JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 08 Issue 01
2024

Research Article
https://doi.org/10.56979/801/2024

Security Challenges and Attacks in IoT: A Survey

Qurra tul Aain[1], Irshad Ahmed Sumra[2], and Mariam Khan[1]

[1]Department of Information Technology, Lahore Garrison University, Lahore, 54000, Pakistan.
[2]Department of Computer Science, Lahore Garrison University, Lahore, 54000, Pakistan.
*Corresponding Author Qurra tul Aain. Email: aain.sabbir.leo@gmail.com

Received: November 11, 2024 **Accepted:** December 01, 2024

Abstract: A network of interconnected devices with the ability to gather, analyze, and exchange data is known as the Internet of Things, or IoT. This technology has various benefits, including simplicity of use, efficiency, and automation. Additionally, there's a serious security concern. One of the challenges is the variety of IoT devices with various hardware, software, and communication protocols. Among the many advantages of this technology are its ease of use, automation, and efficiency. It does, however, also come with a number of very real security risks. The vast array of IoT devices with different operating systems, hardware, and communication protocols, as well as the intricate and large-scale IoT networks with several domains, levels and stakeholders, are some of these issues. Moreover, it commonly occurs that some features are absent from IoT devices. The younger generation is growing more and more interested in blockchain technology since it is specifically tailored to the information age. In this survey paper, it will discuss in detail the security challenges and possible solution to secure the Internet of Things (IoT). The Secure IoT give benefits to end users through its applications in different fields. Significant advancements in distributed systems have resulted from the development of IoT technology across several sectors.

Keywords: Internet of Things; IoT Devices; Security; Communication Protocols; Security Challenges.

1. Introduction

Security is one of the core topics in internet of things (IOT) network. The IoT refers to a network of physical objects, sensors, actuators, and software programs that connect and share data over the internet. IoT devices have brought convenience, efficiency, and automation, but also pose significant security concerns, such as the heterogeneity and diversity of IoT devices with different hardware, software, and communication protocols. The paper offers an organized brief summary of the IoT security challenges and its goals, along with a catalogue of security attacks for IoT architecture and corrective measures [1]. To address these challenges, IoT security must incorporate implementation of security by design and security by default principles for IoT development and deployment by adopting risk-based and adaptive security mechanisms for IoT management, operation, and enhancing security awareness and education among IoT users and stakeholders IoT security, addressing attacks, challenges and countermeasures and analyzing security threats in IoT layered architecture. It highlights the importance of IoT security, especially as the number of devices in IoT is rapidly growing and integrating with all aspects of society. The paper outlines various security threats and countermeasures, and discusses the challenges and research directions to overcome these security issues. The authors also point out the limitations and future directions for IoT security. Internet of Things (IoT) and defines its main concepts, highlighting the challenges the technology faces in ensuring function and operability. The authors focus on security-related challenges and present a number of actions and future work to enhance IoT security (privacy, lightweight crypto). In In this research

work, the authors propose a reference model to analyze and summarize IoT security issues and provide a detailed analysis of the applications and services security issues that IoT faces. He challenges and vulnerabilities related to cyber security in smart homes based on Internet of Things (IoT) technology. It provides an overview of IoT and smart homes, and examines the common cybersecurity issues that threaten smart home security. The paper also provides some suggestions and recommendations on the effective security mechanisms that can be used to mitigate cyberattacks on the IoT-based smart homes. The security problems and threats related to Internet of Things (IoT) devices. IoT refers to a network where physical objects, like sensors and actuators, and software programs connect and share data over the internet. These devices make our lives more convenient, efficient, and automated, but they also come with significant security risks. This is because IoT devices have different types of hardware, software, and ways of communicating, which makes it hard to secure them all properly [2].

The paper gives a detailed review of these security challenges and goals. It also lists various types of security attacks that can happen in IoT systems and offers possible solutions. To tackle these problems, the paper suggests that IoT security should follow certain principles:

Security by Design: This means building security features into devices from the very beginning, during the design phase.

Security by Default: This means ensuring that devices are secure right out of the box, without requiring the user to make many adjustments [3].

