the most demanding and useful technology known as the Internet of Things (IoT). In this field, IoT has been shown one of the important which connect various physical objects with the internet with unique identification. Billions of objects are enabled with the internet and interconnected with each other to interface with Human-to-Machine or Machine-to-Machine to take decisions of data transaction without human involvement.*

This internet enables devices connected to our social life which is terme as Social Internet of Things (SIoT). Hence we can say SIoT is an expansion IoT. People and things are connected with social networks which are known as Human to Things (H2T) interactions. Some of the devices are authentic and some are suspicious. The essential utilization of services within SIoT makes a secured network closely rely on origin of services (Service provider) and services accesed by end terminal (Service requester). Due to a lack of trust technologies, trust SIoT is still not so much popular in the market as demanding technology for the researcher and developer. Device owners are worried about sharing the data or receiving any information. Therefore, trust devices are required to identify in the connected network..Hence minimization of risk and uncertaintity within the system are analyse by the degree of trust for Particular Trust Management System(TMS).

Trust and Trustworthiness are novel fields in social networking environment clearlify by investigating the research article under SIoT. In present paper, our contribution starts with the introduction and then is further fragmented in three phases.The first phase represent the basic of trust and SIoT. Second phase categorizes the trust management solutions from the literature review. The third phase identifies and discusse isssues,challenges and requirement in current scenario of SIoT and also depicts how developing trus and trustworthiness among social devices interaction as challenging task.

Keywords— *Trust Attacks, Trust Management, Internet of Things, Social Internet of Thigs (SIoT)and Social Objects*

I. INTRODUCTION

The recent last two decades, there is drastic changes in the usage of the most demanding and useful technology called as Internet of Things (IoT). Today communities are contionously developed within heterogeneous environment based on common interest, needs, as well as advantages from social relationships. An alternate architecture model is required for the Internet of Things which are loosely coupled and decentralized of smart objects to enhance the sensing, processing, and network capacities [1]. The first idea of socialism of objects was introduced by *Holmquist et. al. in 2001* [2]. Billions of objects enabled with the internet and interconnected with each other to interface with human-to-machine or machine-to-machine to take decisions of data transaction and data transmission without human intervention. These IoT devices describe new world items of heterogeneous objects like sensors, smartwatches, and servo motors where everything has its own identity and independent from other objects [3][4][4]. These IoT devices have distinct features, but at the time of connection, all these parameters are ignored during interface having each other. These IoT devices are used to evolve to solve day-to-day activities. During this process, various protocols (like TCP/IP, SLS, etc.) are followed for data transmission [5].

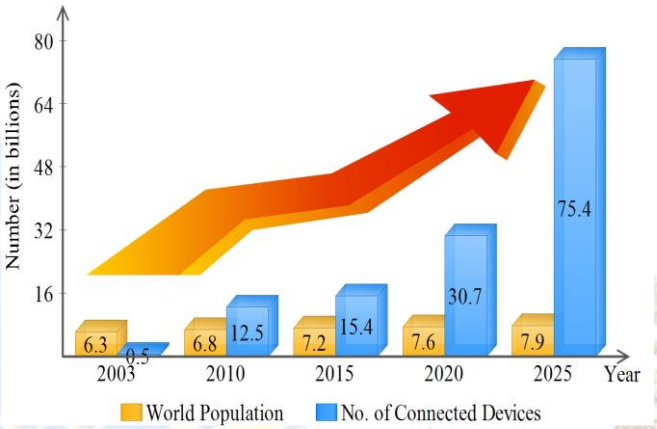


Figure 1: Population and connected devices

The various smart object connecting with internet increased at an exponential rate in day-to-day life. These smart devices are used to consider some relationships. Such smart object performing as social object act as independent object. Therefore, each object is required to communicate its surrounding objects to meet the user requirement. These SOs are controlled by specific social relation ship so formed and rules set by owner of devices [1]. The SIoT environment are collective measures of smart object and social relationship between them[6]. As shown in figure 1, no of populations connected with the connected objects are represented.

In our dynamic and complex life, the role of these internet-enabled objects is to solve social relationships based on common interests and influential needs. To solve complex problems, human interacts with the communities and collaborate with the members of the society. The concept of social network is integrated with IoT, a new paradigm is introduced defined as SIoT. The smart device transforming into smart object are involved as social significance with social consciousness.

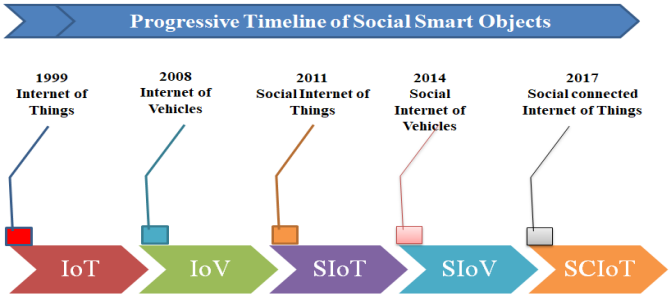


Figure 2: Progressive Timeline of social smart objects

In figure 2, the progressive timeline of social smart objects. By improving the abilities these smart devices using social object scenario allow them to collaborate between the social networks, join communities and manage their relationships without requiring human intervention. Therefore, it makes unique from other connected things and devices. The table1 depicts comparision between these two paradigms of IoT and SIoT. As shown in figure 2, SIoT exists in the third generation of social networks which displaying set of activity and different new relationship within environment of social network. The social environment produced their relationship according to their interactions, protocols set between the objects, and their communication links.

