Applied Data Science and Analysis
Vol.2025, **pp**. 19–82
DOI: https://doi.org/10.58496/ADSA/2025/004; ISSN: 3005-317X
https://mesopotamian.press/journals/index.php/ADSA

Review Article

Integration of Artificial Intelligence, Blockchain, and Quantum Cryptography for Securing the Industrial Internet of Things (IIoT): Recent Advancements and Future Trends

Guma Ali [1*], Aziku Samuel [1], Simon Peter Kabiito [1], Zaward Morish [1], Adebo Thomas [1], Wamusi Robert [1], Asiku Denis [1], Malik Sallam [2,3], Maad M. Mijwil [4,5,6], Jenan Ayad [7], Ayodeji Olalekan Salau[8,9], Klodian Dhoska [10,11]

[1] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda*
[2] *Department of Pathology, Microbiology and Forensic Medicine, School of Medicine, The University of Jordan, Amman, Jordan*
[3] *Department of Clinical Laboratories and Forensic Medicine, Jordan University Hospital, Amman, Jordan*
[4] *College of Administration and Economics, Al-Iraqia University, Baghdad, Iraq*
[5]*Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq*
[6]*Faculty of Engineering, Canadian Institute of Technology, Albania*
[7]*Electro-Mechanical Engineering Department, University of Technology, Baghdad, Iraq*
[8]*Department of Electrical/Electronic and Computer Engineering, Afe Babalola University, Ado-Ekiti, Nigeria*
[9]*Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India*
[10]*Mechanical Department, Polytechnic University of Tirana, Albania*
[11]*Association of Talent under Liberty in Technology (TULTECH), Tallinn, Estonia*

ARTICLE INFO

Article History

Received 12 Jan 2025
Revised: 10 Feb 2025
Accepted 02 Mar 2025
Published 27 Mar 2025

Keywords

Industrial Internet of Things

IIoT security threats and attacks

artificial intelligence

Blockchain technology

quantum cryptography

ABSTRACT

The swift growth of the Industrial Internet of Things (IIoT) offers tremendous potential to boost productivity, facilitate real-time decision-making, and automate procedures in various industries. However, as industries increasingly adopt IIoT, they face paramount data security, privacy, and system integrity challenges. Artificial intelligence (AI), Blockchain, and quantum cryptography are gaining significant attention as solutions to address these challenges. This paper comprehensively surveys advanced technologies and their potential applications for securing IIoT ecosystems. It reviews findings from 196 sources, including peer-reviewed journal articles, conference papers, books, book chapters, reports, and websites published between 2021 and 2025. The survey draws insights from leading platforms like Springer Nature, ACM Digital Library, Frontiers, Wiley Online Library, Taylor & Francis, IGI Global, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, and Google Scholar. This paper explores AI-driven approaches to anomaly detection, predictive maintenance, and adaptive security mechanisms, demonstrating how machine learning (ML) and deep learning (DL) can identify and mitigate threats instantly. It also examines Blockchain technology, emphasizing its decentralized nature, immutability, and ability to secure data sharing and authentication within IIoT networks. The paper discusses quantum cryptography, which utilizes quantum mechanics for theoretically unbreakable encryption, ensuring secure communications in highly sensitive industrial environments. The integration of these technologies is analyzed to create a multi-layered defense against cyber threats, highlighting challenges in scalability, interoperability, and computational overhead. Finally, the paper reviews the current research, limitations and challenges, and future directions for securing IIoT with these advanced technologies. This survey offers valuable insights to researchers, engineers, and industry practitioners working to secure the expanding IIoT infrastructure.

[*] *Corresponding author. Email: a.guma@muni.ac.ug*

1. INTRODUCTION

The world is rapidly transforming into a digital environment where the Internet of Things (IoT) connects countless devices through sensing, communication, networking, and information-processing technologies [1-3]. In the industrial sector, this evolution has led to the rise of the IIoT, driving significant architectural changes in industrial automation and control systems (IACS) [4][5]. The integration of operational technology (OT) and information technology (IT) lies at the heart of this industrial transformation. IT, which focuses on data and software, now impacts the factory floor by analyzing massive data streams and coordinating production operations. Data and communication are used by OT, which oversees physical systems and controls protocols, to improve workflows and boost productivity. This convergence produces a dynamic ecosystem where factories make predictions, machines learn, and production becomes more flexible [6]. The IIoT connects industrial devices like sensors, actuators, processors, network equipment, robots, radio frequency identification tags, other physical objects, and industrial machines, such as industrial storage tanks, centrifuges, industrial mixers, electrical generators, air compressors, material handling equipment, and computer numerical control to the Internet using advanced information and communication technologies [7-11]. This network enables collecting, analyzing, monitoring, and exchanging real-time data from industrial operations to enhance troubleshooting, facilitate timely interventions through actuation and maintenance, improve decision-making, and optimize production and manufacturing processes. IIoT transforms daily industrial operations by enabling real-time machine-to-machine interactions and advanced data analytics. By analyzing sensor data, companies can gain deeper insights into their processes, improve the efficiency and reliability of production lines, unlock new revenue streams, and improve inventory management, equipment maintenance, and energy usage [7][11-13]. By promoting resource efficiency and eco-friendly technologies, this advancement aligns with the United Nations' 2030 agenda for building sustainable infrastructure and industries [14]. Advancements in wireless sensor networks (WSN), IoT, 5G and 6G technologies, AI, machine-to-machine communication (M2M), intelligent robots, intelligent machines, edge computing, fog computing, cloud computing, cyber-physical systems, augmented and virtual reality, Blockchain, big data analytics, and cybersecurity solutions are transforming industries by enabling IIoT to continuously gather data from sensors and intelligent units, securely transmit it to industrial cloud centers, and seamlessly adjust critical parameters through a closed-loop system [15-18].

