Journal of Applied Science, Innovation & Technology (JASIT)

Journal homepage: https://prakritimitrango.com/documents-reports-and-publications/journal/

Review Article

Proposed model for trust evaluation using recommendation and reputation in the Social Internet Things (SIoT): A Review

Gulshan Kumar Yadav*, Najmul Arif, Pawan Kumar Chaurasia

Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow-2260025, India

ARTICLE INFOR: *Received: 18 March 2023; Revised: 01 June 2023; Accepted: 02 June 2023*

***CORRESPONDING AUTHORS**: E-mail: gulsan28etah@gmail.com (G.K. Yadav)*

Abstract

In order to establish social networks or linked smart items, the social internet of things (SIoT) blends social networking principles with the internet of things. In order to cope with offending service provider nodes, it has been developed to create a network of intelligent nodes that are designed for forming social connections. Both the Human-to-Human (H2H) and Things-to-Things (T2T) relationship paradigms must be considered when service requester nodes assess their IoT. Human-to-Thing (H2T) relationships are encouraged by SIoT. Smart "social objects" made possible by SIoT may automatically imitate how people interact with one another in daily life. These social objects have social functions, which enable them to interact with other social objects in their environment and find new social connections. They scurry through the thing social networks. To check out services and learn more about their interests, they prowl around the social networks of things. The idea of trust and trustworthiness in relation to the -created social contexts is still in its early phases of research. The principles of SIoT and trust ideas are covered in this review, along with comparisons and contrasts among SIoT and IoT. Additionally, this study organised and reviewed all of the trust management approaches that have been put forth in the last six years' worth of studies for the SIoT. This study also recognised and addressed the criteria for the burgeoning new generation of SIoT, as well as the difficulties in forging relationships of trust and determining if social things are trustworthy.

Keywords: IoT, Social Internet of Things (SIoT), Trust Management, Challenges in SIoT

1. Introduction

The internet of things (IoT) is a better technology that makes it possible for many physical items to link to one another. The SIoT was recently developed to create a network of items, and it is on this foundation that one may notice a change in generations from devices with a certain amount of intelligence to devices with the awareness to take action when necessary. Without taking this potential into account, the SIoT, which contains trillions of items, cannot continue to develop and advanced. In the SIoT, objects function as independent agents. Objects may communicate with one another and exchange data and facilities while maintaining their identity. The benefits of this propagation are given as follows:

Similar to human networks, a social IoT ensures network adaptability as well as networks navigability, which indicates to the efficient finding of items and services. By utilising a degree of contact between friends and self-regulating items, trust levels might be built the social IoT might make use of enhanced versions of the social network analysis models that were formerly developed (Roopa et al., 2020).

By incorporating the idea of social networking into the iot, devices interact worldwide with various peers while rigorously adhering to predefined patterns. By incorporating the social networking concept of the iot, social internet objects are a viable strategy for accelerating interactions between objects problems. Regardless of whether or whether items are placed on various networks or how far apart they are from one another, openness in the SIoT creates social relationships between them. By setting a trust level, utilising familiarity for transaction filtration with a society-based view of trust, and preventing strange nodes by prioritising the interaction of trusted members, trustworthiness in the SIoT is ensured. The SIoT's purpose is allowing multiple objects to work together efficiently and securely to fulfil end-user demands for dependability, safety, efficiency, and availability. SIoT has not received enough attention in survey studies to be discussed in all of its facets, thus this study chosen to publish a thorough literature review article because Insufficient comprehension of the SIoT systems that compared and investigates (Alghofaili, et al., 2022).

- A great way to explore and learn about the issues posed by SIoT devices is with insufficient knowledge of their structure and behavioural features.
- The absence of a defined procedure for study and article selections makes it easier for other scholars to find appropriate citations and data.
- The absence of conceptual accountability, especially in terms of specifics like formats, datasets, product connections, mankind roles, elements, and in context with current and prospective difficulties, as well as the absence of effective ways to address or foresee them.