Block chain technology is a system for securely storing and sharing information without needing a central authority. It is widely used in areas like the Internet of Things (IoT) because it makes data sharing more transparent, reliable, and secure. Block chain helps protect privacy by keeping user information, data, and locations private while allowing secure data sharing. It is useful in smart cities, healthcare, and other advanced systems by using strong digital security methods. However, challenges like security risks and making different systems work together still need to be solved, and researchers are working to improve it for many uses.[4]

The Internet of Things (IoT) is a technology that lets devices work together and share information automatically, without needing people to control them. It uses things like sensors and software to connect and communicate. IoT has become even better with new technologies like machine learning. It's used in many areas, such as smart homes, smart cities, and schools. For example, in education, IoT helps create modern classrooms and supports students with disabilities using special devices like smart gloves. In daily life, IoT makes things like home security, waste management, air quality, and entertainment better and easier, helping us live smarter and more comfortably.[5]

The paper also suggests adopting risk-based and flexible security strategies for managing and operating IoT devices: This means considering the specific risks associated with different devices and adjusting security measures accordingly. Additionally, it emphasizes the need for increasing security awareness and education among the users and stakeholders involved with IoT. [6]

The paper stresses the importance of IoT security because the number of IoT devices is rapidly increasing, and they are becoming more integrated into all parts of society. It outlines various security threats, like unauthorized access or data breaches, and countermeasures, such as encryption and regular software updates. It also discusses the ongoing challenges and areas where more research is needed to improve IoT security.

The authors of the Research paper highlight the need for protecting privacy, using lightweight cryptography (which means using encryption methods that don't require a lot of computing power), and other security improvements. They propose a model to thoroughly analyze IoT security issues and examine security concerns in different IoT applications and services [7]

Additionally, this research specifically looks at cybersecurity challenges in smart homes that use IoT technology. It provides an overview of how IoT works in smart homes and examines common security issues, such as unauthorized access to smart home devices or data breaches. It also suggests effective security measures to protect against cyberattacks in IoT-based smart homes, such as strong passwords, regular updates, and using secure networks. In simple terms, the paper provides a comprehensive look at the various security issues facing IoT devices and offers practical solutions and future directions for improving IoT security [10].

Smart Cities and Beyond Broader Impact: The establishment of secure frameworks for IoT networks within urban environments is crucial to prevent the exploitation of interconnected infrastructures such as traffic systems, smart grids, or public surveillance. Scalability and Resilience: The implementation of risk-based adaptive mechanisms ensures that systems maintain scalability and resilience as urban areas integrate an increasing number of IoT devices [13]

Human development has increased significantly in the past two centuries due to advancements in Technology, particularly computing power. The introduction of IPv6, which provides unique addresses for objects, has facilitated increased connectivity through devices like computers and smartphones [15]

Human development has grown rapidly in the last two centuries due to new technologies, including computing power and the Internet of Things (IoT). The number of connected devices is increasing rapidly, with predictions of over 38 billion by 2025 and 50 billion by 2030. IoT connects physical and virtual devices using sensors to monitor and control their surroundings. However, challenges such as weak authentication and limited energy, memory, and processing power pose security risks. This paper focuses on identifying security challenges and offering guidance on improving IoT systems, particularly in authentication and access control. It also discusses IoT architecture and compares different authentication methods [18]

IoT devices within smart home environments frequently exhibit vulnerability to various forms of attacks, including but not limited to unauthorized access, data breaches, or malware infections. The absence of standardized security protocols across diverse devices exacerbates these risks. Proposed Countermeasures' Implications: Security by Design and Default: The implementation of security measures at the outset of device production diminishes the burden placed upon users and safeguards against potential exploitation. Encryption and Regular Updates: The integration of encryption alongside consistent software updates augments privacy and data integrity, thereby diminishing the likelihood of unauthorized access. Awareness Programs: The education of users regarding best practices, such as the establishment of robust passwords and the timely updating of firmware, serves to mitigate risks associated with human error. Lightweight Cryptography: This approach yields practical security solutions suitable for resource-constrained IoT devices prevalent in smart home settings, thereby ensuring operational efficiency without sacrificing safety [21].