The global number of IoT devices will nearly double from 15.9 billion in 2023 to over 32.1 billion by 2030. By 2033, China will lead in consumer IoT devices, reaching approximately 8 billion [19]. Kaur [20] reported that IIoT connections will surge to 36.8 billion by 2025. The global IIoT market is set for substantial revenue growth, projected to reach US$275.70 billion in 2025 and expand at a strong annual growth rate (CAGR 2025-2029) of 13.34%, reaching US$454.90 billion by 2029. The United States will drive the most revenue in this market, with an estimated US$99.75 billion by 2025. The IIoT industry is growing due to technological developments and the increasing accessibility of reasonably priced processors and sensors that offer real-time data access. This market includes revenues from components and services that enable connectivity and intelligence, such as hardware (sensors, chips, and IoT-specific components), platforms (IoT platforms and security software), connectivity solutions (cellular, LoRa, SigFox), and services (equipment and system integration and maintenance). The rise of smart cities further accelerates market growth as they use IIoT to enhance efficiency, sustainability, and quality of life through interconnected systems and real-time analytics.

The IIoT is transforming various industries, including manufacturing, healthcare, autonomous driving, home appliances, energy management, utilities, transportation and logistics, smart cities, agriculture, construction, mining, and oil and gas. It reshapes daily life and industrial structures by enabling smart factories, connected supply chains, remote asset management, predictive maintenance, and energy management systems [17][21]. Industrial control systems (ICSs) are crucial in monitoring and controlling industrial operations. It integrates hardware and software to manage essential technologies like supervisory control and data acquisition (SCADA), programmable logic controllers (PLCs), and human-machine interfaces (HMIs) [22][23]. The IIoT transformation relies heavily on the Message Queuing Telemetry Transport (MQTT) protocol, a lightweight, publish-subscribe communication standard for real-time and low-bandwidth scenarios. The protocol enables seamless communication between IIoT devices, including smart sensors, PLCs, and HMIs, forming the backbone of modern industrial systems. Several companies implementing the IIoT in their operational frameworks include (1) 247TailorSteel, a small and medium-sized enterprise that utilizes IIoT in its fully automated factory with proprietary software, SOPHIA, optimizing production, logistics, and online orders; and (2) Siemens embraces IIoT through its MindSphere platform, offering machine connectivity and apps for manufacturing customers. Siemens partnered with Amazon and Microsoft to strengthen its IIoT position and encourages third-party development, exemplified by its acquisition of Mendix, advancing the IIoT ecosystem [24].

The IIoT has transformed the industrial sector by creating intelligent, interconnected systems that enhance operational efficiency, optimize resource management, and minimize downtime. It strengthens public safety and productivity, enables data-driven decision-making, and improves manufacturing operations and quality assurance. IIoT also reduces costs, enhances supply chain efficiency in logistics, and supports predictive maintenance, tracking assets, and process automation. Additionally, it facilitates remote monitoring and control of industrial processes, enhances product quality, and improves worker safety and customer experience. Furthermore, IIoT ensures effective compliance enforcement and helps regulate environmental issues [17][18][25-30].

However, implementing the IIoT faces critical security threats and attacks. These include ransomware and malware, social engineering and phishing attacks, authorization and authentication attacks, privacy violations, and data breaches. It is susceptible to eavesdropping, cross-site scripting, man-in-the-middle (MitM) attacks, spoofing, advanced persistent threats (APT), botnet attacks, buffer overflows, denial-of-service (DoS) and distributed DoS (DDoS) attacks, insider threats, phony node injections, data interception, and tampering. Malicious code injections, node capture attacks, reconnaissance attacks, replay attacks, routing information attacks, side-channel attacks, signature wrapping, sleep deprivation, sniffing, SQL injections, and jamming attacks are further issues. The integrity and operation of IIoT systems are threatened by supply chain, Sybil, wormhole attacks, backdoors, traffic analysis, and unauthorized access and control attacks, making IIoT devices and networks more vulnerable [21][30–39]. Device complexity, heterogeneity, and poor interoperability are issues that the IIoT faces in addition to security problems [40][41].

An additional complicating factor is the growing interest from malicious individuals. Numerous industrial IoT systems have been the target of cybercriminals, such as the 2015 Ukrainian power grid attack that compromised SCADA systems and cut off electricity to 230,000 consumers. In 2018, a Taiwanese chip manufacturer suffered a US$170 million loss due to an IIoT network attack. Bombardier experienced data theft after exploiting a vulnerability in a third-party file-transfer app [24]. The 2017 Triton attack on Middle Eastern petrochemical facilities targeted safety systems with malware aimed at causing catastrophic damage [24]. Attackers exploit vulnerable objects in IIoT devices to take control and launch malicious activities. For example, the Mirai botnet was created by targeting firmware vulnerabilities and used for large-scale DDoS attacks. Insecure network protocols like Modbus can allow unauthorized access, leading to severe consequences. These security threats and challenges on vital industrial control systems have severe consequences, such as data breaches that lead to data loss or manipulation, financial losses, decreased customer trust, service disruption, and damaged reputations. These risks also make it challenging to ensure the reliability and timeliness of data for decision analysis [4][26][42][43]. Industrial environments often face varying security needs and limited resources, making protection more difficult. As of August 2023, the China National Vulnerability Database (CVND) reported 3141 vulnerabilities in industrial control systems, including 1443 high-risk, 1518 medium-risk, and 180 low-risk vulnerabilities, highlighting severe security issues in IIoT [44]. Without effective mitigation strategies, IIoT enterprises could face up to US$90 trillion in losses by 2030 [45]. These statistics emphasize the critical need for improved cybersecurity in IIoT networks.