The SIoT scenario, which enables interaction between people and objects that are connected, sharing of data, and a wide range of compelling applications, was created by integrating social networking principles into the IoTparadigm. Though users are still dubious and wary of this new paradigm. They are worried about their data being revealed and their privacy being

violated. The SIoT paradigm will not become widely adopted enough to be regarded as a mainstream technology and all of its strengths will be destroyed with no reliable solutions to guarantee users' confidential communication and reliable interactions. As the result, managing trust has become a major issue in SIoT in order to guarantee accurate data analysis, competent services, and improved security for customers.

2. The Internet of Things (IoT)

With the idea of ubiquitous computing, the origin of the IoT concept was predicted to go back to the '80s. The goal of IoT is to integrate technology into our way of life. In today's IoT ecosystem, social networking and connections between both technological and physical elements are common place. The IoT infrastructure supports the operation of a number of cutting-edge services (referred to as IoT services) on different platforms, where a sizable number of diverse gadgets collaborate to realise a common goal. The real sensing or duties are carried out by means of IoT services (Alghofaili, et al., 2022).

The linking of digital products, individuals, gadgets, equipment, and various other objects is referred to as the "Internet of Things." It enables communication and connection between machines and human beings. It is seen as the internet's further use. This kind of the web is around data that is formed by things. Things that can be linked with IoT are :

- Connected Homes: interlinking of household appliances to the network.
- Linked Wearables: smartphones, smartwatches, fitness bands, etc.
- Linked Cars: vehicles associated to the network.
- Linked Cities comprise smart meters that can analyse gas, water and electricity usage as well as attached traffic signals and smart bins.

Different networks would be linked, as stated below:
Body Area Network (BAN) - Wearable technology;
Local Area Network (LAN) - Smart Homes;
Wide Area Network (WAN) - Linked Automobiles;
Very Wide Area Network (VWAN) - Smart City.

The Internet of Things has become prevalent in a variety of fields, including farming, medical care, transport, and even educational opportunities. IoT technology integrates a number of duties to achieve the objectives created by smart services. These services are clever actions that provide gadgets the ability to interact with the real world and offer consumers the proper services whenever they need them and from any place.

IoT services in various fields have received increased attention in recent years, these are (Alghofaili et al., 2022)

Healthcare: digital glucometer, blood pressure monitor, etc;
Sports: ball movement tracking, running speed, etc.
Ttransport: self-driving cars, global positioning system (GPS) trackers, and so on;
Smart-cities; Energy engagement; Smart manufacturing; Agriculture;
Wearable devices: smart bands and smartwatches;

3. Social Internet of Things (SIoT)

A subset of the Internet of Things known as the SIoT is capable of interacting socially with other items, including people. SIoT makes an effort to mitigate the difficulties of IoT in the areas of adaptability, trust and identifying resources by taking inspiration from social computing. The SIoT may include representative architecture, which enables navigation by initialising one device and using it to get from to other devices that are linked and link back to it, establishing independent connections among objects and people (Mohammadi et al., 2019).

The SIoT paradigm provides a number of benefits. Because in human social networks a characteristic of trustworthiness is frequently determined based on the amount of relationship among items that are associates, the outcome of the things' social network is frequently shaped as needed to ensure system navigability, safely carry out their creation of objects and products and services, and to ensure reliability. It is common practise to repurpose social network analysis models to address IoT-related problems (which are inherently tied to vast networks of networked things). The devices work together to offer a variety of intelligent services that are used by consumers, businesses, and other devices in daily life. Health Care, innovative homes and offices, automated public transportation, and ecological tracking are just a few of the industries that may employ IoT.

In the Internet of Things, the gadget can act simultaneously as a solution provider and a service requester. IoT incorporates a social networking component, known as SIoT, to create trustworthy connections between gadgets. The Internet of Things (IoT) is a collection of numerous objects and devices that gather data, offer services, offer suggestions, make choices, and perform actions.

