# A Review on Cybersecurity Challenges in IoT Devices

Deepa Barethiya; Chumban Bopche; Tushar Latesh Parate
Department of MCA, G H Raisoni College of Engineering and Management,
Nagpur, Maharashtra, India

**Abstract:**
The Internet of Things (IoT) is revolutionizing the manner in which devices interact, enabling smart environments in sectors such as healthcare, transportation, and power grids. However, this growing interconnectivity comes with serious cybersecurity challenges with the vast number of interconnected devices, limited computing resources, and lack of standardized security practices. This review addresses the most significant cybersecurity threats in IoT environments, particularly in critical infrastructures such as the smart grid, where device compromise can have catastrophic consequences.

The article covers threats such as weak authentication, insecure communication, lack of encryption, and limited device security. It also covers secured device manufacturing practices, hardware protection, and network-level controls. The article also includes a case study of web interface attacks to illustrate real-world threats. Since traditional security controls will be inadequate, the article emphasizes the importance of the use of newer methods such as machine learning and post-quantum cryptography to predict, detect, and counter threats.

In the future, the research urges developers, manufacturers, and researchers to collectively act with urgency to build scalable, secure IoT systems. With more widespread use of IoT, these cybersecurity issues need to be addressed in order to preserve the trust, reliability, and resilience of connected devices and critical services they deliver.

**Keywords:** Internet of Things (IoT), Cybersecurity, Smart Grid, IoT Security Challenges, Critical Infrastructure Protection.

## 1. Introduction:

According to IBM, Internet-connected devices are expected to outnumber human beings, and the evolution of connectivity is also expected to speed up so that in 2020 the number of connected devices will be around 50 billion [1]. The expanding Internet of Things (IoT) has made it possible to connect everything and anything to the internet. It has brought a digital disruption to the physical world by changing the way we engage with technology. With IoT, it is now possible to connect light bulbs, refrigerators, drones, pet feeders, sensors, smart TVs and digital set-top boxes, security cameras, wearables, automotive systems, and medical devices to the internet. Various industries—from healthcare to manufacturing, utilities, transport, and homes—have been transformed and are now more intelligent and efficient.

The term "IoT" was originally coined by Kevin Ashton, a British technology entrepreneur, in 1999. Ashton characterizes IoT as a network where the Internet is connected with the physical world using pervasive sensors [2],[3]. The Internet of Things can be termed as a network of physical things, vehicles, and domestic appliances [4], such as those that are components of smart city infrastructure. Such intelligent devices typically consist of embedded electronics, software, sensors, actuators, and connectivity features which enable them to collect, share, and react to information automatically or by means of human involvement.

But with the rapid growth of IoT devices also

DOI: https://doi.org/10.5281/zenodo.15496886

comes the enormous and complex surface area for cyber attacks. IoT devices differ from computing systems because, in most instances, they are deployed in uncontrolled or physically accessible environments, and thus they are particularly susceptible to a broad spectrum of cybersecurity threats. These include unauthorized access, data breaches, malware infection, DoS attacks, and hijacking of devices. The majority of IoT devices lack sufficient inbuilt security due to limited processing power, financial restrictions, or slothfulness in the manufacturing process. Also, heterogeneity and scale of IoT ecosystems pose challenges towards implementing standardized security measures across platforms and devices.

IOT security is not an option—it's a requirement. The more IoT moves into strategic infrastructure and the mundane aspects of life, any breach can have long-term consequences, from privacy infringement, financial gains, and bodily injury to even threatening human safety. This overview aims to examine the core cybersecurity concerns that accompany IoT devices, analyze existing mitigation strategies, and recommend future steps in securing the Internet of Things.

## 2. Literature Review:

The need for data-on-demand using sophisticated, intuitive queries continues to increase tremendously [2]. This has led to what most researchers refer to as the post-PC era, with intelligent devices and smartphones transforming human-environment interaction. In this dynamic setting, ordinary objects are becoming interactive and informative. Mark Weiser, in some cases described as the father of Ubiquitous Computing, defined this vision as a "smart environment in the physical world that is richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in everyday objects, and connected through a continuous network" [8].

