Review Article

ACCENTS Transactions on Information Security, Vol 7(26)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2022.725001

A survey on IoT security: application areas, security threats, and solution architectures

Animesh Kumar Dubey*
Assistant Professor, Madhyanchal professional University Bhopal, India

Received: 23-February-2022; Revised: 18-April-2022; Accepted: 20-April-2022

Abstract
IoT technology play a significant role in securely managing the interaction between devices. Objects may be empowered to receive, create, transfer and exchange information in a hassle-free manner by using Internet of Things (IoT). The upcoming and existing applications of IoT are really promising to enhance the level of efficiency, automation, and comfort for users. This research work sheds light on discussing why security is important in IoT devices in recent times. Additionally, a detailed explanation of the challenges related to security and the origin of threats in the IoT application is discussed in this research. After analysing the security issues, various existing and emerging technologies concentrated on achieving a high level of trust in the application of IoT are presented in this study. There are four different technologies such as fog computing, blockchain, edge computing and machine learning to increase the security level in IoT that are also discussed in this research paper.

Keywords
IoT technology, Security, Emerging technologies, Machine learning.

1.Introduction
The speed of connecting physical machines to the internet is significantly increasing day by day. As per the recent report by Gartner, around 8.4 billion connected objects are available in the world [1]. It is predicted that the number of things is expected to increase to 20.4 billion by the end of 2022. The utilisation of IoT applications is increasing day by day to make people's life easier. According to Altulaihan et al. [2] in IoT, networks, humans and objects communicate using unconscious and conscious actions. Internet of things (IoT) mainly differs from the internet, which depends on human input to execute. As opined by Tabaa et al., (2020) [3], in different areas such as social media, supply chain management, energy consumption and medicine, the IoT has created many opportunities for economic and social interaction. IoT devices are unique in terms of security vulnerabilities, due to the heterogeneity and complexity of technology. However, addressing the security of IoT devices is more critical. Machine learning methods such as cost-sensitive classification techniques are used in every research to measure the performance of the systems.

*Author for correspondence

This cost per example (CPE) value helps users to analyse the network pattern and take immediate actions to reduce the chances of cyberattacks if any fraudulent activity is found.

$$CPE = 1/ N \Sigma (i=1, 5) \Sigma (j=1, 5) CM (i, j) + C (i, j)$$

This equation enables people to determine the CPE values aims to find the total cost of misclassification of an Intrusion detection system (IDS). CM is denoted as the confusion matrix of the classification model whereas C corresponds to Cost Matrix. Moreover, i and j is used to denote limit of iteration.

IoT has some specific security challenges such as authentication issues, privacy issues, management issues and information storage [1]. In order to mitigate this kind of problem, IoT applications have already developed a fertile ground for various kinds of cyber threats. As depicted by Ferrag et al., (2022) [4], different cyberattacks such as Phishing, SQL Injection, DDoS, Malware and so on have already been deployed in the application of IoT. As stated by Hassija et al., (2019) [1], in the last quadrant of 2016, the Mirai attack signifies infected more than 2.5 million systems connected to the internet through Distributed Denial of Service attacks.

As per the view of Reddy et al., (2022) [5], organisations and people are continuously

experiencing a larger range of security problems due to the ever-increasing and widespread cyberattacks on IoT devices. IoT poses security challenges due to the transient and dynamic nature of linked devices [6]. As a result, an effective cybersecurity technique is required to be developed for analysing the IoT security threat at the early stage and reducing the chances of cyberattacks on IoT applications. The previous work did not provide any knowledge about the effective IoT security solution which can reduce the number of cyberattacks in recent times.

The security problems which directly impact the IoT paradigm have attracted attention from the community of research [7]. In this instance, several ways including Intrusion detection system (IDS), emerging technologies and threat modelling needs to place a strong emphasis to maintain the security of IoT devices more efficiently than before. According to Tawalbeh et al., (2020) [8], as people and organisations are facing continuous security challenges such as privacy issues, authentication issues and so on, it is required to develop a fruitful IoT security solution. As per the report of 2022, the share of attacks of IoT had increased significantly in the first quadrant of 2020 [9]. Moreover, it is found that global IoT attacks have fallen by 19% in the last quadrant of 2021 than the previous quadrant [9]. In this case, they suggested to work based on IoT security, aiming to protect IoT devices from cyberattacks. *Figure 1* shows the Global share of IoT cyberattacks.

