Grenze International Journal of Engineering and Technology, June Issue

Trusted Devices Analysis and Classification Model for Social Internet of Things

Mr. Chethan Raj C[1], Dr.J Hanumanthappa[2] and Ms.Inchara G P[3]
[1]Research Scholar & HoD, Department of Studies in Computer Science, University of Mysore, VTU, Karnataka, India
Email: chethanraj016@gmail.com
[2-3]Department of Studies in Computer Science, University of Mysore, VTU, Karnataka, India
Email: hanums_j@yahoo.com, incharainchu608@gmail.com

***Abstract*— Advanced technology utilization in the heterogeneous device communication in Social Internet of Things (SIoT) field is emerging research area in order to provide efficient communication based on social relationship among the objects in a trusted way. In the field of SIoT in order to establish trusted connection and communication by mitigating from the untrusted activities involved and device participation requires an efficient framework and real time machine leaning model equipped into device intelligence in order classify and also to provide the secure and trust management relationship among the heterogonous interconnected sensor devices. An intelligent solution is needed in an adaptive SIoT environment to identify and classify the malignant and untrusted nodes. Hence efficient trust-based model is required where the trustable nodes are identified using an Intelligent Trust Management Learning Model (ITMLM) for the Social Internet of things is propsed called ITMLM-SIoT. The proposed system integrates numerous factors of trust classification such as direct and indirect trust, transaction factors and other social modeling trust factors. The implementation uses both the human intelligence and device artificial intelligence for trust management classification.**

The proposed system uses a combination of dynamic (interaction-based) and static (graph-based) dataset collection mechanism with reference to object and device communication in an trusted manner that helps in limiting resource overheads of a adaptive & dynamic approach for effective trust model classification by benefiting from its higher accuracy compared to a other existing approach. The paper provides analysis of the trust management model classification and shows the effectiveness of the proposed model in handling different untrust scenarios while requiring limited storage and computational resources in SIoT devices. The proposed machine learning models compares the efficient performance. The proposed model achieved 88.87% and 89.76% of accuracy for the given data set.

***Index Terms*— Social IoT; trust management; Internet of Things services; Trust factor, Trust metric, Trust attribute, Trust classification, Machine learning model.**

I. INTRODUCTION

The Internet of Things (IoT) is spreading faster than any other technology. IoT interconnects the devices ranging from everyday appliances to enterprise infrastructure. Researchers are visualization something greater, such that what if all your devices track your social graph and all of your content were compiled in a way that you could link

Grenze ID: 01.GIJET.10.2.148_1

and manage [27] called as social IoT i.e a complete ecosystem for our connected life. It forms an internet of devices that is centered on persons, building a network beyond IoT into a world of untapped potential at its core. In the real world, user acts as interface between the physical and cyber world, but with exist of IoT, the user is replaced with the system (Automation). In IoT user is not involving in the interaction instead physical world and cyber world interact with each other for specific decision and the status is depends and available on cloud i,e exact action to be taken on the data. In Iot the devices are connected for communication and exchange of the information. In IoT Ecosystem internet is global platform/Backbone. (Iot: Collection of sensor to an embedded devices). The existing SIoT-trust classification are framed based on different trust properties, different trust metrics, nodes distance, cooperative communication and nodes behavior strategy with reference to available social relationship of the smart objects. In this category malignant and misbehaving nodes are identified and learn about the corresponding social object based on the surrounded environment information's acquired through nearest nodes which are impossible in practical approaches. To overcome this problems an efficient classification scheme is required in SIoT networks for trust classification, detection and identification. Imparting novel solutions using intelligence technique for trust classification between devices is concern ultimate choice of designers. In order to increase the robustness and trust between SIoT devices of the system, artificial intelligence algorithms impart positive trust among smart SIoT devices in the network. Social Internet of Things (SIoT) is a paradigm in which the Internet of Things (IoT) concept is not only fused with Social Networks for allowing both people and objects to interact instead SIoT establish communication based on object relationship in order to offer a variety of attractive services and applications. However, with this emerging paradigm the issue is about revealing their data and violating their privacy of devices or data. Without trustworthy mechanisms the SIoT trust management becomes a major challenge to provide qualified services and improved security. Several works in the literature have check with this problem and have proposed different trust-models.

