International Journal of Future Engineering Innovations

Cybersecurity Strategies for Integrating Industrial IoT and Edge Computing: Challenges, Risks, and Future Perspectives

Oluwafemi Alabi Okunlola [1*], Jelil Olaoye [2], Okunlola Olalekan Samuel [3], Adeola Oluwaseyi Okunlola [4], Opeyemi Alao [5]
[1, 5] Department of Management Information Systems (MIS), Lamar University Beaumont Texas, USA
[2] Department of Applied Physical Science, Environmental Science Concentration, Georgia Southern University, Georgia, USA
[3] Department of Mechanical and material Engineering, University of Cincinnati, Ohio USA
[4] Department of Science laboratory technology, Ladoke Akintola University of Technology, Nigeria

* Corresponding Author: **Oluwafemi Alabi Okunlola**

Article Info

ISSN (online): 3049-1215
Volume: 02
Issue: 02
March-April 2025
Received: 06-02-2025
Accepted: 07-03-2025
Page No: 87-95

Abstract
The integration of Industrial Internet of Things (IIoT) with edge computing has revolutionized industrial sectors by enabling real-time data processing, improved automation, and enhanced operational efficiency. However, this convergence introduces a complex cybersecurity landscape due to the increased attack surfaces and vulnerabilities at the device, network, and edge layers. This review explores the cybersecurity challenges and threats associated with the integration of IIoT and edge computing, focusing on the unique vulnerabilities of these systems, including device-level attacks, data breaches, and threats targeting the edge infrastructure. We examine current cybersecurity solutions tailored for IIoT edge environments, such as authentication protocols, encryption mechanisms, intrusion detection systems, and secure firmware management. Additionally, we highlight the key challenges in securing such systems, including the heterogeneity of devices, resource constraints, and the lack of standardized security frameworks. The paper also discusses emerging trends in cybersecurity for IIoT and edge computing, such as the application of artificial intelligence for threat detection, the role of blockchain for decentralized trust, and the adoption of zero trust architectures. Finally, we outline future directions for research and development in this field, emphasizing the need for scalable, lightweight, and resilient security frameworks that can evolve with the growing complexity of IIoT–edge systems.

DOI: https://doi.org/10.54660/IJFEI.2025.2.2.87-95

Keywords: Industrial Internet of Things (IIoT), Edge Computing, Cybersecurity, Edge Security, Threats and Vulnerabilities

1. Introduction

The Industrial Internet of Things (IIoT) is transforming the landscape of industrial automation by providing a platform for interconnected devices and systems. By leveraging sensors, actuators, and communication networks, IIoT facilitates real-time monitoring and control of industrial processes, leading to enhanced efficiency, reduced downtime, and predictive maintenance (Zanella *et al*., 2014) [33]. The IIoT ecosystem is typically composed of numerous heterogeneous devices that communicate over diverse protocols, each contributing to the complexity of the system. With these advancements, edge computing has emerged as a critical enabler, allowing data processing to occur closer to the source rather than relying solely on centralized cloud computing systems (Shi *et al*., 2016) [25]. Edge computing helps address challenges such as high latency, bandwidth limitations, and real-time decision-making requirements in IIoT applications (Ahmed *et al*., 2020) [1]. However, the integration of IIoT with edge computing presents significant cybersecurity challenges due to the distributed nature of both technologies, creating an expanded attack surface for cyber threats (Alaba *et al*., 2017) [2].

As industries adopt IIoT and edge computing, they are increasingly exposed to a wide range of security risks. Unlike traditional IT systems, IIoT networks are deeply embedded in physical environments and often control critical infrastructure, such as power grids, manufacturing lines, and transportation systems. As such, the consequences of cyberattacks targeting IIoT systems are severe, potentially leading to physical damage, production disruptions, and safety risks (Pawlowski *et al*., 2019) [21]. The cybersecurity concerns associated with IIoT–edge integration are particularly acute due to the decentralized nature of edge computing, which often operates in environments with limited resources and may not benefit from the robust security protocols typically implemented in centralized systems (Haleem & Raza, 2020) [11]. In this context, securing IIoT–edge infrastructures becomes a complex and multifaceted challenge that involves not only traditional security measures but also new strategies tailored to the unique characteristics of these technologies.

The primary objective of this review is to examine the cybersecurity challenges and solutions related to the integration of IIoT and edge computing. We will explore various threats and vulnerabilities inherent in IIoT–edge systems, including attacks targeting devices, networks, and data integrity. A key area of focus is the development of cybersecurity solutions designed to address these challenges, such as secure communication protocols, device authentication, data encryption, and intrusion detection mechanisms (Tang *et al*., 2018) [27]. In addition, this review will discuss emerging trends, such as the use of artificial intelligence (AI) and machine learning (ML) for threat detection, the application of blockchain for secure data sharing, and the adoption of zero trust architectures, all of which hold significant potential for enhancing the security posture of IIoT–edge systems (Nugent *et al*., 2020; Dinh *et al*., 2020) [20]. Furthermore, the review will identify key challenges, such as the scalability and resource limitations of security mechanisms at the edge, which hinder the widespread adoption of robust cybersecurity solutions.

The increasing complexity of IIoT–edge systems, coupled with the rapid growth in connected devices, calls for a comprehensive and dynamic approach to cybersecurity. Existing research primarily focuses on either IIoT security or edge computing security in isolation, but the integration of both technologies requires a more holistic view of the threat landscape (Xie *et al*., 2019) [30]. This review aims to bridge this gap by providing a thorough analysis of the security issues specific to IIoT–edge integration, discussing both current solutions and future directions in the field. The ultimate goal is to provide insights into the cybersecurity challenges faced by industrial sectors and offer practical solutions to safeguard IIoT systems and edge computing infrastructures.