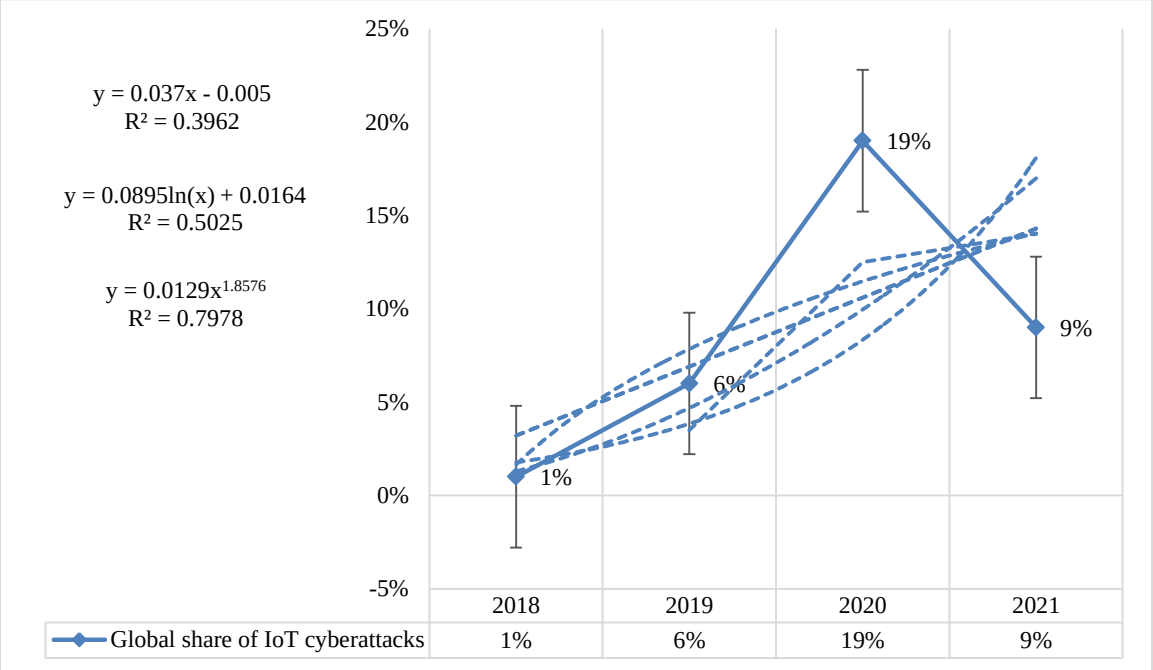


Figure 1 Global share of IoT cyberattacks

The primary objective of this research work is to analyse the importance of securing IoT devices. Additionally, this research work will discuss the ways of securing IoT-generated data in an efficient manner. Moreover, the researcher will emphasise inspecting the security threats of IoT devices and existing solution strategies.

