International Journal of Advanced Education and Research
www.alleducationjournal.com
ISSN: 2455-5746
Received: 09-05-2025, Accepted: 08-06-2025, Published: 23-06-2025
Volume 10, Issue 2, 2025, Page No. 128-133

Security concerns in IOT devices and possible solutions

Harmant Singh, Ashmeet Singh, Dr. Awwab Mohammad
Department of Computer Science and Technology, Manav Rachna University, Faridabad, Haryana, India

Abstract
The rapid expansion of the Internet of Things (IoT) has revolutionized various sectors, including healthcare, smart homes, and industrial automation. However, the increased interconnectivity and reliance on IoT devices have also introduced significant security vulnerabilities. These devices often have limited processing power, memory, and security mechanisms, making them attractive targets for cyberattacks. Common security issues include unauthorized access, data breaches, privacy concerns, and denial-of-service attacks. This paper explores the key security concerns associated with IoT devices and the underlying reasons for their vulnerabilities. It also discusses possible solutions such as enhancing device authentication, data encryption, secure communication protocols, and the integration of artificial intelligence and machine learning for threat detection. Additionally, the role of standardization, regulatory frameworks, and collaboration among industry stakeholders is examined as a means to mitigate risks. The paper concludes by emphasizing the need for a multi-layered security approach to ensure the integrity, confidentiality, and availability of IoT systems while fostering innovation in this rapidly evolving field.

Keywords: Credit card fraud detection, data science, fraud prevention, fraudulent transactions

Introduction

The Internet of Things (IoT) is transforming the way we interact with technology, bringing connectivity to everyday objects and enabling smarter environments. IoT devices, ranging from smart home appliances and wearables to industrial sensors and healthcare monitoring systems, have become an integral part of modern society. With the proliferation of these interconnected devices, IoT is reshaping industries, improving efficiency, and enhancing convenience in our daily lives. However, the very nature of IoT—its reliance on the internet and the interconnection of billions of devices—exposes these systems to a wide range of security threats. Unlike traditional computing systems, many IoT devices are resource-constrained, meaning they lack the processing power, memory, and energy capacity to implement robust security measures. This vulnerability is compounded by the sheer scale of IoT networks, the diversity of devices, and the lack of standardized security protocols. As a result, IoT devices are prone to various types of cyberattacks, such as unauthorized access, data breaches, eavesdropping, and distributed denial-of-service (DDoS) attacks. Furthermore, many IoT devices collect sensitive personal data, heightening concerns about privacy and data protection.The increasing frequency and sophistication of cyberattacks targeting IoT devices have raised alarms among users, businesses, and governments. This highlights the urgent need for comprehensive security frameworks and solutions that can address the unique challenges posed by IoT. In response, this paper examines the security risks associated with IoT devices and explores potential solutions to mitigate these risks. By focusing on enhancing device authentication, ensuring secure communication protocols, utilizing encryption techniques, and implementing advanced threat detection methods, this paper aims to provide a roadmap for improving the security posture of IoT systems.

Definitionofsecurity

Security refers to the protection of systems, networks, and data from unauthorized access, attacks, damage, or theft. It encompasses the practices, measures, and controls put in place to safeguard assets and ensure the confidentiality, integrity, and availability of information. Security can be applied across various domains, including physical security (protection of physical assets), information security (protection of data and information systems), cybersecurity (protection of digital systems and networks), and even personal security (ensuring individuals' safety).

In the context of information systems and technology, security involves the implementation of strategies and tools to prevent or respond to threats such as hacking, malware, fraud, and other malicious activities that can compromise the functionality, privacy, and trustworthiness of digital systems and services.

1. Security concerns in sensor networks in IOT devices

Sensor networks are a critical component of many IoT applications, enabling devices to collect and transmit data from physical environments to centralized systems. These networks are widely used in areas such as smart homes, healthcare, agriculture, environmental monitoring, and industrial automation. However, their widespread adoption has brought about several security concerns due to their unique characteristics and vulnerabilities.

2. Limited Resources (Energy, Memory, and Processing Power)

Many IoT sensor nodes are resource-constrained devices with limited energy supply, memory, and processing power. These limitations hinder the implementation of strong security protocols such as encryption and complex authentication mechanisms, leaving the sensor networks vulnerable to attacks.

