International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(17s) 2026 pp. 1293-1321
https://doi.org/10.70917/ijcisim-2026-4828
Article

A Review Study on Security Enhancements and Privacy considerations In Industrial Internet of Things (IIoT) Applications

Varsha Prafull Patil 1*, Sharada N. Ohatakar[2]

[1]Department of Electronics & Telecommunication Engineering. Cummins College of Engineering, Pune, India
varsha.patil@cumminscollege.in
[2]Department of Electronics & Telecommunication Engineering. Cummins College of Engineering, Pune, India
sharada.ohatkar@cumminscollege.in

Abstract: The Industrial Internet of Things revolutionizes industrial processes by integrating advanced sensors, communication technologies, and data analytics to enhance operational efficiency and decision-making. Security enhancements and privacy considerations in IIoT applications face several challenges. These include safeguarding vast amounts of sensitive data across complex networks, ensuring robust authentication and authorization to prevent unauthorized access, and protecting against sophisticated cyber-attacks like DDoS and man-in-the-middle attacks. This review comprehensively explores and analyses current security challenges and privacy issues inherent in IIoT systems. Machine learning algorithms play a crucial role in enhancing security for IIoT systems by detecting anomalies, predicting potential threats, and automating responses. Blockchain platforms, including Ethereum, offer decentralized and immutable solutions for securing data transactions and ensuring transparency within IIoT environments. Privacy considerations in IIoT applications involve implementing robust data protection measures and ensuring compliance with regulatory standards to safeguard sensitive information. Exploring Ethereum experimentation for IIoT applications provides an opportunity to leverage smart contracts and distributed ledger technology to enhance security, streamline operations, and protect data integrity in industrial settings. Future research in security enhancements and privacy considerations for IIoT applications could explore the integration of emerging technologies such as quantum cryptography and AI-driven threat detection.
Keywords: Industrial Internet of Things, Machine Learning, Blockchain Technology, Ethereum Blockchain, Data Privacy, Smart Contracts

1. INTRODUCTION

The (IIoT) refers to the integration of physical devices, machines, and sensors with digital networks and software applications, enabling enhanced connectivity, data collection, and analysis in industrial environments (Hu et al.,2024). This technological advancement leverages IoT principles to optimize manufacturing processes, improve operational efficiencies, and foster innovation across various sectors, including manufacturing, logistics, energy, and transportation. By interconnecting devices through secure and reliable communication protocols, IIoT facilitates real-time monitoring, predictive maintenance, and advanced automation, ultimately driving productivity and reducing operational costs (Zhang et al., 2024). The adoption of IIoT has revolutionized traditional industrial practices by enabling data-driven decision-making and creating smarter, more adaptive systems. Key components of IIoT include sensors and actuators, edge computing, cloud services, and advanced analytics powered by artificial intelligence (AI) and machine learning (ML). (Soliman et al., 2023) These technologies work together to collect vast amounts of data from industrial assets, process it at the edge or in the cloud, and derive actionable insights to optimize performance and anticipate issues before they arise. As industries continue to embrace digital transformation, IIoT stands at the forefront, offering unprecedented opportunities for innovation, efficiency, and sustainability.

The Industrial Internet of Things revolutionizes industries with connectivity. Security and privacy are critical for safe, efficient operations. (Borgosz et al., 2024) suggested the IIoT is a network of networked devices that uses a variety of technologies, including artificial intelligence, machine learning, cloud computing, soft sensors, and data analytics, to provide real-time insight into the workings of any industrial process, from supply chain management to process optimization and product development. (Gaber et al., 2023) Wide-ranging data collecting and utilisation is made possible by IIoT, which also lowers errors, boosts productivity, and improves process knowledge. Although this innovative approach is the cornerstone of Industry 4.0, the bioprocessing industry is difficult to integrate with IIoT due to the intrinsic operational complexity brought about by the use of living systems or their components in manufacturing. (Alanazi et al., 2023) Manufacturing of biopharmaceuticals and advanced therapies, some of the most valuable biotechnological products on the market, makes up a sizable portion of the sector. These products are subject to stringent regulatory reviews and scrutiny from product conception to patient delivery. (Awotunde et al., 2023) The biopharmaceutical business aspires to a deep understanding of processes; nevertheless, the barriers to implementing IIoT solutions to integrate with bio-manufacturing operations include the difficulty of switching to a new mode of operation, the possibility of priorities not aligning, the requirement for significant investments to support the transition, the constraints placed on the industry by the downtime necessary for the change, and the necessity of regulatory support. (Mu et al., 2024) The Internet of Things can be thought of as a global network infrastructure consisting of a multitude of connected devices that rely on sensing, communication, networking, and information processing technologies. These devices can communicate, sense, or interact with their internal state or external surroundings thanks to their improved sensing, computation, and communication capabilities. (Yao et al., 2024) The (IoE), Systems that are completely networked are already a reality, smooth communication is essential and interoperability among different industrial systems has become more pressing than ever before. (Alshahrani et al., 2023) To address the challenges posed by massive data traffic, demonstrate the potentials of semantic information processing in industrial manufacturing processes and then propose a brief framework of semantic processing and communication systems for industrial networks. (Alshathri et al.,2023)

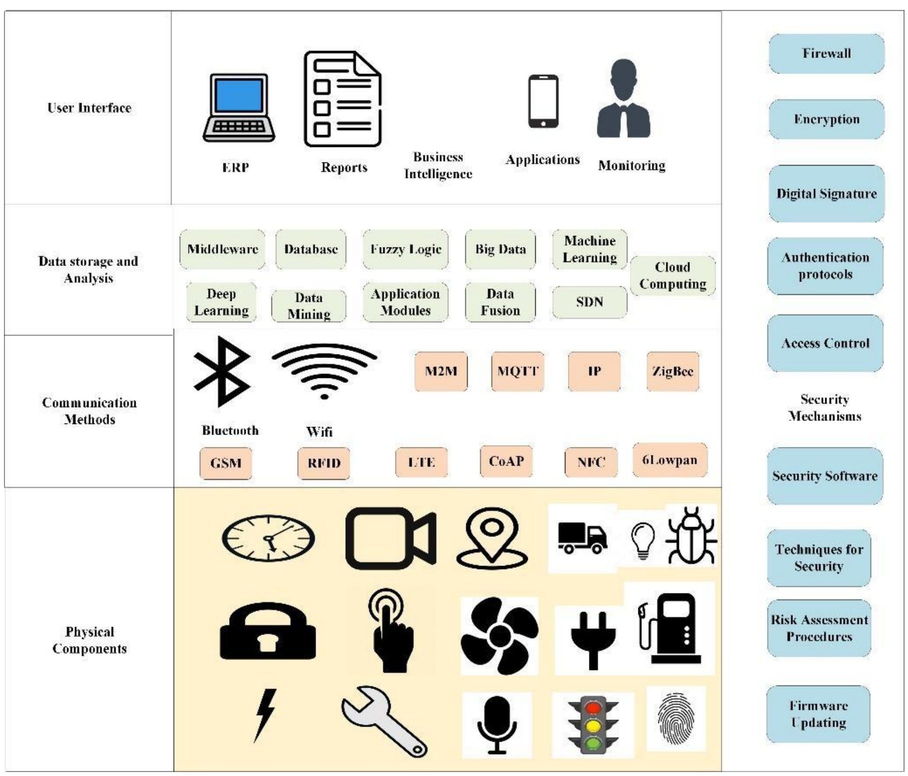

Figure 1: Architecture of IIoT (Alabadi et al., 2022)

Figure 1 presents that by eliminating the existing complexity, aggregation may provide a consistent description of such data. There are currently four primary data aggregations: centralized, in-network, tree-based, and cluster-based techniques. Data Storage: The cloud currently used by IIoT for data storage. The cloud as a platform has robust software and hardware in nature. As storage, the most crucial feature of a cloud is its scalability. Data stored in the cloud can be analyzed or interpreted quickly using AI or data-mining algorithms. Recently, different layers of clouds, such as fog computing, may improve the latency. In addition to the cloud, specific manufacturing networks may use individual data centres or servers to store their data according to their plans and strategies.

Exploring IIoT architecture and components, prioritizing security and privacy safeguards is crucial for robust industrial IoT applications. (Alabadi et al., 2022) the IIoT architecture is built on the collaboration of numerous components or levels. The architecture proposed by the survey. At least, the existence of these components is required if the objectives of IIoT integration are to be met. (Qaddoori et al., 2023) Those components are Physical components: and contain all physical objects in the manufacturing system. The most important items are machines that perform industrial production work. Other objects are sensors, actuators, and gateways; as explained above, they bring other characteristics to the industrial framework Communication Methods IIoT is heavily dependent on the wireless protocol for transferring data between network elements. (Golchha et al., 2023) Communication methods in IIoT need to ful fill various specifications, including low power consumption, high communication capacity, and stable interconnection. Nevertheless, these specifications may vary from sector to sector; for example, M2M connectivity involves a high-reliability link as the highest priority, while high-bandwidth connectivity from computer to cloud is the highest priority. (Divya et al., 2023) Data aggregation methods: Data aggregation is a mechanism in which multi-data packets are obtained, and one output packet is generated. Considering the overwhelming amount of data produced from physical objects, data aggregation is an important feature of IIoT.

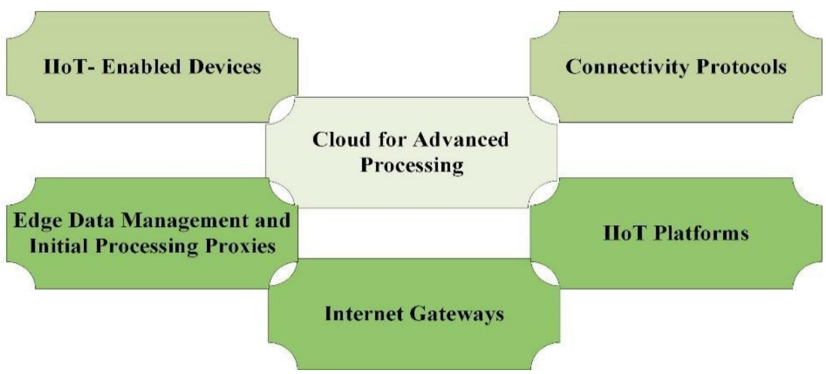

Figure 2: Components of IIoT Architecture (Chiradeep et al., 2023)

Figure 2 represents the Industrial Internet of Things architecture a networked system made up of essential parts that work together to optimize industrial processes. Sensors and actuators that gather and process physical data are the first parts of it. The data is subsequently processed and transmitted by edge devices and gateways over wired (such as Ethernet, Modbus) and wireless (such as Wi-Fi, 5G) connections. There are several levels of data processing, such as edge, fog, and cloud computing, which guarantees scalable and effective data management. Advanced data analysis and machine learning capabilities are offered by analytics platforms, supporting industrial applications that may be accessed through dashboards and mobile apps, including SCADA systems, MES, and ERP. Network, device, and data security procedures are all part of the critical security framework, and industry standards and communication protocols guarantee compliance and interoperability. HMIs and mobile/web interfaces promote human contact, while middleware and APIs enable smooth system integration. Remote monitoring and predictive maintenance technologies, which use data analytics to enhance maintenance and support, and to stop equipment malfunctions. Examining IIoT applications and use cases highlights the imperative of integrating robust security and privacy measures for industrial settings. (Chalapathi et al., 2021) presented the system architecture for a manufacturing-based setup when examining the applications of edge computing in manufacturing. Following the description of this design, a case study centred on the installation of an active maintenance system on a test platform is offered. (Alenezi et al., 2023) Four domains make up System Architecture. To support active system administration, the application domain is in charge of offering thorough supervision over the whole manufacturing system. Hence, the application domain helps to maintain service security while also enabling the system to create flexible, generic, and interoperable intelligent applications. (Sezgin et al., 2023) The data domain is in charge of offering functions like feature extraction, data cleansing, and intelligent inference, which let the system optimize its processes and boost throughput and efficiency. Because of the edge computing node's proximity to the end devices, this domain also has the crucial attribute of enabling quick data access for end nodes, which helps with real-time reaction generation for specific events. (Hasan et al., 2023) Essentially, the network domain makes use of Software Defined Networking architecture to handle control plane and network transmission operations, and it is in charge of establishing the connection between the end devices and the data platform. This domain also uses a Time Sensitive Network (TSN) protocol, which is widely utilized in processing network-related data sequentially and for handling time-sensitive information. (Alnajim et al., 2023) This domain is an essential component of the overall system architecture because it provides common standards for managing and maintaining the time-sensitive nodes. d. The term "device domain" describes the embedded or fixed devices found in field gear, such as robots, controllers, sensors, actuators, and machine tools. (Yin et al., 2023) The ability of this domain to support an infrastructure for adaptable communication models is required to maintain a range of communication protocols. This is achieved by maintaining nodes that dynamically alter the system's execution strategies in response to inputs from the sensors. (Alotaibi et al., 2023) This study frequently observes that well-known protocols like OPC UA and Data Distributed Service (DDS) are used to build the information model on the edge nodes. Ultimately, this domain of the system architecture realizes the unified semantics of information exchange and is in charge of preserving data security and privacy. (Rashid et al., 2023) Study of Active Maintenance in Practice Because edge computing-based frameworks offer better efficiency, easier maintenance, and real-time adaptation, a wide range of industrial projects are shifting to them as cyber-physical systems proliferate. (Bhattacharya et al.,2023) This study shall be reviewing a case study on a customized production line for candy packaging, as entailed, a private cloud was used to provide service to customer orders.

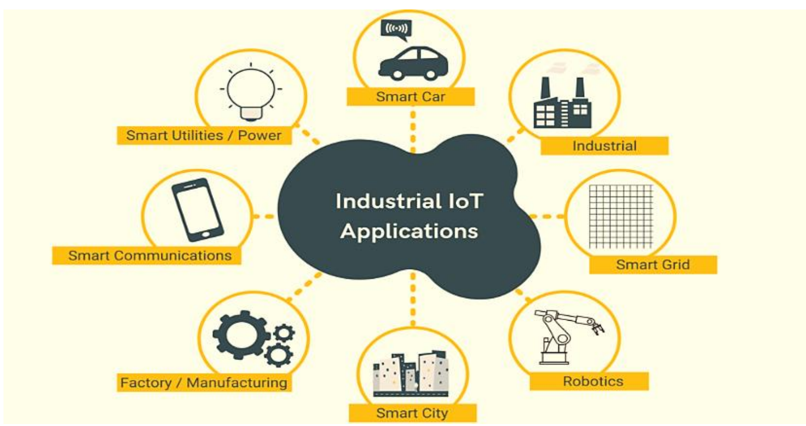

Figure 4: Application of IIoT (Alabadi et al., 2022)

Figure 4 represents manufacturing is the process of making a product; this process typically involves multi-level processing IIoT seeks to bring more innovations to manufacturing and implement a smart factory. Smart devices, electronics, and communication methods can boost production processes in a smart environment. This enhancement mainly affects manufacturing speed and flexibility, which means producing completely flexible production at the highest pace, especially when there is an extensive transition from conventional methods to advanced technologies. Smart factories often have to do with fascinating technological methodologies such as augmented reality, simulations, and virtual prototypes. The authors highlighted the requirements and essential concepts associated with the smart factory, including sustainability and predictive engineering. A general, intelligent factory architecture and explored the operating structure that organizes the involved technical components. Many criteria and challenges in designing a smart factory system have been explored in this work, including a multi-aspect comparison between conventional factories and smart factories. Automated Services Automation is the concept of performing a job with minimal human interference. IIoT can effectively support autonomy based on sensed data, depending on the decision-making process.

