STM JOURNALS

International Journal of
Information Security Engineering

Volume 1, Issue 2, 2023
July—December
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Review IJISE

IoT Security: Issues, the Best Practices and OpenChallenges

Srikanta Kolay[1,*], Tryambak Hiwarkar[2]

Abstract

The Internet of Things (IoT) provides the facility toconnect different devices and communicate and share information over the internet. The Internet of Things (IoT) has emerged as a transformative and pervasive technological paradigm, revolutionizing how we interact with our environment and infusing intelligence into everyday objects and devices. This interconnected ecosystem has unleashed a wave of innovative applications across diverse domains, including healthcare, transportation, agriculture, industrial automation, and smart cities. However, as the IoT footprint expands rapidly, it also brings to the forefront a multitude of complex and pressing security challenges that demand immediate attention and resolution. One of the primary security concerns in the IoT ecosystem is weak authentication and authorization mechanisms. Insufficient encryption measures can lead to data interception and manipulation, exposing confidential information to potential attackers. The lack of automated update mechanisms leaves numerous IoT devices susceptible to known exploits, necessitating the establishment of efficient update processes. With IoT devices deployed in the physical world, they become susceptible to tampering and theft, requiring robust physical security measures to safeguard their integrity. Standardization of security practices across the diverse IoT ecosystem is necessary to establish a unified and robust security framework. Security awareness and education are critical to empowering users and manufacturers to implement secure practices effectively. By comprehensively understanding and actively mitigating the key security issues, adopting best practices, and collaboratively addressing open challenges, we can forge a safer and more resilient IoT landscape that not only fosters innovation but also preserves user privacy and instills confidence in the trustworthiness of IoT technologies. This paper centers on addressing IoT security concerns and exploring the optimal practices to mitigate them. Finally, we point out open challenges as a scope of future research.

Keywords: IoT, IoT security, data security, data privacy, IoT ecosystem, security challenge, IoT devices

***Author for Correspondence**
Srikanta Kolay
E-mail: kolaysrikanta@gmail.com

[1]Research Scholar, Department of Computer Science & Engineering, Sardar Patel University Balaghat, MP, India
[2]Professor & Dean, Department of Computer Science & Engineering, Sardar Patel University Balaghat, MP, India

Received Date: July 20, 2023
Accepted Date: October 10, 2023
Published Date: October 30, 2023

Citation: Srikanta Kolay, Tryambak Hiwarkar. IoT Security: Issues, the Best Practices and Open Challenges. International Journal of Information Security Engineering. 2023; 1(2): 8–15p.

INTRODUCTION

Internet of Things is a collection of "Things" connected via internet [1]. The adoption of the Internet of Things (IoT) is experiencing rapid expansion in tandem with the significant rise of smart devices. However, at the same time, increasing security concerns in IoT framework can make many customers afraid of using IoT devices. By following the best practices one can avoid most of the security risks. Still there are open challenges to secure fully the IoT devices [2].

LITERATURE REVIEW

The Internet of Things (IoT) has transformed our interactions with the environment by facilitating

© STM Journals 2023. All Rights Reserved

device connectivity and internet-based information sharing. Nevertheless, the rapid growth of IoT introduces notable security hurdles, such as inadequate authentication, limited encryption, absence of automated updates, and physical susceptibilities. To tackle these problems, it is imperative to establish uniform security protocols, raise awareness, and enforce strong security measures. This paper is dedicated to examining IoT security issues, proposing strategies for mitigation, and identifying future research challenges. Our objective is to enhance IoT safety, safeguarding privacy and fostering trust in this groundbreaking technology.

IOT ARCHITECHTURE

A typical 5-layer IoT architecture is shown in Figure 1 below.

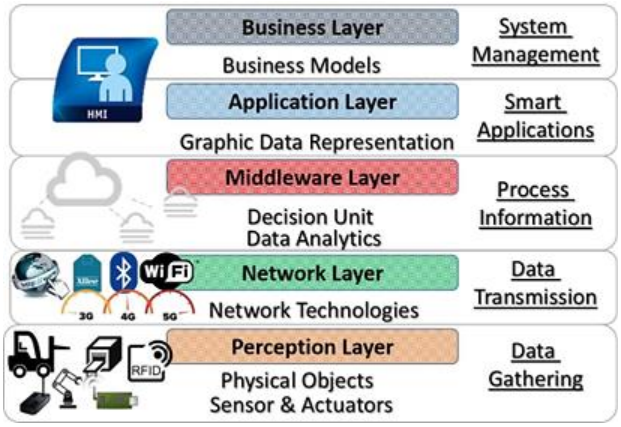

Figure 1. A typical 5-layer IoT Architecture.

