International Journal of Safety and Security Engineering
Vol. 13, No. 2, April, 2023, pp. 341-347
Journal homepage: http://iieta.org/journals/ijsse

Trust Management System in Internet of Things: A Survey

Meghana Lokhande[1*], Dipti Durgesh Patil[2], Sonali Kothari[3], Shital Pawar[4], Shweta Koparde[5]

[1] Department of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune 411044, India
[2] Department of Information Technology, MKSSS's Cummins College of Engineering for Women, Pune 411038, India
[3] Symbiosis Institute of Technology, Symbiosis International (Deemed University), Lavale, Pune 412115, India
[4] Department of Computer Engineering, Bharti Vidyapeeth's College of Engineering for Women, Pune 411046, India
[5] Department of Computer Engineering, Dr. DY Patil Institute of Technology, Pimpri, Pune 412303, India

Corresponding Author Email: meghna.ingole1983@gmail.com

https://doi.org/10.18280/ijsse.130216

Received: 6 March 2023
Accepted: 13 April 2023

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

ABSTRACT

The Internet of Things (IoT) enables the connection of millions of disparate devices to the World Wide Web. Various smart devices must cooperate in order to complete the task. According to security experts, there are lot of risks related to IoT devices. Access control systems and protocols have faced a number of difficulties as a result of the development of the Internet of Things (IoT). 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. In order to increase security and usability of such modern technologies, trust between internet-connected devices and access control techniques is essential. Based on the facts presented, this article will help researchers create better access control techniques for the Internet of Things using trust based approach. The paper examines several access control and trust methods that could be applied in an IoT environment. An access control component is necessary to provide either access services to these recently connected devices or to those that have been joined to the IoT network for a long period. Scalable and dynamic trust computation is needed to provide dynamic access control. This review includes a thorough examination of trust management in a variety of situations and suggested design of trust computation model to provide access permission to IoT devices.

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). According to Bandyopadhyay and Sen [1], IoT provides immediate access to data for improved device functionality and performance. 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. Different WSN protocols have recently been proposed, improving security, dependability, and energy efficiency is discussed in the study [2]. A huge number of devices use a variety of technologies to create direct Internet communication in a densely populated IoT network. As a result, IoT devices are more likely to be vulnerable to potential attacks and network risks. Therefore, it is crucial to comprehend the needs for network security and privacy. 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 discussed in Rathee et al. [3]. 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 monitoring, attacks impose 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. 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.

Rathee et al. [4] 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 the study [5]. 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.

Guo and Chen [6] 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. Bahutair et al. [7] 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.

Caminha et al. [8] 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 by Khan [9]. 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. Zhang et al. [10] describe 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. The authors [11, 12] discussed methods developed by researchers to find the trusted device in IoT. Privacy, safety and privacy implementation challenges in IoT system are discussed in the study by Lee et al. [13]. Trust characteristics are discussed in the studies by Grandison and Sloman [14] and Pranata et al. [15]. A survey on trust computation methods and algorithms in IoT system presented in Wee and Banister [16]. Quality of Service based trust metric is used to evaluate trust value in Nitti et al. [17].

Trust computation security model based on experiences and recommendation is discussed in Hellaoui et al. [18]. Clustered sensor network in machine to machine communication uses trust metric for identifying malicious devices in the study by Yan et al. [19]. The authors [20, 21] proposed trust computation method for analyzing node behavior in sensor network. Trust computation model is designed to monitor sensor node interaction in sensor network discussed in Ganeriwal and Srivastava [22]. Trust parameters in community based Internet of Things are proposed in the studies [23-25]. 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. [26]. The author node trust is evaluated by aggregating trust from common friends and direct experiences.

The numerous research is done on the access control methods to provide safe communication on IoT environment.

In Kaur et al. [27], capability-based strategies are illustrated. It provides a conventional capability-based approach and examines issues with access control from the viewpoint of the user. Additionally, it is said to be more efficient than conventional approaches. Authors suggested conducting a study on IoT context awareness from the viewpoint of the commercial market presented in Perera et al. [28]. The basis for access authorization in Kuhn et al. [29] is Roles, which can only be granted permissions by an administrator. An admin or user cannot alter the privileges provided to a user, and the user may delegate some, all, or none of their role to another user.