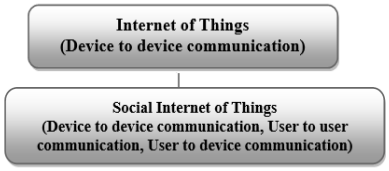


Figure 01: Social Internet of Things

Recently, SIoT technology has emerged in many aspects of life, such as transportation, healthcare, and even education. SIoT technology incorporates several tasks to achieve the goals for which it was developed through smart services. These services are intelligent activities that allow devices to interact with the physical world to provide suitable services to users anytime and anywhere based on the object relationship. However, the remarkable advancement of this technology has increased mechanisms of untrusted nodes and it often take advantage of the SIoTs' heterogeneity to cause trust problems and manipulate the behavior to delude devices' reliability and the service provided through it. Consequently, trust is one of the security challenges that threatens SIoT smart services. Trust management classification and prediction techniques have been widely used to identify untrusted behavior and isolate untrusted objects over the past few years. However, these techniques still have many limitations like ineffectiveness when dealing with a large amount of data with heterogeneous devices and continuously changing behaviors of objects in SIoT network.

II. Related Work

Rapid advancements in communication and computing technologies have let to the evolution of billions of smart objects (e.g., smart machines, smart watch, and smart cars) equipped with sensing, processing, communication capabilities that not only enables an object-object communication across the internet but also forms the well-known paradigm of the Internet of Things (IoT) [1] [2].

This paradigm has undeniably produced enormous business, and opened doors to many applications and services in various valuable sectors [3], and led to a tremendous increase in connected smart objects that are expected to surpass 75.44 billion by 2025 [4]. Furthermore, over the past decade, numerous research endeavors have analyzed the possibilities of integrating the notion of social networking into the IoT ecosystem. This integration has led to a new paradigm of the SIoT, wherein, objects and humans are maintained at social and physical level in order to facilitate the owners of the objects to set the rules for protecting their privacy. Moreover, each object in SIoT is

capable of establishing relationships with other objects in terms of their ownership (relation with the objects belonging to the same owner), social relationship (relation with the objects belonging to the friends in social network), parental relationship (relation with the objects from the same manufacturer), co-location and co-work relationships (relation with the objects from the same location and work environment), and enables autonomous inter-object interaction based on these relationships [5][6].

Trust plays an important role in establishing and maintaining social relationships since social objects only involve themselves in a relationship when the participating objects are trustworthy enough to reduce the probable risk in decision-making [5]. Trustworthy relationships among the objects make it easy for them to only respond to the service requests from the familiar objects in the network, thereby, reducing the exposure to malicious objects [7]. The notion of trust has been studied in many disciplines, i.e., sociology, psychology, and computer science [8][9], nevertheless, the perception of trust in each of these disciplines is different, and therefore, there is no generally acknowledged definition of trust.

In [11], Boa et al. proposed a trust evaluation mechanism, wherein, three trust parameters are considered to evaluate the trustworthiness of an object. The considered parameters are cooperativeness, honesty, and community-of-interest, and to aggregate these parameters, an adaptive weighted sum technique has been suggested. Moreover, their trust model considers direct trust and indirect trust (as recommendations) while quantifying the trust of an object.

Anuoluwapo et al. [12] suggested a dynamic trust evaluation model CTRUST, wherein, objects decide the functional parameters in terms of collaborative context, to estimate the trustworthiness of an object in the SIoT network. Besides, CTRUST includes the decay factor to ensure the trust degradation process more efficiently and in a consistent manner. Nevertheless, weighted trust parameters have been equipped to aggregate the final trust. Each node decides the weights of each parameter at run-time to adjust the trustworthiness of an object in various contexts. Moreover, an adaptive trust protocol for service-oriented architecture is proposed in [13], wherein social similarity and trust feedback are considered to measure the trustworthiness of an object, and the protocol's effectiveness is demonstrated through service-oriented applications. However, an object in the discussed models need to discover the best trust parameters and their respective weights as per the environmental conditions. . There are numerous research works on the trust computational model delineated in the literature targeting different applications of IoT such as vehicular networks [15][16], peer-to-peer networks [17][18], recommendation systems [19][20], and mobile crowdsourcing [21][22].

