Computing&AI Connect
ISSN: 3104-4719
2025, Article ID. 2025.0011, Cite as: www.doi.org/10.69709/CAIC.2025.139199

SCIFINITI PUBLISHING

Review Article

OPEN ACCESS

Security and Privacy in the IIoT: Threats, Possible Security Countermeasures, and Future Challenges

Mircea Țălu[✉,1,2]

[1] Faculty of Automation and Computer Science, The Technical University of Cluj-Napoca, 26-28 George Barițiu St., Cluj-Napoca, 400027 Cluj, Romania
[2] SC ACCESA IT SYSTEMS SRL, Constanta St., no 12, Platinia, CP. 400158 Cluj-Napoca, Romania

Article History
Received: November 03, 2024 Accepted: February 14, 2025 Published: March 17, 2025

Abstract
The development of industrial applications assumes securing Internet of Things (IoT) and Industrial Internet of Things (IIoT) environments, which require continuous monitoring, adaptation, and improvement to protect them from an ever-changing threat landscape. The IIoT architecture requires a holistic approach to IIoT security, involving technical measures, best practices, policies, and ongoing monitoring. Substantial research has been dedicated to investigating IoT security issues and challenges, including within the context of the IIoT. These researches provide valuable insights into the landscape of IoT security, highlighting both general and specific security threats and challenges. They contribute to a comprehensive understanding of IoT and IIoT security from both broad and detailed perspectives. While many studies have discussed IoT and IIoT security challenges, analyzing the gap between security requirements and the actual countermeasures in use, it's crucial to assess whether the countermeasures deployed in real-world industrial environments adequately address these challenges in use, to understand the effectiveness of current security practices. This study presents a comprehensive analysis of the security landscape of IoT/IIoT, addressing attack vectors across architecture layers and evaluating existing countermeasures by focusing on the different layers of security, the threat landscape, scalability of security solutions, ensuring security in complex industrial systems, and addressing security in resource-constrained devices. Additionally, by outlining future research issues and challenges, this approach encourages ongoing investigation and development in the field of IoT/IIoT security. It aims to address these challenges through innovative solutions and collaborative efforts, enhancing the understanding of complexities and strategies required to secure IoT/IIoT systems effectively.

Keywords:
attacks; internet of things (IoT); Industrial Internet of Things (IIoT); Privacy-enhancing technology; security countermeasures; security goals; threats

1. Introduction

The Internet of Things (IoT) involves the interconnection of a wide variety of devices and objects through the Internet, enabling them to collect, exchange, and process data [1–4]. The connectivity (wired or wireless) provided by IoT enables these devices to communicate and collaborate, often leading to enhanced functionality, efficiency, and convenience to create a network of interconnected "things" that can interact and share information to serve various purposes [5,6]. Industrial IoT (IIoT) is the application of IoT to automation applications using industrial communication technologies. Furthermore, IoT devices generally have constrained power, storage, computing, and communications resources.

The rapid growth and adoption of IoT technology are predicted to expand to 75 billion by 2025 [7]. IoT devices provide significant benefits in various domains, including university education, where they enhance smart classrooms and student engagement [8]. However, they also introduce security risks that cybercriminals can exploit [9–12]. Cyber threats focus on vulnerabilities in people, processes, and technology [13–15].

Corresponding Author:
Mircea Țălu, Faculty of Automation and Computer Science, The Technical University of Cluj-Napoca, 26-28 George Barițiu St., 400027 Cluj-Napoca, Romania; SC ACCESA IT SYSTEMS SRL, Constanta St., no 12, Platinia, CP. 400158 Cluj-Napoca, Romania; talu.s.mircea@gmail.com; Tel.: +40-264401200

© 2025 Copyright by the Author.
Licensed as an open access article using a CC BY 4.0 license.

SCIFINITI PUBLISHING

As Industry 4.0 (also called the Fourth Industrial Revolution—defined by the use of information and communication technology in the industry) was implemented on an industrial level, with the evolution of cyber-physical systems, cyber security had to answer new challenges with complex solutions to respond to global vulnerabilities [16,17]. Even Industry 5.0 (which appeared very soon after Industry 4.0—first coined by the German government in 2011) marks a pivotal moment in the evolution of industrial paradigms, and revolutionized technology by integrating physical systems with digital networks. It also introduced new technical infrastructures that expand socio-environmental considerations within Industry 4.0. In this context, the critical role of cyber security is essential to effectively address the spectrum of cyber risks faced by modern organizations, and for finding a diverse range of solutions to block these challenges [17–20].

In the last decade, a significant increase in research and publications focused on analyzing security threats and privacy challenges in the realm of IoT and IIoT. These surveys and reviews aimed to identify vulnerabilities, risks, and potential solutions to address the growing concerns related to the security and privacy of interconnected devices in various contexts [21–24]. The research on IoT security threats and privacy challenges has indeed been prevalent in the general IoT domain rather than the IIoT domain [25–28]. Overall, deep learning and decentralized blockchain technologies, as well as recent modern industry solutions with different resource constraints, were analyzed in IIoT security environments [29–31]. It's important to note that security risks and countermeasures were specific to each industry's technology landscape (from transportation and automotive, manufacturing and industrial, energy, healthcare technology, smart manufacturing, aviation, to defense industry, etc.), according to a tailored approach to address its unique challenges [32–35].

2. IoT and IIoT Architectures

In the literature are proposed different models with a high-level of architecture for IoT/IIoT: the three-layer, four-layer, five-layer, and seven-layers, having different correlations between their components (Table 1).

While the three-layer model can be useful for understanding certain aspects of network operations, it might not fully capture the complexities of IoT/IIoT networks. The traditional architecture with four layers for an IoT/IIoT is composed of: sensing/perception layer, communication/ network layer, data processing and analysis layer, and cloud/storage layer [1,9].

Table 1: Models with a high-level of architecture for IoT/IIoT.