As industries continue to evolve and integrate advanced technologies such as artificial intelligence, big data analytics, and automation, the need for resilient and adaptive cybersecurity solutions becomes ever more pressing. A failure to secure IIoT–edge infrastructures could have disastrous consequences, not only in terms of financial loss but also in terms of national security and public safety. Hence, ensuring the security of IIoT systems is no longer optional but essential for the sustainable and safe deployment of modern industrial systems (Brzozowski *et al*., 2018) [4]. Given the fast-paced development of both IIoT and edge computing technologies, continuous research and development in cybersecurity are critical to addressing the evolving threat landscape.

2. Literature Review and Background Concepts

2.1 Industrial Internet of Things (IIoT)

The Industrial Internet of Things (IIoT) refers to the application of IoT technologies in industrial environments, connecting machines, sensors, actuators, and other devices to facilitate real-time data collection, processing, and decision-making (Zanella *et al*., 2014) [33]. IIoT enables industries such as manufacturing, energy, and transportation to optimize their operations through intelligent automation, predictive maintenance, and enhanced monitoring. At the heart of IIoT are key components, including connected devices (sensors and actuators), communication networks, data analytics systems, and control systems. These components work together to collect data from industrial assets and enable efficient decision-making (Miorandi *et al*., 2012) [19].

A crucial feature of IIoT is its reliance on communication protocols that ensure seamless data exchange between devices and systems. Protocols like MQTT (Message Queuing Telemetry Transport) and OPC UA (Open Platform Communications Unified Architecture) play a vital role in enabling efficient, lightweight communication in industrial environments (Tao *et al*., 2018) [28]. MQTT, for example, is a publish-subscribe protocol that minimizes bandwidth usage and latency, making it ideal for environments with constrained resources (Liu *et al*., 2017) [15]. OPC UA, on the other hand, provides a platform-independent architecture for interoperability among diverse devices, ensuring secure and reliable data exchange between industrial systems (Kouadio *et al*., 2020) [13].

IIoT finds application across a wide range of use cases, including predictive maintenance, asset tracking, and process automation. Predictive maintenance leverages real-time data collected from sensors to predict equipment failures and minimize unplanned downtimes (Lee *et al*., 2015) [14]. Asset tracking enables industries to monitor the location and status of physical assets in real-time, ensuring optimal resource utilization (Gubbi *et al*., 2013) [10]. Process automation uses IIoT technologies to automate repetitive tasks, leading to enhanced productivity, improved quality, and reduced human error (Chien *et al*., 2017). As these use cases demonstrate, IIoT is crucial to optimizing industrial operations, but it also introduces significant cybersecurity challenges, especially when integrated with edge computing.

2.2. Edge Computing in IIoT

Edge computing has emerged as a key enabler of IIoT, addressing several challenges associated with cloud computing, such as high latency, bandwidth limitations, and real-time data processing (Shi *et al*., 2016) [25]. In traditional cloud computing, data is sent to centralized data centers for processing, which can result in significant delays in critical applications. In contrast, edge computing brings data processing closer to the source—at the "edge" of the network, typically on devices such as gateways, routers, or even sensors themselves (Zhang *et al*., 2019) [29]. This proximity reduces latency, enabling real-time decision-making, which is essential for time-sensitive industrial applications such as automated control, robotics, and smart grid management (Ahmed *et al*., 2020) [1].

Edge computing architecture in IIoT is typically hierarchical

and decentralized. In this architecture, edge devices (such as industrial gateways or edge servers) are responsible for processing and analyzing data locally before sending it to the cloud or centralized systems. This decentralized approach alleviates bandwidth congestion by filtering and processing data at the edge, ensuring that only relevant or aggregated information is transmitted to the cloud (Cao *et al*., 2018) [5]. The edge architecture often incorporates several key components, such as sensors, data aggregation systems, and local processing units, which together ensure the efficient collection and processing of data in real-time (Zhao *et al*., 2020) [34].

Edge computing is particularly beneficial in IIoT for several reasons. First, it enables local data processing, which significantly reduces the latency involved in transmitting data to remote data centers. This is especially critical in applications where decisions must be made instantaneously, such as in automated manufacturing lines or smart grid operations (Shi *et al*., 2016) [25]. Second, by processing data locally, edge computing alleviates the strain on cloud infrastructure, ensuring that the network can handle more devices and more data streams. Lastly, edge computing enhances privacy and security by reducing the amount of sensitive data that needs to be transmitted to the cloud, making it less susceptible to interception or tampering (Khan *et al*., 2020) [12]. However, integrating edge computing with IIoT also introduces additional security complexities, as edge devices themselves become potential targets for cyberattacks.

2.3. Cybersecurity Basics in IIoT Context

The integration of IIoT and edge computing necessitates robust cybersecurity measures due to the increased attack surface and complexity of these systems. Cybersecurity in IIoT focuses on protecting critical industrial systems from unauthorized access, ensuring data integrity, and maintaining the availability of devices and networks. The core principles of cybersecurity—often referred to as the CIA triad are essential in the IIoT context: Confidentiality, Integrity, and Availability (Stallings, 2013). Confidentiality ensures that data is accessible only to authorized users, preventing unauthorized entities from accessing sensitive industrial information. Integrity guarantees that data remains unaltered during transmission or storage, thus preventing malicious actors from tampering with operational data. Availability ensures that IIoT systems remain operational and accessible, preventing disruptions due to cyberattacks.

In IIoT systems, cybersecurity is implemented across multiple layers, from device security to network security and application security. At the device layer, ensuring the security of individual sensors, actuators, and other connected devices is paramount. These devices must be authenticated, encrypted, and capable of securely transmitting data (Tao *et al*., 2018) [28]. At the network layer, securing communication protocols such as MQTT and OPC UA becomes critical to prevent data interception or unauthorized access (Zhou *et al*., 2020) [35]. At the application layer, security measures include the use of intrusion detection systems (IDS), firewalls, and secure application design to mitigate the risk of attacks such as denial-of-service (DoS) and man-in-the-middle attacks (Wang *et al*., 2019) [29].