The aforementioned rule does not seem to apply when a user has to temporarily delegate part of their powers or obligations to a trusted user. It demonstrates the need for a safe access control system in an IoT context in Ferraiolo et al. [30]. Theoretically, an approach based on capabilities refers to an unforgeable ticket to obtain resources listed on the capability discussed in Hernández-Ramos et al. [31]. The concept of an organisation, which is defined as a well-organized collection of operational units, serves as the foundation for the Access Control in Organisations system. In order to play out various roles, subjects were used. While a group of things is viewed as a view, a collection of activities can always be conceived of as an activity presentd in Kalam et al. [32]. The primary problem with this paradigm is its centralised structure, which results in a host of complications. It has problems with large-scale implementation, and the absence of a simple instrument or procedure makes it challenging to implement.

I. Trust Computation Model

To identify the node legitimaty, trust computation method is useful. The following trust parameters are considered for trust based device identification.

a. Direct Trust (DTS)

Reliable packet (RPA) and device availability (DAA) parameters are considered for asseing direct trust.

Node n^i direct trust as computed by node n^j at time t is reflected in the DTS. This trust is calculated based on successful packet transmission.

$$\mathrm{DTS}(\mathrm{n}(\mathrm{t})) = \left(\alpha^1 \times RPA(\mathrm{n}^{\mathrm{i,j}})\right) + \left(\alpha^2 \times DAA(\mathrm{n}^{\mathrm{i,j}})\right) \quad (1)$$

b. Indirect Trust (IDS)

Packet Delivery Ratio (PD), Energy Available (EI), and Nearest Node Neighbor (NN) are the parameters used to generate indirect trust ratings. The EI is used to lower a node's energy consumption, the PD is used to estimate a node's packet reception rate, and NN is used to represent the degree of neighbor sensor nodes.

Using a weighting method, the total trust score of node n is calculated:

$$\mathrm{IDS} = \alpha^1 \times \mathrm{PD}^{\mathrm{n}} + \alpha^2 \times \mathrm{EI}^{\mathrm{n}} + \alpha^3 \times \mathrm{NN}^{\mathrm{n}} \quad (2)$$

The values for α^1, α^2, & α^3 are chosen such that sum is 1. The final trust score ranges from 0 to 1. A device is considered to be legitimate if it has a high trust score value.

Access permissions are assigned based on the trust score. The fuzzy inference system uses both direct and indirect trust score for assigning rights to devices shown in Figure 1.

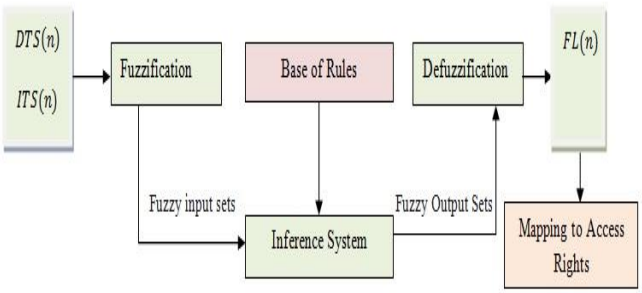

Figure 1. Fuzzy inference system for access control

The fuzzy model mainly consists of four blocks as follows. Fuzzification: The two trust scores are fuzzified and divided into three linguistic variables depending on their values: low, average, and high.

- Base of Rules: Base of rules gives the node reliability based on the rules formed having input values, direct and indirect trust score.
- Inference System: Using the rules from rule base, fuzzy decision has to be taken.
- Defuzzification: This stage takes node reliability (NR) and performs defuzzification to determine the final prediction of node or device.

$$FL(n) = \begin{cases} 1, & NR(n) = =' \text{ highly trusted}' \\ 2 & NR(n) ==' trusted' \\ 3 & NR(n) ==' rather\ trusted' \\ & else\ \ 4 \end{cases} \quad (3)$$

- Access Rights:
  Access rights are given to the devices based on the type of node reliability.
  The suggested method ensures the secured path through which only legitimate devices will communicate with their access permission.

