Research Trends of Network Security in IoT: A Comparative Review

Kapil Joshi[1]

Department of CSE, Uttaranchal of Technology, Uttaranchal University, Dehradun, India

Kapilengg0509@gmail.com

Adarsh Kumar[2]

School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttrakhand, India

adarsh.kumar@ddn.upes.ac.in

Minakshi Memoria[3]

UIT, Uttaranchal University, Dehradun, India

minakshimemoria@gmail.com

Rajiv Kumar[4]

Uttaranchal School of Computing Sciences, Uttaranchal University, Dehradun, India

rajiv.gill1@gmail.com

Abstract.

In the last decade, Technology is constantly evolving and producing new products numerous revolution. The Internet of Things (IoT) is a concept regarded as one of the most significant technological transformation. (IoT) connects two worlds: virtual and physical. We discuss in this paper conduct a comprehensive review of the literature on the various factors, challenges and threats that have had an impact on network security in the IoT domain. To identify the articles for the systematic review, on selected databases, we conducted a keyword search. There are 712 full-text articles in total were discussed, and the findings disclosed that several architectures and protocols are used to secure the IoT. The findings also emphasized the importance of improved IoT network security. In this paper, We also conversed about future studies opportunities, which are expected to inspire more research in the area of IoT network security.

Keywords. Internet of Things (IoT), Network Security, Internet of Things Devices.

1. INTRODUCTION

The Internet of Things (IoT) refers to a collection of physical objects connect via as well as cyberspace communication procedure that takes place inside it. The system facilitates the exchange of massive transferring large amounts of data between devices [1] without the need for Human intervention is required. According to Gartner, The number of people who use interconnected devices will reach 6.4 billion by 2016, which is 30 times the quantity of connected devices in 2009. According to projections, this figure will surpass 20.8 billion by 2020. These devices are now being used in a variety of industries. Indeed, there is a rise in demand for these gadgets in a variety of direction as such as smart homes, wearable’s, e-health, manufacturing automobile, automation, agricultural farming, supply chain, as well as other operational technologies. Regardless of how unexpected surge there are still a little available Concerns about the security of these devices that must be addressed. According to a study conducted by HP, approximately 70% of the majority of commonly used Wearable computing (IoT) devices is vulnerable in user access permissions, encryption, password [2] security, and other areas. These dangers primarily include PUAs, Distributed Rejection of Service (DDoS), or other forms of cybercrime of cybercrime. Some human values are shown in figure 1.1.

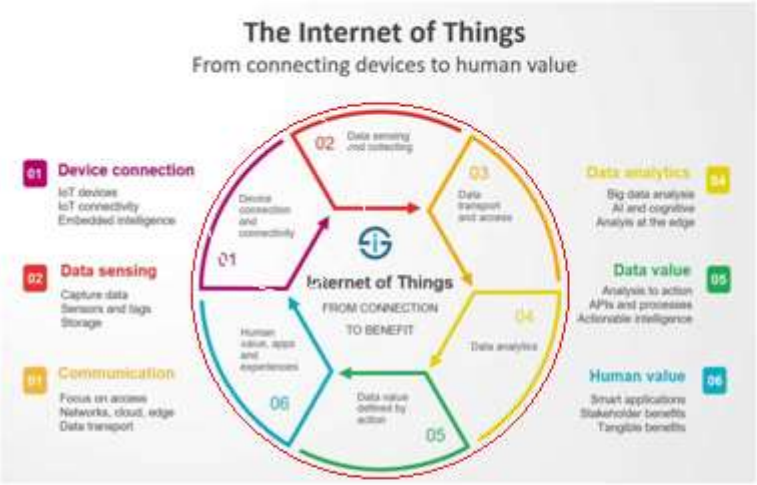

Figure 1.1. IoT for human values [3]

Because IoT devices can communicate with networks require multiple layers of protection. A variety of protocols, security policies, procedures and algorithms, are used to ensure the layers' security. These measures are critical [3] in the fundamental security implications of IoT, which is also the central concept investigated within this paper.

The following is how article is organized: Section 2 goes into great detail about the research process. Section 3 discusses the review's findings, which form the basis for the main discussion in Section 4. Section 5 contains an overview of our significant contribution and a discussion of the study's restriction.

