Survey of Trust Management System in Internet of Things

Meghana P.Lokhande[1], Dipti Durgesh Patil[2], Sonali Tidke[3]†

[1]Department of Computer Engineering,
Pimpri Chinchwad College of Engineering, Pune,
Research Scholar, Smt. Kashibai Navale College of Engineering, Pune, India.
[2] Department of Information Technology, MKSSS's Cummins College of Engineering for Women, Pune, India
[3]Symbiosis Institute of Technology (SIT),
Symbiosis International University, Lavale, Pune, India

Summary
The Internet of Things (IoT) enables the connection of millions of disparate devices to the World Wide Web. To perform the task, a lot of smart gadgets must work together. The gadgets recognize other devices as part of their network service. Keeping participating devices safe is a crucial component of the internet of things. When gadgets communicate with one another, they require a promise of confidence. Trust provides certainty that the gadgets or objects will function as expected. Trust management is more difficult than security management. This review includes a thorough examination of trust management in a variety of situations.

Keywords:
Trust computation, Internet of Things (IoT), IoT security, Social Internet of Things (SIoT)

1. Introduction

A network of heterogeneous machines, devices, and systems connected to the Internet and with a unique identity that makes them able to communicate, is the Internet of Things (IoT). A large number of applications including transportation, smart cities, and remote monitoring are being developed under IoT (Guo et al. 2016). Devices in network are typically identified through Identity management approach. IoT devices provide functional and non functional services to other devices. Functional attributes provide processing task using computational resources. Non functional attributes includes Quality of Services (QoS) with response time and reliability (Bahutair et al 2021). In densely populated IoT network, large number of devices creates direct communication over Internet using combinations of technologies. Consequently, IoT devices are more likely prone to possible attacks and dangers in network. The requirements associated with security and privacy in networks is therefore essential to understand.

Researchers have investigated these problems through the use of cryptography, access control, and trust-based computation. However, the paradigms still have limitations in providing information to other devices through a trusted path on the basis of node behavior. The challenge is to build trust based route that can deal efficiently with malicious nodes. The motivation is to study trust computation techniques for IoT system to identify misbehaving nodes and provide quality of services during route formation. Basically, trust computation illustrates the degree of certainty and assurance of data transmission devices. Trust reduces the risks of dealing with malicious devices. A trust relationship involves the belief that one object has on another based on direct and indirect observations. The next communication to the object can be decided based on this information.

2. Literature Survey

Secured communication channel establishment based trust score of sensor nodes is considered as important parameter while designing secured routing solution. Several cryptographic based approaches proposed to ensure security and privacy during message transmission in different environments (Rathee et al. 2018). These approaches cannot be applicable to resource constrained environment. The cryptographic solution increases storage area, communication and computation overhead. However, due to unbound connection and lack of specific method for network

Manuscript received March 5, 2024
Manuscript revised March 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.3.7

monitoring, attacks imposes severe consequences in Internet. Further delays in transmission result from these challenges.

Trust management system computes trust value of particular node based on current or previous interactions. Trust computation techniques improve security without degrading network performance (Abdulrahman et al. 2021). Trust based approach for IoT system must also deals with scalability and heterogeneity. To date, limited work on trust management system for security improvement is proposed. It is particularly important to identify misbehaving nodes that deliver services to other devices. Using IoT systems, the paper discusses trust management schemes that are at the forefront of innovation.

In (Rathee et al. 2020) proposed trust computation framework for fog environment. It calculates trust score for each device and identifies malicious devices in network. The framework considered the fog devices and IoT devices which will be converted into malicious devices during handoff. A secured routed mechanism is proposed to make system attack resistance. Trust system created between fog and IoT layers. All fog nodes within the table are recorded and malicious nodes are detected. Trust calculation model for IoT system is presented in (Warsun et al. 2019). The author provided survey of existing trust computation techniques and further trust calculation method classification is shown. The article also highlighted with challenges and research ideas in Trust management systems.

Authors in (Guo and Chen 2015) present a trust based algorithm for model driven Internet of Things systems. This approach classifies trust model based on trust dimensions. Author summarizes pros and cons of each trust dimensions and highlights defence scheme against malicious nodes. In (Bahutair et al. 2021)authors proposed trust management framework for potential producer and consumer. It calculates trust for service provider. It identifies trustworthy and untrustworthy IoT services. For accuracy and training time, the effectiveness of the approach is tested on a real-world dataset.

In (Caminha et al. 2018) proposed trust management using machine learning. Author presented elastic sliding window technique for accessing IoT trust by evaluating service attributes. This approach helps in identifying malfunctioned nodes among misbehaving nodes. This method also worked for on off attacks and faulty nodes.