Table 1: IoT and SIoT domain

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

Within the SIoT network, the object can access service associated with network utilising social relationship, and make connection with friends of friends in various environments. These social objects have different behaviors and their services. These social nodes or objects are connected with the neighboring nodes when they have developed trust with each other. There are various malicious nodes owned by the users, used to attack other objects to earn more profit to acquire more services within network. Such malicious nodes are required to identify and restricted in the connected social network. Therefore, trust is the fundamental issue for the interaction of the friendly nodes. When there is trust among the nodes of the social objects, it allows them for various services in similar nodes and is restricted to malicious nodes [7]. Given that trust, management plays a vital role to overcome the perceptions of the uncertainty and risk from malicious nodes.

II. Background

The deep concept of trust and its management is raised by the various researchers using literature review. This section of the paper clarifies the various issues related to Trust and SIoT. The very first article related to trust in SIoT came into existence in 2016[8]. Comparison of trust management surveys for SIoT was explored in [9]. In [10], define the techniques to measure the behavioral trust mobiles node. This work was extended utilising the term SIoT. Nitti et. al. [11] present policies for the computation of the trust from behavioral of the social relationship of the objects. Bao and Ing-Ray proposed model which delas with misbehaviour of nodes whose state changes with the change of time dynamically using dynamic trust management protocol [12]. These nodes are used to measures the trust metrics.

In 2019, Wang et. al. measure a distributed trust management depicting IoT and integrates SDN, BES, and ORES to implement three-tier architecture [13]. Ing-Ray and Bao [14], produced adaptive trust management for SIoT systems in which social relationships are dynamically adapted by the owners of IoT devices in order to analyase the design perpective. To extend the previous work by Ing-Ray and Bao in [15], to design and evaluate a scalable, adaptive, and survival trust management protocol in a dynamic environment. Two types of nodes are considered from the community of interest (CoI) for SIoT which is known as Inter-Community of Interest and Intra- Community of Interest social connections among the nodes as input and this approach achieves the best protocol selections. Michelle et. al. present [16] a fuzzy approach for trust calculation to identify the level of IoT nodes. Further the previous research as an outcome of Fuzzy Trust Based Access Control approach using such model defined for Iot distributed environment to access control dynamically. In [17], Abraham proposed a fuzzy nearest neighbor with Bayesian belief networks to represent trust-based evaluation. In [18], Jia Guo develops a trust protocol known as Adaptive IoT (AIoT) trust.Saied et. al. disscuss the limitation of fault tolerance heterogeneity using context aware multice service strategy todetermine trust by proposing Novel Trust Managenet System (NTMS) [19].

SIoT is the network of the third generation of social networks where the SOs establish a dynamic relationship and behave activities across the various social networks. In the SIoT network, objects establish relationships according to the communication between objects and owners followed by the policies in their communication links [20]. In the SIoT network, the object can communicate by establishing relationships with the friend and friend of its friends in a distributed environment. While SOs build their relationship with trustworthy objects and the services are offered only to those who have a long and good relationship. Atzori et. al. in [11], and Khan et. al. in [21], have explained various relationships between objects and the owner. In [22], Ali et. al. proposed an architecture that provides a foundation for providing lightweight services on the social network of objects. To reduce the complexity of the services, a model is proposed which depict the interoperable service operations on various applications which are known as the sibling object relationship (SIBOR). Instead of the above relationship, in [23], the guardian object relationship (GOR) is explained as a hierarichy of social relationiship based on Internet of vehicles (IoV) which established among the vehicles. Such types of objects relationships are based on the various criteria, specifications, and feature activity patterns. Another effort by Chen et al. [14], describes SIoT networks in three types of social relationships that shows connections with their owners using *a community of interest relationship, social contact relationship and friendship relationship* . The smart objects of relationships provide services with other objects to whom they have established good and long relationships.

III. Trust Management Models for SIOT

In the third section, we depicted classification of trust management in three categories which are shown in figure 3 are as follows; 1) Trust evaluation Models. 2) Trust Management. 3) Context-Aware trust models. Trust is a sensation that exists among living beings equipped with advanced technology. It is one of the important and complex concepts which helps users to make decisions in critical situations.

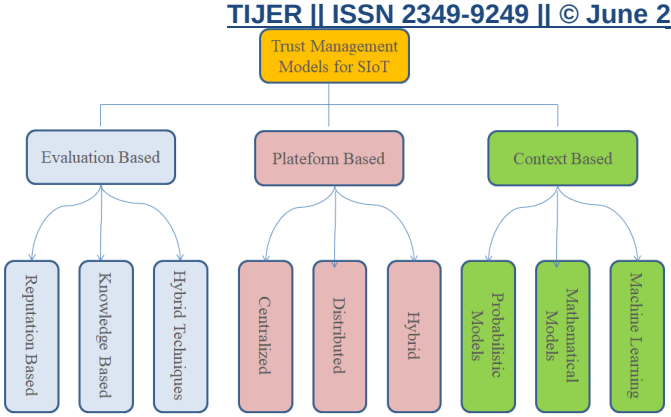


Figure 3: Trust management models

A. Trust Evaluation Models

The review of several Trust evaluation model under SIoT environment are presented here which are described as follows:

Chen et. Al proposed trsut based architecture that amalgamates SDN and IoT with protocol of cross layer authorization which trst based. For evaluation of trust further proposed scheme reagarding behaviour based on reputation evaluation which is known as the Organization Reputation evaluation scheme (ORES) [24]. *Xiao et. Al. describe th significance of guarantor and reputation utilizing Novel trust model* within SIoT environment. Using trustworthiness the reputation of devices is calucated and guarantor nodes are responsible for accessing services. From the simulation, it is found that the trust model charges penalty for malicious activity having capability to detect and analyse misbehavaing node in different scenario under SIoT environment [25].

