REVIEW ARTICLE

Secure Software Engineering for Industrial IoT: A Comprehensive Review of Threat Modeling and Defense Mechanisms

Aamir Ali[1], **Misbah Ali**[1,*], **Uqba Mushtaq**[1] **and Malik Arslan Akram**[2]

[1] Department of Computer Science, COMSATS University Islamabad, Sahiwal campus 57000, Pakistan
[2] Southwest University of Science and Technology, Mianyang 621010, China

Abstract

The Industrial Internet of Things (IIoT) is a foundational pillar of Industry 4.0, enabling real-time data exchange and automation through the integration of smart sensors, actuators, and networked machinery. While this interconnectivity enhances operational efficiency and decision-making on the industrial floor, it also introduces complex cybersecurity challenges. This work reviews literature related to the IIoT with a focus on threat modeling techniques, including mitigation strategies. It comprises the theoretical frameworks and the implemented solutions within the domains of critical infrastructure and manufacturing. The coexistence of legacy control software systems, stringent real-time performance requirements, and heterogeneous modern devices, particularly within SCADA networks and cyber-physical systems, complicates the design and implementation of robust security mechanisms. This review synthesizes recent advancements in IIoT security with a specific focus on threat modeling methodologies and mitigation strategies. Key attack vectors such as denial-of-service (DoS) floods, data injection, and Advanced Persistent Threats (APTs) are examined. The paper further analyzes contemporary defense approaches, including AI-driven intrusion detection systems, blockchain-based trust frameworks, and software-defined networking solutions. This work aims to support both researchers and practitioners in developing scalable, resilient, and secure IIoT infrastructures suitable for modern industrial environments.

Keywords: industrial internet of things, cyber security, denial-of-service, blockchain.

1 Introduction

The Industrial Internet of Things (IIoT) has become the underlying aspect of Industry 4.0, extending the definition of intelligent, interconnected devices to the industries of manufacturing, energy, and logistics. The IIoT brings predictive maintenance, real-time monitoring, and enhanced decision-making to the

Academic Editor:
Summair Raza

Submitted: 16 July 2025
Accepted: 29 July 2025
Published: 17 August 2025

Vol. 1, **No.** 1, 2025.
10.62762/JSE.2025.834259

***Corresponding author:**
✉ Misbah Ali
talktomisbah.ali@gmail.com

Citation
Ali, A., Ali, M., Mushtaq, U., & Akram., M. A. (2025). Secure Software Engineering for Industrial IoT: A Comprehensive Review of Threat Modeling and Defense Mechanisms. *ICCK Journal of Software Engineering*, 1(1), 17–31.

© 2025 by the Authors. Published by Institute of Central Computation and Knowledge. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

industrial world through the integration of sensors, actuators, machinery, and control systems within internet-enabled infrastructures [1]. It plays a crucial role in reducing the downtime of systems, making production workflows smoother, and achieving maximum supply chain efficiency in the automated manufacturing process [2, 3]. As IIoT systems become increasingly integrated with critical infrastructure, they present inherently dynamic cybersecurity vulnerabilities that differ from the standard IT security paradigm. Ubiquitous employment of legacy controllers, low-power embedded systems, and proprietary communication interfaces creates an extremely fragmented and insecure ecosystem. High-profile cyber incidents such as the Stuxnet worm, the BlackEnergy attacks, and the hack of the Oldsmar water facility herald the potential of targeting the IIoT, showcasing the threat that extends beyond process interruption and threatens serious harm to the public [4].

Characteristic of standard IIoT structures is their multi-layered design, which is typically made of the device layer, network layer, and application (cloud) layer. It is the device layer that accommodates the field-level elements like sensors, actuators, and embedded controllers with the function of data acquisition [5]. The network layer allows both internal and external communication via industrial communication protocols like MQTT, Zigbee, Modbus, and OPC-UA [6, 7]. The application layer, which is quite often based on the cloud, accommodates data storage, processing, and analysis via the application of Artificial Intelligence (AI) and machine learning (ML) methodologies to the data retrieved from edge devices [8]. Components of the Industrial Control Systems (ICS), such as Supervisory Control And Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLCs), show significant heterogeneity in their security features [9]. Whereas newer protocols such as the OPC-UA provide improved security features, older ones like Modbus don't provide any encryption and authentication features, which make them especially susceptible to cyber exploitation [10, 11]. The three-tiered architectural structure of the IIoT, showing the interaction between device, network, and application layers and the corresponding security weaknesses, is represented in Figure 1.

IIoT systems are vulnerable, by design, to security attacks at multiple architectural layers. These weaknesses are due, in large measure, to the

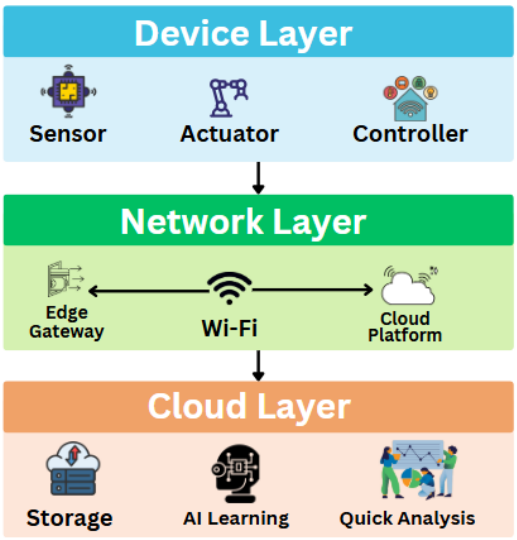

Figure 1. Three-tier architecture of IIoT.

presence of weaknesses in the firmware, the use of communication interfaces that are not encrypted, the lack of adequate authentication processes, and the incorporation of components from third-party suppliers that are inherently insecure. Obsolete firmware, in particular, is an important threat, since it has the potential to be used by an opponent to introduce persistent malware or to enslave devices in a botnet infrastructure. Furthermore, the employment of unsecured communication protocols, like Modbus/TCP, makes the IIoT systems vulnerable to an array of network attacks, including capture attacks, command injection, and replay attacks [12, 13]. The post-deployment weaknesses add further layers of challenge to the threat picture. They involve the injection of malicious hardware or the spread of compromised software patches with clandestine backdoors or security weaknesses. The identification of such threats is particularly difficult given the obscure and complicated nature of supply chain attacks that may infect systems at multiple phases of manufacturing and supply [14]. These risks call for holistic, multi-layered security solutions that address both cyber and physical dimensions of IIoT environments.

While IIoT has greatly facilitated advancements in technology with the emergence of Industry 4.0, the expansion of connectivity, device heterogeneity, legacy systems, and the sophistication of devices has greatly compounded the challenges of security in the intelligent industrial networks. The increasing sophistication of cyberattacks, such as DoS and APTs, highlights the need for advanced security frameworks.

This review is motivated by the need to advance AI and Blockchain technology toward industrial cybersecurity, as well as unifying AI frameworks, to automate gaps in threat modeling and build reliable and secure industrial infrastructures.

