Grenze International Journal of Engineering and Technology, Jan Issue

Research Challenges and Opportunities for Trust Management Systems in IoT Networks

Satish Kamble[1], Dr. Surendra Mahajan[2], Deepak D. Sapkal[3] and Kimi Ramteke[4]
[1]Research Scholar, Department of Computer Engineering, SKNCOE, SPPU, Pune, India
Email:satkam53@gmail.com
[2]Department of Information Technology, PVG'S COET & GKPWIOM, SPPU, Pune, India
Email: sa_mahajan@yahoo.com
[3]Department of Computer Engineering, PVG'S COET & GKPWIOM, SPPU, Pune, India
Email: ddsapkal@gmail.com
[4]Department of Computer Engineering, I[2]IT, SPPU, Pune, India
Email: kimiramteke16@gmail.com

***Abstract*—IoT device applications are rapidly expanding in the current environment. Today, we can find IoT devices in a variety of industries, including agriculture, home security, entertainment, health, transportation, and education. Today, users of IoT devices and applications come from large cities, small towns, and rural areas. Security and trust are vital areas for the success of IoT implementation in IoT applications. When IoT devices engage with one another, trust grows between them. IoT device communications may be made secure by implementing trust-featured systems. Algorithms based on Machine learning, Fuzzy logic, Bayesian, and Entropy can be utilized for trust management systems. Trust management systems are surveyed in this study. Further, this paper highlights research challenges and directions in this area.**

***Index Terms*— IoT, Trust management, Machine learning, Fuzzy logic, Trust-related attacks.**

I. INTRODUCTION

We could never have predicted the extent to which the Internet has changed. A modest pace of progress was initially observed. Innovation and advancement are currently occurring at an amazing rate. By 2025, it's expected that 50 billion things will be linked to the Internet. [1]. In the world of networking devices, a new field called the Internet of Things (IoT) is growing in popularity. The ubiquitous nature of numerous objects, including smartwatches, smartphones, smart home systems, and smart security systems, is the central tenet of the Internet of Things.

In the present scenario, applications of IoT devices are increasing enormously. Today we can find IoT devices in the agriculture sector, home security sector, entertainment sector, health sector, transportation sector, education sector, and many more. People from metro cities, towns, and villages are now using IoT devices and applications. Fig.1. shows IoT applications.

A significant economic benefit is anticipated from IoT devices in the coming years. When an IoT device wants to connect with another device for data and information, a guarantee that the IoT device is trusted and secured is required. Many researchers still struggle with a variety of issues related to IoT research, such as 1) security

Grenze ID: 01.GIJET.10.1.534

issues, 2) connection issues 3) trust issues, 4) energy issues, and 5) authentication issues.
1) Security issues: IoT networks must be protected from comparable assaults because they are a prime target for any information security flaw. The following qualities must be guaranteed for IoT networks to provide effective security.

- Confidentiality: Confidentiality ensures that the most important part of security is preventing information from getting into the wrong hands.
- Integrity: Integrity ensures that senders' information hasn't been changed during transmission.
- Availability: The availability of services in the Internet of Things is determined by how long they continue to operate despite vulnerabilities at all network layers. [1]

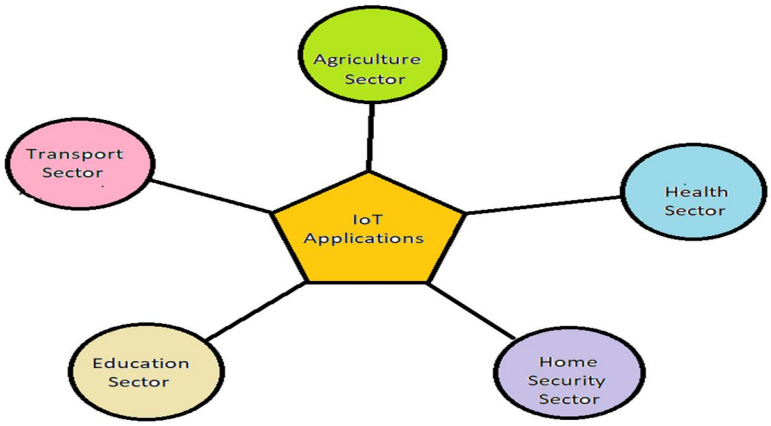

Fig. 1. IoT Applications

2) Connection issues: The better connectedness of everything, including systems, is referred to as the "Internet of Things" (IoT) in modern usage, devices, and ways of giving consumers access anywhere, anytime. The following qualities must be guaranteed for IoT networks to provide effective connections.