The threat models for IIoT systems are diverse and evolving. Common threats include device-based attacks, data breaches, and network-based attacks. Device-based attacks involve compromising individual devices, such as sensors, to manipulate data or gain unauthorized access to the network. Data breaches occur when unauthorized entities access sensitive data, often leading to industrial espionage or the sabotage of critical infrastructure. Network-based attacks, such as DoS or Distributed Denial of Service (DDoS) attacks, can overwhelm industrial networks, disrupting operations and causing downtime (Xu *et al*., 2020) [31]. Additionally, as edge devices play a central role in IIoT systems, the security of edge devices is becoming increasingly important, as they are often deployed in less secure environments and are more vulnerable to physical tampering or software vulnerabilities (Cao *et al*., 2018) [5].

cybersecurity is a fundamental concern in IIoT systems, particularly when integrated with edge computing. The decentralized nature of edge computing introduces new security challenges that require the development of tailored solutions to address the unique threats and vulnerabilities of IIoT–edge architectures. By understanding the basic concepts of IIoT, edge computing, and cybersecurity, stakeholders can better design and implement secure systems that ensure the safety and integrity of industrial operations.

3. Discussion

3.1 Cybersecurity Threat Landscape

The cybersecurity threat landscape for Industrial Internet of Things (IIoT) and edge computing is complex and continually evolving, as these systems are increasingly becoming targets for a wide array of cyberattacks. IIoT systems, which integrate physical devices with digital infrastructures, present an attractive target for malicious actors due to their critical role in industrial operations. The convergence of IIoT and edge computing further complicates the security challenges, as the edge devices and networks involved are often deployed in less secure, distributed environments, increasing the risk of exposure to external and internal threats (Pawlowski *et al*., 2019) [21]. Moreover, the decentralized nature of edge computing means that data is processed at multiple locations, making it more difficult to maintain consistent security measures across the entire system.

One of the primary threats facing IIoT systems is unauthorized access to critical devices and networks. Cybercriminals may exploit vulnerabilities in edge devices, gateways, or communication protocols to gain access to industrial systems (Xie *et al*., 2019) [30]. Once inside the system, attackers can manipulate data, disrupt operations, or even take control of critical infrastructure. Denial-of-service (DoS) attacks, including more sophisticated distributed denial-of-service (DDoS) attacks, are particularly concerning for IIoT networks. These attacks aim to overwhelm network resources, rendering them unavailable for legitimate users and potentially causing widespread operational failures (Zhou *et al*., 2020) [35]. Given the importance of uptime in industrial systems, such attacks can result in significant financial losses, safety risks, and damage to the organization's reputation.

Data breaches and information leakage are also prominent threats in IIoT systems. Sensitive industrial data, such as production metrics, equipment status, and maintenance schedules, is often transmitted over unsecured channels or stored in devices with insufficient protection, making it susceptible to interception or unauthorized access. These breaches could lead to intellectual property theft, sabotage of industrial processes, or espionage by competitors or state-

sponsored actors (Brzozowski *et al*., 2018) [4]. Additionally, man-in-the-middle (MITM) attacks, where attackers intercept and alter communications between devices, are a significant concern, especially in IIoT networks relying on protocols like MQTT or OPC UA, which could be vulnerable if not properly secured (Tao *et al*., 2018) [28].

The physical security of IIoT devices is another critical concern. Many edge devices are deployed in remote or hard-to-secure locations, making them vulnerable to physical tampering. Attackers can physically access devices, modify them, or insert malware to gain control of the system. Such attacks can be particularly dangerous in industries like energy or transportation, where tampering with equipment could have far-reaching consequences, including safety hazards and catastrophic damage to infrastructure (Haleem & Raza, 2020) [11]. Similarly, supply chain attacks are a growing risk, where attackers target vendors or third-party suppliers that provide hardware or software components for IIoT systems. Compromising these vendors can provide attackers with a backdoor into otherwise secure systems (Alaba *et al*., 2017) [2].

A key challenge in defending IIoT systems lies in the heterogeneity of the devices and technologies involved. IIoT environments consist of a wide variety of devices, ranging from legacy equipment with outdated security features to modern, highly advanced sensors and actuators. This diversity creates an inconsistent security posture, with some devices potentially having weak or non-existent security measures, making them vulnerable to exploitation (Miorandi *et al*., 2012) [19]. Moreover, the resource constraints of many edge devices, such as limited processing power, memory, and storage, prevent the implementation of traditional, heavy-duty security mechanisms like encryption or intrusion detection systems (IDS) (Xie *et al*., 2019) [30]. Consequently, these devices are more prone to attacks that exploit these limitations, including buffer overflow attacks, unauthorized code execution, and side-channel attacks.

In addition to these direct threats, insider threats remain a serious concern in IIoT systems. Disgruntled employees, contractors, or other trusted individuals may exploit their knowledge of the network and systems to carry out malicious actions, such as stealing data, altering control systems, or causing equipment malfunctions (Xu *et al*., 2020) [31]. These types of attacks are difficult to detect because the perpetrators often have legitimate access to critical resources and know how to bypass standard security defenses. As industries increasingly rely on third-party vendors and contractors for system integration and maintenance, the risk of insider threats grows, making it crucial to implement strict access controls and continuous monitoring.

