IJISEM
INTERNATIONAL JOURNAL OF INNOVATIONS IN SCIENCE ENGINEERING AND MANAGEMENT

OPEN ACCESS

Volume: 2

Issue: 4

Month: December

Year: 2023

ISSN: 2583-7117

Published: 16.12.2023

Citation:

Mrs. Elavarasi Kesavan "Internet of Things (IoT): A Review of Security Challenges and Solutions" International Journal of Innovations in Science Engineering and Management, vol. 2, no. 4, 2023, pp. 65–71.

DOI:

10.69968/ijisem.2023v2i465-71

Internet of Things (IoT): A Review of Security Challenges and Solutions

Mrs. Elavarasi Kesavan[1]

[1]*Full Stack QA Architect, Cognizant*

Abstract

To improve people's quality of life (QoL), one of the most promising technologies is the Internet of Things (IoT). Since of the variety of IoT settings, it is essential to address and analyse IoT security problems since IoT applications operate differently. To help developers and businesses identify timely and suitable solutions to address particular dangers and provide the finest IoT-based services, it would be helpful to highlight the IoT security problems along with prospective and accessible solutions. It concluded that the growing integration of IoT devices across industries and personal spaces amplifies security and privacy concerns. This review outlined key challenges across IoT architecture layers—sensing, network, middleware, and application—and explored advanced solutions such as machine learning, blockchain, and edge computing. Effective security demands intelligent, adaptive systems capable of identifying threats and mitigating risks in real time. Emerging frameworks like lightweight replay attack detection, deep learning for malware hunting, and memory-efficient key schemes demonstrate promising directions. Continued research and innovation are essential to fortify IoT ecosystems and ensure secure, resilient deployments in the face of evolving cyber threats.

Keywords; Internet of Things (IoT), IoT security issues, Machine learning, Blockchain, Edge computing, Artificial intelligence, Information and Communications Technology (ICT), etc.

INTRODUCTION

The development of a number of technological fields in recent years, including wireless communications, embedded computing, broadband internet access, and automated tracking and identification, has led to the introduction of intelligent objects into our daily life. The term "Internet of Things" (IoT) describes how the Internet is integrated with physical objects found in a variety of contexts, such as smart homes, industrial operations, health monitoring, and environmental monitoring [1]. In the IoT ecosystem, blockchain, cloud computing, AI, machine learning, and humanitarian logistics are essential for increasing productivity, security, and creativity. While humanitarian logistics makes use of IoT capabilities to manage assistance distribution during catastrophes, blockchain guarantees safe and transparent transactions between IoT devices. For smooth communication and analysis of data produced by the Internet of Things, cloud computing offers scalable processing and storage resources [2]. Across a wide variety of industries, including healthcare, transportation, agriculture, and smart cities, machine learning and artificial intelligence improve operational efficiency by enabling intelligent decision-making, predictive analytics, and automation in the IoT ecosystem [3]. "The Information and Communications Technology (ICT)" sector is anticipated to rely heavily on it in the years to come. Businesses may get a competitive edge in the ICT sector by using the potential of IoT technology, which has the potential to improve decision-making, user experiences, and operational efficiency [4].

In IoT-enabled contexts, identifying security threats and creating solutions requires more time and effort. Because everything is connected to the Internet, there are many security issues that the Internet of Things has brought to light. Concerns around end-user privacy are also present.

A lack of technical improvements and the presence of a security problem are the primary reasons why the growth of IoT has stagnated [5]. Thus, despite all of its sophisticated information sharing features, the Internet of Things is a security-flawed idea. For broad and successful adoption, it is thus preferable to take the right actions in its early stages, i.e., providing security, before future development. For IoT applications, security and privacy are crucial concerns. As the IoT has expanded throughout the country and changed people's lives, the demand for privacy and security has increased and become a significant concern [6].