Traditional security measures often fail to tackle emerging security threats, attacks, and challenges [46], requiring innovative solutions to protect industrial infrastructure. Integrating AI, Blockchain, and quantum cryptography will enhance IIoT security by strengthening privacy, preventing cyber threats, and improving operational efficiency. AI detects and mitigates cyberattacks, analyzes vast data streams to identify anomalies, and ensures system integrity by classifying APTs, botnet attacks, and false data injection attempts. It enhances malware detection, network traffic analysis, spam detection, vulnerability management, and behavioral analysis while automating security responses to reduce risks and improve industrial network resilience [47-52]. Blockchain ensures data integrity, prevents unauthorized access, and enables secure transactions through tamper-proof, decentralized systems. It supports secure identity management, encrypted communication, smart contracts, zero-trust networks, and immutable audit trails, facilitating transparent threat intelligence and real-time detection [48][53-55]. Quantum cryptography further fortifies IIoT security by leveraging quantum key distribution (QKD) for ultra-secure communication, preventing unauthorized access, and detecting eavesdropping and MitM attacks. It strengthens authentication, ensures quantum-safe key distribution, and protects IIoT systems from DoS attacks, enhancing cybersecurity and privacy [56-64].

Leveraging AI, Blockchain, and quantum cryptography for securing IIoT remains largely unexplored, as most research focuses on these technologies in isolation. This survey aims to fill that gap by analyzing their combined applications, limitations and challenges, and future potential in IIoT security. By exploring AI-driven threat detection, Blockchain-enabled trust mechanisms, and quantum-secure encryption, this study presents a unified framework to strengthen industrial cybersecurity. A holistic approach that leverages the synergy of these technologies can significantly enhance the security and resilience of IIoT systems. The study explores innovative security solutions that adapt to evolving cyber threats by bridging research gaps and tackling implementation challenges. It identifies key strategies to enhance cybersecurity resilience. Establishing a robust, resilient, and future-proof IIoT security framework will ensure that industrial environments can withstand increasingly sophisticated cyber threats.

The contribution of this comprehensive survey includes:

- Describe the state-of-the-art, i.e., the introduction, components, enabling technologies, architecture, and IIoT applications).
- Explore the cyber threats and attacks in IIoT.
- Examine the current security technologies for securing IIoT systems.

- Explain the roles of AI, Blockchain, and quantum cryptography in securing IIoT.
- State the synergistic integration of AI, Blockchain, and quantum cryptography for securing IIoT.
- Explain the challenges and limitations encountered while integrating AI, Blockchain, and quantum cryptography in securing IIoT.
- Present the future research directions and recommendations for enhancing IIoT security.

The survey is structured into several sections: Section 2 details the materials and methods used, while Section 3 reviews the state-of-the-art. Section 4 presents the cyber threats and attacks in IIoT, followed by Section 5, which examines cybersecurity in IIoT. Section 6 explores how AI, Blockchain, and quantum cryptography contribute to IIoT security, and Section 7 explains the synergistic integration of AI, Blockchain, and quantum cryptography for securing IIoT. Section 8 describes the challenges and limitations encountered while implementing these technologies, while Section 9 outlines future research directions and recommendations. Finally, Section 10 concludes the study.

2. MATERIALS AND METHODS

This survey employs a comprehensive review methodology to analyze how AI, Blockchain, and quantum cryptography enhance IIoT security. The process involves four key phases: literature selection, classification, analysis, and synthesis. Researchers systematically collected relevant literature from journal articles, conference proceedings, books, book chapters, reports, and websites, using targeted keywords to search multiple scientific databases and digital libraries, including Springer Nature, ACM Digital Library, Frontiers, Wiley Online Library, Taylor & Francis, IGI Global, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, and Google Scholar. By focusing on studies published between 2021 and 2025, the review captures the latest advancements in IIoT security, addressing threats and attacks. Additionally, it explores how AI, Blockchain, and quantum cryptography contribute to securing the IIoT. The researchers refined and broadened their search results by using Boolean operators such as AND and OR. They combined search strings like “artificial intelligence” OR “machine learning” OR “deep learning” AND “Blockchain” AND “quantum cryptography” AND “Industrial Internet of Things” OR “IIoT” AND “security” OR “cybersecurity.” Moreover, they manually reviewed the bibliographies of selected papers to identify other relevant references.

