ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803/tg-20210204180217

Original scientific paper

Trust Management Approach for Detection of Malicious Devices in SIoT

Priyanka Hankare*, Sachin Babar, Parikshit Mahalle

Abstract: Internet of Things (IoT) is an innovative era of interrelated devices to provide services to other devices or users. In Social Internet of Thing (SIoT), social networking aspect is used for building relationships between devices. For providing or utilizing services, devices need to trust each other in complex and heterogeneous environments. Separating benign and malicious devices in SIoT is a prime security objective. In literature, several works proposed trust computation models based on trust features. But these models fail to identify malicious devices. This paper focuses on detection of malicious devices. In this paper, basic fundamentals, properties, models and attacks of trust in SIoT are discussed. Up-to-date research distributions on trust management and trust attacks are reviewed and idea of Trust Management using Machine Learning Algorithm (TM-MLA) is proposed for identification of malicious devices.

Keywords: IoT; SIoT; Trust Attacks; Trust Management; Trust properties

1 INTRODUCTION

IoT comprises of large number of devices with ability to sense, gather and produce information from the world around us. The devices interact with one another to deliver wide range of smart services that are utilized by users, manufacturers, and other devices to carry out daily activities [1]. IoT has applicability in many domains like healthcare, smart home and workplaces, intelligent transportation systems, environment monitoring etc. Each device in IoT plays the role of service provider, service requestor, or both. To establish trusted relationships between devices, social networking aspect is used in IoT and this paradigm is called as SIoT. SIoT comprises of various devices/things to gather data, offer services, provide recommendations, make verdicts, and take actions. It has an imperative impact to refresh new advancements of medical services, medical robotics and medical embedded sensor [2]. SIoT also used in crowd-sensing applications [3], coastal management system [4].

In SIoT, the social networking of device owners is used to establish trustworthy social relationship among devices. There are different SIoT relationships among devices. They are:

1. Parental object relationship (POR) exists if devices are owned by the same manufacturer.
2. Co-location object relationship (CLOR) set up among devices if devices are present in a same location.
3. Co-work object relationship (C-WOR) built up between devices working collectively to give a common IoT application.
4. Ownership object relationship (OOR) set up if devices (laptops, smart phones, printers etc.) belong to the same owner.
5. Social object relationship (SOR) exists if devices owners get in touch with one another occasionally or frequently (e.g., devices owned by friends, classmates, colleagues).

Trust performs a key role in IoT. For example, IoT enables real-time alerting, tracking, and monitoring about patient's conditions to doctors. But if the information is not notified on time to doctor by IoT devices, it will be dangerous. So, it is essential to find trustworthiness of device in a network. Security and secrecy are the fundamental encounters in the IoT network. Misbehaving devices may carry out trust attacks based on misuse of trust. In order to fulfil SIoT full deployment the following trust management criterion must be discussed:

1. *Identity*: Identity management handles authentication as well asauthorization. Each device in SIoT has a unique identity. The device hiding its real identity must be detected. Access to SIoT devices, routing information must be authorized.
2. *Availability:* States that SIoT characteristics, SIoT entities, networks and services should be always up to date and work accurately even with failure or malicious attacks on system.
3. *Confidentiality:* It avoids the illegal access to the data and preserves the authorized control on system.
4. *Integrity:* Ensures that data and routing information have not been altered while transferring in a network. The trustee sticks to a bunch of ethics that enables the trustor to accept that the trustee is not malevolent.
5. *Data and Privacy:* The large amount of data is exchanged, shared, processed in SIoT network. In this context, unauthorized access to information is possible. Privacy requirement ensures that identities of SIoT devices must be highly protected from illegal access.
6. *Trust:* Trust could be well estimated in order to find appropriate trustee which can provide the best service for given task of a trustor. Trust management systems have to detect non-trustworthy behavior of device and separate untrusted devices from trusted one.

To date there is a little work on SIoT. Existing methods fails to identify trustworthy and untrustworthy devices. Detecting untrustworthy device is tricky task. In this paper, *Trust Management using Machine Learning Algorithm (TM-MLA)* is proposed to detect malicious device. Paper explores the evolutionary history of trust management for SIoT, examines the SIoT studies and come up with the challenges and idea of TM-MLA.

The paper is organized as follows: Section 2 and 3 discussed research distributions which offer solutions to the trust management and trust attacks in SIoT respectively. Section 4 provides the holistic view on trust management in SIoT, trust model and trust attacks. Section 5 presents the challenges in SIoT. An idea of TM-MLA for detection of malicious devices is presented in Section 6. Evaluation and experimental setup are discussed in section 7. Lastly, Section 8 concludes the paper.

2 EXISTING RESEARCH IN IOT TRUST MANAGEMENT

Chen et al. [6] proposed adaptive trust management protocol in a view of social relationships like using honesty, cooperativeness and community of interest. The protocol defends misbehaving attacks. This protocol is not tested against multitude of dynamically changing atmosphere situations. Trust update depends on recommender node.