An extensive network consisting of various IoT-supported applications and devices is known as an internet of things (IoT)-based cloud infrastructure. This infrastructure encompasses servers, storage, underlying infrastructure, real-time processing, and operations. Moreover, it includes standards and services that are crucial for securing, managing, and connecting different IoT applications and devices [23].

Following the invention of the internet, the internet of things (IoT) is regarded as the next big thing in technology. Kevin Ashton coined the term "Internet of Things" in 1999 [29], and it describes a network that allows data from all connected devices to be collected, processed, and altered to provide new applications [25].

An extensive network consisting of various IoT-supported applications and devices is known as an internet of things (IoT)-based cloud infrastructure. This infrastructure encompasses servers, storage, underlying infrastructure, real-time processing, and operations [26].

In the coming years, with the intelligent decision making, IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together. The IoT is made possible by the latest advancements in RFID and smart sensors. The fundamental idea of the IoT is that it has smart sensors that work directly together without human involvement to deliver new applications. In this survey, we also discuss the significance of security and its challenges [28].

The IoT industry, expected to generate $4 trillion in revenue by 2025, is rapidly growing with 27 billion machines by 2024. However ensuring data confidentiality, integrity and availability is crucial due to large amount of sensitive data generated [30].

2. Materials and Methods

"Ramya et al. [1] an internet-based network of physical items, sensors, actuators, and software applications that may exchange data is called the Internet of Things (IoT), according to research titled "A survey of security challenges, attacks in IoT" by Ramya Prakash et al. Convenience, efficiency, and automation are just a few advantages that IoT offers. Significant security issues with device authentication, access control, and safeguarding private data from hostile assaults are also raised by it. The article provides

an overview of IoT security issues and their objectives, a list of security flaws in IoT design, and recommendations for mitigating them. It also offers insights into IoT security in relation to supporting technologies and architectures. The paper also reviews several other works related to IoT security. For example, Hassija et al. (2019) discussed various application areas and security threats in IoT, while Meneghello et al. (2019) investigated real IoT devices' practical security vulnerabilities. Chen et al. (2017) discussed security solutions for location-based and GPS devices, and Tahir and P. U. (2016) studied malware and malware detection techniques."

"Shalpa et al. [2] Numerous reviews exist regarding IoT security. While some of these researches concentrated on security problems, others concentrated on security solutions using various approaches and techniques. Several IoT security problems were presented in the Hassija et al. study, which also included fog, edge computing, blockchain, and machine learning technologies as potential ways to expand IoT safety. Physical layer security, protocols, and handover protections for mobile-IoT were the subject of another survey. The writers contrasted the current security protocols for Internet of Things mobile applications. IoT mobile computing device security methods based on software and hardware were examined in a systematic review research. The writers covered a range of security verification techniques and emphasized a number of IoT authentication strategies. They also offered suggestions for future study initiatives."

Anass et al. [3] the article titled "A Survey of Security Challenges in Internet of Things" discusses the challenges that IoT (Internet of Things) faces in terms of security. The article starts by defining IoT and discussing its complexity in comparison to the traditional internet. The article then goes on to describe IoT's technical challenges and later focuses its attention on security-related challenges through the use of a layered architecture, which helps in identifying security challenges in IoT. Different levels of the IoT reference model are used to analyze and summarize IoT security issues level-by-level. The article has a three-level architecture starting with device collect data, gateways and, and application service layers. The author's then move on to detail security issues pertinent to each layer. Finally, the study concludes by discussing the emerging security challenges in IoT and identifying future research areas to enhance its security.

"Saurabh et al.[[4] The abstract of the article titled "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network" states that it covers the following topics: possible security attacks on blockchain technology, current security solutions for blockchain, and obstacles to blockchain adoption in IoT networks. It also discusses the concept of blockchain and its application to the Internet of Things (IoT)."

The piece also offers an overview of previous studies and research on the subject, including a number of articles written by other writers that concentrate on using blockchain technology to provide security services and protect privacy in a variety of industries, including healthcare and smart home design.

