IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Special Issue 2, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

An Examination on Trust Based Techniques Using IOT Devices

K.Kowsalyadevi[1], R.Padma[2], N.S.Abinaya[3]

Assistant Professors, Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India[1,2&3]

ABSTRACT: The Internet of Things (IoT) has emerged as one of the most important technologies for the Internet's future, in which physical objects are transformed into digital data. Smart things that can be controlled and monitored through the internet. The Internet of Things (IoT) for reliable data collecting, context awareness, and other benefits as well as increased consumer privacy. IoT has spawned a slew of new services and applications in fields as diverse as finance, healthcare, transportation, and retail. Because there is a risk that huge amounts of sensitive data will be exposed while using these applications, it is vital to examine trust-related issues as well as other security issues that could risk confidential data and personal privacy. In this area, trust management plays a key role for resource constrained IoT devices.

KEYWORDS: Internet of Things, Trust management model, Trust, Security

I. INTRODUCTION

The internet of things is a concept that allows entities to detect and gather data from the real environment then exchange that data via the internet, where it may be analyses and used for a variety of purposes [1]. An item in the internet of things can be a person, a location, temporal data, or a state. We might argue that the IoT is nothing more than the internetworking of gadgets to share data across the internet. Because the devices are equipped with chips and sensors, they can be tracked.

The Internet of Things (IoT) is a unique paradigm that has sparked a lot of curiosity in the modern world since it allows us to use technology to create a smart environment [4]. The IoT's development goal is to connect the environment and physical world to wireless networks, allowing machines, objects, and the workplace to communicate.

Using Internet of Things sensors, things will be able to exchange data with other machines without the need for human intervention. However, because of its openness, the security risk is continuously expanding. As a result, determining whether or not the communication entities are legitimate is critical. To address this issue, an IoT trust management system has been implemented.

In recent years, trust management, which aims to solve distributed security challenges, has become a recent topic of research [3]. Trust management is a helpful technique for providing security services, and it has been employed in a variety of applications as a result. In the IoT, trust management is critical for trustworthy data fusion and mining. So, using a trust management system, IoT may give the appropriate trust service in response to the request. The implementation of IoT trust management is still a work in progress. There are few studies on trust management in the context of the Internet of Things.

The rest of the paper is organized as follows: Section 2 explains the evaluation of existing trust calculation methods. Section 3 surveys three different trust management models named peer trust model, subjective model and dynamic model. Also the detailed procedure of how trust computation is performed in each model is clearly discussed. Section 4 conducts properties of the five trust management modes.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

II. EVALUATION EXISTING TRUST CALCULATION METHODS

Work	Architectural model	Calculation method	Trust metric (parameter)	Performance measures	Focus of experiment	Experiment setup	Tool Contribution
Wang, 2018 [5]	Node level trust, decentralized	Attribute-based access control	. Access control policy.	The relation between policy and decision time.	Propose a framework for access control.	PC simulation involving 1000 access control policy	Propose access control framework
Ammar, 2018 [6]	Cloud-based IoT	-	Architecture, application specification, hardware	-	Comparison of architecture and framework	-	IoT framework survey
Jayasinghe, 2018 [8]	Social IoT Machine learning based	Cooperativeness, frequency	Distribution of trust worthiness	reward system	5776 objects	711 community	Trust prediction model
Caminha, 2018, [9]	Node level, decentralized	Direct trust	Direct trust	Percentage discovered resources	Middleware for trust evaluation	FIWARE-Lab platform for smart city, 2358 sensors	Propose middleware
Yuan, 2018 [10]	Hierarchical model – Direct	indirect (broker)	QoS trust, success rate, information entropy.	Convergence time, task failure ratio. Computational efficiency	Low-overhead trust computing algorithm	NetLogo, 1000 devices, 20 brokers	Multi-source feedback information fusion.
K. Prathapchandran, 2021[7]	Security Model	Direct trust	Qos trust metric	Packet delivery Ratio	Logic Regression	50 Nodes, Tmote Sky	to Detect Misbehaving Nodes
Airehrour , D, 2016 [15]	-	Direct trust	To increase the detection ratio by avoiding collaborative attacks in routing	-	Perceptron and K-means method,	-	-