This study provides a comprehensive review of the security of IIoTS systems focused on literature published between 2015 and 2025. This review is structured to answer the following key questions: (1) What are the dominant IIoT security threats? (2) What modeling approaches are used to identify and assess them? (3) Which mitigation strategies are most promising for deployment in scalable IIoT infrastructures?

The rest of the paper is organized as follows: Section 2 presents security threat modeling approaches in IIoT. Section 3 is focused on challenges and adaptability in IIoT environments. Section 4 illustrates the classification of security threats and cybersecurity attacks in IIoT. Section 5 presents the attack mitigation techniques in IIoT. Section 6 describes the emerging technologies and future trends in IIoT security. Section 7 highlights the challenges in IIoT security and provides future directions. Lastly, section 8 concludes the review while providing final insights on IIoT security. Key Contributions of the Study are presented below:

1. It provides a detailed analysis of IIoT security literature from 2015 to 2025, covering security challenges
2. It addresses the core security concerns, i.e., threats, modeling techniques, and scalable mitigation strategies
3. It discusses future technologies and trends in IIoT security to guide next-generation solutions.
4. It highlights unresolved challenges and proposes future research directions to strengthen IIoT security frameworks

2 Security Threat Modeling Approaches in IIoT

The integration of diverse and large-scale IT (Information Technology) and OT (Operational Technology) components within IIoT environments introduces complex security challenges. Threat modeling plays a critical role in systematically identifying, assessing, and mitigating potential security risks within such infrastructures [15]. This section reviews both conventional and modern threat modeling approaches, with particular attention to their adaptability and limitations in IIoT ecosystems.

2.1 Traditional Threat Modeling Approaches

STRIDE, developed by Microsoft, organizes common cyber threats into six distinct categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. While STRIDE is widely adopted in traditional software systems, its direct applicability in IIoT settings is constrained by the complexity of cyber-physical interactions. The STRIDE security model and its threat categories are presented in Figure 2.

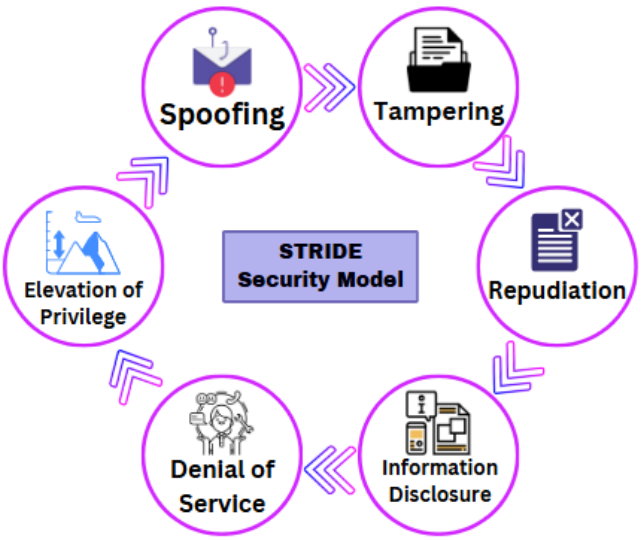

Figure 2. STRIDE security model.

DREAD is a risk assessment model that evaluates threats based on five factors: Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability. Although DREAD provides a structured scoring mechanism, its reliance on static judgments makes it less effective in dynamic IIoT environments where both devices and threat profiles evolve rapidly. Furthermore, it overlooks the immediate safety hazards that have been emphasized in industrial systems [16]. DREAD risk assessment model and its threats are illustrated in Figure 3.

Attack trees provide a hierarchical methodology for modeling potential security threats by decomposing high-level attack objectives into granular, actionable sub-goals and steps. Following this idea, attack graphs model complicated, interconnected infrastructures to enable the study of sophisticated, multi-stage attacks. These visual methods have been successful in the analysis of malware like ransomware and Man-in-The-Middle (MiTM) attacks in the setting of

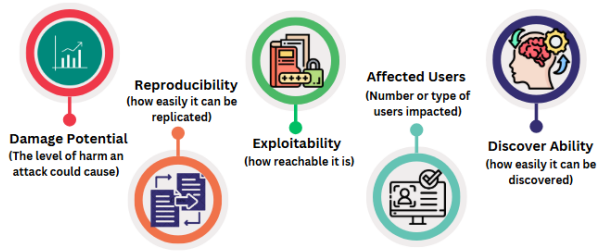

Figure 3. DREAD risk assessment model factors and use in IIoT security threats.

IIoT networks [17]. These approaches, however, are fraught with significant scalability costs, primarily in the highly dynamic IIoT networks with a large and constantly changing number of nodes. Although the work on the automation frameworks and the application of machine learning is still ongoing, no specific solution has yet been deployed that can counteract such limitations. To transcend limitations of conventional failure-based analysis techniques, the STPA-Sec (System-Theoretic Process Analysis for Security) approach has been developed. This method builds on the STAMP (Systems-Theoretic Accident Model and Processes) methodology with the addition of a security-focused view. Different from the usual approaches based on component-level failures, the STPA-Sec is based on the demonstration of system-level weaknesses that emanate from unsafe control actions. It accounts for the complex interactions between human operators, software systems, and hardware components, rendering it particularly suitable for analyzing socio-technical systems such as IIoT infrastructures [18].

Attack trees and graphs are useful in particular attack sequences and technical flaws. However, they tend to overlook the complete system picture, especially the human and organizational elements. On the other hand, STPA-Sec examines unsafe control actions and systemic failures, considering the interactions of humans, software, and hardware, which are beyond the component level. This makes STPA-Sec more useful for socio-technical systems such as the IIoT, as the security threats are not limited to technical failures, but complex interconnections.

Given IIoT's tightly coupled cyber-physical nature and its role in critical infrastructure, STPA-Sec provides a comprehensive modeling framework that emphasizes system dynamics, interdependencies, and emergent vulnerabilities. However, its implementation requires substantial domain expertise and detailed system modeling, which can be resource-intensive. The scalability and automation of STPA-Sec for real-time IIoT applications remain active areas of research [19].

A high-level overview of the STPA-Sec process, highlighting the security vulnerabilities in cyber-physical systems, is shown in Figure 4.

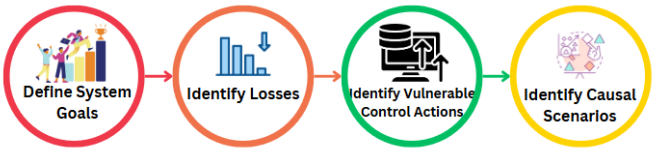

Figure 4. STPA-SEC process.

3 Challenges and Adaptability in IIoT Environments

The integration of diverse devices, communication protocols, and platforms complicates the implementation of consistent threat modeling in IIoT systems [20]. All security mechanisms must account for timing constraints and safety requirements, which limit the extent and complexity of protective measures that can be deployed. Frequent changes in network configurations and device states lead to highly dynamic topologies, making static modeling approaches less effective [5]. The heterogeneity of IIoT environments also includes numerous resource-constrained devices, which limits the feasibility of deploying computationally intensive security frameworks [15]. Despite their practical benefits, traditional threat modeling techniques such as STRIDE, DREAD, and attack trees require complementary system-theoretic approaches to provide effective security assurance in IIoT. This is not due to a lack of perspective in traditional models, but rather because system-theoretic methods embrace interdisciplinary convergence and account for complex system interactions. Future research is actively focused on developing real-time, automated security solutions that can dynamically adapt to evolving threats in IIoT environments [18]. The Classification of IIoT Security Challenges is given below:

1. Device Heterogeneity: Multiple vendors, operating systems, and communication protocols make uniform security difficult to enforce.
2. Real-Time Constraints: Safety-critical applications require low-latency responses, limiting the use of complex security measures.
3. Network Dynamism: Frequent device mobility and reconfiguration lead to unpredictable,

non-static networks.