Energy efficient trust management system for resource constrained application is proposed in (Zeeshan et al. 2018). This approach is used to detect malicious node behavior in IoT system. Author described three algorithms No listening for data forwarding, Listen own data forwarding and Listen to all transmissions for energy efficient IoT network. Energy efficiency is possible by measuring active listening time of IoT nodes. The author (Yan et al. 2014) describes the issues in emerging information technology such as Internet of Things (IoT). Several issues associated with trust, security, and privacy in IoT are outlined in this article. In (Ammar et al. 2018; Mosenia et al. 2016) discussed methods developed by researchers to find the trusted device in IoT. Privacy, safety and privacy implementation challenges in IoT system are discussed in (Lee et al. 2014). Trust characteristics are discussed in (Grandison and Sloman 2000; Pranata et al. 2012). A survey on trust computation methods and algorithms in IoT system presented in (Wee et al. 2016). Quality of Service based trust metric is used to evaluate trust value in (Nitti et al. 2012).

Trust computation security model based on experiences and recommendation is discussed in (Hellaoui et al. 2016). Clustered sensor network in machine to machine communication uses trust metric for identifying malicious devices in (Zhang et al. 2016). In (Yu et al. 2010; Chen et al. 2011) proposed trust computation method for analyzing node behavior in sensor network. Trust computation model is designed to monitor sensor node interaction in sensor network (Ganeriwal and Srivastava 2004). Trust parameters in community based Internet of things are proposed in (Li et al. 2010; Daly and Haahr 2009; Atzori et al. 2011). Among the trust parameters, honesty, cooperation, and community interest serve as indicators of a trusted social network. Direct and indirect trust parameters are measured to determine the value of a node's trust. Authors designed ascertain trust in social using trust based scheme in (Nitti et al. 2014). The author node trust is evaluated by aggregating trust from common friends and direct experiences.

3. Materials and Methods

3.1. Primary database collection

Data can be used for Bibliographic analysis from different sources such as Scopus, web of science, ACM or IEEEXplore. This work is focused on Scopus database. It has advanced search feature which is helpful to find ground level items for bibliometric analysis. Scopus provides citations and abstracts of peer-reviewed research literature, as well as entries in the social sciences, arts, and humanities. A detailed study for bibliometric analysis of data from Scopus database is presented in this section.

3.2. Framing of the Keywords:

Trust computation keywords are categorized into two groups: master keywords and primary keywords. After various combinations of keywords, following set of keywords is finalized.

TITLE-ABS-KEY ("Internet of Things Security") OR trust AND computation OR trust AND management AND system

4. Results and Discussion

Two kinds of analysis are conducted, statistical analysis of the database and network analysis.

4. Statistical Analysis

4.1 Publication Trends

The article with Internet of things security and trust computation technique keywords were searched from the year 2014.

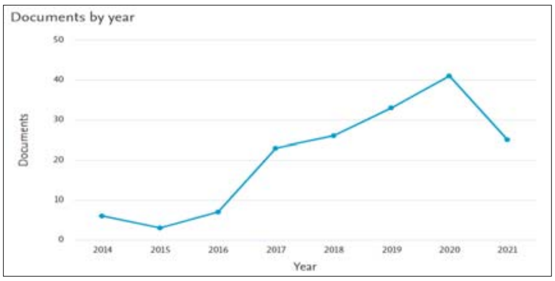

Fig. 1. Year-wise Publication trends
Source: http://www.scopus.com (accessed on 05-08-2021)

It shows improvement in number of publication till year 2020. In year 2020, significant research has done in trust computation techniques.

Table 1. Year wise publication count

Year	Number of documents
2021	25
2020	41
2019	33
2018	26
2017	23
2016	7
2015	3
2014	6

4.2 Document Type Analysis

Document type analysis shows documents of type article, review and conference papers. There are 79.2% of publications published by Scopus that are article-type documents. Article type is followed by conference papers with 23.8% and review with 3.0%. The document type distribution has shown by pie chart in figure 2.

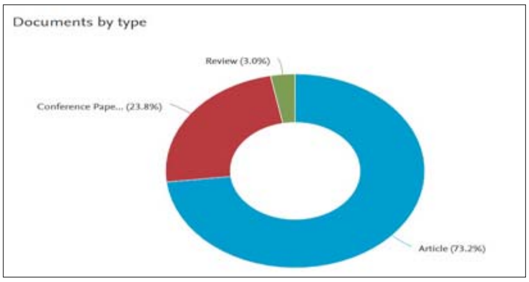

Fig. 2. Documents by type analysis in Pie chart representation

4.3 Analysis by Subject area

Documents with keywords internet of things security using trust computation technique are not only found in engineering and computer science but also in material science, decision science, mathematics, physics, chemistry, and chemical engineering. Figure 3 shows Document analysis by subject areas in pie chart representation.