2. LITERATURE SURVEY

Recent research highlights that machine learning (ML) has become a central approach for enhancing the security of Industrial Internet of Things environments. This section of paper includes applications and use cases, machine learning algorithms for IIoT security, Performance Evaluation of ML Algorithms in IIoT Environments and Challenges of ML-based IIoT Security. The reviewed literature highlights that the integration of Machine Learning, Blockchain, and Privacy-Preserving techniques forms a promising pathway toward secure and autonomous IIoT systems. While Ethereum provides a practical platform for decentralized automation, challenges in scalability, interoperability, and real-time performance remain open research areas. Figure 3 shows section-wise sequence of the contents presented in the manuscript.

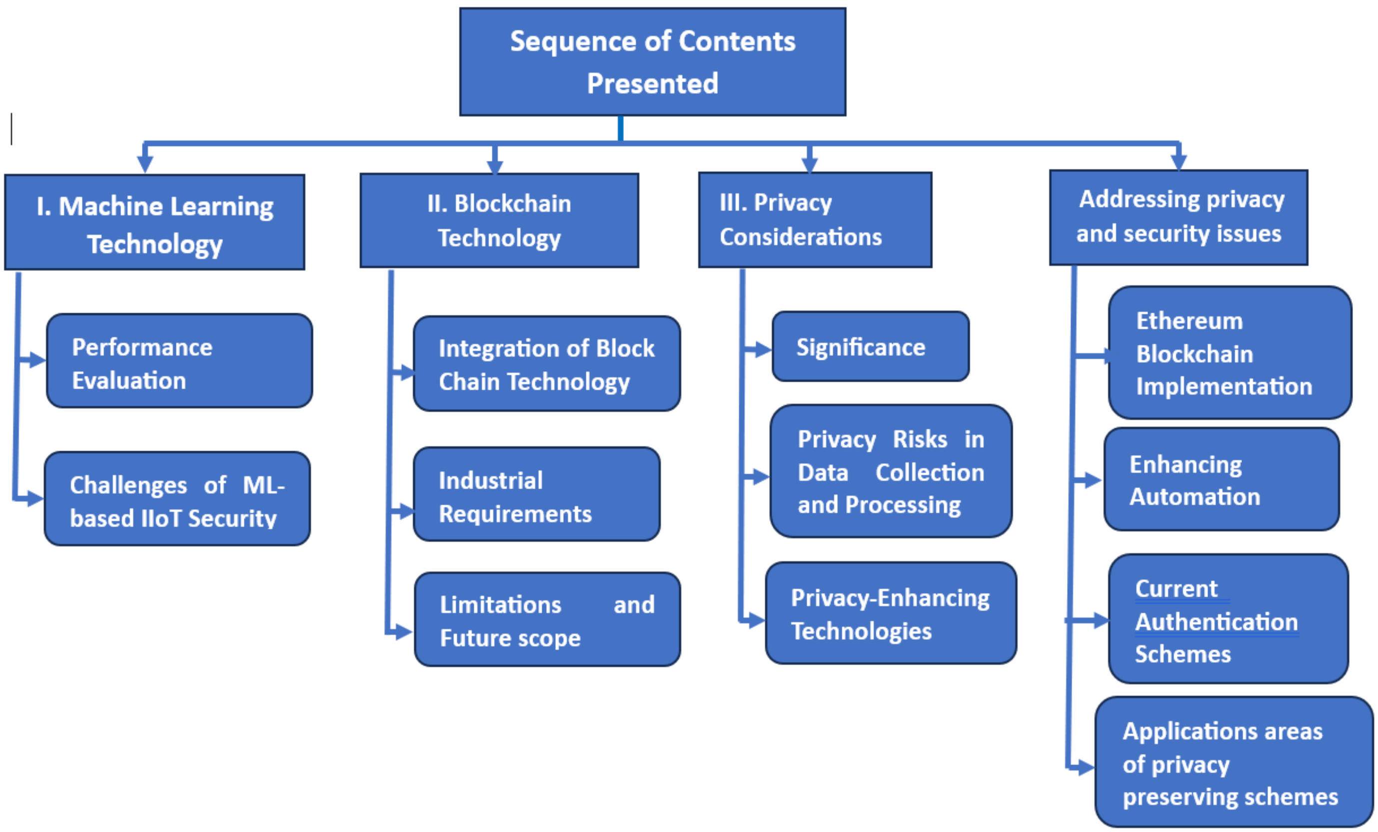

Figure 3: Sequence of the Contents Presented

3. Machine Learning Technology

Machine learning algorithms fortify IIoT security, critical amidst rising concerns. Privacy in IIoT demands comprehensive safeguarding measures. (Tange et al 2020) The industrial environment is where the Internet of Things paradigm is situated. The burgeoning Internet of Industrial and Industrial Technologies, also known as Industry 4.0, holds the potential to completely transform manufacturing and production through the utilization of a vast array of networked embedded sensing devices and the integration of cutting-edge computer technologies like artificial intelligence and fog/cloud computing. (Gopi et al., 2023) Increased interconnectedness, which the IIoT is known for, presents potential for cybercriminals as well as for the sectors that utilize it. Undoubtedly, one of the primary hindrances to the extensive integration of IoT technology at this time is security concerns. (Yazdinejad et al., 2023)

IIoT Security, focusing in particular on the security requirements of the IIoT. The secondary contribution is an analysis of how these needs might be met and the IoT's security enhanced by utilizing the relatively new Fog computing concept. (Rathee et al 2024) With the increasing demand for consumer electronics due to its recent evolution, the personal information that is shared is becoming valuable. In addition, the features of the future generation of Industrial Internet of Things (IIoT) devices include intelligence provision, automation, low cost, lower overhead, efficiency, and remote interactions while exchanging data. To provide a safe and effective transmission mechanism among networked devices, a hybrid trusted model integrating the objective model and fuzzy evaluation matrix approach is used (Khan et al 2024).

Table 1: Advantages and Disadvantages of IoT Devices (Demertzi et al., 2023)

Advantages	
Enhanced efficiency and productivity	Industrial operations can be streamlined and automated with the use of IIoT devices, which will decrease the need for manual labour and boost production.
enhanced gathering and analysis of data	Industrial processes can be streamlined and automated with the use of IIoT devices, which lowers the need for manual labour and boosts output.
Cost savings	IIoT gadgets can save expenses by maximizing energy efficiency, cutting waste, and enhancing asset management.
Remote observation and management	IIoT devices can be remotely controlled and monitored, which eliminates the need for staff to be present on the scene and allows for instantaneous intervention and observation.
Disadvantages	
Security risks	IIoT devices can be remotely controlled and monitored, which eliminates the need for staff to be present on the scene and allows for instantaneous intervention and observation.
Compatibility issues	IIoT devices might not work well with other IIoT devices or with current industrial systems, which could cause integration issues and extra expenses.
Lack of standardization	IIoT device interoperability and compatibility problems are now caused by the necessity for a generally recognized standard.
High implementation costs	IIoT devices can be costly to set up and maintain, especially for small and medium-sized businesses.

3.1 Performance Evaluation

Evaluating ML algorithms in IIoT environments is essential for optimizing performance while ensuring stringent security and privacy measures are upheld. (Alhuqayl et al., 2024) The predictive maintenance in industrial settings, this article investigates the combination of machine learning (ML) techniques and the Industrial Internet of Things. (Lazar et al., 2023) this research aims to improve predictive maintenance in industrial environments through smooth IIoT integration with ML. This work offers an approach that makes use of four different machine-learning models to address the complexity of industrial systems and the shortcomings of conventional maintenance techniques. (Li et al., 2023) The method involves a comprehensive evaluation of the validity of these models, exposing discrepancies that underscore the importance of a meticulous model selection process (Ruiz-Villafranca et al., 2023) Through in-depth data analysis and visualization, the present inquiry analysis determines the most effective model for predictive maintenance tasks. In addition to providing insights into the intricate relationships between IIoT and ML, it gives a possible future direction for the industry. (Ghiasvand et al., 2024) suggest an APT dataset for the IIoT environment that has all the data needed to complete the APT detection task. This is accomplished by creating an IIoT testbed and incorporating more than 20 attack methods that are commonly utilized in APT campaigns.

Certain invariant phases of the APT cycle, such as Defense Evasion, Data Collection and Exfiltration, Discovery and Lateral Movement, and Persistence, are created by the assaults that are carried out. (Rajawat et al., 2023) Through the integration of network logs and provenance logs with comprehensive attack data, the CICAPT-IIoT dataset offers the basis for creating comprehensive cybersecurity solutions. Furthermore, an exhaustive dataset analysis is offered, giving cybersecurity specialists a solid foundation upon which to construct creative and effective security solutions. (Karacayılmaz et al., 2024) defined the potential consequences of these attacks on the safety, reliability, and availability of critical infrastructures. Then propose an expert system that uses artificial intelligence methods including rule-based reasoning, anomaly detection, and reinforcement learning to identify and stop assaults on IIoT devices. (Mishra wet al., 2023) It describes the architecture and implementation of The system, which consists of three main components: a data collector, a data analyser, and a data actuator. (Yazdinejad et al., 2023) It also presents a table that summarizes the main features and capabilities of the system compared to existing solutions. The system's efficacy and performance will be assessed on a testbed comprising IIoT protocols like MQTT and Modbus, along with programmable logic controllers (PLCs). (Abbasi et al., 2023) Evaluate the system's accuracy, latency, and overhead by simulating different IIoT device assaults. The findings demonstrate that, with excellent accuracy, minimal latency, and overhead, the system is capable of identifying and thwarting various forms of assaults against IIoT devices. (Umran et al., 2023)

3.2 Challenges of ML-based IIoT Security

Industrial Internet of Things security based on machine learning (ML) has several major obstacles to overcome. (Baalamurugan et al., 2023) One of the main problems is that IIoT data is heterogeneous and unstructured, making it challenging to get high-quality, labelled data for training. Furthermore, it is difficult yet essential to provide real-time processing and low-latency data handling in large-scale IIoT networks. (Wang et al., 2023) The deployment of sophisticated machine learning models is made more difficult by the limited processing power of many IIoT devices. The picture is further complicated by privacy and security concerns, such as protecting against adversarial attacks and guaranteeing data privacy (Xiao et al., 2023). The complexity is increased by adhering to industry-specific laws and taking ethical issues about data usage and bias in ML models into account. (Ahmed et al., 2023) To address these issues and create ML-based IIoT solutions that are reliable, scalable, and secure, data scientists, cybersecurity specialists, and industry professionals must work together in a multidisciplinary manner. (Sengupta et al., 2023) Obtaining high-quality, labelled data for training is a huge challenge because IIoT data is heterogeneous and unstructured. In large-scale networks, handling low latency and real-time processing is crucial but difficult. Deploying complicated machine learning models is made more difficult by the restricted processing capacity of many IIoT devices (Ali et al., 2023). Two major security problems are protecting against adversarial attacks and ensuring data privacy. Furthermore, many ML models are black-box, which creates trust and interpretability problems (Capocasale et al., 2023). Resource constraints in IIoT environments further complicate deployment, as many industrial nodes have limited computation, memory, and energy resources, which restricts the use of heavy deep learning models. Additionally, the lack of standardized and up-to-date benchmark datasets limits reproducibility and fair comparison of models across studies. Finally, privacy and data-sharing concerns hinder the centralized collection of sensitive industrial traffic, motivating the exploration of federated and privacy-preserving learning, though these approaches introduce new challenges in communication overhead and model convergence.

4. Blockchain Technology

Block chain platforms are transforming IIoT by enhancing security, transparency, and efficiency in industrial operations and data management. (Tamilmani et al., 2023) Industrial Internet of Things block chain platforms use block chain technology with IIoT systems to improve industrial processes security, efficacy, and credibility. By providing decentralized, immutable, and transparent transaction records, block chain solves issues with data integrity, security flaws, and centralized control that traditional IIoT suffers. (Kotey et al., 2023) These systems make use of distributed ledger technology in block chain to establish a safe space for the safe recording, validation, and distribution of IIoT device data across nodes in a network. (Zheng et al., 2023) This feature not only guarantees data integrity but also makes automated smart contracts and machine-to-machine transactions possible, eliminating the need for middlemen and increasing operational effectiveness. Furthermore, block chain improves supply chain management by offering an auditable and transparent record of products and procedures, from the procurement of raw materials to the point of delivery. (Guha Roy et al., 2023) By reducing hazards, enhancing traceability, and facilitating real-time monitoring and predictive maintenance in industrial settings, this transparency can open up new avenues for cost- and innovation-cutting across a range of industries. Blockchain platforms offer secure foundations for IIoT, providing enhanced security and privacy for corporate applications in dynamic environments.

Usman et al., (2024) developed an enhanced role-based access control framework using Hyper Hyperledger block chain tailored for the Industrial Internet of Things. This framework aimed to reduce computational overhead while ensuring efficient information control and real-time responsiveness. Implemented with a layered architecture of chain codes, it effectively managed permission delegation and conflict resolution within dynamic IIoT networks. (Singh et al., 2023) Findings indicated significant improvements over traditional attribute-based methods, showcasing enhanced scalability, tamper-proof data integrity, and flexibility in handling conflicting scenarios. Extensive simulations validated its superior efficiency and scalability under high loads, highlighting its potential for advancing secure access control in IIoT applications. Mahmood et al., (2023) focused on enhancing Industry 4.0 and 5.0 initiatives by integrating digital twins with the IIoT to improve predictive capabilities. It introduces a block chain-based cross-domain authentication protocol aimed at securing interactions among IIoT devices while reducing computational and communication overhead (Razzaq et al., 2023). The protocol achieves significant efficiency gains, showing a 22.67% improvement in computation cost efficiency and a 16.35% increase in communication cost efficiency compared to current methods. It ensures robust data transfer security, protecting against physical attacks, and maintains privacy through guaranteed anonymity and unlink ability of identities across different IIoT domains, thereby supporting secure and efficient operations in interconnected industrial environments. Sanwar et al., (2023) aimed to develop a secure P2P and group communication framework for IIoT, integrating edge computing, consortium block chain, and IPFS-based data storage. It introduces an intelligent threat detection model using modified ECC, PUF, and Lagrange interpolation for secure communications, along with a modified PoV consensus algorithm to address latency in block mining.