Internet of Things and its importance

The Internet of Things (IoT) is a network of physical objects, including appliances, vehicles, and devices, that are equipped with sensors, software, and network connectivity. This enables them to collect and exchange data [7]. IoT devices, which are also referred to as "smart objects," encompass a wide variety of technologies, including straightforward "smart home" devices such as smart thermostats, wearables such as smartwatches and RFID-enabled apparel, and intricate industrial apparatus and transportation systems. Technologists are even imagining the creation of entire "smart cities" that are predicated on IoT technologies. These smart devices are capable of communicating with one another and with other internet-enabled devices on the basis of the Internet of Things. The establishment of a vast network of interconnected devices that can exchange data and perform a variety of tasks autonomously, similar to smartphones and gateways [8].

Better Decision Making: The data that devices can obtain from a variety of sources is substantial due to the presence of multiple sensors. This provides them with a greater amount of information to work with when interpreting the data they receive. Smartphones is an excellent illustration. Based on your age, location, and activity, the device automatically monitors your behaviours on its interface and provides recommendations. Various activities can also be monitored by the phone. This encompasses the sleep patterns, power consumption, and screen time that users spend each day. Companies that manufacture smartphones are receiving vast quantities of data on a daily basis in order to enhance their respective capabilities. Companies are able to promptly identify their strengths and vulnerabilities by observing trends in the utilisation of their devices, which is brought about by the continuous inundation of big data. It is impossible to achieve this understanding without the assistance of embedded sensors and processors that analyse the data [9].

Real-time Tracking and Monitoring: Web-based monitoring and tracking solutions have a lot of promise. IoT monitoring offers an effective way to keep an eye on and track anything, including shipping containers, stolen products, and car fleets. Certain gadgets are even able to detect environmental changes. The efficiency of businesses may be greatly increased by IoT trackers in a variety of sectors. For the business, a breakdown in these items may result in massive losses. In order to provide optimal services, IoT-based trackers must be dependable [10].

Automation: The ease of IoT is a major factor in its creation. Intelligent gadgets that automate routine operations free up human time for other pursuits. In the end, people's workloads are reduced by these gadgets. With smartphones, we can communicate with individuals across the globe. To save ourselves typing, we may even utilise dictation and plan when to send messages. There are also smart refrigerators. Consider having one that can identify when food is nearing expiration and alert the owner to consume it before it's too late. When the milk is almost gone, the smart refrigerator may even recognise it and place an automated order for more. Another example would be a self-driving automobile that connects to the Internet to determine the fastest way to get there. This is the pinnacle of human convenience. IoT has a huge amount of space for innovation [11].

Security challenges in IoT

The Rise of Botnets: The number of botnet assaults has increased recently. Among IoT devices, botnets are networks of computers infected with malicious software that are managed collectively without the owners' knowledge. When malevolent hackers take control of internet-connected devices remotely and exploit the data they get for illicit activities, a botnet is created. It is possible for a hospital or other organization's computer network equipment to be included into a botnet without the management's knowledge. The majority of organisations, including the hospital, do not have real-time security solutions to monitor botnets, which is the issue [12].

The large volume of IoT Devices: Experts in cybersecurity have spent the last several years mostly defending computers and mobile devices. However, both public and private organisations now have a large number of IoT devices. Currently, there are around 7 billion gadgets in use, and by 2020, that figure may rise to 20 billion. More IoT devices translate into more security flaws, which makes things harder for security professionals [13].

Lack of Encryption: One of the main IoT security issues is encryption, even if it's a wonderful way to prevent hackers from accessing data. These Internet of Things devices may not have the same processing and storage capacity as a conventional computer. As a consequence, there is a rise in attacks where hackers may simply alter the algorithms that are intended to provide safety and security [14].

Outdated Legacy Security: The interdependencies of older systems are another issue. Older technology don't appear to fit in with an organisation that has more and more IoT devices. In the event of a breach in a single IoT device, an integrated older system without contemporary security requirements may be violated [15].

User's Privacy: It's crucial for businesses to safeguard user data, which includes information on both internal and external users. Since many employees are using IoT devices that their companies offer, this is a matter for worry. An enterprise's reputation would suffer if there was a breach and data was exposed. Given these issues, one of the most important IoT security issues that has to be resolved is privacy.