3. Unauthorized Access and Device Impersonation

Sensor networks often operate in open or semi-open environments, making them susceptible to unauthorized physical or remote access. Attackers can impersonate

legitimate sensor nodes to inject malicious data into the network or disrupt system operations.

4. Eavesdropping and Data Interception
Many IoT sensor networks transmit sensitive data over wireless channels, which are inherently prone to eavesdropping. If communication channels are not secured, malicious actors can intercept data, leading to privacy breaches and unauthorized access to sensitive information.

5. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
These attacks target the availability of sensor networks by overwhelming them with excessive traffic or resource consumption. The distributed nature of sensor networks makes them particularly vulnerable and such attacks can be difficult to detect and mitigate.

6. Lack of Device Authentication and Key Management
Many sensors lack effective mechanisms for device authentication and key management. This can allow unauthorized or compromised devices to join the network, increasing the risk of security breaches.

7. Physical Tampering and Attacks on Hardware
Sensor nodes are often deployed in uncontrolled or outdoor environments, making them susceptible to physical tampering. Attackers can reverse-engineer hardware or inject malicious code, compromising the entire network.

8. Scalability of Security Solutions
Sensor networks may include thousands or millions of devices, and implementing scalable security measures is a major challenge. Traditional security solutions may not be feasible due to resource constraints.

Possible Solutions to Address SecurityConcerns in Sensor Networks

1. **Lightweight Cryptography and Secure Communication Protocols:** Use lightweight cryptographic algorithms such as Elliptic Curve Cryptography (ECC) and secure protocols like TLS/DTLS to secure communication without overburdening devices.

2. **Device Authentication and Access Control:** Implement strong authentication mechanisms (e.g., PKI, digital certificates) and access control policies to prevent unauthorized device access.

3. **Intrusion Detection Systems (IDS) and Anomaly Detection:** Deploy IDS and machine learning-based anomaly detection systems to identify unusual behaviors and threats in real-time.

4. **Data Encryption and Integrity Checks**
   Encrypt data before transmission and use message authentication codes (MACs) to detect tampering during data exchange.

5. **Physical Security and Tamper Detection**
   Use tamper-resistant enclosures, sensors for detecting unauthorized access, and secure deployment practices to mitigate physical attacks.

6. **Energy-Efficient Security Protocols**
   Develop energy-efficient protocols that balance security with battery and processing constraints (e.g., sleep modes, lightweight key management).

7. **Standardization and Secure Frameworks**
   Follow industry standards and adopt security frameworks that ensure end-to-end protection across devices, networks, and services.

Security Issues in IoT Devices

a. Unauthorized Access and Device Compromise
Due to weak or default authentication mechanisms, attackers can gain control of IoT devices, extract data, or use them for botnet-based DDoS attacks.

b. Data Privacy Concerns
IoT devices collect sensitive data. Without adequate security, this data can be intercepted, stolen, or misused.

c. Eavesdropping and Man-in-the-Middle (MitM) Attacks
Unsecured wireless communications can be intercepted or altered by attackers, compromising data confidentiality and integrity.

d. Insufficient Encryption and Insecure Channels
Many IoT devices lack strong encryption or use insecure communication channels, making transmitted data vulnerable to interception and tampering.

e. Lack of Regular Software Updates and Patching
Many devices do not receive timely updates or security patches, leaving them exposed to known vulnerabilities.

f. Limited Security in Sensor Networks
Sensor networks, especially in remote locations, face challenges such as lack of encryption, weak authentication, and limited intrusion detection due to resource constraints.