Perception Layer

This layer represents the foundational level of the IoT architecture, housing the physical devices or sensors. These devices are tasked with gathering data from their surrounding environment and can encompass a wide range of sensors, including temperature sensors, humidity sensors, motion detectors, cameras, etc. The data collected by these devices is in its raw and unprocessed state.

Network Layer

The network layer functions as the fundamental support of the IoT infrastructure. Its main purpose is to facilitate communication between the devices/sensors in the Perception Layer and the higher layers of the architecture. This layer can use various communication protocols such as Wi-Fi, Bluetooth, Zigbee, cellular networks, LoRaWAN, etc., depending on the requirements of the IoT deployment. The data from the Perception Layer is transmitted through this layer to the next higher layer for processing.

Middleware Layer

The middleware layer functions as an intermediary between the lower layers (Perception and Network) and the upper layers (Application and Business) of the IoT architecture, effectively bridging the communication between them. It provides services and functionalities that facilitate communication, data management, and interoperability. This layer handles tasks like data transformation, protocol translation, device management, and security. Middleware plays a crucial role in ensuring that different devices and platforms can work together seamlessly in an IoT ecosystem.

Application Layer

The application layer is the interface through which end-users interact with the IoT system. It includes user-facing applications that provide various services, functionalities, and data visualization. These applications can be web-based dashboards, mobile apps, or desktop software. Users can monitor and control IoT devices, access data insights, and interact with the IoT system through the applications developed for this layer.

© STM Journals 2023. All Rights Reserved

Business Layer

Business layers use the data for making flowcharts, graphs,The business layer is the topmost layer of the IoT architecture and focuses on the business logic and decision-making processes. It deals with data analysis, data-driven insights, and making informed decisions based on the data collected from the lower layers. This layer may encompass machine learning algorithms, artificial intelligence, data analytics, and other tools aimed at extracting valuable insights from the extensive volumes of data generated by the IoT system. It helps in optimizing processes, improving efficiency, and enabling data-driven innovations.

IOT SECURITY

IoT is now being used in various industries like healthcare,wearables, smart cities, smart factories, smart logistics, home automation, logistics and many other industries. Based on the requirement different types of smart devices are used in different IoT systems.

Unfortunately, IoT has the most significant securityvulnerabilities that are impacting consumers. IoT devices provide a wide accessible surface to attack [3]. So, IoT security is a big concern and IT engineers must focus not only on the functionality of the device but also on the protections of devices from security aspect [4].

SECURITY ISSUES

The widespread adoption of the Internet of Things (IoT) has ushered in a new era of connectivity and convenience, empowering individuals and businesses with smart devices and systems that communicate and automate tasks seamlessly. However, this interconnectedness has not come without its share of challenges, particularly concerning IoT security. The following elaboration delves into the primary issues that pose significant threats to the security of IoT ecosystems [5]:

Weak Authentication and Authorization

One of the most pervasive issues in IoT security is the prevalence of weak authentication and authorization mechanisms. Numerous IoT devices are shipped with default or easily guessable login credentials, rendering them susceptible to brute-force attacks and unauthorized access. When attackers can effortlessly gain entry to an IoT device, they may exploit its functionalities or use it as a steppingstone to launch attacks on other devices or the broader network [6].

Inadequate Encryption

IoT devices continuously gather and transmit massive volumes of data, encompassing sensitive information like personal identifiers, health data, and financial records. Inadequate encryption during data transmission or storage leaves this information susceptible to interception and tampering. Unencrypted data can be intercepted by malicious actors, leading to privacy violations, identity theft, and unauthorized access to critical systems [7].