In SIoT, objects can establish social relationships in an autonomous manner and interact with the other objects in the network based on their social behavior. A fundamental problem that needs attention is establishing of these relationships in a reliable and trusted way, i.e., establishing trustworthy relationships and building trust amongst objects. In addition, it is also indispensable to ascertain and predict an object's behavior in the SIoT network over a period of time.

III. MOTIVATION

SIoT is not the convergence of social networks and IoT instead it is a new paradigm (Pattern/Framework) that set up a social object interaction and relationship between the nodes in an autonomous way based on the rules set by an owner/device/user. SIoT model intends to develop a decentralized approach to foster the interactions among the objects that belong to different communities of members. The goal of SIoT is to publish, find information, and discover novel resources to better implement the services In SIoT objects are capable of creating and managing social-like relationships with each other in an (almost) autonomous way as same as normal human network based. SIoT smart objects acts as social object and that objects are enhanced with some cognitive (logic) capabilities to take initiatives such as sharing information, or connecting with another object in an autonomous way based on the object social relationship as trusted manner. In a heterogeneous environment with distributed services its difficult to trust the service providers in order to fulfill the services. The problem of service discovery and trustworthiness assessment of service providers is even more difficult when the service providers are distributed across networks. Most of the papers attempts to improve the performance and the quality of service of the network without considering about their benefits on trust classification of different devices based on social object relationship among both service provider and consumer. Most of the previous studies classify the trust according to object previous experience and referrals from a limited number of its neighbors, not based on all information in the network. Establishing trustworthy relationships promote a successful cooperation between objects. This necessitates reducing energy and time consumption in the service discovery and trustworthiness computation process as IoT devices are highly resource-constrained. The trust value is affected by not only the service-based

interactions, but also social interactions since the objects to interact with each other in complex patterns based on the several kinds of object relationships in SIoT.

IV. SIOT TRUST

SIoT adds the "intelligence" that allows objects to start, update, and terminate relationships. The selection of which friendship to accept is based on human control settings. In Social IoT commonly refers to the object means physical device and user of the Object/device. SIoT environment based on the relationships between the objects and users devices. Relationships in a SIoT system can be classified into two types:
1.User-Object Relationship (UO Relationship) 2.Object-Object Relationship (OO Relationship)
There are total of 10 types of Object relationships
1. UO Relationship, OOR — Ownership Object Relationship, SOR — Social Object Relationship, SIBOR— Sibling Object Relationship, GSTOR — Guest Object Relationship
2. OO Relationship, POR — Parental Object Relationship, CLOR — Co-Location Object Relationship, CWOR— Co-Work Object Relationship, GOR — Guardian Object Relationship, STGOR — Stranger Object Relationship, SVOR — Service Object Relationship
Machine learning model are effective data analysis approaches to know and classifying regarding the 'trust/usual' and ' untrust/unusual' device behavior as per the relationship between SIoT devices for analyzing the trust. In order to determine natural patterns of communication, the input data of each component of the SIoT system should be obtained and examined, thereby detecting untrusted node at the initial phases is major concern. In addition, the learning techniques may be useful in forecasting untrusted node in real-world implementations.

V SYSTEM MODEL

In order to quantify the trust classification based on object relationships in the SIoT environment, the system model is represented as '$SIoT_M$' that consists of 'N' number of devices and each object is represented as $N=\{D_1, D_2, D_3, D_4, \ldots\ldots D_n\}$. Each devices forms a relationship factor with each other and it is represented as 'R_f', The SIoT Consists of many devices where the with similar object with relationship is represented as 'SO_S' and heterogeneous object with relationship is represented as 'SO_H'. The new and independent object joined to network is represented as 'S_{NI}' within the given set of network. The objects distributed in the SIoT environment is represented as 'O^N_S', thus each individual object provides the different service and service is represented as 'D_S'. The maximum centrality of device connected is represented as 'α' and minimum centrality of device connected is represented as 'β'. The SIoT objects are distributed randomly in an network the objects try to form relationship among the other objects that comes in contact with each other in the network and system model can be represented as shown in below equation 1:

$$SIoT_{M=} \lim_{SOH,\, SOs} R_f(O^N_S(A(D_S))) : \updownarrow(\alpha, \beta) = S_{NI}\, f(O^N_S(A(D_S))) \quad (1)$$