IoT Financial Breaches: There is often a chance that hackers might access sensitive data and steal money when a bank or other organisation uses Internet of Things devices for electronic or e-payments. These days, a lot of businesses are using blockchain or machine intelligence to stop financial fraud before it starts. However, not all businesses or organisations have used this method. Fig. 1 summarises the categories of IoT security attacks [16].

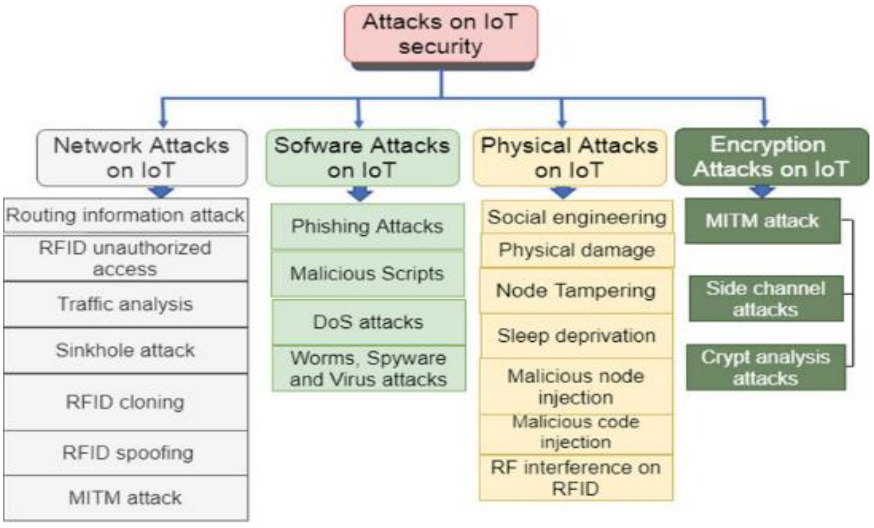

Figure 1 Classification of IoT attacks [16]

Solutions to the Security Challenges in the IoT

In Table 1, the suggested solutions are categorised and explored as follows:

Trust management: Internet of Things (IoT) security necessitates effective trust management. The critical function of trust administration in the IoT-based system. People can overcome the hazards and uncertainty associated with the IoT by implementing trust management. Security and privacy are both factors that contribute to the concept of trust. The perception of trust that users have when communicating in the Internet of Things is defined by their emotional responses. In other words, users are entitled to manage their services at any time and from any location, and they are provided with devices that assist them in comprehending their interactions with IoT systems. Furthermore, they remark that effective management can foster trust in the Internet of Things.

Authentication: There is potential for the development of numerous authentication models for the Internet of Things (IoT) to enhance security and privacy services. By means of a security token, a gateway, a trust chain, or a global trust tree, the models may authenticate. This is to say that each model has its own advantages and disadvantages.

Privacy Solutions: The literature identifies a number of remedies to privacy concerns. Each user ought to have the resources necessary to handle their data. The notion of privacy by design refers to the fact that privacy concerns are taken into consideration throughout the design process. There is also the transparency principle. Transparency in the

context of IoT implies that consumers must be aware of the organisation or body that is handling their data, as well as how and when it is being used. Therefore, in order to strengthen privacy, transparency regulations need to be implemented. Another alternative that has been suggested is data management.

Secure Communication: To handle secure communication, a number of protocols have been developed for Internet of Things systems. For example, the Internet of Things protocol stack may be connected to a traditional Internet host to create an extended Internet, allowing for the use of different security solutions that are already in place. Secure communication protocols by offering solutions for IoT communication security that are based on symmetric and asymmetric pre-distributed keys.