Model	Layers	Description	Use Case/Strength
Three-layer	- Perception Layer - Network Layer - Application Layer	Simplest model, focusing on sensing, transmission, and application processes.	Good for basic IoT applications; lacks depth for complex systems.
Four-layer	- Sensing/Perception Layer - Communication/ Network Layer - Data Processing Layer - Cloud/Storage Layer	Traditional model adding a processing layer between data collection and storage, useful for real-time data analysis.	Suited for intermediate IoT/IIoT applications with processing needs.
Five-layer	- Perception Layer - Transport Layer - Processing Layer - Application Layer - Business Layer	Adds a business layer for decision-making, allowing data to support higher-level business processes and analytics.	Effective for IoT/IIoT systems that need business logic integration.
Seven-layer	- Perception Layer - Connectivity Layer - Edge Computing Layer - Processing Layer - Application Layer - Business Layer - Security Layer	Comprehensive model covering diverse functions, security, and business logic for complex IIoT systems.	Ideal for advanced IIoT systems needing detailed security and analytics layers.

2025, Vol. 2, Article ID. 2025.0011
www.doi.org/10.69709/CAIC.2025.139199

Table 2 provides a concise yet comprehensive overview of the diverse application areas of the IIoT, showcasing its transformative potential across various industries. Each area leverages IIoT technologies to optimize processes, enhance operational efficiency, and drive innovation. Table 3 compares wireless connectivity technologies for IIoT. Wi-Fi (100 m, high data rate, moderate power) suits industrial networks but is vulnerable to DoS and MitM. Bluetooth (10 m, moderate data rate, low power) is used in wearables, with risks of eavesdropping and jamming. ZigBee (100 m, low data rate, low power) fits sensor networks, but faces replay attacks and key cracking. LoRaWAN (15 km, very low data rate, very low power) is ideal for remote monitoring, with risks of data spoofing and weak authentication. 5G (1 km, very high data rate, high power) supports real-time apps but is prone to network slicing and DDoS attacks.

Table 2: Application areas of IIoT.

Application Area	Description	Examples
Manufacturing	Streamlined production and predictive maintenance	Smart factories, robotics
Energy and utilities	Efficient energy management and monitoring	Smart grids, oil pipeline monitoring
Healthcare	Remote monitoring and operational efficiency	Wearable devices, equipment tracking
Transportation and logistics	Optimized routing and asset tracking	Autonomous vehicles, fleet management
Agriculture	Precision farming and resource management	Smart irrigation, soil monitoring

Table 3: A summary of wireless standard connectivity technologies for IIoT.

Technology	Range	Data Rate	Power Consumption	Applications	Vulnerabilities
Wi-Fi	100 m	High	Moderate	Industrial networks	DoS, MitM
Bluetooth	10 m	Moderate	Low	Wearables, short-range devices	Eavesdropping, jamming
ZigBee	100 m	Low	Low	Sensor networks, smart homes	Replay attacks, key cracking
LoRaWAN	15 km	Very low	Very low	Remote monitoring, agriculture	Data spoofing, weak authentication
5G	1 km	Very high	High	Real-time applications	Network slicing attacks, DDoS

The seven-layer model represents a specialized architecture designed to address the intricacies of IoT/IIoT networks, where each layer serves a distinct purpose in facilitating the functionality and efficiency of IoT/IIoT systems (such as perception layer, connectivity layer, edge computing layer, processing layer, application layer, business layer, and security layer) [33]. Application areas of IIoT are shown in Table 2, and a summary of wireless standard connectivity technologies for IIoT is given in Table 3.

Different protocols are utilized across various layers of IIoT systems, each serving distinct functionalities [5,10]. At the perception layer, protocols such as Modbus and OPC-UA facilitate communication between devices, sensors, and control systems, enabling efficient data collection and real-time interaction. The network layer typically employs TCP/IP and UDP for data transmission, with IPv6 gaining traction due to its scalability for extensive IoT systems. Additionally, LoRaWAN and NB-IoT are pivotal for enabling long-range, low-power

SCIFINITI PUBLISHING

communications, particularly in remote IIoT applications. In the data processing and analysis layer, lightweight messaging protocols like MQTT and AMQP support efficient data transfer between sensors and central systems. At the cloud/storage layer, HTTP/HTTPS and RESTful APIs are widely used for secure, standardized communication between cloud servers and IIoT devices, facilitating remote monitoring and management. Finally, the application layer utilizes protocols such as CoAP and XMPP to enable efficient data exchange in resource-constrained environments. Collectively, these protocols ensure seamless communication, robust data integrity, and enhanced security across all layers of IIoT ecosystems.

It is known that technologies can be divided into two broad categories: resource-constrained and resource-unconstrained systems [5,10]. This classification recognizes the different capabilities and challenges of devices and systems within the IoT and IIoT ecosystems, permitting fast deployment, management, and security decisions.

On the other hand, it is known that resource-constrained technologies are characterized by limitations in critical resources (like processing power, memory, energy, and communication bandwidth). These limitations are highlighted for example in devices designed for environments where the following features are essential (low-cost, small form factors, or long battery life). Such devices include modern embedded sensors, actuators, and edge devices used in various industrial environments. It is known that the primary constraints in these systems include the following parameters: a) Processing Power, b) Memory, c) Energy Consumption, and d) Bandwidth, which necessitate the use of lightweight, energy-efficient encryption and compression techniques. Furthermore, resource-constrained systems often use edge computing to minimize delay to the cloud or nearby servers.

On the other hand, resource-unconstrained IoT/IIoT technologies operate in environments where devices have relatively abundant resources, including high processing power, memory, energy, and bandwidth. These systems are typically found in environments where cost is less of an issue, and the devices are either permanently powered or capable of accessing stable power sources. Examples of resource-unconstrained devices include industrial machines, servers, and smart gateways that support more sophisticated operations. These systems typically exhibit: (a) Processing Power, (b) Memory, (c) Energy Consumption, (d) Bandwidth. For security and data management, resource-unconstrained systems can implement more sophisticated encryption algorithms, more extensive monitoring and intrusion detection systems, and data analytics tools that require significant resources.

