

IoT Security in the Age of Smart Devices

Kavya H C¹, Karthik S R² and Dr. Vishwanath Venkatesh Murthy³

^{1,2}Department of MCA, RNS Institute of Technology, Bengaluru, India

Email: kavyahc23mca@rnsit.ac.in, karthiksr23mca@rnsit.ac.in

³Associate Professor, Department of MCA, RNS Institute of Technology, Bengaluru, India

Email: vishwanathmurthy@rnsit.ac.in

Abstract— As smart gadgets pop up more and more in our homes, workplaces, and even in cities, the Internet of Things, or IoT, is really taking off. It's amazing how these devices make our lives easier and more innovative. Here's the deal it brings along some pretty hefty security risks. Seriously, think about it for a second. Any gadget that one uses—the fitness tracker, the smart car, the camera, or even your thermostats—are potential marks to be cyber-attacked. If one really dwells on it, it is indeed scary. IoT environments are much more complex and heterogeneous, which makes it difficult to standardize the implementation of security protocols. In this paper, security vulnerabilities in the IoT are discussed along with real-life risks such as data breaches, unauthorized access, and invasions of privacy. Moreover, it explores novel solutions like encryption and authentication protocols while also exploring AI-based monitoring or edge security. Securing IoT systems is not just a technical hurdle, it's also an essential step towards creating smarter digital environments. Smart devices are evolving rapidly. This paper provides a survey and comparison of various security techniques, algorithms, and methodologies that researchers have developed to make IoT systems more secure in the current smart device age. It discusses typical security issues, surveys a variety of proposed solutions, and analyses how effective they are in securing connected devices.

Index Terms— Internet of Things (IoT), IoT Security, Smart Devices, Cyber-security, Data Privacy, Artificial Intelligence in IoT, Post-Quantum Cryptography, Smart Home Security, Machine Learning, Security Challenges, IoT Vulnerabilities, Blockchain in IoT, Software-Defined Networking (SDN).

I. INTRODUCTION

Internet of Things (IoT) has rapidly emerged as one of the most revolutionary technologies of the new age. Ranging from automated home devices and wearable fitness bands to industrial sensors and networked cars, IoT has integrated itself into almost all aspects of modern life. While the number of smart devices grows at an unparalleled pace, so does the amount of data that they produce— and with that, the potential threats to privacy and security.

Figure 1 shows, the number of connected IoT devices has surged globally from under 5 billion in 2015 to a projected 19.7 billion by 2025 [1]. The rapid growth we're seeing really highlights just how much we depend on interconnected systems these days. It's pretty wild when you think about it! That makes securing these devices more important than ever [2]. So, here's the thing: IoT devices are quite limited in their resources. They work in all sorts of environments and, honestly, many of them don't have strong security features built right in. It's like an open invitation for cyber threats.

I mean, when you have those vulnerabilities, it opens the door to potential breaches, unauthorized access... and those could really disrupt critical services. It's a bit concerning. In order to address this concern, this study will examine the security implications of smart devices in the realm of IoT [3]. It presents an in-depth overview of security threats of IoT Systems, surveys existing solutions, and compares the performance of several methods suggested by researchers. Through pointing out the ongoing work and pinpointing shortcomings, this paper seeks to advance more secure and robust IoT infrastructures.

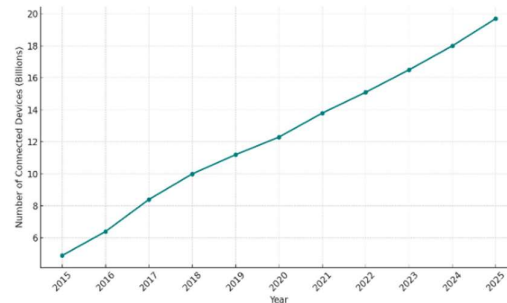


Figure 1: Global Growth of IoT Devices (2015-2025)

II. CHALLENGES

It is quite ironic that, despite the high awareness about vulnerabilities associated with the Internet of Things (IoT), securing these interconnected systems remains a hard nut to crack. Unlike other computing environments, an IoT ecosystem is a diverse collection of devices, each with varying hardware specifications, operating systems, and communication protocols, making it complicated to implement standard security across all platforms [4].

Moreover, most IoT devices are designed with low energy requirements and limited computing power, which restricts them from utilizing standard security software such as firewalls or sophisticated encryption solutions [5]. Communication between devices is mostly happening in unshielded or poorly shielded condition making it easier to intercept or manipulate sensitive data by attackers [6].