Table 1: It Shows the Evaluation of Existing trust methods

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

III. TRUST CALCULATION MODELS

Peer Trust Model

In the peer trust model, trust is evaluated in a dynamic and decentralized manner at each peer. As a result, there is no need for a central database to store all global data in this architecture. Instead, each peer maintains a trust database [8], which is a small database that stores a piece of global trust data. Furthermore, the trust data required to compute the trustworthiness of peers is dispersed across the network.

Each peer has a trust manager who is responsible for two things: submitting input and evaluating trust. Each peer also includes a data locator that allows trust data to be placed appropriately across the network [11]. First the trust manager sends the network feedback about a certain peer, and the data locator reroutes the trust data to the right peers for storage. Second, the trust manager is responsible for calculating a target peer's trustworthiness. The data locator assists in gathering trust data from the network for the target peer and then computing the trust value.

Subjective Trust Management Model

The huge number of nodes, the process of information discovery becomes simple, implying that it enables scalability to a large extent. This model consists of multiple things belonging to a single owner, each of which is capable of forming interactions [12] on its own. This approach enables the creation of a dependable system based on object behaviors.

Dynamic Trust Management Model

Routing is done in dynamic trust mode in an environment that includes both malevolent and selfish nodes as well as trustworthy nodes. The trust management protocol calculates the trust value of each node in the network and then selects a secure routing path based on that value. When a node joins a network [15], the trust related data required to calculate the trust value is acquired from the nodes involved. The protocol detects malicious and selfish nodes based on the computed trust value and reroutes packets accordingly.

IV. PROPERTIES OF TRUST

The properties of trust are discussed in the section shown in Figure 1,

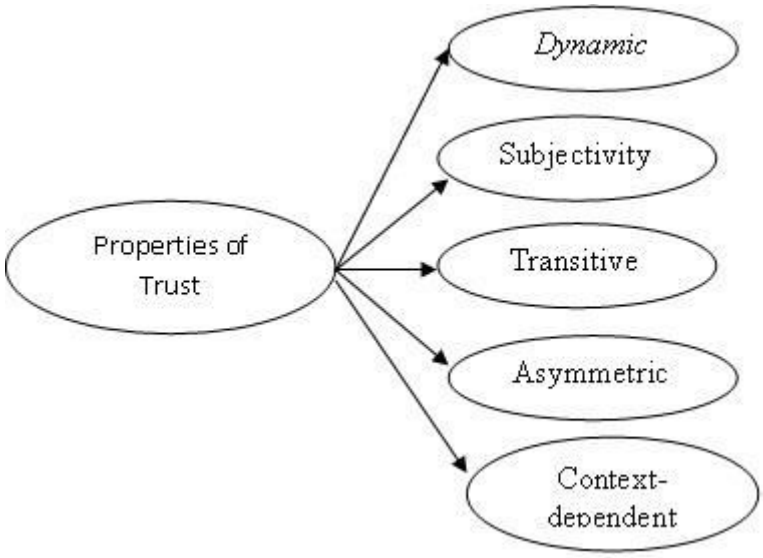

Figure 1: Properties of Trust

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Dynamic

Because the IoT environment is dynamic, trust connections among participating devices will change frequently. As a result, predicting the trust value of one device in relation to another is more difficult. Furthermore, because the IoT allows for scalability, new devices can join or old devices can leave the IoT environment at any time. Subjectivity IoT has several sorts of devices and provides services to users. Every device has different communication experiences with other devices [13].