Challenges in Securing IoT Devices

a. Resource Constraints
IoT devices are often designed with limited processing power, memory, and energy, which restricts the implementation of resource-intensive security mechanisms. Cryptographic algorithms and sophisticated security protocols may be infeasible due to these limitations. This challenge requires the development of lightweight, efficient security solutions tailored to resource-constrained devices.

b. Scalability of Security Solutions
IoT networks can consist of billions of interconnected devices, creating scalability issues for security solutions. Managing and securing such a large number of devices, each with its own vulnerabilities, is complex. Solutions need to be scalable and able to maintain security standards as the network grows, without imposing significant performance or management overhead.

c. Interoperability of Devices and Standards
IoT devices are manufactured by a wide range of vendors, often using different communication protocols, software platforms, and hardware architectures. This lack of standardization makes it difficult to implement uniform

security policies across devices. Interoperability challenges can create security gaps when devices from different manufacturers are integrated into the same system.

d. Physical Security
Many IoT devices are deployed in open or unsecured locations, making them vulnerable to physical tampering. If attackers gain physical access to a device, they can bypass security measures such as authentication and encryption, reverse-engineer hardware, or inject malicious code. Physical attacks are especially concerning in mission-critical IoT systems.

e. Long Device Lifecycles and Support
IoT devices often have long lifecycles, with some remaining in deployment for years without updates or maintenance. Older devices may not support modern encryption standards or security features, leaving them open to exploitation. Maintaining device security throughout the lifecycle, including end-of-life management and secure decommissioning, presents a significant challenge.

Security Considerations in IoT

a. Device Authentication and Identity Management
Establishing secure, unique identities for each IoT device is crucial. Devices must authenticate each other to ensure legitimacy and authorization. Solutions such as Public Key Infrastructure (PKI), digital certificates, and secure boot processes can help verify device identity and establish secure communication channels. Multi-factor authentication and biometrics can also enhance device and user verification.

b. Data Encryption and Integrity
All data transmitted between IoT devices and other parts of the network, such as cloud servers, should be encrypted to ensure confidentiality and integrity. Encryption should be applied both in transit (using protocols like TLS or IPsec) and at rest, using modern, efficient cryptographic algorithms optimized for resource-constrained IoT devices.

c. Secure Software and Firmware Updates
A secure, reliable update mechanism is critical to patching vulnerabilities in IoT devices. Devices should be able to receive over-the-air (OTA) updates that are signed, verified, and encrypted to prevent malicious actors from introducing malware. Regular security updates should be part of the device's lifecycle management.

d. Monitoring and Intrusion Detection
Continuous monitoring of IoT devices and networks can help detect abnormal behavior that may indicate a security breach. Intrusion Detection Systems (IDS) can identify patterns of attack or device compromise, enabling early responses to prevent widespread damage. Machine learning algorithms can be integrated into IDS to improve detection accuracy and reduce false positives.

e. Privacy by Design
Security considerations in IoT devices should incorporate privacy protection as a core design principle. Devices should collect only the minimum necessary data, anonymize sensitive information, and allow users to control their data. Compliance with privacy regulations such as GDPR is essential to ensure user trust and meet legal requirements.

f. Physical Security Measures
Physical protection of IoT devices is also critical. Devices should be tamper-resistant and placed in secure locations to prevent unauthorized access. For critical applications, such as industrial or healthcare IoT, devices should be housed in secure enclosures or protected by access control systems to mitigate the risk of physical tampering.

Possible Solutions for IoT Security

1. Lightweight Cryptography Algorithms
To address resource constraints, lightweight cryptographic algorithms should be used. These algorithms provide adequate security with minimal computational overhead. Techniques such as Elliptic Curve Cryptography (ECC) are well-suited for constrained environments.

2. Blockchain for Secure Data Integrity
Blockchain technology can be used to provide secure, immutable logs for IoT data, ensuring data integrity and enabling transparent audit trails. This helps secure data exchanges, particularly in supply chain and healthcare applications, by making tampering more difficult.

3. IoT Security Standards and Frameworks
Developing industry-wide standards and security frameworks is essential to address interoperability and scalability challenges. Initiatives like the IoT Security Foundation (IoTSF) and the Open Web Application Security Project (OWASP) provide guidelines for securing IoT devices and networks.

4. Multi-Layered Security Approach

Key Solutions for Securing IoT Devices

1. Device Authentication and Access Control
- **Public Key Infrastructure (PKI) and Digital Certificates:** Ensures only trusted devices can join the network.
- **Multi-Factor Authentication (MFA):** Combines password, biometrics, or one-time codes to prevent unauthorized access.
- **Role-Based Access Control (RBAC):** Allows only authorized users/devices to access sensitive functions based on their roles.

