STM JOURNALS

International Journal of
Radio Frequency Innovations

Volume 3, Issue 1, 2025
January–June
DOI (Journal): 10.37591/IJRFI

https://journals.stmjournals.com/ijrfi

Review IJRFI

A Study on Security Requirements of IOT

Jeetendra Singh Yadav[1,*], Tripti Arjariya[1], Ateek Mansoori[2]

Abstract

In terms of speed, internet technologies have surpassed traditional technologies. Although the Internet's explosive growth has allowed it to reach its full potential, there are several security dangers associated with it. Many consumer-grade IoT devices are not designed with robust authentication protocols, making them easy targets for hackers. To address this, stronger multi-factor authentication (MFA) methods and certificate-based authentication should be implemented to ensure that only legitimate devices gain access to sensitive systems. Connecting objects and systems is more important than ever thanks to the growing Internet of Things, or IoT. The area that was concerned with the devices and systems that were connected to the biological system was the security of the Internet of Things. The Internet of Things (IoT) has significantly transformed industries by connecting billions of devices, creating a more intelligent and automated world. However, as IoT systems continue to grow, they introduce several security vulnerabilities that need to be addressed to ensure the safety of sensitive data and devices. One of the primary concerns is data security, as IoT devices constantly collect and transmit vast amounts of sensitive information, such as health metrics, location data, and personal preferences. If these data streams are not encrypted or properly secured, they are vulnerable to interception and manipulation by malicious actors, which could lead to privacy breaches or even system compromises. In addition to data security, device authentication and access control are critical in preventing unauthorized devices from joining IoT networks. Another significant challenge is communication security. IoT devices often communicate over wireless networks, which are inherently susceptible to interception. Without the use of secure communication protocols like TLS/SSL, attackers could eavesdrop on or alter the data being transmitted, compromising the integrity of the system. Insecure channels could also allow attackers to inject malicious commands into the system, potentially causing serious disruptions. Physical security also remains a concern, especially when IoT devices are deployed in environments where physical access cannot be controlled. Devices that are exposed to tampering or theft can be manipulated, leading to breaches. To counter this, tamper-resistant hardware, secure boot processes, and hardware-based encryption can prevent unauthorized physical access to devices and ensure that the data they collect remains safe. Basic dangers, such as those pertaining to data security, persist despite IoT's enormous contributions to technology and society. Things (in the processing devices and integrated systems of the Internet of Things ecosystem) can now collect, send, and receive data via network connection thanks to a unique identification. An overview of IoT security characteristics is given in this study. RFID technologies, security architecture and protocol, WSN integration, and RFID technologies to address security concerns.

***Author for Correspondence**
Jeetendra Singh Yadav
E-mail: jeetendra2201@gmail.com

[1]Associate Professor, Department of Computer Science and Engineering, Bhabha University, Bhopal, Madhya Pradesh, India
[2]Associate Professor, Department of Electrical and Electronics Engineering, Bhabha University, Bhopal, Madhya Pradesh, India

Received Date: March 05, 2025
Accepted Date: March 29, 2025
Published Date: April 07, 2025

Citation: Jeetendra Singh Yadav, Tripti Arjariya, Ateek Mansoori. A Study on Security Requirements of IOT. International Journal of Radio Frequency Innovations. 2025; 3(1): 24–28p.

Keywords: Security, IOT, RFID, challenge, Multi-factor authentication (MFA)

INTRODUCTION

In 1998, the phrase "internet of things" (IoT) was first used to describe uniquely identifiable items, things, and their virtual representations in a structure akin to the internet. Smart electric meter readings, greenhouse monitoring, telemedicine

monitoring, and intelligent transportation are just a few examples of the representative applications that have helped the Internet of Things gain significant traction in recent years. Sensing, information processing, applications and services, heterogeneous access, and extra components like security and privacy are typically the four main parts of the Internet of Things.

