Journal of Distributed Computing and Systems(JDCS)
Vol.9, Issue 1, 2026, Pages 31-50

Integration of Industrial IoT and Blockchain Based on Security and Privacy -A Survey

Maryam Hajiee [1], Zeynab MehraniRad [2], Hediyeh Moradi [3]
Department of Computer Engineering, ST.C., Islamic Azad University, Tehran, Iran

Article History:
Received: 22 January 2026
Received in revised form: 26 March 2026
Accepted: 30 May 2026
Available online: 15 August 2026

Abstract

The Industrial Internet of Things (IIoT) is a cornerstone of Industry 4.0, yet its reliance on centralized architectures introduces critical vulnerabilities, including single points of failure, data tampering, and privacy breaches. As the global number of IoT devices is projected to exceed 40 billion by 2030, traditional security models fail to scale, necessitating decentralized frameworks. Blockchain technology emerges as a transformative solution, offering immutability, transparency, and distributed trust through smart contracts.

This paper provides a comprehensive survey of recent advancements (2022-2025) in integrating blockchain with IIoT infrastructures. We systematically analyze how blockchain-based mechanisms address multi-layer security challenges, focusing on secure device authentication, tamper-proof transaction logging, and decentralized access control. A key contribution of this study is the evaluation of consensus algorithms-such as Proof of Authority (PoA) and Delegated Proof of Stake (DPoS)-optimized for resource-constrained industrial environments to mitigate the high energy consumption of traditional models.

Furthermore, we explore the convergence of blockchain with Edge Computing and Artificial Intelligence (AI) to enhance real-time anomaly detection and reduce latency in distributed IIoT ecosystems. Despite the advantages, practical deployment is hindered by scalability bottlenecks and the limited computational power of edge devices. This survey categorizes emerging solutions, including lightweight cryptographic schemes and hierarchical blockchain architectures, which facilitate secure, multi-party collaboration without central intermediaries. By synthesizing current research trends and identifying open challenges, this work provides a roadmap for building resilient, autonomous, and scalable next-generation industrial networks.

Keywords: IIoT, Blockchain, security, Privacy, Industry 4.0

I. INTRODUCTION

The Internet of Things (IoT) refers to a network of interconnected devices that can be controlled through communication networks, enabling real-time data collection, exchange, and processing [1-7]. These devices can be either mechanical or digital machines that operate over the internet without the need for human interaction [5, 8]. In a broader sense, IoT encompasses any object that collects data through sensors, transmits it via the internet, and communicates through cloud networks [5]. As a result, IoT is considered one of the core infrastructures of the Fourth Industrial Revolution (Industry 4.0), with its primary goal being the automation, digitalization, and data exchange in industrial environments [1, 4, 6, 8-10].

The IoT can be integrated with other technologies such as Artificial Intelligence, Big Data, advanced robotics, Blockchain, and Cloud Computing, thereby optimizing industrial processes [1, 5, 8, 11]. Through sensors in Industrial IoT (IIoT) devices, real-time data is gathered from machines and, when necessary, shared with other systems or devices [1-5]. Utilizing intelligent technologies and data analytics, it can facilitate predictive maintenance, resource management, industrial process optimization [1, 5, 8, 11], and environmental preservation [1, 8, 12].

IIoT is employed to connect machines and devices within industrial environments and focuses on machine-to-machine (M2M) communication in a centralized network. Any malfunction in these systems could lead to high-risk damage, and the volume of data collected in IIoT is significantly larger than in IoT [11, 13]. The use of Blockchain can enhance the automation and security of industrial processes and M2M communications [11].

According to predictions by the IoT Analytics platform, the global number of IoT-connected devices is expected to grow by approximately 13% by 2025, reaching around 25.8 billion devices. This represents an increase of 15.2 billion devices compared to 2019. Furthermore, this figure is anticipated to double by 2030, surpassing 40 billion connected devices worldwide [3, 8, 14, 15]. With the rapid growth and widespread penetration of the Internet of Things across various domains, coupled with the complex nature and resource limitations of devices, numerous challenges related to security and privacy arise [2, 3, 8, 11, 16, 17]. For instance, in 2024, 1.7 billion cyberattacks were reported, marking a 13.3% increase compared to 2023, with the cost of each security breach estimated at $4.2 million [15]. Additionally, 70% of the most commonly used IoT devices are vulnerable to various types of cyberattacks [8]. Therefore, the consequences of these challenges cannot be overlooked and must be addressed.

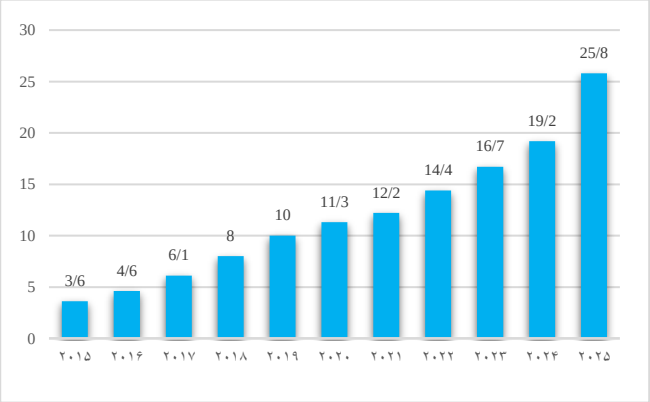

Figure 1- Statistics on IoT Security Challenges

IoT ecosystems, due to their centralized architecture [2], heterogeneity [3, 4, 8, 10, 17, 18], distributed nature [10, 14], and resource limitations [2, 3, 8, 17, 18], face a complex array of threats. These ecosystems consist of numerous nodes and devices with varying capabilities [19], which are susceptible to risks such as data breaches, malware injection, phishing attacks, DDoS and DoS attacks and insider threats [3, 5, 8, 20].

To mitigate these threats, resilient architectures and Fault-Tolerant Systems are essential. In the design of such ecosystems, advanced Intrusion Detection Systems (IDS) [20, 21] and security standards must be implemented at all layers of the system to maintain network security. Moreover, when designing these systems, the impact of the number of devices, communication standards and protocols, and cost analysis for scalability should be considered. Devices must possess attributes such as processing power, communication capability, and security to ensure the integrity and proper functioning of the IIoT system [19].

Centralized security systems are confronted with single points of failure, unauthorized data modifications, and privacy breaches [2, 7, 20, 22, 23]. Additionally, dependence on opaque third-party services represents another significant challenge in industrial IoT [2, 4, 7, 11, 17, 21, 23].

II. Research Purpose

The purpose of this survey is to provide a comprehensive and structured analysis of the security challenges in the Industrial Internet of Things (IIoT) and to evaluate the potential of blockchain technology as a decentralized solution for enhancing trust, privacy, and resilience in industrial environments. By systematically examining existing literature, this study highlights the limitations of traditional centralized security models, identifies the major threats across different layers of IIoT architectures, and reviews state-of-the-art cryptographic, consensus, and anomaly-detection mechanisms. Furthermore, the survey aims to assess how blockchain through its inherent features such as decentralization, immutability, transparency, and smart contracts can address IIoT vulnerabilities and support secure, scalable, and autonomous industrial ecosystems. Ultimately, this work seeks to synthesize current research trends, identify open challenges, and provide insights that guide future advancements in secure IIoT–blockchain integration.

III. Research Methodology

This study adopts a systematic literature review (SLR) methodology to provide a comprehensive and unbiased overview of blockchain-based security and privacy solutions in Industrial Internet of Things (IIoT) environments. The review process was carefully designed to ensure transparency, reproducibility, and methodological rigor, and it consists of four main stages: formulation of research questions, literature identification and selection, data extraction and synthesis, and quality assessment.

A. Research Questions

The review is driven by four core research questions that define the scope and objectives of this survey:

- RQ1: What are the main security and privacy challenges in IIoT ecosystems?
- RQ2: In what ways can blockchain technology mitigate these challenges?
- RQ3: What blockchain-based solutions have been proposed for securing IIoT, and what are their respective strengths and limitations?
- RQ4: What open issues and future research directions remain in this area?

These questions ensure that the survey not only summarizes existing work but also critically evaluates current approaches and identifies research gaps.

B. Literature Search Strategy

A systematic search was conducted across five major academic databases: IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Google Scholar. The search query was formulated using combinations of keywords and Boolean operators as follows:

("Industrial IoT" OR "IIoT") AND "blockchain" AND ("security" OR "privacy") AND ("survey" OR "review" OR "framework")

To capture recent advances, the publication period was restricted to studies published between 2018 and 2025. The initial search yielded more than 500 candidate papers.

C. Inclusion and Exclusion Criteria

The retrieved studies were filtered using predefined inclusion and exclusion criteria.

Inclusion criteria:

- Peer-reviewed journal articles, conference papers, and well-established survey studies.
- Works explicitly addressing blockchain integration for IIoT security and/or privacy.
- Studies proposing architectures, frameworks, or empirical evaluations.

Exclusion criteria:

- Non-English publications.

- Studies focusing on generic IoT scenarios without industrial context.
- Editorials, short abstracts, and duplicate or overlapping works.

D. Study Selection Process

The selection procedure followed the PRISMA framework. First, titles and abstracts were screened to remove irrelevant papers. Next, the full texts of the remaining articles were examined against the inclusion and exclusion criteria. Finally, forward and backward snowballing was applied to identify additional relevant studies from the reference lists of the selected papers. This multi-stage process resulted in a final dataset of 72 high-quality papers for detailed analysis.

E. Data Extraction and Synthesis

A structured data extraction form was designed to collect key information from each study, including authorship, publication year, venue, proposed solution, blockchain type, consensus mechanism, cryptographic methods, evaluation metrics, and reported strengths and limitations. The extracted information was synthesized thematically to answer the research questions. The comparative results are summarized in a series of tables (Tables 1–18) to facilitate cross-study analysis.

F. Quality Assessment

To ensure the reliability of the findings, each paper was evaluated based on three dimensions: (i) credibility of the publication venue, (ii) methodological rigor in terms of experimental design and validation, and (iii) relevance to IIoT security and blockchain integration. Studies with limited methodological transparency or weak evaluation were explicitly marked as having potential limitations.

G. Methodological Limitations

Despite the systematic nature of the review, certain limitations remain. The selection of databases and keywords may have introduced bias, while the exclusion of non-English and grey literature may have led to the omission of some relevant contributions. Furthermore, given the rapid evolution of blockchain and IIoT technologies, very recent studies published after the search period may not be included.

IV. STRUCTURE OF THE PAPER

The remainder of this survey is organized as follows. Section V presents the research background, including blockchain fundamentals, consensus algorithms, smart contracts, IoT security requirements, lightweight cryptography, zero-knowledge proofs, IIoT architecture, and computing architectures. Section VI provides a comprehensive review of the selected research papers and presents a comparative analysis of their proposed approaches. Finally, Section VII concludes the survey, while Section VIII outlines future research directions.