2. Research Approach

We have conducted a systematic research approach on multiple methods. Further we are classifying the three categories. These are as below:

2.1. Research Overview

We conducted a systematic review addressing the research questions posed above using a non-experimental approach based on content analysis. The content analysis contributes to the development of a methodical and structured reach to identifying and trying to describe text materials in the current body of knowledge [4]. We refined the text materials in this paper using a table of contents with to categories the key components of the text content that [3] will serve as appropriate examples, use categories and sub-categories. We documented our findings, and Sections 3 and 4 of this article discuss our findings based on those observations.

2.2. Classification Framework

We discuss in this paper used the procedures [4] proposed by Higgins and Green as well as Kitchenham et al. for conducting a thorough analysis of classification guidelines was conducted. The rulebook includes six descriptors: journal year, or title, conference, volume number, associated SDLC Phase, author keywords, security phase relevance, as well as key security terms.

2.3. Data Collection

We used keyword searches to search the databases of Science Direct, Springer, ACM Digital Library, IEEE Xplore, and Wiley InterScience [5]. To choose the texts or publications for analysis, use the phrase 'IoT but also NETWORK SECURITY' in the 'AND' format. The search term was used in Full Text and Metadata. The procedure was carried out throughout the months of November and December of 2016. During the search, we excluded standards, prefaces, editorials, courses, workshops, tutorials, poster sessions, and other English language articles. Text substances or articles are retrieved during in the lookup of the databases [6].

There are 2906 matches listed there are duplicates in Table 1. We filtered the pulled articles further to determine their suitability for use. We used to detect exclusion articles applicable to the Internet of Things and network security domains [6]. Database analyses are performed in figure 2.1.

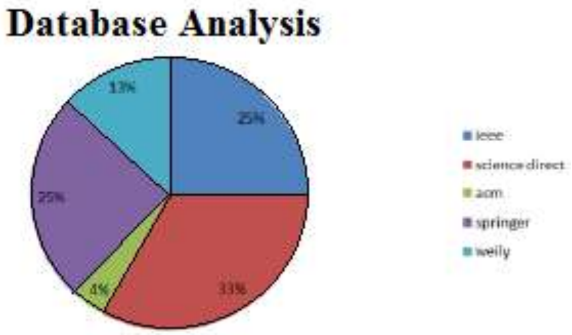

Figure 2.1. Database Analysis in Various Journal

Table 2.1 Results on Database

Sr. No.	Database (Conference & Journal)	No. Of Hits
1	IEEE Xplore	740
2	ACM Digital Library	121
3	Science Direct	974
4	Springer Link	725
5	Wiley Inter Science	390
6	**Total**	**2,950**

3. FINDINGS

We conducted a systematic review of 712 articles resulting from the database selection process. There are 627 journal articles, 5 booklets, but also 80 conference proceedings among the number 712. 535 papers have been published among these years 2010, 2013, 2017 and 2021. Papers submitted among 2014 and 2016 (including both years), and eight articles published between the years 1983 and 2009. Given the range of annual publications, it is clear that fascination with an emphasis on IoT safety has increased exponentially in the last 3 years when compared to previous years [7].

We identified critical security issues associated with IoT networks that are highly dynamic and have highlighted network characteristics in this paper. We discovered that every IoT device should be secure and dependable in order to satisfy the privacy requirements, particularly when these devices are used together including applications such as defence, sciences of medicine, automobiles, and so on, where the primary concern is security. However, because of their Despite their small shape, such IoT devices have a lot of power limited computational ability, making [8] It is difficult to provide security as a result of risks associated with securing these devices against eavesdroppers, Computer viruses, Denial of Provider Phishing, Spoofing, and other threats others have emerged as critical topics to research in the sense of Internet of Things security. Because of Because of the limited authority of such IoT devices, it is difficult to create an effective architecture for sensor data storage and networking.