The development of novel health care, medical robots, and integrated healthcare sensors are all significantly impacted. Additionally, it is utilised in systems for crowd observation and coastal administration.

4. Relationships in the SIoT Network

The IoT and object relationships are created by utilising human intelligence to take part in the organization's phase (setting up, uphold modify, dismiss and communicate for information). Relationships building is highly impacted by several characteristics such as object kind, movement scheme, method, processing capability and frequency of contact. These connections happen naturally, but only with this permission (Simon et al., 2022).

Different SIoT connections exist between devices are given follows:

4.1 Parental Object Relationship (POR): It is made up of related entities (manufacturer, item type, standard, and batches) that simultaneously produce homogenous products. This connection is regarded as static since there has been little change since it was established during the manufacturing phase.

4.2 Co-Location Object Relationship (C-LOR): It develops between things that are either homogenous or heterogeneous and are in a fixed position. Since this kind of connection is established at the initialization phase, it is static until the connection's length is changed by the developer.

4.3 Co-Work Object Relationship (C-WOR): It is created in the SIoT between items that are either homogenous or heterogeneous sometimes carry out a similar job. As a result, this connection is established to carry out the choice and will not alter until there are additional modifications to the relationship's duration or frequency of communication.

4.4 Ownership Object Relationship (OOR): It is made up of several items/devices (such as computers, cell phones, printers and copiers etc.) possessed by a single person who has the ability to increase physiological processes rates.

4.5 Social Object Relationship (SOR): It develops between diverse or homogeneous items as a result of frequently or ongoing interaction between things whose owners interact with one another (things possessed by friends, mates, colleagues and other individuals) or by allowing for autonomous mobility. Afterthat, things share profiles at random with the owner's consent.

5. Challenges in SIoT

The following issues with trust management confront SIoT:

5.1 Decapability of the device

Devices are vary in terms of their computing power, storage space regulations, connectivity stacks, operating systems, and input/output channels, prior trust management methods cannot be implemented to all SIoT software applications. All such device characteristics should be taken into account by the trust management algorithms. Managing extensive networks, a significant number of events are generated through device communication. Current platforms can't manage such a large volume of transaction data efficiently. The trust management method should have sufficient strength to control both the massive volume of devices and the inter-device communication (Hankare et al., 2021).

6. SIoT Parameters:

The SIoT system changes when new devices are added and current ones are removed. Therefore, trust management methods should take into account the dynamic nature of devices, including their fluctuating behaviour, membership, interaction patterns, topography and site modifications. With the number of gadgets increasing, it is getting harder and harder to find reliable devices. Human existence is made easier with SIoT. So, a lot of information is exchanged among the human beings via smartphones in today's society. If data is exchanged with untrusted users or gadgets, there is a possibility that it may be misused. Therefore, it is necessary to design an algorithm with criteria that distinguish between a tool's trustworthy and dangerous behaviour and as a result, permit sharing in a regulated way to prevent malicious assaults (Hankare et al., 2021).

Trustworthy feature selection In the IoT, trust is a major problem since devices need to locate the right trustee in order to have a healthy exchange of information. In order to ensure that trust systems are accurate and effective, it is crucial to choose the right trust characteristics. The computation of the total trust value takes into account a certain collection of trust features, including popularity, integrity, the community of concern, correlation, and rating periodicity. In the SIoT network, the simplest devices are rated by the literature work, but hostile devices' attacks are not picked up. Finally, in the older systems, trust calculations do not take into account the continuous shift in trust attribute requirements. Adaptation of the trust feature set to proactively support the significance of the transaction if the determination of trust to be more accurate.

6.1 Trust Aggregation: To obtain a distinct convergent value, trust aggregation involves combining trust observations. Dynamic weighted sum (DWS), static weighted sum (SWS), Bayesian model (BM), and fuzzy logic (FL) are the key aggregation approaches examined in the study. For the gathering of trust values, the majority of the prior techniques employed a weighted sum approach. However, there are several issues involved with this method. When determining a weighting factor, there are various possibilities. As weights instructed to trust elements might different from one to another, systems have failed to recognise which attribute has the largest influence on trust in a given scenario. In this study, the trust ratings and the identification of undesirable devices are combined using a machine learning technique (Hankare et al., 2021).