4. Limited Resources: Constrained CPU, memory, and power prevent the deployment of advanced security solutions.
5. Modeling Limitations: Traditional security models fail to account for interactions between human, software, and hardware components.
6. Adaptive Threat Landscape: Continuously evolving attack techniques demand a dynamic, AI-driven defense mechanism

4 Classification of Security Threats and Cyber Attacks in IIoT Environments

While the integration of advanced devices into industrial systems boosts automation and productivity, it also introduces a wide range of cybersecurity vulnerabilities. Security threats in IIoT environments can generally be categorized into four main types: 1) Network-level attacks (e.g., DDoS, Man-in-the-Middle), which encompass the communication channels within the network. On the network layer, threats such as DDoS and MitM attacks aim to interrupt or capture the flow of information. These attacks could result in loss of information accuracy, unwanted surveillance, or total communication failure. 2) Device-level threats (e.g., firmware tampering, botnets), focus on the IIoT devices such as sensors and controllers. The risks include unauthorized firmware modification, illegal control, and botnet access. Device-level threats may compromise and disrupt network-wide operations, and in turn endanger the behavior of the devices. 3) Physical-layer attacks (e.g., device tampering, sensor spoofing) expose the system to device-related threats such as theft, tampering, or spoofing, which could alter source data. Digital protections are often bypassed by physical attacks, and such attacks tend to be difficult to detect in real-time. 4) Application/infrastructure-level vulnerabilities (e.g., VNF misuse, insecure APIs). These vulnerabilities cover user interaction components, insecure application interface and software errors, and misuse of virtual network functions. Loss of control over sensitive data, services, or industrial processes and information may result from an attack of this nature. Mitigating risks at each layer is essential for building resilient IIoT systems.

Among the most widespread threats in IIoT are Distributed Denial of Service (DDoS) attacks, which flood networks with illegitimate traffic, leading to prolonged congestion and potential service disruption [15]. Machine learning has been applied to optimize VNF placement on fog nodes, reducing DDoS impact and improving latency [16]. For example, over 105 million IoT-focused DDoS attacks were recorded within six months, originating from more than 276,000 IP addresses [14].

Jamming attacks are particularly effective against communication protocols like ZigBee, LoRa, and IEEE 802.15.4, where signal interference can disrupt communication between devices. These attacks are difficult to detect and prevent due to their stealthy nature [21]. MiTM attacks, on the other hand, enable attackers to intercept or manipulate data exchanged between IIoT components. For instance, researchers once found a flaw in Amazon Alexa that allowed attackers to steal tokens and gain unauthorized access [22]. These examples highlight the critical need for securing communications using multi-factor authentication and ongoing monitoring of data integrity.

IIoT devices are frequent targets of cyberattacks because of their inherent limitations, such as low processing power, outdated firmware, and the use of weak, default authentication credentials. Firmware tampering is a major concern, involving the malicious alteration or injection of code during updates, especially in devices lacking secure boot mechanisms or cryptographic verification of their code [15]. Another common attack vector is the creation of botnets, as seen with the Mirai malware. It exploits open network ports and factory-default login credentials to take control of IIoT devices and use them to launch massive Distributed Denial-of-Service (DDoS) attacks [14].

Resource exhaustion attacks also present a serious challenge to IIoT systems. These attacks take advantage of the limited computing resources, such as memory and processing power of embedded devices, effectively preventing the implementation of standard security tools like intrusion detection systems (IDS), antivirus software, or endpoint protection platforms [26].

In addition, physical security flaws pose significant threats, especially to IIoT nodes deployed in remote or unattended locations. Physical tampering with devices can disable safety features and insert malicious changes that go unnoticed during normal operation. Even at the manufacturing stage, attackers can embed hardware Trojans, malicious alterations to

circuit designs that stay dormant until triggered, posing long-term risks to the system's reliability and trustworthiness [23].

Sensor spoofing attacks involve manipulating environmental inputs such as temperature or electromagnetic noise to mislead control decisions. These tactics are particularly damaging in critical infrastructure [24]. Side-channel attacks, including power analysis and voltage glitching, can extract sensitive data by exploiting hardware-level behaviors [25].

Cloud and edge platforms are central to IIoT operations, yet present new attack surfaces. Insecure APIs, weak encryption, and poor access controls can lead to unauthorized access and data breaches [27]. Improperly managed VNFs (Virtual Network Functions), especially in fog nodes, may delay security operations or allow adversaries to inject malicious traffic. Delays in VNF execution can lead to missed opportunities for real-time threat mitigation [14]. Misconfigured cloud environments and inadequate identity management often lead to shared-space breaches and data leakage across tenants. A brief summary of security threats and cyberattacks is presented in Table 1.

5 Attack Mitigation Techniques in IIoT

The increasing complexity and vulnerabilities of IIoT systems demand multi-layered and advanced defense mechanisms for intelligent protection. This section outlines key mitigation strategies, categorized according to the enabling technologies, and evaluates their respective performance metrics. Ensuring data confidentiality, integrity, and availability in IIoT environments is imperative due to the heightened risks of unauthorized access, data tampering, and information leakage. Given the resource-constrained nature of many IIoT devices, particularly with respect to processing power and energy capacity, lightweight cryptographic schemes such as AES-128 and Elliptic Curve Cryptography (ECC) are commonly employed to achieve secure communication [28].

To further protect the confidentiality and integrity of data during transmission, secure communication protocols such as Datagram Transport Layer Security (DTLS), IPSec, and IEEE 802.15.4e are typically used [29]. Although hash functions like MD5 and SHA-1 were classically used for the purpose of verifying integrity, they are being replaced by the more secure SHA-256 algorithm today. User and device authentication are carried out with the help of Public Key Infrastructure (PKI) and digital signature schemes, respectively, but both of these methods have their limitations in the large-scale implementations of IIoT due to the complexities involved in key and certificate management, and the likely introduction of latency due to the encryption overhead [30]. For that reason, symmetric encryption methods and lightweight crypto techniques are preferred in the implementation of the IIoT, particularly in latency-constrained applications [28].

Apart from the use of cryptographic protection, the evolution of machine learning (ML) and deep learning (DL) has increased the effectiveness of Intrusion Detection Systems (IDS) in the IIoT setting substantially. Such smart systems provide higher adaptability and responsiveness with respect to conventional rule-based IDS through the provision of quick threat identification and mitigation. ML models like Random Forest, Support Vector Machines (SVM), and K-Nearest Neighbors (KNN), and DL structures like Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks have proved to be highly effective in recognizing a wide array of cyber-attacks, namely MiTM attacks, Distributed Denial-of-Service (DDoS), and zero-day exploits [14].