Chen et al. [7] proposed an adaptive IoT trust protocol for SoA based IoT systems with adaptive filtering technique. This protocol includes SIoT constraints like scalability, storage and computational costs of devices. For assessing social similarity and filtering trust feedback based on social similarity, three social relationships, i.e., friendship, social contact, and community of interest are considered. This trust protocol is resilient to attacks such as SPA, BMA, BSA and OSA. However, this approach doesn't consider QoS trust factor for trust composition.

Truong N. B. et al. [8] proposed a trust prototype with three aspects that is Reputation, Recommendation, and Knowledge. This prototype finds the trustworthy devices by setting a trust channel between devices and improves the network performance. Only trustor's preferences are taken into account for the calculation of trust score. But trustee's factors like opinion, willingness, and capability are also important for trust calculation. This approach doesn't put forward clarification to confirm the adaptability of the SIoT system.

Ikarm Ud Din et al. [9] did investigation of trust managing practices for IoT. Contributions and limitations of these techniques are presented in a different perspective. This paper provides an overview of how different systems fit together without examining different standards to bring preferred functionalities.

Juan Chen et al. [10] developed a trust architecture by taking into account the technique of Soft Defined Network (SDN) in IoT, and a cross-layer authorization protocol based on IoTrust. Behavior-based Reputation Evaluation Scheme for the device (BES) and an Organization Reputation Evaluation Scheme (ORES) are used for trust establishment. Hypothetical analysis signifies that the developed trust architecture can resilient to modification attack, replay attack, and message dropping attack. This architecture does not work well on heterogeneous devices.

Xiao H et al. [11] proposed a trust model for SIoTon the basis of guarantor and reputation. Credit and reputation are the two parameters used by the model. Every device has its own reputation stored in it. If device provides accurate results then he is rewarded. If device is defective then he has to provide some rewards to other devices. This approach provides same trust value for all devices owned by same user. Storage, computing capacity of objects and energy consumption are the limitations of this model.

Zhiting Lin et al. [12] built a trust model on 5 aspects: 1) mutuality of trustor and trustee; 2) inferential transfer of trust; 3) transitivity of trust; 4) trustworthiness update; and 5) trustworthiness affected by dynamic environment. Behavioral changes in devices, membership changes and the changes in working patterns are considered in this model.

Upul Jayasinghe et al. [13] built a trust model classifier using SVM algorithm into two classes, trustworthy and untrustworthy. For calculation of trust scores, knowledge, experience and reputation trust metrics are used. Event based trust update scheme is used.

Anuoluwapo A. Adewuyi et al. [14] built a trust model, CTRUST for collaborative applications. Trust decay and belief functions are used in model for decaying the past trust values with time and guiding the acceptance of trust recommendations from another node respectively. The model assigns weights to the trust metrics as per their importance. However, the privacy aspects are not considered.

Abdelghani et al. [15] presented a trust management system to detect the malicious devices, block and isolate them using supervised approach of machine learning algorithm. Subjective trust features like Reputation, honesty, quality of provider, similarity, direct experience, rating frequency and rating trend etc. are used to calculate trust score.

Hui et al. [16, 17] implemented a contextualsystemto find out trusted device in SIoT. To calculate the trust between IoT objects and their owners, system considers the concepts from social and physiological science.

Muhammad Ajmal Azad [18] implemented the trust model for preserving privacy of IoT devices as well as user is. The trust score is updated in self-enforcing manner without help of third party. Social relationship between users as well as devices is considered by this model.

Table 1 Categorization of existing research according to SIoT relationship type

Reference paper	Relationship Type	
	Device to device relationship	User to user relationship
[6]		✓
[7]		✓
[8]		✓
[11]		✓
[18]	✓	✓

Tab. 1 summarizes the existing research from relationship type viewpoints. It shows that mostly user to user relationship is considered for trust management. But SIoT network has two important components, user and device. Hence, the social relationship between user-user, device-device and user-device must be taken into account for calculation of trust.

3 EXISTING RESEARCH IN IOT TRUST ATTACKS

Jean Caminha et al., [19] initiated a SIoT method on the basis of machine learning and an elastic slide window method that enabled to detect OO attacks (RA) in IoT. This method differentiates attacker devices from broken devices.

Truong et al., [20] presented a trust composition technique integrated with social trust metrics of the SIoT components such as common interest, cooperativeness and honesty similarity. To calculate weighted sum direct views, global judgements, and personal experiences are used through Bayesian technique. The scheme prevents attacks such as BMA, BSA and SPA. Reputation of device is not considered while trust computation.

Chen et al., [21] presented an access service recommendation scheme for effective service composition in SIoT environment. For trustworthiness analysis of SIoT devices a coherent recommendation metric is introduced. This approach defends attacks such as BMA, BSA and SPA. In this scheme, an energy aware mechanism is taken into account for SIoT privacy and load management. However, SIoT limitations such as device space, scalability and processing capacity have not been considered.