The researchers defined explicit inclusion and exclusion criteria to select relevant studies for the survey. They included only English-language research papers focusing on AI, Blockchain, and quantum cryptography in IIoT security, particularly those discussing their application in industrial environments. Their selection prioritized peer-reviewed journal articles, conference papers, review articles, high-quality technical reports, and books or book chapters specifically addressing these technologies. They also favored research presenting empirical results, methodologies, or frameworks relevant to IIoT security, with a preference for studies published between 2021 and 2025. Conversely, they excluded non-English papers unless a translated version was available, studies on AI, Blockchain, or quantum cryptography that lacked an IIoT focus, and research covering IoT without distinguishing industrial requirements. They also ruled out non-peer-reviewed sources, studies without rigorous scientific methodologies, opinion-based articles lacking empirical support, and popular media or blog posts unless cited by credible sources for unique insights. Furthermore, they excluded studies that failed to provide practical insights, solutions, or methodologies for securing IIoT systems and research published before January 2021, as it may be outdated or address obsolete technology.

Nine researchers independently gathered relevant materials from selected databases using predefined key details, including the title, authors, publication year, objectives, research questions, study design, analysis methods, results, and conclusions. They also extracted data related to IIoT, focusing on security threats and attacks and the role of AI, Blockchain, and quantum cryptography in enhancing IIoT security. To ensure consistency and accuracy, they followed a structured data extraction approach. Initially, the researchers identified over 1,130 publications through academic search engines and databases. After removing duplicates and screening abstracts, they narrowed the dataset to 926 publications. Further eligibility assessments reduced this number to 573; 196 publications met the inclusion criteria. These publications came from various sources, including five from Springer Nature, one from ACM Digital Library, two from Frontiers, seven from Wiley Online Library, eight from Taylor & Francis, two from IGI Global, ten from Springer, nineteen from ScienceDirect, thirty-five from MDPI, fifty-six from IEEE Xplore Digital Library, and fifty-one from Google Scholar. The researchers carefully evaluated, categorized, and assessed these publications to ensure their relevance to the study objectives. Fig. 1 displays the distribution of selected research publications by paper type.

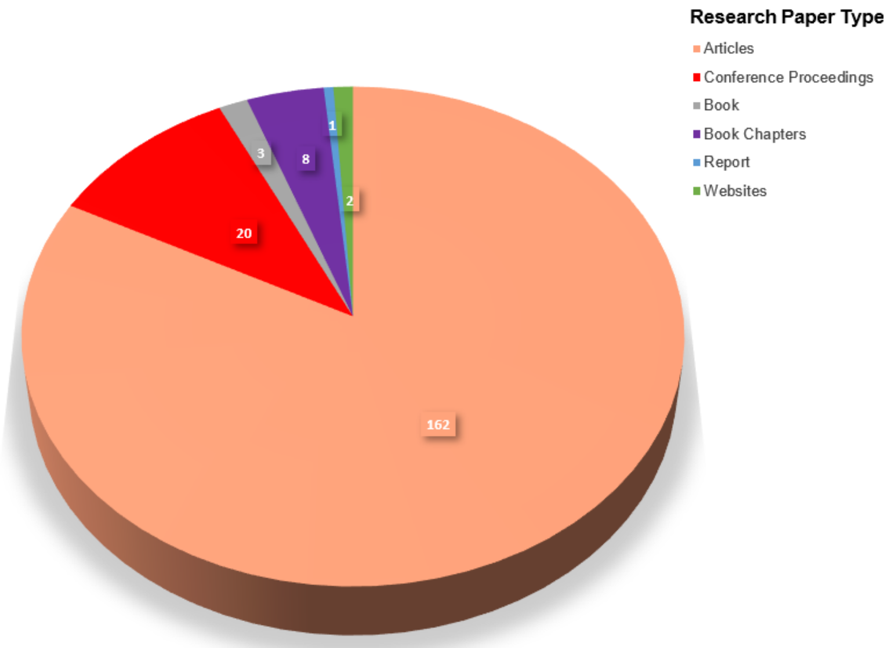

Fig. 1. Displays the distribution of selected research publications by paper type.

Fig. 2 displays the distribution of selected publications across various digital libraries.