4.1 Integration of Block Chain Technology

Block chain integration in IIoT enhances security. This study explores advancements safeguarding Industrial IoT applications against emerging threats. (Mishra et al., 2023) The Industrial Internet of Things and block chain technologies are changing how industries handle security and data integrity. In IIoT scenarios, managing large volumes of sensitive data and safeguarding connected devices require greater trust and transparency, which the immutable, decentralized ledger of the blockchain offers (Adhikari et al., 2023). With the aid of blockchain technology, this paper aims to investigate the most recent developments in security for IIoT applications. Blockchain's ability to provide an impenetrable record of transactions and device interactions is one of the main topics of investigation. (Trivedi et al., 2023) To lessen dependency on centralized authorities and reduce vulnerability to cyber-attacks, it also looks at how smart contracts might automate and secure processes within IIoT networks. The findings provide insight into case studies and research findings that demonstrate the potential of block chain technology to improve IIoT cybersecurity measures, including safe data exchange, robust supply chain management, and enhanced authentication. (González et al., 2023) Blockchain can completely transform industrial security procedures, opening the door to safer and more effective IIoT installations. These developments highlight this possibility. Bobde et al., (2024) aimed to enhance security in Industrial IoT networks using block chain technology. It introduces a methodology involving data collection, compression, and encryption with ChaCha20-Poly1305. A private block chain gateway manages data based on confidentiality levels, utilizing cloud servers or IPFS for storage. (Liu et al., 2023) The system employs a proof of authority consensus mechanism and Zero Knowledge Proof challenges for device authorization, balancing security and accessibility. The methodology effectively mitigates IoT network vulnerabilities by securing data integrity, confidentiality, and access control. (Garba et al., 2023) It enhances operational efficiency through optimized data retrieval and classification, demonstrating robustness against evolving security threats. The evaluation highlights significant improvements in security measures and system reliability, validating blockchain's role in fortifying Industrial IoT networks against cyber risks while maintaining efficient data management and accessibility.

Integrating blockchain technology into IIoT enhances security and privacy, critical for advancing industrial applications in interconnected digital ecosystems. Owen et al., (2024) investigated integrating blockchain technology into IIoT to enhance trust, security, and data integrity. It explores blockchain's fundamentals, consensus mechanisms, and suitable architectures for IIoT. The research identifies future research opportunities for advancing block chain integration in IIoT, emphasizing interdisciplinary collaboration for maximizing its benefits. Block chain integration enhances trust and security in IIoT by mitigating single points of failure and vulnerabilities. (Rao et al., 2023) It improves data integrity and transparency, benefiting industrial processes and supply chains. Challenges like scalability and energy consumption are addressed through scalable solutions and efficient consensus algorithms. (Rodríguez et al., 2023) Real-world implementations demonstrate practical benefits, encouraging adoption across industries. Economic implications include the potential for new business models based on enhanced trust. Future research should focus on optimizing block chain performance in IIoT, fostering collaboration between academia, industry, and policymakers to realize block chain's full potential in industrial applications. Yeap et al., (2024) aimed to propose a security framework for IIoT integrating block chain, cryptographic techniques, smart contracts, and deep learning-based IDS. It addresses vulnerabilities in traditional authentication methods by ensuring data integrity, enhancing user verification, and securing communications.

4.2 Industrial requirements of Blockchain

Unlocking the potential of block chain technology in industrial settings, this study delves into the practical applications of block chain in IIoT, (Selvarajan et al., 2023) exploring advancements in security and more. The practical applications of Block chain in industrial settings are increasingly significant, particularly in enhancing the security of Industrial Internet of Things (IIoT) applications. Block chain, originally developed for cryptocurrency transactions, (Singh, et al., 2023) offers a decentralized and immutable ledger system that can ensure transparency, traceability, and security in various industrial processes. In the framework of IIoT, where interconnected devices and systems are vulnerable to cyber threats, Block chain provides several benefits. (D'Angelo et al., 2023) It can establish a secure and trusted environment for data exchange and transactions between devices, reducing the risk of data tampering and unauthorized access. Additionally, Block chain's smart contracts enable automated and secure execution of agreements, (Ashok et al., 2023) enhancing operational efficiency and reliability. This evaluation focuses on exploring recent advancements in securing IIoT applications through Blockchain technology. It examines how Block chain's decentralized nature and cryptographic principles strengthen the resilience of industrial networks against cyberattacks and data breaches. (Patel et al., 2023) By analyzing real-world case studies and technological innovations, the study aims to provide insights into leveraging Blockchain for secure and efficient industrial operations in the era of digital transformation.

Blockchain finds practical applications, bolstering security and privacy in IIoT environments crucial for operational integrity and trust. Onifade et al., (2024) explored how blockchain technology can be applied in the mining sector to enhance transparency, efficiency, and ethical practices. It seeks to evaluate the feasibility and scalability of blockchain solutions in addressing operational inefficiencies, data omissions, security flaws, and corruption within the industry. (Ali et al., 2023) Additionally, the study aims to assess the potential of blockchain to modernize supply chains, mitigate sustainability risks, and improve industry reputation through enhanced data integrity and traceability. (Nagaty et al., 2023) The study identifies several potential applications of blockchain in the minerals industry, including conflict minerals tracking, preventing cheating scandals in mineral resources reporting, optimizing rock mechanics designs and monitoring strategies, improving blasting designs and operations, enhancing mine ventilation systems, (Altunay et al., 2023) streamlining mining machinery maintenance and management, and optimizing mining surveying processes. While stakeholders are increasingly exploring blockchain's capabilities, widespread adoption faces challenges related to technological complexity, scalability concerns, regulatory compliance, and industry-wide acceptance. (Wang et al., 2023) Nevertheless, early adopters are leveraging blockchain to pilot solutions that could significantly transform mining operations towards greater transparency and ethical standards. Naef et al., (2024) aimed to explore how firms overcome barriers to adopting blockchain in supply chain operations, focusing on the tension between centralised leadership and decentralised control in blockchain projects, and understanding the collaborative efforts necessary for successful implementation.

4.3 Limitations and Future Scope

Exploring security advancements in Industrial IoT applications reveals challenges and opportunities for blockchain adoption. Blockchain integration in Industrial Internet of Things (IIoT) applications brings opportunities and problems. (Abdullah et al.,2023) With its decentralized and unchangeable record, blockchain provides improved security by reducing the possibility of tampering and unwanted access while authenticating and tracking data transfers across IIoT networks. (Khan et al., 2023) Nevertheless, there are difficulties, such as issues with scalability brought on by the massive amount of data produced by IIoT devices and the computational power needed for block chain consensus processes. Another obstacle is still interoperability between various IIoT platforms and block chain protocols. Blockchain technology presents opportunities for improving data integrity, stakeholder confidence, and transparency in industrial operations. (Peter et al., 2023) Through the use of smart contracts, it may automate transactions, guarantee product provenance, and optimize supply chain management. To fully achieve blockchain's promise to revolutionize industrial operations and secure sensitive data across interconnected systems, research is concentrated on optimizing blockchain's performance in IIoT contexts and overcoming these issues.

Figure 5: Challenges for Block Chain Adoption (Noida et al., 2023)

Figure 5 represents the significant challenges that impede the widespread adoption of blockchain technology in Industrial Internet of Things applications. Key obstacles include the high implementation costs, essential for managing the extensive devices and data in IIoT environments. Security remains paramount to protect sensitive data and ensure the integrity of critical IIoT operations against unauthorized access and illegal activities like fraud. Privacy concerns arise due to the collection and processing of personal data within blockchain systems. Scalability issues must be addressed to handle the growing volume of transactions from IIoT devices efficiently. Additionally, there is a shortage of skilled blockchain professionals specific to IIoT, hindering adoption. High energy consumption raises sustainability concerns, particularly in energy-intensive IIoT sectors. Integration complexities with legacy systems further challenge blockchain adoption in traditional industries like manufacturing. Addressing these challenges through enhanced security, privacy technologies, scalability solutions, and increased awareness is crucial to realizing blockchain's full potential in IIoT applications.

Exploring blockchain in IIoT reveals critical security and privacy opportunities, addressing challenges with enhanced technological solutions. Rahman et al., (2024) explored delves into the integration of Artificial Intelligence

(AI) with Blockchain (BC) in the smart Industrial Internet of Things, examining its implications, benefits, and challenges. It explores state-of-the-art applications where AI augments decision-making and automation capabilities, complemented by BC's decentralized ledger ensuring data integrity and trust (Aouedi et al., 2023). The study identifies key benefits such as enhanced system efficiency, improved security measures, and streamlined automation across diverse sectors. Challenges like scalability, interoperability, and security vulnerabilities are addressed with proposed strategies and tools (Syamala et al., 2023). By highlighting the synergistic advantages of AI, BC, and smart IIoT, (Arnold et al., 2023) addressed the barriers hindering organizations' adoption of Industrial Internet of Things (IIoT) platforms, categorizing challenges into technological, organizational, and environmental dimensions. Through a Delphi study involving 22 international experts from academia and practice, the research identifies and categorizes 29 specific challenges (Karthik et al., 2023). Key findings reveal significant differences in the perceived importance of these challenges between academics and practitioners. These discrepancies highlight varying priorities and perspectives that impact adoption strategies and implementation approaches. The study emphasizes the critical need for tailored solutions to overcome these multifaceted barriers and promote the widespread adoption of IIoT platforms. (Issa et al., 2023) By providing insights into the relative significance of each challenge and the differing perceptions across stakeholders, the research contributes to advancing the understanding and effective deployment of IIoT technologies in both research and practical applications, fostering innovation and operational efficiencies in industrial settings. Sharma et al., (2023) investigated the hurdles hindering blockchain adoption in Indian government sectors for public-service delivery. Through an extensive review of the literature and focus-group discussions with policymakers and blockchain experts, 12 critical challenges have been identified (Rajagopal et al., 2023). These include the necessity for legislative backing, adequate technological infrastructure, governance frameworks, and fostering public trust. Employing interpretive structural modelling and MICMAC analysis, the research establishes a hierarchical framework that prioritizes these challenges based on their interrelationships and impacts (Lakhan et al., 2023).

5. Privacy considerations in IIoT applications

The Industrial Internet of Things transforms industries by combining smart devices to increase automation and efficiency, but it also poses serious security and privacy risks. (Rahman et al., 2023) Multi-factor authentication, role-based access management, and secure protocols like VPNs and TLS are examples of important security measures. Protecting data integrity and preventing unauthorized access requires intrusion detection systems and data encryption, both in transit and at rest. Transparency and security are improved in IIoT transactions by secure communication protocols like MQTT and block chain technology. (Ucbas et al., 2023) The main goals of privacy considerations are control, user permission, and data reduction. These goals guarantee that users are informed of data practices and that only data that is required is gathered. Protecting user privacy requires using anonymization techniques and adhering to laws like the CCPA and GDPR. (Al-Zoubi et al., 2023) The implementation of these measures, from smart factories to smart grids, is demonstrated through case studies in the manufacturing, healthcare, and energy sectors. In the future, edge computing for decentralized security, quantum encryption for ultra-secure communications, and AI integration for predictive analytics are all expected. (Rehan et al., 2023) IIoT applications must be protected by ongoing research and attention to legal requirements for industries to fully realize the potential of IIoT while upholding user confidence and data security. One of the most important privacy strategies is data minimization, which limits exposure to possible breaches by gathering just the information necessary to carry out a given function. (Sharma et al., 2023) To guarantee that users are properly informed about data collecting, processing, and sharing practices and have the means to alter their privacy preferences, user permission and control are also essential (Gangwani et al., 2023). Techniques such as data anonymization and pseudonymization are used to preserve data utility while safeguarding personally identifiable information (PII). To stop data from being linked back to specific people, these techniques entail hiding or deleting identifiable information. However, to keep the data relevant for analysis and operational needs, data usability and anonymization must be balanced (Goyal et al.,2023). For IIoT applications, especially those that operate internationally, compliance with legal and regulatory frameworks, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), is imperative (Bobde et al., 2023). IIoT solutions are guaranteed to comply with strict privacy regulations, safeguarding user data and upholding confidence, by adhering to industry-specific standards, such as NERC CIP for the electricity sector or HIPAA for the healthcare business.

5.1 Significance in IIoT environment

The security of sensitive data gathered, stored, and sent by networked devices and systems is referred to as privacy in the Industrial Internet of Things. (Tripathi et al., 2023) This includes preventing unauthorized access, misuse, or exposure of operational data, personally identifiable information (PII), and other confidential information. Privacy controls guarantee that data is managed in a way that respects user rights and complies with legal requirements. Large volumes of data, including sensitive operational and personal data, are produced by IIoT data protection systems. (Alshudukhi et al., 2023) Adequate privacy safeguards avert data breaches and illegal access, which can result in monetary losses and harm to one's reputation. Adherence to Regulations Complying with privacy laws like the CCPA and GDPR as well as industry-specific guidelines is crucial to avoiding fines and making sure IIoT apps follow the law. User Trust Maintaining strong privacy policies fosters confidence among users and other stakeholders. (Kumar et al., 2023) Customers are more inclined to interact with and support IIoT applications when they are aware that their data is secure. Operational Integrity to Privacy safeguards contribute to the preservation of IIoT system integrity by guarding against data manipulation and guaranteeing correct data utilization, both of which are essential for producing trustworthy business decisions and sustaining operational effectiveness. (Falayi et al., 2023) Establishing privacy is essential for the safe and efficient use of IIoT technologies, as it promotes compliance, trust, and operational dependability.