Nivedita et al. [5] The paper discusses how IoT technology is growing in various fields and its importance in achieving high-security requirements. It highlights that IoT devices face various security challenges such as attacks in IoT layers, low processor speed, power, and memory, and provides countermeasures to address these challenges. The report cited before highlights the rapid growth and importance of Internet of Things (IoT) technologies across several sectors. The key points brought up are summarized as follows:

IoT is becoming more widespread across several industries, indicating its wide range of applications and significance in modern technology and daily life. Ensuring robust security measures are implemented is crucial as the Internet of Things expands. This is because IoT devices often handle sensitive data and are necessary for critical systems. Attacks on IoT levels: Internet of Things (IoT) systems often consist of several layers, such as the application, network, and perception layers, all of which are vulnerable to different types of attacks. Providing security is challenging.

Hamed et al. [6] A survey of the literature on the security of IoT is given in the study "Security and Internet of Things: Benefits, Challenges, and Future Perspectives" by Hamed Taherdoost. In the paper's introduction, the significance of system security and defense against cyberattacks for Internet of Things systems is emphasized. It highlights that any weakness in an Internet of Things system might result in a catastrophic failure that affects a huge number of people, and it implies that IoT security teams are now juggling an increasing number of challenges, including those related to operations, diversity, ownership,

inventories, data volume, and threats. The study continues by reviewing the literature on security and IoT with an emphasis on the circumstances, uses, problems, and prospects for the future. According to the assessment, IoT network security has Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home" is itself a literature review that covers previous research articles regarding cybersecurity, cyber-attacks, and solutions for Internet of Things (IoT)-based smart homes. The literature review titled "Cyber Security Challenges, Attacks, and Solutions for Internet of Things Based Smart Home" summarizes and analyzes the previous research articles focused on the cybersecurity areas of IoT-based smart homes. It covers three main areas:

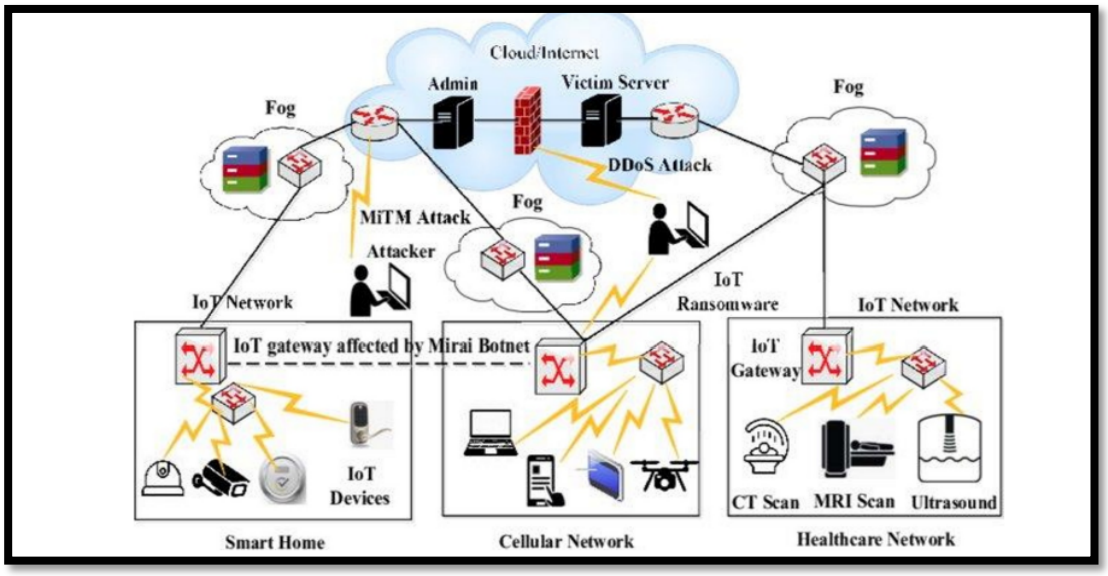

Figure 1. Attack scenario of IoT security in various application areas [1]

"The above figure illustrates the showcasing diverse IoT attack scenarios across application areas, including smart homes, healthcare and industrial systems.

Cybersecurity Challenges: The review identifies and discusses the various security challenges faced by smart home IoT devices. These challenges might include vulnerabilities due to device limitations, the complexity of managing different interconnected devices, and privacy concerns.

Cyber-Attacks: The review categorizes and describes different types of cyber-attacks that target IoT devices in smart homes. These could range from hacking and data breaches to more sophisticated attacks like denial-of-service (DoS) and malware.