6.2 Trust Update

The trusted update is dependent on other nodes' recommendations; hence, the trust update rating is determined by factoring in the value that a different node or suggestion provides. What happens, though, if the source of recommendation node is malicious? The trust is updated to reflect the node's expertise and/or prior experience. The capacity of the device is determined by how well it performed in the prior task, including any gains or losses resulting from the completion of the task, the device's good or poor behaviour, successful or failed interactions, the packet found and differentiated, etc. What if the trustor and trustee don't communicate for a long period of time? When upgrading the trust, it's important to evaluate how much time has passed since the last encounter. If there is no communication between nodes andtrust deteriorates. Trust attributes like recommendations and prior trust values are subject to trust decay. The prior trust value depreciates when a new conversation of interaction is created. To support past trust efficacy, direct evaluation, and advice, an overall trust is updated. The permitted number of interactions throughout the period serves as the basis for calculating the previous trust productivity (Hankare et al., 2021).

7. Trust Management in SIoT

Trust is important in many different disciplines, including the fields of sociology, psychology, history, finance, electoral politics, organisational leadership, technology progress, international relations, computers and networking. Definitions of trust and its cross-disciplinary applications are frequently found (Khan et al, 2020). Fig. 1 shows trust management in SIOT.

They may define the trust as “a degree of individual assurance in an entity's conduct”. To enable the estimate and care of trust in diverse systems or organisations, plans are established and referred to as "Trust Management (TM)". By defining it as a single autonomous way in the network architecture to analyse and ascertain security protocols, information, and connections, Blaze developed this phrase. When evaluating the behaviour of entities, TM offers a potential alternative to cryptography-based methods, which are unavailable or unable to assure system stability in the absence of outsiders or nefarious opponents. Reduced hazards and unpredictability are connected with an implementation of various services while trustworthy system operation is maintained (Hankare et al., 2021).

By acting as an intermediary layer connecting service requesters and suppliers in service-oriented settings like IoT

and SIoT, TM promotes trustworthy relationships and helps with managing resources, restricting access, dependable service structure, etc

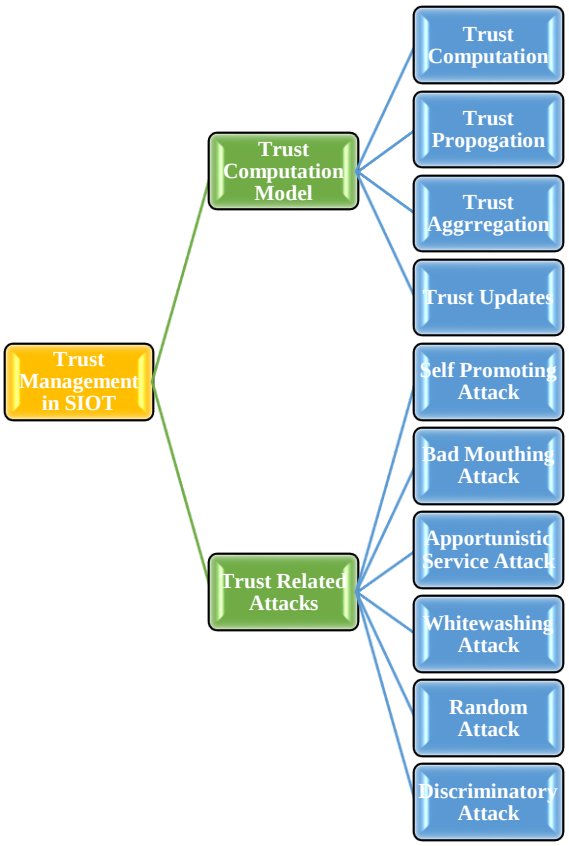

Fig. 1 Trust management by applying SIOT

.