- Interoperability: Consumers need gadgets that are simple to use, simple to connect to, and interoperable, therefore this is a major concern. [3]
- Self-Management: IoT devices have the ability to monitor their own operational health and warn users of potential issues in advance of a shutdown.
- Signaling: IoT data streams play a key role in the reliable bidirectional signaling that is essential for gathering data & forwarding between devices in an IoT device network. [2].

3) Trust issues: The actions used to develop, verify, and trust relationships between connected devices are connected to the concept of trust in IoT networks [3].
4) Energy issues: In IoT networks, energy management presents a difficult problem. Energy use is primarily driven by IoT communication. By carefully applying algorithms, allocating computer resources, and designing efficient communication protocols, it is possible to maximize energy efficiency [4].
5) Authentication issues: Due to the vast number of digital objects in the IoT architecture, identifying and authenticating every IoT object is challenging. As a result, creating and executing efficient procedures to manage and control IoT devices is a crucial activity [5].
Section II. gives a definition of trust in IoT. Section III. gives a brief description of the existing literature. Section IV. gives research challenges and directions in this area. section V. gives the conclusion.

II. TRUST IN IOT

Trust between IoT devices gets developed when they start interacting with each other. In the IoT networks, two interacting entities are named trustor and trustee. A trustor is one who wants to access some specific services from an IoT device. The trustee wants to provide some specific services to IoT devices.
In the literature we can find various definitions of Trust:
Definition 1: Trust is measurable confidence between Trustor and Trustee for a defined time interval [6].
Definition 2: Trust is a subjective probability between Trustor and Trustee for a defined time interval [7].
Recent research in this domain identifies five components playing a vital role in developing trust management systems. This can be categorized as 1) Trust measure, 2) Trust circulation, 3) Trust algorithm, 4) Trust generation, and 5) Attacks. as in Fig. 2.

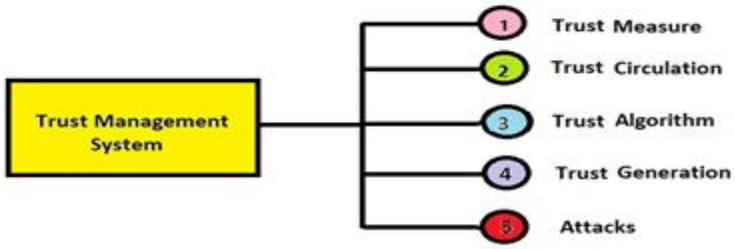

Fig. 2. Trust Components

1) Trust Measure: The concept of trust measure describes what should be considered when calculating trust. Among the measures of trust are social trust and quality of service (QoS).

QoS Trust: According to this concept, the ability of an IoT device to carry out a desired service is used as a metric for determining how trustworthy the device is.

Social Trust: Devices build social ties based on a social IoT system. The social IoT system is closely tied to social trust. Several metrics, including Friendship, Co-work Relationships, and Cooperativeness are already utilized in this category [12].

2) Trust Circulation: How to spread trust proof among peers is referred to as trust circulation. There are typically two types of trust circulation schemes: distributed and centralized.

Distributed: Distributed trust circulation is the independent transmission of trust observations by IoT devices to other IoT devices they come into contact with. This is especially true in IoT scenarios that emulate various networks, where it can be difficult to set up or reach a centralized organization. A decentralized trust circulation model that allows each node to determine the trust value of its neighboring nodes was proposed by Subramanian et al. [15].

Centralized: The transmission of trust observations by IoT devices to centrally situated nodes is known as centralized trust circulation. Typically, the cluster head is a center node. Thirukkumaran et al. [11] presented a technique in which the entire sensor network is partitioned into small clusters, and one cluster head (CH) is elected for each cluster region based on high energy.

3) Trust Algorithm: Trust aggregation algorithms are applied by collecting QoS and Social trust metrics. There are a variety of Trust aggregation algorithms used by researchers namely fuzzy logic [8], [9], [10], [11], machine learning [12],[13],[14], and Bayesian inference [16].