Table 1 Classification of the proposed solutions [16]

S. No.	Problem	Proposed solution
1	The risks and uncertainty involving the IoT	IoT risks and uncertainties may be mitigated with the use of trust management. For security and privacy, each device must have faith in the other throughout communication.
2	The vulnerability of authentication schemes makes them remain insecure in its protection of user privacy	There are many IoT authentication approaches that may aid with privacy and security.
3	Lack of privacy consideration in the design of the IoT devices	In order to protect sensitive information from the public domain, assist users in acquiring the necessary tools to manage their own data privately.
4	Lack of policy enforcement role	Security for the Internet of Things (IoT) through software. It offers a security architecture solution for the purpose of monitoring and controlling the environment.
5	Fault-tolerant security challenge	Help the gadget protect itself against threats and network outages. Encouraging ethical and safe usage
6	Lack of adequate IoT protocol for secure communication	The Internet of Things protocol stack may work with traditional Internet hosts to provide an expanded Internet that allows for safe communication using a variety of current security methods.

LITERATURE REVIEW

(Lu, 2023) [4] With its ability to bring automation and intelligence to a wide range of application areas, the Internet of Things is becoming a global trend that offers both security issues and benefits. It is used in a number of industries, including as smart cities, home automation, smart grids, and healthcare. Cyberattacks, data breaches, and other malevolent actions are more likely to occur as the number of IoT-connected devices rises. In order to safeguard the data being sent, it is imperative that secure protocols and encryption techniques be used. In this study, IoT security vulnerabilities are identified and summarised. Identifying common security and privacy concerns is covered after a discussion of security risks across the various IoT architectural levels. The topic of security countermeasures is also covered.

(Mazhar et al., 2023) [17] This study examines IoT security intelligence from all possible perspectives. Using machine learning and deep learning to extract information from raw data is a novel way to defend IoT devices from various threats. In light of our results, we conclude by talking about pertinent research questions and possible future directions. In order to protect IoT devices and identify attack trends in unstructured data, this article looks at machine learning and deep learning. In light of these discoveries, we talk about the difficulties that researchers encounter and possible future paths for this field of study. The material on this website may be used as a technical resource and reference by anybody interested in cybersecurity or the Internet of Things.

(Rekha et al., 2023) [18] The work progress of IoT is examined in this research, which also identifies and briefly addresses various safety issues and concerns that need to be identified. Consideration must be given to dependable and useful IoT protection in order to safeguard information privacy, professionalism, honesty, encryption, intrusion detection, and recognition capabilities, as well as adaptability, interoperability, and usability. New IoT methods from the scientific, educational, and industrial sectors are presented and addressed in terms of specific realities by examining some of the recent IoT research. Developing and implementing appropriate IoT applications that can guarantee honesty, security, and integrity in linked situations is crucial, based on the findings of this paper.

(Ali et al., 2021) [19] A new paradigm in technology, the Internet of Things (IoT), sometimes referred to as the Internet of Everything, is a global network of linked devices. Information technology (IT) gains a new dimension with the Internet of Things (IoT), allowing devices to connect with other equipment and people. The IT sector and researchers created a variety of IoT systems and devices. IoT principles may be used and implemented in a variety of ways. IoT is becoming more intentional with concepts like smart cities and smart homes, which raises security issues. Gathering reported security vulnerabilities, classifying them, and offering ways to address those IoT security issues are the goals of this article.

(Azrour et al., 2021) [20] These days, a wide range of industries, including the home, healthcare, telecommunications, environment, construction, water management, and energy, employ the new IoT technology. Computers, laptops, and mobile devices are not the same as Internet of Things technology, which uses embedded devices. Security is becoming more important for IoT systems because of the exchange of personal data produced by sensors and the potential to merge the real and virtual worlds. IoT also necessitates the use of lightweight encryption methods. In order to guide authentication procedures and establish a secure IoT service, this article aims to highlight the security problems and critical concerns that are anticipated to develop in the IoT environment.