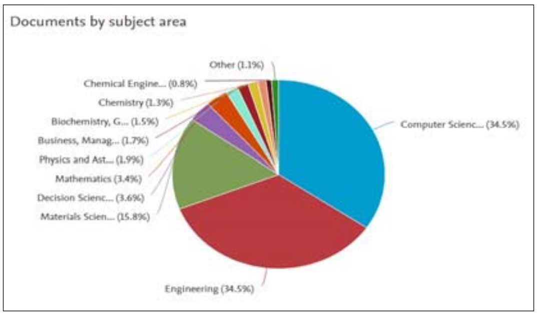

Fig. 3. Documents by subject area in Pie chart representation

4.4 Geographical Analysis

Figure 4 presents details of countries involved for trust computation research. It shows China carried out detailed research on IoT security using trust computation. The research in Internet of Things security is carried by various countries all over world. The top 10 countries research in same area is considered for analysis.

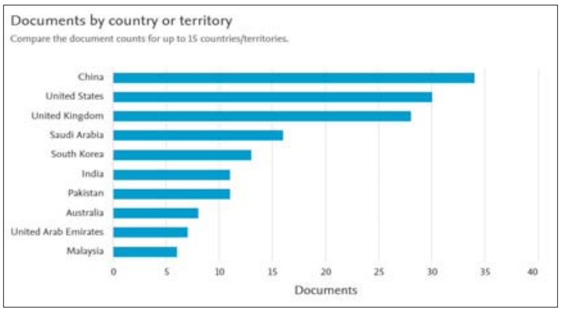

Fig. 4. Publications by Country analysis

4.5 Document Analysis by Affiliations

This type of analysis shows research work carried out in Internet of Things security by different organizations. Figure 5 shows document analysis by affiliations using Scopus database. Top 15 organizations contributed to research are shown along with count of documents. King Saud University has done most of the work in this research area.

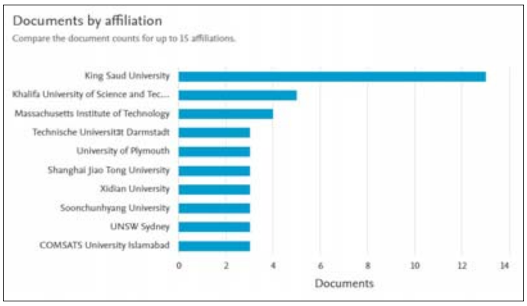

Fig. 5. Document analysis by affiliations

4.6 Source Type Analysis

In this section, Figure 6 presented analysis of number of research article published in renowned journal. It is observed that maximum numbers of articles are published in IEEE Access followed by Computers Materials and Continua, Sensors, Wireless Communications and Mobile Computing and Advances in Intelligent Systems and Computing. Table gives documents per year by source.

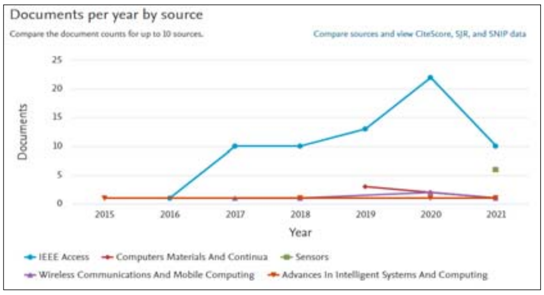

Fig. 6. Document per year by source

Table 2: Per year document by source (Scopus database accessed on 05-08-2021)

Source	Documents
IEEE Access	66
Computers Materials and Continua	6
Sensors	6
Wireless Communications and Mobile Computing	5
Advances in Intelligent Systems and Computing	4

4.7 Analysis by Funding Agencies

Figure 7 shows research analysis done by funding agencies. According to National Natural Science Foundation of China, the maximum funds have been allocated for IoT security research. European commission, horizon 2020 Framework programme and many more funding sponsors as shown figure 7 have provided funds to carry out research.