3. MATERIALS AND METHODS

1. Primary database collection

Data can be used for Bibliographic analysis from different sources such as Scopus, web of science, ACM or IEEEXplore. The study looks at current work that has used a trust-based methodology as well as static analysis. It offers a sophisticated search capability that can be used to locate materials for bibliometric analysis. Scopus provides citations and abstracts of peer-reviewed research literature, as well as entries in the social sciences, arts, and humanities. Scopus database provides the detailed dataset which helps in analyzing the work done on particular topic till the mentioned period. A detailed study for bibliometric analysis of data from Scopus database is presented in this section.

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. STATISTICAL ANALYSIS

4.1 Publication trends

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

It shows improvement in number of publications till year 2020. In year 2020, significant research has done in trust computation techniques (Figure 2).

4.2 Document type analysis

Document type analysis shows documents of type article, review and conference papers.

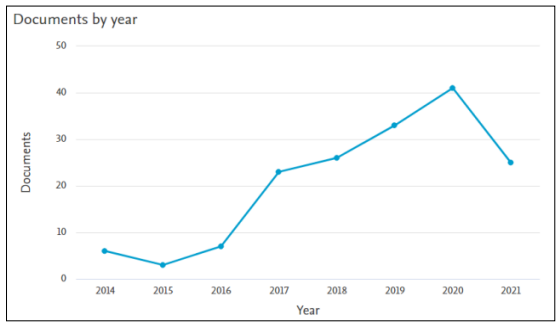

Figure 2. Year-wise publication trends
Source: http://www.scopus.com (accessed on 05-08-2021)

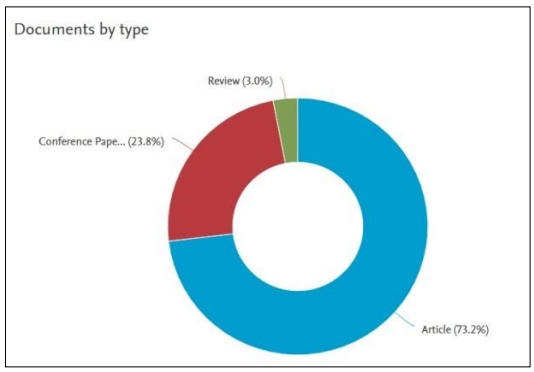

Figure 3. Documents by type analysis in Pie chart representation

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

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 3 and year wise count is shown in Table 1.

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 4 shows Document analysis by subject areas in pie chart representation.