Abderrahim et al. [22] proposed a trust management system that integrates direct-indirect trust, transaction factors and social modelling of trust. This model is resilient to OOA attacks. Kalman filter technique is used to measure trust value and defend probable attacks.

Mariam Masmoudi [23] proposed a trust evaluation model to find out malicious devices using deep learning technique. Subjective trust features like Reputation, honesty, quality of provider, similarity, direct experience, and rating frequency etc. are used to calculate trust score. This approach defends attacks such as BMA, BSA and SPA, DA. However, Specific set of features are used for detection of malicious devices.

Tab. 2 summarizes the existing research from trust attack viewpoints. The features used in literature are not able to identify all types attacks. Specific set of trust features are used for detection of all kinds of attacks. But some features are more related with one type of attack and less with another. For e.g. the similarity has more relation with DA and less with SPA attack.

Table 2 Categorization of existing research according to trust attacks

Ref paper	Trust attacks						
	SPA	BMA	OSA	BSA	WA	OOA	DA
[19]						✓	
[7]	✓	✓	✓	✓			
[20]	✓	✓		✓			
[21]	✓	✓		✓			
[22]						✓	
[23]	✓	✓		✓			✓

Tab. 3 summarizes the existing research on trust features and trust aggregation technique used for trust model implementation. It seems from presented work that there is still lot of work needs to be done in the area of trust management. As shown in Tab. 3, trust aggregation is done with dynamic or static weighted sum approach, fuzzy logic and machine learning algorithms. Though the popular choice for trust aggregation is weighted sum approach, where weights can be assigned to trust features as per their importance in transaction, which trust feature makes more influence on transaction is very difficult to identify.

Table 3 Categorization of existing research according to trust features and aggregation techniques

Ref paper	Trust Features	Trust Aggregation Technique Used
[6]	Honesty, Cooperativeness and Community of Interest	Weighted Sum
[7]	Friendship, Social Contact, and Community of Interest	Bayesian Model
[8]	Reputation, Recommendation, and Knowledge	Fuzzy and Multi-Criteria Utility Theory
[11]	Social Cooperativeness	Probability
[20]	Cooperativeness, Community-Interest, Honesty and Similarity	Weighted Sum
[21]	Coherent Recommendation	Weighted Sum
[22]	Community of Interest	Weighted Sum
[13]	Knowledge, Experience and Reputation	Machine Learning Algorithms

4 TRUST MANAGEMENT IN SIoT

The concept of trust has been studied in numerous fields like psychology, sociology, computer science etc. Each of these fields gives different aspect of trust. Trust is estimate of various qualities like honesty, cooperativeness, willingness, expectation, faith, confidence. Trust has two important entities: trustor and trustee. The trustor has a goal, its own need. It entrusts the trustee by evaluating trustee's competence and willingness.

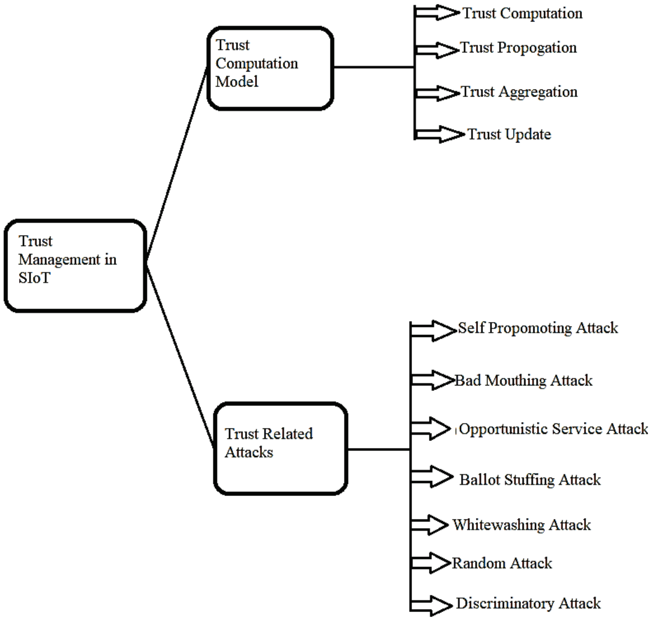

Figure 1 Trust management in SIoT

In today's world so much data is shared among community using devices like apps, computers, sensors, cameras etc. If data is shared with non-trusted clients/devices, it may be used for malicious purpose. For example, Charlie (the trustor/evaluator) wants to use Carlos (the trustee/performer) images placed at Carlos device. Charlie trusts Carlos so he is confident that he will get the images form Carlos device. But at the same time Carlos needs to ensure that Charlie will not misuse the images. It is important that the receiver as well as sender must trust each other for healthy exchange of data. Trust management becomes a supreme question in SIoT for assurance of reliable trust model and improved object's security [5].

In our study, the trust management is considered from two perspective: trust computation model and trust attacks. Fig. 1 depicts the proposed framework of trust management in SIoT.