4) Trust Generation: The process of creating an overall trust from several trust attributes is known as trust generation. In the literature, the concept of single-trust or multi-trust trust generation is discussed.

Single-Trust: In a single-trust generation only one trust attribute value is used for calculating the overall trust value. Ahmed et al. [18] use only feedback given by neighboring IoT devices.

Multi-Trust: In a multi-trust generation multiple trust attribute values are used for calculating overall trust value. Almogren et al. [9] use Integrity and compatibility as multi-trust attributes.

5) Attacks:

In the literature, we can find the following types of trust-related attacks.

1. A malicious node acts aggressively towards everyone (ME) when they are present. This is the simplest form of attack; nodes always give poor recommendations and services, irrespective of the requester [19].

2. Discrimination Attack (DA): Depending on who is requesting services, a rogue node alters its behavior. This means that a node has the right to discriminate against nodes that are not its friends or have tenuous social relationships. Because of this, certain devices may view the node as helpful while others may view it negatively [20].

3. On-Off Attack (OOA): A node frequently switches between being benign (ON) and evil (OFF) in order to adjust its behavior. During the ON state, the node increases its trust, which is then used to launch attacks on the network [21].

4. Whitewashing Attack (WA): A node with a negative trust value disjoins the IoT network. The new identity is allotted on joining the network and the node's trust value is initialized to a standard value fixed.

5. Self-Promoting Attack (SPA): A rogue node makes positive recommendations for itself. Once chosen as a provider, it simply offers subpar services [23].

6. Bad Mouthing Attack (BMA): A number of nodes band together in this attempt to damage the reputation of a good node. A malicious node will simply make bogus suggestions to lessen the possibility that good nodes would be chosen as providers [24].

7. Ballot Stuffing Attack (BSA): BSA is a particular kind of collusive assault in which one malicious node helps another in an effort to strengthen its reputation and raise its chances of being picked as the service provider [25].

III. Literature Survey

Alshehri et al. [8] Fuzzy logic for a cluster-based architecture has been presented. The system consists of numerous master nodes and one super node. Bad service providers, on-off assaults, and con-behavior attacks were the three types of attacks that this system handled. They consider the direct score, prior score, and routing score when calculating the trust score. All trust calculations are performed by the master nodes. By using an algorithm, nodes were categorized as trusted, semi-trusted, and untrusted. This system uses the quality of service as a direct score. Routing scores are created through the examination of service responses from a node in a different cluster.

Almogren et al. [9] suggested the FTM-IoMT as a trust management system to aid the medical industry. FTM-IoMT uses fuzzy logic to decide whether a requesting node is reliable or not. The suggested model uses compatibility and integrity as two trust attributes. The suggested model employs fuzzy logic processing to identify Sybil and compromised nodes. The server will reject the request if it is marked by the requesting node as malicious. In addition to providing the services requested, the server updates the local database's trust value for the requesting node. This system has a centralized organizational structure.

Chen et al. [10] developed a fuzzy logic in IoT systems. The fuzzy logic is the foundation of this system. Both direct and indirect trust techniques are used in this system. Monitoring the nearby nodes results in direct trust. It employs the end-to-end packet forwarding ratio (EPFR), the average energy consumption (AEC), and the packet delivery ratio (PDR) to calculate direct trust and indirect trust. Global trust is determined using fuzzy reputation membership using direct and indirect trust models. With the other two models already in use, this system compared the performance of its model. The TRM-IoT model outperforms the other two models now in use. TRM-IoT has a higher likelihood of detecting malicious nodes than either of the other two models. This system model can be improved by implementing a more advanced global trust calculating mechanism.

Thirukkumaran et al. [11] (TAACS-FL) has been proposed for IoT. This system uses data integrity, successful forward ratio (SFR), and energy consumption rate (ECR) as trust attributes. In this approach, determining the trust value for each cluster member is the responsibility of the cluster leader. The cluster head determines the trust value using fuzzy logic. Nodes are given access rights such as send, receive, forward, and drop according to their trust value. This system takes into account three different attack types: data modification, selfish behavior, and packet dropper. The simulation is carried out with NS-2. The (TAACS-FL) proposed for IoT ensures scalability and energy efficiency.