(Mehdipour, 2020) [21] Although the Internet of Things (IoT) is expanding rapidly, privacy and security flaws are the main obstacles to its widespread use. Traditional security and privacy methods are not relevant to the Internet of Things (IoT) because to its decentralised architecture and the resource limitations of most of its components. Secure interaction and communication across many devices is feasible, but it may be costly, time-consuming, and complicated. The present security models, which are mostly centralised, must be replaced with new ones. An overview of the layers and components of the IoT architecture, security problems and difficulties at various levels, some solutions, and future perspectives are given in this article.

(HaddadPajouh & M. Parizi, 2019) [22] This article offers a thorough analysis of IoT security concerns, constraints, specifications, and existing and prospective fixes. In order to define security attributes and needs for each layer, the study expands on a taxonomy that uses the three-layer IoT architecture as a guide. This survey's primary contribution is the architectural classification of prospective IoT security threats and issues. In order to help readers better understand how to address and implement best practices to avoid the current IoT security dangers on each tier, IoT security issues and solutions are then further categorised by the layered architecture.

(Aldowah et al., 2019) [23] This study summarises the security risks and difficulties that need to be taken into account after reviewing the advancements in IoT research. Aside from heterogeneity, scalability, and availability, effective and functional security for the Internet of Things is necessary to provide data privacy, confidentiality, integrity, authentication, access control, and identification. Taking these realities into account, new IoT solutions from the technical, academic, and industrial sides are presented and explored by evaluating some of the most recent IoT research. According to the study's conclusions, it is necessary to develop and implement suitable IoT solutions that can provide integrity, confidentiality, and anonymity in diverse settings.

CONCLUSION

In conclusion, the rapid proliferation of IoT devices across industries and personal applications has significantly amplified security and privacy concerns. This review has provided a comprehensive taxonomy of IoT security challenges across the Application, Network, and Edge layers, emphasizing the necessity of layered protection strategies. Effective IoT security demands a deep understanding of system architecture and potential vulnerabilities at each level, including the sensing, network, middleware, gateway, and application layers. Cyberattacks targeting these layers necessitate adaptive, intelligent defenses such as machine learning and deep learning-based models that utilize IoT-specific data attributes for threat detection and mitigation. Emerging technologies like blockchain and edge computing offer promising solutions to enhance security, reduce latency, and protect user privacy. Notable advancements such as lightweight replay attack detection frameworks for healthcare, RNN-based malware threat hunting, and MEMK schemes for secure data transmission illustrate the ongoing efforts to address specific security needs. Tools like IoT Scanner further aid in identifying and mitigating privacy threats in localized IoT networks. Despite these innovations, considerable research gaps remain, particularly in balancing security with resource constraints and interoperability. Continued interdisciplinary research is essential to develop robust, scalable, and efficient solutions that can secure the evolving landscape of IoT ecosystems against increasingly sophisticated cyber threats.

REFERENCES

[1] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and Solutions Survey," Sensors, vol. 22, no. 19, pp. 1–51, 2022, doi: 10.3390/s22197433.

[2] N. A. Khan, A. Awang, and S. A. A. Karim, "Security in Internet of Things: A Review," IEEE Access, vol. 10, no. September, pp. 104649–104670, 2022, doi: 10.1109/ACCESS.2022.3209355.

[3] Bharat Batham 2023. Fog Computational-Based Deep Learning Model for Optimization of Micro Grid Connected WSN With Load Balancing. International Journal of Innovations in Science, Engineering And Management. 2, 3 (Sep. 2023), 97–103.

[4] Y. Lu, "Security and Privacy of Internet of Things: A Review of Challenges and Solutions," J. Cyber Secur. Mobil, vol. 12, no. 6, pp. 813–844, 2023, doi: 10.13052/jcsm2245-1439.1261.

[5] A. K. Abed and A. Anupam, "Review of security issues in Internet of Things and artificial intelligence-driven solutions," Secur. Priv., vol. 6, no. 3, pp. 1–18, 2023, doi: 10.1002/spy2.285.

[6] M. Aziz Al Kabir, W. Elmedany, and M. S. Sharif, "Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques," J. Cyber Secur. Technol., vol. 7, no. 4, pp. 199–223, 2023, doi: 10.1080/23742917.2023.2228053.