Apart from the technical limitations, there is no agreed international standard to ensure worldwide security, and the visibility of devices in uncontrolled environments increases their susceptibility to condition [7].

These are the primary threats represented in Figure 2, representing the first problems that researchers and developers consider to secure IoT Systems.



Figure 2: Security Threats

III. LITERATURE SURVEY

The paper by Rawn Mahmoud and colleagues summarizes the new security environment in the Internet of Things (IoT) and highlights its most serious weaknesses. Although the quantity and capabilities of IoT devices continue to increase, the authors point out that protecting these systems is one of the most important technological challenges of our day. They begin by describing the primary reasons for attacks on IoT systems, including their widespread adoption, non-standardization, and poor inherent security capabilities. The article

discusses prevalent threats such as unauthorized access to devices, denial-of-service (DoS) attacks, and data breaches. The presence of IoT systems often entails a large number of devices communicating over many platforms, which increases the likelihood of security vulnerabilities, also making these issues more complicated. They also identify the necessity of future studies to create lightweight security protocols specific to the unique limitations of IoT devices.[8]

Rawn Mahmoud and others in their paper proposed IoT security principles shown in the Figure 3.



Figure 3: IoT Security Principles [8]

The study conducted by Renu Shrivastav has elaborated on these new vulnerabilities, focusing on the unique security vulnerabilities in IoT space and the way this is responded by security solutions [9]. So difficult is the task to secure IoT devices that the paper begins with an acknowledgment of that fact, focusing on the wide array of networking, processing power, and role they play in our lives: It is difficult to provide security measures to these small devices with low energy and high capability of mobility, because of their heterogeneous devices and obscure connectivity, functionality, and limited computation capability.[9]

The primary risks, says Shrivastav, are physical tampering, data breaches, unauthorized access and insecure communication. As more and more devices get connected to the internet, that attack surface expands, increasing the risk of cyberattacks. The study looks at a number of contemporary strategies to deal with these problems. One of the main focuses is lightweight encryption, which ensures information confidentiality and is suitable for devices with very low resources [9]. Blockchain is also mentioned in the paper as a decentralized file system, which appears to be a good way to improve device authentication forensically and secure information exchange. Using machine learning algorithms for intrusion detection and real-time anomaly monitoring is another novel strategy being discussed. This can significantly enhance the proactive defence capabilities of IoT systems. [9]

Tinashe Magara and Yousheng Zhou address the growing privacy and security concerns associated with smart home settings in their 2024 paper [10]. Regarding the subject, the writers stress how user information in smart speakers, cameras, lightbulbs, and other household appliances is or may become vulnerable due to unmatched user access. The authors address some of the most important topics, including data acquisition methods, anonymization of identities, storage duration, and cross-platform data sharing with other platforms or third parties [10]. The most careless of these is "behavioural profiling," which can result from constant data monitoring.

This is a significant article regarding the rise of privacy protections in comparison to system IoTs [10]. There is not adequate specific detailed based security framework for most smart devices available due to their power consumption being heavy and methodical light weight low powered devices constraints. Magara and Zhou emphasize the importance of adaptable, scalable, and energy-efficient security models that are capable of adapting to various devices and applications.

Tinashe Magara and Yousheng Zhou in their paper proposed a IoT Security Solutions in the following Figure 4

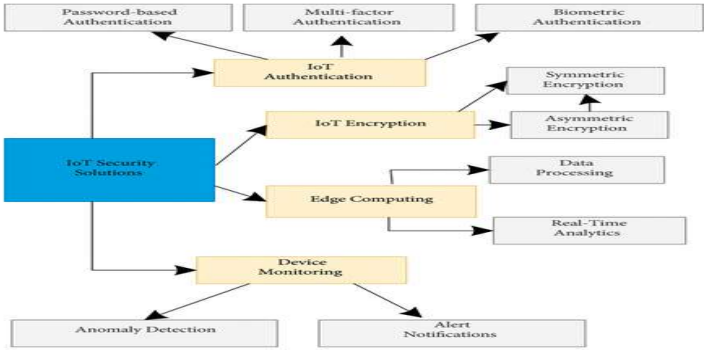


Figure 4: Proposed IoT Security Solutions [10].