Cooperation and collaboration among people are made possible by the critical role that trust plays in human relationships. Trust is a key element of SIoT since the SIoT model imitates human social contexts and Social Objects can handle social relationships by imitating human inherent nature. For instance, using the idea of reputation may be used to gauge how trustworthy an item is.

Calculating the tendency of the trustor, the trustworthiness of the trustee, and the surrounding factors, which are thought to be the subjective and asymmetrical connection between the trustor and the trustee (Malekshahi Rad et al., 2020).

In the SIoT, trust models assess social interactions and social factors that are supported by trust. In this ecosystem, Social IoT gadgets communicate with other gadgets those are interested to share or communicate. As a result of more regular encounters, communities are formed and relationships are strengthened.

Trust models assist in decision-making and offer trustworthy recommendations for a particular activity by gathering both direct and indirect views about the service vendor and assessing the predicted trustworthiness, or the service vendor's level of trust. When the trust level exceeds the cut-off point, the transaction is finally finished. The trust management method uses the network reputation of objects, the recommendations of nearby socially linked objects, and the historical behaviour of SOs in terms of delivering services or conducting transactions to analyse the behaviour of SOs in SIoT (Mohammadi et al., 2021).

A TM process life cycle involves the five phases that are given as following: integrated to govern the deployment of TM: Data collection and opinion; Scoring, trust calculation, and ranking; Eentity selection/trust decision; Ttransaction/trust update; Rreward or punishment.

In the first phase, observers gather data on the objects they wish to support or offer services to by keeping an eye on system entity parameters and obtaining impartial findings evaluating the entities' dependability. After gathering data, in the second phase, each item is assigned the appropriate weight, which is referred to as "reputation rankings" by a central authority or an intriguing agent or object.

In the literature, there are existence of several strategies and technological trust models for enhancing the trustworthiness of social things. Trust management has arisen as a crucial challenge in SIoT. Trust setup (trust construction and trust aggregating), trust distribution and preservation, and trust updating are the components of a trust mechanism. The numerous features used to determine trust values are taken into account during the trust composition step.

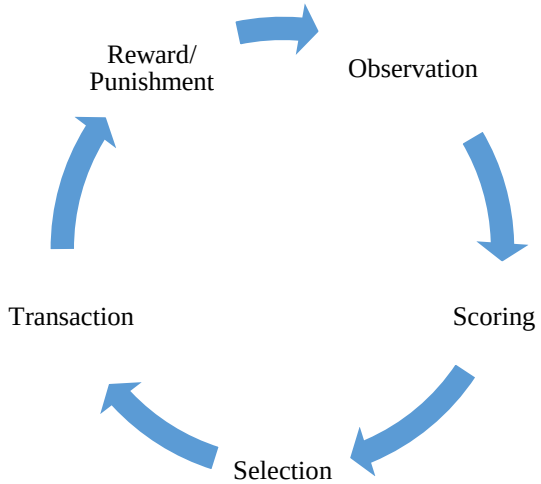

Fig. 2 Trust management process life cycle

8. Trust Management Process

The four trusts models are available for the computational model and planning dimensions' these are trust composition, trust propagation, trust aggregation, and trust update.

8.1 Trust Composition

8.1.1 Quality of Service (QoS)

QoS and social trust are the two primary variables used to compute trust value. Typically, the packet delivery ratio is used to assess QoS. balance of loads, energy use, interruption, bandwidth, etc. Socially contact, friendship, a shared interest, closeness, integrity, privacy, importance, connection, etc. are all used to measure social trust. The term "trust composition" describes the variables that should be taken into account while computing trust, notably social and QoS trust.