One such example is the SmartSentry system that implements an ML and DL hybrid model to detect online threats in the IIoT network. The system discusses the application of classifiers such as Random Forest, Decision Tree, SVM, KNN, and Deep Neural Networks (DNN) on the dataset Edge-IIoTset and shows its applicability in protecting the IIoT network. PCA was utilized in the process of feature selection, SMOTE managed class imbalance, and standardization was used in feature scaling [31, 32].

The DNN model achieved 100% accuracy in binary classification and over 94% in multi-class tasks (6- and 15-class problems), showcasing its ability to detect complex and diverse attack patterns. AI/ML-based IDS can learn, adapt, and respond to new threat vectors, making them highly suitable for dynamic IIoT environments. Unlike traditional signature-based systems, these models can identify previously unseen anomalies regardless of network topology complexity. However, they require large labeled datasets and high computational power. Processing overhead can delay responses in time-sensitive IIoT applications. Deploying optimized ML models on edge or fog nodes helps reduce latency, but such environments demand

Table 1. Multi-layer taxonomy of IIoT security threats with real-world incidents.

Category	Threats	Example Incident	Mitigation	Detection Difficulty	Common Industries Affected
Network-level	DDoS, jamming, MitM	105M IoT DDoS attacks in 6 months [14]	Anomaly detection, secure routing	High	Manufacturing, Smart Grids, Healthcare
Device-level	Firmware tampering, botnets	Alexa token hijack [22]; Mirai botnet [14]	Secure boot, lightweight encryption	Medium-High	Consumer IoT, Critical Infrastructure
Cloud /Edge-level	VNF misplacement, data leakage	Breach from VNF latency [14]	Access control, blockchain-based validation	Medium	Logistics, Industrial Automation
Physical-level	Tampering, sensor spoofing	Grid sensor manipulation [24]	Tamper-proof hardware, physical monitoring	Low-Medium	Oil & Gas, Utilities, Defense
Application-level	Weak auth, insider threats	Token theft on voice assistant [22]	MFA, access logging	Low	Retail, Smart Homes, Transportation

lightweight, resource-efficient algorithms [28]. An AI/ML-based IDS Workflow in IIoT is shown in Figure 5.

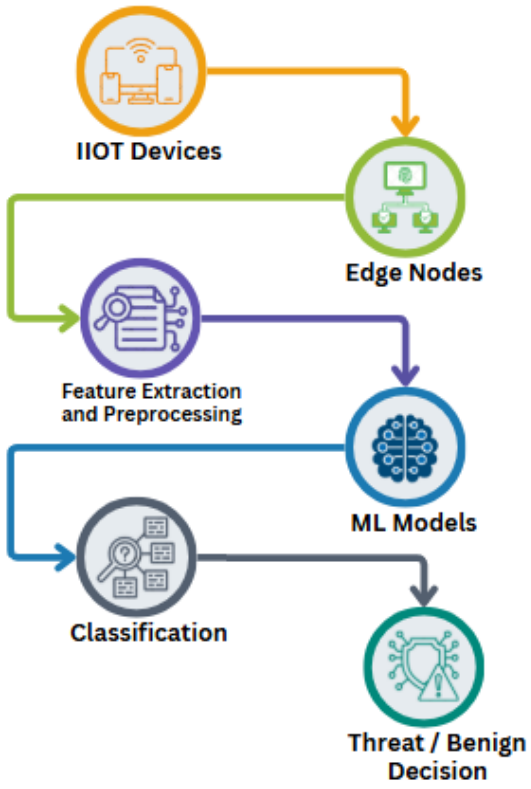

Figure 5. AI/ML-based IDS Workflow in IIOT.

Emerging technologies like blockchain and federated learning (FL) offer promising enhancements for IIoT security and privacy. These distributed systems address key concerns such as data integrity, authentication, and confidentiality in decentralized, resource-constrained environments. Blockchain provides immutable distributed ledgers that enhance trust by recording device interactions and command logs, preventing unauthorized changes [33]. Advanced implementations such as multi-chain architectures and token-based access control further improve interoperability and trust across heterogeneous IIoT domains.

Federated learning enables collaborative training of machine learning models without transmitting raw data to a central server, preserving privacy while reducing bandwidth usage. This approach is particularly effective for anomaly detection and security monitoring across distributed IIoT nodes [34]. Despite their advantages, these technologies also pose deployment challenges. Blockchain's consensus mechanisms (e.g., Proof-of-Work or Proof-of-Authority) introduce latency and require significant computing resources, hindering real-time application scalability. FL faces difficulties in managing device heterogeneity, unstable communication, and ensuring consistent model

convergence [35].

Placing security mechanisms closer to IIoT devices improves detection speed and reduces latency. Fog-based IDS solutions deploy Virtual Network Functions (VNFs) including firewalls, deep packet inspection (DPI), and anomaly detection at the network edge [36, 37]. A performance-aware ML framework has been proposed to dynamically reassign VNFs closer to vulnerable IIoT clusters, enabling faster responses to DDoS and other cyber threats [38]. This localized deployment improves response times, reduces congestion, and enhances reliability in mission-critical applications. Fog-based VNF deployment offers superior responsiveness compared to cloud-based systems due to localized decision-making and data filtering. However, challenges remain in scaling these solutions, particularly in ensuring that fog nodes have adequate computing and storage capacity. Additionally, operators must strategically allocate VNFs to maintain service quality while minimizing resource strain. Balancing dynamic VNF assignment with continuous security coverage is critical for building robust IIoT infrastructures [39]. A brief summary of attack mitigation techniques in IIoT is presented in Table 2.

Among these techniques, the most advanced in real-time threat response for IIoT environments is are integration of fog computing with AI/ML-based intrusion detection systems (IDS). In Figure 6, a comparative evaluation of the latency impacts alongside scalability and resource expenditure of IIoT mitigation techniques is presented.

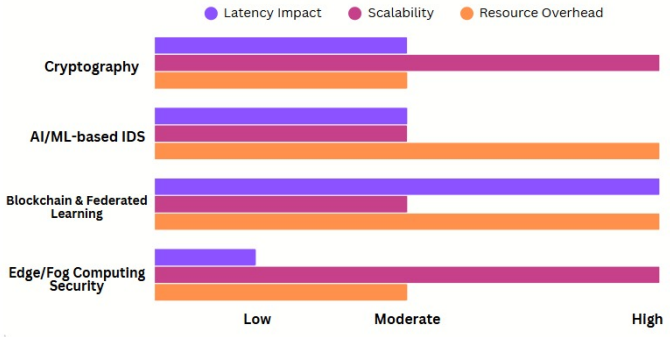

Figure 6. Comparative analysis of IIoT mitigation techniques.

6 Emerging technologies and future trends in IIoT security

The integration of the IIoT with critical infrastructural systems is gaining traction alongside the growth of smart manufacturing and industrial automation. These advancements are propelling innovations in security frameworks designed to mitigate risks that are typically neglected by conventional security approaches. This part addresses new technologies and trends anticipated to influence the future of providing cybersecurity in IIoT environments.