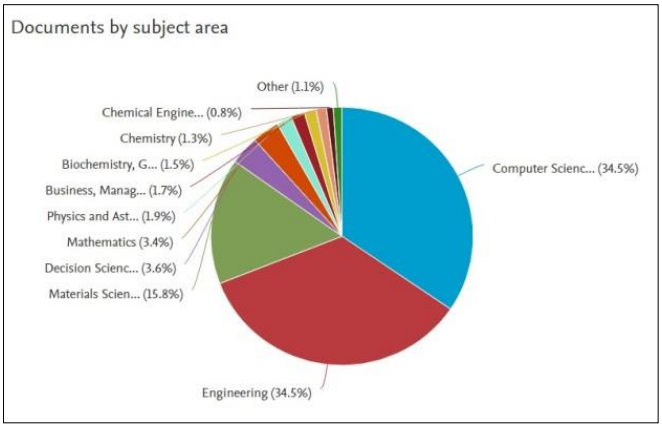

Figure 4. Documents by subject area in Pie chart representation

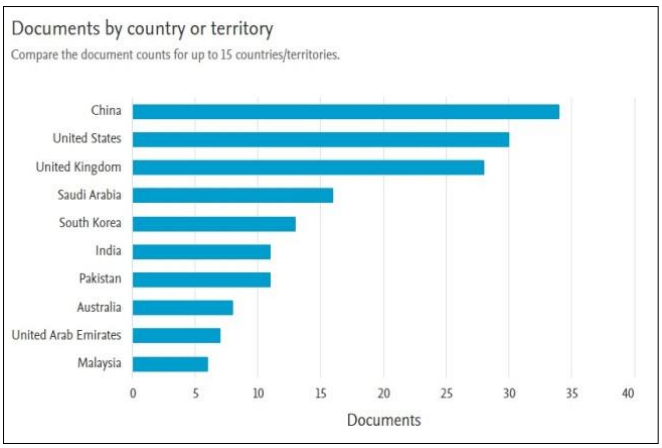

Figure 5. Publications by country analysis

4.4 Geographical analysis

Figure 5 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.

4.5 Document analysis by affiliations

This type of analysis shows research work carried out in Internet of Things security by different organizations. Figure 6 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.

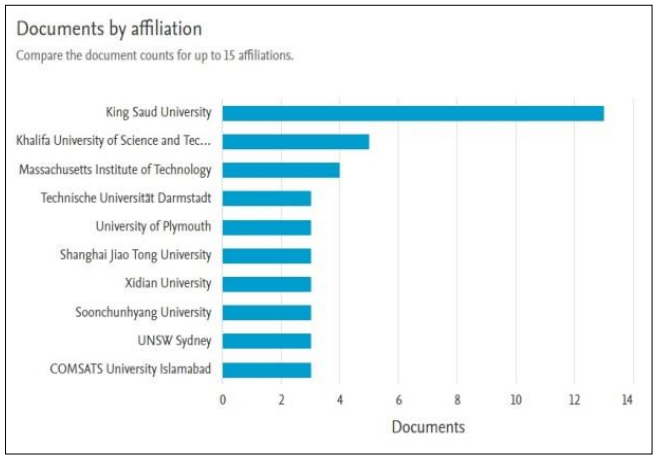

Figure 6. Document analysis by affiliations

4.6 Source type analysis

In this section, Figure 7 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.

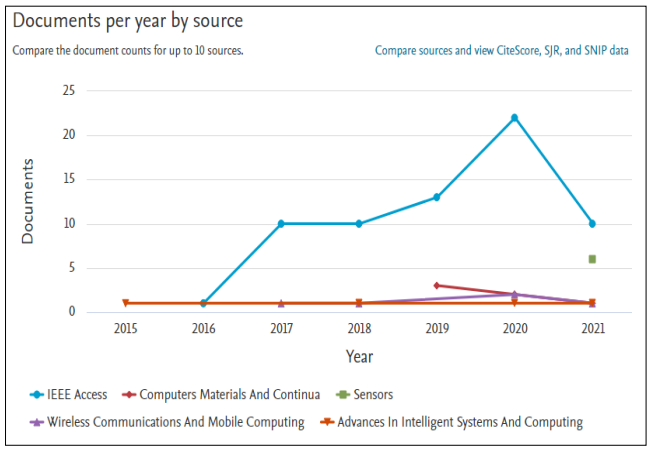

Figure 7. Document per year by source

4.7 Analysis by funding agencies

Table 2 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 in Figure 8 have provided funds to carry out research.

4.8 Analysis on number of documents by author

Figure 9 below shows top 15 authors' research work. Kurdi, H. has maximum number of publications in this research area.