IoT is now a well-known buzzword, and as a result, new industry applications will emerge, such as machine-to-machine (M2M) communications, cyber-transportation systems (CTS), and cyber-physical systems (CPS) [1].

In 1998, the term "Internet of Things" (IoT) was first proposed to describe easily identifiable objects, things, and things with an Internet-like structure [2]. The Internet of Things (IoT) concept has gained significant popularity in recent years due to a few representative applications (e.g., intelligent transportation, telemedicine monitoring, and intelligent greenhouse monitoring while reading electricity meters). The four primary components of the Internet of Things are typically acquisition, heterogeneous access, information processing, applications, and services, along with supplementary elements like data security and protection.

The Internet of Things is a popular catchphrase these days. The following IoT-related industrial applications will surface, such as machine-to-machine communication (M2M), cyber-physics systems (CPS), and cybernetic transport systems (CTS) [3].

At the very outset, regarding the aspect of security, IoT will become one area where serious problems will arise challenges. The reason of its occurrence are as follows:

- The IoT extends the "internet" through traditional internet, mobile networks, sensor networks, etc.
- The actuators of all things are connected to the "internet".
- The "things" will communicate with each other. Thus, the new security and privacy problems are going to arise. We must spend more time and effort researching those issues related to the confidentiality, authenticity and integrity of data in the IoT field.

LITERATURE REVIEW

Jayakumar *et al*. proposed a strategy for achieving a safe state in the Internet of Things in terms of RFID innovations [4]. They used RFID technology to protect and secure data. While considering a situation involving RFID in a safe state using IOT; to accomplish this, each item is assigned a unique item code (UPC). The Electronic Product Code (EPC), which underpins MIT's automatic focus ID, has the potential to replace the UPC. Each glossy label would include the article's manufacturer, name, a 40-bit serial number, and 96-bit data. Scarfskin's correspondence was handled by a system known as the Object Naming Service. The item data can be restored from this database and displayed immediately on the manufacturer's computers. They proposed a "murder password" and an "access password" to ensure data validation, classification, and reliability at various levels of correspondence.

IoT security was examined by Abomasa [5] in light of digital security threats, vulnerabilities, filters, and attacks. This document's primary goal was to distinguish between the various kinds of gatecrashers that pose security threats to the Internet of Things. Single attacks, coordinated protests, and inspection offices are examples of intruders. Every situation would require a different combination of expertise, capital grants, inspiration, and risk tolerance. By observing and recording all of the hazards and a few characters on the screen, it was easier to determine which frailties could be exploited. IoT hackers typically possessed complete DY filter functionality, despite a few minor physical compromises. Only a small percentage of all IoT devices would be vulnerable to physical bargain attacks in the worst circumstances. These issues should be coordinated by IoT engineering in order to identify these occurrences and outfit themselves with inexpensive devices. The hackers employed a variety of tactics, tools, and processes to exploit their weaknesses in a particular situation in order to accomplish their

objectives. In light of this, it is critical that an organization comprehends the attacker's goals and capabilities in order to prevent possible harm. Lastly, more research ought to lessen possible risks as well as their effects.

To support this new area, Suo *et al*. examined the development of IoT research and focused on security [6]. The safety requirements are revealed by a thorough examination of the architecture and safety features. Based on this, we go over the current status of research on important technologies like cryptographic algorithms, communications security, sensor data protection, and encryption mechanisms. We also briefly outline the difficulties.

Kumar *et al*. believed that the idea of the Internet of Things (IoT) allows billions of devices including sensors, smartphones, and other network devices, to be connected and communicate with one another [7]. The Internet of Things can be a system whereby the detector technology's integrated objects communicate with one another wirelessly to create, share, and transmit knowledge without the need for human interaction. In a number of ways, this connection is important, such as for prompt coordination with numerous basic devices like sensors, routers, thermostats, Fitbits, etc. These networks are extremely vulnerable to attacks because of their open and diverse nature. Thus, this technology's primary concerns are data security and protection [6]. The common IoT vulnerabilities covered in this paper include denial of service (DDoS) attacks and attacks against changes in background data. The study covers privacy and security concerns in a number of areas, including device connections, spam, web interface vulnerabilities, data storage problems, IoT network problems like Sybil attacks, cloud connectivity issues, industrial IoT attacks, IoT environment protection, and current defenses.