The application of Artificial Intelligence (AI) and Machine Learning (ML) technologies is transforming the security capabilities of IIoT systems by providing real-time threat identification and evaluation, behavior monitoring, and adaptive threat response. These smart systems defend IIoT networks by counteracting anomalous patterns and dynamically evaluating and responding to the emerging threats, thus adding another layer of security [31, 40]. As an example, one recent study put forward a supervised learning model that used XGBoost for the optimal allocation of VNFs that included firewalls and intrusion detection systems (IDS) at fog computing nodes. The model gave an accuracy of 99.40% in strategic placement identification during DDoS attack scenarios [14]. Moreover, Long Short Term Memory (LSTM) and Random Forest classifiers have advanced AI techniques that effectively detect complex cyber threats such as MiTM and ransomware intrusions [17]. These models are better compared to traditional rule-based systems because they do not rely solely on historical data. These models are better than traditional rule-based systems because they are more flexible to zero-day exploits and advanced persistent threats (APTs) adaptability.

The adoption of Federated Learning (FL) is a noteworthy development, allowing individual IIoT nodes to locally train models without exchanging sensitive raw data. This decentralized method improves data privacy and anomaly detection system responsiveness and scalability. However, the edge device constraints in IIoT environments from evolving cyber threats continue to pose challenges when trying to implement AI/ML models. These challenges have sparked interest in lightweight models and in hybrid fog, edge, and cloud-layered deployment architectures, which aim to provide real-time protection while conserving resources.

The use of lightweight DTLS over CoAP and IPv6 over 6LoWPAN has recently gained traction. These protocols provide low-power wide-area network (LPWAN) encrypted communication employing economically efficient cryptographic methods like ECC and AES-128, designed for resource-constrained IIoT devices. While supporting

Table 2. Summary of Attack Mitigation Techniques in IIoT

Mitigation Technique	Key Techniques	Latency Impact	Scalability	Resource Overhead	Notes
Cryptography	AES, ECC, DTLS, hash functions	Moderate	High (with efficient key management)	Low to Moderate	Needs a balance between strength and device limits
AI/ML-based IDS	XGBoost, Random Forest, Fog-based models	Variable (depends on model complexity)	Moderate (distributed ML helps)	High (training and inference)	Edge deployment reduces latency, requires optimization
Blockchain & Federated Learning	Distributed ledger, decentralized ML	High (blockchain consensus delays)	Moderate to Low (depending on network)	High (computational and communication)	Suitable for integrity & privacy, less for real-time control
Edge/Fog Computing Security	VNFs, local IDS, adaptive VNF placement	Low	High	Moderate	Real-time analytics closer to the data source

low-power sensor-level processing, a practical balance between device efficiency and encryption level remains challenging. As a promising new approach to augment cybersecurity in IIoT systems, twin digital technologies, which create virtual replicas of physical assets are achieving traction. The continuous comparison of sensor input data against operating benchmarks allows for the simulation of systems in real time and the detection of deviations from expected behaviors. This enables early identification of deviations that may indicate cyber intrusions, thereby supporting predictive maintenance and threat response strategies.

For example, some studies use AI-driven digital twins with techniques like autoencoders and LSTM networks to detect anomalies in manufacturing processes [42]. Other research has shown that digital twins can simulate potential attack scenarios in industrial control systems and apply ensemble classifiers to accurately detect real-time threats [43].

To address privacy concerns in distributed industrial environments, privacy-preserving machine learning models are gaining prominence. While some VNF placement studies have not directly implemented such methods, they emphasize the need for federated learning and on-device training to avoid centralized data exposure and support regulatory compliance (e.g., GDPR) [33]. Federated learning trains models locally and eliminates the need for data centralization, but it introduces synchronization and convergence challenges, especially across heterogeneous IIoT nodes. In addition, homomorphic encryption (HE) and secure multi-party computation (SMPC) are being explored to enable confidential data processing without revealing raw information. A framework called SmartCrypt demonstrated efficient time-series data aggregation using homomorphic encryption, outperforming traditional schemes in throughput and scalability [44].

Other approaches combine additive HE with SMPC for privacy-preserving joint analysis in blockchain-integrated IIoT systems, ensuring confidentiality without disclosing individual data contributions [45]. Collectively, these privacy-preserving techniques, including FL, HE, and SMPC, offer promising solutions for secure collaborative analytics in IIoT. However, their implementation complexity, including latency and communication overhead, poses significant deployment challenges.

The Industrial Internet of Things requires advanced IDS technologies that can perform real-time threat detection and response. Deploying IDS at fog or edge nodes closer to IIoT devices reduces detection latency and enables prompt local reactions to security incidents, which is crucial for bandwidth-limited environments [46]. One study demonstrated how VNFs placed at network edges can act as near-device cybersecurity agents, significantly reducing attack response time. Fog-level IDSs enable rapid anomaly

detection and augment the response speed of mitigation for temporally-sensitive attacks, including DDoS and others [14]. Figure 7 illustrates the application of federated learning, homomorphic encryption, and SMPC into the IIoT ecosystem.

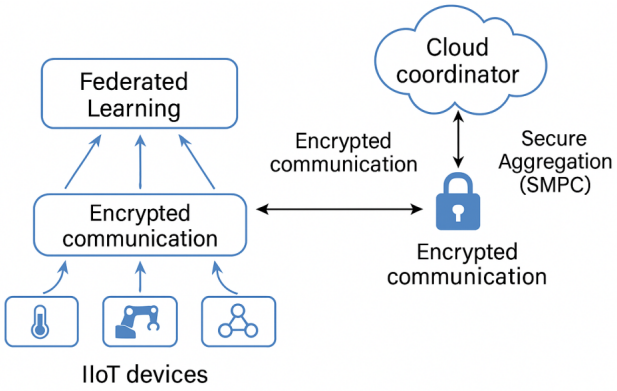

Figure 7. The integration of federated learning, homomorphic encryption, and SMPC in IIoT.

The adaptability of IIoT security systems is greatly improved by combining signature-based detection with anomaly-based models. This hybrid approach allows for strong defense against both familiar threats and new, emerging attacks. Signature-based methods are effective at identifying previously known attack patterns, while anomaly-based techniques offer the flexibility to detect unusual or evolving intrusions [41]. This shift reflects a broader trend in the industry from traditional, reactive security to smarter, proactive, and distributed strategies designed specifically for IIoT environments.

The integration of artificial intelligence (AI) with edge computing and lightweight cryptography is helping IIoT security systems become more scalable, responsive, and resilient. At the same time, privacy-focused solutions are being developed through technologies like federated learning, homomorphic encryption, and digital twin architectures. These innovations aim to protect sensitive data while still improving threat detection accuracy [40, 47]. Overall, these advances highlight a growing focus on adaptive, decentralized cybersecurity models that are better suited to the complex and constantly changing nature of industrial IoT systems. For an overview of the latest developments in IIoT security, see Table 3.