Solutions: The review also highlights the various solutions and countermeasures proposed in existing research to tackle the identified security challenges and prevent cyber-attacks. These solutions might involve improved encryption methods, secure communication protocols, and other security technologies designed to protect smart home IoT devices and networks.

Overall, this literature review provides a comprehensive overview of the current state of research on cybersecurity for IoT-based smart homes, summarizing existing knowledge and identifying areas that require further investigation.

Gaurav et al. [7] A survey of the literature on layer-wise security protocols for wireless sensor networks (WSNs) and the internet of things (IoT) is presented in the paper "A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open-Issues". The writers go over the difficulties and problems that come with creating a safe WSN as well as the reasons why conventional security methods might not be suitable for WSNs. The article looks at WSN and IoT standards and protocols, as well as the history, technological challenges, and security features of IoT. Using the Cooja, a ContikiOS simulator, the impact of several assaults on the network's performance and outstanding challenges in cybersecurity are also measured.

Gaurav et al. [8] The study paper provides a survey of the literature on cybersecurity threats, vulnerabilities, and defenses for Internet of Things-based smart homes. It examines current publications on the most prevalent cybersecurity problems and cyberattacks that take use of smart home settings'

weaknesses, offering significant insights on the risks, weaknesses, and security associated with smart homes.

It also outlines several security measures, such as encryption, robust user authentication, proper technological setups, resident security awareness, and network monitoring that may be utilized to lessen assaults on Internet of Things-based smart homes.

Talal et al. [9] This study surveys current IoT threats, classifies them, identifies countermeasures, and identifies the most common IoT assaults. The three levels of the Internet of Things architecture are described in the article as perception, network, and application layers. Service administration and data storage from the network layer in the database are the functions of the middleware layer. IoT vulnerabilities and potential assaults are also described. The paper's conclusion emphasizes the necessity of an IoT technology-specific security mechanism that is both lightweight and resilient while handling the majority of security issues.

Jyoti et al. [10] "A Survey on IoT Security: Attacks, Challenges, and Countermeasures" is a research article that examines the many security risks and issues that exist inside the Internet of Things (IoT). The article starts out by going over the fundamentals of the Internet of Things, its architecture, and the cutting-edge technologies that are employed in the industry. After that, it explores the many security risks and assaults that Internet of Things (IoT) devices may encounter and examines each security risk at every level of the IoT architecture. The article presents current statistics and forecasts the number of IoT devices likely to be deployed in the upcoming years in order to examine the significance of security in the IoT ecosystem."

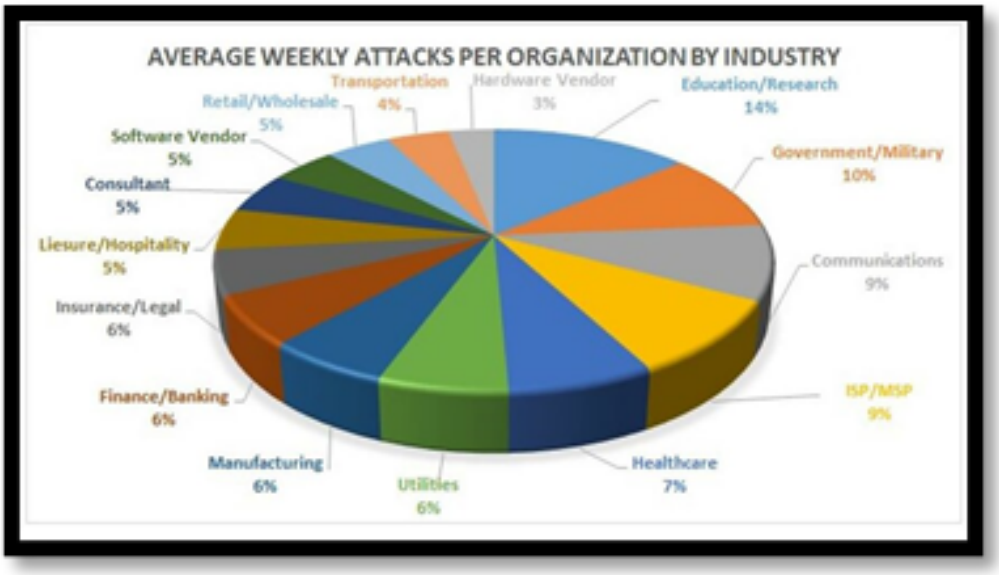

Figure 2. Average weekly attacks per organization [3]

The above figure shows how IoT security can be attacked in different applications. Almost every part of our daily lives, like hospitals, industries, and homes, uses IoT applications and can be affected by the different attacks.