Lack of Device Updates and Patch Management

Many IoT devices suffer from poor or non-existent update and patch management practices. Software vulnerabilities are continually discovered, and regular updates are necessary to address these vulnerabilities and strengthen the device's security. Nevertheless, attaining timely and automated updates in IoT ecosystems can be challenging due to their inherent complexity. Consequently, many devices remain unpatched and vulnerable, providing a lucrative target for cybercriminals [8].

Privacy Concerns

IoT devices often collect sensitive user data to provide personalized services and automation.

Nonetheless, mishandling or unauthorized access to this data can result in substantial privacy issues. Whether through data breaches or improper data sharing practices, compromised privacy can lead to a loss of user trust and raise ethical questions about data ownership and consent [9].

© STM Journals 2023. All Rights Reserved

Physical Security Challenges

IoT devices deployed in the physical world face unique physical security challenges. Physical tampering, theft, and destruction of these devices can have severe consequences. For example, compromised smart home devices may expose residents to physical threats, while compromised industrial IoT devices may lead to costly production disruptions [10].

Supply Chain Vulnerabilities

The IoT supply chain involves multiple entities, from manufacturers to distributors and service providers. Each point in the supply chain introduces potential vulnerabilities that malicious actors can exploit to compromise devices before they even reach end-users. An insecure supply chain can lead to widespread security breaches and undermine the trustworthiness of IoT devices.

Interoperability Issues

IoT devices and systems frequently originate from diverse manufacturers, each adhering to their own set of protocols and standards. The lack of standardized communication protocols and interoperability can create security gaps and complexities when integrating devices into a cohesive IoT ecosystem. These gaps may be exploited by attackers to compromise the overall system.

BEST PRACTICES

As the Internet of Things (IoT) continues to expand and integrate into various aspects of our lives, ensuring robust security practices becomes paramount to safeguarding sensitive data and mitigating potential threats. The following elaboration delves into the best practices that can enhance the security of IoT systems [11]:

Strong Authentication and Authorization

Implementing strong authentication mechanisms is the foundation of IoT security. Devices should utilize secure login credentials, such as unique usernames and strong passwords, to prevent unauthorized access. Multi-factor authentication (MFA), combining something a user knows (password) with something they possess (smartphone token), adds an extra layer of protection. Additionally, proper authorization protocols ensure that users and devices have limited access only to the resources they need, reducing the risk of privilege escalation.

End-to-End Encryption

To protect data during transmission and storage, robust encryption protocols must be adopted. End-to-end encryption guarantees that data is encrypted at its source and remains encrypted throughout its transmission until it reaches its designated destination. This prevents eavesdropping and tampering by unauthorized entities, guaranteeing data confidentiality and integrity.

Regular Software Update

Keeping the IoT devices and their associated software up to date is of utmost importance to address known vulnerabilities and enhance security. Manufacturers should provide automated and timely updates to patch any security flaws that might be discovered after the device's deployment. Additionally, users should be educated and encouraged to apply updates promptly to maintain the security of their IoT devices [12].

Privacy by Design

Incorporating a privacy-by-design approach ensures that privacy considerations are embedded into the entire development lifecycle of IoT devices and services. This includes data minimization, where only necessary data is collected, and anonymization or pseudonymization of data to protect user identities. Implementing privacy by design principles helps avoid privacy violations and builds trust with users.

© STM Journals 2023. All Rights Reserved

Physical Security Measures

For IoT devices deployed in the physical world, physical security is crucial. Devices should incorporate tamper-resistant hardware and secure enclosures to protect against physical attacks and unauthorized access. Moreover, secure boot processes ensure that the device's software is authentic and untampered during startup.

Secure Supply Chain

Collaboration with suppliers and partners is essential to ensuring a secure IoT supply chain. Manufacturers should conduct thorough security assessments during the procurement process to identify and mitigate potential risks in the supply chain. Regular audits and evaluations of suppliers can help maintain the integrity of IoT devices throughout their lifecycle.

Security Monitoring and Incident Response

The implementation of comprehensive security monitoring is vital for real-time detection and response to potential threats. Employing intrusion detection systems, anomaly detection, and behavior analytics aids in identifying suspicious activities. Furthermore, having a well-defined incident response plan in place ensures that security breaches are swiftly addressed, minimizing potential damage.

User Education and Awareness

It is essential to educate users about IoT security best practices. Users should be informed about the importance of strong passwords, regular updates, and the potential risks associated with IoT devices. Raising awareness about phishing attacks and social engineering can also help users recognize and avoid potential security threats.