Furthermore, ransomware attacks are becoming more prevalent in IIoT systems, as attackers target critical industrial infrastructure and demand payment for restoring access to locked systems. Ransomware attacks have already disrupted operations in various industries, including manufacturing, healthcare, and energy, by encrypting important files and demanding a ransom to decrypt them. Such attacks can lead to prolonged downtime, financial losses, and significant reputational damage (Zhao *et al*., 2020) [34]. The rise in ransomware is particularly concerning in IIoT systems, where downtime or system failure can result in not only financial loss but also the jeopardizing of public safety and environmental risks.

Lastly, emerging threats related to artificial intelligence (AI) and machine learning (ML) also present new challenges for IIoT cybersecurity. AI and ML algorithms, while offering immense potential for improving operational efficiencies, can also be weaponized by attackers to launch highly sophisticated attacks. For example, attackers may use AI to create more advanced phishing schemes, exploit vulnerabilities, or automate attacks at scale (Nugent *et al*., 2020) [20]. As IIoT and edge computing systems increasingly incorporate AI-driven applications, securing these technologies against malicious use becomes critical to prevent automated cyberattacks that could scale rapidly and be more difficult to detect.

The threat landscape for IIoT and edge computing is vast and varied, encompassing both traditional cyber threats and new, emerging risks. The convergence of these technologies has created new vulnerabilities, especially at the edge, where devices may be more easily compromised due to limited resources, insecure communications, and physical exposure. As the adoption of IIoT and edge computing continues to grow, industries must prioritize the development of advanced cybersecurity strategies that account for these evolving threats. This includes securing devices, ensuring robust network protection, adopting new threat detection technologies, and fostering a culture of continuous monitoring and response to emerging threats.

3.2. Current Cybersecurity Solutions

Authentication & Access Control

Authentication and access control are foundational components of any cybersecurity strategy in IIoT systems, as they help ensure that only authorized users and devices can access sensitive industrial resources. Role-based access control (RBAC) is one of the most common methods for managing access in IIoT environments. RBAC assigns permissions based on the roles users hold within an organization, limiting access to critical systems according to job responsibilities. This approach ensures that only authorized personnel can perform certain actions or access particular data, reducing the risk of insider threats and unauthorized access. However, in IIoT systems, especially those operating in dynamic and large-scale environments, RBAC may not be sufficient on its own, as the risk of cyber threats increases with the complexity of the network.

To bolster access control, multi-factor authentication (MFA) is becoming increasingly common in industrial systems (Chen *et al*., 2020) [6]. MFA requires users to provide multiple forms of identification—such as a password, a biometric scan, or a hardware token—before being granted access to a system. This greatly enhances security by ensuring that unauthorized users, even if they manage to compromise one factor (e.g., a password), cannot easily gain access. MFA is particularly vital in IIoT systems where remote management and access are often required, and devices are interconnected across geographically dispersed locations. By combining multiple verification factors, MFA provides a higher level of assurance that only legitimate users can interact with critical systems and data.

Data Security

The protection of data in IIoT systems is essential, as these systems often handle sensitive and proprietary information. Encryption is a core technique used to safeguard data both at rest and in transit. End-to-end encryption (E2EE) ensures that data is encrypted on the sender's side and decrypted only by

the intended recipient, protecting it from eavesdropping and tampering (Xu *et al*., 2020) [31]. In IIoT systems, this is particularly important due to the vast amounts of data transmitted between devices, edge nodes, and centralized systems. Data encryption can prevent unauthorized access to sensitive industrial data, such as production metrics or equipment status, reducing the risk of data breaches and espionage.

Alongside encryption, secure data transmission protocols are critical for safeguarding communication between devices, edge nodes, and cloud servers. For example, protocols like Transport Layer Security (TLS) and Secure Sockets Layer (SSL) provide encryption for data transmitted over networks (Liu *et al*., 2017) [15]. By employing these secure transmission protocols, IIoT systems can mitigate the risk of data interception or modification while the data is being transmitted. Furthermore, data integrity checks—such as the use of hashing algorithms—can verify that the data has not been altered during transmission, ensuring that the data received by the recipient is exactly as it was sent.

Network Security

Network security plays a crucial role in protecting IIoT systems from external threats, such as cyberattacks targeting vulnerabilities in the communication infrastructure. Intrusion Detection Systems (IDS) are commonly deployed to monitor network traffic for signs of malicious activity. These systems use both signature-based and anomaly-based detection techniques to identify unauthorized or suspicious activity (Alazab *et al*., 2019) [3]. Signature-based IDS can detect known attack patterns by comparing network traffic against a database of predefined signatures, while anomaly-based IDS can identify deviations from normal network behavior, helping to detect previously unknown or evolving threats. IDS can be deployed both at the edge and at central network points to enhance the overall security posture.

Firewalls also play a significant role in IIoT network security by establishing perimeter defense mechanisms that filter incoming and outgoing traffic based on predefined rules (Zhou *et al*., 2020) [35]. Firewalls can be used to block unauthorized devices from accessing industrial networks and prevent malicious traffic from penetrating critical systems. Additionally, Software-Defined Networking (SDN)-based solutions are gaining traction in industrial environments due to their ability to provide dynamic and flexible control over network traffic. SDN can enable real-time threat detection and network segmentation, isolating compromised network segments from the rest of the system to limit the scope of an attack (Mahmood *et al*., 2018) [17]. By leveraging SDN, IIoT systems can adapt quickly to emerging threats and ensure network resilience.

Device & Firmware Security

Securing the devices themselves is critical to the overall security of IIoT systems. **Secure boot** is one of the most effective methods for ensuring that only trusted firmware is executed on IIoT devices. During the boot process, the device verifies the integrity of the firmware before allowing it to run, preventing malicious code or unauthorized firmware from being loaded (Yang *et al*., 2019) [32]. This process is essential in preventing attacks that aim to compromise IIoT devices at the firmware level, which could lead to the manipulation of device behavior or unauthorized access to the broader network.