Jayasinghe et al. [12] developed a machine-learning approach for detecting transactions between IoT nodes as trustworthy or untrustworthy. This system uses the Reward System, Mutuality and Centrality, Community of Interest, Co-work Relationship, Cooperativeness, Frequency, and Duration as trust attributes. IoT device interactions are categorized as trustworthy or untrustworthy using the k-means clustering technique. The system is trained using a support vector machine for classification. The outcomes showed that the model had a 0.4175% false positive rate and a prediction accuracy of 89.74%.

Marche et al. [13] proposed a trust management system making use of a machine learning model. This model uses computation capabilities, relationship factors, and external opinion as the trust attributes. The system acquires dynamic knowledge from past transactions using the machine learning approach. This system uses an incremental support vector machine(iSVM) model for training. The suggested model has been tested against every type of attack. This system is capable of repelling all potential attacks. The performance of the iSVM was compared with that of the incremental Logistic Regression (iLR) and the incremental Radial Basis Function network (iRBF), two well-known machine learning techniques. The data demonstrate that iSVM performs better than the other two.

Alghofaili et al. [14] created a deep-learning model for IoT networks. Packet loss, delay, and throughput are used as QoS trust parameters in this paradigm. This model employs the SMART technique to determine a node's trust value and determine whether it is trustworthy or not. The LSTM was also utilized to accurately identify behavioral changes. This system outperforms other machine learning methods in comparison tests. The system employs a decentralized model for trust propagation.

Subramanian et al. [15] use the linear regression technique. This system uses trust attributes such as availability, integrity, security, honesty, and privacy. The trust circulation model used by this system allows each node to count the trust value of its neighboring nodes. Simulations are run, and the results demonstrate that malicious nodes are successfully detected.

Janani et al. [16] developed a model using Bayesian and evidence theorems. Both direct and indirect trust are used. The Bayesian theory is used to determine direct trust, while the Dempster-Shafer (DS) evidence theory is used to determine indirect trust. The direct and indirect components are incorporated for calculating the hybrid trust. QualNet 4.5 simulator is used to conduct effective simulations. This system tackles packet dropping, flooding, wormhole, black hole, and Sybil attacks.
Xueqiang et al. [17] developed a solution using an entropy. This system utilized QoS metrics such as data repetition rate, packet size abnormality, data correlation, and volatility of transmission delay. Mathematical methods such as Information Entropy are used to assign weight to nodes. The direct and indirect trust values are then added for getting the overall trust. The suggested method does a good job of detecting malicious nodes and can deal with assaults including forwarding attacks, data forgery attacks, denial-of-service attacks, and on/off attacks.
Ahmed et al. [18] developed a solution using entropy. It uses Jaccard Similarity Score. The solution for this model is entropy-based and depends on the similarity score. The suggested model iteratively updates trust values with each communication to discriminate between malicious and honest nodes.
Table I. Gives a detailed classification of Trust components described in the papers referred. Table 2. gives the attack handled in the papers referred.

TABLE I. TRUST COMPONENTS IN THE PAPERS REFERRED

Component		Papers
Trust Measure	QoS trust	[8], [9], [10], [11], [12], [14], [15], [16], [17], [18]
	Social trust	[12], [13]
Trust Circulation	Centralized	[8], [9], [11],
	Distributed	[10], [12], [13], [14], [15], [16], [17], [18]
Trust Algorithm	Fuzzy logic	[8], [9], [10], [11]
	Machine learning	[12], [13], [14]
	Bayesian	[16]
	Entropy	[17], [18]
	Linear Regression	[15]
Trust generation	Single-Trust	[18]
	Multi-Trust	[8], [9], [10], [11], [12], [13], [14], [15], [16], [17]

TABLE II. ATTACK HANDLED IN THE PAPERS REFERRED

Papers	Attack Handled
[8]	Bad service provider, on-off attack, con-behavior attack
[9]	Sybil and compromised nodes
[10]	Malicious node
[11]	Data modification, selfish behavior, and packet dropper
[12]	Untrustworthy transactions
[13]	Malicious with everyone, Discrimination attack, On-Off Attack, Whitewashing Attack, Bad Mouthing Attack, Ballot Stuffing Attack
[14]	Misbehaving node
[15]	Misbehaving node
[16]	Packet dropping, flooding, wormhole, black hole, and Sybil attacks.
[17]	forwarding attack, data forgery attack, DoS at-tack, and on/off attack.
[18]	Malicious node