Explore the crucial role of privacy in IIoT, emphasizing security enhancements and vital privacy considerations in industrial applications. (Pinto et al., 2024) Designing new services and business models that enhance customer experience and pleasure is made possible by data from the Internet of Things (IoT). These data are valuable information sources for a wide range of fields, such as bio surveillance, smart cities, smart health, and disaster management. However, because this scenario calls for the collecting of personal data, it presents additional difficulties in protecting data privacy (Jiang et al., 2023). As a result, strive to present up-to-date knowledge about privacy-related challenges in the context of the Internet of Things, with an emphasis on research that uses the Personal Data Store (PDS) as a workable remedy for these issues (Gaba et al.,2023). To do this, it carries out a methodical mapping review to locate, assess, and comprehend pertinent material regarding privacy concerns and PDS-based solutions in the context of the Internet of Things. (Luz et al., 2024). Industrial Internet of Things devices have revolutionized industrial processes, enabling efficient data collection and analysis. However, the pervasive connectivity and large-scale data sharing in IIoT ecosystems have raised significant concerns regarding the protection of sensitive information (Shah et al., 2023). The application of differential privacy techniques as a promising solution to safeguard sensitive data in industrial IoT environments. Differential privacy is a privacy-preserving framework that focuses on minimizing the risk of re-identifying individuals' information while allowing meaningful analysis of aggregated data (Parmar et al., 2023). Differential privacy approaches guarantee that the statistical characteristics and patterns of the original data may still be recovered by introducing controlled noise into the gathered data while the privacy of individuals is protected. The collection and analysis of sensitive data are essential for optimizing processes and improving productivity, (Al Hwaitat et al., 2023) the deployment of differential privacy techniques can address privacy concerns without compromising the utility of the data.

5.2 Privacy Risks in Data Collection and Processing

The vast and interconnected structure of these systems makes privacy risks in IIoT data collecting and processing substantial. Since weak security measures might let bad actors take advantage of private data, unauthorized data access is a serious problem. If operational or personal data is compromised, data misuse may result, potentially creating fraud or a competitive disadvantage. (Sivaselvan et al., 2023) When sensitive information is exposed due to system vulnerabilities, there is a risk of data breaches that could affect both persons and companies. When merged with other datasets, inadequate anonymization procedures may lead to the re-identification of specific persons. Furthermore, privacy issues and non-compliance with regulations might result from a lack of user consent and transparency regarding data processing. (Sánchez-de la Rosa et al., 2023) Transnational data transfers provide challenges to privacy management since they necessitate compliance with diverse local laws. Privacy hazards are further increased by improper data retention procedures, such as keeping data longer than necessary. Finally, data breaches might occur due to insufficient security measures, such as weak encryption and inadequate access controls. Strong security mechanisms, legal compliance, and user transparency regarding data handling procedures are crucial for IIoT privacy protection to reduce these threats.

Research into the complexities of privacy risks in IIoT data operations, focusing on security enhancements and crucial privacy considerations. (Frank et al., 2024) Security concerns in IIoT deployments revolve around vulner abilities in the systems and potential attack vectors. Inadequate authentication and authorization mechanisms, weak encryption and data protection, and the lack of secure software and firmware updates are some vulned abilities that can be exploited. Attack vectors include physical attacks, network-based attacks data breaches, and insider threats. The consequences of security breaches in IIoT can result in operational disruptions, compromise of sensitive information, and safety risks. Multifaceted solutions are needed to address the security and trust deficits. Along with the development of best practices and industry-wide standards, it entails improved cooperation and communication to foster trust via accountability and openness (Fitzpatrick et al., 2023). Robust security measures, such as strong authentication, encryption, and regular security assessments, are essential. Continuous monitoring, incident response planning, and security education and awareness programs. (Madhwal et al., 2023) It is imperative to solve the significant challenges of the trust deficit and security concerns in IIoT deployments. The industry may reduce risks and guarantee the safe and effective implementation of IIoT technologies by emphasizing trust-building, putting strong security measures in place, and encouraging ongoing monitoring and education. To overcome these obstacles and establish a safe IIoT ecosystem, stakeholders must continue their efforts and work together.

5.3 Privacy-Enhancing Techniques

Industrial Internet of Things applications require the protection of sensitive data, which is why privacy-enhancing technologies, or PETs, are essential. The protection of data, while it is in transit and at rest using protocols like TLS and algorithms like AES, renders it unreadable to unauthorized parties. This is why data encryption is essential. By hiding or removing personal identifiers from data, data anonymization and pseudonymization techniques lower the possibility of re-identification while maintaining the usefulness of the data. By preventing parties from disclosing confidential information to one another, Secure Multi-Party Computation improves privacy when sharing data between parties. Differential privacy introduces noise into data while maintaining the confidentiality of individual records and offering insightful information for analysis. (Cabrera-Gutiérrez et al., 2023) Block chain technology, which uses decentralized ledgers and smart contracts, provides transaction transparency and immutability, data integrity protection, and safe access control. By incorporating privacy safeguards from the beginning of the construction of IIoT systems, Privacy-By-construction principles guarantee that data protection is a fundamental component of system architecture. By putting these PETs into practice, privacy risks are reduced and IIoT systems may function securely while upholding user confidence and regulatory compliance. (Khordadpour et al., 2024) Internet of Things (IoT) environments are a revolutionary step towards ensuring robust security and enhanced privacy. This study explored the particular difficulties and remedies related to protecting Internet of Things (IoT) systems built on blockchain technology, emphasizing the value of anonymous audits in enhancing security and privacy. Provide a revolutionary framework that blends cutting-edge security protocols designed for Internet of Things scenarios with the decentralized nature of block chains. Utilizing anonymization techniques in auditing procedures is essential to the strategy since it protects user privacy while preserving the integrity and openness of block chain transactions. It describes the block chain architecture used in Internet of Things contexts, highlighting the process and particular security measures used. Introduce a security protocol as well that combines anonymous auditing approaches with tools that improve privacy, such as improved cryptography techniques.

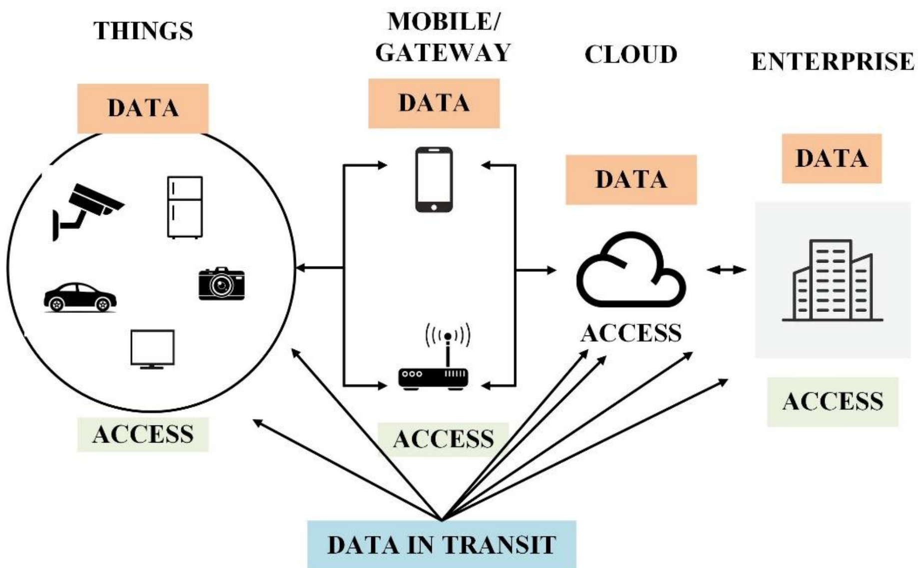

Figure 6: Security and Privacy in IIOT (Lawrence Jacob et al., 2022)

Figure 6 illustrates the architecture and security considerations within an Industrial Internet of Things system. It outlines key components including IoT devices (sensors, cameras), mobile/gateway devices for data processing and transmission, cloud services for data storage and analytics, and the enterprise managing the entire system. Data flows through these components, posing security challenges such as unauthorized access and interception during transmission. Critical security measures highlighted include data protection strict access controls, compliance with privacy regulations, network security to prevent breaches, and securing IoT devices against vulnerabilities. These measures aim to safeguard sensitive data and maintain the integrity of IIoT operations. By implementing robust security and privacy protocols, organizations can mitigate risks and ensure secure data exchange across their IIoT ecosystem, fostering reliability and trust in data-driven decision-making and operational efficiencies.

Advanced privacy-enhancing technologies tailored for IIoT, emphasizing security upgrades and essential privacy considerations in industrial IoT applications. (Pennekamp et al.,2024) Stakeholders are gathering enormous volumes of data as a result of the Industrial Internet of Things , which is causing industrial processes and environments to become more networked and integrated. The majority of information is still frequently contained in local information silos, even though international information sharing and industrial partnerships in the IIoT promise to improve efficiency, sustainability, and product quality, among other benefits. Apart from the challenges posed by interoperability, the primary barrier to the complete implementation of these advancements in practice continues to be the confidentiality concerns of relevant stakeholders, which significantly impede current industrial partnerships in the real world. This dissertation fills this vital research gap as a result. Because current methods of sharing information while protecting privacy do not scale to IIoT applications at the industry level. The requirement for AI model training to derive useful insights from massive volumes of sensor data has increased as a result of industrial Internet of Things (IoT) applications. However, sharing sensitive industrial data for cooperative model training raises data privacy issues. In industrial IoT environments, federated learning has emerged as a viable technique that allows for collaborative training of AI models while maintaining data privacy. To overcome the issues around data privacy, this article looks into the application of federated learning in industrial IoT. (Jonathan et al., 2024) explained the industrial IoT and the role that AI model training plays in this domain. It draws attention to the problems with data privacy and offers federated learning as a possible fix. Federated learning's concept, elements, benefits, and drawbacks are all described. Next, the use of federated learning in industrial IoT is examined, with a focus on the advantages it provides for training AI models. To show how federated learning may be successfully used in industrial IoT contexts, case studies and examples are provided. One of the most important aspects of federated learning is data privacy preservation. It explores the methods and strategies used to safeguard private information during training. Additionally, federated learning is contrasted with other privacy-preserving methods.

6. Addressing privacy and security issues in IIoT with Ethereum platform

Progression in security for Industrial IoT applications is complemented by investigating Ethereum experiments. It entails determining how Industrial Internet of Things technologies can be improved using Ethereum blockchain technology. In IIoT contexts, Ethereum's capabilities in smart contracts and decentralized applications (DApps) offer potential advantages like automation, transparency, and data integrity. Ethereum is being investigated by researchers and practitioners for its potential to manage IIoT devices securely, analyze data in real-time, and facilitate trustless interactions between stakeholders and devices. On the other hand, the article Exploring security developments in Industrial IoT applications concentrates on improving the security protocols inside IIoT networks. This covers techniques for safeguarding data integrity, reducing the risk of cyberattacks, and guaranteeing the dependability of IIoT networks. (Li et al., 2023) Technological developments in encryption, authentication methods, and anomaly detection systems are essential for protecting confidential information and preserving business continuity in industrial environments. Collectively, these investigations seek to leverage Ethereum's technology innovations to optimize IIoT systems while tackling important security issues. IIoT applications may be able to increase operational efficiency, robustness, and trustworthiness by incorporating safe blockchain platforms like Ethereum.

Explore Ethereum's potential for IIoT applications, highlighting security enhancements and critical privacy considerations in industrial IoT environments. (Goyal et al., 2024) aimed to develop a novel IIoT framework to mitigate cyberattacks leveraging Ethereum blockchain technology in industrial applications. By integrating supervised learning and quantum classifiers, the framework enables real-time detection and prevention of fraudulent Ethereum transaction patterns. Initial trials demonstrate superior performance with reduced false positives and improved detection accuracy compared to conventional methods. This approach addresses critical vulnerabilities inherent in Ethereum-enabled IIoT devices, enhancing overall security and resilience against cyber threats in industrial environments. The findings underscore the potential of advanced technologies such as quantum computing and machine learning to fortify the security framework of IIoT systems, ensuring robust protection and reliability in industrial operations. (Gulia et al., 2024) explored the application of blockchain technology to Internet of Things devices, with an emphasis on improving security, privacy, and data integrity. It comprehensively covers blockchain architecture, working principles, types, applications, and platforms relevant to IoT environments. The study seeks to identify the potential benefits of blockchain, discuss real-world applications, analyze various platforms, and address challenges associated with its implementation in IoT. Blockchain offers decentralized consensus, immutability, and transparent transaction records that bolster IoT security. Integration with IoT enhances trust in data exchange, mitigates risks of compromised devices, and improves overall system reliability. Real-world applications span industries such as healthcare, supply chain management, and smart cities, demonstrating diverse uses and benefits. Challenges include scalability issues, energy consumption concerns, and interoperability complexities, highlighting areas for further research and development to fully leverage blockchain's potential in IoT ecosystems. (Wahrstätter et al., 2024) aimed to introduce OpenFL, a collateral-backed reputation system on Ethereum, to enhance trust in decentralized Federated Learning (FL). It focuses on integrating blockchain to mitigate scalability, latency, and privacy issues in permissionless FL frameworks.

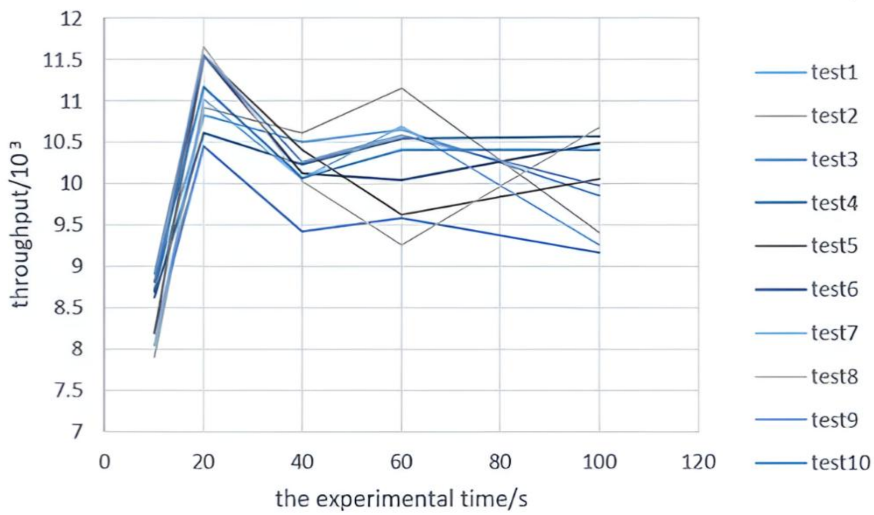

Figure 7: Transaction Throughput of Different Blocks (Xie et al., 2022)

Figure 7 illustrates transaction throughput comparisons across different blockchain tests (1, 2, 8,10). Each test is represented by a set of throughput values measured in transactions per second (TPS). These values reflect the capability of each blockchain implementation to process and confirm transactions within a specified time frame. Figure 6 underscores the performance implications of blockchain technology. Higher TPS values indicate improved transaction processing speed, crucial for IIoT applications where real-time data handling is essential. Security enhancements such as robust encryption, secure access controls, and tamper-resistant data storage are vital to safeguarding sensitive IIoT data within blockchain systems. Privacy considerations involve protecting personal and proprietary information from unauthorized access and ensuring compliance with privacy regulations. By analyzing transaction throughput data in Figure 6 alongside security and privacy measures, when deciding which blockchain solutions to use in IIoT environments, businesses can make well-informed choices that strike a balance between security and privacy requirements and performance.