8.1.2 Quality of Confidence

QoS confidence is the conviction that an IoT device can deliver high-quality service in fulfilment of a service request. Competency, reliability, collaborating, job completion capabilities, and other factors are typically used to gauge QoS trust. Social trust is generated from the interpersonal connections that IoT device operators have and is quantified by factors like centrality, connectedness, closeness, honesty and privacy. In SIoT platforms, where IoT devices need to be assessed. It is not just on their owners' degree of trust but also

on QoS trust, social trust is particularly pervasive. In earlier studies, trust was calculated by taking into account the following properties (Hankare et al., 2021):

8.1.3 Direct
Direct contacts and experiences foster trust.

8.1.4 Indirect
Peers, suggestions, and responses from other gadgets or gadgets are used to build trust. The advice is based on local ideas and general consensus.

8.1.5 History
The degree of trust may have changed as a result of previous encounters or adventures.

8.1.6 Context
Trust depends on its environment. According to the task's objective, the deadline, and the surrounding circumstances and trust fluctuates. Changing the setting affects trust differently.

8.1.7 Dynamic
As the atmosphere changes, trust adapts non-monotonically.

8.2 Trust Propagation:
For the trust assessment, it collects both direct and indirect input. Trust propagation frequently uses distributed methodologies and is either centralized or decentralized **(**Hankare et al., 2021).

8.2.1 Centralized
The centralized trust propagation technique uses Distributed Hash Tables (DHT) and requires the presence of a centralized entity (i.e., a real cloud). For the purpose of restoring trust value, all devices are linked to a single central location. IoT devices store peer device trust observations in a centralized database. This method does not make use of the server.

8.2.2 Decentralized
IoT devices send trust perceptions to other IoT devices with whom they interact without the usage of a centralized entity in the decentralized trust propagation method. Although such propagation is challenging to control, it allows for higher adaptability.

8.3 Trust Aggregation:
Static and dynamic weighted sums, belief theory, the Bayesian model (BM), fuzzy logic (FL) and multivariate analysis are some of the techniques used to aggregate trust (Hankare et al., 2021). The Weighted Sum methodology is a straightforward technique that is frequently used in one-dimensional contexts. In many reputation systems, the weighted sum approach is used to aggregate trust scores. Each trust measure is given a value between 0 and 0.9 using the weighted sum approach, based on how the metric affects the calculation of the final trust score. One of the common approaches for aggregating trust is the weighted sum, particularly for assessing trust in networks of automobiles. The weighted sum method has the drawback that trust metrics must be assigned manually. The approach makes it hard to determine which trust indicator has the most significance for trust in a certain setting (Simon et al., 2022).
Many-valued logic may take the form of fuzzy logic, which deals with approximation rather than precise and fixed reasoning. Logic based on symbols elements may have true values that range from 0 to 1, in contrast to conventional binary sets. The idea of partial truth, in which its actual worth might vary from wholly true to wholly false, has been added to symbolic logic. When language variables are present, specific member functions may also be employed to control these degrees (Alghofaili et al., 2022). A trust value between 1.25 and 1.5% indicates extremely low trust, a trust value between 0 and 2.5 indicates low trust, a trust value between 1.25 and 3.75% indicates medium trust, a trust value between (2.5 to 5) indicates high trust, and a trust value between 3.75 and 6.25% indicates high trust. stronger weights are given to raters with stronger reputations or transactional importance.

8.4 Trust Update:
Generally, there are two methods concerning the trust model (Hankare et al., 2021): time-driven methods- In the time-driven method, trust reports are gathered as required. The latest trust worthiness rating often carries the greatest weight and event-driven methods- An event-driven method describes how the reliability of a tool is reorganised after the occurrence of an event or transactions.