IV. RESEARCH CHALLENGES AND DIRECTIONS

First, more investigation into cutting-edge social trust metrics and quality of service metrics is needed. Combining these two metrics is a topic for additional research. The quality of service metrics packet forwarding ratio (PFR), energy consumption (EC), and packet delivery ratio (PDR) can be integrated with social trust measures such as co-work location, community-of-interest, and friendship.
Second, more research is required in trust aggregation algorithms. In literature, we can find fuzzy logic is explored by various authors but it is having its limitations. Fuzzy logic relies on human judgment and linguistic variables, which can introduce subjectivity into the decision-making process. The choice of membership functions and fuzzy rules is often based on expert knowledge or intuition, making the results susceptible to bias. Large quantities of high-quality data are essential for the training of machine learning models. Models that are

erroneous or biased can result from insufficient or biased data. Obtaining and preparing relevant and representative datasets can be time-consuming and resource-intensive. Machine learning models can suffer from overfitting, which occurs when the model is too closely suited to the training data and performs poorly on new, uncontaminated data. Overfitting may occur when there aren't enough training data or the model is very complex.

IoT systems often involve complex relationships and dependencies among devices, users, and environmental factors. Capturing these dependencies accurately in a Bayesian model can be challenging, as it requires defining conditional probabilities and modeling complex interactions. In situations where dependencies are not well understood or change dynamically, building accurate Bayesian models can be difficult.

Entropy calculations require estimating probabilities of different events or states. In IoT trust management, accurately determining probabilities can be challenging due to factors such as limited data availability, device heterogeneity, and dynamic network conditions. Estimating probabilities with accuracy and reliability becomes difficult, especially in large-scale and dynamic IoT environments.

IoT trust management systems can be improved by combining entropy with other trust assessment techniques to enhance the overall trust management system. It can complement probabilistic models, machine learning algorithms, or reputation systems by providing an additional perspective on uncertainty and information content. A more comprehensive and robust trust assessment framework can be developed by combining entropy with other approaches.

Third, IoT devices often have limited computational power, memory, and energy resources. Designing lightweight trust management algorithms that consume minimal resources is essential for practical deployment in resource-constrained IoT environments. Further research is needed in developing the IoT trust management system for resource-constrained IoT environments.

Fourth, IoT encompasses a wide range of devices, protocols, and technologies with varying capabilities and characteristics. It's difficult to create a trust management system that can work with heterogeneous IoT devices and seamlessly connect with various platforms and communication protocols. A greater amount of research is needed to develop an IoT trust management system that can manage the heterogeneity of IoT devices.

Fifth, a greater amount of research is needed to develop an IoT trust management system that can counteract various trust-related attacks.

V. Conclusion

The trust management system in IoT networks is the main topic of this study and survey. According to this study, IoT trust management systems can be categorized into trust measures, trust circulation, trust algorithms, trust generation, and attacks. The work done using different trust aggregation algorithms, including fuzzy logic, machine learning, Bayesian, and entropy, is thoroughly analyzed in this research. To help other academics interested in conducting a study on the trust model in IoT systems, research gaps, and problems are also highlighted.

Acknowledgment

All the authors would like to thank the Computer Engineering Department of SKNCOE, SPPU, Pune, for providing motivation in the Trust Management System in IoT networks.

References

[1] A. Srivastava, S. Gupta, M. Quamara, P. Chaudhary, and V. J. Aski, ‘‘Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects,’’ Int. J. Commun. Syst., vol. 33, no. 12, pp. 1–40, 2020.

[2] S. S. I. Samuel, "A review of connectivity challenges in iot-smart home", 2016 3rd MEC International conference on big data and smart city (ICBDSC), pp. 1-4, 2016.

[3] Warsun Najib, Selo Sulistyo, Widyawan, “Survey on Trust Calculation Methods in Internet of Things”, Procedia Computer Science, Volume 161, 2019, Pages 1300-1307.

[4] S. S. Prasad and C. Kumar, "An energy efficient and reliable internet of things", Communication Information & Computing Technology (ICCICT) 2012 International Conference on. IEEE, pp. 1-4, 2012.

[5] L. Prathibha and K. Fatima, "Exploring security and authentication issues in Internet of Things", Proc. 2nd Int. Conf. Intell. Comput. Control Sys. (ICICCS), pp. 673-678, Jun. 2018.

[6] Overview of trust provisioning for information and communication technology infrastructures and services, ITU-T, Recommendation Y.3052, 2017.