7 Challenges and Future Directions

The IIoT has great potential to transform the automation of industrial processes using real-time data, capital, decision making, and optimizing processes in real-time. Nevertheless, an unresolved set of security problems continues to stand in the way of the exploitation of IIoT's full potential value. One such gaping problem is apparent in a vast distributed and heterogeneous IIoT network with incorporates IIoT components. The scalability of their security mechanisms is rather modest in resolving targeted security issues. Due to the diversity of security devices, limited device intercommunication, and the absence of centralized supervision, classical centralized security systems are obsolete in today's IIoT environments [33, 48]. The spread of advanced technology increases the likelihood of inconsistent protocols and interfaces, introducing fragmented control methods... hence elevating the pre-existing Security problems, including the lack of device and network integrity. Another significant issue is the absence of a standard, comprehensive, and global security paradigm. Current IIoT security solutions are often highly proprietary and provide minimal security and cross-platform collaboration, further segregating systems into architectural silos along vendor and industry lines [49]. This absence of standardization in defence architecture hampers the ability to implement scalable, robust, integrated responses coordinated across the tiers of IIoT ecosystems.

Latency-sensitive IIoT applications, such as those involving real-time industrial control, also face the latency-security trade-off. Although strong encryption and authentication mechanisms are vital for securing the IIoT systems, they incur a significant delay, which may be detrimental to time-critical industrial operations [40, 50]. Another issue of concern is data privacy, especially because IIoT systems are designed to capture, relay, and process sensitive operational data. Weak protective measures could result in significant data leaks, which may breach regulatory requirements, such as the General Data Protection Regulation (GDPR) and other relevant industry compliance regulations [51].

In addition, cybersecurity threats are addressed insufficiently with a majority of operational frameworks, as they fail to respond to new and rapidly evolving risk scenarios. They are often based on static thresholds and historical data, which makes them useless for real-time cyberattacks and unpredictable attack angles [14, 52]. This emphasizes the need for intelligence and more flexible defense systems for automated responses.

Table 3. Summary of emerging technologies and the future in IIoT security.

Innovation	Techniques	Benefits	Challenges
AI-driven Threat Prediction	ML-based VNF placement (XGBoost), traffic classification	Fast, adaptive, highly accurate	Requires retraining and quality data
Lightweight Security Protocols	ECC, DTLS, secure CoAP, AES-128	Efficient on constrained devices	Trade-off with robustness
Digital Twin Security	Virtual replicas for anomaly simulation	Predictive detection, system modeling	High initial setup, not yet mainstream
Privacy-Preserving ML	On-device learning, federated models	Reduces data exposure risks	Complex coordination
Real-Time IDS Systems	Fog-based IDS, fast mitigation VNFs	Low latency, local response	Edge resource constraints

To meet these issues, shifts requiring a need for cross-domain and scalable security, which go beyond traditional approaches, are on the rise. The merging of IIoT with 5G advancements and cloud computing services opens up possibilities for more robust, scalable, and adaptive defensive infrastructures [38, 53]. Moreover, employing a ZTA (Zero Trust Architecture) configured specifically for IIoT frameworks can improve overall network security by enforcing continuous identity validation, eliminating implicit trust assumptions, insider threats, and horizontal movement on trusted connections.

A promising emerging solution involves utilizing digital twin technology, which simulates physical assets in real time. Digital twins enhance proactive anomaly detection and risk forecasting while enabling virtual patch testing, minimizing live-update disruptions, and improving security agility [54–56]. Moreover, as the complexity and autonomy of IIoT systems grow, the inclusion of explainable artificial intelligence (XAI) becomes more critical. By providing human-readable rationales for model decisions, particularly in anomaly detection, XAI enhances transparency, trust, and accountability in industrial systems essential to business operations.

This ensures accountability and trust in automated threat detection systems, particularly where decisions impact safety or compliance [57]. Emerging Generative AI (GenAI) models such as GANs and transformers are increasingly being used for generating synthetic data, simulating sophisticated attacks, and enhancing detection accuracy in low-data environments [31]. Lastly, future architectures should embed policy-driven automation to enhance consistency, responsiveness, and compliance. Techniques such as intent-based networking, coupled with formal policy specification languages, can help enforce adaptive security rules, minimize manual errors, and reduce reaction time during cyber incidents [58]. The year-wise distribution of targeted studies is provided in Table 4.

A visual summary of the year-wise distribution of selected studies is provided in Figure 8.

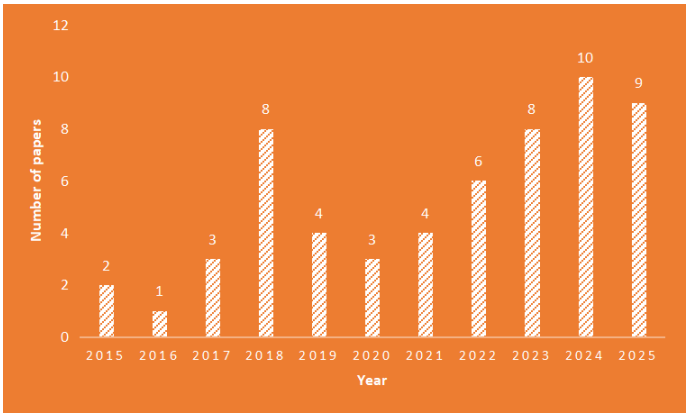

Figure 8. Year-wise distribution of selected studies.

8 Conclusion

The IIoT offers transformative advantages for industrial systems but also introduces significant cybersecurity challenges. This review has examined key threats such as DoS, data injection, and APTs, along with mitigation approaches including threat modeling, AI-driven IDS, blockchain frameworks, and software-defined networking. Persistent challenges such as scalability, fragmented standards, latency-security trade-offs, and real-time monitoring limitations remain unresolved. The growing heterogeneity of IIoT devices, lack of unified policies, and privacy concerns further complicate secure

Table 4. Year-wise summary of selected studies.

Year	References	Contribution
2015	[29, 48]	Early cryptography protocols and basic IIoT security frameworks
2016	[24]	Physical layer threats, such as jamming and device tampering
2017	[2, 21, 22]	Introduction of lightweight protocols; MiTM attack case studies
2018	[6, 7, 11, 12, 27, 49–51]	Standardization issues, threat modeling (STRIDE/DREAD), data privacy, and protocol vulnerabilities
2019	[8, 13, 37, 52]	Blockchain security use cases and early AI for IDS
2020	[1, 9, 35]	Security architectures and fog computing for IIoT security
2021	[5, 18, 23, 25]	STPA-Sec modeling, physical attacks, and hardware security
2022	[15, 30, 36, 39, 43, 44]	ML-based IDS, VNF deployments, and homomorphic encryption
2023	[10, 14, 20, 26, 38, 46, 53, 57]	Edge computing, federated learning, privacy-preserving techniques, and XAI
2024	[4, 16, 19, 28, 31, 32, 40, 47, 54, 56]	Discuss AI-based model classifiers like SVM, NB, DT,RF, CNN, LSTM, Digital twins enhance proactive anomaly detection and risk forecasting
2025	[3, 17, 33, 34, 41, 42, 45, 55, 58]	To address privacy concerns in distributed industrial environments, privacy-preserving machine learning models are gaining prominence. Distributed systems address key concerns.

deployments. Emerging solutions like digital twins for threat simulation, Zero Trust Architectures for continuous verification, and generative AI for synthetic anomaly detection represent promising directions. Likewise, explainable AI (XAI) and policy-driven automation will be essential for building resilient, interpretable, and adaptive security systems. A secure, scalable, and future-ready IIoT ecosystem will depend on the seamless integration of these advanced technologies with regulatory compliance and real-time responsiveness. This review aims to guide both researchers and practitioners toward sustainable cybersecurity innovations in the era of Industry 4.0. Despite providing a broad overview of IIoT security strategies this review is limited by the rapidly evolving nature of the field where many solutions are still in experimental or at prototype stages. Additionally, the review focuses primarily on technical aspects and does not deeply explore regulatory, organizational or economic barriers to the security solution implementations.