V. RESEARCH BACKGROUND

A. Blockchain

Blockchain is a distributed ledger technology that functions as a "register," recording transactions within this network, such that each node (participating computer) validates and stores the block of data being exchanged [11, 12, 14, 16, 24, 26]. Each new block contains at least the cryptographic hash of the previous block, along with the transaction-related data [16]. Given the massive volume of data generated in the Industrial Internet of Things (IIoT), blockchain can maintain the ledger of data exchanges or transactions in an immutable manner [1, 4, 11, 12, 14, 16, 17, 22, 24, 25].

The advantages of employing blockchain in the Industrial Internet of Things (IIoT) include improved data security, decentralization, and enhanced trustworthiness [4,24], data immutability, and the automation of processes through smart contracts, which reduces the need for intermediaries [1]. Smart contracts are algorithms that execute on the blockchain whenever a predefined action occurs; all network nodes receive this algorithm and execute it according to the defined logic [11]. Smart contracts are used for managing data transactions and controlling access. These contracts enforce predefined rules and ensure data traceability and auditing[26].

The distributed and immutable nature of blockchain makes it ideal for traceability [1, 18, 21, 22] and data provenance[14]. In the context of IoT, blockchain provides a secure and transparent method for recording and sharing data. Therefore, blockchain is highly suitable for implementing data storage traceability and access management [1, 16, 22].

For example, the proposed framework in [27], which combines trust-based device evaluation with a private blockchain, achieved a success rate of approximately 91% in maintaining secure and reliable network operations. This performance significantly outperformed the baseline IIoT network without blockchain integration, which was more vulnerable to malicious device attacks and data tampering.

Table 1 Advantages of Blockchain in Integration with IIoT

Decentralization	[1, 2, 4, 7, 11, 12, 14, 16, 17, 21, 22, 24, 25]
Security	[1, 7, 11, 16, 17, 21, 22, 24, 25]
Transparency	[1, 2, 7, 12, 14, 16, 17, 21, 22, 24, 25]
Immutability	[1, 4, 11, 12, 14, 16, 17, 22, 24, 25, 28]
Authentication and Access Control	[2, 17]
Integrity	[5, 21, 25]

Table 2 Challenges of Blockchain in Integration with IIoT

Scalability	[1, 2, 4, 7, 11, 12, 16, 17, 29]
Energy Consumption	[1, 11, 12, 16, 17, 29]
Complexity Integration	[11, 12, 16, 17, 21]

Cost	[1, 2, 11, 16, 17]
Regulatory Compliance	[2, 16, 17]
Privacy and Data Security	[1, 4, 11, 17, 29]
Interoperability Between IoT Devices and Blockchain	[2, 4, 11, 12]

The selection of a consensus mechanism is a central issue in the integration of Blockchain and IoT [1, 17]. Well-known consensus algorithms, such as Proof of Work (PoW) and Proof of Stake (PoS), are employed for data validation, alongside cryptographic mechanisms like SHA-256 hashing, asymmetric key pairs for node authentication, and data segmentation in off-chain and on-chain modes[4, 11]. However, traditional PoW and PoS algorithms are not particularly effective for limited IoT scenarios [17], as they have high energy consumption [1] and are vulnerable to security threats [30]. Consequently, low-energy consensus systems are being used to reduce the energy consumption of blockchain networks [17]. The implementation of these methods is highly complex and faces interoperability challenges, which hinder their widespread adoption[2].

B. Consensus Algorithm

A consensus algorithm is a process that ensures collective agreement and stores information in the decentralized database of the network. In blockchain, consensus is used to ensure that all nodes in the network agree on the current state of the network and the validity of transactions. This is crucial for maintaining the security and integrity of the blockchain. The consensus algorithm guarantees that the data between nodes remains consistent for a given proposal. An appropriate consensus algorithm can keep the blockchain network active and provide a steady, efficient computational power flow throughout the entire network, while a weak algorithm can make the network vulnerable to attacks, leading to its paralysis. Therefore, the use of an appropriate consensus algorithm for each application type can ensure data storage efficiency, transaction finality, and data integrity [28, 31].

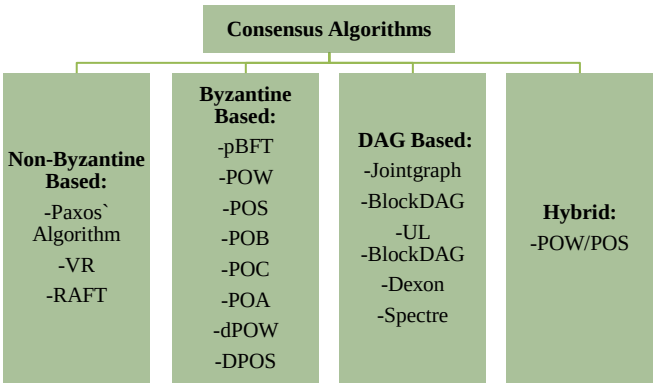

Figure 2- Overview of major categories of blockchain consensus mechanisms and their representative algorithms

1) Proof of Authority (PoA)

Proof of Authority (PoA) is a consensus algorithm specifically designed for private blockchains and provides an effective solution to the needs of these networks. Compared to other consensus mechanisms, the PoA algorithm has a lower level of decentralization and relies on the reputation and authority of validators, rather than on technical competition. This mechanism automatically filters low-commitment or inactive validators and does not require high computational power, resulting in very low energy consumption [32].

One of the main advantages of PoA is its ability to process a larger number of transactions simultaneously and reduce their confirmation time. This algorithm requires fewer computational and energy resources compared to Proof of Work (PoW) and Proof of Stake (PoS), while also providing adequate resistance to 51% attacks, making it an appropriate choice for private blockchain networks. To enhance transaction security, PoA typically requires multiple confirmations from different validators to ensure that transactions remain secure and valid [30, 31].

However, unlike PoW and PoS, traditional versions of PoA are vulnerable to low-cost cloning attacks. To address this weakness, solutions such as the use of threshold cryptography and hierarchical clustering of validators have been proposed [31].

2) Proof of Work (PoW)

Proof of Work (PoW) is one of the oldest consensus mechanisms in blockchain, ensuring security, integrity, and resistance to network attacks through significant computational power consumption [31]. In this algorithm, miners validate and add new blocks to the chain by finding a suitable "Nonce" that brings the block's hash to meet predefined conditions. However, PoW has a very high energy consumption, and even with hardware optimization, significant energy reduction is difficult, leading to considerable environmental impacts. These limitations, especially in resource-constrained environments such as the Internet of Things (IoT), have prompted the shift towards alternative solutions like Proof-of-Stake (PoS) or Directed Acyclic Graph (DAG)-based structures, which can reduce energy consumption by over 99%, although they come with challenges, such as the potential for validator centralization [32].

3) Proof of Stake (PoS)

Proof of Stake (PoS) is a consensus mechanism that, instead of relying on energy-intensive computational competition, uses the staking of nodes to select the validator for the next block. In this method, nodes that share their resources within the network are chosen randomly or based on a combination of criteria such as the size of their stake, increasing their chances of being selected for transaction validation and block creation. PoS has significantly lower energy consumption compared to traditional methods and contributes to the decentralization and security of the network, as setting up a node does not require expensive equipment. Additionally, this approach can help manage trust between devices, validate data transactions, and reduce energy consumption in large-scale networks, such as those in the Internet of Things (IoT). To ensure proper functioning,

backup mechanisms for absent validators are also considered[31].

4) Delegated Proof of Stake (DPoS)

A voting system based on PoS has been introduced, reducing the time required to produce a block to 3 seconds. As a result, it consumes significantly less energy compared to PoW. In a DPoS-based system, the network nodes are divided into three groups: witnesses, delegates, and workers. The core component of the system, the witnesses, is selected by all nodes through resource-based voting.

Table 3-Consensus Algorithms

Feature	PoW	PoS	PoA	DPoS
Openness	Permissionless	Permissionless	Permissioned	Permissionless
Trust	Trustless	Trustless	Participants (Authorities)	Trustless
Adversary Tolerance	<25%	<51%	<51%	<51%
Resource Consumption	High	High	Low	Medium
Latency	High	Medium	Low	High
Transaction Rate	Low	High	High	High
Throughput	Low	Medium	High	High
Energy Consumption	High	Medium	Low	Low

C. Smart Contract

A smart contract is a digital agreement whose terms are recorded as code on the blockchain. These contracts are executed automatically, eliminating the need for intermediaries or third-party entities, thus enabling transactions between parties without direct contact and reducing costs. The advantages of smart contracts include reduced transaction risk, lowered service and management costs, increased process efficiency, and the establishment of trust between parties. However, software errors or vulnerabilities can lead to financial and reputational damages, as smart contracts are immutable once deployed, meaning that if errors occur, they must be canceled and re-implemented. This technology enables the secure and automatic execution of real-world contract provisions in a digital environment and is recognized across various industries as an efficient alternative to traditional transaction mechanism [33-35].

D. Security in Multi-Layer IoT Architecture

As a convergent and multi-network system, the Internet of Things (IoT) not only shares many common security issues with sensor networks, mobile communication networks, and the Internet but also introduces unique security features and challenges in areas such as privacy protection, authentication, access control, and secure data storage and management [21]. The IoT network structure significantly differs from traditional IT models [5]; in particular, sensor nodes in the perception layer are typically deployed in unsupervised environments and are highly limited in terms of processing power, energy, and memory [2, 8, 11, 16, 17, 21].

Given the variability in the number of layers in the IoT architecture, the security of Industrial IoT (IIoT) is a multi-dimensional issue, with attacks capable of targeting any layer of the architecture. Since IoT extends the sensor network and application layer over existing networks, its vulnerability to intrusion and misuse is higher than that of traditional network systems, and many common security solutions are not capable of providing reliable protection [21]. These characteristics have made IoT security a complex and multi-faceted issue. Moreover, security attacks can target different layers of the IoT architecture, and each layer is vulnerable to specific threats[5]. These attacks are generally classified into two broad categories: active attacks that disrupt the network's operation, and passive attacks that covertly collect information without causing disruption. One of the most common attacks that can affect all layers of IoT is a Denial-of-Service (DoS) attack, which disrupts access to network services and resources [5].