This table summarizes the focus areas, key points, technologies/approaches, security challenges discussed, security solutions proposed, and future research suggestions for each study mentioned in your provided literature review.

There are some of the things covered in the table:

1. An overview of IoT security challenges, issues, flaws, and mitigation
2. Security threats in application areas, fog computing, edge computing, blockchain, and machine learning
3. Practical security vulnerabilities in real IoT devices
4. Security solutions for location-based and GPS devices
5. Malware detection techniques for IoT
6. A layered security architecture analysis
7. Security attacks, current solutions, and obstacles in adoption of blockchain for IoT
8. A literature review on IoT security challenges and benefits

9. Security risks at the architecture, perception, network, and application layers

Table 1. Survey of Related Work to IoT

Author Name	Focus Area	Key points	Approaches	Security Challenges	Solutions of security	Future Suggestions
Ramya Prakash [1]	IoT Security Challenges	Overview of security issues, flaws, and mitigation	N/A	Device authentication, access control, dataprotection	Recommendations for mitigation	Insights Into supporting technologies and architectures
SHAPLA KHANAM[2]	IoT Security and Technologies	Application areas, security threats, integration of new technologies	Fog computing, edge computing, blockchain, machine learning	Various IoT security threats	Use of emerging technologies for security	N/A
Anass Sedrati [3]	Practical IoT Security	Real IoT devices' vulnerabilities	N/A	Practical security vulnerabilities in IoT devices	N/A	N/A
SAURABH SINGH [4]	Location-based and GPS Devices	Security solutions for specific IoT devices	N/A	Security issues in location-based and GPS devices	N/A	N/A
NIVEDITA MISHRA [5]	Malware Detection	Malware and detection techniques	N/A	Malware threats in IoT	Malware detection techniques	N/A
Hamed Taherdoost [6]	IoT Security Challenges	Layered architecture analysis of security issues	N/A	Security issues in device, gateway, and application service layers	N/A	identification of future research areas

3. Conclusion

Our world is being revolutionized by the Internet of Things (IoT), which connects gadgets, allows data sharing, and improves automation, efficiency, and ease. However, because of the variety of hardware, software, and communication protocols, as well as the complexity of large-scale IoT networks, the proliferation of IoT devices poses serious security concerns. This survey has looked at a range of IoT security risks and weaknesses, including as malware attacks, illegal access, and data breaches. It highlights how crucial it is to implement all-encompassing security measures, such as risk-based security policies,

security by design and default principles, and raising user and stakeholder knowledge of security issues. While IoT systems continue to expand and integrate into critical sectors, the security challenges must not be underestimated. Emerging technologies like edge computing and blockchain offer robust solutions tailored to IoT's dynamic and heterogeneous nature. Their adoption, coupled with other innovations like fog computing and machine learning, represents a significant step toward a more secure and resilient IoT ecosystem. The combination of cutting-edge technologies like edge computing, blockchain, fog computing, and machine learning offers promise in addressing these issues. These innovations can provide strong security.