Valamarthi and Kowshalya[26] described trust management scheme for the behavior of the object. Trust is calculated on the node's experience and then it is stored and shared between the network to take decisions against the malicious network. Trust values are updated frequently after 30 seconds. These trust values are used for future trust calculation and predicted the future behavior of the node and prevent malicious nodes. Kowshalya and Valarmathi [27] proposed a framework known as DTrustInfer computes trust by using the two factor named dependability and centrality. Authentic nodes are selected based on higher values of centrality. To evaluate the framework, the SWIM simulator has been used along with the Brigkite data set and the Epinions data set.

Jayasinghe et. al. [28] depicted recommendation plus reputation-based trust computation model. The author proposed a trust calculation model to calculate the trust scores of nodes which is more robust. The recommendation is based on its friends and social relations and the reputation is based on the opinion of the other. Only reputation and recommendation are considered for trust computation and while leaving the knowledge metric being a baised property.*Truong et. Al.* [29] considered experience , reutation and knowledge (REK) for trust models which are based on three indicators known as direct observation, experience and third party opinion. Experience is calculated with the help of trust attributes, including current relationships.Knowledge is calculated with the help of three metric are integrity benevolence and ability

B. Trust Management Platforms (TMPs)

TMPs can be used as centralised and decentralized. In order to provide authorization and authentication access control based service are utilised in IoT devices.

Abderrahim et al. have proposed integrated SIoT transaction factor direct and indirect trust and trust of social modelling.The value of trusted administrator depend on how calculation of trust value is done for particular groupand discarding malicious nodes from same community. The performance of the system is measured and check compatibility with SATIoT model and shown experiment result *Troung et. al.* proposed a trust based platform under SIoT environment. The services depend on recommendation, knowledge and reputation . The recommendation is determine on personal basis, while reputation rely on oponion and knowledge signify how trustworthiness calculated referring a node. Trust is measured with two parameters by utilizing fuzzy based mechanism and a reputation-based algorithm.

Azad et. Al.measured trustworthinessusing third party by proposing self enforcing trust management model. The proposed scenario is used as strict protocol zero knowledge proofs (ZPK). The proposed approach interacted with the nodes and used the feedback value of IoT devices.

C. Context-Based Trust Models

The review of context based trust evaluation method for SIoT presented in this section. *LinDong* proposed a contextually based trust model based on various parameters are trustor, trustee, trustworthiness evaluation, and context. The researcher considered the model by using a dataset from Facebook, Google+, and Twitter. *Khani et. al.* proposed a novel contextual-based model known as mutual context aware trustworthy service evaluation by utilising the context related to trust in SIoT environment. Considering effectiveness of the approach determine its impact, the researcher have collected a random 600 dataset from service provide by devices and service consuming devices

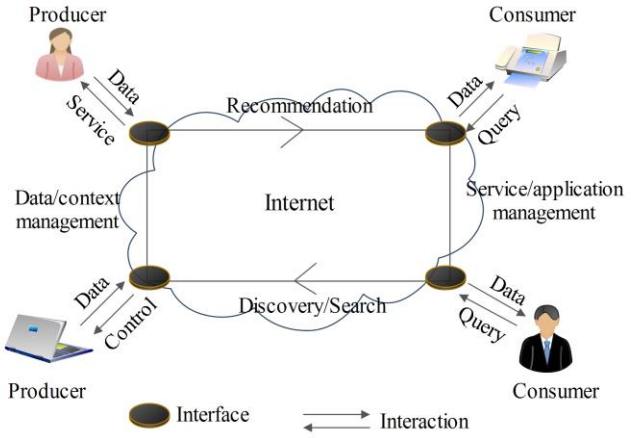
Chen proposed approach for accesibilty of services recommendations under SIoT throgh records and profiles are maintained by each node. Trustworthiness is calculated by using the previous and current performance of reputation based on directband indirect current status and social object relation ship status are used. One or more nodes are selected on priority according to the service requirements and interactions with trustworthiness. The performance was evaluated in concern of network stability, rating accuracy, and dynamic behavior. *Rafey et. al.* have presented a distributed context-based social trust model for IoT. In this model, to improve the result of trust, the social relationships between nodes and the context of interactions are influenced and used trust in the form of 1) trust between the nodes and, 2) trust between the owners of the nodes. The trustworthiness is calculated based on direct interactions and the recommendations of other nodes. Simulation is performed in the presence and absence of malicious nodes by using the CBSTM-IoT model to find the actual status of the node.

D. SIoT architecture:

The SIoT architecture shows the ecosystem where people allow smart devices to interface within a social framework. The framework provides various services on Web Technologies. Various attempts have been done by the researchers to develop an architecture for the SIoT system. In [30], the social approach of the COSMOS introduces. It supports the flow of knowledge between things to provide s system that learns, evaluates, and observes the usage and communication patterns to gain new knowledge. To extend the previous work of social network Voutyras et. al. [31], integrates social networking and can be extended to a network of Things and discuss the four main components of Social Network Analysis (SNA) are Friends Management (FM) Profiling, and Policy Management (PPM), Social Monitoring (SM), and Social Analysis (SA). SM determines all the tools

and architecture required for the social properties while in SA determines the nearby nodes and patterns for finding prominent entities.