4.1 Trust Computation Model

The design dimensions of trust model are: trust composition, trust propagation, trust aggregation and trust update.

4.1.1 Trust Composition

QoS (quality of service) and social trust are the two main ways to determine the trust value. QoS is usually measured by packet delivery ratio, load balance, energy consumption, delay, bandwidth etc. Social trust is estimated by factors like social contact, friendship, community of interest, intimacy, honesty, privacy, centrality, and connectivity etc. In previous research [6-8, 11], trust was computed by considering following properties:

a) Direct: Trust established on direct experiences, interactions.
b) Indirect: Trust constructed on recommendations, feedbacks from other devices or peers. The recommendation relies on surrounding suggestions and global opinions.
c) History: Past interactions or experiences may have impact on present trust level.
d) Context: Trust is context dependent [5]. Trust changes depending on (i) target of task, (ii) time span, and (iii) environment. Trust varies if context is changed.
e) Dynamic: Trust changes non-monotonically with varying situations of environment.

4.1.2 Trust Propagation

It gathers the direct observations and indirect feedbacks for the trust evaluation. Centralized and distributed approaches are used for trust propagation.

a) Centralized approach: For restoring trust value, all devices are connected to centralized entity (e.g physical cloud).
b) Distributed approach: IoT devices store trust observations towards their peer devices. Centralized server is not used by this approach.

4.1.3 Trust Aggregation

Trust is aggregated using methods like static and dynamic weighted sum, Belief Theory, Bayesian Model (BM) and Fuzzy Logic (FL), Regression Analysis.

4.1.4 Trust Update

In general, there are two approaches involving the trust model: time-driven approaches and event-driven approaches. In the time-driven approach, trust reports are collected occasionally. Usually, the latest trustworthiness assessment gets bigger weights. Event-driven approach refers to a device trustworthiness that restructured after an event or transaction is made.

4.2 Trust Attack

Misbehaving or Malicious devices attack SIoT system to disrupt the functionality of SIoT network operations. Different trust related attacks performed by malicious devices are as follows:

1. Self-promoting attack (SPA): can boost its significance by bragging itself in order to be chosen as a service point.
2. Bad mouthing attack (BMA): reduces the likelihood of good devices to be chosen as service points as prominence of these devices are ruined by providing bad trust evaluation against them.
3. Opportunistic service attacks (OSA): perform good services when device reputation falls.
4. Ballot stuffing attack (BSA): increases the chance of malicious devices to be chosen as a service point as good recommendations are provided by other defective devices to them.
5. Whitewashing attack (WA): fades out malicious devices bad image by exiting from the application and then returning again.
6. Random attacks (RA): also called as On-Off Attacks (OOA). A malicious device can provide better and poor services randomly to avoid being rated as low trust device. This attack is hardest to detect.
7. Discriminatory attacks (DA): perform by malicious device on other devices having fewer common friends.

5 CHALLENGES OF SIOT

SIoT faces following number of challenges of trust management.

1. Device capability

Previous trust management solutions can't be applied directly to all SIoT applications as devices are having different computational power, storage capacity, standard, communication stacks, operating system, I/O channels. Trust management algorithm should take into consideration all such device requirements.

2. Handling large network

Communication between devices produces large number of transactions. Existing systems does not scale well to handle such large number of transaction information. The trust management algorithm should be powerful to control the giant number of devices as well as communication between them.

3. Existing device leaving and new device joining

SIoT system evolves with existing device leaving and new device joining. So, trust management algorithm should consider dynamicity of device like changeable behaviour of device, their membership changes, interaction pattern changes, network topology changes and location changes.

4. Finding trustworthy device

With rising number of devices, it's very difficult to find out trustworthy devices. SIoT makes human's life more comfortable. In today's world so much data is shared among community using devices. If data is shared with non-trusted clients/devices, it may be used for malicious purpose. So, there is a need to design algorithm specifying rules which identify trusted and malicious behaviour of a device and hence enable sharing in controlled manner to avoid malicious attacks.

5. Selection of trust features

Trust is an important challenge in SIoT where device needs to find correct trustee for healthy exchange of data between them. Selecting appropriate trust features is necessary in trust management as accuracy, performance of trust systems depends on this. As shown in table III, specific set of trust features like reputation, honesty, community of interest, similarity, rating frequency are considered for the calculation of overall trust value. The literature work stated in section 2 and 3 rates the best device in SIoT network but fail to detect attacks performed by malicious device. Lastly, in the earlier systems [6, 7] the dynamic change in trust feature criteria is not considered while trust computations. For more accuracy of trust computation there is need to change the features of trust dynamically based on importance of transaction.

6. Trust aggregation

As shown in Tab. 3, most of the previous approaches used weighted sum approach for aggregation of trust values. However, there are numerous shortcomings in this practice. There are several likelihoods when it comes to assess a weighting factor. Systems fails to recognize which feature makes the most impact on trust in specific setting as weights assigned to trust features may vary from one to another. This approach cannot identify malicious and benign behaviour of node. Hence machine learning approach is used for combining the trust scores and detection of malicious devices in this research.