Over-the-Air (OTA) updates are also critical for maintaining the security of IIoT devices over time. These updates allow manufacturers to remotely patch security vulnerabilities or update device firmware to mitigate newly discovered threats. OTA updates provide an efficient mechanism for keeping IIoT systems secure without requiring physical access to devices, which is especially valuable in environments where devices are distributed across large geographic areas (Sicari *et al*., 2018) [26]. However, OTA updates must be secured to prevent attackers from intercepting and injecting malicious firmware during the update process, which could compromise the entire device fleet.

Finally, the integration of Trusted Platform Modules (TPM) in IIoT devices adds another layer of security by providing hardware-based protection for cryptographic keys, credentials, and other sensitive data (Santos *et al*., 2020) [24]. TPM chips can securely store private keys and perform cryptographic operations, ensuring that even if a device is physically compromised, the sensitive data remains protected.

Edge-Specific Solutions

The decentralized nature of edge computing in IIoT environments introduces unique security challenges, as edge devices often operate in environments with limited resources and are more exposed to physical tampering. To address these challenges, lightweight encryption techniques are being developed to ensure that data can be securely processed and transmitted even in resource-constrained edge devices. These techniques minimize the computational overhead typically associated with encryption, allowing edge devices to maintain performance while ensuring the confidentiality and integrity of the data (Xu *et al*., 2020) [31]. Lightweight encryption algorithms, such as Elliptic Curve Cryptography (ECC), provide strong security with minimal computational requirements, making them ideal for IIoT edge devices.

In addition to lightweight encryption, edge-based Intrusion Detection Systems (IDS) are increasingly being deployed to monitor local network traffic and detect potential security threats at the edge. Edge IDS can provide faster detection and response times by processing data locally, reducing the need for data to be sent to the cloud or central servers for analysis (Liu *et al*., 2019) [30]. These systems can help identify suspicious behavior or attacks before they spread throughout the entire network, providing an additional layer of protection against cyber threats.

Trust management at the edge is another emerging solution to improve security in IIoT systems. Trust management protocols can be used to evaluate the trustworthiness of devices and establish secure communication channels based on the assessed trust levels (Pillai *et al*., 2020) [22]. By continuously monitoring device behaviors and interactions within the network, these systems can detect and isolate untrusted devices, preventing them from compromising the integrity of the entire IIoT system. Trust management can be particularly important in environments with heterogeneous devices, where the security posture of individual devices may vary significantly.

3.3. Challenges in Securing IIoT–Edge Systems

Heterogeneity of Devices and Protocols

One of the most significant challenges in securing IIoT-edge systems is the heterogeneity of the devices and protocols used across industrial environments. IIoT systems typically

consist of a wide range of devices, from legacy machinery with limited processing capabilities to modern sensors equipped with advanced communication capabilities (Miorandi *et al*., 2012) [19]. These devices often use different communication protocols, such as MQTT, OPC UA, and CoAP, each with varying security features. The diversity of devices and protocols complicates the development of a unified security solution that can be applied across the entire network. Securing such a heterogeneous ecosystem requires solutions that are adaptable to different hardware and communication standards, which can be a significant barrier to effective cybersecurity in IIoT systems (Brzozowski *et al*., 2018) [4]. Furthermore, the need for seamless interoperability between diverse devices and networks introduces additional complexities, making it difficult to enforce consistent security policies and mitigate potential vulnerabilities.

Resource Constraints (Computational Power, Energy)

IIoT-edge systems often operate in resource-constrained environments where devices have limited computational power, memory, and energy resources (Xie *et al*., 2019) [30]. Many edge devices are low-cost, with minimal processing capabilities, making it challenging to implement traditional security mechanisms like full encryption, anomaly detection, or intrusion prevention systems (IDS) without significantly impacting performance. As a result, security measures must be lightweight and optimized to run efficiently on devices with constrained resources. Techniques such as lightweight encryption and hardware-based security solutions like Trusted Platform Modules (TPM) are often employed, but these solutions may not always provide the level of protection required for high-risk industrial environments (Yang *et al*., 2019) [32]. Additionally, the need for continuous operation and long battery life in many edge devices exacerbates the challenge of balancing security with energy efficiency, as security mechanisms can drain power resources, reducing device longevity and overall system performance.

Lack of Standardization

The lack of standardization in IIoT systems is another major challenge. With numerous vendors, technologies, and communication protocols involved in industrial IoT, security measures are often inconsistent across different devices and platforms (Miorandi *et al*., 2012) [19]. The absence of universally adopted security standards makes it difficult to establish a cohesive, interoperable security framework for IIoT-edge systems. As a result, each organization may implement its own security policies, leading to a fragmented security landscape with potential gaps and vulnerabilities. The lack of standardized security practices also hinders the development of security tools and solutions that can be easily integrated across diverse industrial systems. Moreover, the rapidly evolving nature of IIoT technology further complicates efforts to create standardized security protocols that can keep pace with emerging threats and advancements in industrial systems (Brzozowski *et al*., 2018) [4].

Scalability of Security Frameworks

As IIoT systems grow in size and complexity, the scalability of security frameworks becomes a critical concern. Industrial environments are often large-scale and dynamic, with thousands or even millions of connected devices. Ensuring that security mechanisms can scale effectively across such a vast number of devices and sensors is challenging. Traditional security solutions may struggle to keep up with the sheer volume of data generated by IIoT systems, leading to performance bottlenecks, slow response times, or inadequate threat detection capabilities (Alazab *et al*., 2019) [3]. Additionally, as IIoT systems continue to evolve, new devices and protocols are introduced regularly, further complicating the task of scaling security solutions to protect an increasingly diverse infrastructure. A scalable security framework must be able to handle large numbers of devices, manage complex networks, and support real-time monitoring and response to security events, all while maintaining low overhead and minimizing latency (Mahmood *et al*., 2018) [17].