6.1 Implementing Blockchain on Ethereum Platform

Ethereum Blockchain in IIoT complements advances in security for Industrial IoT applications. The analysis examines how Ethereum blockchain technology might be incorporated into Industrial Internet of Things applications, with a particular emphasis on how this could improve security. Potential advantages include enhanced data integrity, transparency, and automation in IIoT contexts provided by Ethereum's decentralized ledger and smart contract features. The purpose of this integration is to provide a tamper-resistant framework for recording and verifying transactions across networked devices, thereby addressing security challenges. (Brandín et al., 2023) Concurrently, the study Investigating Security Progress in Industrial IoT Applications looks at new security methods that are specifically designed for IIoT systems. To lessen cyberthreats that target industrial devices and networks, it addresses developments in encryption, authentication, and anomaly detection. The evaluation also looks at how new technologies like blockchain might support operational resilience and data protection in IIoT environments. Collectively, these viewpoints draw attention to the changing environment at the intersection of IIoT security breakthroughs and Ethereum blockchain advances, to strengthen industrial operations' defences against cybersecurity threats and facilitate more reliable and efficient data management and automation procedures.

(Asri et al., 2024) aims to enhance blockchain-based authentication through the integration of Ethereum smart contracts and AI-driven anomaly detection in Industrial Internet of Things contexts. The objectives include fortifying security measures against evolving threats and ensuring transparency, adaptability, and robust authentication capabilities for IIoT applications. The integration of AI-driven anomaly detection with blockchain-based authentication, coupled with Ethereum smart contracts for two-factor authentication (2FA) and GFE algorithms, significantly enhances security in IIoT. Experimental results demonstrate improved threat detection and mitigation, ensuring resilient defence mechanisms against vulnerabilities. This approach fosters transparency and adaptability, enabling effective data-driven decision-making while safeguarding IIoT operations from unauthorized access and cyber threats.

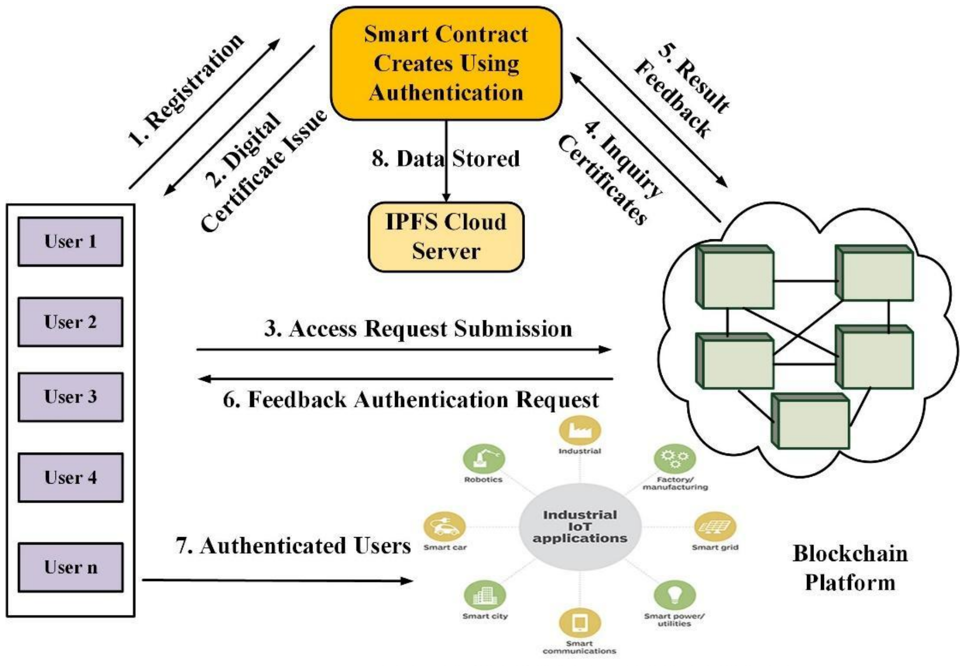

Figure 8: Block Chain Application in IIoT (Amith Kumar et al., 2022)

Figure 8 illustrates a blockchain-based system tailored for user authentication and data management in Industrial Internet of Things applications. The process begins with user registration and issuance of digital certificates for authentication. Users then submit access requests, initiating the creation of smart contracts that define access permissions based on authentication credentials. Upon approval, users receive inquiry certificates reflecting their access rights. They subsequently provide feedback on accessed data, which undergoes authentication for validity. Verified users gain secure access to the system and data, which is stored on an IPFS cloud server for enhanced security. Blockchain functions as a distributed ledger, recording all interactions and transactions in a transparent, immutable manner. This framework ensures data integrity, enhances security through its tamper-proof nature, and facilitates efficient access control management via smart contracts. Benefits include heightened trust and transparency in data sharing processes, streamlined access management, and secure data storage, making it ideal for enhancing operational reliability and security in IIoT environments.

(Singh et al., 2023) aimed to thoroughly explore the integration of blockchain technology into the Internet of Things, leading to the development of Blockchain-based IoT (BIoT) applications. It begins by examining how blockchain can be adapted to fulfil the specific requirements of IoT, such as seamless authentication, data privacy, security, resilience against attacks, deployment simplicity, and self-maintenance. The study then delves into detailing prominent BIoT applications, illustrating how blockchain enhances traditional cloud-based IoT by providing advantages like heightened security and decentralized data management. Factors influencing BIoT development, including technical and operational considerations, are comprehensively covered. Additionally, the paper identifies current challenges in BIoT implementation and offers recommendations to assist future researchers and developers in overcoming these obstacles, thereby facilitating the successful deployment of advanced BIoT applications in various domains. Aims to tackle critical data security challenges in the Industrial Internet of Things by proposing a Privacy-Preserving Support Vector Machine (PP-SVM) training method using blockchain-encoded IoT data. Key objectives include developing a secure SVM training approach ensuring confidentiality and integrity across diverse data sources.

Blockchain integration facilitates secure data exchange among decentralized nodes with encryption techniques safeguarding sensitive IoT messages. Implementation of the Paillier homomorphic cryptographic algorithm enables secure algebraic operations during SVM training, preserving data privacy. (Masood et al., 2023) Rigorous security assessments validate SVM model parameter confidentiality and protect sensitive information from each data source. The proposed PP-SVM method effectively mitigates data security risks in IIoT. Experimental results demonstrate enhanced confidentiality through blockchain-based encryption, ensuring IoT data integrity. The developed SVM algorithm minimizes communication steps, enhancing computational efficiency. Robust security measures confirm data privacy across decentralized networks. Extensive testing validates the approach's practical viability, highlighting its potential for secure deployment in real-world IIoT applications.

6.2 Enhancing automation with Blockchain

Enhancing IIoT automation in industries through smart contracts transforms operational efficiency and reliability. Smart contracts can be used to improve IIoT automation in companies by utilizing blockchain technology to improve operational dependability and efficiency. Smart contracts are self-executing programs that, when certain requirements are satisfied, automatically carry out established rules that have been encoded into software. Smart contracts enable automated transactions and procedures Within the framework of the Industrial Internet of Things, linked devices do away with the need for middlemen and cut down on operational expenses and delays. At the same time, it concentrates on improving security protocols in IIoT settings. To reduce cybersecurity risks aimed at industrial systems, it explores developments in authentication, encryption, and anomaly detection systems. The evaluation also takes into account how blockchain technology, particularly smart contracts, may support data transparency and integrity while strengthening IIoT infrastructure's defences against changing cyberthreats. Collectively, these developments demonstrate how smart contracts in IIoT may reinforce cybersecurity safeguards, increase transparency, and streamline processes. Industries can optimize workflows, guarantee data integrity, and improve overall resilience in their IIoT implementations by incorporating secure automation mechanisms like smart contracts.

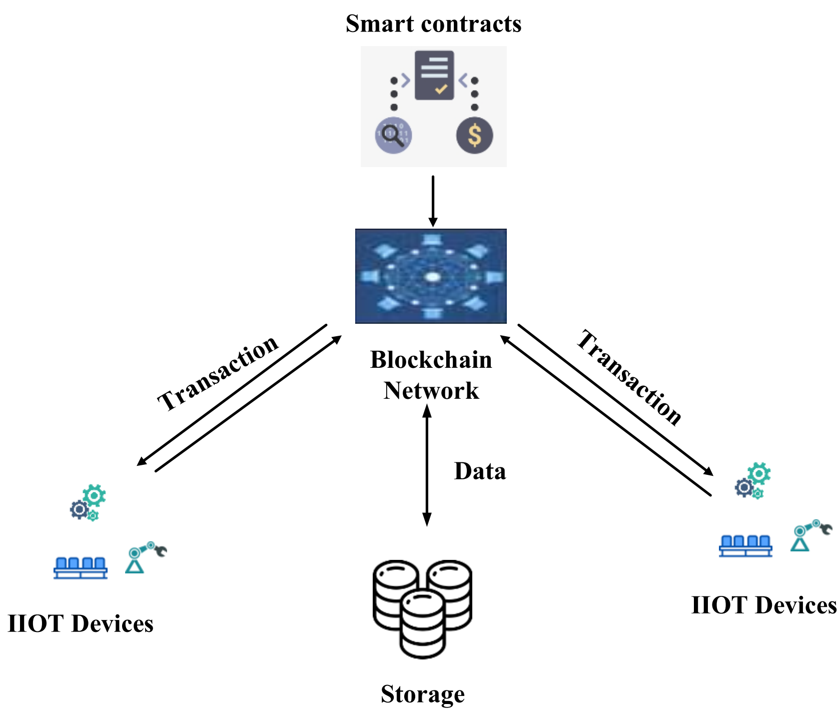

Figure 9: Integration of Blockchain, Smart Contract, and IIoT-Based System (Dwivedi et al., 2021)

Figure 9 depicts a blockchain-based system architecture tailored for Industrial Internet of Things applications. IIoT devices generate and transmit data to the blockchain network, where transactions are recorded on a distributed ledger ensuring data integrity. Smart contracts, encoded with predefined terms, automate and enforce rules for data sharing and processing. Data and smart contracts are securely stored within the system. This setup facilitates secure, transparent, and trustworthy interactions within IIoT environments. It enhances security by leveraging blockchain's immutability and decentralization, ensuring tamper-proof records of data exchanges. Smart contracts streamline operations by automating processes based on predefined conditions, thereby optimizing efficiency and reliability in IIoT applications (Kumar et al., 2024). Overall, the integration of blockchain, smart contracts, and IIoT systems enhances operational integrity and security while promoting transparent data management and automated contractual agreements.

Explore the integration of smart contracts to enhance IIoT automation, emphasizing security enhancements and pivotal privacy considerations in industrial applications. Introduced a smart contracts management system that integrates blockchain and edge computing to address security challenges in the Industrial Internet of Things. Key objectives include developing robust smart contracts to mitigate IoT hardware vulnerabilities, enhancing password security, and ensuring data encryption and integrity. Blockchain technology is utilized for secure transaction management, facilitating streamlined data consolidation and improved privacy across various platforms. Integration of edge computing optimizes network efficiency by decentralizing computational tasks, enhancing scalability for real-time data processing in IIoT environments. This approach aims to bolster security measures and advance the reliability of IIoT applications through innovative technological convergence. The proposed smart contracts management system effectively addresses IIoT security concerns by leveraging blockchain's secure ledger and edge computing's decentralized computational capabilities. Experimental validation demonstrates improved reliability through enhanced data management practices and scalable infrastructure, illustrating its potential to enhance security and advance IIoT applications in practical settings. (Singh et al., 2024) studied were to integrate predictive maintenance (PdM) with the Industrial Internet of Things using deep learning (DL), while addressing security risks and managing large volumes of time series data.

Proposed a decentralized framework leveraging blockchain for security and the IPFS, or interplanetary file system, for storing data. The findings demonstrate that this approach effectively ensures data integrity and security while maintaining high accuracy in predictive analysis tasks. Performance analyses validated the framework's efficiency in terms of accuracy, execution time, and computational cost. Security evaluations underscored the robustness of the decentralized architecture against potential attacks, leveraging blockchain's immutability and smart contract capabilities. Overall, the integrated framework represents a significant advancement in industrial maintenance strategies, offering a secure, scalable solution for handling complex data sets in IIoT environments, thereby enhancing operational reliability and efficiency. (Benias et al., 2023) Investigated the feasibility of leveraging blockchain and smart contracts to enhance cybersecurity within the Industrial Internet of Things framework. It begins with an introduction to IIoT, blockchain, and smart contracts, outlining their fundamental concepts and properties. A comprehensive literature review identifies both the advantages and challenges associated with implementing these technologies. Challenges are categorized into architecture and privacy-related issues, each further subdivided to highlight specific complexities. The study highlights typical use cases to demonstrate the useful integration of smart contracts and blockchain technology to improve IIoT cybersecurity. Finally, the study proposes a conceptual framework for future research directions in IIoT cybersecurity, aiming to address identified challenges and capitalize on the benefits offered by blockchain and smart contracts.

6.3 Current Privacy-Preserving Authentication Schemes

Literature shows a strong trend towards using blockchain to build decentralized, transparent, and privacy-enhanced authentication frameworks for critical cyber-physical systems like connected vehicles, drones, and industrial IoT. Few of them are elaborated below.

6.3.1 Scheme 1: BTC2PA (blockchain-assisted, conditional privacy-preserving authentication)

Rawat et al. (2025) proposed BTC2PA, a blockchain-assisted scheme that combines conditional privacy (traceability of misbehaving vehicles by a trusted authority) with a distributed trust-computation layer implemented on a permissioned blockchain. The design uses on-chain records for trust score aggregation while keeping identity-linking information off-chain until conditional reveal is required; this provides accountability without continuous exposure of vehicle identities. BTC2PA is notable for its system-level treatment of trust and revocation in addition to message authentication, but it incurs blockchain related latencies and storage overheads that must be accounted for in high-mobility scenarios. When comparing blockchain-based approaches in our paper, BTC2PA is a good representative to discuss tradeoffs between decentralised trust management and real-time constraints of connected vehicles.