Alam et. al. in [23], proposed a three layers scenario for the architecture of cyber physical system the social IoV are; physical entities, social entities and cyber entities. Ortiz et. al. [32], describe genuine SIoT architecture where combination of users, service and devives are allowed to establish the connection. The architecture for SIoT is represented in figure 4, which describes the components of SIoT [32].



1) Actors: The social activities of users initiated by the actors where the logic brings out the IOT world to warranty the navigation of network. SIoT provides appproriate environment to actors and devices to interact with each other and share the data and control signals.

2) Intelligent system: The responsibility of the intelligent system is for the management and orchestration of actors.

3) Interface: It is one of the most important components of architecture design. This component is used to communicate with the device through the Internet. The third critria based on actors dealing with interface to perform intreraction interaction.

4) Internet: It provides the environment for open access among all the entities involved in the Social network.

E. SIOT Applications

Today, the internet is used in every sector of industry and social life. By using internet in social appropriate flow of information and management provides better provision of services. Some of the application domains are potential use in various sectors are as follows:

1) Traffic Management: Sam is a salesman who regularly visit city regarding marketing purpose. Sam's car may enquire different car in SIoT environment to get update about the traffic routes for a particular destination.

2) Health: It is one of the important domain which get benefited from the Social IoT. Smart sensors for health, smart watch, smart ambulance are very useful to provide help at the spot in minimum time.

3) Education: Sam is a researcher and searching some papers related to machine learning malicious attack topics. But he couldn't find the relevant papers related to the problem. Then he send the message on various social sites groups and gets a revert message immediately.

4) Industry: Jon runs the automobile company and having some technical issues in its vehicle. Despite of calling technician, he required to search on youtube solution by himself. He used a co-work relationship and find the industry owners who are working in the same field provide services.

5) Supply Chain Management: Joy runs a logistic company and provides services to track the location, drivers and materials by using links between his devices and of drivers. Here the Joy applied co-work relationship and provide the devices to their employers regarding purpose of tracking.

6) Retail Management: Suppose a customer enters in the supermarket and confuse about the items. The mart app and the home refrigerator map the items and check the available items and required items. On the base of app decisions, customer can take quick decisions whether to buy the finished items or to buy a new item.

7) *Agriculture:* Sam is a farmer who started new farming of vegetables. He needs suggestions regarding a seasonal vegetable. He can consult with the co-work farmers or social relation farmers who may have previous experience and share the knowledge on single window or multiple devices come together.

Figure 4: SIOT Applications

F. Social Relationship among Objects

Such social relationship can be formed various parameters like device specification, patterns, application installed and the quality of services [11]. There are basically five types of relationships established which are as follows:

1) Co-location Relationship (CLOR): Such types of relationships established which are in the same location like school, oofice and home etc.

2) Cowork Relationship (CWOR): Such types of relationships are established When particular object working together and share same application for IoT service.

3) Paretal Relationship (POR): Such types of relationship established which describes the common objects unchanged by time.

4) Guardian Object Relationship (GOR):

5) Stranger Object Relationship (STGOR): It apply for those object which shows their presence of one another in unidentified environment or in the public network. For example, some peoples are meet with each other for some purpose but they are fully aware of each other.

6) Service Object Relationship (SVOR): Such type of relationship is established when delaing with same service composition to provide a request for service.

7) Guest Object Relationship (GSTOR): It is used to establish the relationship between objects which perform as a

guest role like a personal visit to friend house and getting a reward as a guest.

IV. TRUST EVALUATION IN SOCIAL INTERNET OF THINGS

Trust concept is not new in the field of psychology or computer science. It is very difficult to detailed discussion about the concept of trust. Before developing the trust ,trustee and trustor must agreed on various parameters such as location, time,activity. Trust can be explained with the general example. If a person named Sam trust on his friend Nick and Nick trust his friend Ved. It means Sam can trust on Nick which shows transitive trust. The transitive relation of trust is shown in the figure. This shows the potential of the trustwho doent known directly.

A. Trust Properties

From the various survey, it is found that trust can be computed in various ways depending on its properties and functions. Depending on the trust function, it can be categorized as described in detail:

1) Direct Vs Indirect: This indicates that the trust is based on the direct interactions and observation between the trustee and the truster. While in indirect trust, trustee and trustor don't have past experience or interactions. Trust can be built from the opinion and the recommendation from other nodes.

***2) Local Vs Global*:** Local nodes define a couple of the nodes considered from one couple to another couple. For example a node I can trust on J and another node X distrust on the same J node. While global node is known as a reputation node that every node has a unique trust value in the network which is known for all the nodes.

3) Subjective Vs Objective: Subjective is a personal opinion based on various factors or proof, and it may carry more weight than other nodes. While in objective case, trust is computed and based on QoS properties of a device.

4) Rank Vs Threshold: If a node obtained trust by comparing trust from other nodes, therefore we can say that the node can assign rank on the base of its standing position. It is known as the rank based trust. On the other hand, if a trust is computed by comparing its value to a threshold, it is known as trustworthy otherwise untrustworthy.

5) *Transaction Vs Opinion:* If the trust of a node is measured based on the transactions from other nodes, it is known as transaction trust while on the other hand if the trustworthiness is based on the opinion of the other nodes of system, then it is known as the opinion based trust.