3. IoT Cyber Attacks

Several recent studies continue to show that IoT devices remain highly vulnerable to cyberattacks because of insecure firmware, weak authentication mechanisms, outdated software, and insufficient security-by-design practices [36]. Recent cybersecurity reports indicate a substantial increase in IoT-targeted cyberattacks worldwide. Europe records the highest average number of weekly attacks per organization, followed by the Asia-Pacific region and Latin America. In addition, IoT malware attacks increased markedly during 2023, reflecting the growing exposure of connected devices to cyber threats [37]. Addressing these challenges requires a multi-faceted approach, including: robust security measures, regular updates, network segmentation, IoT/IIoT security standards, user education, and threat monitoring.

4. Review Methodology

There are five steps involved in the methodology for reviewing: (a) Formulating review questions; (b) Identifying pertinent literature; (c) Evaluating the quality of studies; (d) Summarizing the gathered evidence; and (e) Interpreting the research findings.

5. Classification of Attacks in Information Security

According to the specific architecture for IoT/IIoT there are different cyber-attacks with the corresponding security solutions for each of the IoT/IIoT layers [38–40]. Furthermore, the specific security challenges and solutions can vary greatly based on the industry, the types of devices, the technology stack, and the threat landscape [41–43]. The following section discusses cybersecurity for a traditional IoT/IIoT architecture consisting of four layers (Figure 1).

A. Security attacks and potential security countermeasures for the sensing/perception layer

The perception layer is where devices, sensors, cameras, and actuators collect data from the physical world and it serves as a critical interface between the physical environment and the digital IoT/IIoT system [43]. Attacks targeting the perception layer aim to manipulate or deceive these sensors to compromise the integrity, confidentiality, or availability of the data being collected.

2025, Vol. 2, Article ID. 2025.0011
www.doi.org/10.69709/CAIC.2025.139199

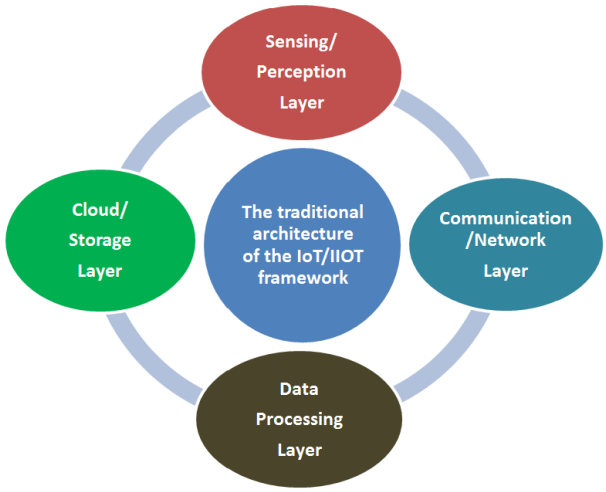


Figure 1: A traditional architecture with four layers for an IoT/IIoT.

Some security attacks in the perception layer include adversarial attacks, where attackers manipulate input data so that it appears normal to human observers but misleads machine learning models or computer vision systems; spoofing attacks, in which attackers provide false sensory information to sensors or systems; jamming, where attackers disrupt communication between sensors and their controlling systems by emitting electromagnetic interference or using noise to drown out legitimate signals; physical attacks, where attackers physically manipulate sensors or their components to compromise their accuracy or function; data injection, where attackers inject malicious data into sensor inputs to manipulate system behavior; eavesdropping, which involves intercepting sensory data transmitted between sensors and control systems; replay attacks, where attackers capture legitimate sensor data and replay it later to deceive the system; manipulation of sensor calibration, where attackers modify sensor calibration settings to skew the perception of the environment; physical tampering, where attackers physically tamper with sensors to compromise their functionality; sensor data falsification, where attackers manipulate raw sensor data before it reaches the processing systems; and privacy violations, where attackers exploit vulnerabilities to access personal or sensitive data collected by sensors, violating user privacy.

Some possible security solutions proposed by experts include device authentication and authorization, which involves implementing strong authentication mechanisms using unique device identifiers, secure keys, and certificates; secure communication, where modern encryption protocols secure communication between IoT/IIoT devices and central control systems to prevent eavesdropping, data manipulation, and unauthorized access to sensory data; firmware and software security, which ensures regular updates and patches for firmware and software, along with code signing before they are applied to devices; anomaly detection, where mechanisms identify unusual behavior or deviations in sensory data, supported by machine learning algorithms to detect potential attacks; intrusion detection and prevention systems (IDPS), which monitor network traffic and sensor data for signs of intrusion attempts, and include automated responses to isolate compromised devices; physical security, involving measures to protect IoT/IIoT devices from tampering, theft, and unauthorized access; secure boot and device initialization, ensuring only trusted and verified software runs on devices; data validation and filtering, where incoming sensory data is validated and filtered to identify and discard compromised or manipulated data; privacy by design, which minimizes the collection of sensitive data, anonymizes or pseudonymizes data whenever possible; network segmentation, which divides the network into segments to isolate devices and limit the impact of a compromised device; security auditing and monitoring, where the security posture of devices and infrastructure is regularly audited, and real-time monitoring detects and responds to security incidents; vendor and supply chain security, which involves working with trusted vendors who follow secure development practices; and user education and awareness, which educates users about IoT/IIoT security risks and best practices for maintaining secure configurations.

These security solutions and practices are a pivotal direction to protect and continuously monitor the perception layer in IoT/IIoT systems to avoid cyber-attacks.

B. Security attacks and potential security countermeasures for the communication/network layer

The communication/network layer (wire-connected or wireless based on the protocol) in the IoT/IIoT process facilitates the data exchange between the data collected by sensors and its utilization in applications [43].