6.3.2 Scheme 2: Anonymous & privacy-preserving lightweight authentication for UAV-assisted IoAV (SLAP-IoAV).

Shariq M. Jamil et al.(2025) present a provably secure, lightweight authentication protocol designed for UAV-assisted Internet of Autonomous Vehicles that emphasises anonymity and resistance to physical capture attacks. The scheme achieves efficiency by relying on low-cost primitives (hashes, XOR, small ECC operations) and formally analyses security (e.g., unforgeability, anonymity) under standard models — making it well suited for resource-constrained drones and vehicular edge nodes. Use this paper to justify lightweight cryptographic choices in aerial/vehicular joint networks and to contrast formally-proved lightweight protocols against heavier, PKI-centric alternatives.

6.3.3 Scheme 3: PSLAP — provable, lightweight privacy-preserving authentication for autonomous vehicles (Computer Networks).

Shariq, M., Ahmed et al. (2025) in PSLAP designed a provably secure protocol that balances privacy (unlinkability/conditional anonymity) with computation/communication efficiency—using a combination of XOR, one-way hashes and ECC. Their formal proofs and performance results show that carefully chosen lightweight constructions can meet AV security requirements with lower overhead than classic PKI approaches. Cite PSLAP when arguing that formal, provable security is achievable without heavyweight crypto, and when benchmarking latency and computational cost in resource-limited vehicular endpoints.

6.3.4 Scheme 4: Provably secure and reliable privacy-preserving authentication for drone-to-drone communications.

Shariq M. Das et al. (2025) focuses on drone-to-drone (D2D) authentication inside Internet of Autonomous Things deployments, combining ECC and one-way hashes to offer provable security guarantees while also addressing reliability under lossy wireless links. It is useful when you need to discuss protocols tailored specifically for peer-to-peer aerial links (as opposed to vehicle-infrastructure links) and for highlighting design choices that improve robustness to packet loss and intermittent connectivity. Use it to motivate separate threat-models for drone networks and to justify the inclusion of reliability metrics (e.g., success rate under packet loss) in your evaluation.

6.3.5 Scheme 5: TS-PAID: Two-Stage PUF-based lightweight authentication for Internet of Drones.

Shehzad, A., Chaudhry et al.(2024/2025) TS-PAID uses Physically Unclonable Functions (PUFs) in a two-stage handshake to provide low-overhead, hardware-rooted authentication for drones. Because PUFs bind identity to physical hardware, TS-PAID improves resistance to cloning and certain physical attacks while keeping communication costs low — attractive for small UAVs with constrained energy and computation. Mention TS-PAID when discussing hardware-anchored authentication alternatives (PUF vs. purely cryptographic keys), and when considering resilience to device capture/cloning in your threat model.

6.3.6 Scheme 6: LightKey: Lightweight secure key-agreement for Internet of Vehicles.

Vasudev, H., Shariq et al. (2024) has designed a LightKey is a lightweight key-agreement and authentication protocol designed for vehicular networks; the authors evaluate its resistance to common attacks and measure computation/communication overhead suitable for vehicle-grade hardware. LightKey is a useful comparator when discussing key-establishment methods (mutual authentication + session key) optimized for vehicular latency and frequent handovers. Contrast its key-agreement design with the blockchain-assisted trust approaches (e.g., BTC2PA) to make clear the differences between ephemeral session security and long-term trust management

6.4 Application areas of the Privacy preserving schemes

Innovations in security for industrial IoT applications meet with IIoT applications and real-world deployments. To maximize efficiency and boost production, industrial settings are being used to test the possibilities and real-world applications of the Industrial Internet of Things. IIoT applications, where sensors, actuators, and other IoT devices gather and communicate data for real-time monitoring and control, span a wide range of industries, including manufacturing, logistics, energy, and healthcare. In the interim, it looks at current advancements in the security of these networked systems. (Mathur et al., 2023) It talks about cybersecurity measures that have advanced, like anomaly detection systems designed for IIoT contexts, authentication methods, and encryption. To protect sensitive information, stop illegal access, and ensure operational continuity in industrial settings, the study underlines the significance of implementing strong security measures. Collectively, these viewpoints highlight the changing environment where useful applications of IIoT technologies meet cybersecurity breakthroughs. Industries may enhance process efficiency, and reliability, and reduce the risk of cyber threats in their operating environments by incorporating secure and efficient IoT deployments with better security protocols.

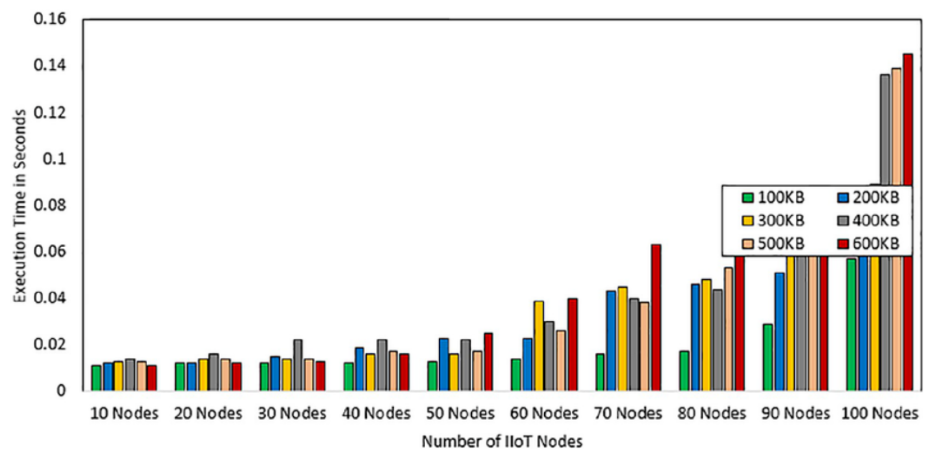

Figure 10: Industrial Internet of Things Nodes on Blockchain Network (Chhotaray et al., 2024)

Figure 10 illustrates how file size and the number of IIoT nodes affect block mining execution time in a blockchain network. It shows that as file sizes increase, so does the time required for block mining. Similarly, an increase in the number of IIoT nodes also extends execution times due to higher computational demands. These observations have several implications for blockchain network performance in IIoT applications. Larger files and more nodes can strain resources and reduce overall efficiency, necessitating optimization strategies. Factors like encryption methods, file compression techniques, and network conditions play critical roles in influencing block mining performance. Addressing these considerations is crucial for designing scalable and efficient blockchain solutions for IIoT environments, ensuring timely and reliable data processing while managing computational and network overhead effectively.

The convergence of IIoT offers transformative industrial applications, emphasizing security enhancements and privacy considerations crucial for operational integrity and confidentiality. (Chhotaray et al., 2024) Explored the transformative impact of the Industrial Internet of Things (IIoT) on modern manufacturing, particularly within the context of Industry 4.0. It introduces the technologies underpinning IIoT and provides a comprehensive overview of its key components and functionalities. The objectives include elucidating how IIoT facilitates enhanced connectivity, real-time data acquisition, remote monitoring, and analytics-driven decision-making in industrial environments. Highlight the primary benefits of IIoT in manufacturing, such as improved operational efficiency, predictive maintenance capabilities, reduced downtime, and optimized resource utilization. (Aliyu et al.,2023) Moreover, the chapter discusses the characteristics of IIoT systems that enable seamless integration of machines, sensors, and processes to create smart production units. It underscores the role of big data analytics in transforming traditional industrial methods into agile, data-driven processes that enhance productivity and competitiveness. Overall, the chapter serves to educate on the strategic advantages and technological advancements that IIoT brings to the manufacturing sector in the era of digital transformation. Meira et al., 2023) Determined a practical implementation of Industrial IoT (IIoT) using 5G technology and evaluated its effectiveness in enhancing manufacturing operations. Infrastructure-wise, the study focuses on deploying 5G IoT devices for real-time data collection from shop floor assets, leveraging the flexibility and performance of 5G networks (Rath et al., 2023).

7. Summary of security and privacy challenges in IIoT using ML and Blockchain solution

Around 150 papers are referred and the summary of the key research trends is as mentioned below.

Blockchain solutions introduce high computational and communication overheads (Capocasale et al., 2023; Mishra et al., 2023) and face scalability and interoperability issues (Kotey et al., 2023; Naef et al., 2024). Edge and fog security mechanisms remain constrained by resource limitations (Chalapathi et al., 2021; Sánchez-de la Rosa et al., 2023). Furthermore, AI-based intrusion detection models often lack explainability and trustworthiness (Arnold et al., 2023; Hasan et al., 2023). For instance, blockchain-assisted data trading and IIoT marketplaces have been proposed (Abbasi et al., 2023; González et al., 2023), yet scalability in industrial settings remains limited. Integrating IIoT with 5G, edge computing, and federated learning (Hu et al., 2024; Meira et al., 2023) could enable real-time and scalable security. Future work should also consider cross-industry applicability in healthcare (Abdullah et al., 2023; Rahman et al., 2023), manufacturing (Chhotaray et al., 2024; Hu et al., 2024), and energy domains (Li et al., 2023; Naef et al., 2024), along with policy and governance frameworks for compliance and trust (Naef et al., 2024; Pennekamp et al., 2024).

The current body of research on IIoT security and blockchain integration demonstrates a diverse distribution of focus areas and methodological approaches. The most extensively studied domain is blockchain security and privacy in IIoT (20%), where researchers primarily rely on simulations and proof-of-concept frameworks to validate security guarantees. A significant portion of work also addresses the integration of blockchain with edge and fog computing (14%), often through framework implementations and real-time performance evaluations, underscoring the importance of low-latency and resource-efficient solutions.

AI, ML, and data science in IIoT (17%) have emerged as a major research theme, with studies validating models using publicly available datasets and controlled IIoT testbeds. Similarly, blockchain for industrial applications (15%) is increasingly explored through case studies and pilot deployments, reflecting growing interest in applied, sector-specific solutions. Federated learning in IIoT (8%) is gaining momentum, with studies largely focusing on model training experiments and simulation-based validations to ensure privacy-preserving distributed intelligence.

Smaller but significant streams of research include smart contracts and automation in IIoT (6%), often examined through performance tests and prototype deployments, as well as testbeds and connectivity (6%), which emphasize real-world trials. Research on blockchain challenges and barriers (5%) remains largely survey-based, while data sharing and privacy in IIoT (5%) emphasizes privacy metric evaluations through simulations. Emerging areas such as IIoT standards and architecture (3%), blockchain and IoT convergence (3%), and emerging trends in IIoT (4%) are typically addressed in conceptual or theoretical studies, pointing toward opportunities for more experimental validation.

Overall, the distribution suggests that while foundational issues like security, privacy, and integration dominate the literature, practical deployments and testbed-driven evaluations are gradually increasing, highlighting a shift from conceptual models toward applied and real-world implementations.

Table 2: Summary Table of Experimental Work Done

Category	% Focus	Experimental Work Done
Blockchain Security and Privacy in IIoT	20%	Simulations, proof-of-concept frameworks
Integration of Blockchain with Edge/Fog	14%	Framework implementation, real-time tests
AI, ML, and Data Science in IIoT	17%	Dataset-based validation, IIoT testbeds
Blockchain for Industrial Applications	15%	Case studies, pilot deployments
Federated Learning in IIoT	8%	Model training experiments, simulations
Smart Contracts and Automation in IIoT	6%	Smart contract deployment, performance tests
Testbeds, Connectivity in IIoT	6%	Real-world testbeds, field trials
Blockchain Challenges and Barriers	5%	Survey studies, qualitative analysis
Data Sharing and Privacy in IIoT	5%	Simulations, privacy metric evaluations
Emerging Trends in IIoT	4%	Conceptual discussions, literature reviews
Blockchain and IoT Convergence	3%	Simulations, case studies
IIoT Standards and Architecture	3%	Theoretical models, design considerations

8. CONCLUSION:

This study examines recent advancements in security within Industrial Internet of Things (IIoT) applications. It explores strategies and technologies aimed at fortifying IIoT systems against emerging cyber threats, emphasizing the critical need for robust security measures due to the interconnected nature of industrial devices. Key topics include encryption techniques to secure data transmission, authentication protocols to verify device identities, and anomaly detection systems to detect and respond to suspicious activities. The review also discusses the integration of blockchain technology for enhancing data integrity and transparency in IIoT environments. Challenges such as scalability, interoperability, and compliance with industry standards are addressed, alongside promising developments in AI-driven security solutions and edge computing. Overall, the review underscores the evolving landscape of IIoT security, highlighting the importance of continuous innovation and strategic implementation to safeguard industrial operations against cybersecurity risks effectively.

Funding

This research received no funding.

Declaration of AI Technology usage

We declare that the following Artificial Intelligence (AI) technologies and AI-assisted tools were employed in the preparation of this article:

ChatGPT and DeepSeek: Assisted in summarization.

Grammarly: Used in grammar checking

Turnitin: Plagiarism checking

Declaration of conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acronyms and Abbreviations

IIoT – Industrial Internet of Things

IoT – Internet of Things

ML – Machine Learning

AI – Artificial Intelligence

DL – Deep Learning

IDS – Intrusion Detection System

CNN – Convolutional Neural Network

LSTM – Long Short-Term Memory

FL – Federated Learning

DDoS – Distributed Denial of Service

DoS – Denial of Service

SVM – Support Vector Machine

RF – Random Forest

NB – Naïve Bayes

DT – Decision Tree

KNN – K-Nearest Neighbor

GAN – Generative Adversarial Network

AUC – Area Under Curve

ROC – Receiver Operating Characteristic

PR-AUC – Precision-Recall Area Under Curve

FPR – False Positive Rate

FNR – False Negative Rate

HIDS – Host-based Intrusion Detection System

NIDS – Network-based Intrusion Detection System

P2P – Peer-to-Peer

ECC – Elliptic Curve Cryptography, PKI – Public Key Infrastructure

REFERENCES

1. Abbasi, M., Prieto, J., Shahraki, A., & Corchado, J. M. (2023). Industrial data monetization: A blockchain-based industrial IoT data trading system. Internet of Things, 24, 100959.
2. Abdullah, S., Arshad, J., Khan, M. M., Alazab, M., & Salah, K. (2023). PRISED tangle: A privacy-aware framework for smart healthcare data sharing using IOTA tangle. Complex & Intelligent Systems, 9(3), 3023-3041.
3. Adhikari, N., & Ramkumar, M. (2023). IoT and blockchain integration: Applications, opportunities, and challenges. Network, 3(1), 115-141.