7. Trust update

In [6, 24, 25], the trust update depends on recommendation of other node i.e. the trust update score is computed using value provided by another node or recommender. But what if the recommender node is malicious? In [6, 18, 26, 27] the trust is updated based on previous experience or trust score and ability of node. The ability of device is calculated from his performance in previous task i.e. gain/damage after performing task or good conduct or bad conduct of device or successful/unsuccessful communications, packet received and differentiation etc. What if for longer time there is no interaction among trustor and trustee? It is necessary to take into account the time elapsed for previous interaction while updating the trust. In [14], the trust is decayed if there no interaction between nodes. The trust decay is applied on trust features like recommendation, previous trust value. When new session of interaction is made, previous trust value is decayed. The overall trust is updated based on previous trust effectiveness, direct assessment, and recommendation. Previous trust effectiveness is calculated based on number of interactions in the time interval. After every new interaction with j, previous trust is updated. But what if the node *j* becomes unavailable in the network, and node *i* gets no next chance of interaction with node *j* or *i* provides recommendation to *k* about *j* before next interaction with *j*. In such cases, *i* will provide old trust value. Hence time driven trust approach is used in our research

6 PROPOSED MODEL

The TM-MLAwill focus mainly on fifth, sixth and seventh challenge. TM-MLA will be implemented using trust features as per attack context and dynamically varying surrounding situations to detect the malicious devices. Five attacks will be considered in the proposed model: 1. SPA; 2. BSA; 3. BMA; 4. DA; 5. OSA. Fig. 2 depicts the system architecture.

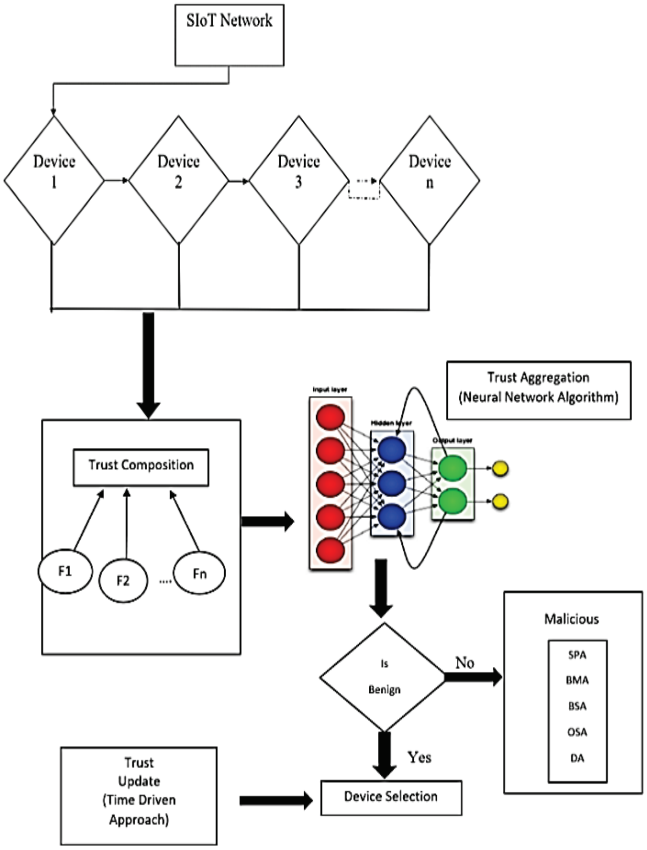

Figure 2 System architecture

TM-MLA will consist of mainly three phases - trust composition, trust aggregation and trust update phase.

- In trust composition phase different features will be chosen as per the context of attack. For trust computation process, the trustee node will be selected from the set of nodes based on trust features.
- In trust aggregation phase machine learning based approach, Artificial Neural Network (ANN) algorithm

will be used to get the trust score to defeat the drawback of past trust aggregation techniques. At the output layer of ANN, a probability is derived which decides whether the trustee for given task of trustor is malicious or benign. After selection of trustee node, the trustor will assign a task to trustee.

- In trust update phase, time driven approach will be used for updating the trust score. In this approach, previous or stored trust values of a device will decay with time and more weightage will be given to latest trust values. After certain number of times, the previous trust values will no longer relevant. The Eq. (1) will be used to decay the trust over time. Depending on result given by trustee for the assigned task, the trust will decay.

$$T_{kl}(\text{current}) = \left(T_{kl}(\text{initial value}) \times (1 - Decay\_rate)\right)^{x} \qquad (1)$$

Where: T_{kl}(current) - current trust estimation T_{kl} of trustee node l by trustor node k at time t; T_{kl}(initial value) - trust estimation value at initial time; *Decay_rate* - rate at which trust decays; x - duration required to decay trust value as per decay rate.