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

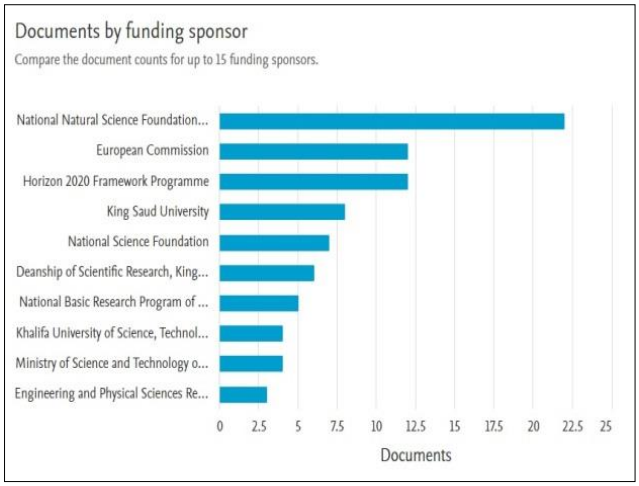

Figure 8. Documents by funding agencies

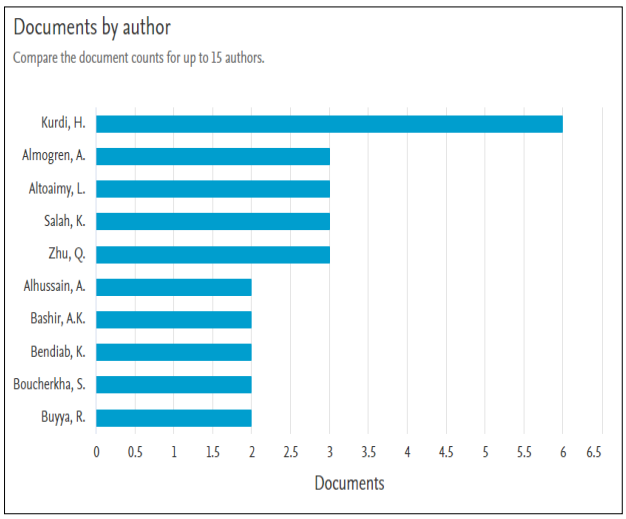

Figure 9. Number of documents by author

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. The open source VOS tool provides detailed network analysis by providing the input as keywords. The author have to search the database by giving relevant input keyword. The tool itself provides the values that author need to be represented in result form. Co-occurrences and index keyword using overlay visualization in VOS viewer in shown in Figure 10. Minimum number of keyword occurrence is selected as 3 from total 1217 documents and 132 keywords meet the threshold.