4. Ahmed, S. F., Alam, M. S. B., Hoque, M., Lameesa, A., Afrin, S., Farah, T., Kabir, M., Shafiullah, G. M., & Muyeen, S. M. (2023). Industrial Internet of Things enabled technologies, challenges, and future directions. Computers and Electrical Engineering, 110, 108847.
5. Alanazi, R., & Aljuhani, A. (2023a). Anomaly detection for industrial Internet of Things cyberattacks. Computer Systems Science & Engineering, 44(3).
6. Alenezi, N., & Aljuhani, A. (2023b). Intelligent intrusion detection for industrial Internet of Things using clustering techniques. Computer Systems Science & Engineering, 46(3).
7. Alnajim, A. M., Habib, S., Islam, M., Thwin, S. M., & Alotaibi, F. (2023). A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in the Industrial Internet of Things. Technologies, 11(6), 161.
8. Alotaibi, B. (2023). A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. Sensors, 23(17), 7470.
9. Alshahrani, H., Khan, A., Rizwan, M., Reshan, M. S. A., Sulaiman, A., & Shaikh, A. (2023). Intrusion detection framework for industrial Internet of things using software-defined network. Sustainability, 15(11), 9001.
10. Alshathri, S., El-Sayed, A., El Shafai, W., & Hemdan, E. E. D. (2023a). An efficient intrusion detection framework for industrial Internet of Things security. Computer Systems Science & Engineering, 46(1), 819-834.
11. Alshudukhi, K. S., Khemakhem, M. A., Eassa, F. E., & Jambi, K. M. (2023). An interoperable blockchain security framework based on microservices and smart contract in IoT environment. Electronics, 12(3), 776.
12. Al-Zoubi, A., Saadeddin, T., & Dmour, M. (2023). An Ethereum private network for data management in blockchain of things ecosystem. International Journal of Online Biomedical Engineering, 19(1), 38-58.
13. Altunay, H. C., & Albayrak, Z. (2023). A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks. Engineering Science and Technology, an International Journal, 38, 101322.
14. Aouedi, O., & Piamrat, K. (2023). F-bids: Federated-blending based intrusion detection system. Pervasive and Mobile Computing, 89, 101750.
15. Arnold, L., Karnebogen, P., & Urbach, N. (2023). Challenges of organizations' adoption of industrial IoT platforms-results of a Delphi study. International Journal of Innovation and Technology Management, 20(06), 2350041.
16. Ashok, K., & Gopikrishnan, S. (2023). Statistical analysis of remote health monitoring based IoT security models & deployments from a pragmatic perspective. IEEE Access, 11, 2621-2651.
17. Asri, A. S., Boestamam, F. F., Zakaria, H. Z. B., Omar, M. A. A. R., Yahya, M. H. I. B. M., & Faisal, M. (2024). Enhancing IIoT security: AI-driven blockchain-based authentication scheme. International Journal of Computer Technology and Science, 1(3), 20-40.
18. Awotunde, J. B., Folorunso, S. O., Imoize, A. L., Odunuga, J. O., Lee, C. C., Li, C. T., & Do, D. T. (2023a). An ensemble tree-based model for intrusion detection in industrial Internet of things networks. Applied Sciences, 13(4), 2479.
19. Baalamurugan, K. M., P, P., Bacanin, N., Venkatachalam, K., Askar, S. S., & Abouhawwash, M. (2023). RETRACTED ARTICLE: Blockchain-enabled K-harmonic framework for industrial IoT-based systems. Scientific Reports, 13(1), 1004.
20. Benias, N., & Benardos, P. (2023, June). Cybersecurity challenges of blockchain and smart contracts technologies in IIoT. In International Conference on Flexible Automation and Intelligent Manufacturing (pp. 729-740). Cham: Springer Nature Switzerland.
21. Bhattacharya, S., & Pandey, M. (2023, March). Anomalies detection on contemporary industrial Internet of Things data for securing crucial devices. In Proceedings of Third International Conference on Advances in Computer Engineering and Communication Systems: ICACECS 2022 (pp. 11-20). Singapore: Springer Nature Singapore.
22. Bobde, Y., Narayanan, G., Jati, M., Raj, R. S. P., Cvitić, I., & Peraković, D. (2024). Enhancing industrial IoT network security through blockchain integration. Electronics, 13(4), 687.
23. Borgosz, L., & Dikicioglu, D. (2024). Industrial Internet of Things: What does it mean for the bioprocess industries? Biochemical Engineering Journal, 201, 109122.
24. Brandín, R., & Abrishami, S. (2024). IoT-BIM and blockchain integration for enhanced data traceability in offsite manufacturing. Automation in Construction, 159, 105266.
25. Cabrera-Gutiérrez, A. J., Castillo, E., Escobar-Molero, A., Cruz-Cozar, J., Morales, D. P., & Parrilla, L. (2023). Secure sensor prototype using hardware security modules and trusted execution environments in a blockchain application: wine logistic use case. Electronics, 12(13), 2987.
26. Capocasale, V., Gotta, D., & Perboli, G. (2023). Comparative analysis of permissioned blockchain frameworks for industrial applications. Blockchain: Research and Applications, 4(1), 100113.
27. Chalapathi, G. S. S., Chamola, V., Vaish, A., & Buyya, R. (2021). Industrial Internet of Things (IIoT) applications of edge and fog computing: A review and future directions. Fog/edge computing for security, privacy, and applications, 293-325.
28. Chhotaray, P., Behera, B. C., Moharana, B. R., Muduli, K., & Sephyrin, F. T. R. (2024). Enhancement of manufacturing sector performance with the application of industrial Internet of Things (IIoT). In Smart technologies for improved performance of manufacturing systems and services (pp. 1-19). CRC Press.
29. D'Angelo, G., Farsimadan, E., Ficco, M., Palmieri, F., & Robustelli, A. (2023). Privacy-preserving malware detection in Android-based IoT devices through federated Markov chains. Future Generation Computer Systems, 148, 93-105.
30. Demertzi, V., Demertzis, S., & Demertzis, K. (2023). An overview of privacy dimensions on the industrial Internet of Things (IIoT). Algorithms, 16(8), 378.

31. Divya, N. S., & Vatambeti, R. (2023). Detecting false data injection attacks in industrial Internet of Things using an optimized bidirectional gated recurrent unit-swarm optimization algorithm model. Acadlore Transactions on AI and Machine Learning, 2(2), 75-83.
32. Dwivedi, S. K., Roy, P., Karda, C., Agrawal, S., & Amin, R. (2021). Blockchain-based Internet of things and industrial IoT: a comprehensive survey. Security and Communication Networks, 2021(1), 7142048.
33. Falayi, A., Wang, Q., Liao, W., & Yu, W. (2023). Survey of distributed and decentralized IoT securities: approaches using deep learning and blockchain technology. Future Internet, 15(5), 178.
34. Fitzpatrick, P., & Thorpe, C. (2024, June). An investigation into the feasibility of using distributed digital ledger technology for digital forensics for industrial IoT. In European Conference on Cyber Warfare and Security (Vol. 23, No. 1, pp. 827-835).
35. Frank, E. (2024). Industrial Internet of Things (IIoT) security challenges: Exploring the trust deficit and security concerns in the context of IIoT deployments.
36. Gaba, S., Khan, H., Almalki, K. J., Jabbari, A., Budhiraja, I., Kumar, V., Singh, A., Singh, K. K., Askar, S. S., & Abouhawwash, M. (2023). Holochain: An agent-centric distributed hash table security in smart IoT applications. IEEE Access.
37. Gaber, T., Awotunde, J. B., Folorunso, S. O., Ajagbe, S. A., & Eldesouky, E. (2023b). Industrial Internet of Things intrusion detection method using machine learning and optimization techniques. Wireless Communications and Mobile Computing, 2023(1), 3939895.
38. Garba, A., Khoury, D., Balian, P., Haddad, S., Sayah, J., Chen, Z., Guan, Z., Hamdan, H., Charafeddine, J., & Al-Mutib, K. (2023). LightCERT4IoTs: Blockchain-based lightweight certificates authentication for IoT applications. IEEE Access, 11, 28370-28383.
39. Gangwani, P., Perez-Pons, A., Joshi, S., Upadhyay, H., & Lagos, L. (2023). Integration of data science and IoT with blockchain for Industry 4.0. In Blockchain and its applications in Industry 4.0 (pp. 139-177). Singapore: Springer Nature Singapore.
40. Golchha, R., Joshi, A., & Gupta, G. P. (2023). Voting-based ensemble learning approach for cyber attack detection in industrial Internet of Things. Procedia Computer Science, 218, 1752-1759.
41. Gopi, R., Sheeba, R., Anguraj, K., Chelladurai, T., Alshahrani, H. M., Nemri, N., & Lamoudan, T. (2023). Intelligent intrusion detection system for industrial Internet of Things environment. Computer Systems Science & Engineering, 44(2).
42. González, V., Sánchez, L., Lanza, J., Santana, J. R., Sotres, P., & García, A. E. (2023). On the use of blockchain to enable a highly scalable Internet of Things data marketplace. Internet of Things, 22, 100722.
43. Goyal, S. B., Rajawat, A. S., Shandilya, R., & Malik, V. (2023a). Cognitive adaptive systems for industrial internet of things using reinforcement algorithm. Electronics, 12(1), 217.
44. Goyal, S. B., Rajawat, A. S., Shandilya, R., & Malik, V. (2023b). Efficient IIoT framework for mitigating Ethereum attacks in industrial applications using supervised learning with quantum classifiers. In Applied data science and smart systems (pp. 544-551). CRC Press.
45. Gulia, P., Gill, N. S., Yahya, M., Gupta, P., Shukla, P. K., & Shukla, P. K. (2024). Exploring the potential of blockchain technology in an IoT-enabled environment: A review. IEEE Access, 12, 31197-31227.
46. Guha Roy, D. (2023). Blockedge: A privacy-aware secured edge computing framework using blockchain for industry 4.0. Sensors, 23(5), 2502.
47. Hasan, M. K., Sulaiman, R., Islam, S., & Rehman, A. U. (2023). An explainable ensemble deep learning approach for intrusion detection in industrial Internet of Things. IEEE Access.
48. Hu, Y., Jia, Q., Yao, Y., Lee, Y., Lee, M., Wang, C., Zhou, X., Xie, R., & Yu, F. R. (2024). Industrial Internet of Things intelligence empowering smart manufacturing: A literature review. IEEE Internet of Things Journal.
49. Issa, W., Moustafa, N., Turnbull, B., Sohrabi, N., & Tari, Z. (2023). Blockchain-based federated learning for securing internet of things: A comprehensive survey. ACM Computing Surveys, 55(9), 1-43.
50. Jonathan, & H Luz, A. (2024). Investigating the use of federated learning to enable collaborative AI model training while preserving data privacy in industrial IoT settings (No. 13279). EasyChair.
51. Karthik, S. A., Hemalatha, R., Aruna, R., Deivakani, M., Reddy, R. V. K., & Boopathi, S. (2023). Study on healthcare security system-integrated Internet of Things (IoT). In Perspectives and considerations on the evolution of smart systems (pp. 342-362). IGI Global.
52. Khan, A. A., Laghari, A. A., Li, P., Dootio, M. A., & Karim, S. (2023). The collaborative role of blockchain, artificial intelligence, and industrial Internet of Things in digitalization of small and medium-size enterprises. Scientific Reports, 13(1), 1656.
53. Khordadpour, P., & Ahmadi, S. (2024). Security and privacy enhancing in blockchain-based IoT environments via anonym auditing. arXiv preprint arXiv:2403.01356.
54. Kiran, A., Mathivanan, P., Mahdal, M., Sairam, K., Chauhan, D., & Talasila, V. (2023). Enhancing data security in IoT networks with blockchain-based management and adaptive clustering techniques. Mathematics, 11(9), 2073.
55. Kotey, S. D., Tchao, E. T., Ahmed, A. R., Agbemenu, A. S., Nunoo-Mensah, H., Sikora, A., Welte, D., & Keelson, E. (2023). Blockchain interoperability: The state of heterogenous blockchain-to-blockchain communication. IET Communications, 17(8), 891-914.