The division these things can be grouped together as "communities" used to ensure the security of the Internet of Things. Furthermore, when appropriate authorization is obtained, these communities can communicate with one another. As a result, data transmission is dangerous. As a result, Data traffic security among devices and cloud must also be a priority [9]. There are numerous available methods for enforcing data reliability. Encryption methods Additional Security Surface (SSL) and Transport Layer Security (TLS) are two examples (TLS). There are also Secure Mesh protocols, for example, have been used in Environmental noise Assisted Living (AAL), especially in e-Healthcare is a lightweight DDoS defense algorithm attacks, and Wireless protocols are layered (Internet, PHY/MAC, and Capacity for innovation). IPv6/IPv4, TCP/UDP, and 6LoWPAN are all part of the network/communication layer. The Wireless HART, UWB, IrDA, but also PLC 802.X series are all part of the PHY/MAC layer. CoAP, SNMP, DNS, and DLMS are examples of application layer protocols.

There are some numerous There are protection alternatives available for wireless networks, but 802.15.4 link-layer safety is the most common widely used. Unless data integrity is important, a concern, the 6LoWPAN system is operational the way to go because It is capable of supporting per-hop security arrangements via Cryptographic devices with symmetric keys [10] This system guarantees confidential operation, Authentication at the source, replay safety, data transformation, and semantic protection In addition, the network provides straight web entry via standards that are open In relation to network IP Security (IPSec) procedures are embedded for security the TCP/IP protocol stack is implemented using software in the operating system, Linux and NetBSD are two examples. Even so, the protocol is computationally demanding, which has a significant impact on network performance. Previously, web access or web transfer relied based upon that application layer CoAP method allowed with web transfer limited Networks and nodes. This procedure incorporates NoSec, PreShared-Key, Raw Public Key, as well as Identification card are examples of security modes have been shown to be useful in terms of transport layer security However, CoAP remains less secure putting data dependability at risk, particularly DDoS attacks are prevented. As a result, Security of the Datagram Network Layer (DTLS) protocol is used to ensure the required genuineness, confidentiality, and integrity Cookies in the web protocol domain provide protection. Typically, a collection of application layer protocols is put in place. ZigBee is a popular collection that is built around the IEEE 802.15.4 Mac. The protocol set is capable of be used to build effective and efficient network meshes with 216 devices are possible. These mesh networks have been shown to be have low energy consumption. They have a low data rate and are self-configuring [11].

Each and every of the protocols mentioned above send metadata, such as the source and destination identifies between nodes that are highly vulnerable to a variety of attacks, the most common of which are eavesdropping and packet injection. The Wireless HART protocol is useful for gaining maximum control so over process environment for measurement. Because of The procedure is robust and reliable due to the TDMA-based MAC sub layer incorporated within using TSMP technology and ratio of availability of more than 99.73 percent. There are some restrictions in the architecture of security that must be addressed. The Procedure for trying to carry Authentication for Internet Connectivity (PANA) is a different network protocol that allows authenticated network access can be used to address questions about webbing access authenticity on the architecture. It is an EAP that uses UDP protocol that operates between an EAP authenticator and an EAP peer [12].

A deep-packet anomaly detection reach with high performance and low weight can run on small Internet of Things devices is as well a viable option. The method employs n-gram bit-patterns for modeling payloads efficiently and flexibly, with the n-gram dimension varying by dimension. Elliptic Curve Cryptography (ECC) is beneficial for developing portable Public Key Cryptosystems to achieve lightweight integration (PKC). It is primarily due to the system's key size is small, short and operand length relatively minimal arithmetic requirements Authority over the protection of the data and communication transfer pathway is also exercised available for the Black Network via Black SDN is an IoT network architecture employs As the trusted third-party link, an SDN controller is used. Using encryption to protect the top corner and payload protect against a variety One surefire method is the use of attacks. The ICN, a fresh (inter-) connectivity paradigm, is often used to connect all networks of such network functions and protocols, as well as to the system's core, information identifiers ICN is most advantageous in terms of information [13] retrieval flexibility. Through flexible semantic-rich identifiers, ICN enables information "advertisement" and "retrieval." It differs because of location -based IP addresses have been examples of identifiers.

In this case study, we examined IoT security and analyzed security features and requirements at various layers. It is possible, based on findings that as the Internet of Things evolve increased security issues will emerge.