Some common attacks that can affect the communication/network layer of IoT/IIoT systems include Man-in-the-Middle (MitM) attacks, where an attacker intercepts and alters communication between IoT devices or between devices and the central system, leading to data manipulation, eavesdropping, or unauthorized access to sensitive information; Denial of Service (DoS) attacks, where attackers flood communication channels with excessive traffic, overwhelming the IoT network and causing service disruption; Distributed Denial of Service (DDoS) attacks, which are similar to DoS but are orchestrated from multiple sources, making them more difficult to

mitigate and affecting IoT networks' functionality; Replay attacks, where attackers capture legitimate communication between IoT devices and replay it later to gain unauthorized access or perform malicious actions; Eavesdropping, where attackers intercept and listen to communication between IoT devices, potentially exposing sensitive data; Spoofing attacks, where attackers forge the identity of an IoT/IIoT device to gain unauthorized access to the network or deceive other devices, including methods like MAC address spoofing, IP address spoofing, or faking device identities; Jamming attacks, where attackers interfere with wireless communication signals by emitting radio frequency noise, disrupting communication between IoT/IIoT devices; Physical attacks, where attackers physically tamper with communication cables or devices, disrupting communication flow or stealing data; Traffic analysis, where attackers analyze communication traffic patterns to gain insights into IoT/IIoT system behavior or infer sensitive information; Malware injection, where malicious software is injected into IoT/IIoT devices through compromised communication channels, leading to data breaches or unauthorized control; IoT/IIoT botnets, where attackers compromise a large number of vulnerable IoT/IIoT devices to create a botnet that can be used for DDoS attacks, data breaches, and more; and Zero-Day exploits, where attackers target undiscovered vulnerabilities (zero-days) in communication protocols or devices, exploiting them for unauthorized access or control.

To protect the communication/network layer, security solutions include encryption, implementing strong encryption mechanisms to secure data during transmission; authentication and authorization, using robust methods to ensure only authorized devices communicate with each other; access control, defining policies to restrict which devices can communicate based on roles, permissions, and trust levels; firewalls and Intrusion Detection Systems (IDS), using these systems to monitor network traffic, detect anomalies, and block malicious activities; network segmentation, dividing the IoT/IIoT network into segments or VLANs to isolate critical devices from less critical ones, reducing attack surfaces; Intrusion Prevention Systems (IPS), which automatically react to detected threats by blocking suspicious traffic in real time; secure communication protocols, selecting protocols that offer security features like encryption and authentication; secure boot and updates, ensuring devices only accept authorized firmware updates to prevent unauthorized tampering; secure key management, properly managing cryptographic keys used for encryption, authentication, and signing; network monitoring and logging, regularly monitoring network traffic and maintaining logs to identify and respond to security incidents; firmware and software updates, keeping IoT devices' software up to date to patch vulnerabilities; DoS protection, implementing mechanisms like rate limiting or traffic filtering to mitigate DoS and DDoS attacks; network behavior analysis, using tools to detect abnormal communication patterns that indicate potential attacks or compromised devices; network redundancy, implementing failover mechanisms to ensure network availability during failures or attacks; honeypots and deception, using these techniques to divert attackers' attention away from critical network parts; vendor security guidelines, following security practices from IoT/IIoT device manufacturers to ensure secure device configurations; regular security assessments, conducting penetration testing and security assessments to identify network vulnerabilities; security awareness training, educating users and stakeholders about security best practices; network isolation, isolating critical IoT/IIoT systems from external networks to limit exposure to threats; and secure cloud integration, ensuring secure integration with cloud services by implementing proper authentication, encryption, and data protection practices.

The main array of strategies designed to protect these threats in the communication/network layer are strong encryption, secure authentication mechanisms, intrusion detection systems, regular software updates, and continuous monitoring.

C. Security attacks and potential security countermeasures for the data processing and analysis layer

The data processing and analysis layer constitutes the basic platform of the IoT/IIoT system, which handles the collected data from sensors and devices, processes it, makes decisions as well as streamlines their operation [43].

Common security attacks that target the data processing and analysis layer include data injection attacks, where attackers insert malicious or unauthorized data into the processing pipeline, leading to incorrect analysis results and compromised decision-making; data poisoning, where attackers manipulate input data to intentionally bias analysis results, leading to incorrect insights or decisions; model poisoning attacks, where attackers manipulate machine learning models used for analysis by feeding them malicious training data, causing the models to make incorrect predictions or decisions; model inversion attacks, where attackers exploit vulnerabilities in machine learning models to reverse engineer sensitive data used during training, potentially compromising data privacy; side-channel attacks, where attackers exploit unintended channels of information leakage, such as power consumption patterns or timing variations, to infer sensitive information being processed; orchestration attacks, where attackers compromise the workflow orchestration within

2025, Vol. 2, Article ID. 2025.0011
www.doi.org/10.69709/CAIC.2025.139199

the data processing layer, disrupting data flow and analysis; data leakage, where unauthorized parties gain access to sensitive data processed within this layer, leading to privacy breaches and potential misuse; backdoor exploitation, where attackers exploit hidden vulnerabilities or backdoors in the processing and analysis software to gain unauthorized access or control; falsified insights, where attackers manipulate analysis results presented to decision-makers, leading to incorrect conclusions and potentially harmful actions; resource exhaustion attacks, where attackers consume excessive computational resources within the data processing layer, causing slowdowns or crashes; zero-day exploits, where attackers exploit previously unknown vulnerabilities in the software or hardware components of the data processing and analysis layer; timing attacks, where attackers exploit variations in timing during data processing to gain insights into internal operations and potentially infer sensitive information; memory corruption attacks, where attackers exploit vulnerabilities in memory management to execute malicious code within the data processing and analysis components; Man-in-the-Middle (MitM) attacks, where attackers intercept and manipulate data between the data source and the processing layer, potentially altering the results of analysis; and evasion attacks, where attackers design input data to evade detection by security mechanisms, allowing malicious content to pass through and compromise the data processing layer.