Although these innovations have provided unparalleled convenience, automation, and efficiency, they have also presented a broad spectrum of cybersecurity threats. As IoT devices find their way into the fabric of everyday life and critical infrastructure, they offer a rich target for an adversary. The heterogeneity and scale in IoT ecosystems render it difficult to provide a one-size-fits-all security solution, leaving most devices vulnerable to attacks such as spoofing, eavesdropping, denial-of-service (DoS), and man-in-the-middle (MitM) intrusions[5].

Among the most significant IoT security issues is a lack of adequate end-to-end encryption and authentication procedures, especially on constrained devices. A majority of IoT deployments focus more on functionality and low costs at the expense of secure protocols. In addition, firmware updates are often overlooked, and vulnerabilities still exist even when exploits are no longer unknown. This practice of neglecting upkeep can lead to ongoing attack channels in critical systems[6].

Also, the majority of IoT systems operate in settings where physical security is not feasible, which means it is easier for devices to be hacked or accessed without permission. The absence of standardized security requirements and certifications among IoT device manufacturers makes the situation even more complex[7].

Together, here reviewed literature suggests that while IoT is a revolutionary technology, its accelerated growth undermines the existing security mechanisms. The consensus among experts is that immediate necessity is for lightweight cryptographic algorithms, secure communication protocols, device authentication methods, and regulatory level standardsexclusively for the IOT environment.

## 3. Methodology:

The methodology used for this review paper is a systematic review of published literature, industry case studies, and reported cybersecurity incidents involving IoT environments.

DOI: https://doi.org/10.5281/zenodo.15496886

This includes peer-reviewed research papers, vulnerability databases (e.g., CVE listings), and white papers from technology vendors. The evaluation framework aligns with conventional information security objectives—confidentiality, integrity, and availability (CIA)—and IoT-specific concerns such as scalability, heterogeneity, physical security, and device lifecycle management

The article categorizes and analyzes security concerns on different layers of the IoT ecosystem: hardware, firmware, communication protocols, network infrastructure, and web-based user interfaces. Particular emphasis is also placed on evaluating technological aspects of smart systems, using the example of massive IoT deployment such as Smart Grids.

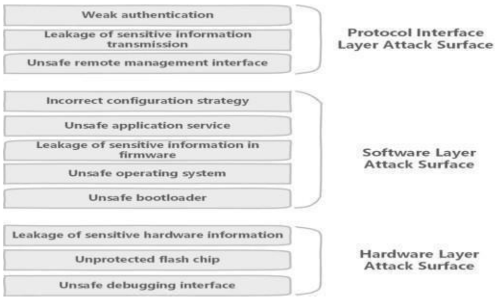
Weak authentication
Leakage of sensitive information transmission
Unsafe remote management interface
Protocol Interface Layer Attack Surface
Incorrect configuration strategy
Unsafe application service
Leakage of sensitive information in firmware
Unsafe operating system
Unsafe bootloader
Software Layer Attack Surface
Leakage of sensitive hardware information
Unprotected flash chip
Unsafe debugging interface
Hardware Layer Attack Surface

Fig. IoT Device Attack Surface Diagram

### 3.1 Components and Architecture of IOT:

IOT infrastructures typically consist of a wide variety of sensors and hardware devices that comprise Wireless Sensor Networks (WSNs), RFID tags, actuators, GPS modules, magnetometers, waspmote sensors, infrared and ultrasonic sensors, and embedded controllers and gateways. These devices are typically supplemented with silicon integrated circuits (ICs) and nano-electronic systems with the main objective of achieving miniaturization, low cost, and high performance.

### 3.2 Smart Grid as a Use Case:

Smart Grid (SG) represents one of the biggest-scale actual-world implementations of IoT technology. It involves several IoT devices—from power plants to household appliances—to enable dynamic energy management and two-way communication among consumers and providers [10][11].