In their 2023 research, Tehseen Mazhar and his colleagues explore how artificial intelligence, namely machine learning (ML) and deep learning (DL), can be utilized to improve threat detection and protection in IoT systems [11]. They highlight the fact that conventional security measures tend to lag behind in dealing with real-time information and identifying advanced cyber-attacks. This is where the new SQL is so critical and AI becomes an essential tool for deploying IoT security and enabling it to continually learn from data patterns, emerging threats and even zero-day threats. Their [11] work exposes how ML and DL models can be trained to identify anomalies and unusual patterns in IoT device networks to allow for intrusions to be detected well before any damage is caused. But the authors also point out some challenges, including the difficulty of obtaining high-quality training data and the limitations of IoT devices, which might not be able to handle sophisticated AI models.

The article encourages further research into lightweight AI models that can work well on low-power devices without compromising on accuracy [11]. It also encourages the development of smarter, more responsive security controls. The authors also advocate for better privacy policies, which are transparent and understandable to users. According to them, people should have more control over their own information and be properly informed about how their information is used or shared.

Tehseen Mazhar and other's in their paper proposed an machine learning based security framework to improve the security of IoT products.

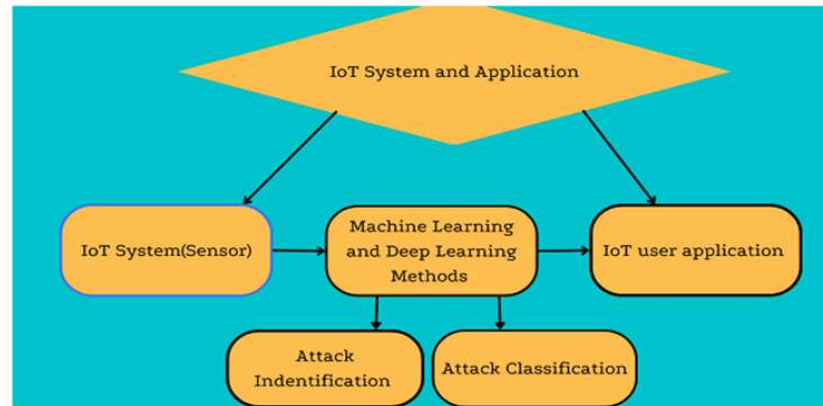


Figure 5: A machine learning security framework for IoT systems [11]

With IoT devices growing both in personal and industrial application, the paper by Mauro Conti and Ali, emphasizes how such connected devices are becoming more vulnerable to cyber-attacks [12]. The authors stress that the majority of these IoT devices are constructed with limited resources, which compromises affordability and usability with robust security features. Consequently, they face risks such as malware infection, unauthorized access, and data modification. Considerable focus within this paper is dedicated to the issue of tracking and analyzing IoT cyber attacks in ancillary device compromise situations. This illustrates that methodical tracking for malicious activity is based on identifying compromised devices and capturing digital footprints with minimal disruption to normal network operations.

The article highlights other limitations in IoT forensics which do not include methods for standardize devising procedures for investigating and data retrieval for devices with limited processing and storage capabilities. The authors conclude IoT systems need to be designed with integrated active forensic capabilities facilitating surveillance and responsive actions to cyber attacks, and therefore argue this issue requires further exploration.[12]

In a related study, Ahmid Maroua and Kazar Okba tackle the ever-growing use of the IOT and its varying security concerns [13]. The authors highlight the need of recognizing and resolving the developing security dangers in this domain as more and more devices get connected.

The paper begins by outlining the various layers of the Internet of Things architecture, including the perception, network, and application layers, and describing the significance of each layer in achieving functionality and communication between smart objects. The researchers stress that each of these layers is susceptible to exploitation if it is not adequately safeguarded. This is one of the paper's key contributions: identifying the fundamental security requirements of an IoT system as its availability, confidentiality, integrity, and

authentication. Because most devices are constrained by limited processing capabilities and energy, the authors emphasize that conventional security methods are often inappropriate for IoT environments [13].

While discussing the emerging healthcare, Sudeep Tanwar and Jigna Jhaveri Hathaliya define healthcare 4.0. They noted that it is the employment of IoT in modern-day medical systems. They claim, thus, the adoption of smart devices in healthcare, like wearable sensors, cloud-based platforms, and remote monitoring equipment, opened new strategies to improving patient care but has also brought in challenges of severe security and privacy threats [15].

