IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, February 2026
Impact Factor: 8.2

Cyber security Threats in the Internet of Things (IoT) Ecosystem: A Review

Basavaraj H Mirji[1] and Suresh S[2]
Research Scholar, Srinivas University, Mangalore, Karnataka[1]
Assistant Professor, CSE Dept, Rajarambapu Institute of Technology, Sangli, Maharashtra, India[1]
Assistant Professor, CSE Dept., Rajarambapu Institute of Technology, Sangli, Maharashtra, India[2]
basavcs007@gmail.com and s.suresh@ritindia.edu

Abstract: *The rapid growth of the Internet of Things (IoT) has transformed traditional computing by enabling billions of interconnected devices to collect, process, and exchange data autonomously. While IoT technologies provide significant benefits across domains such as healthcare, smart cities, industrial automation, and transportation, they also introduce complex cyber security challenges. Limited device resources, heterogeneity, large-scale deployment, and weak security configurations make IoT ecosystems attractive targets for cyber attackers. This review paper presents a comprehensive analysis of cyber security threats in the IoT ecosystem. It discusses IoT architecture, threat models, major attack vectors, security challenges, and existing countermeasures. Additionally, emerging solutions based on machine learning, Blockchain, and zero-trust architectures are reviewed, along with future research directions.*

Keywords: Internet of Things, IoT Security, Cyber security Threats, Attacks, Privacy, Machine Learning, Smart Systems

I. INTRODUCTION

The Internet of Things (IoT) refers to a network of physical objects embedded with sensors, software, and communication technologies that enable them to connect and exchange data over the internet. IoT has revolutionized many sectors, including healthcare, smart homes, smart grids, agriculture, transportation, and industrial control systems. According to recent estimates, billions of IoT devices are deployed worldwide, and this number continues to grow rapidly.

Despite its advantages, IoT introduces severe cyber security risks. Many IoT devices operate with limited computational power, memory, and energy, which restricts the implementation of traditional security mechanisms. Furthermore, insecure communication protocols, poor authentication, lack of updates, and human negligence expose IoT systems to cyber-attacks. This paper reviews the major cyber security threats affecting the IoT ecosystem and discusses existing and emerging mitigation strategies.

II. IOT ARCHITECTURE AND SECURITY LAYERS

A typical IoT architecture consists of multiple layers, each with unique security requirements:

• **Perception Layer:** Includes sensors, actuators, and smart devices responsible for data collection. Vulnerable to physical attacks, node capture, and spoofing.

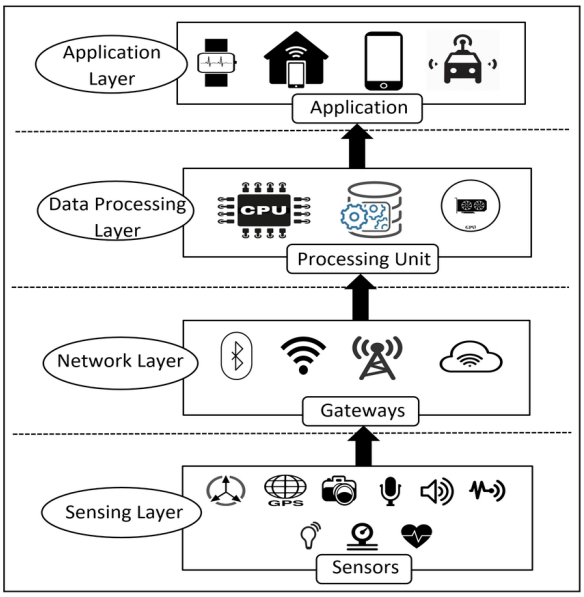
• **Transport (Network) Layer:** Handles data transmission through wired or wireless networks. Susceptible to eavesdropping, man-in-the-middle attacks, and denial-of-service attacks.

• **Processing (Middleware) Layer:** Responsible for data storage, processing, and analytics, often using cloud or edge computing. Vulnerable to malware, data breaches, and unauthorized access.

• **Application Layer**: Provides user-oriented services such as smart healthcare, smart homes, and industrial monitoring. Exposed to application-level attacks and privacy violations.