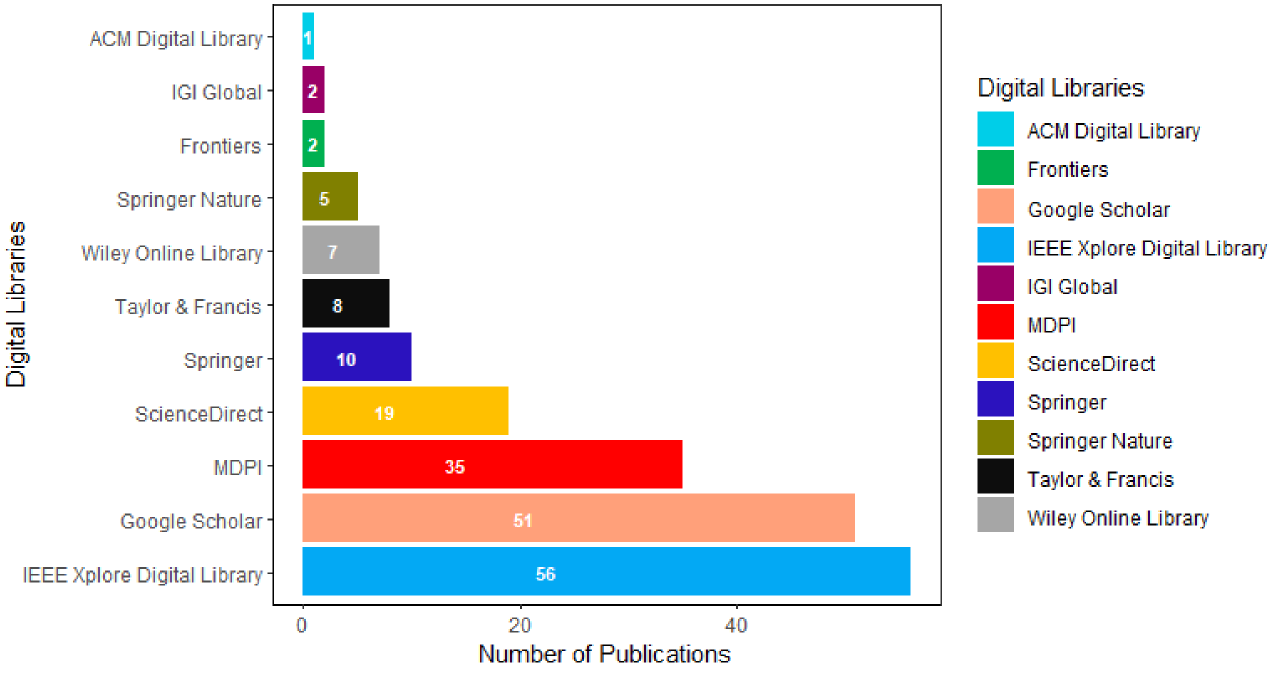

Fig. 2. Shows the distribution of selected publications across various digital libraries.

Fig. 3 summarizes how selected papers are distributed across digital libraries according to paper type.

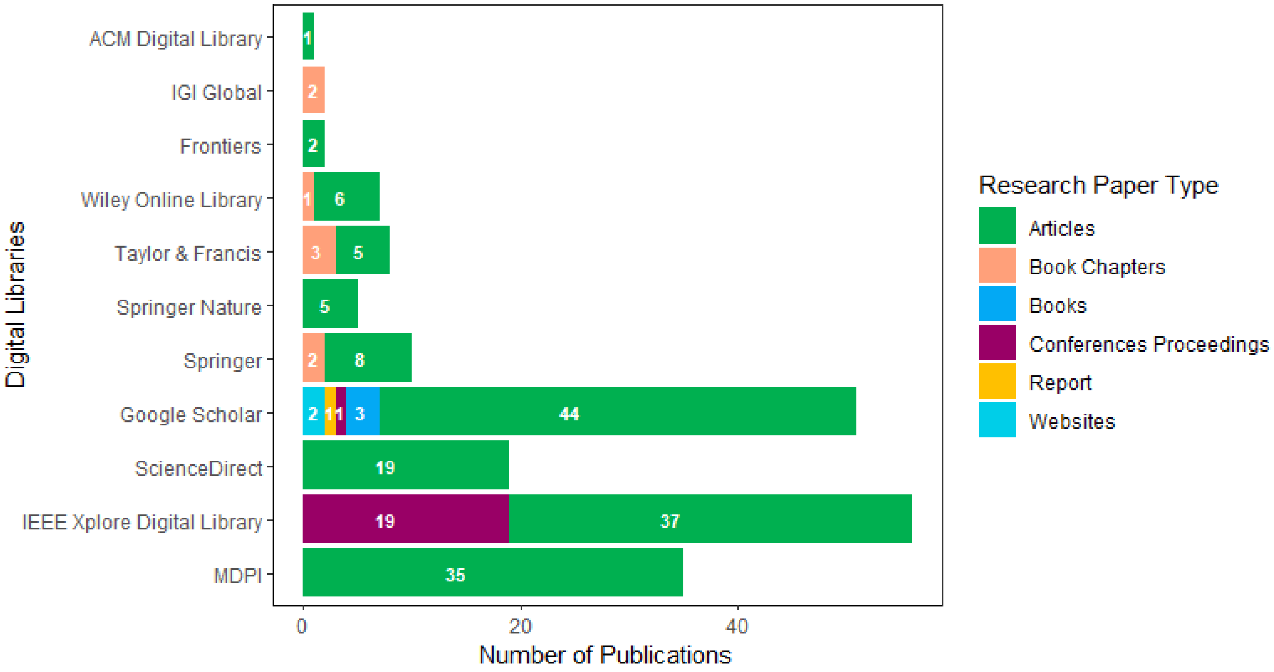

Fig. 3. Summarizes how selected papers are distributed across digital libraries according to paper type.

Fig. 4 displays the distribution of selected papers across digital libraries, organized by publication year.