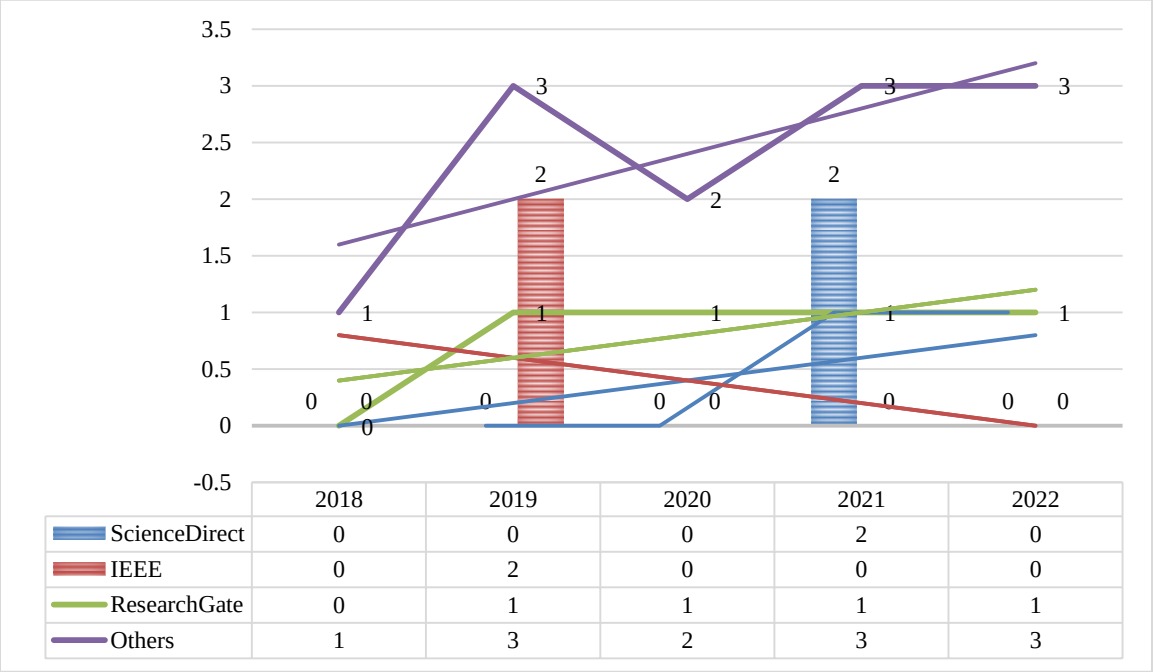
This research paper aims to provide a comprehensive review and analysis of the complex aspects related to IoT security. The paper covers all the significant factors that have contributed to the development of IoT security. The research paper has several contributions, including the classification of IoT applications and the specific privacy and security issues related to IoT devices. Additionally, the paper provides a detailed overview of the sources of different threats in different layers of the Internet of Things.

Furthermore, the paper presents realistic and detailed recommendations to improve the infrastructure of IoT to foster secure interactions. These recommendations aim to address the security challenges that exist in IoT and help to mitigate the threats to IoT devices. The research paper concludes

with a complete assessment of the challenges, issues, and future directions for creating secure IoT software. This assessment provides a comprehensive understanding of the current state of IoT security and the measures that can be taken to improve it in the future.

2.Literature review

This section is focused on explaining the security challenges that are being faced by people while using IoT technology in developing smart applications. A total of 20 relevant articles and journals have been inspected in this work to evaluate the impacts of IoT security on organisational performance and human society. ResearchGate, IEEE, ScienceDirect, MDPI, Springer and so many other publications have been considered by the researcher to gain in-depth knowledge about the technologies used to maintain security in IoT applications, which include Edge Computing, Fog Computing, Blockchain and ML methods. At the initial stage, the researcher has chosen 40 authentic articles and journals to review the concept of IoT security and its importance in keeping private records confidential and improving the performance of ongoing operations. After eliminating the incredible sources and non-English papers, the researcher selected 20 research papers finally to accomplish the research goal. The proper distribution of research papers considered from 2018 to 2022 is shown in the *Figure 2*.



	2018	2019	2020	2021	2022
ScienceDirect	0	0	0	2	0
IEEE	0	2	0	0	0
ResearchGate	0	1	1	1	1
Others	1	3	2	3	3

Figure 2 Total distribution of selected research papers

The perception of IoT notion is visualised to improve the quality of life and manage daily based work easily [9]. According to Sahu et al., (2021) [10], the IoT solution significantly enhances the regular routines of disabled and elderly people, by increasing their self-confidence and autonomy. As stated by [9], wearable and implantable IoT devices extract and monitor visual measurements to authorise or enable the emergency alerting option to increase the survival chances of patients. Al-Khafajiy et al., (2019) [11] claimed that IoT technology helps the healthcare sector in reducing response time in the context of any health incidence such as sudden death symptoms during sleep. It demonstrates the usefulness of people-centric IoT solutions. On the other hand, there is a safety-centric IoT resolution that enables people to overcome hazardous scenarios and situations. For example, the idea of connected vehicles helps to reduce the chances of accidents by preventing drivers from diverging the accurate path [12]. As per the opinion of Alkinani et al.,(2021) [13], IoT technology helps people to get notifications regarding nearby medical and road assistance in case of any accidents happened.