To safeguard the data processing and analysis layer, security solutions include data encryption, which encrypts data both in transit and at rest to ensure sensitive information remains secure; access control and authentication, implementing strict access controls to limit who can access and modify data and processing components; data integrity checks, using checksums, hash functions, and digital signatures to verify data integrity during transit and processing, helping to detect tampering or unauthorized modifications; secure APIs and interfaces, securing the APIs and interfaces connecting to the data processing and analysis layer by implementing security measures such as rate limiting, input validation, and access controls to prevent unauthorized access; security patching and updates, keeping software components, frameworks, and libraries up to date with the latest security patches; intrusion detection and prevention, implementing systems to monitor for suspicious activities or patterns within the data processing and analysis layer; machine learning model security, applying techniques such as adversarial training and model hardening to enhance model security against attacks like poisoning and inversion; data anonymization and pseudonymization, protecting user privacy by anonymizing or pseudonymizing data before it enters the processing layer to prevent the direct identification of individuals from the data; security testing and auditing, conducting regular security assessments, vulnerability scans, and penetration testing on data processing and analysis components to identify and address potential weaknesses; secure development practices, using secure coding practices when developing software components in the layer to avoid common vulnerabilities such as injection attacks and buffer overflows; logging and monitoring, setting up logging and monitoring systems to track activities within the layer; behavioral analytics, implementing behavior-based anomaly detection to identify deviations from expected behavior that may indicate security breaches; data retention policies, defining clear retention policies to ensure data is not stored longer than necessary, reducing the potential impact of data breaches; incident response plans, developing well-defined plans outlining steps to be taken in case of a security breach; and third-party risk management, implementing security best practices for third-party services or components used within the layer.

To mitigate these threats in the data processing and analysis layer, it is recommended to implement a combination of security solutions and best practices.

D. Security attacks and potential security countermeasures for the cloud/storage layer

The cloud/storage layer handles the storage of data generated by IoT/IIoT devices in a cloud-based environment, making it accessible for analysis, processing, and retrieval to be included in various applications, from improving operational efficiency to creating new services and products [43].

Common security attacks that target the cloud/storage layer include data breaches, where attackers gain unauthorized access to sensitive data stored in the cloud, leading to data breaches; data leakage, which involves the unintentional exposure of data to unauthorized parties; DoS and DDoS attacks, which overwhelm the cloud infrastructure's resources, making services unavailable to legitimate users by flooding the network or services with excessive traffic, causing system slowdowns or outages; Man-in-the-Middle (MitM) attacks, where an attacker intercepts and potentially alters communication between the client and the cloud storage layer, leading to data manipulation, eavesdropping, and unauthorized access; injection attacks, where attackers inject malicious code or commands into input fields or data streams, exploiting vulnerabilities in applications or databases; Cross-Site Scripting (XSS), where attackers inject malicious scripts into web applications, which are then executed by unsuspecting users, stealing sensitive data or performing

actions on behalf of the user; malware and ransomware, where malicious software is uploaded to the cloud storage layer, potentially infecting other files or systems, and ransomware encrypts data stored in the cloud, demanding payment for decryption; insecure APIs, which can be exploited if not properly secured, allowing attackers to gain unauthorized access, manipulate data, or perform administrative actions; data tampering, where attackers alter or manipulate data stored in the cloud, leading to incorrect analysis and decision-making; insider threats, where malicious or negligent actions from employees or individuals with legitimate access to the cloud storage layer result in data breaches or unauthorized access; account hijacking, where attackers compromise user accounts through techniques like credential stuffing, phishing, or brute-force attacks; and elevation of privilege, where an attacker gains unauthorized access to a low-privilege account and attempts to escalate privileges to gain administrative access to the cloud storage layer.

To safeguard the cloud/storage layer, security solutions include strong authentication and access control, implementing multi-factor authentication (MFA) for user accounts accessing the cloud storage; encryption, using strong encryption algorithms for data at rest and in transit to prevent eavesdropping and MitM attacks, and employing client-side encryption to ensure data confidentiality before it reaches the cloud; regular auditing and monitoring, setting up monitoring and logging to track access and activities in the cloud storage layer, and implementing intrusion detection and prevention systems (IDS/IPS) to identify and block malicious activities, as well as establishing alerts for suspicious behavior or unauthorized access attempts; network security, using firewalls and network security groups to restrict incoming and outgoing traffic to the cloud storage, along with network segmentation to isolate critical components from less secure areas; API security, securing APIs using authentication and authorization mechanisms, implementing rate-limiting and API quotas to prevent abuse and DoS attacks, and regularly updating and patching API components to fix vulnerabilities; vulnerability management, regularly scanning and assessing the cloud storage layer for vulnerabilities using assessment tools, and keeping all software and systems up to date with the latest security patches; data backup and recovery, implementing regular data backups and ensuring secure storage, and testing data restoration procedures to ensure quick recovery in case of data loss or ransomware attacks; incident response plans, developing comprehensive plans that outline steps to take in case of a security breach; secure development practices, adhering to secure coding practices when developing applications that interact with the cloud storage, and performing code reviews and security testing to identify and fix vulnerabilities early in development; employee training and awareness, training employees and users on security best practices, phishing prevention, and safe cloud service use; cloud provider security services, leveraging built-in security services offered by cloud providers to protect against web-based attacks; and third-party security solutions, implementing solutions like intrusion detection systems, endpoint protection, and data loss prevention tools.

To mitigate these risks in the cloud/storage layer, it is important to implement a security strategy that includes strong access controls, encryption, regular security assessments, continuous monitoring, intrusion detection systems, patch management, and employee training.

6. Taxonomy of IIoT Security Attacks and Solutions

This section shows a taxonomy to classify common security attacks and solutions in the IIoT, categorizing them by attack vector (e.g., network, device, software), target (e.g., devices, networks, protocols), and impact (e.g., denial of service, data integrity, confidentiality breaches) [10,22–26].

Corresponding security solutions are mapped to each category of attacks. For example, network-based attacks such MitM and DoS are mitigated by encryption and firewall systems, which are mandatory for ensuring data confidentiality and system availability. Device-based attacks are mitigated by physical security measures and device authentication protocols, while software-based attacks are countered using anti-malware software and secure coding practices.

Furthermore, the taxonomy distinguishes between mandatory and optional features in security solutions. Mandatory features are essential for ensuring basic protection, such as encryption and authentication. Optional features, which enhance the security posture, include anomaly detection systems and real-time monitoring.

To validate the correctness and completeness of the proposed taxonomy, existing IIoT security solutions and research approaches are classified. For instance, IDS are classified into two main categories: signature-based IDS and anomaly-based IDS. Signature-based IDS, which relies on known attack patterns, is classified as a mandatory solution due to its effectiveness in detecting well-known threats. In contrast, anomaly-based IDS, which uses machine learning to detect novel or unknown attacks, is classified as an optional solution providing additional security layers for more complex threats.