Real-Time Constraints

Many IIoT systems, especially in critical infrastructure sectors such as manufacturing, energy, and transportation, have real-time constraints that pose a significant challenge to cybersecurity efforts. In these systems, the speed of data processing and decision-making is crucial, as delays could result in operational inefficiencies, safety risks, or financial losses (Xu *et al*., 2020) [31]. Security solutions that introduce latency, such as network traffic analysis or data encryption, can negatively impact the performance of real-time applications. For example, implementing a heavy-duty intrusion detection system (IDS) or performing complex encryption operations on data before it is transmitted may cause delays that disrupt time-sensitive industrial processes. Therefore, security measures must be designed to function within stringent time constraints, ensuring that the integrity and confidentiality of data are maintained without affecting system performance or real-time decision-making capabilities (Santos *et al*., 2020) [24].

4. Emerging Trends & Future Directions

AI/ML for Security

Artificial Intelligence (AI) and Machine Learning (ML) are rapidly becoming essential tools in the cybersecurity arsenal for IIoT and edge systems. AI and ML algorithms are particularly effective for threat detection and anomaly detection in large-scale, complex environments where traditional rule-based systems may fall short (Xu *et al*., 2020) [31]. These techniques can identify patterns and behaviors within vast amounts of network traffic and sensor data, enabling the detection of previously unknown threats or anomalies that deviate from normal operating conditions. For example, machine learning models can be trained to recognize the behavior of legitimate devices and detect deviations indicative of a cyberattack, such as unauthorized access attempts or unusual traffic patterns. ML-based intrusion detection systems (IDS) can operate at the edge, providing near-instantaneous analysis and response, which is crucial for maintaining security in real-time industrial operations. As the IIoT ecosystem continues to evolve, the use of AI/ML for predictive threat modeling and automated responses will become increasingly vital for safeguarding industrial systems against sophisticated cyberattacks (Nugent *et al*., 2020) [20].

Blockchain and DLT

Blockchain technology and Distributed Ledger Technologies (DLT) are gaining attention as promising solutions for enhancing trust and secure data sharing in IIoT systems. Blockchain provides a decentralized and tamper-resistant mechanism for recording transactions, making it particularly

suitable for environments where data integrity is critical (Zhou *et al*., 2020) [35]. In IIoT applications, blockchain can be used to ensure that data collected from sensors, devices, or machines is securely logged and auditable, preventing unauthorized tampering. Furthermore, blockchain can facilitate secure data sharing between parties in an IIoT ecosystem, ensuring that only authorized entities can access and interact with the data. By leveraging blockchain's transparency and immutability, organizations can establish a trusted network of devices and data providers, making it more difficult for malicious actors to compromise the system. Additionally, blockchain-based smart contracts can automate security-related processes, such as access control or system updates, further enhancing the overall security posture of IIoT-edge systems (Maksymov *et al*., 2020) [18].

Zero Trust Architecture in IIoT

The Zero Trust Architecture (ZTA) is an emerging cybersecurity model that assumes no device or user, whether inside or outside the network, is trustworthy by default (Fritz *et al*., 2020) [8]. In IIoT-edge systems, implementing ZTA can significantly enhance security by continuously verifying and authenticating every request for access to resources, regardless of the origin. This approach contrasts with traditional perimeter-based security models, which rely on a trusted internal network. ZTA applies the principle of least privilege, ensuring that devices and users are granted only the minimum level of access necessary to perform their tasks. For IIoT systems, ZTA helps mitigate the risks associated with the growing number of connected devices and the increased attack surface that comes with the integration of edge computing. By using continuous authentication and monitoring, ZTA ensures that even if an attacker gains initial access to a system, they are unable to move laterally or escalate privileges without detection.

Federated Learning for Privacy-preserving Edge Intelligence

Federated Learning (FL) is a decentralized machine learning approach that allows devices to collaboratively learn models while keeping their data localized, ensuring that sensitive information does not need to leave the device (Zhao *et al*., 2020) [34]. This technique is especially valuable in privacy-preserving edge intelligence for IIoT systems. In federated learning, edge devices process and analyze local data to update a global model without sharing the raw data itself, thus minimizing the risk of exposing sensitive industrial data to external threats. FL can be used to improve security by enabling devices at the edge to detect anomalies and make decisions based on locally gathered data, without requiring that data to be transmitted to a central server. This approach not only enhances privacy but also reduces the bandwidth required for data transmission, making it a highly efficient and secure solution for real-time decision-making in IIoT systems (Yang *et al*., 2020).

Quantum-Resistant Encryption (for Long-term Viability)

As quantum computing advances, there is increasing concern about its potential to break current encryption algorithms used in IIoT systems. Quantum-resistant encryption aims to develop cryptographic methods that are secure even in the face of quantum computing capabilities (Gisin *et al*., 2020) [9]. Since quantum computers have the potential to solve certain mathematical problems much faster than classical computers, they could render traditional encryption techniques, such as RSA and ECC, vulnerable. The development of quantum-resistant algorithms, such as lattice-based cryptography and code-based cryptography, is crucial for ensuring the long-term viability of secure IIoT-edge systems. By preparing for the advent of quantum computing, industries can ensure that their IIoT systems remain secure even as quantum technologies become more prevalent.

4.1. Comparative Analysis of Cybersecurity Solutions for IIoT–Edge Systems

To assess the effectiveness and applicability of various cybersecurity solutions for IIoT-edge systems, we compare them based on four key criteria: security coverage, performance, scalability, and suitability for IIoT/Edge. The table below outlines the comparative analysis of common cybersecurity approaches, including traditional security measures, lightweight encryption, machine learning-based solutions, and blockchain.