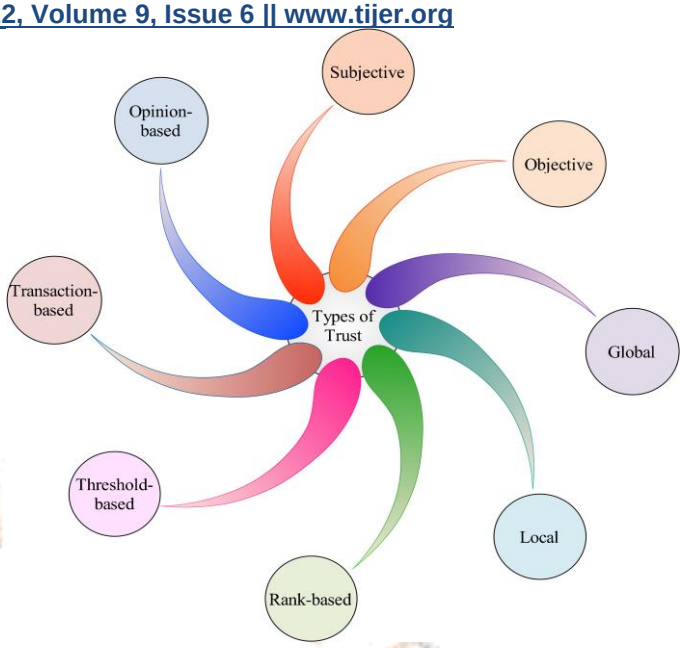


Figure 5: Trust Categories

G. Trust-Based Attacks

The objective of malicious nodes is to interrupt the functionality of the network and the IoT services. Troung et. al. proposed a trust-based technique integrated with social trust metrics. To calculate the weighted sum of direct views, global decisions and experiences are applied by using Bayesian techniques to prevent attacks BMA, BSA, and SPA. Chen et. al. proposed an access service recommendation for SIoT environment. This approach defends the attacks related to BMA, BSA, and SPA. Mariam Masmooudi [] proposed a trust evaluation model to identify malicious attacks and calculate the trust score. This technique is used to defend from the attacks like BMA, BSA, SPA and DA. Some of the trust related attacks which are as follows:

1) Self-promoting Attacks (SPA): It is one of the attack techniques where malicious nodes, provides bad services, try to improve the reputation in order to be a member as a service providers in the social network.

2) Bad-mounting Attacks (BMA): These malicious nodes try to destroy the reputation of proper functioning of the nodes in order to reduce their probability to be selected as a service providers.

3) Ballot stuffing Attacks (BSA): These malicious nodes try to improve the reputation of the other malicious nodes in order to improve the probability to be selected as the service providers.

***4) White-washing Attacks (WWA)*:** It is a malicious nodes that can remove and rejoin to improve the reputation.

5) *Discriminatory Attacks (DA):* These malicious nodes attacks prejudice other nodes, without any social relationship due to human tendency towards strangers.

6) *Opportunistic service Attacks (OSA)*: It is a malicious nodes which can provide good service by overambitious to gain high reputation, generally in case of when the market reputation is decreased due to bad services.

Table 2: Trust Attacks Comparison

Ref.	Malicious Trust Attacks					
	SPA	BMA	BSA	WWA	DA	OSA
[15]	√	√	√			
[33]	√	√	√			
[12]	√	√	√			
[14]	√	√	√			
[9]	√	√	√			
[11]	√	√	√	√		√
[17]	√					

H. SIoT Trust Models

Trust Management System (TMS) are liable for transforming trust-related activities like trust calculation, trust gathering, trust storage, trust update etc. It is required when in two stages when a node wants to require a particular service and when a node receives some information from another node and it verifies whether that information can be trusted or not.

Trust Composition (TC): It refers to the types of parameters selected for the creation of trust value. The quality of trust may categorize into two phases which are as follows:

- ***QoS Trust:*** The parameters may represent the quality node is offering, or calculated from the social behavior, representing the social nature of the network. Parameters of QoS are data delivery, positive or negative, response time, throughput, availability, etc.
- ***Social Trust:*** It can be calculated for honesty, intimacy, healthiness, cooperativeness, selfishness, etc.

Table 3: Classification of Trust Models

Ref.	1		2		3					4	
	A	B	C	D	E	F	G	H	I	J	K
[15]	√	√		√			√			√	
[33]	√	√		√		√	√			√	
[12]	√	√		√		√				√	
[14]	√	√		√						√	√
[9]		√		√					√	√	√
[11]		√							√	√	

1= Trust Composition, 2 = Trust Propagation,
3 = Trust Aggregation, 4 = Trust Update.

A= QoS Trust, B = Social Trust,
C = Centralized D = Distributed
E = Weighted Sum (WS), F = Belief Theory,
G = Bayesian Inference, H = Fuzzy Logic,
I = Regression Analysis J = Event-Driven,
K = Time-Driven

Trust-Formation (TF): It affects the humble trust value either on single-factor or multiple-factor. Trust values are calculated on a single factor. TMS is based on multiple factors. These factors can be considered multiple in numbers or they can be either QoS factors or social factors. Such types of trust are categorized into parts are; single trust and multiple trusts.

Trust-Decision (TD): Calculating the trust values, TMS provides services to requesting nodes. Similar services may be provided by the multiple nodes. In such cases, TMS identified trustworthiness values of all such providers and the requesting node, then selects one service provider. Requesting node, for the trustworthiness value; asking node may verify the trustworthiness value. It can be decided whether the trust value received information is correct or not or it is only depending on the calculated value. The whole approach is based on two approaches, as shown in figure 6, which are as follows:

- ***Policy-based Trust (PBT):*** Based on decision-making for storing, maintaining, and sharing services among the nodes. Services are used to create trust-relationship among nodes on fixed policies. It is based on access control, verification of credentials and permitting or allowing access control on policies.