Self-healing features: Smart grids are designed to reconfigure automatically in the event of natural disasters, blackouts, or cyber attacks. They can isolate faulted segments autonomously, re-route power, and prevent cascading failures.

Data-based energy management: Similar to data packets being delivered on the internet, smart grids deliver energy packets using routers and gateways to identify most cost-effective routes of transmission [11].

This real-world application provides valuable lessons regarding both benefits and limitations of large IoT networks.

### 3.3 Cybersecurity Controls in IoT:

In order to quantify the cybersecurity posture of IoT devices, we discuss a variety of technical techniques and best practices:

Hardware-based Security: IoT devices with Trusted Platform Modules (TPMs) or Hardware Security Modules (HSMs) can safely store cryptographic keys, encrypt/decrypt data, and authenticate device identities.

Data Encryption: Encrypted protocols must be implemented to ensure data in transit and data at rest confidentiality between connected IoT devices.

Network Security: IDPS, firewalls, secure gateways, and network segmentation are reviewed for their ability to secure against network-based assaults.

Secure Device Design: Adding "security by design" throughout the entire product development process—from architecture to deployment—insures that IoT devices are secure against known and future threats [1].

### 3.3.1 Critical Cybersecurity Challenges

The largest impediments to IoT adoption is the lack of good security protocols. These are supplementary to traditional information system security objectives—confidentiality, integrity, and availability (CIA)—but are compounded by the unique characteristics of IoT devices such as:

- Resource limitations making it hard to implement traditional cryptographic algorithms.
- Variability of protocols across device makers.

DOI: https://doi.org/10.5281/zenodo.15496886

- Vulnerability to physical attacks and environmental interference.
- Sparse or non-existent firmware updates.

**Cyber Security Challenges:**

Different from traditional IT environments, IoT devices usually execute in resource-constrained, heterogeneous, and physically accessible environments exposed to more attack threats. Though the fundamental information system security objectives of confidentiality, integrity, and availability (CIA) continue to apply, the unique structure of IoT creates new threat dimensions and raises the attack surface considerably [12].

The primary IoT cybersecurity issues are:

**1. Device Heterogeneity:**

IoT systems are made up of a wide range of devices possessing varying capabilities, architectures, and communication protocols. This heterogeneity complicates the application of global security standards to be implemented and hinders interoperability as well as shared threat management.

**2. Limited Processing Power and Memory:**

The majority of IoT devices are built with limited processing and storage capacity to reduce cost and size. As a result, they lack the capability to support conventional encryption algorithms, secure boot processes, or intrusion detection mechanisms.

**3. Firmware and Software Vulnerabilities:**

Due to poor or non-existent software patching processes, the majority of IoT devices remain vulnerable to known exploits. Even where updates are available, they are not applied by users.

**4. Lack of Standardization**:

The absence of global standards for IoT device security creates uneven application of security controls across manufacturers and platforms.

**5. Data Privacy and Leakage Risks:**

IoT devices are constantly collecting, transmitting, and storing sensitive personal or operational data. Without proper encryption and data governance procedures, the data can be intercepted or exploited.

**6. Insecure Communication Channels:**

A number of these appliances send data over insecure wireless networks (e.g., Wi-Fi, Zigbee, Bluetooth), which may be spoofed, hijacked using man-in-the-middle (MitM) attacks, or intercepted.

## 4. Benefits:

IOT integration of electric power systems revolutionized the conventional grid to the Smart Grid—a very sensitive, digitally empowered, and data-centric system. The following are the benefits that identify how IoT makes grid management efficient, efficient, and interactive:

### 4.1 Advanced Metering Infrastructure

The application of IoT technologies makes it possible to install Advanced Metering Infrastructure, which automatically reads, analyzes, and reports energy consumption. Smart meters communicate with utility companies in real-time, allowing for effective billing, detection of outages, remote disconnection/reconnection, and accurate demand forecasting.