IoT is mainly considered as the distributed and interconnected network of embedded devices connected and interacting through wireless and wired

communication technologies [14]. Hassija et al., (2019) [1] stated that in the network of IoT, different systems with different characteristics and capabilities are able to interact with each other through communication protocols. It is evident that, in larger organisations, different devices remain connected with each other through Ethernet in order to manage their ongoing tasks. As suggested by Hughes-Lartey et al., (2021) [15], it is required to maintain security in IoT devices to protect both organisation and customer records from data theft, corruption and hacking. As opined by Li et al., (2018) [16], the deployment of the Internet of Things on a large scale brings major security challenges. These security challenges include the development and design of storage and networking architecture for devices, data communication protocols, Protection of the Internet of Things from application interfaces and malicious attacks and Proactive identification [14].

The enormous connectivity of IoT systems needs a low-cost solution and ultra-low power that helps in efficient network functioning [17]. As stated by Hassija et al., (2019) [1], in order to successfully realisation and development of IoT, it is vital to analyse the cause of privacy and security issues. However, the solution to the privacy and security issues of IoT in the Internet of Things requires optimised algorithms and cross-layer designs. In any IoT system, there are 4 important layers. As per the view of Yazdinejad et al., (2022) [18], the first layer (Perceptron layer) incorporates the use of different actuators and sensors to discern information or data to perform different functionalities. Chanal and Kakkasageri (2020) [19] claimed that the second layer is known as the network layer which is utilised to transmit the gathered information. It is noticed that most IoT applications are deployed in the third layer, named the middleware layer [1]. Kotsiopoulos et al., (2021) [20] stated that the fourth layer is called the Application layer where various types of end-to-end applications are there like smart transports, smart factories and smart grids.

Three layers including the Application layer, Network layer and Physical layer, have a major chance of threats. As illustrated by Altulaihan et al. [2], the most common threats in the Application layer are Eavesdropping, Node Capture, Boot attacks, timing attacks and side-channel attacks. In contrast to [1], routing attacks, Sybill attacks, DDoS attacks and man-in-the-middle attacks are examples of threats that are seen in the network layer. Gunduz and Das (2020) [21] focused on identifying the common threats in the application layer including malicious code injection, Data Theft, a Snipping attack, DDoS and so on.

The common emerging technologies that are used in maintaining the security of IoT devices are blockchain, edge computing, fog computing and machine learning [1]. According to Kumar and Sharma (2021) [22], among these four technologies, the most popular technology is Blockchain technology in terms of maintaining security in IoT devices. 47% of people prefer using blockchain technology to reduce the risk of DDoS attacks affecting their devices. Additionally, machine learning is utilized to maintain IoT device security in 20% of cases [2]. It is noticed that fog computing is in the same demand as machine learning in the field of IoT security [23]. *Figure 3* shows the most used technologies for IoT threats.