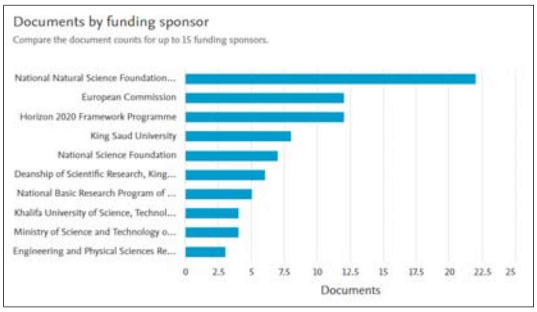

Fig. 7. Documents by funding agencies

4.8 Analysis on Number of Documents by Author

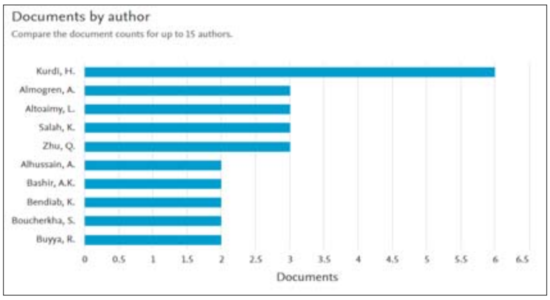

Fig. 8. Number of documents by author

Figure 8 below shows top 15 authors' research work. Kurdi, H. has maximum number of publication in this research area.

5. Network Analysis

5.1 Co-occurrence of author's keywords

Statistical parameter relationship is represented using network analysis. VOS viewer is open source software for constructing and visualizing bibliographic coupling. The network for analysis is constructed using data downloaded from Scopus database. Co-citation, co-occurrence and co-authorship relationship construction and visualization are possible using VOS viewer open source tool. Trust computation and trust management system keywords are used for finding research document in Scopus database. Co-occurrences and index keyword using overlay visualization in VOS viewer in shown in figure 9. Minimum number of keyword occurrence is selected as 3 from total 1217 documents and 132 keywords meet the threshold.

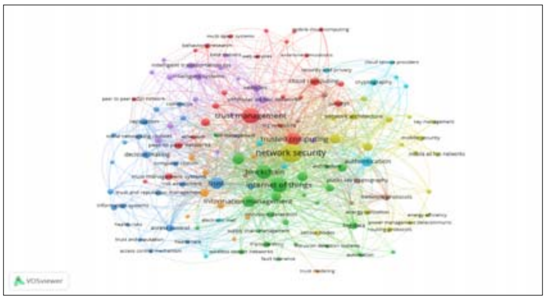

Fig. 9. Co-occurrence of author's keywords overlay visualization

5.2 Co-authorship and author's analysis

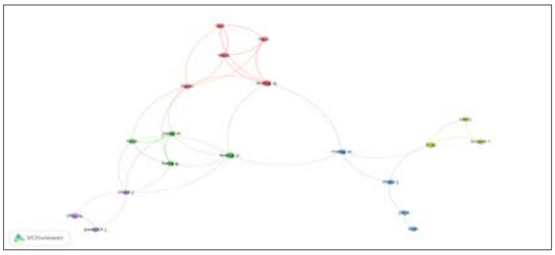

Fig. 10. Overlay visualization co-authorship and author analysis

Figure 10 shows overlay visualization for co-authorship analysis for Scopus database. 56 authors are selected and 2 minimum documents are considered.

5.3 Citations and authors

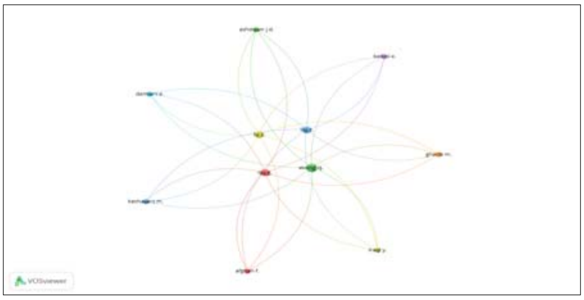

Fig. 11. Citation analysis using VOS Viewer

Figure 11 shows publication title network using VOS viewer citations are considered. Color and label indicates citation linkage by publication.

6. Conclusion

Bibliometric analysis on trust computation in Internet of Things security is carried out using Scopus database. The database is considered from the year 2014 to 2021. Total 164 articles are retrieved using keyword search. The document analysis show worldwide research contribution. Based on document-by-year analysis, it appears that most research work was published in

2020. China followed by United States and United Kingdom have major contribution in IoT area. The subject area analysis has shown 68.5% contribution Computer Science and Engineering field. This analysis is conducted using the VOS Viewer 1.6.16 version of the software. An analysis is performed using parameters like co-authorship and co-occurrence. Based on network analysis with different parameters, the biggest contributions to this topic have come during the period 2019 and 2020. It could be commented that trust computation in IoT has great potential in the future.