E. Intrusion Detection System (IDS)

Intrusion protection encompasses two aspects: pre-intrusion and post-intrusion protection. Pre-intrusion protection refers to the safeguarding of the network perimeter, and common technologies include network firewalls [33-35]. Post-intrusion protection concerns intrusion detection (IDS) [20, 21]. An Intrusion Detection System (IDS) is a system that monitors network traffic and activities, identifying any abnormal or malicious behavior that deviates from expected or predefined patterns. IDSs are divided into two main categories: signature-based and anomaly-based [20, 21]. These systems face challenges in Industrial Internet of Things (IIoT) environments, as traditional systems are designed for static and standardized IT environments and are not compatible with dynamic and multi-faceted IIoT networks [22]. The signature-based method cannot account for the continuous changes in cyber-attack techniques and requires constant database update [22], but it provides high accuracy, low false-positive rates, and fast execution times for known attacks [36]. Anomaly-based detection methods often generate high false-positive rates due to the complexity of IIoT traffic and the suboptimal base behavior of devices [22], but they have the advantage of identifying new or ambiguous attacks [36]. One of the challenges of IIoT devices is their limited computational power and memory, which leads to delays in threat detection and response [2, 8, 11, 16, 17, 19]. One proposed solution to

address this challenge is the use of AI-based technologies, which are gaining attention due to their ability to learn complex patterns and provide high accuracy in detection[20, 21]. For instance, ensemble models such as AdaBoost and Random Forest (RF), which combine multiple algorithms, offer high accuracy [36].

While AI helps in identifying security anomalies in IIoT, centralized security systems face challenges such as single points of failure, unauthorized data modifications, and privacy breaches [2, 7, 21, 24]. Additionally, reliance on non-transparent third-party services is another challenge in Industrial IoT [2, 4, 7, 11, 17, 19]. Therefore, a decentralized, tamper-proof, and scalable security framework is required to protect IIoT networks [2], and blockchain technology can assist in addressing these challenges.

F. Cryptography in Resource-Constrained Devices

Given the limited resources of IoT devices, implementing high-cost security protocols appears to be impractical [4, 8, 37]. As a result, in early IoT deployments, encryption is sometimes neglected, or static default credentials are used, leading to serious vulnerabilities. The lack of strong authentication by default is a well-known and, indeed, very common issue, allowing attackers to easily join the network [21, 37]. Network-based attacks such as MitM and DoS are mitigated by solutions like encryption and firewall systems, which are mandatory to ensure data confidentiality and system availability [8, 21].

Common cryptographic solutions like AES, while providing strong security guarantees, are unsuitable for IoT nodes due to resource constraints such as processing power, memory, and battery life [3, 4, 8, 9, 37]. To address these challenges, one proposed solution is the integration of lightweight encryption and blockchain, which guarantees confidentiality, integrity, and authentication with minimal computational overhead [3, 4, 8, 9, 37].

G. Lightweight cryptography

Lightweight cryptography is introduced as a low-cost and efficient approach for securing resource-constrained devices in the IoT. By eliminating the need for heavy certificates and employing compact key-exchange protocols, pre-shared symmetric keys, and elliptic-curve-based schemes, this method reduces energy consumption and latency while maintaining security, authentication, and data integrity. Due to memory, processing power, and bandwidth limitations in large-scale IoT networks, lightweight approaches are more practical and scalable [3, 37, 38].

Recent research directions focus on integrating lightweight cryptography with artificial intelligence, blockchain, and steganology to provide secure, scalable, and energy-efficient systems. Among these, blockchain, by offering a decentralized trust infrastructure and immutable records of interactions, can serve as an effective complement to integrity in dynamic and resource-constrained IoT environments [39].

Systematic review studies [3] indicate that elliptic-curve cryptography (ECC), due to its favorable strength-to-key-size ratio, has been widely adopted in IoT systems and is suitable for resource-constrained environments. However, standard ECC requires substantial computation and memory; therefore, to become lightweight, energy-efficient, and secure for authentication and confidentiality in IoT, it must be optimized. For greater adaptability, hybrid ECC models integrate auxiliary components such as fuzzy logic, blockchain mechanisms, and chaotic mappings. These integrations enable ECC to become more adaptive, decentralized, and resilient against evolving attack vectors.
ECC provides a high level of security while being lightweight due to its small key sizes. However, the implementation of ECC can be complex, and if improperly executed, it may introduce potential vulnerabilities [40].

Blockchain–ECC hybrid models ensure that trust propagation is preserved in multi-node systems such as IoT–Cloud and IoT–Drone infrastructures. Blockchain-based ECC sacrifices part of its energy efficiency in exchange for enhanced security or decentralization, which is advantageous

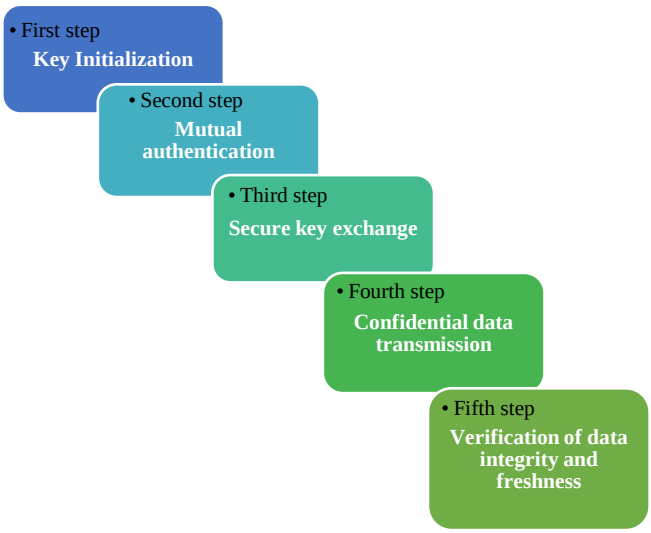

Figure 3-Five fundamental steps for the operation of a lightweight cryptographic algorithm

in high-risk IoT–Drone and IoT–Cloud environments [41].

Table 4-Cryptographic characteristics of ECC in integration with resource-constrained systems

Challenges	Advantages
Latency due to consensus mechanisms	Data integrity
Scalability bottlenecks	Decentralized trust

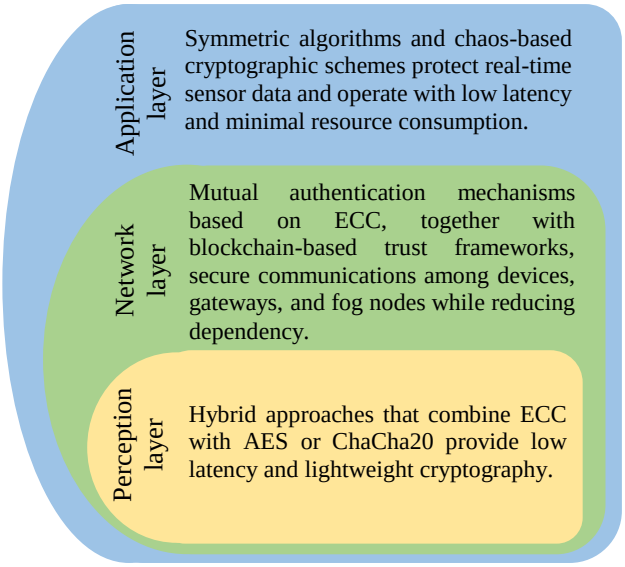

Figure 4-Cryptography across the various layers of the Internet of Things architecture

H. Zero-Knowledge Proof (ZKP)

A zero-knowledge proof (ZKP) is a cryptographic protocol by which a prover convinces a verifier that a given statement about private data is true without revealing any additional information beyond the validity of that statement. ZKPs guarantees that completeness, soundness and zero-knowledge [22].

ZKPs appear in interactive proofs and non-interactive proofs operational modes. Practically relevant families include zk-SNARKs, zk-STARKs, and other schemes such as Bulletproofs and folding-based constructions; each family trades off prover time, verifier time, proof size, setup requirements, and post-quantum resilience. These tradeoffs are central to selecting ZKP primitives for blockchain and resource-constrained IIoT deployments.

Table 5- ZKP mechanisms

zk-SNARKs	succinct, non-interactive arguments of knowledge that require a trusted setup in many instantiations
zk-STARKs	scalable transparent arguments based on collision-resistant hashes without trusted setup

In blockchain-integrated IIoT systems, ZKPs serve two main security functions: privacy-preserving verification enabling devices or users to prove without disclosing raw secrets or sensitive telemetry; and confidential validation on-chain allowing validators or smart contracts to check assertions about off-chain computation/data without receiving the underlying data, thereby reducing data exposure while preserving auditability and traceability. These uses have been repeatedly identified in recent journal surveys and system papers as among the principal motivations for applying ZKPs in blockchain-based IoT ecosystems.

Although ZKPs offer strong privacy guarantees, their deployment in Industrial IoT is constrained by prover computational cost, memory, communication overhead, and setup complexity. Resource-constrained end devices like sensors and actuators often cannot serve as full provers for heavy ZKP constructions; accordingly, contemporary research emphasizes lightweight ZKP protocols, delegation/remote-proving architectures, or hybrid designs in which fog/edge nodes or dedicated hardware assist or act as provers while preserving end-device privacy and non-repudiation. These practical performance and engineering challenges must be balanced against the security and trust objectives when integrating ZKPs into IIoT or blockchain stacks.

I. Layered IIoT Architecture

The layered architecture plays a key role in managing complexity and enhancing the flexibility of modern manufacturing systems. By separating functionalities and creating distinct layers, this architecture enables systems to be modular, adaptive, and distributed, such that each layer operates independently yet in coordination with the others. Moreover, a layered architecture ensures the scalability and efficiency of networks and cloud resources when handling the high volume of IoT data, and it enables effective orchestration of software and hardware components within decentralized and heterogeneous environments. Accordingly, this architecture is considered a fundamental tool for building self-optimizing systems, reducing production and delivery time, and executing distributed applications in Industry 4.0 [19].

There is no single, unified reference architecture for the Industrial Internet of Things [13].

The most common IoT architectures consist of three layers, although some proposals include up to eight levels.

Table 6- Layered IIoT Architecture

model	Layers	Description	Use cases	Ref.
Three layers	Perception Layer Network Layer Application Layer	The simplest model, focused on sensing processes, data transmission, and application.	Suitable for basic IoT applications; however, it lacks sufficient depth for complex systems.	[8, 14, 21, 42, 43]

Four layers	Sensing/Perception Layer Communication/Network Layer Data Processing Layer Cloud/Storage Layer	The traditional model, which adds a processing layer between data collection and storage; suitable for real-time data analytics.	Suitable for mid-range IoT/IIoT applications with processing requirements.	[5, 8, 13, 43]
Five layers	Perception Layer Transport Layer Processing Layer Application Layer Business Layer	Adding a business layer for decision-making and supporting business processes and high-level analytics.	Effective for IoT/IIoT systems that require integration of business logic.	[42]
Seven layers	Perception Layer Connectivity Layer Edge Computing Layer Processing Layer Application Layer Business Layer Security Layer	A comprehensive model that incorporates diverse functionalities, security, and business logic for complex IIoT systems.	Suitable for advanced IIoT systems with stringent security and analytical requirements.	[8]

1) Perception Layer

The perception layer is the lowest and one of the most sensitive [5] layers of the Internet of Things architecture, and its function is to interact directly with the physical environment, identify objects, and collect real-time data through various sensors and actuators [3, 5, 6, 14, 21, 44].