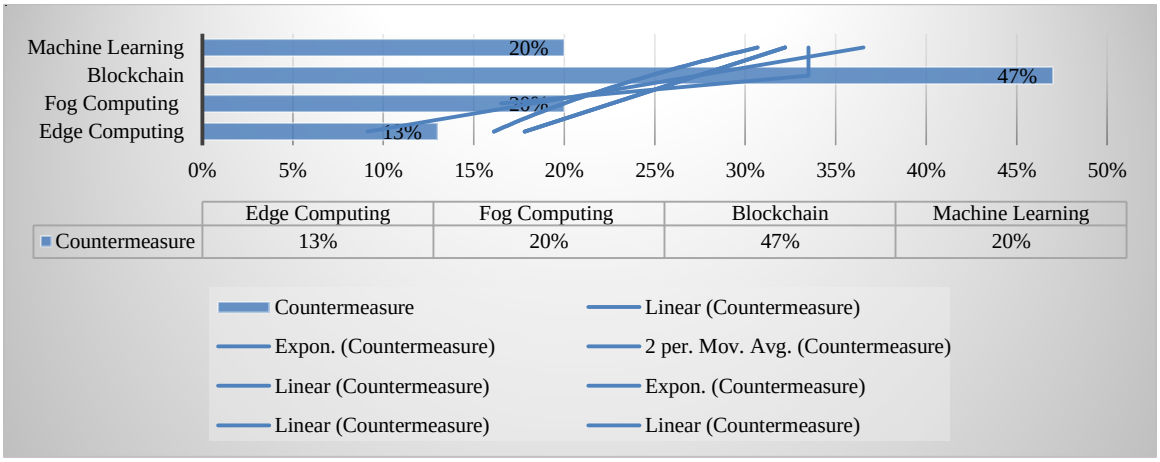


Figure 3 Most used technologies for IoT threats

As the number of security attacks in IoT applications is continuously increasing, it is required to take immediate action to reduce the chances of IoT security attacks [1]. One of the primary concerns related to IoT security is the identification of an effective threat detection method, that will have a low probability of showing false alarms and a high probability of giving accurate detection if there is a chance of any security risks. As suggested by Deep et al., (2022) [24], application layered protocols should be improved because there are still several security issues and challenges that require to be addressed. In contrast to Arisdakessian et al., (2022) [25], future research is also needed in terms of detecting the chances of different cyberattacks in each layer of IoT architectures. Blockchain technology needs to be leveraged in recent times due to its distributed nature [26]. Hassija et al.,(2019) [1]argued that distributed characteristics of blockchain technology allow people to store data in a secure way.

One of the main gaps in this research work is the stipulated time to identify different IoT security threats and their impacts on human society and organisational performance. In this instance, the researcher has not been able to inspect sufficient journals and articles based on IoT security issues and threats. The limited sample size and the restricted word count also indicate major gaps in this research work. *Table 1* shows the review analysis.

Table 1 Review analysis considering method, results, and gaps

S. No.	Source	Method	Results	Gap
1	Rani et al., (2021) [27]	A virtual method is used in this article and "forensic handling methodologies"	End to end communication is a vital thing in this era of the wireless communication. Man in the middle attack issue is a major issue which needs to be mitigated with the better architecture.	Complex implementation in the testing is a gap which is identified in this article. Physical limitation is a limitation as well.
2	Roy *et al.*, (2018) [28]	Distributed trust method	Blockchain technology is a major technology. Industrial automation is the future direction. Proof-of-Work (Pow) is a solution and technique which helps to maximise the trustworthiness of data such as computational data.	The "typical scaling issues" are some issues. It is evident that 51% of the attack seems to be a serious threat.
3	Mohanta et al., (2020) [29]	Machine learning is used in this article Artificial intelligence.	The decentralized/distributed network is a highly used in some aspects. As per the report of Cisco, it can be said that at this time, there is a usage of devices which are beyond 50 million. Radiofrequency identification (RFID) is used as well. Fog and edge computing is discussed in this paper as well.	Large volumes of data cannot be managed sometimes.
4	Mohanta et al., (2019) [30]	Truffle framework is used in this paper. The "Ethereum Blockchain connected to an ethereum wallet account" is in this account. This research paper has followed the experimental setup in an effective way.	It has been analysed that the authentication scheme is a major scheme which needs to be undertaken. Iot is a cost-effective method in recent times, which has manifested the living standard in an effective way. Two-factor authentication is a major plan in recent times.	It has been analysed that the storage capacity of a fog device is also limited", it needs to be maximised for the better purpose of the cloud system.
5	Aman *et al*., (2020) [31]	Machine-to-Machine (M2M), ICN based on Iot and others	It has been analysed that the IOT trend intends to manifest in future communication. This IOT is comprised of different things which are "protocols, technologies, application, frameworks, security, communication, architecture, challenges, etc." In architecture, there are three different layers which are top, bottom and middle.	Lack of storage and data scheme is a threat which is identified in this paper.
6	Khanam *et al*., (2020) [32]	Machine learning Cloud platform Middleware and others	This paper is aimed to discuss the classification of the internet of things	It is evident that there are different gaps like "• Firewall IoT devices to filter packets", its error and others.

S. No.	Source	Method	Results	Gap
7	Fahim and Sillitti (2019) [33]	Automation detection Machine learning method Decision tree model The anomaly detection method Time series pattern data	The aim of this paper is to discuss that intrusion is a major threat which needs to be mitigated.	Huge statistical data cannot be managed, in this paper, it is reported.
8	Mishra and Kertesz (2020) [34]	Iot reference model Computer interaction Machine learning	The IOT reference model in the health care tends to manifest the connection of the people. Digital infrastructure in the healthcare sector has become five times better. There is an additional reference model of MQTT.	It can be said that MQTT based broker does not have the capability and ability of encryption.