After training stage, the model will be utilized to assess the performance of algorithm to detect the trust related attacks.

Table 4 Dataset

Trustor Device	Type of Request	Trustee Device	Trust Features						Trust Score	Malicious (M) or Benign (B)
A	Image	B	-	-	-	-	-	-	0.85	B
B	Video	C	-	-	-	-	-	-	0.33	M
-	-	-	-	-	-	-	-	-	-	B
C	Location request	A	-	-	-	-	-	-	0.68	B

7 RESULT AND ANALYSIS

There are two main parts in SIoT: 1. Devices; 2. Users. $D = D1, D2, \ldots, Dn$ are the set of devices owned by users in network and $U = U1, U2, \ldots, Un$ are the set of users of SIoT network. The Fig. 3 depicts the idea of SIoT network. The communication between users and devices is shown by using the edges between them. Each device will provide services to the users or other devices. For evaluating the performance of proposed model, the data of Facebook, Quora, and Twitter social network will be considered. The request-response patterns, task sharing, interactions among devices will be analyzed for the creation of dataset. This information will be stored in table format as shown in Tab. 4.

The real-world network will be formed between devices like mobiles and laptops. 10,000 records will be used for implementation. Out of 10,000, 80% of the data will be used for training and 20% will be used for testing. To train the model collaborative filtering approach will be used. Theproposed model will find potential trustees for given task of trustor, detect malicious or benign devices in SIoT network.

After implementation of model, the correctness will be analyzed in two ways: 1. By comparing the model with previous approaches and 2. By calculating the accuracy of model using precision, recall, and *F-measure* methods. *Precision* (or positive predictive value) is the ratio of count of accurately-detected-matching records to the count of pair of records that were detected as matching. It is shown in Eq. (2).

$$Precision = \frac{TP}{TP + FP} \qquad (2)$$

Recall (or sensitivity) is the ratio of count of accurately detected matching records to the total count of matching records in the test set. It is shown in Eq. (3).

$$Recall = \frac{TP}{TP + FN} \qquad (3)$$

Where: *TP* (true positive) refers to matching instances that are correctly identified as matching by algorithm. *FP* (false positive) refers to non-matching instances that are erroneously-detected as matching. *FN* (false negative) refers to matching instances that mislabeled as non-matching.

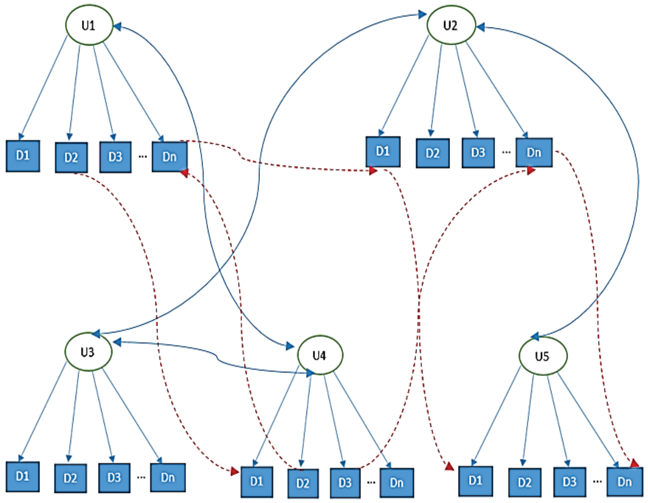

Figure 3 SIoT network

F-measure as shown in Eq. (4), is a combination of precision and recall. It is calculated by taking harmonic mean of precision and recall.

$$F\text{-}measure = \frac{2 \times Precision \times Recall}{Precision + Recall} \qquad (4)$$

The average accuracy of the trust models with weighted mean approach [6, 26, 29] is shown in Fig. 4. Our method of trust update does not depend on recommender node. Thus, there is no chance that untrustworthy node will provide fake recommendations to benign node and good recommendations to malicious node. So, TM-MLA defends against BSA, BMA and SPA. Time driven trust decay method declines the trust if there is no interaction or less frequent interaction between trustor and trustee. Therefore, the TM-MLA prevents OSA and DA attack. Hence proposed algorithm surely maximizes the accuracy by giving better recall i.e., a TPR, lower FPR and higher TNR as ML based approach is used for trust aggregation. Confusion matrix will be used to exhibit the efficiency of our model against weighted mean methods.