4. DISCUSSIONS

This paragraph discusses the findings as part of our comprehensive study of 712 IoT network security articles As analyzed, the goal of the majority of the object was to find a method of conveying data security in Iot systems. This research paper adheres to positivism as a paradigm, which studies observable and classifiable facts. The writings that were the qualitative research methodology were used in the review to find outcome that focused on achieving IoT network security. There are a few examples Instances where both qualitative methods are used noteworthy. Both approaches were used in these articles to develop algorithms, architecture, and procedures [14] that are efficient.

We also observe that the primary approach used in articles about network security in IoT is experimental research. The approach's main goal has been to identify various network security potential attacks. The use it is also possible to use real case analysis as a method strategy noteworthy, with specific configurations chosen to deal with problems such as IoT network security [15].

In terms of distribution of articles, and over half of those centered on IoT [16] network security have been published because 2010 The rise in the number of published object demonstrates how the domain is attracting researchers from all around the world Growing system complexities, diverse business scenarios [17], and an extremely competitive and vibrant global market to function [18], survive, and sustain could explain the increased interest. We discovered that the majority of the articles focused on providing IoT security. Traditional methods are giving way to more advanced techniques that improve the security of IoT devices [19]. This study also had the following limitations:

- Using different keywords for the search may result in different results. As a result, the keywords were used selected to give a concise overview of the current trends in IoT network [20-23] safety.
- It used as the same keyword in multiple places different libraries in various locations times may yield mismatch results (For example, because of a search engine or library updates).

As per the current record, we found the latest graph on available data mentioned in figure 4.1

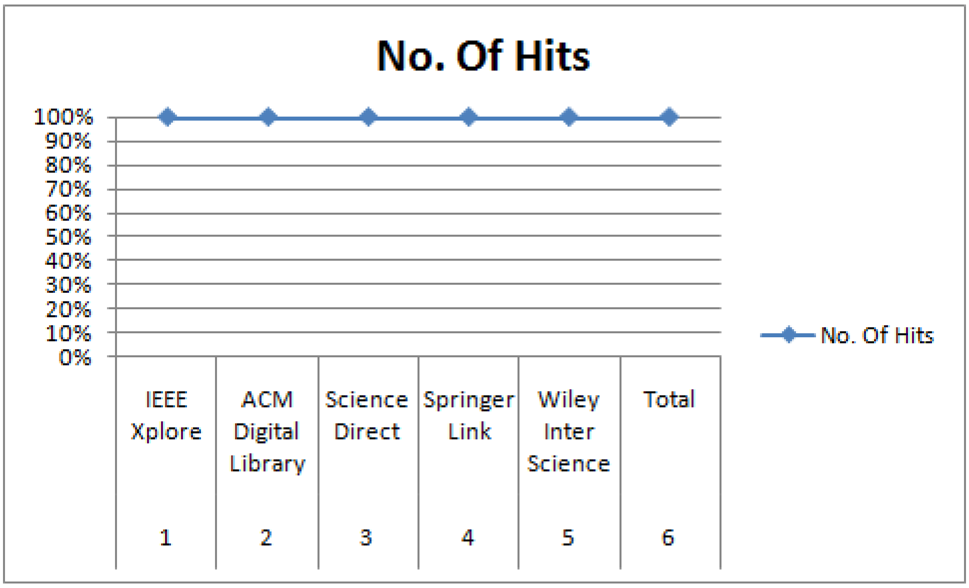

Figure 4.1. Number of Hits (As per Year)