VI. PROBLEM FORMULATION

It is essential for trust classification from the SIoT point of view. In SIoT, trust is characterized as the "confidence" of a trustor in a trustee to achieve an objective under a particular setting inside a particular time span. Trust is a dynamic process that involves trustor, trustee, and the underlying context. The trust computation process in this paper follows three steps: 1) social relationships request, 2) interactions in terms of the number of successful packets transmission, and 3) trust evaluation by quantifying the trust metrics from step 1 and step 2 and trust update.
SIoT plays an important role in enhancing real-time smart applications. In SIoT, smart things may join the network and may leave the system based on mutual trust among them. The application and service acts as intermediary between the sensor devices. Due to this rapidly expansion of SIoT environment, there is a chance for explosion of the data also trust and securing the data is highly challenging. In order to understand and handle the SIoT modifications, frequent updating of trusted device is essential, hence require and trust classification model for each event and its represented as 'E' with respect to time 'T' and corresponding object relationship.
Implementing of trust classification in SIoT using traditional approaches is ineffective, hence an machine learning techniques are proposed to address the trust classification problem in SIoT. Machine learning can be used for analyzing normal or abnormal behavior of the SIoT interactions as trust factor. The SIoT classification model is represented as 'S_C', the classification model easily track the trust and untrusted objects based on the dataset and object relationship. As the devices are distributed in SIoT network, each object offers and provides the data and

its service represented as 'OR_λ' and this process are visible to other object, where the untrusted device might modify the data and service of the other devices shown in equation 2.

$$\lim \; SO_S, SO_H(\alpha, \beta) = ES_{NI}\, f\,(O^N{}_S(A\,(D_S)R_F)) + S_C{}^T\, OR_\lambda \qquad (2)$$

The event 'E" exits between the objects for the specific service and the objects is trusted is represented as '1' , otherwise '0' as shown below equation 3.

$$E(S_{NI,}\, O^N{}_S) = \begin{cases} 1 & \text{if trusted object} \\ 0 & \text{otherwise} \end{cases} \qquad (3)$$

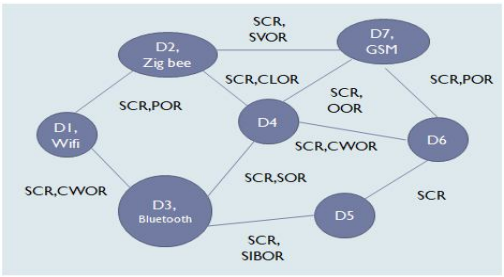
The fig 2 represents the Service(S), Communication model (C), Relationship type(R), (SCR) are the components required to select best and optimal trusted services. The relationship among the each object is verified based on device centrality in the SIoT network and to find the network establishment $O^N{}_S$ of all the individual objects (S_{NI}) with homogeneous and heterogenous objects is shown in an equation 4.

$$S_{NI}(SO_H, SO_S) = \lim_{n\to\infty} \sum_{n=SOH}^{n} \; Object - Relationship - Type \;\; f(S_{NI,}\, O^N{}_S) \qquad (4)$$

Inorder to obtain the object relationship the objects centrality among the distributed objects requires the minimum and maximum centrality connectivity based on relationship factor in an specified time with optimal classifiers to classify the node is trusted or not in an equation 5.

$$(\beta \leftarrow\!\text{-}\!> \alpha) = \lim_{n\to\infty} \sum_{n=\beta}^{\alpha} \; f(ScT\; OR\lambda) \qquad (5)$$

The connected objects linked into relationship OR_λ with the Classifier $S_{c,}$ Where all classified node with trust is represented as 1 otherwise it is 0 as shown in equation 6.