This layer includes sensors, RFID tags, scanners, actuators, and physical identification modules that are typically highly constrained in terms of energy, memory, and processing capability [5, 8, 14]. These limitations make the perception layer the most vulnerable part of IoT, and a large portion of security attacks directly target this layer [8].

Communication among sensors and actuators is usually carried out via lightweight wireless technologies such as RFID, NFC, ZigBee, BLE, or low-power proprietary protocols. These technologies enable real-time interaction, efficient data collection, and object control; however, they exhibit low resistance to signal disruptions, electromagnetic interference[5], and denial-of-service attacks.

Given the limited computational and processing power, physical deployment in untrusted environments, extensive use of short-range wireless communications (such as RFID, NFC and ZigBee), and the absence of strong cryptographic mechanisms, this layer is highly vulnerable [8, 12].

Table 7- Security threats in the perception layer

Title	Description	Reference
Eavesdropping	Eavesdropping on data transmitted between sensors and the control system	[5, 8]
Physical attack	Sensors, PLCs, RTUs, and industrial devices are typically deployed in exposed environments. The goal of such attacks is the physical destruction of nodes, which disrupts their accuracy or operational functionality.	[8, 21, 42]
Channel Blocking / Jamming	In jamming attacks, adversaries disrupt communication between sensors and control systems by generating electromagnetic interference or producing noise.	[8, 21]
Counterfeit Attack / Spoofing	In spoofing attacks, adversaries provide falsified sensory information to sensors or systems.	[8, 21, 42]
Replay Attack	The attacker replays a user's usage process or authentication record, or transmits previously eavesdropped valid information to the receiver after some time in order to deceive the system's trust and achieve the intended attack objective.	[8, 21]
Tampering / Data Injection	The attacker injects malicious data into the sensor input and manipulates the system's behavior.	[8, 21]
Node Capture	Node Capture occurs at this layer, in which the attacker gains full control of a node and extracts all data passing through it. In addition, the attacker may replace or modify existing nodes in this layer.	[5, 42]
Adversarial Attacks	In adversarial attacks, adversaries manipulate input data in a way that appears natural to human observers but deceives machine-learning or computer-vision systems.	[8]

Proposed approaches for addressing security issues in the perception layer:

Device Authentication and Authorization [3, 9, 38]

- Use of unique identifiers for each sensor or actuator
- Lightweight keys suitable for low-power devices
- Digital certificates to ensure authenticated access

Secure Communication [38, 41, 44, 45]

- Implementation of cryptographic protocols compatible with energy constraints, such as AES-CCM, DTLS, or ECC-based schemes
- Protection of data against eavesdropping, tampering, and identity spoofing
- Ensuring the security of sensor data exchange with central control systems

Firmware and Software Security [14, 44]

- Providing secure and regular firmware updates
- Use of digital signatures to validate code prior to deployment on devices
- Prevention of malicious code injection or counterfeit firmware

Anomaly Detection [20, 36, 44, 45]

- Identification of abnormal sensor or actuator behavior using machine learning algorithms
- Detection of potential attacks such as data injection, physical attacks, or signal disruption
- Delivery of early warnings for proactive security measures

2) Network Layer

The network layer in IoT/IIoT architecture is responsible for transferring data from the perception layer to application systems and data-processing platforms [8, 14]. This layer includes gateway devices that handle the collection, storage, and routing of data to cloud platforms. These devices enable communication with resource-constrained devices through low-power protocols while simultaneously interacting with cloud servers via high-performance communication protocols [14]. The network layer supports various types of protocols, each optimized for specific applications and requirements; however, this diversity can also introduce security challenges [46].

Table 8-Protocols used in the network layer

Cellular connectivity using LPWAN technologies (LTE-M and NB-IoT).		Transmission of small data packets from low-power IoT devices to wide-area networks suitable for long-duration communication.	[14, 47]
	Bluetooth	Wi-Fi provides high-bandwidth connectivity over medium distances and for low-volume data transmission, suitable for devices that require high-speed communication.	[14, 18, 21, 46]
	Wi-Fi	It provides fast, low-power communication for device-to-device connectivity over short distances (up to approximately 100 meters).	[14, 21, 46]
	Zigbee	It establishes device communications through a mesh network, enabling automatic interconnection without the need for complex infrastructure.	[3, 14, 18, 21]
	RFID	High-speed and low-cost data transmission between devices and storage systems over short distances with high scalability.	[3, 14, 18]
IPv6		IPv6, by providing an enormous addressing space, advanced support for stateless autoconfiguration, simplified routing processes, more integrated security through the mandatory inclusion of IPsec, and improved scalability, is well suited for large-scale networks.	[8, 18]

Table 9-Security threats in the network layer

Title	Description	Reference
DoS / DDoS attacks	Attackers saturate communication channels with excessive traffic, disabling the IoT network through Denial-of-Service (DoS) attacks; distributed denial-of-service (DDoS) attacks, which are similar to DoS but launched from multiple sources, are more difficult to mitigate and disrupt the operation of IoT networks	[8, 14, 21, 42]

Man in the Middle	The attacker intercepts and alters the communication between IoT devices or between the devices and the central system, resulting in data manipulation, eavesdropping, or unauthorized access to sensitive information.	[8, 14, 42]
Eavesdropping	Attackers eavesdrop on the communication between IoT devices and potentially expose sensitive data.	[8, 42]
Spoofing	The attacker forges the identity of an IoT/IIoT device in order to gain unauthorized access to the network or to deceive other devices.	[8, 42]
Jamming	The attacker disrupts the wireless communication between IoT/IIoT devices by emitting radio-frequency noise.	[5, 8]
Replay Attack	Replay attacks, in which attackers record legitimate communications between IoT devices and later replay them to gain unauthorized access or perform malicious actions.	[8]

Network segmentation divides the network into separate segments so that devices are isolated and the impact of a compromised device is limited; security auditing and monitoring, in which the security posture of devices and infrastructure is regularly audited and real-time monitoring is conducted to detect and respond to security incidents; supplier and supply chain security, which involves collaborating with trusted vendors that follow secure development practices; and user training and awareness, which informs users about IoT/IIoT security risks and best practices for maintaining secure configurations [8].

Table 10- Methods for combating security threats in the network layer

Methods		**Ref.**
	Transport Layer Encryption	
	Lightweight Cryptography	
	End-to-End Encryption	
	Device Authentication	
	Mutual Authentication	
	Network-based IDS/IPS (NIDS/NIPS)	
	Edge-AI–based IDS	
	Segmentation between OT and IT equipment	
	Virtual LANs (VLANs) for separating different types of IoT devices	
	Micro-Segmentation	
	Zero Trust Network Segmentation	
Secure communication with Cloud and Edge.		[37, 52]

3) Data Processing Layer

The third layer is the Data Processing Layer which can be considered the core of the IoT system, as it includes various components that perform the operations required for developing IoT-based applications. This layer is dedicated to data collection and processing and encompasses storage, filtering, aggregation, computation, and analysis of information received from the network layer. Data are retrieved from heterogeneous devices through different communication protocols, providing an abstraction from specific technologies. In fact, this middleware level enables interoperability among connected devices. Moreover, the integration of open communication protocols and middleware facilitates connectivity with legacy devices [13].

J. Computing Architecture in the Industrial IoT

1) Edge Computing

To address the need for processing the large volume of data generated by heterogeneous devices, edge computing has been introduced as a key solution [14], deploying computational resources close to the data source (at the network edge) to enhance computational performance and reduce the load on cloud infrastructures [8, 12, 14, 53, 54]. The edge layer functions as a layer composed of processing, storage, and bandwidth resources for edge devices and can execute many real-time tasks before transmitting data to the cloud core [12, 54]. Therefore, resource-constrained devices typically use edge computing to minimize latency in interacting with the cloud or neighboring servers [8].

Edge servers can self-recover and operate independently in the event of network outages [12]. Utilizing edge servers to compute authentication operations and verify data integrity can significantly reduce computational costs and management overhead [7].

The emergence of a new network model known as EIIoT (Edge-based IIoT) is a direct response to the insufficiency of computational and storage capabilities in IIoT end devices. By deploying edge servers near end devices, limitations in processing power and storage capacity are compensated for, and real-time requirements and big-data-driven processing demands are largely addressed. Meanwhile, excessive offloading of computational tasks to edge servers by applications can lead to overload and bottlenecks on edge servers, which itself constitutes a research and engineering challenge in industrial implementations [55].

Edge-based architectures combined with technologies such as blockchain can significantly reduce latency and service time compared to traditional IIoT systems. Moreover, blockchain-based smart contracts can enhance the security of edge computing [12].

However, blockchain requires high computational power and sufficient storage capacity to execute consensus mechanisms, particularly when allocating resources within edge computing. Therefore, the critical challenge in blockchain-based resource allocation is enabling the deployment and scalability of blockchain within edge computing environments.

2) Fog Computing

Fog computing was first introduced by Cisco in 2012 as a middle-layer computing paradigm that brings cloud capabilities closer to the network edge. It can be viewed as an intermediate layer between edge and cloud computing, encompassing not only computational capabilities but also networking, storage, and other services.

Network components in fog computing mitigate issues related to geographical coverage and high latency by managing resources and supporting mobility and location awareness of distributed nodes. This layer estimates and tracks the physical location of connected devices and the likelihood of their departure or movement across different regions. Components such as routers, access points, switches, and base stations can constitute the fog layer. Depending on the application, the number of devices and the network topology may vary and include structures such as star or mesh configurations.

In addition, the fog layer includes servers that store temporary data, which is cleared after a certain period, such as every few weeks. Compared to edge computing, devices and servers in the fog layer are more powerful and capable of performing more advanced analytics and dynamically and optimally allocating resources.

Fog computing generally covers larger networks such as multiple buildings with tens or hundreds of devices while edge computing is typically limited to smaller networks, such as several wearable devices or IoT devices in a smart home. For this reason, the volume of data in the fog layer is usually much greater than that aggregated at the edge, making it particularly important for managing big data and maintaining communication quality.

Despite the higher computational power of fog devices, not all computational tasks can be executed in this layer; for example, training deep learning models with tens or hundreds of layers requires processing on cloud servers. Therefore, it is essential to determine which tasks should be executed in the fog layer and which should be delegated to higher layers to achieve both high energy efficiency and low latency [53].

3) Cloud Computing

The cloud computing architecture for Industrial Internet of Things systems is a multilayer distributed framework that coordinates processing and storage from the sensor layer to cloud data centers and ensures scalable and manageable services. In this architecture, the edge layer reduces latency and preserves the privacy of sensitive data, while the cloud layer performs heavy analytical processing; to enhance security, contemporary architectures leverage a combination of SDN for enforcing network policies and blockchain to guarantee data integrity and traceability, and they also implement Zero-Trust models along with cryptographic mechanisms [4, 52, 55].