Additionally, widely-used encryption algorithms such as AES (Advanced Encryption Standard), are eval-

2025, Vol. 2, Article ID. 2025.0011
www.doi.org/10.69709/CAIC.2025.139199

uated, which are mandatory for resource-unconstrained IIoT devices that require high levels of data protection. For resource-constrained IIoT devices, lightweight cryptographic algorithms such as ASCON, PRESENT, GIFT, and SPECK are commonly employed because they provide an effective balance between security, computational complexity, memory requirements, and energy efficiency [44]. These algorithms are categorized as optional features for these devices. By applying the taxonomy to classify these existing solutions, the proposed framework is demonstrated to be both comprehensive and effective in categorizing IIoT security solutions.

7. Future Challenges

Security and privacy challenges in the context of the IoT/IIoT continue to evolve as technology advances. The following potential research directions in the security of the IoT/IIoT domains could be [10,22–26] (Figure 2):

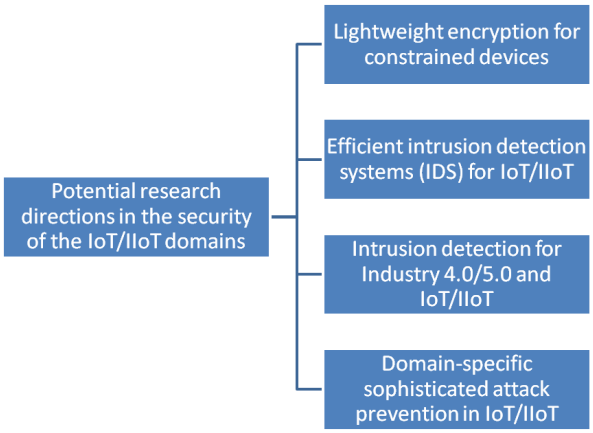


Figure 2: The potential research directions in the security of the IoT/IIoT domains.

(a) Lightweight encryption for constrained devices: IoT/IIoT devices often operates under significant resource constraints, including limited processing power, memory, and battery life. Developing lightweight encryption algorithms that ensure robust security while maintaining efficiency is critical. This involves exploring cryptographic techniques that minimize computational overhead without compromising data confidentiality and integrity. For example, Elliptic Curve Cryptography (ECC) provides a modern solution for resource-constrained devices by offering strong encryption with smaller key sizes, which is ideal for devices such as smart sensors used in industrial applications.

(b) Efficient IDS for IoT/IIoT: The heterogeneity and scale of IoT/IIoT networks make traditional IDS approaches insufficient. Research is required to design adaptive and scalable IDS solutions that can detect and respond to sophisticated threats in real-time. Techniques such as machine learning and anomaly detection can play a pivotal role in achieving this goal. For instance, as autonomous IIoT systems increase in complexity, anomaly-based IDS powered by machine learning algorithms can detect new or unknown attack patterns, which traditional signature-based methods might miss.

(c) Intrusion detection for Industry 4.0/5.0: As industries transition toward Industry 4.0 and beyond, the complexity of interconnected systems increases. These environments demand intrusion detection mechanisms tailored to specific industrial processes, integrating predictive analytics to anticipate and mitigate threats proactively. For example, in autonomous manufacturing systems, an attack targeting control systems can have major consequences. Thus, security mechanisms must detect abnormal behavior in real-time and respond to prevent disruptions or damage.

(d) Domain-specific sophisticated attack prevention: IoT/IIoT applications span diverse domains, including healthcare, manufacturing, and transportation, each with distinct security requirements. Research into domain-specific attack prevention strategies that leverage contextual awareness and customized security policies is essential to ensure comprehensive protection. For instance, in the medical field, healthcare IoT devices, such as wearable health monitors, necessitate particular security measures to protect the sensitivity of the processed data. On the other hand, every specific domain can adopt particular solutions to obtain stronger protection against targeted threats.

Based on the practical of IoT/IIoT security, it has recognized some different gaps and limitations such as:

(a) The lack of standardization among universal IoT/IIoT security standards from different manufacturers often results in interoperability issues in security implementations. The main research direction is to develop standardized protocols and frameworks that ensure consistency and compatibility across diverse ecosystems.

(b) Limited context-aware solutions, to adapt solutions to the specific operational conditions and threat landscapes. For instance, adaptive encryption schemes can be developed to enhance both security and performance.

(c) Insufficient scalability of the security solutions to accommodate the fast proliferation of IoT/IIoT devices. Future research should develop scalable architectures that can support billions of interconnected devices without decreasing their performance.

(d) Resource constraints due to the implementation of traditional security mechanisms on modern IoT/IIoT devices restrict the innovation in lightweight security techniques and efficient algorithms.

(e) The dynamic evolving cyber threat landscape necessitates a modern, novel, and continuous adaptation of security measures to detect and mitigate unknown attacks in autonomous IIoT systems.

These challenges highlight the complexities of IIoT security and demonstrate the need for continuous research and innovation to address evolving security needs and protect the growing ecosystem of interconnected devices.

Advancements in lightweight security algorithms, efficient intrusion detection methods, and robust countermeasures will play a pivotal role in enhancing the security and reliability of interconnected IoT/IIoT systems. As researchers continue to explore these domains, collaboration among academia, industry, and policymakers will be essential in shaping the future of secure IoT/IIoT ecosystems.

8. Conclusions

The article's primary objective is to present a holistic perspective on IoT/IIoT security, emphasizing the anticipation of potential attacks, the implementation of appropriate countermeasures, and the identification of limitations through well-considered solutions. By proposing an architectural framework tailored to address these challenges, particularly within industrial contexts, the work highlights the importance of a comprehensive, multi-layered approach to security. This approach integrates advanced security practices, adaptability to dynamic threat landscapes, and collaboration between academia, industry, and policymakers to build resilient and secure IoT/IIoT systems. As the IoT/IIoT ecosystem continues to expand, it is crucial to prioritize the development of adaptive, scalable, and proactive security mechanisms. These mechanisms must respond to emerging threats while ensuring the privacy and safety of connected systems. The integration of cutting-edge technologies, along with effective governance and regulation, will be pivotal in maintaining the integrity, confidentiality, and availability of critical infrastructures and services. Ultimately, this approach not only mitigates current security risks but also prepares IoT/IIoT environments for future challenges, ensuring their continued reliability and trustworthiness in an increasingly interconnected world.