DOI: 10.48175/IJARSCT-31306

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, February 2026
Impact Factor: 8.2



III. CYBERSECURITY THREATS IN THE IOT ECOSYSTEM

1. Device-Level Threats (Perception Layer)

Device-level threats target IoT sensors, actuators, and embedded systems.

- Physical Tampering: Unauthorized physical access to IoT devices
- Device Cloning: Replication of legitimate device identities
- Malicious Firmware Updates: Installation of unauthorized or infected firmware
- Weak Authentication: Use of default or hardcoded credentials

Impact: Device compromise, fake data injection, loss of control

2. Network-Level Threats (Transport Layer)

These threats affect communication between IoT devices and servers.

- Man-in-the-Middle (MITM) Attacks: Intercepting and altering data in transit
- Eavesdropping: Passive listening to network communication
- Denial of Service (DoS / DDoS): Flooding the network to disrupt services
- Routing Attacks: Sinkhole and wormhole attacks in IoT routing protocols

Impact: Data theft, service unavailability, network disruption

3. Data-Level Threats (Processing Layer)

Data-level threats compromise stored or processed information.

- Data Leakage: Unauthorized access to sensitive data
- Data Manipulation: Alteration of sensor or system data
- Replay Attacks: Reusing captured valid data packets
- Insecure Cloud Storage: Misconfigured or poorly protected cloud services

Impact: Loss of data integrity, privacy violations

4. Application-Level Threats (Application Layer)

These threats target IoT applications and user Interfaces.

DOI: 10.48175/IJARSCT-31306

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, February 2026 Impact Factor: 8.2

• Insecure APIs: Poorly protected application programming interfaces
• Malware and Ransomware: Malicious software attacks

5. System and Management Threats (Business Layer)
Management-level threats affect monitoring, control, and governance.
• Poor Access Control: Lack of role-based access mechanisms
• Insufficient Monitoring: Failure to detect intrusions and anomalies
• Insider Threats: Malicious or negligent internal users
• Policy Misconfiguration: Incorrect or weak security policies
Impact: Large-scale system compromise

6. Supply Chain Threats
Supply chain threats can affect IoT systems at any stage.
• Hardware or Software Backdoors
• Compromised Third-Party Components
• Counterfeit Devices
Impact: Long-term hidden vulnerabilities

7. Privacy Threats
IoT devices often collect sensitive personal data.
• Location Tracking
• Unauthorized Surveillance
• Personal Data Exposure
Impact: Privacy violations and legal issues

IoT Layer	Major Threats
Device Layer	Physical tampering, device cloning, malicious firmware
Network Layer	Man-in-the-Middle (MITM), DoS / DDoS attacks, eavesdropping
Data Layer	Data leakage, replay attacks, data manipulation
Application Layer	Insecure APIs, malware, unauthorized access
Management Layer	Insider threats, policy misconfiguration, poor access control
Supply Chain	Hardware/software backdoors, counterfeit devices, compromised third-party components

Summary table

IV. MAJOR IOT ATTACK SCENARIOS

IoT systems are vulnerable to various real-world Cyber-attack scenarios due to weak security Controls, large attack surfaces, and
Resource Constrained devices. The following are major IoT Attack scenarios commonly discussed in Cyber security.

1. Botnet Attacks (e.g., Mirai Botnet)
Attackers compromise IoT devices such as
Cameras and routers using default credentials
And Convert them into botnets.
Impact: Large-scale DDoS attacks, service
Disruption

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, February 2026
Impact Factor: 8.2

2. Man-in-the-Middle (MITM) Attacks
Attackers intercept communication between IoT Devices and servers to steal or manipulate data.
Impact: Data theft, command manipulation

3. Firmware Replacement Attacks
Malicious firmware is installed on IoT devices Due to insecure update mechanisms.
Impact: Permanent device compromise, Backdoors.

4. Data Injection Attacks
Attackers inject false sensor data into the IoT System.
Impact: Wrong decisions in Healthcare, smart Grid, and industrial systems.