Table 11- Security threats in the cloud layer

Threat	Description
Data Interception	Occurs when sensitive data transmitted between IoT devices and cloud services is intercepted due to lack of encryption. Attackers may also manipulate data during transmission.
Identity Spoofing	Malicious actors impersonate legitimate IoT devices or cloud services to gain unauthorized access or disrupt operations. Traditional authentication mechanisms are often insufficient.
Man-in-the-Middle (MITM) Attacks	Attackers secretly intercept and manipulate communication between devices and cloud platforms, enabling eavesdropping, data alteration, and command injection.
Distributed Denial-of-Service (DDoS) Attacks	Vulnerable IoT devices can be hijacked and used to overwhelm cloud servers with excessive traffic.
Firmware Exploitation	Insecure or outdated firmware exposes vulnerabilities that attackers can exploit to gain unauthorized access.
Wireless Communication Vulnerabilities	IoT devices relying on Wi-Fi, Bluetooth, Zigbee, or LoRaWAN are susceptible to RF jamming and protocol-level exploits.

VI. LITERATURE REVIEW

Article [25] aims to optimize resource utilization in blockchain networks and enhance security by integrating AI and blockchain. The proposed framework comprises three layers: sensor, edge, and cloud. Within this framework, a legitimacy score mechanism is employed, which is a simple yet robust approach for calculating legitimacy scores and increases accountability among nodes participating in blockchain transactions. This mechanism helps manage the complexities of trust computation in blockchain operations; however, it is not capable of providing optimal data privacy. To ensure maximum data integrity, non-repudiation, and confidentiality in large-scale IoT environments, the framework utilizes the Decentralized Evidence Matrix and the Proof of Authority (PoA) consensus mechanism. Additionally, a neural prediction model optimized with a metaheuristic algorithm is implemented for dynamic detection and classification of cyber threats. This approach reduces the computational load issues present in many AI-based methods within network security.

Evaluations in the article indicate that the proposed framework can increase detection accuracy up to 89% and reduce processing time by 34%, representing a significant improvement compared to existing blockchain-based

methods. Moreover, detection accuracy improves by 8.1% compared to conventional AI models. The framework also achieves approximately 20% increase in transaction throughput, 22% reduction in resource consumption, 19% reduction in confirmation time relative to conventional frameworks.

However, the article does not address three critical issues: Scalability and computational complexity: When AI models, blockchain, edge computing, and cloud computing are integrated, considering the limited resources of IoT devices, significant latency may occur. The article does not provide detailed measurements of processing time, energy consumption, or network bandwidth under real-world conditions.

Resistance to sophisticated and hybrid attacks: Complex and hybrid attacks, such as Sybil attacks or legitimacy score forgery, are not investigated.

Real-world large-scale implementation: The maximum number of nodes evaluated was 500, which may not reflect real network challenges, such as interference or high computational load.

The study [2] addresses security, privacy, and explainability challenges in IIoT by integrating federated learning, explainable artificial intelligence (XAI), and blockchain. This framework employs two mechanisms homomorphic encryption (HE) and blockchain-based smart contracts to ensure the security of sensitive IIoT data. Hierarchical homomorphic encryption, such as CKKS, preserves data confidentiality throughout the federated learning (FL) process and enhances data security in high-risk scenarios, such as edge processing or transmission to cloud servers.

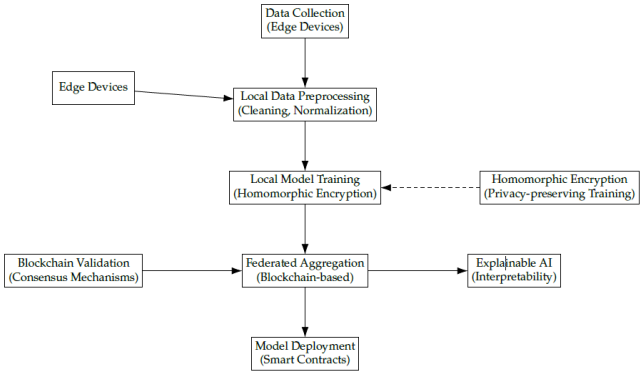

Figure 5- Architecture of the introduced framework [2]

Data collection begins at edge devices, after which local data undergoes preprocessing procedures such as cleaning and normalization to ensure quality and consistency. Subsequently, the local model is trained using homomorphic encryption, thereby maintaining data confidentiality during computations. Federated aggregation is then performed with blockchain support, ensuring secure, transparent, and immutable communications. The XAI module provides interpretability, offering meaningful insights into the model's behavior. Finally, the updated model is redistributed to edge devices via smart contracts, completing the training cycle.

The study reports that the framework's performance remains stable as the number of devices scales up to 1,000 edge devices and effectively manages varying data sizes from 10 GB to 100 GB. However, this represents a theoretical design and simulation assumption rather than a practical implementation; in the experiment, federated training was conducted using only 2 client nodes over 3 rounds. Therefore, the simulation is highly limited and does not adequately reflect real industrial conditions (e.g., large numbers of devices, data heterogeneity, network dependencies, differences in hardware resources, or compromised/unreliable nodes).

The study utilized a simple, publicly available dataset, which does not reflect IIoT complexities such as IoT sensors, machine-generated data, noise, variable conditions, temporal or sensor data, device errors, and failures. Hence, good performance on CIFAR-10 does not necessarily indicate success in real industrial environments. Additionally, the framework provides limited information regarding the model type and its architecture.

The framework employs homomorphic encryption for privacy preservation, which introduces a significant computational burden. Although the authors used a GPU (Tesla T4) in their experiments to mitigate costs, real IIoT devices typically have limited computational resources.

The framework assumes that edge device nodes are relatively trustworthy and benign, without addressing compromised or malicious nodes. For secure industrial applications, mechanisms such as malicious node detection via anomaly detection methods, adaptive node weighting, blockchain-based trust scores, and robust aggregation techniques should be incorporated.

Table 12- The statistical data of the paper [2]

Value	Metric
95.0%	Overall accuracy of the framework in IIoT scenarios
99.72%	Final accuracy of the global model after training
0.0150	Reported loss at the end of training
294.48 seconds	Average training time per round (Baseline)
300 milliseconds	Model processing and update latency
15 seconds	Time to record the model hash on the blockchain

The study in [22] focuses on authentication, group key management, and cryptographic security. It employs a private blockchain based on OpenEthereum and is managed in a Python simulation environment via web3.py. Through an identity-based authentication mechanism utilizing group keys, this scheme reduces repeated key exchanges and encryption computations, ensuring efficient identity authentication among various parties in the supply chain. Additionally, a dynamic group key management mechanism, based on a binary key tree, automates key allocation and updates, reduces the computational costs associated with traditional key replacement, and enhances the security and scalability of the supply chain system.

The architecture comprises terminal nodes, base stations, and a private blockchain network connecting the base stations. When a terminal enters the range of a base station, authentication is performed and the group key (GK) is

distributed; the communication between the terminal and the base station is encrypted. When the terminal leaves the range of the base station, the base station updates the key. Transaction data are recorded on the blockchain.

This study does not utilize actual IoT hardware and relies on software simulation. The paper focuses on algorithm design and proof of concept and does not evaluate the framework's performance at a large scale. Furthermore, the actual number of nodes and base stations is not specified, and the consensus mechanism is not defined.

Table 13- The statistical data of the paper [22]

Metric	Value
Authentication time (50 devices)	Up to 5000 ms
Random value generation cost (16-bit)	0.45 ms
Hash function cost (160-bit)	2.75 ms
Cryptographic pairing cost (176-bit)	9.56 ms
Average user registration time (10 users)	963 ms
Average sensor data storage time (100 devices)	1908 ms
Maximum throughput (TPS)	1273 transactions/sec
Bitcoin throughput	7 transactions/sec
Ethereum throughput	27 transactions/sec

The study in [4] examines a hybrid framework called PriModChain for privacy preservation in Industrial IoT, which integrates blockchain technology, federated learning, smart contracts, and Differential Privacy (DP). Federated learning is employed at the device level without sharing raw data for model training. By introducing DP noise, statistical anonymization is achieved, and blockchain is used to establish trust, record interactions transparently, and prevent data tampering. Consequently, an integrated system is created that supports decentralized learning, ensures privacy and security, and protects raw data from exposure.

The limitations of PriModChain are evaluated based on two metrics: latency and computational cost. Considering resource constraints and the heterogeneous hardware capabilities of devices, employing Differential Privacy increases the computational load and processing cost during the model training phase. Additionally, the use of blockchain imposes significant computational overhead in the consensus process, transaction recording, and verification. In federated learning, the high volume of model parameters and mandatory synchronization among all nodes in each federated training round, followed by coordination with the blockchain and the addition of DP noise, results in substantial latency. Therefore, despite its strong performance in ensuring privacy and security, this hybrid framework exhibits high latency and computational cost, making it unsuitable for real-time applications and networks with stringent delay requirements.

The study presented in [56] introduces and evaluates a Privacy-Personalized Identity (PPID) system; this system is a blockchain-based digital identity management framework that leverages the intrinsic security and decentralization properties of blockchain. PPID comprises two primary security layers: the underlying blockchain layer and the application layer (the service execution environment).

PPID operates as a decentralized system and does not store any plaintext. Only cryptographic commitments and zero-knowledge proofs (ZKPs) are recorded on the blockchain, which prevents disclosure of users' sensitive information. The Groth16 algorithm is employed to generate the zero-knowledge proofs. This protocol guarantees fundamental ZKP properties completeness, soundness, and zero-knowledge and enables verification of data integrity without revealing the underlying information. Specific computational security within PPID is enforced via computational commitments to protect user privacy. Verification processes are executed through smart contracts, eliminating single points of failure. To mitigate replay attacks, a unique, time-sensitive challenge factor (θ) is introduced to prevent malicious re-submission of legitimate user requests. Furthermore, one-time tokens are recorded after use and users' IdP addresses are included in the computations to prevent manipulation or substitution of parameters by adversaries.

The application layer emphasizes preserving user privacy in interactions with services. Users disclose only the minimum information required to service providers (SPs), and no additional data is stored on the blockchain. Consequently, SPs cannot infer users' full identities solely from blockchain addresses. Even if an adversary attempts to reveal a user's certificate identity, decoding the ZKP public key is practically infeasible because the zero-knowledge proof process and 256-bit Pedersen commitments prevent such disclosure. Users also employ randomized certificates to achieve unlinkability between identity and credentials. Timestamping of certificates ensures that they are unique and timely, while expired or previously used credentials are rendered invalid. Verification processes disclose only the essential data to SPs, and any public identity attribute required is selectively released by the authorities.

The system was evaluated on the Ethereum blockchain. The study reported a processing capacity of approximately 15 transactions per second (TPS) for public blockchains, which may pose scalability challenges for large-scale deployments. Achieving higher throughput may necessitate the use of private or consortium blockchains, which can increase system complexity and operational costs. Additionally, system response time increases with the number of nodes and requests. The PPID smart contracts are designed to be gas-efficient to reduce blockchain operational costs. Use of private or consortium chains can substantially lower operational costs while still preserving user privacy.