### 4.2 Enhanced Reliability and Self-Healing Ability

An intelligent grid based on IoT is self-repairing in nature, i.e., faults are automatically sensed by the network and it redesigns itself for the restoration of normal operation. This minimizes downtime due to internal faults or external disturbances, thereby improving system reliability and toughness of the power distribution network [6].

### 4.3 Efficiency of Power Management

IoT devices support bi-directional exchange of power, which supports the consumer not just in using power but also to supply power that is wasted in the process to the grid. With this facet combined with sources of energy that are green, such as solar or biogas, power sustainability and decentralization increase.

## 5. Challenges

Cybersecurity remains one of the largest and most complex challenges in the Internet of Things (IoT) domain. With so many connected devices, IoT systems are highly vulnerable to different types of cyber attacks such as

DOI: https://doi.org/10.5281/zenodo.15496886

espionage, data theft, sabotage, and ransomware. In a United States-based survey, 54% of cyberattacks were on energy infrastructure, which reflects the increased risk to critical infrastructure [10].

### 5.1 Key Security Challenges in IOT:

Three fundamental problems render it difficult to deploy effective security controls in IoT systems [2]:

- Highly Distributed Environments: IoT applications run on various and geographically dispersed locations, and hence centralized control and monitoring become difficult.
- Heterogeneous Devices: The heterogeneity of smart devices with various architectures, protocols, and operating systems makes universal security enforcement difficult.
- Resource Limitations: Most IoT devices have low power, processing, and memory capabilities, which limits the application of conventional security features [7].

Consequently, standard cybersecurity models do not function effectively in IoT landscapes and need innovative strategies specific to the peculiar nature of IoT systems.

### 5.2 Vulnerabilities in IOT-Based Virtual Power Plant (VPP):

IoT-based Virtual Power Plants (VPPs) are especially vulnerable due to their hierarchical architecture based on Advanced Metering Infrastructure (AMI), SCADA systems, power monitoring equipment, and demand-response units. The hierarchical architecture of such systems offers various points of entry for intrusions. A single compromised node can trigger cascading failures, resulting in system-wide outages.

### Sensor Limitations:

Several IoT sensors in the present generation lack features that are basic and essential like situational intelligence, secure protocols of communication, and power efficiency [4]. They are exposed to abuse and manipulation due to these shortcomings. Additionally, low-power wireless networks, which are the standard for many IoT installations, require high-end security solutions that balance protection with energy efficiency reduction [6].

## 6. Future Direction in IoT Devices Security Research

The future of IoT device security is about to be revolutionized with the advancement of artificial intelligence (AI), machine learning (ML), and adaptive security solutions. As the spread of connected devices expands to critical industries, security solutions that don't just detect but also anticipate and block threats in real-time are now imperative.

### 6.1 Intelligent and Adaptive Device Security

The integration of deep learning, reinforcement learning, and neural network models into IoT devices is a revolutionary prospect. These intelligent systems can monitor behavioral patterns, identify anomalies, and react to emerging threats in real-time. In future research, these models will be integrated at the device level so that autonomous threat detection and self-healing capabilities minimize human intervention.

### 6.2 Securing the Digital Evolution of Devices

The shift from analog to digital control systems in smart environments—energy, healthcare, and industrial automation—has raised device functionality exponentially but also added new vulnerabilities. While digital systems provide better monitoring and control, they also raise the attack surface. Future research will have to focus on creating security-focused embedded systems that are cyber-intrusion resilient, even under constrained computational and power budgets.

### Evolving Threat Environment for IoT Devices

With escalating cyberattacks growing more sophisticated and targeted, IoT devices must support an increasingly evolving threat environment. Legacy static security solutions no longer suffice. New security models must incorporate:

- Integration of real-time threat intelligence
- Response mechanisms built into the device firmware
- Lightweight cryptography protocols for low-power IoT devices

DOI: https://doi.org/10.5281/zenodo.15496886

- Blockchain and decentralized trust to enhance device authentication and data integrity.