PROPOSED METHODOLOGY

Table 1 highlights the contributions of various researchers in the field of IoT security. It covers aspects such as authentication mechanisms, cyberattack classifications, encryption technologies, and common IoT vulnerabilities.

SECURITY REQUIREMENTS

As illustrated in Figure 1, we can compile the security requirements for every level based on the analysis above:

Perceptual Layer

To start, node authentication is necessary to stop unauthorized access to the node. Second, data encryption is necessary to ensure the confidentiality of information transferred between nodes, and deciding on a data encryption key beforehand is a crucial step.

Table 1. Summary of key research contributions on IoT security and cyberattack mitigation.

Author name	Contribution
Jaykumar *et al. [4]*	The "murder of secret words" and "passwords" at the different levels of correspondence were used to validate the information's sincerity and confidentiality.
Abomhara and Koien [5]	It primarily describes cyberattacks on Internet of Things devices. Individual attacks, organized groups, and secret services are the three main categories of intruders. The IoT architecture must be able to identify intruders in order to withstand cyberattacks.
Suo *et al.* [6]	Examine the state of important technologies, such as key encryption mechanisms, communication security, sensor data protection, and cryptographic algorithms, and briefly list the difficulties.
Kumar *et al. [7]*	Common IoT vulnerabilities like denial of service (DDoS) and attacks against changes in background data are the main focus. It covers a wide range of privacy and security topics, including device connections, spam, web interface vulnerabilities, cloud connectivity concerns, industrial IoT attacks, data storage issues, and IoT network problems like Sybil attacks.

The more resources required, the more robust the security measures. Light encryption technology, which includes the light encryption algorithm and protocol, becomes crucial in order to address this issue. Simultaneously, the authenticity and integrity of sensor data are turned into research objectives [7].

Network Layer

It is challenging to implement current communication security measures at this level. One kind of security mechanism that is necessary for preventing unauthorized nodes is identity authentication. Integrity and confidentiality are equally important. As a result, we must also establish a mechanism for data integrity and confidentiality. It is a particularly dangerous network attack technique that is frequently used on the Internet, along with the Distributed Denial of Service (DDoS) exploitation. Therefore, in order to protect the vulnerable node from a DDOS attack, another issue must be fixed at this level.

Support Layer

Cloud computing, secure multi-stakeholder processing, nearly all strong encryption algorithms and protocols, improved system security technology, and antivirus software are all necessary for this level of support.

Application Layer

Two components are required to address the application-level security issue. In a heterogeneous network, the first is key agreement and authentication; the second is user privacy protection. Additionally, management and education are crucial for information security, especially when it comes to password management [8].

All things considered, IoT security technology is crucial and fraught with difficulties. Furthermore, rules and laws are also crucial.

IOT SECURITY: DATA AUTHENTICATION

Despite using encryption to protect the data, one of the issues was data authentication. Security can be compromised if the data cannot be protected in an authentic way. Despite their complexity, authentication issues are definitely a security risk. It paid more attention to the information that was presented in the side attacks than to the actual content. Connecting devices was the IoT concept. Data communication security was not a top concern when developing such devices [9]. Devices with outdated operating systems and UN software patches are susceptible to hacker attacks. The corporate level was to be the starting point for the IOT security solution. Regular citizens and business owners need to be adequately trained to safeguard their IOT devices in order to lower security risks. The security issues with different technologies have been described in this study.