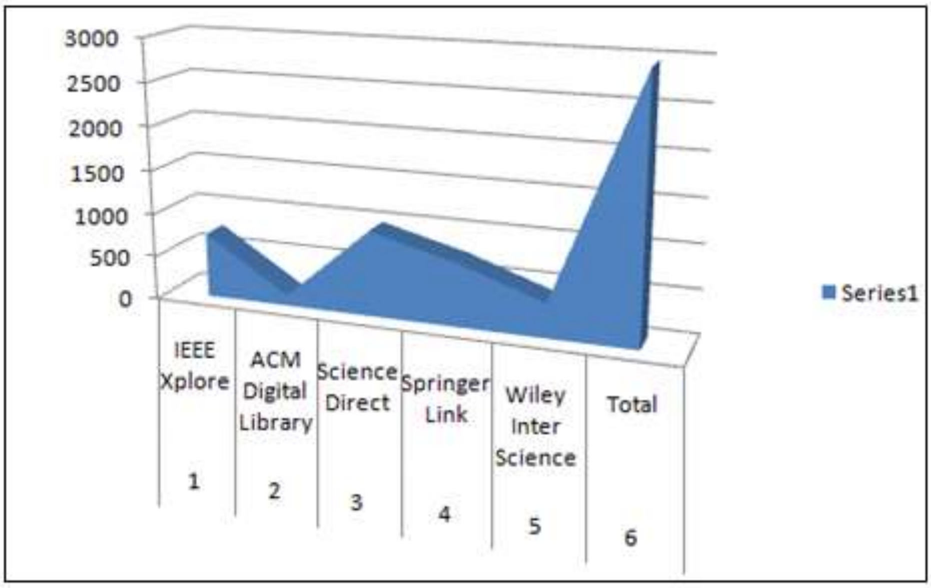

Figure 4.2. Increasing the Accessibility of Publication

5. CONCLUSIONS

Network safety is critical in Internet of Things. This strength in the position is particularly apparent urgent given how the potential consequences grew widely publicized following and the effect of attacks has become more radical. It could because of IoT encompass a diverse set of applications. Some one of the most significant IoT challenges are currently Safety, privacy, and confidentiality are all major concerns heterogeneity conduct, network capacity restriction and the massive data management and processing amounts of data in providing useful information. We investigated various to date, the preferences that have impacted data security in IoT in this paper. We based our findings on the findings of a thorough examination of chapter analyzed materials and articles that addressed our research concerns. Our discoveries suggest that the quantity of significant contribution to ensure IoT device security has increased in recent times and that is distinct levels of safety is being considered. The application of proper procedures in the Internet of Things allows for communication that is interoperable between limited Internet of Things devices and services.

There are some limitations to the study must be considered. The publications included with the review of the literature can still be relevant called into question. The method by which the databases and conference proceedings were chosen for our systematic review still needs to be refined. Because of the specific objectives and goals, a bias analysis as a result of article or text material selection it is still possible. There is also a chance that the results obtained by searching for 'IoT As well as NETWORK SECURITY' in specific channels will be insufficient. There could be articles that are not found in the search because the terms the terms "IoT" as well as "NETWORK SECURITY" really aren't signifiers or components of the retrieval. Further research may be conducted with an emphasis on the potential increase in external consideration network security concerns the reality that there's been a greater emphasis on different levels of safety could be the driving principle. Furthermore, A few of the outside factors to consider when considering IoT security is attention to business considerations, which is also an excellent context for further research. All of these alternatives should entice researchers to participate in this area of questioning and research.

6. REFERENCES

[1] Naz, Sumera, Muhammad Akram, Mohammed M. Ali Al-Shamiri, and Muhammad Ramzan Saeed. "Evaluation of network security service provider using 2-tuple linguistic complex-rung orthopair fuzzy COPRAS method." Complexity 2022 (2022).

[2] Yu, Jing, Xiaojun Ye, and Hongbo Li. "A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network." Future Generation Computer Systems 129 (2022): 399-406.

[3] Zhao, Mengwei, Hui Gao, Guiwu Wei, Cun Wei, and Yanfeng Guo. "Model for Network Security Service Provider Selection with probabilistic uncertain linguistic TODIM method based on prospect theory." Technological and Economic Development of Economy 28, no. 3 (2022): 638-654.

[4] Shin, Gun-Yoon, Sung-Sam Hong, Jung-Sik Lee, In-Sung Han, Hwa-Kyung Kim, and Haeng-Rok Oh. "Network Security Node-Edge Scoring System Using Attack Graph Based on Vulnerability Correlation." Applied Sciences 12, no. 14 (2022): 6852.

[5] Russell, James Stanley, Paul Scott, and Ahmad Attarha. "Stochastic shaping of aggregator energy and reserve bids to ensure network security." Electric Power Systems Research 212 (2022): 108418.

[6] Du, Meiyan. "Application of information communication network security management and control based on big data technology." International Journal of Communication Systems 35, no. 5 (2022): e4643.