Standardization and Certification

Encouraging standardization of IoT security practices and obtaining third-party security certifications can provide a level of confidence in the security of IoT devices. Compliance with recognized security standards and obtaining industry certifications demonstrates a commitment to security and quality.

OPEN CHALLENGES

Guaranteeing security and privacy in the architecture of the Internet of Things (IoT) is a multifaceted and continually evolving undertaking. Numerous unresolved challenges persist in this domain, necessitating continuous research, collaboration, and innovation. The following are key open challenges in IoT architecture for ensuring security and privacy [13]:

Interoperability and Standardization

The diversity of IoT devices, platforms, and communication protocols hampers seamless integration and poses security risks. Lack of standardized security mechanisms and protocols can lead to inconsistencies in security implementations across different IoT components. Achieving interoperability and establishing robust security standards that apply universally is crucial for a cohesive and secure IoT ecosystem.

Scalability and Complexity

As the number of IoT devices and data streams grows exponentially, scaling security measures becomes increasingly complex [14]. Traditional security solutions may struggle to cope with the sheer volume of data and the dynamic nature of IoT environments. Developing scalable and adaptive security architectures that can efficiently manage the vast IoT landscape remains a significant challenge.

Device Heterogeneity

IoT encompasses a wide range of devices with varying capabilities and resource constraints. Securing resource-constrained devices, such as sensors and actuators, while maintaining their functionality is a

© STM Journals 2023. All Rights Reserved

challenge. Addressing the security needs of heterogeneous devices requires tailored security solutions that can accommodate diverse architectures.

Security in Edge Computing

Edge computing, which processes data closer to the source, introduces new security challenges. The distributed nature of edge computing may expose devices to different threat landscapes, necessitating robust security mechanisms for edge nodes and communication channels. Ensuring secure data transmission and processing at the edge is essential to protect sensitive information [15].

Data Privacy and Ownership

IoT devices frequently gather extensive quantities of personal and sensitive data. Determining data ownership, defining data usage policies, and ensuring user consent for data collection and processing pose significant privacy challenges. Respecting data privacy rights and implementing privacy-enhancing technologies while maintaining data utility remains a delicate balance.

Security Updates and Patch Management

Ensuring that IoT devices are regularly updated with the latest security patches is crucial for mitigating vulnerabilities. However, IoT devices often lack automated update mechanisms, making it challenging to deliver timely security updates. Ensuring a robust and secure update mechanism that does not disrupt device operations is essential.

Security by Design

Implementing security measures at the early stages of IoT device and system development is crucial. However, security considerations are often an afterthought, leading to poorly secured IoT solutions. Integrating security by design principles from the outset of development can help prevent security vulnerabilities and privacy breaches.

Security Monitoring and Threat Intelligence

Detecting and responding to security threats in real-time is challenging in large-scale IoT deployments. IoT architectures must incorporate effective security monitoring and threat intelligence systems to identify and mitigate potential threats promptly.

Trust and Identity Management

Establishing trust among IoT devices and ensuring secure identity management is vital to prevent unauthorized access and malicious activities. Managing device identities, access control, and device authentication in a scalable and secure manner is an ongoing challenge.

Legacy Device Security

Existing IoT deployments often include legacy devices that may lack modern security features or be incompatible with newer security solutions. Ensuring the security of legacy devices and integrating them into a secure IoT architecture requires careful consideration and retrofitting of security measures.

Resolving these open challenges in IoT architecture necessitates collaboration among industry stakeholders, researchers, and policymakers. Emphasizing security and privacy throughout the entire IoT ecosystem's lifecycle, from device design to data management, is essential to building a trustworthy and secure IoT landscape. By proactively addressing these challenges, the IoT community can pave the way for a more resilient, secure, and privacy preserving IoT future.

CONCLUSION

The Internet of Things (IoT) has caused a paradigm shift in the way we engage with technology, delivering unparalleled convenience and efficiency across various facets of everyday life. Nonetheless,

© STM Journals 2023. All Rights Reserved

with the continuous expansion of the IoT ecosystem, numerous security challenges arise that require prompt attention and proactive measures. This paper has provided a comprehensive exploration of IoT security, encompassing the critical issues, best practices, and open challenges that define the current state of IoT security.