[7] Dubey, P. 2023. The Role of Artificial Intelligence in Modern Human Resource Management: A Review. International Journal of Innovations in Science, Engineering And Management. 2, 4 (Nov. 2023), 59–64. DOI:https://doi.org/10.69968/ijisem.2023v2i459-64.

[8] T. Rajmohan, P. H. Nguyen, and N. Ferry, "A decade of research on patterns and architectures for IoT security," Cybersecurity, vol. 5, no. 1, 2022, doi: 10.1186/s42400-021-00104-7.

[9] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," J. Big Data, vol. 6, no. 1, 2019, doi: 10.1186/s40537-019-0268-2.

[10] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," Hawaii Int. Conf. Syst. Sci., pp. 5772–5781, 2016, doi: 10.1109/HICSS.2016.714.

[11] M. Aqeel, F. Ali, M. W. Iqbal, T. A. Rana, M. Arif, and M. R. Auwul, "A Review of Security and Privacy Concerns in the Internet of Things (IoT)," J. Sensors, 2022, doi: 10.1155/2022/5724168.

[12] M. K. Saini and R. K. Saini, "Internet of Things (IoT) Applications and Security Challenges: A Review," SSRN Electron. J., 2019, doi: 10.2139/ssrn.4903947.

[13] H. Taherdoost, "Security and Internet of Things: Benefits, Challenges, and Future Perspectives, Electron" vol. 12, no. 8, pp. 1–22, 2023, doi: 10.3390/electronics12081901.

[14] P. Goel, A. Jain, and D. Juneja, "Security Issues on Internet of Things (IoT): A Recent Challenges and Countermeasures," Int. J. Res. Appl. Sci. Eng. Technol., vol. 11, no. 12, pp. 2033–2039, 2023, doi: 10.22214/ijraset.2023.57760.

[15] H. Pourrahmani, A. Yavarinasab, A. M. H. Monazzah, and J. Van herle, "A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain," Internet of Things (Netherlands), vol. 23, no. June, p. 100888, 2023, doi: 10.1016/j.iot.2023.100888.

[16] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhawaldeh, and H. Arshad, A Review on the Security of the Internet of Things: Challenges and Solutions, vol. 119, no. 3. Springer US, 2021. doi: 10.1007/s11277-021-08348-9.

[17] T. Mazhar et al., "Analysis of IoT Security Challenges and Its Solutions Using Artificial," brain Sci., vol. 13, 2023.

[18] S. Rekha, L. Thirupathi, S. Renikunta, and R. Gangula, "Study of security issues and solutions in Internet of Things (IoT)," Mater. Today Proc., vol. 80, no. xxxx, pp. 3554–3559, 2023, doi: 10.1016/j.matpr.2021.07.295.

[19] R. F. Ali, A. Muneer, P. D. D. Dominic, S. M. Taib, and E. A. A. Ghaleb, "Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review," Springer Nat. Singapore Pte Ltd., 2021, doi: 10.1007/978-981-16-8059-5_9.

[20] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of Things Security: Challenges and Key Issues," Secur. Commun. Networks, vol. 2021, no. September, 2021, doi: 10.1155/2021/5533843.

[21] F. Mehdipour, "A Review of IoT Security Challenges and Solutions," Proc. 8th Int. Japan-Africa Conf. Electron. Commun. Comput, pp. 1–6,

2020, doi: 10.1109/JAC-ECC51597.2020.9355854.

[22] H. HaddadPajouh and R. M. Parizi, “A survey on internet of things security: Requirements, challenges, and solutions,” Internet of Things (Netherlands), vol. 14, p. 100129, 2019, doi: 10.1016/j.iot.2019.100129.

[23] H. Aldowah, S. Ul Rehman, and I. Umar, Security in internet of things: Issues, challenges and solutions, vol. 843, no. September 2021. Springer International Publishing, 2019. doi: 10.1007/978-3-319-99007-1_38.