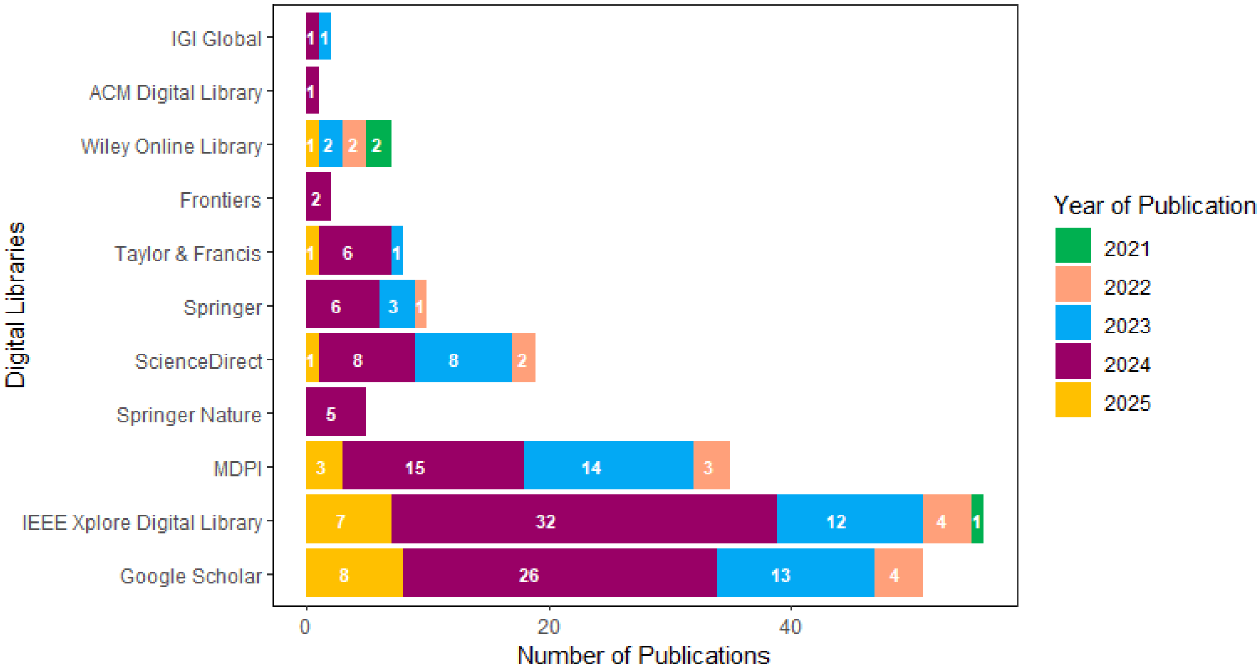

Fig. 4. Displays the distribution of selected papers across digital libraries, organized by publication year.

The research team selected papers using a multi-step procedure that ensured their reliability, methodological rigor, and relevance. Strict selection criteria were used, emphasizing validity, reliability, coherence, timeliness, citation effect, and peer-review status. They took confounding variables and possible bias into account. They recorded all sources, created a reference database, and eliminated duplicates using a reference management tool after querying several databases. The group then performed a systematic screening procedure, examining abstracts, titles, and keywords before doing full-text evaluations. They found and assembled a final collection of excellent studies using this exacting methodology for additional examination.

The researchers used qualitative synthesis and theme analysis techniques to compile and examine their gathered material. They looked at the particular IIoT security issues each study addressed and grouped studies according to whether they focused on AI, Blockchain, or quantum cryptography. They examined implementation frameworks, synergy possibilities, and integration methodologies for studies examining the integration of numerous technologies. They used comparative analysis approaches to find emergent trends, contrasts, and common themes. They meticulously evaluated the reliability and impact of each study, interviewed subject-matter experts, and compared findings with previous research to guarantee the validity of their findings. Using a grading system, they assessed each study's methodological soundness, dependability, and overall contribution to IIoT security. Ethical approval was unnecessary since the study was based on published research; however, the team carefully listed all their sources to uphold academic integrity.

Despite its meticulous approach, the study admits several shortcomings. While the dependence on particular databases may have missed pertinent work from other sources, excluding non-English studies may have missed necessary research. The study might have overlooked critical regional developments in IIoT security because many databases have a Western bias. The study also recognizes the risk of publication bias since research papers with positive results are more likely to appear in academic literature. Furthermore, the absence of quantitative analysis or empirical data may weaken the review's robustness, as qualitative assessments alone may not fully substantiate key claims. Lastly, the rapidly evolving nature of AI, Blockchain, and quantum cryptography means that some findings may become outdated as new advancements emerge.

3. STATE-OF-THE-ART

3.1. Introduction to IIoT

The industrial IoT connects industrial systems and processes to the Internet by integrating devices, sensors, machines, and software, enabling real-time data collection, sharing, and analysis. This technology enhances manufacturing, energy, agriculture, and logistics by improving decision-making, automating operations, and increasing efficiency [65]. By embedding sensors and leveraging communication technologies like Wi-Fi, Bluetooth, and cellular networks, IIoT ensures continuous monitoring of performance, environmental conditions, and operational status [66]. These devices transmit data to cloud platforms or local edge devices, allowing IIoT systems to detect irregularities, predict future conditions, and respond autonomously [67]. As a result, industries reduce downtime, enhance safety, optimize resource management, and strengthen operational resilience, leading to significant cost savings [68]. Fig. 5 illustrates a futuristic industrial setting where interconnected machinery and advanced data visualization highlight the power of IIoT in fostering connectivity and technological progress.

Fig. 5. Illustrates a futuristic industrial setting with interconnected machinery and advanced data visualization, emphasizing connectivity and innovation [69].

3.2. Components of IIoT

Table 1 briefly describes the main components of IIoT systems.

TABLE I. BRIEF DESCRIPTIONS OF THE MAIN COMPONENTS OF IIOT SYSTEMS.