List of Abbreviations

AES	Advanced Encryption Standard
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
CoAP	Constrained Application Protocol
DoS	Denial of Service
DDoS	Distributed Denial of Service
ECC	Elliptic Curve Cryptography
HTTP/ HTTPS	Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure
IDS	Intrusion Detection Systems
IDPS	Intrusion Detection and Prevention Systems
IIoT	Industrial Internet of Things
IPS	Intrusion Prevention Systems
IoT	Internet of Things
LoRaWAN	Long Range Wide Area Network
MFA	Multi-Factor Authentication
MitM	Man-in-the-Middle
MQTT	Message Queuing Telemetry Transport
NB-IoT	Narrowband Internet of Things
OPC-UA	Open Platform Communications Unified Architecture
RESTful APIs	Representational State Transfer APIs
SIMD	Single Instruction, Multiple Data
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
XMPP	Extensible Messaging and Presence Protocol
XSS	Cross-Site Scripting

Author Contributions

The author confirms sole responsibility for the conception, design, literature review, analysis, interpretation, manuscript drafting, visualization, critical revisions, and final approval of the article.

Conflicts of Interest

The author declares no conflict of interest.

Funding

No external funding was received for this research.

Acknowledgments

Nothing to acknowledge.

AI Declaration

The author confirms that no content in this manuscript was generated using artificial intelligence (AI) tools and that the author takes full responsibility for the accuracy and integrity of the work.

References

[1] T. Kramp, R. van Kranenburg, and S. Lange, "Introduction to the internet of things," in *Enabling Things to Talk*, A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. van Kranenburg, S. Lange, and S. Meissner, Eds., Berlin/Heidelberg: Springer, 2013. [CrossRef]

[2] H. Tran-Dang, N. Krommenacker, P. Charpentier, and D. S. Kim, "Toward the Internet of Things for physical internet: Perspectives and challenges," *IEEE Internet Things J.*, vol. 7, pp. 4711–4736, 2020. [CrossRef]

[3] M. Ţălu, "Innovation in scalability: Event-driven autoscaling in Kubernetes," *Today Softw. Mag.*, vol. 139, 2024. [View Online]

[4] R. Dallaev, T. Pisarenko, Ş. Ţălu, D. Sobola, J. Majzner, and N. Papež, "Current applications and challenges of the Internet of Things," *New Trends Comput. Sci.*, vol. 1, no. 1, pp. 51–61, 2023. [CrossRef]

[5] K. M. Hou, X. Diao, H. Shi, H. Ding, H. Zhou, and C. de Vaulx, "Trends and challenges in AIoT/IIoT/IoT implementation," *Sensors*, vol. 23, no. 11, 2023, Art. no. 5074. [CrossRef] [PubMed]

[6] H. Yu, J. He, R. Liu, and D. Ji, "On the security of data collection and transmission from wireless sensor networks in the context of Internet of Things," *Int. J. Distrib. Sens. Netw.*, vol. 2013, no. 9, 2013, Art. no. 806505. [CrossRef]

[7] M. Girard, "Standards for cybersecure IoT devices: A way forward," CIGI Policy Brief No. 160, Centre for International Governance Innovation, Waterloo, ON, Canada, Jul. 15, 2020. [Online]. Available: https://www.cigionline.org/publications/standards-cybersecure-iot-devices-way-forward/

[8] M. Ţălu, "Exploring IoT applications for transforming university education: Smart classrooms, student engagement, and innovations in teacher and student-focused technologies, " *Bul. Ilm. Sarj. Tek. Elektro.*, vol. 7, no. 1, pp. 9–29, 2025. [CrossRef]

[9] A. Nazarov, D. Nazarov, and Ş. Ţălu, "Information security of the Internet of Things," in *Proc. Int. Sci. Pract. Conf. Comput. Inf. Secur. (INFSEC 2021)* (SCITEPRESS—Science and Technology Publications, Lda, vol. 1), Yekaterinburg, Russia, 2021, pp. 136–139. [CrossRef]

[10] S. P. Kumar, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and solutions survey," *Sensors*, vol. 22, no. 19, 2022, Art no. 7433. [CrossRef]

[11] S. H. Mekala, Z. Baig, A. Anwar, and S. Zeadally, "Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions," *Comput. Commun.*, vol. 208, pp. 294–320, 2023. [CrossRef]

[12] N. Mishra and S. Pandya, "Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," *IEEE Access*, vol. 9, pp. 59353–59377, 2021. [CrossRef]

[13] Ş. Ţălu, "Strategic measures in improving cybersecurity management in micro and small enterprises," in *Proc. 2nd Int. Sci. and Pract. Conf. on Digital Economy (ISCDE)*, Yekaterinburg, Russia, Nov. 5–6, 2020, Adv. Econ. Bus. Manag. Res., vol. 156, pp. 522–528, 2020. [CrossRef]

[14] L. Logrippo, "Multi-level models for data security in networks and in the Internet of things," *J. Inf. Secur. Appl.*, vol. 58, 2021, Art. no. 102778. [CrossRef]

[15] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors*, vol. 20, 2020, Art. no. 3625. [CrossRef] [PubMed]

[16] T. Bányai, Á. Bányai, and I. Kaczmar, Eds., *Supply Chain—Recent Advances and New Perspectives in the Industry 4.0 Era*. London, UK: IntechOpen Limited, 2022. [CrossRef]

[17] M. C. Zizic, M. Mladineo, N. Gjeldum, and L. Celent, "From industry 4.0 towards industry 5.0: A review and analysis of paradigm shift for the people, organization and technology," *Energies*, vol. 15, 2022, Art. no. 5221. [CrossRef]