Hathaliya and Tanwar outline the main dangers, which include identity theft, device manipulation, unauthorized access, and data leaks [15]. The need for protective measures increases due to the sensitive nature of medical data, which is often sought after. The study also examines various countermeasures and solutions that have been suggested, such as encryption techniques, secure data repositories, and more recent developments like blockchain and artificial intelligence. The ability of these solutions to safeguard health-related data without compromising system efficiency is evaluated.

IV. COMPARATIVE STUDY OF IoT SECURITY IN THE SMART DEVICES ERA

Internet of Things (IoT) security has become more important than ever as smart devices, such as wearable health trackers, connected cars, and smart home appliances, become more and more integrated into our daily lives. Many researchers have analysed this issue from a variety of angles and providing the possible solutions ranging from network architecture to cryptography to artificial intelligence. This study compares some of these notable approaches, highlighting how each tackles the growing threats in IoT systems.

A. Adapting to Context: Smart Home Security

The work on the security system by Khanpara et al. [16] enforces the idea that the system reacts to the way and timing in which the devices are utilized. For example, the system can notify about a device if it is generally used in the day and later in the night it starts to show activities. This way the approach is more personalized and proactive. It finds a special application in smart homes while not so much in the areas where the usage pattern is not easily predicted.

B. Using Artificial Intelligence to Detect Threats

Mazhar and his team [11] examined the use of AI - machine learning, in particular, - to identify threats as they happen. The main idea is that computers could get better at stopping the attack even before it occurs due to unexpected activities, e.g., an abrupt increase in data volume. It is useful to spot any unexpected or unexplainable actions, though it requires frequent updates and efficient training data to be consistent..

C. Preparing for the Future: Quantum-Resistant Security

Kumar, Ottaviani, Gill, and Buyya [17] focused on the future risks of quantum computing—which, they argue, could break existing encryption techniques. They suggest moving toward post-quantum cryptography—encryption that can withstand quantum attacks. Sounds like a promising idea, but it's still very early in development, and may be too heavy for small IoT devices at this point.

D. Protecting Health Data in Smart Hospitals

In the field of healthcare, Hathaliya and Tanwar [15] demonstrated how IoT can expose sensitive medical data. And they called for privacy advances — such as secure data sharing and encryption, and perhaps even blockchain technology — to be bolstered against such threats. Their work is especially pertinent as the use of these “remote monitoring” devices continues to grow, but deploying these solutions across old, fragmented systems can be complicated.

E. SDN and Machine Learning Integration

Restuccia, D'Oro, and Melodia [14] introduced an unified solution with software defined networking (SDN) in combination with machine learning to achieve centralized control for networks and threat detection on-the-fly. This fusion builds a supple security structure that keeps up with emerging threats. But is based on the centralized controllers, which might be a single failure point.

V. CONCLUSION

In this present time and age, smart devices like smartwatches, smart TVs, home assistants, and smart refrigerators have become common accreditable additions to our daily existence. As all of these gadgets

communicate via the internet, it becomes pertinent that they are protected against cyber threats. Otherwise, an unsuspecting person can easily be endowed with sensitive data, invade privacy, or defraud the gadget through malware installation. Smart devices are supposed to be easing our lives and at performing tasks efficiently, whether they be home assistants, fitness trackers, or medical devices and factory machinery. However, if not well-protected, these smart devices can pose huge threats, as hackers can try to either attack these devices or steal data from them.

The first major problem with IoT devices is that the vast majority are not built to be extremely secure. Their hardware is typically primitive, making it difficult to tack on aggressive security measures, as you would on a regular computer. AND on top of all that, they're all manufactured differently by different companies who don't have to follow the same rules or standards. This lack of consistency makes it easier for hackers to find weak spots and break into the system. We need to bring a blend of clever solutions — for example deploying artificial intelligence to identify threats, smarter encryption that doesn't just store the key under the doormat, and “smart” systems that can behave in flexible ways that are nevertheless predictable to people. There should be firm rules, globally, that any company that's making an IoT device must learn the best practices and follow some rules to make sure these products are going to be secure and they're not something I'm going to be shooting at during the zombie apocalypse.

Securing IoT devices is never going to be the job of just one person. There is a role for everyone — the workers who make the devices, the people who study or strive to improve security, the government and even you. All of those people working together, and staying vigilant about new threats to cyberspace, and we're going to be capable of creating a safer and smarter and more connected world.