Table 14-Review of the framework presented in the paper [56]

Advantages	Limitations
High privacy and security	Scalability limitations
Ability to optimize smart contracts	High computational complexity
Prevention of replay attacks	Requirement for private/consortium blockchains with associated costs
Unlinkability between identity, credentials, and verification process	Latency in large-scale deployments

Resistance to parameter-substitution attacks	Limited throughput on public blockchains
Storage efficiency	Spatial and temporal complexity in management and large-scale evaluation

Public blockchains such as Ethereum exhibit throughput on the order of ~15 TPS; in scenarios with a large number of users or transactions, response times increase and the system may experience delays. To attain higher throughput, deployment on private or consortium blockchains is required, which entails greater complexity and cost. The use of ZKPs and the Groth16 algorithm also renders the system's computations complex and computationally intensive.

The study presented in [5] introduces and evaluates a Privacy-Personalized Identity (PPID) system; this system is a blockchain-based digital identity management framework that leverages the intrinsic security and decentralization properties of blockchain. PPID comprises two primary security layers: the underlying blockchain layer and the application layer (the service execution environment).

PPID operates as a decentralized system and does not store any plaintext. Only cryptographic commitments and zero-knowledge proofs (ZKPs) are recorded on the blockchain, which prevents disclosure of users' sensitive information. The Groth16 algorithm is employed to generate the zero-knowledge proofs. This protocol guarantees fundamental ZKP properties completeness, soundness, and zero-knowledge and enables verification of data integrity without revealing the underlying information. Specific computational security within PPID is enforced via computational commitments to protect user privacy. Verification processes are executed through smart contracts, eliminating single points of failure. To mitigate replay attacks, a unique, time-sensitive challenge factor (θ) is introduced to prevent malicious re-submission of legitimate user requests. Furthermore, one-time tokens are recorded after use and users' IdP addresses are included in the computations to prevent manipulation or substitution of parameters by adversaries.

The application layer emphasizes preserving user privacy in interactions with services. Users disclose only the minimum information required to service providers (SPs), and no additional data is stored on the blockchain. Consequently, SPs cannot infer users' full identities solely from blockchain addresses. Even if an adversary attempts to reveal a user's certificate identity, decoding the ZKP public key is practically infeasible because the zero-knowledge proof process and 256-bit Pedersen commitments prevent such disclosure. Users also employ randomized certificates to achieve unlinkability between identity and credentials. Timestamping of certificates ensures that they are unique and timely, while expired or previously used credentials are rendered invalid. Verification processes disclose only the essential data to SPs, and any public identity attribute required is selectively released by the authorities.

The system was evaluated on the Ethereum blockchain. The study reported a processing capacity of approximately 15 transactions per second (TPS) for public blockchains, which may pose scalability challenges for large-scale deployments. Achieving higher throughput may necessitate the use of private or consortium blockchains, which can increase system complexity and operational costs. Additionally, system response time increases with the number of nodes and requests. The PPID smart contracts are designed to be gas-efficient to reduce blockchain operational costs. Use of private or consortium chains can substantially lower operational costs while still preserving user privacy.

Table 15- Review of the framework presented in the paper [5]

Advantages	Limitations
High privacy and security	Scalability limitations
Ability to optimize smart contracts	High computational complexity
Prevention of replay attacks	Requirement for private/consortium blockchains with associated costs
Unlinkability between identity, credentials, and verification process	Latency in large-scale deployments
Resistance to parameter-substitution attacks	Limited throughput on public blockchains
Storage efficiency	Spatial and temporal complexity in management and large-scale evaluation

Public blockchains such as Ethereum exhibit throughput on the order of ~15 TPS; in scenarios with a large number of users or transactions, response times increase and the system may experience delays. To attain higher throughput, deployment on private or consortium blockchains is required, which entails greater complexity and cost. The use of ZKPs and the Groth16 algorithm also renders the system's computations complex and computationally intensive.

In paper [23], a secure mechanism for data exchange in Industrial IoT environments is presented, utilizing blockchain and smart contracts, and leveraging advanced cryptography for data protection. Data are initially processed on factory servers and encrypted using PEKS (Public Key Encryption with Keyword Search) along with keyword-based indices, while access control based on Zero-Knowledge Proof and Pedersen Commitment ensures that only authorized users can view the data, with the ability to revoke or modify access rights. The security of the system is guaranteed through data immutability, privacy preservation, data integrity, and traceability of all transactions. Simulations were conducted on a test Ethereum network with 10 nodes, and the results demonstrated that, compared to other schemes, this approach achieves lower and more efficient index and trapdoor generation time and exhibits satisfactory performance in executing smart contracts, enabling the system to transfer data securely, reliably, and efficiently among users.

Table 16- The statistical data of the paper [23]

Metrics	Value
Trapdoor Generation Time	Proposed scheme: 2 encryptions + 1 hash – BASE: 2 encryptions

Index Generation Time	Proposed scheme: 1 bilinear computation + 1 hash – CL-dPAEKS and SCF-MCLPEKS: higher
Keyword Retrieval Time	Proposed scheme: 3 bilinear computations
Smart Contract Execution Cost (Gas Cost)	Contract 1: 1,431,432 – Contract 2: 1,659,097 – Contract 3: 2,850,488 – Contract 4: 137,141

Article [7] presents an innovative framework for securing IoT-based systems in Industry 4.0, designed on the basis of a hybrid blockchain architecture and edge computing. The primary objective of this research is to establish an integrated and scalable platform that ensures the confidentiality, integrity, and availability of industrial data in smart environments.

One of the most significant security achievements of this study is the use of the Proof-of-Authority (PoA) consensus mechanism in the private blockchain. Relying on the verified identities of nodes, this approach enables fast and low-cost transaction validation while consuming substantially less energy compared to methods such as Proof-of-Work or Proof-of-Stake. The choice of PoA allows the proposed framework to align with the efficiency, low latency, and security-control requirements of Industry 4.0.

From the perspective of data management and validity, the paper introduces a processing pipeline that includes data cleansing, normalization, and encoding prior to storage on the blockchain. Each industrial datum, once converted into a transaction, is recorded in the distributed ledger along with a timestamp, signature, and encryption. Although the exact cryptographic algorithm is not specified, the researchers evaluated the security of the generated keys using NIST's suite of randomness tests, indicating a strong focus on cryptographic robustness and the prevention of potential key weaknesses.

The use of edge computing is another security strength of the system. Performing preliminary processing at the edge not only reduces latency and the volume of transmitted data but also decreases the risk of attacks associated with continuous data transfer to the cloud and limits the attack surface. The system's hybrid architecture comprising both public and private blockchains also enables multilayer access, role separation, and the application of fine-grained security controls.

Finally, the article proposes future directions for enhancing the security of this framework, including the adoption of quantum-resistant cryptography, the use of zero-knowledge proofs to strengthen privacy, and the integration of artificial intelligence and machine learning to develop threat-prediction systems.

Article [8] presents a hybrid framework for securing Industrial Internet of Things (IIoT) networks, utilizing Convolutional Neural Networks (CNNs) for intrusion detection and reinforcement learning combined with blockchain for attack prevention and mitigation. The use of CNNs enables real-time identification of anomalous behaviors, while blockchain ensures data integrity and secure communications. Although technical details such as the consensus mechanism or cryptographic algorithms are not specified, the integration of reinforcement learning with blockchain represents an innovative approach to reducing vulnerabilities in IIoT networks. This framework exemplifies emerging security paradigms that, rather than focusing solely on intrusion detection, also incorporate proactive response and prevention, providing a foundation for designing more resilient systems.

Table 17-Hardware specifications used for the simulation

Hardware	Ref.
Tesla T4 GPU, with 1.59 GHz clock, 40 cores, 16 GB memory, bandwidth up to 300 GB/s	[26]
Intel Core i7 processor, 16 GB RAM, running 64-bit CentOS 7	[22]
Intel Core i7 CPU @3.60 GHz and 16GB RAM.	[23]
Intel Workstation with I7 CPU with NVIDIA GPU, 16GB RAM and 3.2 GHZ frequency	[56]

Table 18-Summary of the reviewed papers

Computing Architecture	Number of Nodes	Dataset	AI Model	Blockchain Network	Cryptographic Technique	Data Management and Verification	Consensus Mechanism	Integration	Ref.
Edge + Cloud	200 –500 nodes	CIC-IoT	Neural Network + Metaheuristic Algorithms	Ethereum-based	SHA-3	Decentralized Evidence Matrix	PoA	Blockchain + AI	[25]
Edge	2 nodes	CIFAR-10	ML + FL	Ethereum-based	homomorphic encryption (HE)	Blockchain + smart contracts	DPoS	Federated Learning (FL) + Blockchain + Explainable AI (XAI)	[26]

–	–	–	–	private blockchain	ZKP + Group Key (GK) Key management: binary key-tree structure	Data and events are recorded on the blockchain ledger	–	Blockchain + group key management (binary key-tree) + zero-knowledge proof (ZKP)	[22]
Edge + Cloud		MNIST	ML + FL	Ethereum-based	differential privacy	Blockchain + smart contracts	default consensus of Ethereum	Blockchain+ ML + differential privacy+ Federated Learning	[4]
–	–	–	–	Ethereum Sepolia testnet	ZK-SNARK + Shamir Secret Sharing (SSS)	Blockchain + smart contracts	PoW	multi-channel blockchain + decentralized identity (DID) system + decentralized storage (via IPFS) + privacy-preserving computation center	[55]
Cloud + Edge	10 nodes	–	–	Ethereum-based test network using Ganache	PEKS + ZKPoK + Pedersen commitments+ Bilinear maps	Blockchain + smart contracts	default consensus of Ethereum	Blockchain + PEKS + ZKPoK + Pedersen commitments	[23]
Edge	not specified	not specified	Keras (with TensorFlow backend)	Private Blockchain + Hybrid Model	advanced cryptographic algorithms (not specified)	Data and events are recorded on the blockchain ledger + NIST Randomness Tests	PoA	Hybrid Blockchain (Public + Private)	[56]
–	–	–	CNN	–	–	Data and events are recorded on the blockchain ledger	–	CNN (DL) + blockchain-assisted RL	[45]

VII. CONCLUSION

The rapid digital transformation of industrial environments has positioned the Industrial Internet of Things (IIoT) as a foundational pillar of modern manufacturing, automation, and data-driven decision-making. However, the very characteristics that make IIoT attractive its large-scale connectivity, heterogeneity, distributed nature, and reliance on resource-constrained devices also expose it to a wide spectrum of security and privacy vulnerabilities. Centralized architectures further exacerbate these challenges, creating single points of failure, trust dependencies, and inadequate resilience against evolving cyber threats.