References

1. Prakash, Ramya, Neeli Jyoti, and S. Manjunatha. "A survey of security challenges, attacks in IoT." E3S Web of Conferences. Vol. 491. EDP Sciences, 2024.
2. Khanam, Shapla, et al. "A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things." IEEE access 8 (2020): 219709-219743.
3. Sedrati, Anass, and Abdellatif Mezrioui. "A survey of security challenges in internet of things." Advances in Science, Technology and Engineering Systems Journal 3.1 (2018): 274-280.
4. Singh, Saurabh, ASM Sanwar Hosen, and Byungun Yoon. "Blockchain security attacks, challenges, and solutions for the future distributed iot network." Ieee Access 9 (2021): 13938-13959.
5. Mishra, Nivedita, and Sharnil Pandya. "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review." IEEE Access 9 (2021): 59353-59377.
6. Taherdoost, Hamed. "Security and internet of things: benefits, challenges, and future perspectives." Electronics 12.8 (2023): 1901.
7. Sharma, G., et al. "A Survey on Layer-Wise Security Attacks in IoT: Attacks, Countermeasures, and Open-Issues. Electronics 2021, 10, 2365." (2021).
8. Abdullah, Talal A., et al. "A review of cyber security challenges attacks and solutions for Internet of Things based smart home." Int. J. Comput. Sci. Netw. Secur 19.9 (2019): 139.
9. Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017.
10. Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017.
11. Abba Ari, Ado Adamou, et al. "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges." Applied Computing and Informatics 20.1/2 (2024): 119-141.
12. Kathole, Atul B., et al. "Challenges and Key Issues in IoT Privacy and Security." Communication Technologies and Security Challenges in IoT: Present and Future. Singapore: Springer Nature Singapore, 2024. 37-50.
13. Kaur, Kawalpreet, et al. "Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies." Frontiers in Computer Science 6 (2024): 1420680.
14. Ahanger, Tariq Ahamed, and Abdullah Aljumah. "Internet of Things: A comprehensive study of security issues and defense mechanisms." IEEE Access 7 (2018): 11020-11028.
15. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, ''A survey on IoT security: Application areas, security threats, and solution architectures,'' IEEE
16. V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, ''Security, privacy and trust for smart mobile- Internet of Things (M-IoT): A survey,'' IEEE Access, vol. 8, pp. 167123–167163, 2019, doi: 10.1109/ACCESS.2020.3022661.
17. Shaukat, Kamran, et al. "A review on security challenges in internet of things (IoT)." 2021 26th international conference on automation and computing (ICAC). IEEE, 2021.
18. Deogirikar, J., & Vidhate, A. (2017, February). Security attacks in IoT: A survey. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 32-37). IEEE.
19. Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions and future directions." 2016 49th Hawaii International Conference on System Sciences (HICSS). IEEE, 2016.
20. Abdullah, T. A., Ali, W., Malebary, S., & Ahmed, A. A. (2019). A review of cyber security challenges attacks and solutions for Internet of Things based smart home. Int. J. Comput. Sci. Netw. Secur, 19(9), 139.
21. Azrour, Mourade, et al. "Internet of things security: challenges and key issues." Security and Communication Networks 2021.1 (2021): 5533843.
22. Sha, Kewei, et al. "On security challenges and open issues in Internet of Things." Future generation computer systems 83 (2018): 326-337.
23. Xu, Teng, James B. Wendt, and Miodrag Potkonjak. "Security of IoT systems: Design challenges and opportunities." 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). IEEE, 2014.
24. Litoussi, Mohamed, et al. "IoT security: challenges and countermeasures." Procedia Computer Science 177 (2020): 503-508.
25. Dargaoui, Souhayla, et al. "An overview of the security challenges in IoT environment." Advanced technology for smart environment and energy (2023): 151-160.

26. Bazgir, Ehsan, et al. "Security aspects in IoT based cloud computing." World Journal of Advanced Research and Reviews 20.3 (2023): 540-551.
27. Shah, A. M., Aljubayri, M., Khan, M. F., Alqahtani, J., Sulaiman, A., & Shaikh, A. (2023). ILSM: Incorporated Lightweight Security Model for Improving QOS in WSN. Computer Systems Science & Engineering, 46(2).
28. Lone, Aejaz Nazir, Suhel Mustajab, and Mahfooz Alam. "A comprehensive study on cybersecurity challenges and opportunities in the IoT world." Security and Privacy 6.6 (2023): e318.
29. F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, ‘‘IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices,’’ IEEE Internet Things J., vol. 6, no. 5, pp. 8182–8201, Oct. 2019, doi
30. Huan, N. T. Y., & Zukarnain, Z. A. (2024). A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications. IEEE Access.
31. Kizza, J. M. (2024). Internet of things (iot): growth, challenges, and security. In Guide to Computer Network Security (pp. 557-573). Cham: Springer International Publishing.

.