56. Kumar, R., Javeed, D., Aljuhani, A., Jolfaei, A., Kumar, P., & Islam, A. N. (2023). Blockchain-based authentication and explainable AI for securing consumer IoT applications. IEEE Transactions on Consumer Electronics.
57. Kumar, V., & Das, S. K. The convergence of blockchain and edge computing for smart contracts management in IIOT. Sarala Birla University, 84.
58. Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., & Kumar, N. (2023). DRLBTS: Deep reinforcement learning-aware blockchain-based healthcare system. Scientific Reports, 13(1), 4124.
59. Lazar, A. J. P., Soundararaj, S., Sonthi, V. K., Palanisamy, V. R., Subramaniyan, V., & Sengan, S. (2023). Gaussian differential privacy integrated machine learning model for industrial Internet of Things. SN Computer Science, 4(5), 454.
60. Li, F., Lin, J., & Han, H. (2023). FSL: Federated sequential learning-based cyberattack detection for industrial Internet of Things. Industrial Artificial Intelligence, 1(1), 4.
61. Li, L., Jin, D., Zhang, T., & Li, N. (2023). A secure, reliable and low-cost distributed storage scheme based on blockchain and IPFS for firefighting IoT data. IEEE Access.
62. Liu, H., & Chen, Y. (2023). Using blockchain technology in IoT manufacture environment for intelligence prediction. Soft Computing, 27(3), 1715-1729.
63. Luz, A., & Jonathan, H. (2024). Exploring the application of differential privacy techniques to protect sensitive data in industrial IoT environments (No. 13280). EasyChair.
64. Madhwal, Y., Yanovich, Y., Balachander, S., Poojaa, K. H., Saranya, R., & Subashini, B. (2023). Enhancing supply chain efficiency and security: A proof of concept for IoT device integration with blockchain. IEEE Access.
65. Mahmood, K., Shamshad, S., Saleem, M. A., Kharel, R., Das, A. K., Shetty, S., & Rodrigues, J. J. (2023). Blockchain and PUF-based secure key establishment protocol for cross-domain digital twins in industrial Internet of Things architecture. Journal of Advanced Research.
66. Masood, A. B., Hasan, A., Vassiliou, V., & Lestas, M. (2023). A blockchain-based data-driven fault-tolerant control system for smart factories in Industry 4.0. Computer Communications, 204, 158-171.
67. Mathur, S., Kalla, A., Gür, G., Bohra, M. K., & Liyanage, M. (2023). A survey on role of blockchain for IoT: Applications and technical aspects. Computer Networks, 227, 109726.
68. Meira, J., Matos, G., Perdigão, A., Cação, J., Resende, C., Moreira, W., Antunes, M., Quevedo, J., Moutinho, R., Oliveira, J., & Rendeiro, P. (2023). Industrial Internet of Things over 5G: A practical implementation. Sensors, 23(11), 5199.
69. Mishra, N., Islam, S. H., & Zeadally, S. (2023). A survey on security and cryptographic perspective of industrial Internet of things. Internet of Things, 101037.
70. Mishra, R. A., Kalla, A., Braeken, A., & Liyanage, M. (2023). Blockchain regulated verifiable and automatic key refreshment mechanism for IoT. IEEE Access, 11, 21758-21770.
71. Mu, X., & Antwi-Afari, M. F. (2024). The applications of Internet of Things (IoT) in industrial management: A science mapping review. International Journal of Production Research, 62(5), 1928-1952.
72. Naef, S., Wagner, S. M., & Saur, C. (2024). Blockchain and network governance: Learning from applications in the supply chain sector. Production Planning & Control, 35(9), 932-946.
73. Nagaty, K. A. (2023). IoT commercial and industrial applications and AI-powered IoT. In Frontiers of quality electronic design (QED) AI, IoT and hardware security (pp. 465-500). Cham: Springer International Publishing.
74. Onifade, M., Adebisi, J. A., & Zvarivadza, T. (2024). Recent advances in blockchain technology: Prospects, applications and constraints in the minerals industry. International Journal of Mining, Reclamation and Environment, 1-37.
75. Owen, J. (2024). Blockchain integration for enhanced trust in IIoT environments.
76. Pancari, S., Rashid, A., Zheng, J., Patel, S., Wang, Y., & Fu, J. (2023). A systematic comparison between the Ethereum and Hyperledger Fabric blockchain platforms for attribute-based access control in smart home IoT environments. Sensors, 23(16), 7046.
77. Pandey, A. K., Saxena, R., Awasthi, A., & Sunil, M. P. (2023). Privacy preserved data sharing using blockchain and support vector machine for industrial IoT applications. Measurement: Sensors, 29, 100891.
78. Parmar, M., & Shah, P. (2023). Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application. International Journal of Electrical & Computer Engineering (2088-8708), 13(4).
79. Patel, C., Bashir, A. K., AlZubi, A. A., & Jhaveri, R. (2023). EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element. Digital Communications and Networks, 9(2), 358-366.
80. Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. ICT Express, 9(4), 571-588.
81. Pennekamp, J., Wehrle, K., & Kerschbaum, F. (2024). Secure collaborations for the industrial Internet of Things. Shaker.
82. Peter, O., Pradhan, A., & Mbohwa, C. (2023). Industrial Internet of things (IIoT): Opportunities, challenges, and requirements in manufacturing businesses in emerging economies. Procedia Computer Science, 217, 856-865.
83. Pinto, G. P., Donta, P. K., Dustdar, S., & Prazeres, C. (2024). A systematic review on privacy-aware IoT personal data stores. Sensors, 24(7), 2197.
84. Qaddoori, S. L., & Ali, Q. I. (2023). An efficient security model for industrial Internet of Things (IIoT) system based on machine learning principles. Al-Rafidain Engineering Journal (AREJ), 28(1), 329-340.
85. Rahman, A., Hossain, M. S., Muhammad, G., Kundu, D., Debnath, T., Rahman, M., Khan, M. S. I., Tiwari, P., & Band, S. S. (2023). Federated learning-based AI approaches in smart healthcare: Concepts, taxonomies, challenges, and open issues. Cluster Computing, 26(4), 2271-2311.

86. Rahman, A., Kundu, D., Debnath, T., Rahman, M., Aishi, A. A., & Islam, J. (2024). Blockchain-based AI methods for managing industrial IoT: Recent developments, integration challenges and opportunities. arXiv preprint arXiv:2405.12550.
87. Rajagopal, S. M., Supriya, M., & Buyya, R. (2023). FedSDM: Federated learning based smart decision-making module for ECG data in IoT integrated Edge-Fog-Cloud computing environments. Internet of Things, 22, 100784.
88. Rajawat, A. S., Goyal, S. B., Chauhan, C., Bedi, P., Prasad, M., & Jan, T. (2023). Cognitive adaptive systems for industrial internet of things using reinforcement algorithm. Electronics, 12(1), 217.
89. Rao, P. M., & Deebak, B. D. (2023). Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing, 14(8), 10517-10553.
90. Rashid, M. M., Khan, S. U., Eusufzai, F., Redwan, M. A., Sabuj, S. R., & Elsharief, M. (2023). A federated learning-based approach for improving intrusion detection in industrial Internet of things networks. Network, 3(1), 158-179.
91. Rath, K. C., Kumar, R., & Mishra, B. K. (2023). Implementation of the Industrial Internet of Things (IIoT) is the tool of digital transformation technology. In Internet of Things (pp. 61-84). Apple Academic Press.
92. Rawat, G. S., Singh, K., Shariq, M., Das, A. K., Chaudhry, S. A., & Lorenz, P. (2025). BTC2PA: A Blockchain-Assisted Trust Computation With Conditional Privacy-Preserving Authentication for Connected Vehicles. IEEE Transactions on Intelligent Transportation Systems, 26(1), 1134–1148.
93. Razzaq, A., Altamimi, A. B., Alreshidi, A., Ghayyur, S. A. K., Khan, W., & Alsaffar, M. (2023). IoT data sharing platform in web 3.0 using blockchain technology. Electronics, 12(5), 1233.
94. Rehan, M., Javed, A. R., Kryvinska, N., Gadekallu, T. R., Srivastava, G., & Jalil, Z. (2023). Supply chain management using an industrial Internet of Things hyperledger fabric network. Human-centric Computing and Information Sciences, 13.
95. Rodríguez, E., Otero, B., & Canal, R. (2023). A survey of machine and deep learning methods for privacy protection in the Internet of things. Sensors, 23(3), 1252.
96. Ruiz-Villafranca, S., Carrillo-Mondéjar, J., Castelo Gómez, J. M., & Roldán-Gómez, J. (2023). MECInOT: A multi-access edge computing and industrial Internet of things emulator for the modelling and study of cybersecurity threats. The Journal of Supercomputing, 79(11), 11895-11933.
97. Sánchez-de la Rosa, M., Núñez-Gómez, C., Caminero, M. B., & Carrión, C. (2023). Exploring the use of blockchain in resource-constrained fog computing environments. Software: Practice and Experience, 53(4), 971-987.
98. Sanwar Hosen, A. S. M. S., Sharma, P., Puthal, D., Ra, I. H., & Cho, G. H. (2023, July). SECBlock-IIoT: A secure blockchain-enabled edge computing framework for industrial Internet of Things. In ASSS'23: Proceedings of the Third International Symposium on Advanced Security on Software and Systems. Association for Computing Machinery (ACM).
99. Sezgin, A., & Boyacı, A. (2023). AID4I: An intrusion detection framework for industrial Internet of Things using automated machine learning. Computers, Materials & Continua, 76(2).
100. Selvarajan, S., Srivastava, G., Khadidos, A. O., Khadidos, A. O., Baza, M., Alshehri, A., & Lin, J. C. W. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. Journal of Cloud Computing, 12(1), 38.
101. Sengupta, J., Ruj, S., & Bit, S. D. (2023). FairShare: Blockchain-enabled fair, accountable and secure data sharing for industrial IoT. IEEE Transactions on Network and Service Management, 20(3), 2929-2941.
102. Shah, H., Shah, D., Jadav, N. K., Gupta, R., Tanwar, S., Alfarraj, O., Tolba, A., Raboaca, M. S., & Marina, V. (2023). Deep learning-based malicious smart contract and intrusion detection system for IoT environment. Mathematics, 11(2), 418.
103. Sharma, R., & Villányi, B. (2023). A sustainable Ethereum merge-based Big-Data gathering and dissemination in IIoT system. Alexandria Engineering Journal, 69, 109-119.
104. Sharma, S. K., Misra, S. K., & Dwivedi, Y. K. (2023). A hierarchical framework of challenges for blockchain adoption in public services. Implications for decision-makers. Scandinavian Journal of Information Systems, 35(1), 3.
105. Shariq, M., Ahmed, I. T., Masud, M., Berini, A., & Jamil, N. (2025). Design of a provable secure lightweight privacy-preserving authentication protocol for autonomous vehicles in IoT systems. Computer Networks, 261, 111155.
106. Shariq, M., Das, A. K., Chaudhry, S. A., & others. (2025). Provably Secure and Reliable Privacy-Preserving Authentication Scheme for Drone-to-Drone Communications in Internet of Autonomous Things. IEEE/ACM (journal/transaction entry).
107. Shariq, M., Jamil, N., & Rawat, G. S. (2025). An anonymous and privacy-preserving lightweight authentication protocol for secure communication in UAV-assisted IoAV networks. Computer Communications, 239, 108192.
108. Shehzad, A., Chaudhry, S. A., & colleagues. (2025). TS-PAID: A Two-Stage PUF-based lightweight Authentication protocol for Internet of Drones. IEEE Access, 13.
109. Singh, J., Gimekar, A., & Venkatesan, S. (2023). An efficient lightweight authentication scheme for human-centered industrial Internet of Things. International Journal of Communication Systems, 36(12), e4189.
110. Singh, S., Rosak-Szyrocka, J., & Tamàndl, L. (2023). Development, service-oriented architecture, and security of blockchain technology for industry 4.0 IoT application. HighTech and Innovation Journal, 4(1), 134-156.
111. Singh, V. P., Biswas, S. S., Tanweer, S., & Alankar, B. (2024, January). Enhancing security in wireless communications through blockchain and smart contracts: A comprehensive study. In International Conference on Smart Computing and Communication (pp. 25-36). Singapore: Springer Nature Singapore.

112. Sivaselvan, N., Bhat, K. V., Rajarajan, M., & Das, A. K. (2023). A new scalable and secure access control scheme using blockchain technology for IoT. IEEE Transactions on Network and Service Management, 20(3), 2957-2974.
113. Soliman, S., Oudah, W., & Aljuhani, A. (2023c). Deep learning-based intrusion detection approach for securing industrial Internet of Things. Alexandria Engineering Journal, 81, 371-383.
114. Syamala, M., Komala, C. R., Pramila, P. V., Dash, S., Meenakshi, S., & Boopathi, S. (2023). Machine learning-integrated IoT-based smart home energy management system. In Handbook of research on deep learning techniques for cloud-based industrial IoT (pp. 219-235). IGI Global.
115. Tamilmani, S., Mohan, T., Jeyalakshmi, S., Shukla, G. P., Gehlot, A., & Shukla, S. K. (2023, January). Blockchain integrated with industrial IOT towards Industry 4.0. In 2023 International Conference on Artificial Intelligence and Smart Communication (AISC) (pp. 575-581). IEEE.
116. Thakur, G., Kumar, P., Jangirala, S., Das, A. K., & Park, Y. (2023). An effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environment. IEEE Access, 11, 26877-26892.
117. Tripathi, A. K., Akul Krishnan, K., & Pandey, A. C. (2023). A novel blockchain and Internet of things-based food traceability system for smart cities. Wireless Personal Communications, 129(3), 2157-2180.
118. Trivedi, C., Rao, U. P., Parmar, K., Bhattacharya, P., Tanwar, S., & Sharma, R. (2023). A transformative shift toward blockchain-based IoT environments: Consensus, smart contracts, and future directions. Security and Privacy, 6(5), e308.
119. Ucbas, Y., Eleyan, A., Hammoudeh, M., & Alohaly, M. (2023). Performance and scalability analysis of Ethereum and hyperledger fabric. IEEE Access.
120. Umran, S. M., Lu, S., Abduljabbar, Z. A., & Tang, X. (2023). A blockchain-based architecture for securing industrial IoTs data in electric smart grid. Computers, Materials & Continua, 74(3).
121. Usman, M., Sarfraz, M. S., Aftab, M. U., Habib, U., & Javed, S. (2024). A blockchain based scalable domain access control framework for industrial Internet of Things. IEEE Access.
122. Vasudev, H., Shariq, M., & Dwivedi, S. K. (2024). LightKey: Lightweight and secure key agreement protocol for effective communication in Internet of Vehicles. Proceedings of the 25th International Conference on Distributed Computing and Networking (ICDCN '24). DOI:10.1145/3631461.3631558.
123. Wahrstätter, A., Khan, S., & Svetinovic, D. (2024). OpenFL: A scalable and secure decentralized federated learning system on the Ethereum blockchain. Internet of Things, 26, 101174.
124. Wang, W., Huang, H., Yin, Z., Gadekallu, T. R., Alazab, M., & Su, C. (2023). Smart contract token-based privacy-preserving access control system for industrial Internet of Things. Digital Communications and Networks, 9(2), 337-346.
125. Wang, Y., Su, Z., Guo, S., Dai, M., Luan, T. H., & Liu, Y. (2023). A survey on digital twins: Architecture, enabling technologies, security and privacy, and future prospects. IEEE Internet of Things Journal, 10(17), 14965-14987.
126. Xie, Y., Li, Y., & Ma, Y. (2022). Data privacy security mechanism of industrial Internet of things based on blockchain. Applied Sciences, 12(14), 6859.
127. Yao, S., Lu, Y., Niu, K., Dai, J., Dong, C., & Zhang, P. (2024). Semantic information processing for interoperability in the Industrial Internet of Things. Fundamental Research, 4(1), 8-12.
128. Yazdinejad, A., Kazemi, M., Parizi, R. M., Dehghantanha, A., & Karimipour, H. (2023a). An ensemble deep learning model for cyber threat hunting in industrial internet of things. Digital Communications and Networks, 9(1), 101-110.
129. Yazdinejad, A., Zolfaghari, B., Dehghantanha, A., Karimipour, H., Srivastava, G., & Parizi, R. M. (2023b). Accurate threat hunting in industrial Internet of Things edge devices. Digital Communications and Networks, 9(5), 1123-1130.
130. Yeap, D. L. K., Tat, J. J. S., Xing, J. N. Y., Ting, J. S. Y., Chin, M. L. P., & Faisal, M. (2024). Securing industrial IoT: Blockchain-integrated solutions for enhanced privacy, authentication, and efficiency. International Journal of Computer Technology and Science, 1(3), 01-19.
131. Yin, J., Zhang, C., Xie, W., Liang, G., Zhang, L., & Gui, G. (2023). Anomaly traffic detection based on feature fluctuation for secure industrial Internet of things. Peer-to-Peer Networking and Applications, 16(4), 1680-1695.
132. Zhang, T., Xue, C., Wang, J., Yun, Z., Lin, N., & Han, S. (2024). A survey on industrial Internet of Things (IIoT) testbeds for connectivity research. arXiv preprint arXiv:2404.17485.
133. Zheng, P., Xu, X., & Wang, L. (2023). Editorial notes: Industrial Internet-of-Things (IIoT)-enabled digital servitisation. International Journal of Production Research, 61(12), 3844-3848.