This survey has examined blockchain as a promising decentralized security framework capable of addressing many of the structural weaknesses inherent in IIoT ecosystems. Through its core properties immutability, transparency, decentralized trust, cryptographic assurance, secure consensus, and programmable automation via smart contracts blockchain can significantly enhance the integrity, confidentiality, and traceability of IIoT systems. Our review shows that blockchain-based architectures enable secure device identity management, tamper-proof logging, automated access control, trustworthy supply-chain traceability, and more resilient multi-stakeholder interactions. When combined with edge/fog computing and lightweight cryptography, blockchain can extend strong security guarantees even to highly constrained industrial devices.

Despite these advantages, integrating blockchain with IIoT remains non-trivial. Key challenges include scalability

limitations, storage overhead, computational demands of consensus mechanisms, interoperability issues, regulatory considerations, and the practical constraints of end devices. Moreover, cryptographic tools such as ZKP and ECC, though powerful, introduce computational burdens that must be balanced with IIoT's latency and energy requirements. Emerging paradigms including hierarchical blockchain models, cross-layer security architectures, hybrid on-chain/off-chain designs, and distributed resource allocation via edge and fog computing indicate promising pathways to mitigate these limitations.

Overall, the integration of blockchain and IIoT is neither a universal remedy nor an incremental enhancement; rather, it represents a transformational shift toward decentralized, auditable, and resilient industrial systems. As industrial infrastructures continue to expand, the demand for trustworthy automation will intensify. Future research must therefore focus on energy-efficient consensus mechanisms, lightweight blockchain architectures, privacy-preserving computation for instance ZKPs and secure multi-party computation, AI-driven intrusion detection, interoperable standards, and practical large-scale deployments. Achieving these goals will be essential for realizing secure, scalable, and privacy-preserving IIoT ecosystems capable of supporting the next generation of Industry 4.0 and beyond.

VIII. FUTURE RESEARCH DIRECTIONS

Despite the promising role of blockchain in strengthening the security and privacy of Industrial IoT systems, several research gaps must be addressed to achieve scalable and practical integration. One of the most critical areas for future work is the development of lightweight and IIoT-centric consensus mechanisms. Conventional algorithms such as PoW, PoS, and PoA are not fully compatible with the stringent latency, energy, and throughput requirements of industrial environments. Therefore, future studies should investigate deterministic and low-overhead consensus protocols, hierarchical or federated consensus models, and DAG-based or sharded blockchain structures capable of supporting high-velocity industrial data while maintaining decentralization and trust.

Privacy-preserving computation is another prominent direction as industrial operations increasingly involve sensitive telemetry, proprietary production data, and real-time analytics. The integration of zero-knowledge proofs, privacy-preserving smart contracts, secure multi-party computation, and confidential on-chain verification can substantially enhance privacy while maintaining auditability. However, existing ZKP systems remain computationally expensive for resource-constrained devices. Thus, future research must focus on designing lightweight ZKP constructions, hardware-assisted proving mechanisms, and architectures in which edge or fog nodes assist in generating proofs without compromising confidentiality.

Scalability challenges also motivate the exploration of hybrid on-chain and off-chain architectures. Since storing or processing large IIoT datasets directly on the blockchain is impractical, future solutions should combine on-chain integrity with off-chain encrypted storage and computation. This includes the integration of decentralized storage systems, trusted execution environments, and state-channel-based real-time machine-to-machine interactions. Such hybrid approaches offer a balance between performance, privacy, and verifiability, enabling blockchain to support industrial applications requiring high throughput and low latency.

There is also a growing need for advanced, blockchain-enhanced intrusion detection and autonomous defense mechanisms. Traditional centralized IDS solutions struggle in dynamic and heterogeneous IIoT environments, and machine learning–based approaches face challenges related to trust, data sharing, and adversarial manipulation. Future research should explore distributed IDS frameworks coordinated through blockchain, federated learning-based anomaly detection, and autonomous response systems powered by smart contracts. These integrated approaches could enable self-organizing, self-healing industrial networks capable of responding to threats in real time.

Effective integration of blockchain with edge, fog, and cloud computing is another major research direction. While edge and fog computing provide low-latency computation and reduce the load on cloud infrastructures, they also introduce new complexity in deploying blockchain components across distributed layers. Future studies must develop resource-aware deployment strategies, adaptive task migration policies, and energy-efficient mechanisms that allow constrained IIoT devices to participate in blockchain-based security frameworks without compromising performance.

Interoperability and standardization remain essential challenges as industrial environments involve diverse devices, communication protocols, and vendor-specific platforms. Achieving broad adoption will require unified interoperability frameworks, cross-chain communication mechanisms, standardized data models, and industry-specific guidelines that align blockchain-based IIoT systems with regulatory, operational, and cybersecurity standards. Establishing such standards is vital for ensuring compatibility, lowering integration costs, and supporting multi-stakeholder industrial ecosystems.

Finally, there is a significant need for real-world deployments, open testbeds, and empirical evaluations of blockchain-enabled IIoT. While academic research has produced numerous conceptual models and simulated prototypes, large-scale industrial implementations remain limited. Future work should emphasize practical case studies in manufacturing, smart grids, logistics, and critical infrastructure, along with long-term evaluations of scalability, cost, reliability, and maintainability. Developing benchmark datasets and standardized test environments will also support reproducibility and accelerate innovation.

REFERENCES:

[1] *M. Soori, F. K. G. Jough, R. Dastres, and B. Arezoo, "Blockchains for industrial Internet of Things in sustainable supply chain management of industry 4.0, a review," Sustainable Manufacturing and Service Economics, vol. 3, p. 100026, 2024/01/01/*

2024,doi: https://doi.org/10.1016/j.smse.2024.100026.

[2] *"Blockchain-Based Decentralized Security for IoT applications," Artificial Intelligence & Robotics Development Journal, vol. 5, no. 4, pp. 409–427, 10/01 2025, doi: 10.52098/airdj.20255468.*

[3] *S. A. Ansari and S. Ali, "A systematic review of lightweight cryptographic schemes for security and privacy in IoT," Discover Computing, vol. 28, no. 1, p. 266, 2025/11/14 2025, doi: 10.1007/s10791-025-09755-3.*

[4] *R. Kaur, T. Rodrigues, N. Kadir, and R. Kashef, "A Survey on Privacy Preservation Techniques in IoT Systems," Sensors, vol. 25, no. 22, p. 6967, 2025. [Online]. Available: https://www.mdpi.com/1424-8220/25/22/6967.*

[5] *A. A. Laghari, H. Li, A. A. Khan, Y. Shoulin, S. Karim, and M. A. K. Khani, "Internet of Things (IoT) applications security trends and challenges," Discover Internet of Things, vol. 4, no. 1, p. 36, 2024/12/24 2024, doi: 10.1007/s43926-024-00090-5.*

[6] *R. L. Kumar, F. Khan, S. Kadry, and S. Rho, "A Survey on blockchain for industrial Internet of Things," Alexandria Engineering Journal, vol. 61, no. 8, pp. 6001–6022, 2022/08/01/ 2022, doi: https://doi.org/10.1016/j.aej.2021.11.023.*

[7] *P. Shojaei, E. Vlahu-Gjorgievska, and Y.-W. Chow, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," Computers, vol. 13, no. 2, p. 41, 2024. [Online]. Available: https://www.mdpi.com/2073-431X/13/2/41.*

[8] *M. Țălu, "Security and Privacy in the IIoT: Threats, Possible Security Countermeasures, and Future Challenges," Computing&AI Connect, vol. 2, 02/15 2025, doi: 10.69709/CAIC.2025.139199.*

[9] *M. Al-Shatari, F. A. Hussin, A. A. Aziz, T. A. E. Eisa, X.-T. Tran, and M. E. E. Dalam, "IoT Edge Device Security: An Efficient Lightweight Authenticated Encryption Scheme Based on LED and PHOTON," Applied Sciences, vol. 13, no. 18, p. 10345, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/18/10345.*

[10] *K. Fizza et al., "A Survey on Evaluating the Quality of Autonomic Internet of Things Applications," IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 567–590, 2023, doi: 10.1109/COMST.2022.3205377.*

[11] *P. Mariano, C. Garrocho, C. Cavalcanti, and R. Rabelo, Blockchain Applied to Security in Industrial Internet of Things Devices. 2024, pp. 345–353.*

[12] *S. Asaithambi, S. Nallusamy, J. Yang, S. Prajapat, G. Kumar, and P. S. Rathore, "A secure and trustworthy blockchain-assisted edge computing architecture for industrial internet of things," Scientific Reports, vol. 15, no. 1, p. 15410, 2025/05/02 2025, doi: 10.1038/s41598-025-00337-3.*

[13] *D. Calderón, F. J. Folgado, I. González, and A. J. Calderón, "Implementation and Experimental Application of Industrial IoT Architecture Using Automation and IoT Hardware/Software," Sensors, vol. 24, no. 24, p. 8074, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/24/8074.*

[14] *H. Sebestyen, D. E. Popescu, and R. D. Zmaranda, "A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories," Computers, vol. 14, no. 2, p. 61, 2025. [Online]. Available: https://www.mdpi.com/2073-431X/14/2/61.*

[15] *H. Singhvi, "THE INTERNET OF THINGS IN 2025: TRENDS, BUSINESS MODELS, AND FUTURE DIRECTIONS FOR A CONNECTED WORLD," INTERNATIONAL JOURNAL OF INTERNET OF THINGS, vol. 3, pp. 17–24, 05/17 2025, doi: 10.34218/IJIOT_03_01_003.*

[16] *I. Khan, Y. Majib, R. Ullah, and O. Rana, "Blockchain Applications for Internet of Things — A Survey," Internet of Things, vol. 27, p. 101254, 2024/10/01/ 2024, doi: https://doi.org/10.1016/j.iot.2024.101254.*

[17] *W. Shujaa, M. Alanzi, and S. Sankaranarayanan, "Enhancing IoT security through blockchain integration," (in English), Frontiers in Computer Science, Review vol. Volume 7 - 2025, 2025–October–29 2025, doi: 10.3389/fcomp.2025.1670473.*

[18] *M. Salayma, "Risk and threat mitigation techniques in internet of things (IoT) environments: a survey," (in English), Frontiers in the Internet of Things, Systematic Review vol. Volume 2 - 2023, 2024–January–23 2024, doi: 10.3389/friot.2023.1306018.*

[19] *W. Oñate and R. Sanz, "Analysis of architectures implemented for IIoT," Heliyon, vol. 9, no. 1, 2023, doi: 10.1016/j.heliyon.2023.e12868.*

[20] *S. A R and J. Katiravan, "Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain based cyber security," Scientific Reports, vol. 15, no. 1, p. 22369, 2025/07/01 2025, doi: 10.1038/s41598-025-04164-4.*

[21] *P. Sun, Y. Wan, Z. Wu, Z. Fang, and Q. Li, "A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions," Computers & Security, vol. 148, p. 104097, 2025/01/01/ 2025, doi: https://doi.org/10.1016/j.cose.2024.104097.*

[22] *C. Wang, X. Zhao, Q. Liu, T. Chen, and T. Liu, "A Security Authentication Scheme for Mobile Industrial IoT Supply Chains Based on Blockchain and Group Key Management," Digital Communications and Networks, 2025/08/18/ 2025, doi: https://doi.org/10.1016/j.dcan.2025.08.003.*

[23] *Y. Liu, R. Huo, N. Gao, C. Chi, and T. Huang, "A Security Data Exchange Mechanism for IIoT Based on Blockchain," presented at the Proceedings of the 2025 4th International Conference on*

Cryptography, Network Security and Communication Technology, 2025. [Online]. Available: https://doi.org/10.1145/3723890.3723905.