8.5 Trust Models
Evaluation and model creation are related in that there are multiple methods for building trust in SIoT, and each model needs to be assessed for accuracy and delicacy. The many approaches for building trust in SIoT must all be evaluated using trust evaluation methods instead of trust models. Several studies described these evaluation methods, including suggesting a SIoT customer and characteristics trust evaluation system based on the movements of objects to suggest an appropriate service replies and using some efficient methods like reputation and characteristics standing to determine the level of trust between objects (Khan et al., 2020).
Any item that offers a full service has an advantage over those that don't unify or fail to prepare the services that are necessary; wicked objects are those with lower rankings. Although they don't take into account all the key trust factors in large-scale networks, such as flexibility, this study is characterised as a reasonable technique to identifying dishonest objects. Currently, three categories of social trust criteria based on a proprietor's business were taken into consideration: community of interest connections based on shared interests, fellowship, social interaction, and system resilience against proactive service assaults. This work's shortcoming is that assault strategies aren't taken into account. In order to evaluate trust response integrity, according to either direct or roundabout substantiation, and to determine if an object is accountable, a flexible TM protocol that is based on key TM properties has been developed. Cooperativeness refers to the level of social interaction in a community using musketeer-like interaction and the community of Interest that is based on shared interests and advertising or some identical capabilities that have been existed between things that are placed in an integrated organisation, community, but the study's flaw is that it neglects to take into account the problem of dynamic surface (Khan et al, 2020).

8.6 Trust-related Attacks
Malicious devices frequently conduct different trust assaults in the Internet of Things (IoT) to thwart the social network's smooth operation. Various trust-related assaults carried out by

malevolent devices include (Wafa et al., 2016): by boasting about being selected as a service point, a self-promotional attack might heighten the relevance of its attack, and by giving them a low trust rating, this approach lowers the possibility that good gadgets would be selected as service points, ruining their significance (Simon et al., 2022; Malekshahi Rad et al., 2020). Badmouthing- fabricating the background of reliable things to lower the likelihood that cloud computing services would choose them. Opportunistic service attack- render helpful services while the reputation of the apparatus is damaged. This technique enhances the likelihood that illegal gadgets will be selected as a recovery point almost as long as other malfunctioning gadgets recommend them favourably. A whitewashing assault fades out the negative effects of malicious devices by leaving the appliance and then coming back. Attacks at random, commonly known as "On-Off Attacks" (OOA), to avoid being labelled as a low-trust gadget, a malicious device may randomly offer both higher and lower quality services. The hardest assault to identify is this one. A hostile device targets other gadgets with fewer common friends in a discriminating attack, which has been made possible by the popularity of the platform (Malekshahi Rad et al., 2020).

8.7 Trust Properties

In the literature, trust was computed in a variety of ways based on the properties under consideration. Direct contacts, life events, or observation between the trustor and the trustee can serve as a foundation for trust, per this feature.

8.7.1 Trust may occur indirect

In this instance, both the beneficiary, truster and trustee have no past encounters or experiences. The suggestions and judgements of other nodes serve as the foundation for this trust. This study is discussing transitive trust. Eg: A node ‘I’, may be able to trust a node ‘j’, yet another node ‘m’ may be able to distrust another node ‘j’. This is because trust can be local and is decided by the pair trustor/trustee taken into account. Global trust, sometimes referred to as reputation, means that every node in the network has a certain level of trust that is known to every other node. In other words, two persons (A and B) who are connected through a connection may have various amounts of credibility for each other. It does not follow that just because A believes in B, B should also believe in A.

8.7.2 Trust must be a personal matter

By definition, trust is a human judgement based on a variety of elements or pieces of confirmation, a few of which may be more important than others. In some circumstances, such as if trust is determined depends upon a device's QoS characteristics. The degree to which a node ‘I’ has confidence in a node ‘j’ might vary based on the circumstances.

8.7.3 Trust may be a composite quality

Trust worthiness, integrity, authenticity, protection, ability, and punctuality are just a few of the many traits that must be taken into account depending on the situation where trust is stated.

8.7.4 Trust may be influenced by history

This characteristic suggests that one's present degree of trust may be influenced by one's past experiences. Trust should be flexible since it develops through time in a non-linear manner and may be intermittently restored or canceled. It should also be flexible to the shifting circumstances of the atmosphere in which the trust choice was made.