2. Data Encryption and Secure Communication
- **End-to-End Encryption (E2EE):** Protects data at rest and in transit using algorithms like AES.
- **Secure Communication Protocols:** TLS and DTLS can prevent interception and man-in-the-middle attacks.
- **Lightweight Cryptography:** ECC provides strong encryption with low resource use.

3. **Regular Software Updates and Patch Management**
- **OTA Updates:** Secure and remote firmware updates that are signed and verified.
- **Automated Patch Management:** Ensures timely security patches without manual intervention.
- End-of-Life Management: Secure decommissioning of obsolete devices to prevent data leakage.

4. **Intrusion Detection and Anomaly Detection**
- **Intrusion Detection Systems (IDS):** Monitors for abnormal network behavior.
- **Machine Learning-Based Detection:** Identifies patterns that deviate from normal behavior.
- Behavioral Analytics: Builds a profile of typical behavior for each device to detect threats.

5. **Secure Boot and Hardware-Based Security**
- **Secure Boot:** Prevents execution of unauthorized software at startup.
- **Hardware Security Modules (HSMs):** Securely store cryptographic keys.
- **Root of Trust (RoT):** Verifies software integrity from the hardware layer up.

6. **Privacy by Design**
- **Data Minimization:** Collect only what's necessary.
- **Anonymization and Pseudonymization:** Protects sensitive personal information.
- **User Consent and Data Control:** Offers transparency and control over data collection and sharing.

7. **Secure Physical Deployment**
- **Tamper Detection:** Alerts for physical interference.
- **Secure Enclosures:** Prevent unauthorized physical access.
- **Geofencing:** Restricts device function to specific locations.

8. **Blockchain for Data Integrity and Transparency**
- **Immutable Data Logging:** Prevents unauthorized data changes.
- **Decentralized Security:** Removes single points of failure.
- Smart Contracts: Automate and enforce security policies.

9. **Security Standards and Best Practices**
- **Adoption of Industry Standards:** Use frameworks from IoTSF, OWASP, etc.
- **Secure Development Lifecycle (SDLC):** Integrate security into every development phase.
- **Risk Assessment and Threat Modeling:** Identify and address vulnerabilities proactively.

10. **User Education and Awareness**
- **Training and Awareness Programs:** Teach users about password hygiene, threat recognition, etc.
- **Best Practices for Device Configuration:** Encourage strong passwords, enable 2FA, and keep firmware up to date.

2. Organizing IoT Devices Protection Development Cycle

To effectively secure IoT devices, it is critical to adopt a structured approach that encompasses the entire development lifecycle. This lifecycle should integrate security measures at every stage—from planning and design to deployment and decommissioning—to ensure that the final product is resilient to threats. Below is an organized framework for the protection development cycle of IoT devices, outlining key stages, activities, and considerations for securing IoT systems.

1. **Planning and Risk Assessment**

Objective: Identify potential security risks and define security requirements for the IoT device based on its intended application, environment, and use case.

Key Activities
- **Threat Modeling:** Conduct a thorough analysis to identify potential threats and vulnerabilities that could impact the device, network, or users. Consider attack vectors such as unauthorized access, data interception, device tampering, and denial-of-service attacks.
- **Risk Assessment:** Evaluate the risk posed by each identified threat in terms of likelihood and potential impact. Prioritize risks to be mitigated through security controls.
- **Define Security Objectives:** Establish clear security goals and guidelines for the IoT device, such as ensuring confidentiality, integrity, availability, and privacy. This also includes compliance with industry standards and regulations (e.g., GDPR, NIST, ISO/IEC 27001).

Considerations
- **Data Sensitivity:** The type of data being collected and processed (e.g., personal, health-related, financial) will determine the required level of security.
- **Device Environment:** The deployment environment (e.g., remote, industrial, healthcare) may dictate specific security measures, such as physical tamper resistance or secure network protocols.

2. **Design and Development**

Objective: Integrate security into the design and development of the IoT device to ensure that protective features are embedded from the outset.