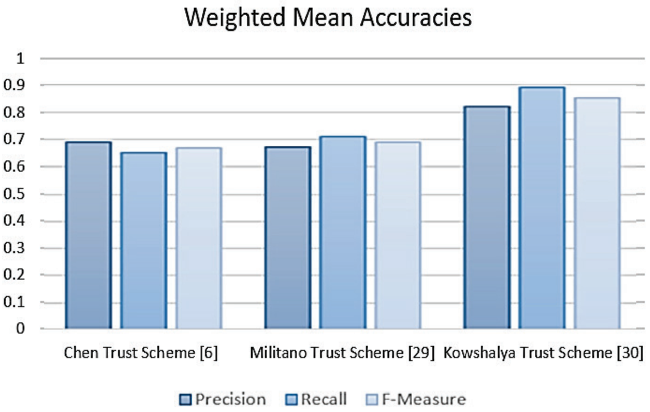

Figure 4 Comparison of Trust Estimation accuracies

8 CONCLUSION

SIoT assures to provide scalable services with trillions of interrelated devices. Trust management in SIoT is an important research issue in previously proposed mechanisms. In this paper, the overview of the SIoT paradigm, basic fundamentals of trust, its properties and trust computation model has been presented. The latest research studies on SIoT trust management and trust attacks have been reviewed. The challenges and trust management model are presented. TM-MLA will detect the malicious devices performing attacks on a system. As trust features will be chosen according to attack context, the better and strong results will be achieved. Machine learning based trust aggregation structure used in the TM-MLA model eliminates the traditional shortcomings of weighted sum. TM-MLA removes the drawbacks of previous trust update. So, it's a more dependable method.

Notice

This paper was presented at IC2ST-2021 – International Conference on Convergence of Smart Technologies. This conference was organized in Pune, India by Aspire Research Foundation, January 9-10, 2021. The paper will not be published anywhere else.

9 REFERENCES

[1] Ortiz, M., Hussein, D., Park, S., Han, S. N., & Crespi, N. (2014). The cluster between Internet of Things and social networks: Review and research challenges. *IEEE Internet Things J., 1*(3), 206-215. https://doi.org/10.1109/JIOT.2014.2318835
Hassanien, E., Bhatnagar, R., Eldeen, N., Khalifa, M., & Taha, M. H. N. (2020). Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications. *Springer: Studies in Computational Intelligence book series SCI, vol. 846*. https://doi.org/10.1007/978-3-030-24513-9

[2] Atzori, L., Girau, R., Pilloni, V., & Uras, M. (2019). R2: Assignment of sensing tasks to IoT devices: Exploitation of a social network of objects. *IEEE Internet of Things Journal, 6*(2), 2679-2692. https://doi.org/10.1109/JIOT.2018.2873501

[3] Girau, R., Anedda, M., Fadda, M., Farina, M., Floris, A., Sole, M., & Giusto, D. (2020). Coastal monitoring system based on Social Internet of Things platform. *IEEE Internet of Things Journal, 7*(2). https://doi.org/10.1109/JIOT.2019.2954202

[4] Roopa, M. S., Pattar, S., Buyya, R., Venugopal, K. R., Iyengar, S. S., & Patnaik, L. M. (2019). Social Internet of Things (SIoT): Foundations, thrust areas, systematic review. *Computer Communications, 139*, 32-57. https://doi.org/10.1016/j.comcom.2019.03.009

[5] Chen, I. R., Bao, F., & Guo, J. (2016). Trust-based service management for social Internet of Things systems. *IEEE Transactions on Dependable and Secure Computing, 13*(99), 1-1. https://doi.org/10.1109/TDSC.2015.2420552

[6] Chen, I. R., Guo, J., & Bao, F. (2016). Trust management for SOA-based IoT and its application to service composition. *IEEE Transactions on Services Computing, 9*(3), 482-495. https://doi.org/10.1109/TSC.2014.2365797

[7] Truong, N. B., Um, T. W., & Lee, G. M. (2016). A reputation and knowledge-based trust service platform for trustworthy social internet of things. *Innovations in Clouds, Internet and Networks (ICIN)*, Paris, France.

[8] Kim, B.-S., Hassan, S., & Khan, M. K. (2018). Trust management techniques for the Internet of Things: A survey. *IEEE Access, 7*, 29763-29787. https://doi.org/10.1109/ACCESS.2018.2880838

[9] Chen, J., Tian, Z., Cui, X., Yin, L., & Wang, X. (2019). Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence and Humanized Computing, 10*(2), 3099-3107. https://doi.org/10.1007/s12652-018-0887-z

[10] Xiao, H., Sidhu, N., & Christianson, B. (2015). Guarantor and reputation-based trust model for social internet of things. *International Wireless Communications and Mobile Computing Conference (IWCMC 2015)*, 600-605. https://doi.org/10.1109/IWCMC.2015.7289151

[11] Lin, Z. & Dong, L. (2018). Clarifying trust in social Internet of Things. *IEEE Transactions on Knowledge and Data Engineering, 30*(2). https://doi.org/10.1109/TKDE.2017.2762678

[12] Jayasinghe, U., Lee, G. M., Um, T. W., & Shi, Q. (2019). Machine learning based trust computational model for IoT services. *IEEE Transactions on Sustainable Computing, 4*(1). https://doi.org/10.1109/TSUSC.2018.2839623

[13] Adewuyi, A. A., Cheng, H., Shi, Q., Cao, J., MacDermott, Á., & Wang, X. (2019). CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things. IEEE Internet of Things Journal, 6(3), 5432-5445. https://doi.org/10.1109/JIOT.2019.2902022