Table 1

Cybersecurity Solution	Security Coverage	Performance	Scalability	Suitability for IIoT/Edge
Role-based Access Control (RBAC)	Moderate: Protects access based on user roles, limiting the exposure of sensitive data.	High: Minimal performance overhead.	Moderate: Difficult to scale in dynamic, large-scale environments with frequent device changes.	Moderate: Effective for managing user access but limited for device-level security in IIoT.
Multi-factor Authentication (MFA)	High: Provides an additional layer of security by requiring multiple forms of verification.	Low to Moderate: Can increase overhead, particularly in real-time systems.	Moderate: Scaling MFA requires additional infrastructure for managing authentication factors.	Moderate: Effective for user authentication but may not address device-level security concerns.
Encryption (e.g., AES, ECC)	High: Ensures confidentiality and integrity of data.	Moderate to Low: Encryption introduces computational overhead, which can affect performance on resource-constrained devices.	Moderate: While scalable, encryption protocols require significant resources and may introduce latency in large systems.	Moderate: Useful for protecting sensitive data but may cause performance bottlenecks in resource-constrained edge devices.
Intrusion Detection Systems (IDS)	High: Monitors network traffic for signs of malicious activity.	Moderate: Can lead to performance degradation due to continuous monitoring.	Moderate: IDS solutions need to be scalable to handle large amounts of data generated by IIoT systems.	High: Well-suited for network monitoring at both the edge and central locations.

Blockchain (DLT)	Very High: Provides decentralized, immutable records for secure data transactions.	Moderate to Low: Blockchain can introduce latency and overhead, particularly with consensus mechanisms.	High: Scales well across large, distributed networks, particularly for secure data sharing.	High: Suitable for environments requiring trust and secure, transparent data sharing.
Machine Learning-based Detection	Very High: Capable of detecting unknown threats by identifying patterns and anomalies in data.	Moderate: Machine learning models require significant computational resources and may introduce latency.	High: Scalable, as machine learning models can continuously learn and adapt to new threats.	Very High: Ideal for edge devices where local threat detection and response are necessary.
Zero Trust Architecture (ZTA)	Very High: Continuously authenticates and verifies every device, user, and request.	Moderate: Increased complexity can affect performance due to constant verification.	Low to Moderate: Scaling ZTA requires significant infrastructure changes and complex management.	Moderate to High: Provides robust security for distributed systems but may add complexity in large-scale deployments.
Federated Learning (FL)	High: Preserves privacy by processing data locally on devices.	High: Reduces data transmission and works efficiently in resource-constrained environments.	High: Scales effectively across distributed networks of devices.	Very High: Perfect for edge computing, as it supports decentralized, privacy-preserving machine learning.
Quantum-resistant Encryption	Very High: Ensures long-term security even against quantum computing threats.	Low: Quantum-resistant algorithms are computationally expensive and may cause significant overhead.	Moderate: Implementation of quantum-resistant algorithms may require specialized hardware and adjustments to current systems.	Low to Moderate: While important for future-proofing, quantum-resistant encryption may not be practical for current resource-constrained edge devices.

5. Conclusion

In this review, we have explored the multifaceted landscape of cybersecurity for Industrial Internet of Things (IIoT) systems integrated with edge computing. As industrial systems become increasingly interconnected and reliant on real-time data processing at the edge, securing these environments against cyber threats is paramount.

One of the key insights from this analysis is the recognition of the unique security challenges faced by IIoT-edge systems. These systems are marked by a high degree of heterogeneity in terms of devices, protocols, and communication methods, making it difficult to implement universal security solutions. Furthermore, the resource constraints of edge devices, such as limited computational power and energy capacity, add another layer of complexity to securing IIoT systems effectively. As industrial systems grow larger and more complex, scalable security frameworks are essential to ensure that devices and data remain protected without compromising system performance or real-time capabilities. The lack of standardization across IIoT platforms further complicates the task of securing these systems, highlighting the need for more universally accepted security protocols.

Despite these challenges, the integration of advanced cybersecurity solutions offers promising avenues for enhancing IIoT security. Solutions such as blockchain, machine learning-based threat detection, and federated learning at the edge are some of the most promising advancements. These technologies provide strong security coverage, facilitate real-time threat detection, and support privacy-preserving mechanisms that align with the needs of IIoT systems. As cybersecurity solutions evolve, quantum-resistant encryption and the Zero Trust Architecture are emerging as long-term strategies to ensure the robustness and adaptability of IIoT systems, especially in light of quantum computing advancements.

The importance of integrated cybersecurity cannot be overstated. To ensure the safe operation of IIoT systems, security measures must not only protect data at rest and in transit but also monitor and manage devices, networks, and users in real time. Moreover, cybersecurity should be viewed as an integral part of the system architecture, with a focus on continuous monitoring, anomaly detection, and risk mitigation. As the landscape of threats evolves, cybersecurity for IIoT will need to be dynamic, adapting to new attack vectors while maintaining the agility and efficiency required for industrial environments.

Looking ahead, several future directions stand out as particularly promising. The integration of AI/ML for threat detection at the edge, coupled with blockchain for decentralized data trust, represents a powerful synergy for securing IIoT systems. Additionally, federated learning offers a forward-thinking solution to privacy concerns while preserving the efficiency of edge computing. Zero Trust Architecture is poised to become a core security paradigm in IIoT, ensuring that all entities—whether internal or external—are continuously validated before accessing critical resources. Finally, quantum-resistant encryption will become increasingly important to future-proof IIoT systems against emerging computational threats.

In conclusion, securing IIoT systems integrated with edge computing requires a multi-layered approach that encompasses a range of technologies and strategies. The evolution of cybersecurity in this domain will depend on continuous innovation, collaboration across industries, and the development of standards that can unify disparate systems. By addressing the challenges and leveraging the most promising technologies, we can build more secure, resilient, and efficient IIoT-edge ecosystems that are prepared for the future.