The analysis of IoT security issues revealed vulnerabilities such as weak authentication, inadequate encryption, and the absence of regular updates, which can expose devices to potential cyberattacks and data breaches. Privacy emerged as a paramount concern, as the collection of vast amounts of personal data demands robust privacy-by-design principles to protect user information and trust.

The incorporation of best practices offered valuable guidelines to bolster IoT security. From implementing strong authentication and end-to-end encryption to advocating regular software updates and user education, these practices lay the groundwork for establishing a more secure and resilient IoT ecosystem. Physical security measures, supply chain scrutiny, and government regulations further reinforce the security posture of IoT devices and networks.

Despite the progress made in addressing IoT security challenges, several open challenges persist. Standardization, resource limitations, and the integration of AI and ML technologies present ongoing hurdles that require innovative solutions. Ensuring security and privacy in edge computing, handling data ownership and privacy rights, and managing updates for legacy devices remain critical areas that demand attention and expertise.

REFERENCES

1. Kolay S, Hiwarkar T. Evaluation Of The Privacy-Protecting Effects Of Learning-Based Iot Ecosystem Behavior. Journal of Data Acquisition and Processing. 2022;37(5):1873–1883.
2. Yang Y, Wu L, Yin G, Li L, Zhao H. A survey on security and privacy issues in Internet-of-Things. IEEE Internet of things Journal. 2017 Apr 17;4(5):1250–1258.
3. Lin J, Yu W, Zhang N, Yang X, Zhang H, Zhao W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE internet of things journal. 2017 Mar 15;4(5):1125–1142.
4. Rajmohan T, Nguyen PH, Ferry N. A decade of research on patterns and architectures for IoT security. Cybersecurity. 2022 Dec;5:1–29.
5. Moinuddin K, Srikantha N, Lokesh KS, Narayana A. A survey on secure communication protocols for IoT systems. Int. J. Eng. Comput. Sci. 2017 Jul;6(6).
6. Ferrag MA, Maglaras LA, Janicke H, Jiang J, Shu L. Authentication protocols for internet of things: a comprehensive survey. Security and Communication Networks. 2017 Nov 6;2017.
7. Fremantle P, Scott P. A survey of secure middleware for the Internet of Things. PeerJ Computer Science. 2017 May 8;3:e114.
8. Srivastava A, Gupta S, Quamara M, Chaudhary P, Aski VJ. Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. International Journal of Communication Systems. 2020 Aug;33(12):e4443.
9. Verma V, Bhatia M. Analysis of Security Measures on the Internet of Things based Applications. In 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC) 2022 Oct 20 (pp. 526–534). IEEE.
10. da Cunha V, Carvalho V, Machado J, Soares F. Industrial Networks Protocols PROFIBUS and RS485–A Description of the Most Common Problems. InInternational Conference on Reliable Systems Engineering 2022 Aug 26 (pp. 367–374). Cham: Springer International Publishing.
11. Koul N, Kumar N, Sayeed A, Verma C, Raboca MS. Data exchange techniques for internet of robotic things: Recent developments. IEEE Access. 2022 Sep 26.
12. Liu Y, Yu W, Rahayu W, Dillon T. An Evaluative Study on IoT ecosystem for Smart Predictive Maintenance (IoT-SPM) in Manufacturing: Multi-view Requirements and Data Quality. IEEE Internet of Things Journal. 2023 Feb 22.

© STM Journals 2023. All Rights Reserved

13. Zhou J, Cao Z, Dong X, Vasilakos AV. Security and privacy for cloud-based IoT: Challenges. IEEE Communications Magazine. 2017 Jan 19;55(1):26–33.
14. Sharbaf MS. IoT Driving New Business Model, and IoT Security, Privacy, and Awareness Challenges. In2022 IEEE 8th World Forum on Internet of Things (WF-IoT) 2022 Oct 26 (pp. 1–4). IEEE.
15. Samaila MG, Neto M, Fernandes DA, Freire MM, Inácio PR. Challenges of securing Internet of Things devices: A survey. Security and Privacy. 2018 Mar;1(2):e20.

© STM Journals 2023. All Rights Reserved