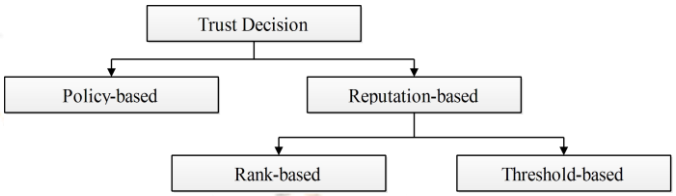


Figure 6: Trust Decision classification

- ***Reputation-based Trust (RBT):*** The concept of trust evaluation service-providing nodes from the service requesting node or other nodes of the network. Estimating trust, requesting node decided whether the service-provider node is trusted or not. Trust calculation is based on various parameters like; subjective/objective, opinion/transaction, local/global as explained previously. Trust reputation is by rank or threshold function.

Trust Update (TU): In the update record, requesting nodes for the transaction for the specific service provider and monitor agreed on some specific parameters for future reference in decision making. Trust value updated upon the performance. The whole process of trust is categorized into two phases:

- ***Event-Driven:*** Trust value updated after an event or interaction occurred. The transaction is completed or the service received, but the rest of the services are being received.
- ***Time-Driven:*** It is activated time-to-time without any wait for an event. Trust values are calculated based on services provided at the time of requirement.

Trust Calculation: Collecting information from various nodes, TMS calculates the trust value of each node of a particular service of the nodes. The value of trust is calculated, depending on the policy of the system is categorized and shown in figure 7. Trust can be calculated in two ways are as follows:

- ***Trust Aggregation:*** Gathering information from the system on various parameters, information should aggregate in a manner to calculate a single trust value, based on the measured parameters [34]. The process of trust aggregation is described as follows:
  - **i) Weighted-Sum (WS):** One of the most popular methods, for the calculation of aggregate values and comparison from other alternate methods on given parameters. The weight is assigned to estimate criteria and multiplied with the measured criteria. Weight may be static or dynamic, depending on the criteria [35].
  - **ii) Belief-Theory (BT):** It is also known as evidence theory or Dempster-Shafer theory [36]. Merges the evidence collected from various sources and converts into belief. Each evidence has its value and lies between 0 and 1, 0 refers no support for the evidence and 1 refers support for the evidence [36].
  - **iii) Bayesian-Inference (BI):** Bayesian theory arrive at a surface probability of an item, given a prior probability

iv) and likelihood function. It is based on the Bayes theorem.

v) Fuzzy-Logic (FL): Boolean logic has only two values 0 and 1. Fuzzy logic considers all the values lie between 0 and 1 [37]. It becomes attractive for trust aggregate value which cannot be categorized between 0 and 1. Fuzzy logic works for degrees of members of different intervals of values. These fuzzy values are combined to reach a single trust value [38]. Fuzzy is categorized into three steps, fuzzification, fuzzy rules, and defuzzification.

vi) Regression-Analysis (RA): To study the relationship between various objects. Forecast one variable change concerning other values. Variables are known as dependent and independent. Two types of regression analysis are as follows:

a. **Simple Regression:** It is used for one dependent variable in respect to every independent variable.

b. Multiple Regression: It is used for multiple independent variables for each dependent variable.

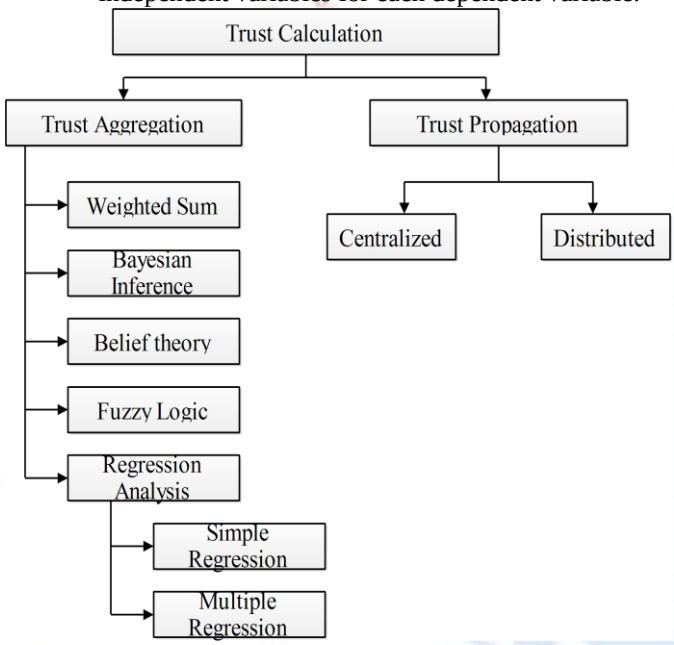


Figure 7: Trust Calculation Classification

Trust Propagation (TP): Information of trust-flows or reproduces through the network. Two processes under this technique are as follows:

- ***Centralized:*** One node is responsible for collecting trust-related information, trust calculation, storing, and spreading on the network. If the network is a failure on a single point, the entire trust management system may destroy.
- ***Distributed:*** Information collection and trust calculation performed by the nodes. Each node operates and is spread over the network for the usage of the other nodes, either spontaneous or receiving requests. Removes the problem of single-point failure, calculating trust, and sending out without bias information.