6. References

1. Ahmed S, Rehman MH, Malik A. A survey of edge computing in industrial IoT: Concepts, architectures, applications, and challenges. Journal of Industrial Information Integration 2020;20:100174.
2. Alaba FA, Othman M, Jamil N. IoT security: A survey of threats and countermeasures. Proceedings of the 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Control, and Automation (ICSTM) 2017;1-6. https://doi.org/10.1109/ICSTM.2017.8240456
3. Alazab M, Tang M, Hossain M. Industrial IoT network security: Attacks, threats, and countermeasures. IEEE Access 2019;7:87021-87031.

4. Brzozowski M, Bhat R, Dvorak A. Cybersecurity challenges in the Industrial Internet of Things: A survey. IEEE Access 2018;6:66435-66452.
5. Cao Y, Yang X, Li J. A survey of edge computing in IIoT: Challenges, security threats, and solutions. IEEE Access 2018;6:12794-12805.
6. Chen X, Xie L, Zhang Y. Multi-factor authentication for IoT: Security and performance analysis. Journal of Network and Computer Applications 2020;169:102747.
7. Dinh HC, Lee CS, Lee HJ. Blockchain-based security solutions for edge computing: A survey. Journal of Computer Science and Technology 2020;35(4):726-746.
8. Fritz M, Meidan Y, Dief M. Zero trust architecture for industrial IoT security. IEEE Access 2020;8:235041-235050.
9. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Reviews of Modern Physics 2020;74(1):145-193.
10. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 2013;29(7):1645-1660.
11. Haleem A, Raza M. Edge computing security for IIoT: A comprehensive survey. Computer Networks 2020;181:107405.
12. Khan R, Rehman M, Ahmed S. Security challenges in industrial IoT and edge computing: A survey. Journal of Computing and Security 2020;1(4):90-109.
13. Kouadio OD, Djaha MS, Aswat S. Edge computing in IIoT: A comprehensive survey. IEEE Transactions on Industrial Informatics 2020;16(5):3229-3237.
14. Lee J, Davari H, Singh J. Industrial big data analytics and cyber-physical systems for future smart manufacturing. Journal of Manufacturing Science and Engineering 2015;137(3):34009.
15. Liu C, Yang H, Liu J. Secure communication protocols for IoT applications: A review. Proceedings of the International Conference on Computer and Communications (ICCC) 2017;418-423.
16. Liu Z, Xiao L, Zhang M. A review of MQTT in IoT systems. Procedia Computer Science 2017;113:98-105.
17. Mahmood A, Zeng D, Song H. SDN-based security solutions for industrial IoT networks: A survey. IEEE Access 2018;6:21484-21496.
18. Maksymov Y, Drozd V, Perelmuter M. Blockchain for Industrial IoT: A survey of security applications. Journal of Network and Computer Applications 2020;145:102393.
19. Miorandi D, Sicari S, Pellegrini F, Chlamtac I. Internet of things: Vision, applications, and research challenges. Ad Hoc Networks 2012;10(7):1497-1516.
20. Nugent C, Jara AJ, Reyes F. Using machine learning for security in industrial IoT: Challenges and opportunities. IEEE Internet of Things Journal 2020;7(12):11017-11025.
21. Pawlowski S, Schmitt J, Wolf T. Cybersecurity for industrial IoT: A survey of techniques and technologies. International Journal of Advanced Computer Science and Applications 2019;10(11):103-110.
22. Pillai R, Shah S, Tan K. Trust management for edge devices in industrial IoT: Approaches and challenges. Future Generation Computer Systems 2020;108:106-118.
23. Sandhu R, Coyne EJ, Feinstein HL. Role-based access control models. IEEE Computer 1996;29(2):38-47.
24. Santos F, Pinto A, Almeida M. Securing IIoT devices with Trusted Platform Modules: A review. IEEE Transactions on Industrial Informatics 2020;16(3):1904-1913.
25. Shi W, Cao J, Zhang Q, Li Y, Xu L. Edge computing: Vision and challenges. IEEE Internet of Things Journal 2016;3(5):637-646.
26. Sicari S, Rizzardi M, Grieco L. Securing industrial IoT through Over-the-Air updates. International Journal of Computer Applications 2018;180(18):17-23.
27. Tang M, Zhou Z, Zhang W. A survey of cybersecurity in industrial IoT systems. Security and Privacy 2018;1(2):e45.
28. Tao F, Cheng J, Zhang L. Internet of Things and industrial wireless networks. Springer Handbook of Industrial Automation 2018;175-190.
29. Wang W, Zhang D, Li M. Cyber-physical security in industrial IoT systems: A survey of attacks and countermeasures. IEEE Access 2019;7:68454-68468.
30. Xie L, Liu L, Xu Z. Security in edge computing for IIoT: A comprehensive survey. IEEE Transactions on Industrial Informatics 2019;15(6):3467-3476.
31. Xu H, Li X, Li B. Lightweight encryption for secure communication in IIoT. IEEE Internet of Things Journal 2020;7(5):4506-4517.
32. Yang Y, Zhao Z, Zhang S. Secure boot mechanism in IoT: Solutions and challenges. International Journal of Ad Hoc and Ubiquitous Computing 2019;31(3):189-202.
33. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of Things for smart cities. IEEE Internet of Things Journal 2014;1(1):22-32.
34. Zhao Y, Li S, Zhang D. Edge computing in IIoT: A survey. Journal of Industrial Information Integration 2020;18:100169.
35. Zhou M, Lu J, Wu D. Cybersecurity challenges in industrial Internet of Things: A review. Computers, Materials & Continua 2020;64(1):411-430.