REFERENCES

- [1] IoT Analytics. "State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally." IoT Analytics, 2024.
- [2] SentinelOne. "Top 10 IoT Security Risks and How to Mitigate Them." SentinelOne, November 5, 2024.
- [3] S. Millar, 'IoT Security Challenges and Mitigations: An Introduction', ArXiv, vol. abs/2112.14618, 2021.
- [4] Jurcut, A., Niculcea, T., Ranaweera, P. et al. Security Considerations for Internet of Things: A Survey. SN COMPUT. SCI. 1, 193 (2020) <https://doi.org/10.1007/s42979-020-00201-3>.
- [5] Syeda Manjia Tahsien, Hadis Karimipour, Petros Spachos, Machine learning based solutions for security of Internet of Things (IoT): A survey, Journal of Network and Computer Applications, Volume 161, 2020, 102630, ISSN 1084-8045, <https://doi.org/10.1016/j.jnca.2020.102630>.
- [6] A., Sharma, V., Ghosh, S., Karar, V., Lee, K., & Choi, C. (2020). Threats and Corrective Measures for IoT Security with Observance of Cybercrime: A Survey. <https://doi.org/10.1155/2021/5579148>.
- [7] Singh, N, R Buyya, and H Kim. 2025. 'Securing Cloud-Based Internet of Things: Challenges and Mitigations'. Sensors 25 (1). <https://doi.org/10.3390/s25010079>.
- [8] "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures" by Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan.
- [9] R. Shrivastav, "Securing Internet of Things (IoT) Devices: Challenges and Solutions," International Journal for Research in Robotics & Technology, vol. 3, no. 1, pp. 26–30, Jan–Mar 2024.
- [10] Tinashe Magara and Yousheng Zhou, Internet of Things (IoT) of Smart Homes: Privacy and Security, Journal of Electrical and Computer Engineering, 2024, <https://doi.org/10.1155/2024/7716956>
- [11] T. Mazhar, A. Khan, and M. Raza, "Deep Learning Approaches for Real-Time IoT Threat Detection," International Journal of Computer Applications, vol. 185, no. 7, pp. 12–18, 2023.
- [12] Conti, Mauro & Dehghantanha, Ali & Franke, Katrin & Watson, Steve. (2017). Internet of Things Security and Forensics: Challenges and Opportunities. Future Generation Computer Systems.
- [13] Ahmid, Maroua & Kazar, Okba. (2021). A Comprehensive review of the Internet of Things Security. Journal of Applied Security Research.
- [14] F.Restuccia, S. D'Oro and T. Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," in IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4829-4842, Dec. 2018.
- [15] Hathaliya, Jigna & Tanwar, Sudeep. (2020). An Exhaustive Survey on Security and Privacy Issues in Healthcare 4.0. Computer Communications.
- [16] P. Khanpara, K. Lavingia, R. Trivedi, S. Tanwar, A. Verma, and R. Sharma, "A Context-Aware Internet of Things-Driven Security Scheme for Smart Homes," Security and Privacy, Sep. 2022. <https://doi.org/10.1002/spy2.269>
- [17] A. Kumar, C. Ottaviani, S.S. Gill, and R. Buyya, 'Securing the future internet of things with post-quantum cryptography' SECURITY AND PRIVACY, vol. 5, no. 2, Dec. 2021.
- [18] Chowdhury S, Covic A, Acharya RY, Dupee S, Ganji F, Forte D. Physical security in the post-quantum era: a survey on side-channel analysis, random number generators, and physically unclonable functions.
- [19] Bisheh-Niasar M, Azarderakhsh R, Mozaffari- Ketmani M. High-speed NTT-based polynomial multiplication accelerator for CRYSTALS-Kyber post-quantum cryptography. Cryptol ePrint Arch Tech Reo. 2021; 563: 2021.

- [20] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network intrusion detection for IoT security based on learning techniques", IEEE Communications Surveys & Tutorials 2019.
- [21] C. Vorakulpipat, E. Rattanalerdnusrorn, P. Thaenkaew and H. D. Hai, "Recent challenges trends and concerns related to IoT security: An evolutionary study", 2018 20th International Conference on Advanced Communication Technology (ICACT), pp. 405-410, 2018.
- [22] S. Ganti, R. K. Vankayalapati, P. Krishnamoorthy, P. S. Thakare, U. A. Nayak and P. Vignesh, "Enhancing IoT-Driven Smart Home Security and Automation with a GCN Model," 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2025.