V. TRUST CHALLENGES

SIoT is a new research area, that intends various challenges in the area of security and trust management. It requires the features of smart objects to establish a social network of their or join the other network in ownership. Controls and issues are raised when security and trust came into knowledge. Some points are raised here which are the challenges intended by SIoT and its usage.

- ***Establish a relationship between Smart Objects:*** To establish a relationship between different objects based on trust is shared between the members. Therefore, a reliable trust model is required that incorporate various types of relationship between objects to make trust decisions.
- ***Policy Obedience:*** Policy should be defined by the owners of the object between the networks. These policies will differ with each owner or the object due to heterogeneity. The decision may be taken during a policy violation.
- ***Node's consideration from recommendation:*** The models are connected with a trust nodes recommendation made by that node. A node cannot be trusted on service, because a node might be a good node for providing information of the other nodes, but it is not good in the reference of the service.
- ***Heterogeneous Nodes:*** It plays an important role in the reputation of a device. The network consists of heterogeneous IoT devices and every device has its capacity, computation, complexity, and energy consumption. Very few researchers have considered the heterogeneous during implementing the models.
- ***Resource Constraint:*** In this IoT network every device tries to acquire resources while providing any solutions. TMS with higher computation and storage capacity affects the low configuration of the devices for one time of services. The major focus is on device energy, developing trust models for SIoT.
- ***Condition Awareness:*** One of the important domains of TMS during evaluating trust on various devices in the multi-service environment. The behavior of the device is not uniform in every environment. The device may perform good behavior with lightweight services, dodder the services with the heavyweight. Therefore, the service of conditional is aware in the multi-environment.
- ***Dynamic Nodes:*** It is very difficult to process the TMS to collect the actual status and behavior of the devices. Most of the researchers consider only static weight assignment, for trust attributes in trust calculation. The effective and adaptive methodology may consider for dynamic assignment to reduce weights of dependent applications.
- ***Scalable Framework:*** SIoT network consists of a huge no of nodes connected. Therefore, a scalable framework is required, to maintain the performance and does not degrade, when the nodes are increased.
- ***Required Trust Evaluation models:*** With the implementation of distributed computation, trust is one of the major issues during interaction among different nodes. While the leading approaches for trust management shows their presence in case of peer to peer networks .the shortage of such model hase been found in SIoT environment.

VI. CONCLUSION

For the last decades, things are connected with the internet. Now it is increased continuously at an exponential rate after connecting things with social. The Social Internet of Things has been used in every application. SIoT provides various services on these things. It is difficult to verify whether the services are a trustee or not. The present paper reviewed on latest work done on trust and SIoT to locate things and provide services. To establish a relationship between objects, the interaction between devices and users, manage the trust, calculate trust, and the challenges of SIoTand trust.

REFERENCES

[1] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," *IEEE Internet Comput.*, vol. 14, no. 1, pp. 44–51, 2010, doi:

10.1109/MIC.2009.143.

[2] L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H. W. Gellersen, "Smart-its friends: A technique for users to easily establish connections between smart artefacts," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2201, pp. 116–122, 2001, doi: 10.1007/3-540-45427-6_10.

[3] B. Jafarian, N. Yazdani, and M. Sayad Haghighi, "Discrimination-aware trust management for social internet of things," *Comput. Networks*, vol. 178, no. April, 2020, doi: 10.1016/j.comnet.2020.107254.

[4] A. Hameed and A. Alomary, "Security issues in IoT: A survey," *2019 Int. Conf. Innov. Intell. Informatics, Comput. Technol. 3ICT 2019*, pp. 1–5, 2019, doi: 10.1109/3ICT.2019.8910320.

[5] W. Najib, S. Sulistyo, and Widyawan, "Survey on trust calculation methods in internet of things," *Procedia Comput. Sci.*, vol. 161, pp. 1300–1307, 2019, doi: 10.1016/j.procs.2019.11.245.

[6] N. Gulati and P. D. Kaur, *When things become friends: A semantic perspective on the social Internet of Things*, vol. 670. Springer Singapore, 2019.

[7] Z. Lin and L. Dong, "Clarifying Trust in Social Internet of Things," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 2, pp. 234–248, 2018, doi: 10.1109/TKDE.2017.2762678.

[8] 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.

[9] 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.

[10] S. Adali *et al.*, "Measuring behavioral trust in social networks," *ISI 2010 - 2010 IEEE Int. Conf. Intell. Secur. Informatics Public Saf. Secur.*, pp. 150–152, 2010, doi: 10.1109/ISI.2010.5484757.

[11] 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," *Comput. Networks*, vol. 56, no. 16, pp. 3594–3608, 2012, doi: 10.1016/j.comnet.2012.07.010.

[12] F. Bao and I. R. Chen, "Dynamic trust management for internet of things applications," *Self-IoT'12 - Proc. 2012 Int. Work. Self-Aware Internet Things, Co-located with ICAC'12*, pp. 1–6, 2012, doi: 10.1145/2378023.2378025.

[13] J. Chen, Z. Tian, X. Cui, L. Yin, and X. Wang, "Trust architecture and reputation evaluation for internet of things," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 8, pp. 3099–3107, 2019, doi: 10.1007/s12652-018-0887-z.

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

[15] F. Bao, I. R. Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based internet of things systems," *Proc. - 2013 11th Int. Symp. Auton. Decentralized Syst. ISADS 2013*, 2013, doi: 10.1109/ISADS.2013.6513398.