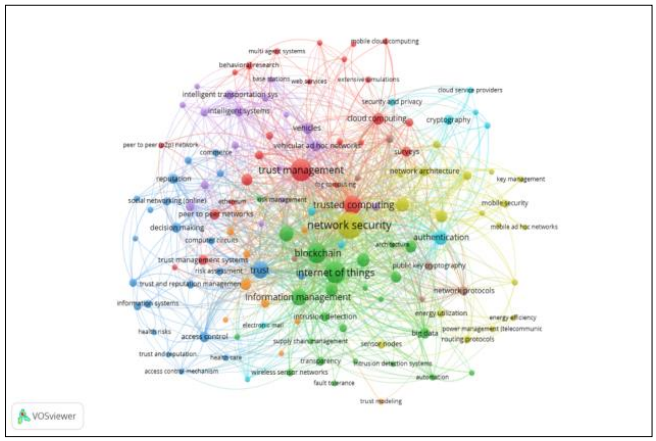

Figure 10. Co-occurrence of author's keywords overlay visualization

5.2 Co-authorship and author's analysis

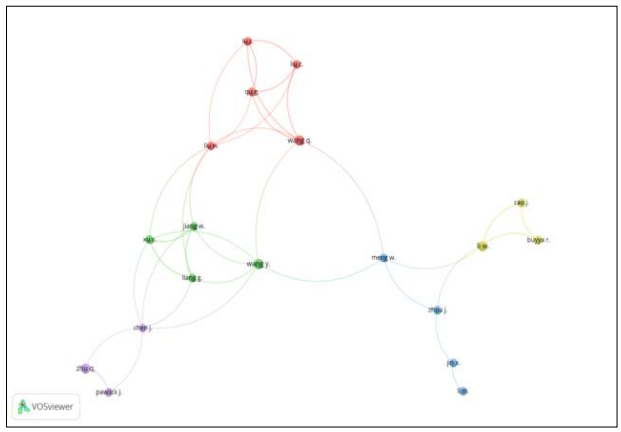

Figure 11. Overlay visualization co-authorship and author analysis

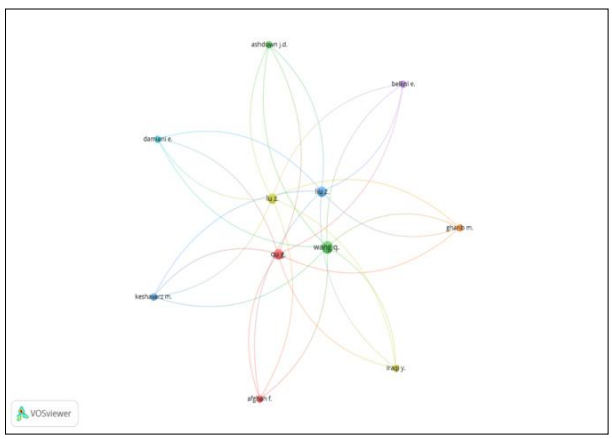

Figure 12. Citation analysis using VOS viewer

Figure 11 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

Figure 12 shows publication title network using VOS viewer citations are considered. Color and label indicate 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 shows 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. The suggested techniques help in providing secured network by identifying legitimate devices using their trust score. This ensures secured end to end communication. It could be commented that trust computation in IoT has great potential in the future.

REFERENCES

[1] Bandyopadhyay, D., Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1): 49-69. https://link.springer.com/article/10.1007/s11277-011-0288-5#citeas

[2] Chhabra, A., Vashishth, V., Sharma, D. K. (2018). A fuzzy logic and game theory-based adaptive approach for securing opportunistic networks against black hole attacks. International Journal of Communication Systems, 31(4): e3487. https://doi.org/10.1002/dac.3487

[3] Rathee, G., Saini, H., Singh, G. (2018). Aspects of trusted routing communication in smart networks. Wireless Personal Communications, 98(2): 2367-2387. https://doi.org/10.1007/s11277-017-4978-5

[4] Rathee, G., Sandhu, R., Saini, H., Sivaram, M., Dhasarathan, V. (2020). A trust computed framework for IoT.

[5] Najib, W., Sulistyo, S. (2019). Survey on trust calculation methods in Internet of Things. Procedia Computer Science, 161: 1300-1307. https://doi.org/10.1016/j.procs.2019.11.245

[6] 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.

[7] Bahutair, M., Bouguettaya, A., Neiat, A.G. (2021). Multi-perspective trust management framework for crowd sourced IoT services. ArXiv, abs/2101.04244.

[8] Caminha, J., Perkusich, A., Perkusich, M. (2018). A smart trust management method to detect on-off attacks in the Internet of Things. Security and Communication Networks, 2018: 6063456. https://doi.org/10.1155/2018/6063456

[9] Khan, Z.A. (2018). Using energy-efficient trust management to protect IoT networks for smart cities. Sustainable Cities and Society, 40: 1-15. https://doi.org/10.1016/j.scs.2018.03.026

[10] Zhang, T., Yan, L., Yang, Y. (2018). Trust evaluation method for clustered wireless sensor networks based on cloud model. Wireless Networks, 24: 777-797. https://doi.org/10.1007/s11276-016-1368-y.

[11] Ammar, M., Russello, G., Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38: 8-27. https://doi.org/10.1016/j.jisa.2017.11.002

[12] Mosenia, A., Jha, N.K. (2016). A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, 5(4): 586-602. https://doi.org/10.1109/TETC.2016.2606384

[13] Lee, J.Y., Lin, W.C., Huang, Y.H. (2014). A lightweight authentication protocol for internet of things. In 2014 International Symposium on Next-Generation Electronics (ISNE), Kwei-Shan Tao-Yuan, Taiwan, pp. 1-2. https://doi.org/10.1109/ISNE.2014.6839375

[14] Grandison, T., Sloman, M. (2000). A survey of trust in internet applications. IEEE Communications Surveys & Tutorials, 3(4): 2-16. https://doi.org/10.1109/COMST.2000.5340804

[15] Pranata, I., Skinner, G., Athauda, R. (2012). A holistic review on trust and reputation management systems for digital environments. International Journal of Computer and Information Technology, 1(1): 44-53.