3.Discussion and analysis

Based on the literature discussed it is found that there is a close relationship between the IoT environment and the smart home and smart city environments in today's internet era. Cloud computing has emerged as a powerful solution for storing data in a virtual way, making it a popular choice for users with the increasing use of devices worldwide. It is estimated that around 50 million people use a device regularly. These users can be classified into two categories: intra-device and inter-device.

Intra-device users refer to those who use only one device at a time, such as a smartphone or laptop. On the other hand, inter-device users refer to those who use multiple devices at once, such as a smartwatch, tablet, and laptop. With the rise of IoT devices, it has become more common for users to be both intra-device and inter-device users, which has created a greater need for secure and efficient data storage solutions.

Cloud computing has emerged as a viable solution to meet these needs. It allows for virtual storage of data, enabling users to access their data from multiple devices. Additionally, cloud computing provides a robust storage system that can handle vast amounts of data, making it an ideal choice for those who use multiple devices simultaneously. The increasing number of device users and the growing need for secure and efficient data storage solutions have made cloud computing an essential technology in today's world. With its ability to store data virtually and handle large amounts of data, it has become a popular choice for users across the globe.

Blockchain technology is a major player in the technology world today. One important application of this technology is software-defined networking (SDN)-based IoT security solutions, which aim to unify the IoT in an effective way. The IoT paradigm has encompassed a wide range of areas such as smart cities, homes, cars, manufacturing, e-healthcare, transportation, wearables, farming, and much more. Two types of data sets, centralized and decentralized, are utilized in the IoT environment. It has been analyzed that a sensitive framework is required to mitigate the risks and hazards associated with IoT. This study has incorporated facts such as anomaly detection, analysis, and prediction techniques in the IoT environment. Threats and corrective measures for IoT security with observance of cybercrime are increasing day by day and need to be addressed.

In summary, the incorporation of blockchain technology and the SDN-based IoT security solutions aim to mitigate the risks associated with IoT security. As the IoT paradigm expands into various sectors, a sensitive framework is needed to manage the growing number of threats and to ensure safe and secure interactions between devices (*Figure 4*).

4.Conclusion

IoT is a technology that comes with its unique security challenges, and it is essential to address them for the secure functioning of IoT applications. The security concerns related to IoT include identity, privacy, management, and information storage. These concerns make IoT applications vulnerable to cyber threats, such as phishing, SQL injection, DDoS, malware, and more. For example, the Mirai attack in 2016 exploited DDoS attacks and infected more than 2.5 million internet-connected systems. The continuous occurrence of cyberattacks has put organizations and individuals in a vulnerable position. To address these security concerns, this research aims to critically analyze and discuss each layer's threats in IoT-enabled devices and develop an effective strategy to mitigate new IoT security threats in applications. By reviewing this research study, future researchers will gain in-depth knowledge about IoT security, enabling them to start their work on securing IoT devices effectively. This study aims to contribute towards developing a sensitive

framework to mitigate risk and hazards in IoT-enabled devices. Future work will focus on exploring anomaly detection, analysis, and prediction techniques in IoT environments.

In conclusion, it is evident that the threats and corrective measures for IoT security with observance of cybercrime are increasing day by day and need to be mitigated.