S/No	Component	Brief Description	References
1	Sensors and actuators	Sensors serve as the IIoT's eyes and ears, continuously collecting vital operational and environmental data such as motion, light intensity, temperature, pressure, and humidity. Industries may boost automation, monitor, and build digital twins to make processes more predictable by incorporating cameras and sensors into conventional machinery. These devices are essential for smart manufacturing, monitoring robotics, machine status, and ambient conditions to facilitate data-driven decision-making. Sensors that collect and process data enable motion-activated security systems, vibration sensors for predictive maintenance, optical sensors for quality control, real-time monitoring, and the correct storage of heat-sensitive products. Through the collection, processing, and analysis of data, sensors in IIoT ecosystems foster intelligence and efficiency. Actuators work directly with the physical environment and sensors to execute control commands. In reaction to sensor data, they automate tasks such as adjusting valves, turning on lights, turning on pumps, and adjusting machine speeds. For instance, an actuator can automatically close the valve to limit more leaks if a system detects a liquid leak from a tank. By putting corrective or preventative measures into place, actuators help to maintain optimal operating conditions and increase industrial efficiency.	[17][28][70][71]
2	Connectivity and communication protocols	Reliable wired and wireless communication networks are necessary for IIoT to transmit data from far locations. Using protocols like Ethernet, Modbus, PROFINET, and CAN bus, wired systems offer robust, quick, and low-latency connectivity, ideal for industrial applications. Wireless technologies such as Wi-Fi, Bluetooth, Zigbee, LoRaWAN, LoRa, NB-IoT, and Sigfox provide more flexibility and straightforward installation. Industrial protocols such as OPC UA, MQTT, Modbus (RTU/TCP), PROFINET, EtherNet/IP, HART, BACnet, may Bus, DNP3, and DDS facilitate the easy exchange of data between devices, sensors, and machines. These standards are essential for mobile and flexible deployments because they allow long-distance communication without physical connections and enable real-time monitoring, automation, and control.	[28][71]
3	Edge devices and edge computing	Edge devices link sensors, actuators, and the cloud by processing data locally before transferring it to a central system. By reducing latency and keeping critical data near its source, edge computing enables faster response times and reduces the burden on cloud infrastructure. Industrial gateways facilitate seamless data exchange in manufacturing by connecting sensors, PLCs, machines, and robotics through open data interfaces. These gateways collect, translate, and transmit data between legacy equipment and modern IIoT networks, ensuring interoperability and efficient decision-making. PLCs empower industrial employees to monitor and control tools and processes. HMIs, such as tablets, integrated screens, or computer monitors, help users manage operations, detect issues, and understand industrial workflows.	[24][70][72]
4	Cloud and data storage	Cloud computing is vital in IIoT by offering scalable storage, computing power, and analytics. It enables businesses to store and process the massive data generated by IIoT devices while providing access to insights and control from anywhere through cloud services for data storage, analytics, and remote access. Edge computing complements this by processing data near its source, minimizing latency, and enabling real-time analysis. This approach is essential for IIoT, ensuring faster decision-making and enhancing operational efficiency.	[73][74]
5	Data analytics and artificial intelligence	IIoT devices generate large volumes of data that need real-time processing to provide predictive insights and enable automation. By collecting this data, IIoT helps in making informed decisions. Machine learning and data analytics algorithms examine the data to produce actionable insights, spot irregularities, and predict maintenance requirements, increasing productivity and efficiency.	[75]
6	Cybersecurity and data protection	Security is crucial in the IoT, as it safeguards sensitive data and defends against malicious attacks that could compromise information integrity, confidentiality, and availability. In the IIoT, security measures focus on protecting devices and managing data transmission and storage. As industrial systems become more interconnected, ensuring robust cybersecurity is essential. Firewalls, encryption, and access controls protect IIoT networks from potential threats.	[28]
7	Industrial Control Systems and SCADA	SCADA systems manage and monitor industrial processes by communicating with field controllers, collecting real-time data, and displaying it through an HMI to help operators track and control operations effectively. Manufacturing execution systems improve productivity by capturing real-time data to streamline production cycles, manage work orders, schedule tasks, and monitor downtime, reducing reliance on paper. ERP systems centralize data to oversee ordering, finances, human resources, and operations, enabling seamless departmental connectivity, enhancing customer service, and providing employees with real-time information to boost productivity. Integrating IIoT with ICS further enhances automation and operational efficiency.	[24]

8	Human-machine interfaces (HMIs) and digital twins	HMIs give factory workers an easy-to-use interface for monitoring tools, controlling operations, and interacting with industrial systems. Tablets, integrated screens, and computer monitors are interfaces essential for managing operations and comprehending industrial activities. HMI simplifies the administration of intricate industrial processes by interacting with IIoT systems to display real-time data and alarms while empowering operators to control equipment. Digital twins improve performance, enable simulations, and improve real-time monitoring. For example, they enhance augmented reality HMIs for maintenance technicians, forecast maintenance requirements, and increase wind turbine efficiency.	[24][76]
9	Robotics and automation	IIoT makes the deployment of autonomous systems that improve accuracy and efficiency possible. By combining automation, robotics, and IoT technology, industries significantly increase productivity, accuracy, and safety. Robots gather and evaluate data instantly and then make decisions on their own to maximize efficiency. Autonomous mobile robots (AMRs) optimize warehouse logistics, industrial robots do repetitive tasks like welding, assembly, and material handling, and collaborative robots (cobots) work with humans in factories. This combination of automation, IIoT, and robotics promotes creative manufacturing techniques, reduces downtime, and increases scalability.	[24][28]
10	Wearable and industrial devices	Wearable devices like smartwatches, fitness bands, and smart glasses have gained significant popularity in the IIoT space by tracking physical activities, health parameters, location, and more. These devices provide users with valuable features to monitor and improve their well-being, such as real-time heartbeat monitoring that alerts individuals to potential abnormalities. In industrial environments, devices like production monitoring sensors, computer numerical control machines, and autonomous industrial vehicles are crucial in optimizing production processes, boosting efficiency, and enhancing workplace safety. For instance, real-time data collected by monitoring sensors helps identify inefficiencies and improve overall plant performance.	[28]
11	Supply chain and asset tracking	IIoT is vital in logistics, supply chain management, and asset tracking through technologies like RFID and GPS. These tools enable real-time asset tracking, fleet management, and warehouse inventory management. Additionally, Blockchain enhances IIoT by securing transaction records and ensuring supply chain transparency. For instance, smart warehouses leverage IIoT sensors to automate and streamline inventory tracking processes.	[24][28]
12	Industrial IoT platform and warehouse management system	The industrial IoT system includes software that analyzes data gathered and transmitted from the field. This application can make decisions and transmit commands to edge controls. A warehouse management system oversees all operations, provides visibility, and controls vital procedures like picking, packing, sorting, receiving, storing, and location management. By automating these procedures, the system lessens the need for warehouse employees to make choices about operations and inventory.	[24][71]