Data Availability Statement

Data will be made available on request.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieta, A. (2020). Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0. *Journal of Manufacturing Systems, 57*, 367-378. [Crossref]

[2] Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal, 4*(6), 1802-1831. [Crossref]

[3] Lezzi, M., Corallo, A., Lazoi, M., & Nimis, A. (2025). Measuring cyber resilience in industrial IoT:

a systematic literature review. *Management Review Quarterly*, 1-55. [Crossref]

[4] Presekal, A., Ştefanov, A., Rajkumar, V. S., Semertzis, I., & Palensky, P. (2024). Advanced persistent threat kill chain for cyber-physical power systems. *IEEE Access*. [Crossref]

[5] Serror, M., Hack, S., Henze, M., Schuba, M., & Wehrle, K. (2020). Challenges and opportunities in securing the industrial internet of things. *IEEE Transactions on Industrial Informatics, 17*(5), 2985-2996. [Crossref]

[6] Ekolle, Z. E., Kimio, K., & Ryuji, K. (2018, November). Intelligent security monitoring in time series of DDoS attack on IoT networks using grammar base filtering and clustering. In *2018 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)* (pp. 37-42). IEEE. [Crossref]

[7] Sikder, A. K., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. S. (2018). A survey on sensor-based threats to internet-of-things (iot) devices and applications. *arXiv preprint arXiv:1802.02041*.

[8] Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Edge intelligence: Paving the last mile of artificial intelligence with edge computing. *Proceedings of the IEEE, 107*(8), 1738-1762. [Crossref]

[9] Pliatsios, D., Sarigiannidis, P., Lagkas, T., & Sarigiannidis, A. G. (2020). A survey on SCADA systems: secure protocols, incidents, threats and tactics. *IEEE Communications Surveys & Tutorials, 22*(3), 1942-1976. [Crossref]

[10] Rathee, G., Ahmad, F., Jaglan, N., & Konstantinou, C. (2022). A secure and trusted mechanism for industrial IoT network using blockchain. *IEEE Transactions on Industrial Informatics, 19*(2), 1894-1902. [Crossref]

[11] Görmüş, S., Aydın, H., & Ulutaş, G. (2018). Nesnelerin interneti teknolojisi için güvenlik: Var olan mekanizmalar, protokoller ve yaşanılan zorlukların araştırılması. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 33*(4), 1247-1272. [Crossref]

[12] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544-546. [Crossref]

[13] Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials, 21*(3), 2702-2733. [Crossref]

[14] De Oliveira, G. W., Nogueira, M., dos Santos, A. L., & Batista, D. M. (2023). Intelligent VNF placement to mitigate DDoS attacks on industrial IoT. *IEEE Transactions on Network and Service Management, 20*(2), 1319-1331. [Crossref]

[15] Sarjan, H., Ameli, A., & Ghafouri, M. (2022). Cyber-security of industrial internet of things in electric power systems. *IEEE Access, 10*, 92390-92409. [Crossref]

[16] Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems, 4*, 186-202. [Crossref]

[17] Ali, M. A., & Al-Sharafi, S. A. H. (2025). Intrusion detection in IoT networks using machine learning and deep learning approaches for MitM attack mitigation. *Discover Internet of Things, 5*(1), 1-13. [Crossref]

[18] Yu, J., Wagner, S., & Luo, F. (2021). Data-flow-based adaption of the system-theoretic process analysis for security (STPA-sec). *PeerJ Computer Science, 7*, e362. [Crossref]

[19] Silawi, E., Shaked, A., & Reich, Y. (2024, July). TRANSLATING THE STPA-SEC SECURITY METHOD INTO A MODEL-BASED ENGINEERING APPROACH. In *INCOSE International Symposium* (Vol. 34, No. 1, pp. 1948-1963). [Crossref]

[20] Gupta, S. K., Chandan, R. R., Shukla, R., Singh, P., Pandey, A. K., & Jaiswal, A. K. (2023). Original Research Article Heterogeneity issues in IoT-driven devices and services. *Journal of Autonomous Intelligence, 6*(2). [Crossref]

[21] Panchal, A. C., Khadse, V. M., & Mahalle, P. N. (2018, November). Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures. In *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)* (pp. 124-130). IEEE. [Crossref]

[22] Lei, X., Tu, G. H., Liu, A. X., Ali, K., Li, C. Y., & Xie, T. (2017). The insecurity of home digital voice assistants–amazon alexa as a case study. *arXiv preprint arXiv:1712.03327*.

[23] Jain, A., Zhou, Z., & Guin, U. (2021, May). Survey of recent developments for hardware trojan detection. In *2021 IEEE international symposium on circuits and systems (iscas)* (pp. 1-5). IEEE. [Crossref]

[24] Choo, K. K. R., Domingo-Ferrer, J., & Zhang, L. (2016). Cloud cryptography: Theory, practice and future research directions. *Future Generation Computer Systems, 62*, 51-53. [Crossref]

[25] Shepherd, C., Markantonakis, K., Van Heijningen, N., Aboulkassimi, D., Gaine, C., Heckmann, T., & Naccache, D. (2021). Physical fault injection and side-channel attacks on mobile devices: A comprehensive analysis. *Computers & Security, 111*, 102471. [Crossref]

[26] Alotaibi, B. (2023). A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors, 23*(17), 7470. [Crossref]

[27] Sharma, P. K., & Park, J. H. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems, 86*, 650-655. [Crossref]

[28] Kumar, S., Kumar, D., Dangi, R., Choudhary, G., Dragoni, N., & You, I. (2024). A review of lightweight

security and privacy for resource-constrained IoT devices. *Computers, Materials and Continua, 78*(1), 31-63. [CrossRef]

[29] Vučinić, M., Tourancheau, B., Watteyne, T., Rousseau, F., Duda, A., Guizzetti, R., & Damon, L. (2015, August). DTLS performance in duty-cycled networks. In *2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* (pp. 1333-1338). IEEE. [Crossref]

[30] Astorga, J., Barcelo, M., Urbieta, A., & Jacob, E. (2022). Revisiting the feasibility of public key cryptography in light of iiot communications. *Sensors, 22*(7), 2561. [Crossref]

[31] Kavitha, D., & Thejas, S. (2024). Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. *IEEE Access*. [Crossref]

[32] Sadhwani, S., Modi, U. K., Muthalagu, R., & Pawar, P. M. (2024). SmartSentry: Cyber threat intelligence in industrial IoT. *IEEE Access, 12*, 34720-34740. [Crossref]

[33] Ali, A., Husain, M., & Hans, P. (2025). Federated Learning-Enhanced Blockchain Framework for Privacy-Preserving Intrusion Detection in Industrial IoT. *arXiv preprint arXiv:2505.15376*.