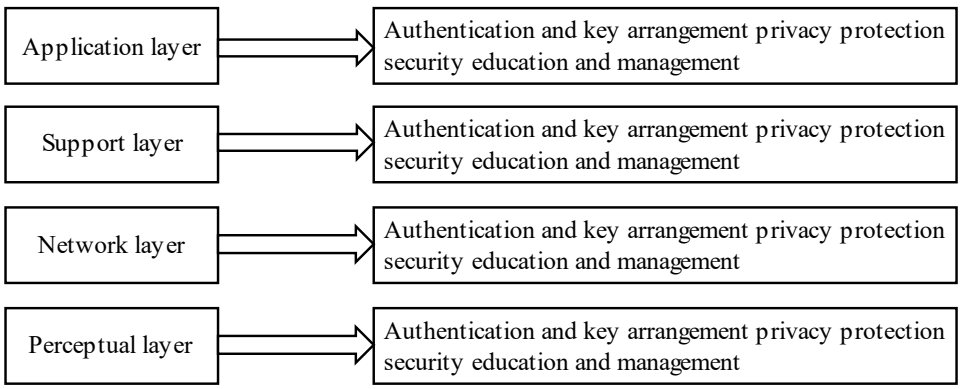

Figure 1. Security requirement of layer.

SECURITY ISSUES

It is not necessary to look at a technology's shortcomings before concentrating on its many advantages. Over the years, IoT development has slowed down because of inactive development and subpar improvements brought about by IoT security. Because of the various applications of IoT, the data encryption concept gathers a lot of data. The data was gathered and processed worldwide in the IoT environment. When data is accessible online, IoT security can be achieved through the use of SSL (Secure Socket Layer Protocol). A wireless protocol with built-in encryption was necessary, though, to use wireless data transmission [10].

CONCLUSION

IoT technology presents a number of opportunities and novel uses. But for privacy and security, this is crucial. The primary issues with security and data protection have been discussed in this study from a variety of perspectives, including RFID technology, algorithms, architecture, etc. Numerous algorithms and technologies are used to reduce security and privacy concerns, but they cannot be completely eliminated. This idea is still being researched. IoT will become a technological and social development boom after studies.

REFERENCES

1. Wan J, Yan H, Suo H, Li F. Advances in cyber-physical systems research. KSII Transactions on Internet and Information Systems (TIIS). 2011; 5(11): 1891–908.
2. Weber RRH. Internet of things – new security and privacy challenges. Comput Law Secur Rev. 2010; 26(1): 23–30.
3. Baheti R, Gill H. Cyber-physical systems. In: Samad T, Annaswamy A, editors. The Impact of Control Technology: Overview, Success Stories, and Research Challenges. Piscataway (NJ): IEEE Control Systems Society; 2011. p. 161–6.
4. Jaykumar J, Blessy A. Secure smart environment using IOT based on RFID. Int J Comput Sci Inf Technol. 2014; 5(2): 2493–2496.
5. Abomhara M. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J Cyber Secur Mobil. 2015; 4(1): 65–88.
6. Hui Suo, Jiafu Wan. Security in the Internet of Things: A Review. 2012 International Conference on Computer Science and Electronics Engineering. 2012; 648–651.
7. Nishant Kumar, Madhuri J. Review on security and privacy concerns in Internet of Things. International Conference on IoT and Application (ICIOT). 2017; 1–25.
8. Yang G, Xu J, Chen W, Qi ZH, Wang HY. Security characteristic and technology in the internet of things. Journal of Nanjing University of Posts and Telecommunications (Natural Science). 2010 Aug; 30(4): 20–29.
9. Mayer CP. Security and privacy challenges in the internet of things. Electron Commun EASST. 2009; 17: 1–12.
10. Ding C, Yang LJ, Wu M. Security architecture and key technologies for IoT/CPS. ZTE Communications. 2011 Feb; 17(1): 11–16.
11. Weber RH, Studer E. Cyber security ZTE Technology Journal, in the Internet of Things: Legal aspects. Comput Law Secur Rev. 2016; 32(5): 715–728.