[24] *A. Ruzbahani, AI-Protected Blockchain-based IoT environments: Harnessing the Future of Network Security and Privacy. 2024.*

[25] *B. U. I. Khan, K. W. Goh, A. R. Khan, M. F. Zuhairi, and M. Chaimanee, "Integrating AI and Blockchain for Enhanced Data Security in IoT-Driven Smart Cities," Processes, vol. 12, no. 9, p. 1825, 2024. [Online]. Available: https://www.mdpi.com/2227-9717/12/9/1825.*

[26] *I. B. Ababio et al., "A Blockchain-Assisted Federated Learning Framework for Secure and Self-Optimizing Digital Twins in Industrial IoT," Future Internet, vol. 17, no. 1, p. 13, 2025. [Online]. Available: https://www.mdpi.com/1999-5903/17/1/13.*

[27] *G. Rathee, F. Ahmad, N. Jaglan, and C. Konstantinou, "A secure and trusted mechanism for industrial IoT network using blockchain," IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1894–1902, 2022.*

[28] *Z. Hussein, M. A. Salama, and S. A. El-Rahman, "Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms," Cybersecurity, vol. 6, no. 1, p. 30, 2023/11/03 2023, doi: 10.1186/s42400-023-00163-y.*

[29] *N. M. Chacko, N. V. G, M. Balachandra, and M. T, "Lightweight Consensus in Blockchain: A Systematic Literature Review," ACM Comput. Surv., vol. 58, no. 3, p. Article 78, 2025, doi: 10.1145/3768149.*

[30] *S.-P. Lu, C.-L. Lei, and M.-H. Tsai, "An efficient Proof-of-Authority consensus scheme against cloning attacks," Computer Communications, vol. 228, p. 107975, 2024/12/01/ 2024, doi: https://doi.org/10.1016/j.comcom.2024.107975.*

[31] *S. Fahim, S. Mahmood, and S. M. Rahman, Blockchain: A Comparative Study of Consensus Algorithms PoW, PoS, PoA, PoV. 2023.*

[32] *A. Zimba, K. O. Phiri, M. Mulenga, and G. Mukupa, "A systematic literature review of blockchain technology and energy efficiency based on consensus mechanisms, architectural innovations, and sustainable solutions," Discover Analytics, vol. 3, no. 1, p. 14, 2025/09/29 2025, doi: 10.1007/s44257-025-00041-6.*

[33] *H. Taherdoost, "Smart Contracts in Blockchain Technology: A Critical Review," Information, vol. 14, p. 117, 02/13 2023, doi: 10.3390/info14020117.*

[34] *A. Gupta and K. Lakhwani, "Enhancing blockchain quality-of-service: a comparative analysis and novel smart contract mechanism," Discover Applied Sciences, vol. 7, no. 8, p. 807, 2025/07/20 2025, doi: 10.1007/s42452-025-07395-2.*

[35] *M. F. Shaikh, S. H. Hassan, A. Maccaro, G. Pratesi, and D. Piaggio, "A blockchain framework using proof of authority and smart contracts for ethical and secure healthcare asset management," (in English), Frontiers in Public Health, Methods vol. Volume 13 - 2025, 2025–September–23 2025, doi: 10.3389/fpubh.2025.1638546.*

[36] *M. M. Rahman, S. A. Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," Cyber Security and Applications, vol. 3, p. 100082, 2025/12/01/ 2025, doi: https://doi.org/10.1016/j.csa.2024.100082.*

[37] *B. Gusita, A. Anton, C. Stangaciu, D. Stanescu, L. Gaina, and M. Micea, "Securing IoT edge: a survey on lightweight cryptography, anonymous routing and communication protocol enhancements," International Journal of Information Security, vol. 24, 05/31 2025, doi: 10.1007/s10207-025-01071-7.*

[38] *S. Khan, P. A. F. L. martins, B. Sousa, and V. Pereira, "A Comprehensive Review on Lightweight Cryptographic Mechanisms for Industrial Internet of Things Systems," ACM Comput. Surv., vol. 58, no. 1, p. Article 23, 2025, doi: 10.1145/3757734.*

[39] *N. O. Gavriilidis, S. T. Halkidis, and S. Petridou, "Empirical Evaluation of TLS-Enhanced MQTT on IoT Devices for V2X Use Cases," Applied Sciences, vol. 15, no. 15, p. 8398, 2025. [Online]. Available: https://www.mdpi.com/2076-3417/15/15/8398.*

[40] *J. K. Phiang, Y. Vivian Yong Siew, H. bin Hilmi, L. Dedree Leonna, Z. Ng Ee, and F. Muhammad, "Enhancing Security in Industrial IoT Through Blockchain-based Authentication Mechanisms," International Journal of Electrical Engineering, Mathematics and Computer Science, vol. 1, no. 3, pp. 43–61, 07/15 2024, doi: 10.62951/ijeemcs.v1i3.20.*

[41] *M. D. Alanazi, "A triple-layer authentication framework with elliptic curve cryptography for securing IoT-assisted wireless sensor networks," PLOS ONE, vol. 20, no. 8, p. e0329011, 2025, doi: 10.1371/journal.pone.0329011.*

[42] *B. Alotaibi, "A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities," Sensors, vol. 23, no. 17, p. 7470, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/17/7470.*

[43] *D. A. Patil and S. G, "A comprehensive survey on securing the social internet of things: protocols, threat mitigation, technological integrations, tools, and performance metrics," Scientific Reports, vol. 15, no. 1, p. 40190, 2025/11/17 2025, doi: 10.1038/s41598-025-23865-4.*

[44] *X. Feng, X. Zhu, Q. L. Han, W. Zhou, S. Wen, and Y. Xiang, "Detecting Vulnerability on IoT Device Firmware: A Survey," IEEE/CAA Journal of Automatica Sinica, vol. 10, no. 1, pp. 25–41, 2023, doi: 10.1109/JAS.2022.105860.*

[45] *M. Srinivasan and N. C. Senthilkumar, "Intrusion Detection and Prevention System (IDPS) Model for IIoT Environments Using Hybridized Framework,"*

IEEE Access, vol. 13, pp. 26608–26621, 2025, doi: 10.1109/ACCESS.2025.3538461.

[46] *O. Aouedi et al., "A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions," IEEE Communications Surveys & Tutorials, vol. 27, no. 2, pp. 1238–1292, 2025, doi: 10.1109/COMST.2024.3430368.*

[47] *C. Milarokostas, D. Tsolkas, N. Passas, and L. Merakos, "A Comprehensive Study on LPWANs With a Focus on the Potential of LoRa/LoRaWAN Systems," IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 825–867, 2023, doi: 10.1109/COMST.2022.3229846.*

[48] *A. Sunny, M. Rahman, H. Arman, M. Islam, M. D. Reza, and M. Khan, End-to-End Encrypted IoT System for Military Communications. 2025.*

[49] *A. Shahidinejad and J. Abawajy, "An All-Inclusive Taxonomy and Critical Review of Blockchain-Assisted Authentication and Session Key Generation Protocols for IoT," ACM Computing Surveys, vol. 56, 02/10 2024, doi: 10.1145/3645087.*

[50] *C. Liu et al., "Dissecting zero trust: research landscape and its implementation in IoT," Cybersecurity, vol. 7, no. 1, p. 20, 2024/05/03 2024, doi: 10.1186/s42400-024-00212-0.*

[51] *C. Zanasi, S. Russo, and M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," Ad Hoc Networks, vol. 156, p. 103414, 2024/04/01/ 2024, doi: https://doi.org/10.1016/j.adhoc.2024.103414.*

[52] *C. Savaglio, P. Mazzei, and G. Fortino, "Edge Intelligence for Industrial IoT: Opportunities and Limitations," Procedia Computer Science, vol. 232, pp. 397–405, 2024/01/01/ 2024, doi: https://doi.org/10.1016/j.procs.2024.01.039.*

[53] *T. Nguyen, H. Nguyen, and T. Nguyen Gia, "Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications," Journal of Network and Computer Applications, vol. 226, p. 103884, 2024/06/01/ 2024, doi: https://doi.org/10.1016/j.jnca.2024.103884.*

[54] *S. Shen, X. Wu, P. Sun, H. Zhou, Z. Wu, and S. Yu, "Optimal privacy preservation strategies with signaling Q-learning for edge-computing-based IoT resource grant systems," Expert Syst. Appl., vol. 225, no. C, p. 13, 2023, doi: 10.1016/j.eswa.2023.120192.*

[55] *G. Wu, Z. Xu, H. Zhang, S. Shen, and S. Yu, "Multi-agent DRL for joint completion delay and energy consumption with queuing theory in MEC-based IIoT," Journal of Parallel and Distributed Computing, vol. 176, pp. 80–94, 2023/06/01/ 2023, doi: https://doi.org/10.1016/j.jpdc.2023.02.008.*

[56] *H. Yu, G. Wang, A. Dong, Y. Han, Y. Wang, and J. Yu, "Blockchain-enabled privacy protection scheme for IoT digital identity management," High-Confidence Computing, vol. 5, no. 4, p. 100320, 2025/12/01/ 2025, doi: https://doi.org/10.1016/j.hcc.2025.100320.*

How to cite: M. Hajiee, Z. MehraniRad, H. Moradi, **Integration of Industrial IoT and Blockchain Based on Security and Privacy- A Survey**, Journal of Distributed Computing and Systems (JDCS), Vol 9, Issue1,Pages31-50, 2026.

Maryam Hajiee received her Ph.D. degree in Computer Engineering with a specialization in Software Systems. Her research interests include Wireless Sensor Networks, the Internet of Things (IoT), Artificial Intelligence, and Quantum Computing.
Email: mhajiee@iau.ac.ir

Zeynab Mehrani-Rad is an undergraduate student of Computer Engineering at Islamic Azad University, South Tehran Branch. Her research interests include quantum computing, information security, computer networks, and blockchain technology.
Email: zeynab.mehranirad@iau.ir

Hediyeh Moradi is an undergraduate student of Computer Engineering at Islamic Azad University, South Tehran Branch. Her research interests include information security, network security, blockchain technology, cryptography, and quantum computing.
Email: hediyeh.moradi@iau.ir