Transitive

If device d1 trusts device d2, and device d2 trusts device d3 at the same time, device d1 does not need to trust device d3. In this situation, the transitivity between device d1 and device d3 and the device d1's reliance on the device d3's third-party references.

Asymmetric

Due to the heterogeneity of the devices, they differ in terms of memory, bandwidth, battery, processing and computing power [11]. As a result, the device with the highest capacity may be hesitant to trust the device with the lowest capacity, and vice versa.

Context-dependent

A device with high computational power is deemed trusted, while a device with low computational power is considered untrustworthy but not malicious.

V. CONCLUSION

The IoT environment is made up of a variety of devices, proper security procedures are required to maintain the environment security. With this in mind, this review paper focuses on trust based methods for light weight devices that are always resource constrained in this environment. This paper discussed some of the substantial works towards trust-based methods, models and properties in the IoT environment. In the future, the research work will be focusing on the trust based mechanism using machine learning over the Internet of Things based environment.

REFERENCES

[1]. Xuanxia Yao, Fadi Farha et. al.," Security and privacy issues of physical objects in the IoT: Challenges and opportunities", Digital Communications and Networks, https://doi.org/10.1016/j.dcan.2020.09.001, 2020

[2]. H. Liu, H. Ning, Y. Yue, Y. Wan, L.T. Yang, "Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices, Future Generation Computer Systems 78 (976–986), https://doi.org/10.1016/j.future.2017.04.014, 2018.

[3].H. Liu, X. Yao, T. Yang, H. Ning, Cooperative privacy preservation for wearable devices in hybrid computing-based smart health, IEEE Internet of Things Journal 6 (2) 1352–1362, https://doi.org/10.1109/JIOT.2018.2843561, 2019.

[4]. X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on block chain for internet of things, Computing Communication, 136(2) (2019) 10–29, https://doi.org/10.1016/j.com, 2019.

[5] Wang, J., H. Wang, H. Zhang, and N. Cao. (2018) "Trust and Attribute-Based Dynamic Access Control Model for Internet of Things", Proc. - 2017 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2017 Jan. pp. 342–345.

[6] Ammar, M., G. Russello, and B. Crispo. (2018) "Internet of Things: A survey on the security of IoT frameworks." J. Information Security Appl. 38: 8–27.

[7] K Prathapchandran, T Janani ,A Trust-Based Security Model to Detect Misbehaving Nodes in Internet of Things (IoT) Environment using Logistic Regression, Journal of Physics: Conference Series, 2021.

[8] Jayasinghe, U., G. M. Lee, T.-W. Um, and Q. Shi. (2018) "Machine Learning based Trust Computational Model for IoT Services." IEEE Trans. Sustain. Comput. 3782 (c): 1–10.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

[9]Caminha, J., A. Perkusich, and M. Perkusich. (2018) "A Smart Middleware to Perform Semantic Discovery and Trust Evaluation for the Internet of Things" in CCNC 2018 - 2018 15th IEEE Annu. Consum. Commun. Netw. Conf. Jan. pp. 1–2.

[10] Yuan, J., and X. Li. (2018) "A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion." IEEE Access 6: 23626–23638.

[11] Patel HB, Jinwala DC (2019) Black hole detection in 6LoWPAN based internet of things: an anomaly based approach. In: TENCON 2019-2019 IEEE Region 10 Conference
(TENCON). IEEE, pp 947–954 12.

[13]M, Kaliyar P, Rabbani MM, Ranise S (2018) SPLIT: Contiki a secure and scalable RPL routing protocol for internet of things. In: 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, pp 1–8.

[14] Hatzivasilis G, Papaefstathiou I, & Manifavas C (2017). SCOTRES: Secure Routing for IoT and CPS. IEEE Internet of Things Journal, 4(6), 2129–2141. doi:10.1109/jiot.2017.2752801.

[15] Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Securing RPL routing protocol from blackhole attacks using a trust-based mechanism. 2016. 26th International Telecommunication Networks

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details