[7] Afzal, Rafia, and Raja Kumar Murugesan. "Rule-based anomaly detection model with stateful correlation enhancing mobile network security." Intell. Autom. Soft Comput 31, no. 3 (2022): 1825-1841.

[8] Vinoth, S., Hari Leela Vemula, Bhadrappa Haralayya, Pradeep Mamgain, Mohammed Faez Hasan, and Mohd Naved. "Application of cloud computing in banking and e-commerce and related security threats." Materials Today: Proceedings 51 (2022): 2172-2175.

[9] Kryshtanovych, Myroslav, Ivan Dragan, Nataliia Chubinska, Natalia Arkhireiska, and Roman Storozhev. "Personnel Security System in the Context of Public Administration." IJCSNS International Journal of Computer Science and Network Security 22, no. 1 (2022): 248-254.

[10] Iyappan, Perumal, Jayakumar Loganathan, Manoj Kumar Verma, Ankur Dumka, Rajesh Singh, Anita Gehlot, Shaik Vaseem Akram, Sukhdeep Kaur, and Kapil Joshi. "A generic and smart automation system for home using internet of things." Bulletin of Electrical Engineering and Informatics 11, no. 5 (2022): 2727-2736.

[11] Diwakar, Manoj, Kanika Sharma, Ravi Dhaundiyal, Sheetal Bawane, Kapil Joshi, and Prabhishek Singh. "A review on autonomous remote security and mobile surveillance using internet of things." In Journal of Physics: Conference Series, vol. 1854, no. 1, p. 012034. IOP Publishing, 2021.

[12] Lakshmi, P. Sree, Monika Saxena, Sakshi Koli, Kapil Joshi, Khairul Hafezad Abdullah, and Durgaprasad Gangodkar. "Traffic Response System Based on Data Mining and Internet of Things (Iot) For Preventing Accidents." In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 1092-1096. IEEE, 2022.

[13] Heidari, Arash, Nima Jafari Navimipour, and Mehmet Unal. "Applications of ML/DL in the management of smart cities and societies based on new trends in information technologies: A systematic literature review." Sustainable Cities and Society (2022): 104089.

[14] Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." Computer networks 148 (2019): 283-294.

[15] Lee, Jee Young, and Jungwoo Lee. "Current research trends in IoT security: a systematic mapping study." Mobile Information Systems 2021 (2021).

[16] Ruan, Junhu, Hua Jiang, Chunsheng Zhu, Xiangpei Hu, Yan Shi, Tianjun Liu, Weizhen Rao, and Felix Tung Sun Chan. "Agriculture IoT: Emerging trends, cooperation networks, and outlook." IEEE Wireless Communications 26, no. 6 (2019): 56-63.

[17] Sezer, Sakir. "T1C: IoT Security:-Threats, security challenges and IoT security research and technology trends." In 2018 31st IEEE International System-on-Chip Conference (SOCC), pp. 1-2. IEEE, 2018.

[18] Saheb, Tahereh, and Leila Izadi. "Paradigm of IoT big data analytics in the healthcare industry: A review of scientific literature and mapping of research trends." Telematics and informatics 41 (2019): 70-85.

[19] Kotha, Harika Devi, and V. Mnssvkr Gupta. "IoT application: a survey." Int. J. Eng. Technol 7, no. 2.7 (2018): 891-896.

[20] Kumar, Adarsh, Carlo Ottaviani, Sukhpal Singh Gill, and Rajkumar Buyya. "Securing the future internet of things with post-quantum cryptography." Security and Privacy 5, no. 2 (2022): e200.

[21] Kumar, Adarsh, and Deepak Kumar Sharma. "An optimized multilayer outlier detection for internet of things (IoT) network as industry 4.0 automation and data exchange." In International Conference on Innovative Computing and Communications, pp. 571-584. Springer, Singapore, 2021.

[22] Kumar, Adarsh, and Saurabh Jain. "Drone-based monitoring and redirecting system." In Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead, pp. 163-183. Springer, Cham, 2021.

[23] Kumar, A. "Augusto de Jesus Pacheco D." Kaushik K., Rodrigues JJPC Futuristic View of the Internet of Quantum Drones: Review, Challenges and Research Agenda. Veh. Commun 36 (2022): 100487.