[18] H. R. Chi, C. K. Wu, N. F. Huang, K. F. Tsang, and A. Radwan, "A survey of network automation for Industrial Internet-of-Things toward Industry 5.0," *IEEE Trans. Industr. Inform.*, vol. 19, no. 2, pp. 2065–2077, 2023. [CrossRef]

[19] M. Golovianko, V. Terziyan, V. Branytskyi, and D. Malyk, "Industry 4.0 vs. Industry 5.0: Co-existence, transition, or a hybrid," *Procedia Comput. Sci.,* vol. 217, pp. 102–113, 2023. [CrossRef]

[20] P. Thakur and V. K. Sehgal, "Emerging architecture for heterogeneous smart cyber-physical systems for industry 5.0," *Comput. Ind. Eng.*, vol. 162, 2021. [CrossRef]

[21] A. Nasr, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, "Internet of Things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications," *Sensors*, vol. 21, no. 11, 2021, Art. no. 3654. [CrossRef] [PubMed]

[22] T. S. Fun and A. Samsudin, "Recent technologies, security countermeasure and ongoing challenges of In-

dustrial Internet of Things (IIoT): A survey," *Sensors*, vol. 21, no. 19, 2021, Art. no. 6647. [CrossRef] [PubMed]

[23] S. P. Singh et al., "Cyber security and 5G-assisted Industrial Internet of Things using novel artificial adaption based evolutionary algorithm," *Mobile Netw. Appl.*, vol. 30, pp. 42–58, 2025. [CrossRef]

[24] A. Hani, A. Khan, M. Rizwan, M. S. A. Reshan, A. Sulaiman, and A. Shaikh, "Intrusion detection framework for Industrial Internet of Things using software defined network," *Sustainability*, vol. 15, no. 11, 2023, Art. no. 9001. [CrossRef]

[25] K. Bansal and A. Singhrova, "Review on intrusion detection system for IoT/IIoT -brief study," *Multimed. Tools Appl.*, vol. 83, pp. 23083–23108, 2024. [CrossRef]

[26] T. Gueye, Y. Wang, and M. Rehman, "A novel method to detect cyber-attacks in IoT/IIoT devices on the modbus protocol using deep learning," *Cluster Comput.*, 2023. [CrossRef]

[27] M. Younan, E. H. Houssein, M. Elhoseny, and A. A. Ali, "Challenges and recommended technologies for the industrial internet of things: A comprehensive review," *Measurement*, vol. 151, 2020. [CrossRef]

[28] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, 2020, Art. no. 102481. [CrossRef]

[29] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, and Z. Zou, "A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things," *J. Ind. Inf. Integr.*, vol. 21, 2021. [CrossRef]

[30] G. Rathee, F. Ahmad, R. Sandhu, C. A. Kerrache, and M. A. Azad, "On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things," *Inf. Process Manag.*, vol. 58, 2021. [CrossRef]

[31] F. Ali and S. Mathew, "An efficient multilevel security architecture for blockchain-based IoT networks using principles of cellular automata," *PeerJ Comput. Sci.*, vol. 8, 2022, Art. no. e989. [CrossRef]

[32] M. H. Ali, M. M. Jaber, S. K. Abd, A. Alkhayyat, R. Q. Malik, and M. Hussain Ali, "Application of Internet of Things based efficient security solution for industrial," *Prod. Plan. Control.,* 2023. [CrossRef]

[33] D. G. Darwish, "Improved layered architecture for Internet of Things," *IJCAR*, vol. 4, no. 4, pp. 214–223, 2015. [View Online]

[34] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A systematic survey of Industrial Internet of Things security: Requirements and fog computing opportunities," *IEEE Commun. Surv. Tutor.*, vol. 22, 2020. [CrossRef]

[35] X. Jiang, M. Lora, and S. Chattopadhyay, "An experimental analysis of security vulnerabilities in industrial IoT devices," *ACM Trans. Internet Technol.*, vol. 20, 2020. [CrossRef]

[36] R. Kaksonen, K. Halunen, and J. Röning, "Vulnerabilities in IoT Devices, Backends, Applications, and Components," in *Proc. 9th Int. Conf. Inf. Syst. Secur. Priv. Vol. 1: ICISSP*, pp. 659–668, 2023. [CrossRef]

[37] J. Ferdous, R. Islam, A. Mahboubi, and M. Z. Islam, "A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms," *IEEE Access*, vol. 11, pp. 121118–121141, 2023. [CrossRef]

[38] D. Teng, "Industrial Internet of Things anti-intrusion detection system by neural network in the context of Internet of Things for privacy law security protection," *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–17, 2022. [CrossRef]

[39] H. Shahid, H. Ashraf, H. Javed, M. Humayun, N. Jhanjhi, and M. A. AlZain, "Energy optimised security against wormhole attack in IoT-based wireless sensor networks," *Comput. Mater. Contin.*, vol. 68, pp. 1967–1981, 2021. [CrossRef]

[40] U. Narayanan, V. Paul, and S. Joseph, "Decentralized blockchain based authentication for secure data sharing in Cloud-IoT: DeBlock-Sec," *J. Ambient Intell. Humaniz. Comput.*, vol. 13, pp. 769–787, 2021. [CrossRef]

[41] M. I. Ahmed, and G. Kannan, "Cloud-based remote RFID authentication for security of smart Internet of Things applications," *J. Inf. Knowl. Manag.*, vol. 20, 2021, Art. no. 2140004. [CrossRef]

[42] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021. [CrossRef]

[43] K. S. Mohamed, *The Era of Internet of Things*. Cham: Springer Nature Switzerland AG, 2019. [CrossRef]

[44] S. Sivagurunathan and V. M. Ganeshan, "Lightweight cryptography (LWC) algorithms in terms of software metrics for Industrial Internet of Things (IIoT)," *Adv. Appl. Math. Sci.*, vol. 22, no.1, pp. 127–137, 2022. [View Online]

Disclaimer/Publisher's Note: The views expressed in this article are those of the author(s) and do not necessarily reflect the views of the publisher or editors. The publisher and editors assume no responsibility for any injury or damage resulting from the use of information contained herein.