Figire 2: SIoT System Model

$$OR_\lambda, S_c{}^T = \begin{cases} 1 & \text{if trusted object} \\ 0 & \text{otherwise} \end{cases} \qquad (6)$$

TABLE I: SYSTEM MODEL NOTATIONS

Variable	Descripition
$SIoT_M$	System Model
R_f	Relationship factor
N=1,2,3,,,,n	Number of Objects
$O^N{}_S$	Distributed objects in SIoT environment
OR_λ	Connected Relationship objects Represents Service
S_{NI}	New and independent object joined into network
S_C	Service Classification
SO_H	Heterogeneous object with relationship
SO_S	Homogenous Objects
T	Time
E	Event
α	Maximum centrality of device connected
β	Minimum centrality of device connected is represented

VII. COMPARITIVE STUDY

Paper	Trust Metrics	Trust Algorithms	Trust Result
[29]	Reputation score, data accuracy, interaction frequency	Fuzzy logic, Support Vector Machines	Trusted, Untrusted, Partially Trusted
[30]	User reviews, device behavior patterns, anomaly detection	Bayesian Networks, Collaborative Filtering	High Trust, Low Trust, Uncertain
[31]	Secure data sharing, consensus mechanisms, transaction history	Distributed Ledger Technology, Smart Contracts	Identify and counter the selfish behaviour of nodes,
Proposed System	Object Relationship, Device Centrality and device type	Voting Classifier, Random forest and Decision Tree	The proposed model achieved 88.87% and 89.76% of accuracy for the given data set.

VII. RESULTS

The SIoT specific data set based on object relationship for trust devices classification is not exist in real time, however the data set is modified from the SIoT repository and with reference to existing dataset the new dataset is created to train the model for classify the node as trusted or not. The data set includes the different services followed by different attributes of device id, device name, device type, device relationship factor, trust factors, device centrality, and so on. Device id represents the unique id of each device, device type can be private device, public device, static device, mobility. By creating the sample dataset consist of 10000 devices the classification model is trained in order to classify the trusted node or not.

The below fig depicts the result of the model implemented with reference to given dataset that includes the relationship type of an object, device centrality, device mobility, communication model, trust evaluated value and trust classifier based on different trust attributes.