[34] Karunamurthy, A., Vijayan, K., Kshirsagar, P. R., & Tan, K. T. (2025). An optimal federated learning-based intrusion detection for IoT environment. *Scientific Reports, 15*(1), 8696. [Crossref]

[35] Liu, Y., Garg, S., Nie, J., Zhang, Y., Xiong, Z., Kang, J., & Hossain, M. S. (2020). Deep anomaly detection for time-series data in industrial IoT: A communication-efficient on-device federated learning approach. *IEEE Internet of Things Journal, 8*(8), 6348-6358. [Crossref]

[36] Rafique, Y., Leivadeas, A., & Ibnkahla, M. (2022, April). An IoT-aware VNF placement proof of concept in a hybrid edge-cloud smart city environment. In *2022 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1395-1400). IEEE. [Crossref]

[37] Forti, S., Paganelli, F., & Brogi, A. (2022). Probabilistic QoS-aware placement of VNF chains at the edge. *Theory and Practice of Logic Programming, 22*(1), 1-36. [Crossref]

[38] Mohamed, D., & Ismael, O. (2023). Enhancement of an IoT hybrid intrusion detection system based on fog-to-cloud computing. *Journal of Cloud Computing, 12*(1), 41. [Crossref]

[39] Gudla, S. P. K., Bhoi, S. K., Nayak, S. R., Singh, K. K., Verma, A., & Izonin, I. (2022). A deep intelligent attack detection framework for fog-based IoT systems. *Computational Intelligence and Neuroscience, 2022*(1), 6967938. [Crossref]

[40] Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. *Computers and Education: Artificial Intelligence, 7*, 100327. [Crossref]

[41] Abdullahi, S. M., & Lazarova-Molnar, S. (2025). On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: a comprehensive guide with recent advances. *International Journal of Information Security, 24*(1), 53. [Crossref]

[42] Kerkeni, R., Mhalla, A., & Bouzrara, K. (2025). Unsupervised Learning and Digital Twin Applied to Predictive Maintenance for Industry 4.0. *Journal of Electrical and Computer Engineering, 2025*(1), 3295799. [Crossref]

[43] Varghese, S. A., Ghadim, A. D., Balador, A., Alimadadi, Z., & Papadimitratos, P. (2022, March). Digital twin-based intrusion detection for industrial control systems. In *2022 IEEE international conference on pervasive computing and communications workshops and other affiliated events (PerCom workshops)* (pp. 611-617). IEEE. [Crossref]

[44] Halder, S., & Newe, T. (2022). Enabling secure time-series data sharing via homomorphic encryption in cloud-assisted IIoT. *Future Generation Computer Systems, 133*, 351-363. [Crossref]

[45] Tawfik, A. M., Al-Ahwal, A., Eldien, A. S. T., & Zayed, H. H. (2025). PriCollabAnalysis: privacy-preserving healthcare collaborative analysis on blockchain using homomorphic encryption and secure multiparty computation. *Cluster Computing, 28*(3), 191. [Crossref]

[46] Songhorabadi, M., Rahimi, M., MoghadamFarid, A., & Kashani, M. H. (2023). Fog computing approaches in IoT-enabled smart cities. *Journal of Network and Computer Applications, 211*, 103557. [Crossref]

[47] Sharma, G. (2024). A survey on secure communication technologies for smart grid cyber physical system. *e-Prime-Advances in Electrical Engineering, Electronics and Energy, 10*, 100831. [Crossref]

[48] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks, 76*, 146-164. [Crossref]

[49] Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE access, 6*, 46134-46145. [Crossref]

[50] Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks, 141*, 199-221. [Crossref]

[51] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access, 6*, 32979-33001. [Crossref]

[52] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access, 7*, 82721-82743. [Crossref]

[53] Chui, K. T., Gupta, B. B., Liu, J., Arya, V., Nedjah, N., Almomani, A., & Chaurasia, P. (2023). A survey of internet of things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions. *Information, 14*(7), 388. [Crossref]

[54] Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks, 156*, 103414. [Crossref]

[55] Asim, M., Tariq, N., Awad, A. I., Waheed, F., Ullah, U., & Murtaza, G. (2025). SecT: A Zero-Trust Framework for Secure Remote Access in Next-Generation Industrial Networks. *IEEE Journal on Selected Areas in Communications*. [Crossref]

[56] Xu, L., Yu, H., Qin, H., Chai, Y., Yan, N., Li, D., & Chen, Y. (2023). Digital twin for aquaponics factory: Analysis, opportunities, and research challenges. *IEEE Transactions on Industrial Informatics, 20*(4), 5060-5073. [Crossref]

[57] Gaitan-Cardenas, M. C., Abdelsalam, M., & Roy, K. (2023, July). Explainable AI-based intrusion detection systems for cloud and IoT. In *2023 32nd International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-7). IEEE. [Crossref]

[58] Trantzas, K., Brodimas, D., Agko, B., Tziavas, G. C., Tranoris, C., Denazis, S., & Birbas, A. (2025). Intent-driven network automation through sustainable multimodal generative AI. *EURASIP Journal on Wireless Communications and Networking, 2025*(1), 42. [Crossref]



AAMIR ALI is a dedicated researcher in artificial intelligence, healthcare analytics, and IoT environments. His expertise includes machine and deep learning applications in medical diagnosis, speech recognition, and facial emotion recognition. He has also worked on IoT-focused projects such as malware classification, anomaly detection, and cyberattack prediction. Aamir is passionate about developing AI-driven solutions for early disease detection and improving patient care. He actively contributes to interdisciplinary research across clinical and image data domains. (Email: amirali4436823@gmail.com)



Misbah Ali is a PhD scholar at COMSATS university Islamabad, with research interests in Machine Learning, Deep Learning, Generative Artificial Intelligence, and Software Engineering. Her work focuses on the development of secure, intelligent systems across domains such as healthcare, education, and industrial cyber-security. She has authored multiple peer-reviewed publications and presented her research at international conferences. She also contributes to the academic community as a reviewer for several reputed journals. (Email: talktomisbah.ali@gmail.com)



Uqba Mushtaq received a Bachelor of Science (BS) degree in Computer Science from COMSATS University Islamabad, Sahiwal Campus. Her research interests include Artificial Intelligence, Machine Learning, Deep Learning, and Ensemble Learning. She is particularly interested in developing intelligent systems that can support decision-making and improve real-world applications such as healthcare diagnostics and predictive modeling. Uqba is passionate about applying data-driven approaches to solve complex problems and aims to contribute to innovative AI solutions in both academic and industrial settings. (Email: uqbamushtaq160@gmail.com)



Malik Arslan Akram is a student in Software Engineering at Southwest University of Science and Technology, China specializing in Automatic Speech Recognition (ASR), Natural Language Processing (NLP), and deep learning. His research focuses on optimizing real-time dialogue systems using large language models and advanced model engineering. He is passionate about developing innovative AI solutions that enhance seamless and intelligent human–machine communication. (Email: arsslan96@mails.swust.edu.cn)