Key Activities
- **Secure Architecture Design:** Architect the system with security in mind, including secure communication protocols (e.g., TLS, VPN), encryption algorithms (e.g., AES, ECC), and access control mechanisms (e.g., RBAC, MFA). Ensure that devices can securely authenticate one another and that sensitive data is protected at all stages.
- **Device Authentication:** Implement strong authentication mechanisms, such as Public Key Infrastructure (PKI), digital certificates, or secure hardware modules (e.g., TPM), to verify the identity of devices and users.
- **Privacy by Design:** Incorporate privacy features into the design, including data minimization, anonymization, and user consent management. Ensure compliance with relevant privacy regulations (e.g., GDPR).
- **Secure Software Development:** Follow secure coding practices and conduct static and dynamic analysis to

detect vulnerabilities in the software. Incorporate code obfuscation and anti-tampering techniques to protect against reverse engineering.
- **Use of Secure Hardware:** Select secure hardware components with built-in features like secure boot, hardware-based key storage, and tamper detection.

Considerations
- **Resource Constraints:** Ensure that security measures are optimized for the limited processing power, memory, and energy availability of IoT devices.
- **Scalability:** Design the security framework to scale efficiently as the IoT network grows, addressing challenges such as network load and device diversity.

3. Prototyping and Testing
Objective: Test the prototype for security vulnerabilities and ensure that security mechanisms function as intended under real-world conditions.

Key Activities
- **Penetration Testing:** Perform ethical hacking and penetration testing on the IoT device and network infrastructure to identify potential weaknesses.
- **Vulnerability Scanning:** Use automated scanners to detect common security flaws in firmware, APIs, and communication protocols.
- **Security Audits and Code Reviews:** Conduct thorough audits of both hardware and software to ensure security requirements are met. Perform manual and automated code reviews.
- **Compliance Testing:** Verify that the device meets relevant security standards and regulations (e.g., IEC 62443 for industrial IoT, ISO/IEC 27001).

Considerations
- **Simulated Attacks:** Test devices under realistic attack scenarios to evaluate their ability to defend against various threats.
- **User and Device Behavior:** Analyze how users interact with the device to identify potential misuse (e.g., weak passwords or unencrypted communication).

4. Deployment and Installation
Objective: Deploy IoT devices securely, ensuring correct configuration and protection of communication channels.

Key Activities
- **Secure Boot and Firmware Installation:** Ensure devices are initialized securely with verified, digitally signed firmware to prevent tampering.
- **Network Segmentation:** Segment devices into isolated networks to prevent lateral movement during security breaches.
- **Secure Key Management:** Implement secure key management for device-to-cloud communication, ensuring keys are safely stored, rotated, and managed.
- **Device Authentication During Deployment:** Use strong authentication mechanisms to ensure only authorized devices are deployed to the network.

Considerations
- **Over-the-Air (OTA) Updates:** Enable secure, encrypted OTA updates to support remote patching.
- **Physical Security:** Apply tamper-resistant solutions for critical infrastructure based on physical deployment locations.

5. Monitoring and Incident Response
Objective: Continuously monitor IoT devices for abnormal behavior and implement an effective incident response plan.

Key Activities
- **Continuous Monitoring:** Use tools to collect and analyze data from devices and networks in real time. Employ machine learning and anomaly detection to identify threats.
- **Intrusion Detection Systems (IDS):** Deploy IDS to detect unauthorized access and malicious activity.
- **Incident Response Plan:** Maintain a detailed plan for responding to breaches, including containment, mitigation, and recovery.

Considerations
- **Real-time Alerts:** Provide administrators with immediate alerts for suspicious activity.
- **Forensics and Data Integrity:** Maintain immutable logs of interactions and communications to support post-incident investigations.

6. Maintenance and Updates
Objective: Keep IoT devices secure during their operational lifespan through updates, patches, and ongoing improvements.

Key Activities:
- **Routine Patching and Updates:** Ensure devices receive timely updates to address vulnerabilities. Automate the patch management process.
- **Security Audits:** Conduct regular audits to evaluate the effectiveness of security controls.
- **End-of-Life (EOL) Management:** Safely decommission devices, erasing sensitive data and disconnecting them from the network.

Considerations:
- **Legacy Device Support:** Implement mechanisms for managing and updating legacy devices.
- **Extended Device Lifespan:** Maintain security for long-lifespan devices through hardware upgrades and secure decommissioning.