[14] Abdelghani, W., Zayani, C. A., Amous, I., & Sèdes, F. (2019). Trust Evaluation Model for Attack Detection in Social Internet of Things. In: Zemmari A., Mosbah M., Cuppens-Boulahia N., Cuppens F. (eds) *Risks and Security of Internet and Systems, CRiSIS 2018. Lecture Notes in Computer Science, vol 11391*. Springer, Cham, 48-64. https://doi.org/10.1007/978-3-030-12143-3_5

[15] Xia, H., Xiao, F., Zhang, S., Hu, C., & Cheng, X. (2019). Trustworthiness inference framework in the social internet of

things: A context aware approach. *IEEE Infocom 2019 - IEEE Conference on Computer Communications*, 838-846. https://doi.org/10.1109/INFOCOM.2019.8737491

[16] Xia, H., Hu, C.-Q., Xiao, F., Cheng, X.-G., & Pan, Z.-K. (2019). An efficient social-like semantic-aware service discovery mechanism for large-scale Internet of Things. *Computer Networks, 152*, 210-220. https://doi.org/10.1016/j.comnet.2019.02.006

[17] Azad, M. A., Bag, S., Hao, F., & Shalaginov, A. (2020). Decentralized self-enforcing trust management system for social internet of things. *Internet of Things Journal IEEE, 7*(4), 2690-2703. https://doi.org/10.1109/JIOT.2019.2962282

[18] Caminha, J., Perknnusich, A., & Perkusich, M. (2018). A smart trust management method to detect on-off attacks. *Hindawi Security and Communication Networks, Vol. 2018*, Article ID-6063456. https://doi.org/10.1155/2018/6063456

[19] Truong, N. B., Lee, H., Askwith, B., & Lee, G. M. (2017). Toward a trust evaluation mechanism in the Social Internet of Things. *Sensors 17*(6). https://doi.org/10.3390/s17061346

[20] Chen, Z., Ling, R., Huang, C.-M., & Zhu, X. (2016). A scheme of access service recommendation for the Social Internet of Things. *Int. J. Commun. Syst. 29*(4). https://doi.org/10.1002/dac.2930

[21] Abderrahim, O. B., Elhdhili, M. H., & Saidane, L. (2017). TMCoI-SIOT: A trust management system based on communities of interest for the Social Internet of Things. *Wireless Communications and Mobile Computing Conference, IWCMC 2017*, IEEE, 747-752. https://doi.org/10.1109/IWCMC.2017.7986378

[22] Masmoudi, M., Abdelghani, W., Amous, I., & Sèdes, F. (2019). Deep learning for trust-related attacks detection in social internet of things. *International Conference on e-Business Engineering*, Springer. https://doi.org/10.1007/978-3-030-34986-8_28

[23] Abbas, A. H. & Iqbal, F. (2019). Context based trust formation using direct user-experience in the Internet of Things (IoT). *2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, Sydney, Australia, 424-430.

[24] Oualhaj, O. A., Mohamed, A., Guizani, M., and Erbad, A. (2020). Blockchain based decentralized trust management framework. *International Wireless Communications and Mobile Computing (IWCMC 2020)*, Limassol, Cyprus, 2210-2215. https://doi.org/10.1109/IWCMC48107.2020.9148247

[25] Kowshalya, A. M. & Valarmathi, M. L. (2017). Trust management for reliable decision making among social objects in the Social Internet of Things. *IET Networks, 6*(4), 75-80. https://doi.org/10.1049/iet-net.2017.0021

[26] He, Y., Han, G., Jiang, J., Wang, H., & Martinez-Garcia, M. (2020). A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks. *IEEE Transactions on Mobile Computing*. https://doi.org/10.1109/TMC.2020.3020313

[27] Sagar, S., Mahmood, A., Sheng, Q. Z., & Zhang, W. E. (2020). Trust computational heuristic for social internet of things: A machine learning-based approach. *IEEE International Conference on Communication*. https://doi.org/10.1109/ICC40277.2020.9148767

[28] Militano, L., Orsino, A., Araniti, G., Nitti, M., Atzori, L., & Iera, A. (2016). Trusted D2D-based data uploading in in-band narrowband-IoT with social awareness. *IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 1-6. https://doi.org/10.1109/PIMRC.2016.7794568

Authors' contacts:

Ms **Priyanka Hankare**
(Corresponding author)
AISSMS IOIT, Pune
RTO road, Sangamwadi, Pune-411001, India
E-mail: priyankahankare92@gmail.com

Mr **Sachin Babar**
STES, Lonavala
Kusgaon (BK) off. Mumbai-Pune Expressway, Lonavala-410401, India
E-mail: sdbabar@gmail.com

Mr **Parikshit Mahalle**
SKNCOE, Pune
Wadgaon (BK), Pune-411041, India
E-mail: aalborg.pnm@gmail.com