References

[1] Abdulrahman Aminu Ghali, Rohiza Ahmad and Hitham Alhussian 2021. A Framework for Mitigating DDoS and DOS Attacks in IoT Environment Using Hybrid Approach. Electronics, 10, 1282.

[2] 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.

[3] Bahutair, M., Bouguettaya, A., & Neiat, A.G. 2021. Multi-Perspective Trust Management Framework for Crowd sourced IoT Services. ArXiv, abs/2101.04244.

[4] Caminha, Jean & Perkusich, Angelo & Perkusich, Mirko. 2018. A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things. Security and Communication Networks. 2018. 1-10. 10.1155/2018/6063456.

[5] Chen D, Chang G, Sun D, Li J, Jia J, Wang X. 2011. TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things. Comput Sci Inf Syst; 8(4):1207e28.

[6] E. M. Daly, and M. Haahr 2009. Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs. IEEE Transactions on Mobile Computing, vol. 8, no. 5, pp. 606-621.

[7] Ganeriwal S, Srivastava M. B. 2004. Reputation-based framework for high integrity sensor networks. In: Proc. ACM security for adhoc and sensor networks. p. 66e7.

[8] Grandison, T., and M. Sloman. 2000. A Survey of Trust in Internet Applications." IEEE Communication Surveys Tutorials 3 (4): 2–16.

[9] Guo, J., & Chen, I. 2015. A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems. *2015 IEEE International Conference on Services Computing*, 324-331

[10] Guo, Jia & Chen, Ing-Ray & Tsai, Jeffrey. 2016. A Survey of Trust Computation Models for Service Management in Internet of Things Systems. Computer Communications. 97. 10.1016/j.comcom.2016.10.012.

[11] H. Hellaoui, A. Bouabdallah, and M. Koudil 2016. TAS-IoT: Trust-Based Adaptive Security in the IoT," in Proceedings of the 41st IEEE Conference on Local Computer Networks (LCN '16), pp. 599–602.

[12] Lee, J.-Y., W.-C. Lin, and Y.H. Huang. 2014. A Lightweight Authentication Protocol for Internet of Things", in International Symposium on Next-Generation Electronics (ISNE).

[13] L. Atzori, A. Iera, and G. Morabito 2011. SIoT: Giving a Social Structure to the Internet of Things," *IEEE Communication Letters,* vol. 15, no. 11, pp. 1193-1195.

[14] M. Nitti, R. Girau, L. Atzori, and S. Member 2014. Trustworthiness Management in the Social Internet of Things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253–1266.

[15] Mosenia, A., and N. K. Jha. 2016. A Comprehensive Study of Security of Internet-of-Things." IEEE Trans. Emerg. Top. Comput. 5 (4): 1– 1.

[16] Nitti, M., R. Girau, L. Atzori, A. Iera, and G. Morabito. 2012. A Subjective Model for Trustworthiness Evaluation in the Social Internet Of Things. IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Comm. - (PIMRC). pp. 18–23.

[17] Pranata, I., G. Skinner, and R. Athauda. 2012. A Holistic Review on Trust and Reputation Management Systems for Digital Environments. Int. J. Comput. Inf. Technol. 1 (1): 44–53.

[18] Q. Li, S. Zhu, and G. Cao 2010. Routing in Socially Selfish Delay Tolerant Networks. IEEE Conference on Computer Communications, San Diego, CA, pp. 1-9.

[19] Rathee, G., Saini, H., & Singh, G. 2018. Aspects of trusted routing communication in smart networks. Wireless Personal Communications, 98(2), 2367–2387.

[20] Rathee Geetanjali, Sandhu Rajinder, Saini Hemraj, Sivaram, M, Vigneswaran, Dhasarathan 2020. A trust computed framework for IoT devices and fog computing environment. Wireless Networks; New York Vol. 26, Iss. 4, pp.1-13.

[21] T. Zhang, L. Yan, and Y. Yang 2016. Trust evaluation method for clustered wireless sensor networks based on cloud model," Wireless Networks, pp. 1–21.

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

[23] Wee, B. Van, and D. Banister 2016. How to Write a Literature Review Paper. Transp. Rev. 36 (2): 278–288.

[24] Yan, Z., P. Zhang, and A. V. Vasilakos. 2014. A Survey on Trust Management for Internet of Things." J. Netw. Comput. Appl. 42: 120– 134.

[25] Yu H, et al. 2010. A survey of trust and reputation management systems in wireless communications. Proc IEEE 2010; 98(10):1755e72.

[26] Zeeshan Ali Khan 2018. Using energy-efficient trust management to protect IoT networks for smart cities, Sustainable Cities and Society, Volume 40, Pages 1-15.