5. Denial of Service (DoS / DDoS) Attacks
IoT networks or servers are flooded with
Excessive traffic to disrupt services.
Impact: System downtime, unavailability of Services

V. SECURITY CHALLENGES IN IOT

IoT security faces several fundamental challenges:
• Resource constraints of devices
• Heterogeneity of hardware and protocols
• Scalability and device management
• Lack of standard security frameworks
• Infrequent firmware updates
• Human factors and misconfiguration

Solution to Security threats:
Security challenges in IoT networks can be significant. Some common threats and potential solutions include:

- **Unauthorized Access:** Use robust authentication techniques, such as two-factor authentication, and update device credentials frequently.
- **Data Integrity and Privacy:** Ensure that devices receive regular security upgrades and encrypt data while it's in transit and at rest.
- **Vulnerabilities in Devices:** Perform frequent security audits and ensure that software and devices are updated with security fixes. Segmenting IoT devices on different networks and using secure communication protocols (such as TLS/SSL) can help prevent network eavesdropping.
- **DoS (denial-of-service)** attacks: To lessen DoS assaults, use traffic filtering and intrusion detection systems.
- **Physical Tampering:** Protect physical access to devices and make use of tamper-evident hardware. Protect against Man-in-the-Middle Attacks by using intrusion detection and robust certificate-based authentication.
- **Insider Threats:** Monitor network activity, restrict access to critical systems, and run background checks on staff members.
- **Lack of Standardization:** Encourage the use of industry standards and best practices for IoT security.

VI. EXISTING COUNTERMEASURES AND SOLUTIONS

Cryptographic Techniques
Lightweight encryption and authentication protocols are used to secure constrained devices.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, February 2026
Impact Factor: 8.2

Network Security Solutions
Firewalls, intrusion detection systems (IDS), and secure routing protocols help protect IoT networks.

Device Management and Access Control
Strong authentication, authorization, and secure boot mechanisms enhance device-level security.

Machine Learning-Based Security
Machine learning techniques are increasingly used for anomaly detection, intrusion detection, and malware classification in IoT environments.

Blockchain-Based Security
Blockchain provides decentralized trust, data integrity, and secure identity management for IoT systems.

VII. FUTURE RESEARCH DIRECTIONS

Future IoT security research should focus on:
- Lightweight and adaptive security protocols
- AI-driven autonomous security systems
- Zero-trust architectures for IoT
- Secure edge and fog computing
- Privacy-preserving data analytics
- International IoT security standards and regulations

VIII. CONCLUSION

The Internet of Things has become a cornerstone of modern digital infrastructure, but its widespread adoption has introduced significant cyber security and privacy challenges. This review has analyzed major threats across different layers of the IoT ecosystem and highlighted existing security mechanisms and emerging solutions. Addressing IoT cyber security requires a holistic approach that integrates technological innovation, standardization, user awareness, and regulatory support. Continuous research and collaboration among stakeholders are essential to build resilient and secure IoT ecosystems

REFERENCES

[1]. Atzori, L., Iera, A., & Morabito, G., "The Internet of Things: A Survey," Computer Networks, Elsevier, vol. 54, no. 15, pp. 2787–2805, 2010.
[2]. Roman, R., Zhou, J., & Lopez, J., "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.
[3]. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A., "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146–164, 2015.
[4]. Weber, R. H., "Internet of Things – New Security and Privacy Challenges," Computer Law & Security Review, vol. 26, no. 1, pp. 23–30, 2010.
[5]. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X., "Fog Computing for the Internet of Things: Security and Privacy Issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.
[6]. NIST, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks," NISTIR 8228, National Institute of Standards and Technology, 2019.
[7]. OWASP Foundation, "OWASP Internet of Things Top 10 Security Risks," OWASP Documentation.
[8]. US-CERT, "Alert (TA16-288A): Heightened DDoS Threat Posed by Mirai and Other Botnets," 2016.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, February 2026
Impact Factor: 8.2

[9]. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J., "DDoS in the IoT: Mirai and Other Botnets," Computer, IEEE, vol. 50, no. 7, pp. 80–84, 2017.

[10]. Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S., "IoT Security: Ongoing Challenges and Research Opportunities," IEEE Service-Oriented Computing and Applications, vol. 8, pp. 230–234, 2014