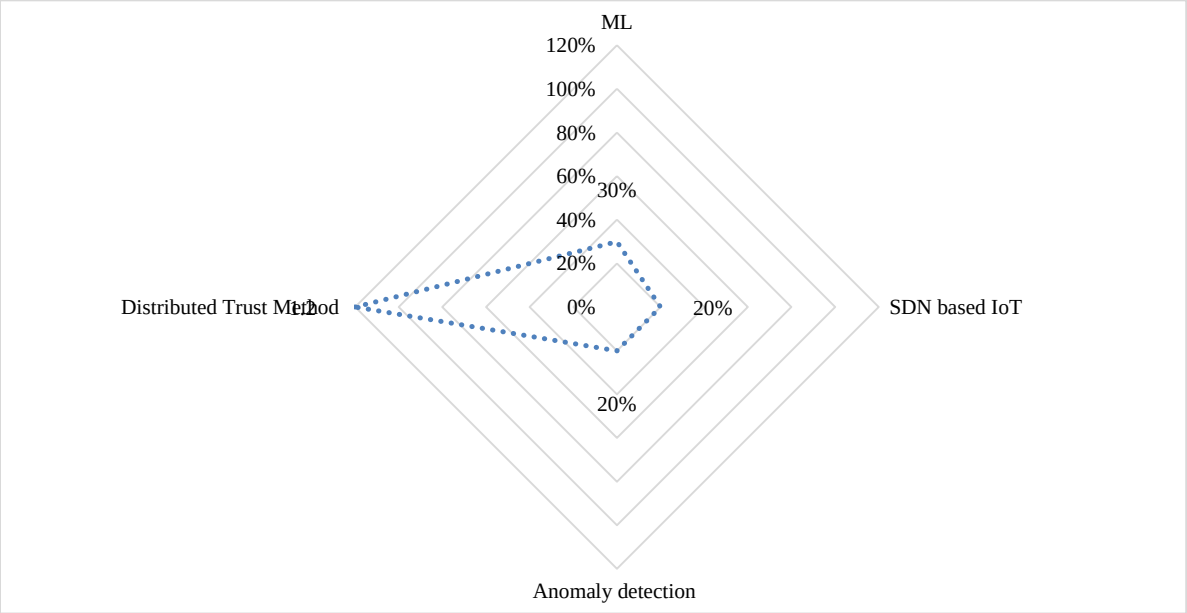


Figure 4 Methodology used in IoT security threat detection

Acknowledgment
None.

Conflicts of interest
The authors have no conflicts of interest to declare.

References
[1] Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access. 2019; 7:82721-43.
[2] Altulaihan E, Almaiah MA, Aljughaiman A. Cybersecurity threats, countermeasures and mitigation techniques on the iot: future research directions. Electronics. 2022; 11(20):1-41.
[3] Tabaa M, Monteiro F, Bensag H, Dandache A. Green industrial internet of things from a smart industry perspectives. Energy Reports. 2020; 6:430-46.
[4] Ferrag MA, Friha O, Hamouda D, Maglaras L, Janicke H. Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access. 2022; 10:40281-306.
[5] Reddy YH, Ali A, Kumar PV, Srinivas MH, Netra K, Achari VJ, et al. A comprehensive survey of internet of things applications, threats, and security issues. South Asian Research Journal of Engineering and Technology. 2022; 4(4):63-77.
[6] Tariq N, Asim M, Al-Obeidat F, Zubair Farooqi M, Baker T, Hammoudeh M, et al. The security of big data in fog-enabled IoT applications including blockchain: a survey. Sensors. 2019; 19(8):1-33.
[7] Neshenko N, Bou-Harb E, Crichigno J, Kaddoum G, Ghani N. Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials. 2019; 21(3):2702-33.
[8] Tawalbeh LA, Muheidat F, Tawalbeh M, Quwaider M. IoT Privacy and security: challenges and solutions. Applied Sciences. 2020; 10(12):1-17.
[9] https://www.statista.com/statistics/1321250/worldwide-internet-of-things-attacks/. Accessed: 12 March 2022.
[10] Sahu D, Pradhan B, Khasnobish A, Verma S, Kim D, Pal K. The internet of things in geriatric healthcare. Journal of Healthcare Engineering. 2021; 2021:1-16.
[11] Al-Khafajiy M, Baker T, Chalmers C, Asim M, Kolivand H, Fahim M, Waraich A. Remote health monitoring of elderly through wearable sensors. Multimedia Tools and Applications. 2019; 78(17):24681-706.
[12] Hamid UZ, Zamzuri H, Limbu DK. Internet of vehicle (IoV) applications in expediting the implementation of smart highway of autonomous vehicle: a survey. Performability in Internet of Things. 2019:137-57.
[13] Alkinani MH, Almazroi AA, Jhanjhi NZ, Khan NA. 5G and IoT based reporting and accident detection (RAD) system to deliver first aid box using unmanned aerial vehicle. Sensors. 2021; 21(20):1-16.