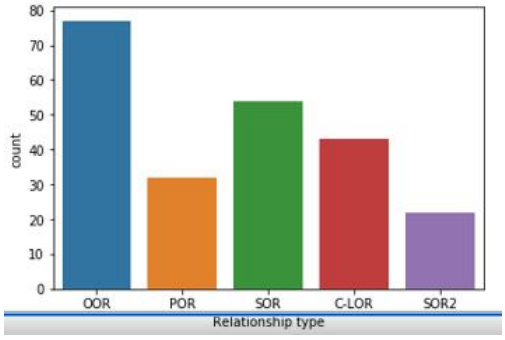


Figure 3: Classifying the object Relationship Type

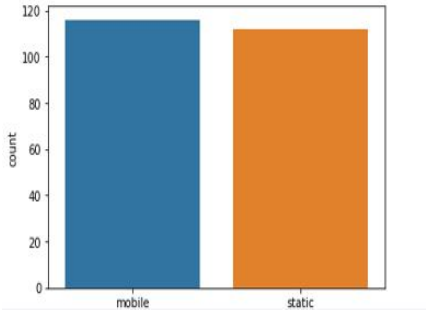


Figure 4: Mobility based Classification

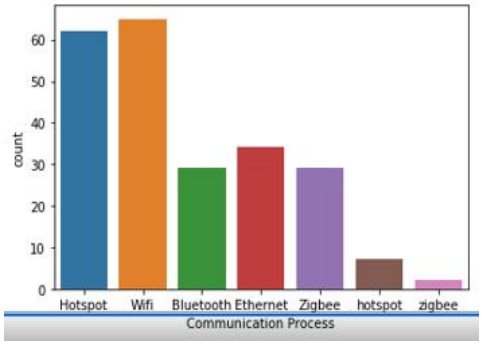


Figure 5: Classification based on Communication

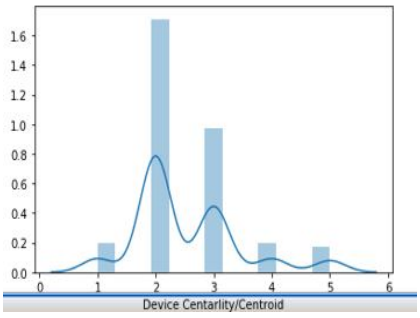


Figure 6: Classification based on Device Centrality

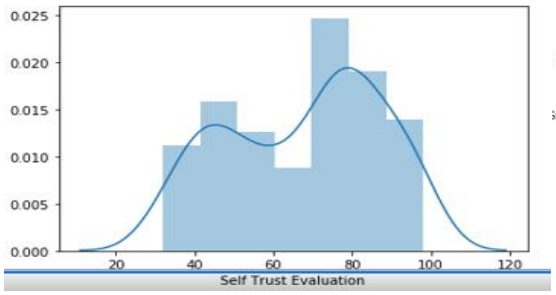


Figure 7: Self Trust Value based on Object Relationship

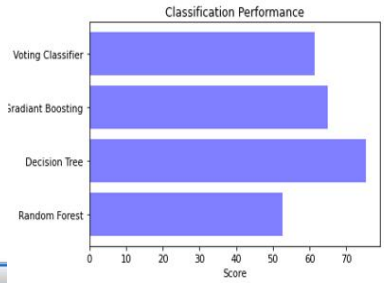


Figure 8: Trust Classification

VIII. CONCLUSION

SIoT is emerging domain across the world in this digital era. At the same time, cybercriminals also expanding their capabilities to launch a faster and sophisticated untrusted activities behaviour against social network and with network attached devices. In order to make the digital transformation in efficient way then the security personnel need to overcome this challenge by providing machine learning assisted trust solutions, which can detect the trust threats and other issues in SIoT and response in an dynamic and faster way. The classification comparison of machine learning model enhances the trust between SIoT devices with reference to given SIoT data set and provides new features and benefits for the developers of SIoT systems. The paper implements the trust, security and privacy in SIoT devices and networks tend to focus on providing suitable solutions for overcoming existing issues in SIoT with accuracy of 89.07%.

In Future work by considering the enhanced SIoT data set integrated with the different learning model to achieve the better accuracy is implemented.

REFERENCES

[1] Giancarlo Fortino and P. Trunfio. Internet of things based on smart objects: Technology, middleware and applications. Springer, 01 2014.

[2] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The Internet of Things: A Survey. Computer Networks, 54(15):2787 – 2805, Oct 2010.

[3] Sonia Khetarpaul, S. Gupta, and L.V. Subramaniam. Spatiotemporal social (sts) data model: correlating social networks and spatiotemporal data. Social Network Analysis and Mining, 6, 12 2016.

[4] Statista, Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. https://www.statista.com/statistics/471264/iot-number-ofconnected- devices-worldwide/. Accessed: 2020-04-15.

[5] Luigi Atzori, Antonio Iera, Giacomo Morabito, and Michele Nitti. The Social Internet of Things (SIoT) – When Social Networks Meet the Internet of Things: Concept, Architecture, and Network Characterization. Computer Networks, 56 (16):3594 – 3608, Nov 2012.

[6] Roopa M.S., Santosh Pattar, Rajkumar Buyya, Venugopal K.R., S.S. Iyengar, and L.M. Patnaik. Social internet of things (siot): Foundations, thrust areas, systematic review and future directions. Computer Communications, 139:32 – 57, 2019.

[7] Jian An, Xiaolin Gui, Wendong Zhang, Jinhua Jiang, and Jianwei Yang. Research on social relations cognitive model of mobile nodes in internet of things. Journal of Network and Computer Applications, 36(2):799 – 810, 2013.

[8] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito. A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things. In Proceeding of 23rd IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications - (PIMRC), pages 18–23, Sep. 2012.

[9] Guido Möllering. The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation, and Suspension. Sociology, 35(2):403–420, May 2001.

[10] H. Xia, F. Xiao, S. Zhang, C. Hu, and X. Cheng. Trustworthiness Inference Framework in the Social Internet of Things: A Context-Aware Approach. In proceeding of IEEE Conference on Computer Communications (INFOCOM), pages

[11] I. Chen, F. Bao, and J. Guo. Trust-Based Service Management for Social Internet of Things Systems. IEEE Transactions on Dependable and Secure Computing, 13 (6):684–696, 2016.