7. Decommissioning and Disposal
Objective: Securely decommission and dispose of IoT devices to protect sensitive data and prevent misuse.

Key Activities:
- **Data Wiping:** Ensure that all data is securely erased before recycling or disposal.
- **Secure Device Disposal:** Follow best practices to mitigate the risk of data recovery or unauthorized reuse.
- **Documentation and Reporting:** Keep records of the decommissioning process to ensure risk management and compliance.

Conclusion
The Internet of Things (IoT) ecosystem has transformed modern life by integrating intelligent devices into various

domains such as healthcare, smart homes, and industrial automation. However, this rapid proliferation has simultaneously introduced a broad spectrum of security challenges stemming from inherent device limitations, heterogeneous architectures, and lack of standardized security practices. Our study highlights that while risks such as unauthorized access, data breaches, and denial-of-service attacks remain prevalent, a combination of robust device authentication, end-to-end encryption, secure communication protocols, and AI/ML-driven threat detection can significantly mitigate these vulnerabilities.

Moreover, the importance of global standardization, effective regulatory frameworks, and active collaboration between manufacturers, policymakers, and cybersecurity professionals cannot be understated. Only through a unified and multi-layered security strategy can the integrity, confidentiality, and availability of IoT systems be assured, ensuring user trust and fostering sustainable growth in this field. The future of IoT security lies in continuous innovation, proactive defense mechanisms, and adaptive solutions that evolve in tandem with emerging threats.

Result

This paper provides an in-depth analysis of the pressing security concerns surrounding IoT devices and outlines practical and technologically feasible solutions to address these risks. The findings suggest that a multi-faceted approach encompassing both technological enhancements and organizational policies is essential for securing IoT ecosystems. Implementation of improved authentication techniques, encryption standards, and AI-based anomaly detection methods can significantly reduce vulnerability exposure. Furthermore, fostering cooperation between industries and regulatory bodies will lead to more resilient and standardized security practices across the IoT landscape.

References

1. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks,2013:57(10):2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018.
2. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks,2015:76:146–164. https://doi.org/10.1016/j.comnet.2014.11.008.
3. Alaba FA, Othman M, Hashem IAT, Alotaibi F. Internet of Things security: A survey. Journal of Network and Computer Applications,2017:88:10–28. https://doi.org/10.1016/j.jnca.2017.04.002.
4. 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,2017:4(5):1125–1142. https://doi.org/10.1109/JIOT.2017.2683200.
5. Mosenia A, Jha NK. A comprehensive study of security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing,2017:5(4):586–602. https://doi.org/10.1109/TETC.2016.2606384.
6. Zhang Y, Ansari N. Security and privacy in the Internet of Things (IoT): Models, algorithms, and applications. Springer International Publishing, 2017.
7. Roman R, Zhou J, Lopez J. On the security of wireless sensor networks. Security and Privacy in Mobile and Wireless Networking,2013:74–90.
8. Weber RH. Internet of Things – New security and privacy challenges. Computer Law & Security Review,2010:26(1):23–30.
9. Sicari S, Rizzardi A, Grieco LA, Boggia G. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks,2015:76:146–164.
10. Cui Y, Chen K, Hu H. A survey of security and privacy issues in Internet of Things. Journal of Network and Computer Applications,2016:59:16–29.
11. Hossain MS, Muhammad G. Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring. Future Generation Computer Systems,2016:56:614–624.
12. IoT Security Foundation. Security for IoT devices and networks: A practical guide, 2020.
13. National Institute of Standards and Technology (NIST). NIST Special Publication 800-53: Security and privacy controls for federal information systems and organizations, 2018.
14. European Union Agency for Cybersecurity (ENISA). IoT security: State of play, 2020.
15. Sharma M. How to protect IoT devices from cyber threats: Best practices, 2020.
16. Bose R, Mullen C. Top IoT security threats and how to mitigate them, 2021.
17. Internet Engineering Task Force (IETF). Security requirements for Internet of Things (IoT). RFC 8576, 2021.
18. ISO/IEC 27001:2013. Information security management systems – Requirements.
19. ISO/IEC 27001 is an international standard that provides a framework for managing information security risks, which is crucial for the protection of IoT systems and devices.