[14] Hussain F, Hussain R, Hassan SA, Hossain E. Machine learning in IoT security: current solutions and future challenges. IEEE Communications Surveys & Tutorials. 2020; 22(3):1686-721.
[15] Hughes-Lartey K, Li M, Botchey FE, Qin Z. Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon. 2021; 7(3):e06522.
[16] Li R, Song T, Mei B, Li H, Cheng X, Sun L. Blockchain for large-scale internet of things data storage and protection. IEEE Transactions on Services Computing. 2018; 12(5):762-71.
[17] Chowdhury MZ, Shahjalal M, Hasan MK, Jang YM. The role of optical wireless communication technologies in 5G/6G and IoT solutions: prospects, directions, and challenges. Applied Sciences. 2019; 9(20):1-20.
[18] Yazdinejad A, Kazemi M, Parizi RM, Dehghantanha A, Karimipour H. An ensemble deep learning model for cyber threat hunting in industrial internet of things. Digital Communications and Networks. 2023; 9(1):101-10.
[19] Chanal PM, Kakkasageri MS. Security and privacy in IOT: a survey. Wireless Personal Communications. 2020; 115:1667-93.
[20] Kotsiopoulos T, Sarigiannidis P, Ioannidis D, Tzovaras D. Machine learning and deep learning in smart manufacturing: the smart grid paradigm. Computer Science Review. 2021.
[21] Gunduz MZ, Das R. Cyber-security on smart grid: threats and potential solutions. Computer networks. 2020; 169:107094.
[22] Kumar R, Sharma R. Leveraging blockchain for ensuring trust in IoT: a survey. Journal of King Saud University-Computer and Information Sciences. 2022; 34(10):8599-622.
[23] Pop P, Zarrin B, Barzegaran M, Schulte S, Punnekkat S, Ruh J, Steiner W. The FORA fog computing platform for industrial IoT. Information Systems. 2021; 98:101727.
[24] Deep S, Zheng X, Jolfaei A, Yu D, Ostovari P, Kashif Bashir A. A survey of security and privacy issues in the Internet of Things from the layered context. Transactions on Emerging Telecommunications Technologies. 2022; 33(6).
[25] Arisdakessian S, Wahab OA, Mourad A, Otrok H, Guizani M. A survey on iot intrusion detection: Federated learning, game theory, social psychology and explainable ai as future directions. IEEE Internet of Things Journal. 2022.
[26] Aristidou C, Marcou E. Blockchain standards and government applications. Journal of ICT Standardization. 2019: 287-312.
[27] Rani S, Kataria A, Sharma V, Ghosh S, Karar V, Lee K, Choi C. Threats and corrective measures for IoT security with observance of cybercrime: a survey. Wireless Communications and Mobile Computing. 2021; 2021:1-30.
[28] Roy S, Ashaduzzaman M, Hassan M, Chowdhury AR. Blockchain for IoT security and management: Current prospects, challenges and future directions. In 5th international conference on networking, systems and security (NSysS) 2018 (pp. 1-9). IEEE.
[29] Mohanta BK, Jena D, Satapathy U, Patnaik S. Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things. 2020.
[30] Mohanta BK, Sahoo A, Patel S, Panda SS, Jena D, Gountia D. Decauth: decentralized authentication scheme for iot device using ethereum blockchain. In TENCON 2019-2019 IEEE region 10 conference (TENCON) 2019 (pp. 558-63). IEEE.
[31] Aman AH, Yadegaridehkordi E, Attarbashi ZS, Hassan R, Park YJ. A survey on trend and classification of internet of things reviews. IEEE Access. 2020; 8:111763-82.
[32] Khanam S, Ahmedy IB, Idris MY, Jaward MH, Sabri AQ. A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. IEEE Access. 2020; 8:219709-43.
[33] Fahim M, Sillitti A. Anomaly detection, analysis and prediction techniques in iot environment: a systematic literature review. IEEE Access. 2019; 7:81664-81.
[34] Mishra B, Kertesz A. The use of MQTT in M2M and IoT systems: a survey. IEEE Access. 2020; 8:201071-86.

Animesh Kumar Dubey is working as Assistant professor with the department of Computer Science and Engineering, at Madhyanchal Professional University, Bhopal, India. He has completed his Bachelor of Engineering (B.E.) and MTech. degree with Computer Science Engineering from Rajeev Gandhi Technical University, Bhopal (M.P.). He has more than 15 publications in reputed, peer-reviewed national and international journals and conferences. His research areas are Data Mining, Optimization, Machine Learning, Cloud Computing and Artificial Intelligence.
Email:animeshdubey123@gmail.com