[12] A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, Á. MacDermott, and X. Wang. CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things. IEEE Internet of Things Journal, 6(3):5432–5445, 2019.

[13] I. Chen, J. Guo, and F. Bao. Trust management for soa-based iot and its application to service composition. IEEE Transactions on Services Computing, 9(3):482–495, 2016.

[14] Subhash Sagar, Adnan Mahmood, Jitander Kumar, and Quan Z. Sheng. A timeaware similarity-based trust computational model for social internet of things. In Globecom 2020 - 2020 IEEE International Global Communications Conference (Globecom), pages 1–6, 2020.

[15] A. Alnasser, H. Sun, and J. Jiang. Recommendation-Based Trust Model for Vehicle-to-Everything (V2X). IEEE Internet of Things Journal, 7(1):440–450, 2020.
[16] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui. A hybrid trust management heuristic for vanets. In 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pages 748–752, 2019.
[17] Li Xiong and Ling Liu. Peertrust: supporting reputation-based trust for peer-topeer electronic communities. IEEE Transactions on Knowledge and Data Engineering, 16(7):843–857, 2004.
[18] Yusuo Hu, Danqi Wang, and Hui Zhong. Socialtrust: Enabling long-term social cooperation in peer-to-peer services. Peer-to-Peer Networking and Applications, 7, 12 2014.
[19] Y. Chen, M. Zhou, Z. Zheng, and D. Chen. Time-aware smart object recommendation in social internet of things. IEEE Internet of Things Journal, 7(3):2014–2027, 2020.
[20] Y. Saleem, N. Crespi, M. H. Rehmani, R. Copeland, D. Hussein, and E. Bertin. Exploitation of social iot for recommendation services. In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), pages 359–364, 2016.
[21] N. B. Truong, G. M. Lee, T. Um, and M. Mackay. Trust Evaluation Mechanism for User Recruitment in Mobile Crowd-Sensing in the Internet of Things. IEEE Transactions on Information Forensics and Security, 14(10):2705–2719, 2019.
[22] B. Ye, Y. Wang, and L. Liu. Crowd trust: A context-aware trust model for worker selection in crowdsourcing environments. In 2015 IEEE International Conference on Web Services, pages 121–128, 2015.
[23] U. Jayasinghe, G. M. Lee, T. Um, and Q. Shi. Machine Learning based Trust Computational Model for IoT Services. IEEE Transactions on Sustainable Computing, 4b(1):39–52, 2019.
[24] S. Sagar, A. Mahmood, Q. Z. Sheng, and W. E. Zhang. Trust computational heuristic for social internet of things: A machine learning-based approach. In ICC 2020 - 2020 IEEE International Conference on Communications (ICC), pages 1–6, 2020.
[25] Yating Wang, Yen-Cheng Lu, Ing-Ray Chen, Jin-Hee Cho, Ananthram Swami, and Chang-Tien Lu. Logittrust : A logit regression-based trust model for mobile ad hoc networks. 2014.
[26] Subhash Sagar, Adnan Mahmood, Quan Z. Sheng, and Munazza Zaib, Wei Emma Zhang, “Towards a Machine Learning-driven Trust Evaluation Model for Social Internet of Things: A Time-aware Approach”, Conference’17, 3 Feb 2021, Washington, DC, USA.
[27] Stergiou, C., Psannis, K.E., Kim, B.-G., Gupta, B.: Secure integration of IoT and cloud computing. Futur. Gener. Comput. Syst. 78(3), 964–975 (2018).
[28] Soro, A., Brereton, M., Roe, P.: Social Internet of Things, 1st edn. Springer (2018)
[29] Sagar, Subhash et al. “Trust–SIoT: Toward Trustworthy Object Classification in the Social Internet of Things.” IEEE Transactions on Network and Service Management 20 (2022): 1210-1223.
[30] Huang, Zhen et al. “A social network approach to trust management in VANETs.” Peer-to-Peer Networking and Applications 7 (2012): 229 - 242.
[31] Arshad, Quratulain et al. “Blockchain-based decentralized trust management in IoT: systems, requirements and challenges.” Complex & Intelligent Systems (2023): 1-22.