[7] D. Gambetta et al., “Can we trust trust,” Trust: Making and breaking cooperative relations, vol. 13, pp. 213–237, 2000.

[8] Mohammad Dahman Alshehri and Farookh Khadeer Hussain, “A fuzzy security protocol for trust management in the internet of things (fuzzy iot)”, Computing, 101(7):791–818, jul 2019.
[9] A. Almogren, I. Mohiuddin, I. Ud Din, H. Almajed and N. Guizani, "FTM-IoMT: Fuzzy-based trust management for preventing sybil attacks in internet of medical things", IEEE Internet Things J ., vol. 8, no. 6, pp. 4485-4497, Mar. 2021.
[10] Dong Chen, Guiran Chang, Dawei Sun, Jiajia Li, Jie Jia, and Xingwei Wang. Trm-iot: A trust management model based on a fuzzy reputation for the internet of things. Comput. Sci. Inf. Syst., 8:1207–1228, 10 2011.
[11] R. Thirukkumaran and P. Muthukannan, “TAACS-FL: trust aware access control system using fuzzy logic for internet of things,” International Journal of Internet Technology and Secured Transactions, vol. 9, no. 1/2, pp. 201–220, 2019.
[12] U. Jayasinghe, G. M. Lee, T.-W. Um and Q. Shi, "Machine learning based trust computational model for IoT services", IEEE Trans. Sustain. Comput., vol. 4, no. 1, pp. 39-52, Jan. 2019.
[13] C. Marche and M. Nitti, "Trust-Related Attacks and Their Detection: A Trust Management Model for the Social IoT," in IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3297-3308, Sept. 2021, doi: 10.1109/TNSM.2020.3046906.
[14] Alghofaili, Y.,Rassam, M.A., “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 2022, 22, 634. https://doi.org/10.3390/s22020634.
[15] Subramanian, Ananda Kumar, Samanta, Aritra, Manickam, Sasmithaa, Kumar, Abhinav, Shiaeles, Stavros and Mahendran, Anand. "Linear Regression Trust Management System for IoT Systems" Cybernetics and Information Technologies, vol.21, no.4, 2021, pp.15-27. https://doi.org/10.2478/cait-2021-0040
[16] V S, J., M S K, M. Efficient trust management with Bayesian-Evidence theorem to secure public key infrastructure-based mobile ad hoc networks. J Wireless Com Network 2018, 25 (2018). https://doi.org/10.1186/s13638-017-1001-5.
[17] Yin, X., Li, S. Trust evaluation model with entropy-based weight assignment for malicious node’s detection in wireless sensor networks. J Wireless Com Network 2019, 198 (2019). https://doi.org/10.1186/s13638-019-1524-z.
[18] S. Ahmed and K. Tepe, "Entropy-based recommendation trust model for machine to machine communications" in Ad Hoc Networks, Springer, pp. 297-305, 2017.
[19] M. Nitti, R. Girau, and L. Atzori, “Trustworthiness management in the social internet of things,” IEEE Transactions on knowledge and data engineering, vol. 26, no. 5, pp. 1253–1266, 2014.
[20] D. Wang, T. Muller, Y. Liu, and J. Zhang, “Towards robust an effective trust management for security: A survey,” in 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2014, pp. 511–518.
[21] J. Caminha, A. Perkusich, and M. Perkusich, “A smart trust management method to detect on-off attacks in the internet of things,” Security and Communication Networks, vol. 2018.
[22] X. Fan, L. Liu, R. Zhang, Q. Jing, and J. Bi, “Decentralized trust management: Risk analysis and trust aggregation,” ACM Computing Surveys (CSUR), vol. 53, no. 1, pp. 1–33, 2020.
[23] A. Altaf, H. Abbas, F. Iqbal, and A. Derhab, “Trust models of internet of smart things: A survey, open issues, and future directions,” Journal of Network and Computer Applications, vol. 137, pp. 93–111, 2019.
[24] J. Guo, R. Chen, and J. J. Tsai, “A survey of trust computation models for service management in internet of things systems,” Computer Communications, vol. 97, pp. 1–14, 2017.
[25] R. Chen and J. Guo, “Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection,” in 2014 IEEE 28th International Conference on Advanced Information Networking and Applications. IEEE, 2014, pp. 49–56.