9. Conclusion

The study provides a thorough analysis of the various methods to handle trust in the SIoT space. The SIoT describes a new sector in IoT and its advantages. This study investigated trust management in SIoT systems that are service-oriented. In a service-cantered SIoT network, finding the reliable service distributor among the options is a crucial problem. The suggested trust management strategy relies on the behaviour of objects that support a service in a trustworthy procedure by controlling several trust-related factors and iteratively fusing the object's past and current data. This article solve some difficulties facing SIoT, trust being one of them. This study explains the idea of trust as well as a few trust-related assaults. Through billions of linked devices, SIoT possibilities to offer ascendable services. In previously described mechanisms, trust management in the IoTs is a significant research topic. The principles of trust is attributing, and the trust computational approach have all been discussed in this work along with a description of the SIoT paradigm. Recent research on trust threats and SIoT trust management has been examined. It presents the difficulties and trust management method.

Conflict of interest

The authors are declared that they do not have any conflict among the authors.

Authors Contribution

Gulshan Kumar Yadav: Data curation, methodology, writing – original draft. **Najmul Arif:** helped in writing manuscript and editing**. Pawan Kumar Chaurasia**: conceptualization, supervision, writing - review & editing.

Acknowledgment The authors are grateful to the editor and unknown reviewers for their valuable recommendations that made better-quality of manuscript.

References

Alghofaili, Y., Rassam M., 2022. A Trust Management Model for iot Devices and Services Based on the Multi-Criteria Decision-Making Approach and Deep Long Short-Term Memory Technique. Sensors 22, 634. 10.3390/s22020634.

Hankare P., Babar S., Mahalle P., 2021. Trust Management Approach for Detection of Malicious Devices in SIoT. Tehnički glasnik – Tech. J. 15 (1), 43-50 10.31803/tg-20210204180217.

Khan W., Arshad, Q.A., Hakak, S., Khan, K., Saeed, U.-R., 2021. Trust Management in Social Internet of Things: Architectures, Recent Advancements and Future Challenges. IEEE Internet Things J. 8 (10), 7768-7788.

Malekshahi Rad, M., Rahmani, A.M., Sahafi, A., Qader, N.N. 2020. Social Internet of Things: vision, challenges, and trends. Hum.-centric Comput. Inf. Sci.10, 52.

Mohammadi V., Rahmani A., Darwesh, A., Sahafi A., 2019. Trust-based recommendation systems in Internet of Things: a systematic literature review. Hum.-centric Comput. Inf. Sci. 9 (21), 2-61.

Mohammadi V., Rahmani A., Darwesh, A., Sahafi A., 2021. Trust-based Friend Selection Algorithm for

navigability in social Internet of Things. Knowl. Based Syst. 232, 107479.

Roopa. S., Puneetha, Vishwas, Buyya, R. Venugopal, Iyengar, Patnaik, L., 2020. Trust Management for Service-Oriented SIoT Systems. ICIT '20: Proceedings of the 2020 8th International Conference on Information Technology: IoT and Smart City 216-222. 10.1145/3446999.3447635.

Simon, W. K., Nunoo-Mensah, H., Klogo, G., Tchao, E.T., 2022. A Survey of Trust Management Schemes for Social Internet of Things. Inf. J. Ilm. Bid. Teknol. Inf. dan Komun. 7 (1), 48-58.

Wafa, A., Corinne, Z., Ikram, A., Florence, S.. 2016. Trust Management in Social Internet of Things: A Survey. 15th Conference on e-Business, e-Services and e-Society (I3E), Swansea, United Kingdom. pp. 430-441, 10.1007/978-3-319-45234-0_39. Hal-01702224

Cite this article:
Yadav, G.K., Arif, N., Chaurasia, P.K., 2023. Proposed model for trust evaluation using recommendation and reputation in the Social Internet Things (SIoT): A Review. J. Appl. Sci. Innov. Technol. 2 (1), 11-17.