## 7. Conclusion

The Internet of Things (IoT) is the next frontier in achieving global and ubiquitous connectivity between heterogeneous communication and computation-capable objects—regardless of access technology, resource capabilities, or geographical location. Of its many applications, the smart grid represents the largest and most visible IoT technology deployment. In this domain, IoT-enabled devices are strategically located along the energy chain—from generation to end-users—offering real-time control, monitoring, and optimization of grid components.

In this study, the challenges and developments in the security of the IoT ecosystem have been examined with specific emphasis on intrusion detection systems (IDS) and privacy of data. Working through datasets like UNSW-NB15 and using machine learning, we demonstrated how smart security systems enhance detection rates and response times in IoT networks.

The dynamic behavior and complexity of critical infrastructure, arising from the integration of optical fiber communications, power line carriers, wireless modules, and dedicated cables, have introduced new cyber vulnerabilities. The current paper reviewed the extensive effects of cyberattacks on critical infrastructures, particularly the energy sector, and highlighted their ill effects on the operation of the grid.

Finally, IoT technologies vastly improve the functionality of smart grids, enabling never-before levels of visibility and control. However, to lead them to their full capability, it is essential that security vulnerabilities must be treated preventively at the design, implementation, and integration phases of IoT systems—especially within mission-critical sectors such as energy. It is essential to constantly carry out research and engage with professionals to ensure that the IoT environment remains secure, robust, and trustworthy as ever against emerging cyber-attacks.

## 8. References

[1] Kenneth Kimani , Vitalice Oduol , Kibet Langat , Cyber Security Challenges for IoT-based Smart Grid Networks, International Journal of Critical Infrastructure Protection (2019)

[2] Lackner M, Markl E, Aburaia M (2018) Cybersecurity Management for (Industrial) Internet of Things: Challenges and Opportunities. J Inform Tech Softw

[3] Vinothkumar Kolluru, Sudeep Mungara, Advaitha Naidu Chintakunta International Journal on Cryptography and Information Security (IJCIS), Vol. 9, No.1/2, June 2019

[4] Samuel Tweneboah-Koduah1 • Knud Erik Skouby1 • Reza Tadayoni1 Cyber Security Threats to IoT Applications and Service Domains Springer Science+Business Media New York 2017.

[5] Olukunle Oladipupo Amoo 1, Femi Osasona 2 Cybersecurity threats in the age of IoT: A review of protective measures Received on 26 December 2023; revised on 03 February 2024.

[6] Sampath Kumar Venkatachary, Jagdish Prasad, Ravi Samikannu, Annamalai Alagappan & Leo John Baptist Andrews (2020) Cybersecurity infrastructure challenges in IoT based virtual power plants, Journal of Statistics and Management Systems

[7] Arif Ali Mughal Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges 2019.

[8] Jianli Pan , Zhicheng Yang Cybersecurity Challenges and Opportunities in the New “Edge Computing + IoT” World.

[9] Akwetey Henry Matey, 2Paul Danquah, 1Godfred Yaw Koi-Akrofi and 1 Isaac Asampana CRITICAL INFRASTRUCTURE CYBERSECURITY CHALLENGES: IOT IN PERSPECTIVE nternational Journal of Network Security & Its Applications (IJNSA) Vol.13, No.4, July 2021

[10] Mariya Ouaissa1 , Mariyam Ouaissa1 Cyber Security Issues for IoT based Smart Grid Infrastructure RESGEVT 2020 IOP Conf. Series: Materials Science and Engineering 937 (2020) 012001 IOP Publishing

[11] Eli Ratih Rahayu , Ariesya Aprillia , Ramzi Zainum Ikhsan Cybersecurity in the Age of IoT and Developing Frameworks for Securing Smart Devices and Networks Journal of Computer

DOI: https://doi.org/10.5281/zenodo.15496886

Science and Technology Application (CORISINTA) Vol. 2, No. 1, 2025

[12] Elias Yasar Akyol, "Barriers of Adopting Progressive Web Applications – A Qualitative Study Focusing on the Swedish Context", Spring 2023: MAGI02.

DOI: https://doi.org/10.5281/zenodo.15496886