[16] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, "A fuzzy approach to trust based access control in internet of things," *2013 3rd Int. Conf. Wirel. Commun. Veh. Technol. Inf. Theory Aerosp. Electron. Syst. VITAE 2013 - Co-located with Glob. Wirel. Summit 2013*, 2013, doi: 10.1109/VITAE.2013.6617083.

[17] M. Panda and A. Abraham, "Development of a reliable trust management model in social internet of things," *Int. J. Trust Manag. Comput. Commun.*, vol. 2, no. 3, p. 229, 2014, doi: 10.1504/ijtmcc.2014.067305.

[18] J. Guo, "Trust-based Service Management of Internet of Things Systems and Its Applications," pp. 1–151, 2018, [Online]. Available: https://vtechworks.lib.vt.edu/bitstream/handle/10919/82854/Guo_J_D_2018.pdf?sequence=1.

[19] 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," *Comput. Secur.*, vol. 39, no. PART B, pp. 351–365, 2013, doi: 10.1016/j.cose.2013.09.001.

[20] A. Khanfor, A. Hamrouni, H. Ghazzai, Y. Yang, and Y. Massoud, "A Trustworthy Recruitment Process for Spatial Mobile Crowdsourcing in Large-scale Social IoT," *2020 IEEE Technol. Eng. Manag. Conf. TEMSCON 2020*, 2020, doi: 10.1109/TEMSCON47658.2020.9140085.

[21] 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 Things J.*, vol. 8, no. 10, pp. 7768–7788, 2021, doi: 10.1109/JIOT.2020.3039296.

[22] S. Ali, M. G. Kibria, M. A. Jarwar, H. K. Lee, and I. Chong, "A Model of Socially Connected Web Objects for IoT Applications," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018, doi: 10.1155/2018/6309509.

[23] K. M. Alam, M. Saini, and A. El Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015, doi: 10.1109/ACCESS.2015.2416657.

[24] J. Chen, Z. Tian, X. Cui, L. Yin, and X. Wang, "Trust architecture and reputation evaluation for internet of things," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 8, pp. 3099–3107, 2019, doi: 10.1007/s12652-018-0887-z.

[25] H. Xiao, N. Sidhu, and B. Christianson, "Guarantor and reputation based trust model for Social Internet of Things," *IWCMC 2015 - 11th Int. Wirel. Commun. Mob. Comput. Conf.*, pp. 600–605, 2015, doi: 10.1109/IWCMC.2015.7289151.

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

[27] A. Meena Kowshalya and M. L. Valarmathi, "Dynamic trust management for secure communications in social internet of things (SIoT)," *Sadhana - Academy Proceedings in Engineering Sciences*, vol. 43, no. 9. 2018, doi: 10.1007/s12046-018-0885-z.

[28] U. Jayasinghe, N. B. Truong, G. M. Lee, and T. W. Um, "RpR: A Trust Computation Model for Social Internet of Things," *Proc. - 13th IEEE Int. Conf. Ubiquitous Intell. Comput. 13th IEEE Int. Conf. Adv. Trust. Comput. 16th IEEE Int. Conf. Scalable Comput. Commun. IEEE Int.*, pp. 930–937, 2017, doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0146.

[29] T. U. . L. G. M. Truong N.B.; Won, N. B. Truong, T.-W. Um, and G. M. Lee, "A reputation and knowledge based trust service platform for trustworthy Social Internet of Things," *Proc. 19th Int. Conf. Innov. Clouds*, no. March, pp. 104–111, 2016.

[30] O. Voutyras, P. Bourelos, D. Kyriazis, and T. Varvarigou, "An architecture supporting knowledge flow in social internet of things systems," *Int. Conf. Wirel. Mob. Comput. Netw. Commun.*, pp. 100–105, 2014, doi: 10.1109/WiMOB.2014.6962156.

[31] O. Voutyras, P. Bourelos, S. Gogouvitis, D. Kyriazis, and T. Varvarigou, "Social monitoring and social analysis in internet of things virtual networks," *2015 18th Int. Conf. Intell. Next Gener. Networks, ICIN 2015*, pp. 244–251, 2015, doi: 10.1109/ICIN.2015.7073838.

[32] A. M. Ortiz *et al.*, "The cluster between Internet of Things and social networks : review and research challenges To cite this version : HAL Id : hal-02284567 The Cluster Between Internet of Things and Social Networks : Review and Research Challenges," 2019.

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

[34] W. Najib, S. Sulistyo, and Widyawan, "Survey on trust calculation methods in internet of things," *Procedia Comput. Sci.*, vol. 161, pp. 1300–1307, 2019, doi: 10.1016/j.procs.2019.11.245.

[35] I. Y. Kim and O. De Weck, "Adaptive weighted sum method for multiobjective optimization," *Collect. Tech. Pap. - 10th AIAA/ISSMO Multidiscip. Anal. Optim. Conf.*, vol. 1, pp. 236–248, 2004, doi: 10.2514/6.2004-4322.

[36] M. Beynon, B. Curry, and P. Morgan, "The Dempster-Shafer theory of evidence: An alternative approach to multicriteria decision modelling," *Omega*, vol. 28, no. 1, pp. 37–50, 2000, doi: 10.1016/S0305-0483(99)00033-X.

[37] G. Zacharia and P. Maes, "Trust Management Through Reputation," *Online*, vol. 12, no. 1, pp. 881–907, 2000.

[38] M. Tahajod, A. Iranmehr, and N. Khozooyi, "Trust management for semantic web," *2009 Int. Conf. Comput. Electr. Eng. ICCEE 2009*, vol. 2, pp. 3–6, 2009, doi: 10.1109/ICCEE.2009.241.