[16] Wee, B.V., Banister, D. (2016). How to write a literature review paper? Transport Reviews, 36(2): 278-288. https://doi.org/10.1080/01441647.2015.1065456

[17] Nitti, M., Girau, R., Atzori, L. (2013). Trustworthiness (2012). A subjective model for trustworthiness evaluation in the Social Internet of Things. In 2012 IEEE 23rd international symposium on personal, indoor and mobile radio communications-(PIMRC), Sydney, NSW, Australia, pp. 18-23. https://doi.org/10.1109/PIMRC.2012.6362662

[18] Hellaoui, H., Bouabdallah, A., Koudil, M. (2016). Tas-iot: Trust-based adaptive security in the IoT. In 2016 IEEE 41st conference on local computer networks (LCN), Dubai, United Arab Emirates, pp. 599-602. https://doi.org/10.1109/LCN.2016.101

[19] Yan, Z., Zhang, P., Vasilakos, A.V. (2014). A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42: 120-134. https://doi.org/10.1016/j.jnca.2014.01.014

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

[21] 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. Computer Science and Information Systems, 8(4): 1207-1228. https://doi.org/10.2298/CSIS110303056C

[22] Ganeriwal S, Srivastava MB. Reputation-base framework for high integrity sensor networks. In: Proc. ACM security for adhoc and sensor networks 2004. p. 66e7.
[23] Li, Q., Zhu, S., Cao, G. (2010). Routing in socially selfish delay tolerant networks. In 2010 Proceedings IEEE Infocom, San Diego, CA, USA, pp. 1-9. https://doi.org/10.1109/INFCOM.2010.5462138
[24] Daly, E.M., Haahr, M. (2008). Social network analysis for information flow in disconnected delay-tolerant MANETs. IEEE Transactions on Mobile Computing, 8(5): 606-621. https://doi.org/10.1109/TMC.2008.161
[25] Atzori, L., Iera, A., Morabito, G. (2011). Siot: Giving a social structure to the Internet of Things. IEEE Communications Letters, 15(11): 1193-1195. https://doi.org/10.1109/LCOMM.2011.090911.111340
[26] Nitti, M., Girau, R., Atzori, L., Iera, A., Morabito, G. (2012). A subjective model for trustworthiness evaluation in the Social Internet of Things. In 2012 IEEE 23rd international symposium on personal, indoor and mobile radio communications-(PIMRC), Sydney, NSW, Australia, pp. 18-23. https://doi.org/10.1109/PIMRC.2012.6362662
[27] Kaur, M., Jadhav, A., Akter, F. (2022). Resource selection from edge-cloud for IIoT and blockchain-based applications in industry 4.0/5.0. Security and Communication Networks, 2022: 1-10. https://doi.org/10.1155/2022/9314052
[28] Perera, C., Liu, C.H., Jayawardena, S., Chen, M. (2014). A survey on Internet of Things from industrial market perspective. IEEE Access, 2: 1660-1679. https://doi.org/10.1109/ACCESS.2015.2389854
[29] Kuhn, D.R., Coyne, E.J., Weil, T.R. (2010). Adding attributes to role-based access control. Computer, 43(6): 79-81.
[30] Ferraiolo, D.F., Barkley, J.F., Kuhn, D.R. (1999). A role-based access control model and reference implementation within a corporate intranet. ACM Transactions on Information and System Security (TISSEC), 2(1): 34-64. https://doi.org/10.1145/300830.300834
[31] Hernández-Ramos, J.L., Jara, A.J., Marin, L., Skarmeta, A.F. (2013). Distributed capability-based access control for the Internet of Things. Journal of Internet Services and Information Security (JISIS), 3(3/4): 1-16.
[32] Kalam, A.A.E., Baida, R.E., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C., Trouessin, G. (2003). Organization based access control. In Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks, Lake Como, Italy, pp. 120-131. https://doi.org/10.1109/POLICY.2003.1206966