3.3. Enabling Technologies in IIoT

Below is a basic description of the leading IIoT-enabling technologies:

3.3.1. Wireless Sensor Network

Wireless sensor networks can easily integrate intelligent technologies into industrial processes. These networks are small, independent devices equipped with sensors and communication modules located strategically to gather and transmit vital data from industrial environments, such as temperature, pressure, and vibration. The information provided helps improve process efficiency and enable predictive maintenance [15].

3.3.2. Internet of Things

Real-time data gathering and actuation made possible by IoT devices facilitates effective production process monitoring, from raw materials to final products. By monitoring factory assets globally, these IIoT-essential devices save labor expenses and eliminate the need for human system administration. IoT devices across manufacturing lines, distribution hubs, and warehouses employ sensors and networking technologies to swiftly detect and relay data, enabling quick calculations and the best possible decision-making. Future urban communities will benefit from the innovative options created by this rising IoT integration with Industry 4.0, which improves industrial production processes [77][78].

3.3.3. Fifth-Generation (5G) and 6G Technologies

The rise of 5G technology and cellular network advancements have transformed how IIoT networks handle massive data generated by machines and devices, previously reliant on Wi-Fi connectivity. These technologies have increased bandwidth, reduced latency, and improved energy efficiency, enabling better management of extensive datasets. With 6G technologies, such as cloud-based extended reality and digital twins, IIoT evolves further, offering the high-speed, low-latency connectivity necessary for real-time applications [17].

3.3.4. Cyber-Physical Systems

Cyber-physical systems (CPS) integrate physical equipment, communication networks, and control systems to link manufacturing settings to the outside world. These technologies are essential to Industry 4.0. CPS makes smart factories possible by fusing the IoT with production. In these factories, machines communicate with one another via sensors, actuators, and data exchanges across networks, guaranteeing real-time information processing. These systems rely on onboard embedded IoT devices to decrease human interaction in industrial environments and increase operational efficiency. Sensors collect data, communication networks transfer it, and IT systems process and analyze it for decision-making to increase automation and operational efficiency. These layers are commonly seen in a CPS design. The transition to more intelligent, autonomous operations in industries like manufacturing and robotics is made easier by CPS, which improves stability, dependability, and security in Industry 4.0 systems by enabling real-time data capture and secure transmission [68][79][80].

3.3.5. Machine-to-Machine Communication

In the IIoT, M2M technology is crucial because it allows machines, sensors, and devices to communicate directly without human interaction. It makes it easier for industrial machinery and systems to transmit real-time data, promoting automation, remote monitoring, and predictive maintenance. M2M technology optimizes manufacturing, energy, and transportation processes, fostering innovation and strengthening overall industrial operations by increasing operational efficiency, reducing downtime, and improving decision-making through data analytics [77].

3.3.6. Blockchain Technology

Because it provides decentralization, traceability, security, and data provenance, Blockchain technology is essential to the IoT. Given the enormous volumes of data produced by IoT-enabled devices in various industries, Blockchain technology guarantees safe data exchange between all stakeholders in the IIoT ecosystem, resolving issues with access control and data privacy. This data is used in device performance analysis, anomaly detection, predictive maintenance, and product lifecycle tracking. Blockchain's distributed ledger system improves IoT security, reduces the risk of fraudulent activity, and offers decentralized access to data. While it faces scalability challenges, particularly as the number of IoT devices increases, its benefits in enhancing communication, trust, and real-time data verification make it a key technology for IIoT. Additionally, smart contracts are essential in automating and securing networked workflows [68][77][80].

3.3.7. Edge computing

By analyzing data closer to its source, a distributed architecture called "edge computing" lessens dependency on centralized cloud servers and improves system efficiency by cutting latency and conserving bandwidth. This approach uses edge devices with enough computing capacity to facilitate local data processing, speedy decision-making, and transfer outcomes to centralized systems. It assists companies in reducing delays, improving security, lowering the danger of data breaches, and enabling real-time data processing. Edge computing, which supports the IIoT, guarantees effective local processing while preserving device connection. It lowers network bottlenecks and enhances privacy by processing sensitive data at the source, but it also raises local costs because edge devices require infrastructure and storage. When edge and cloud computing are combined, real-time processing for time-sensitive applications is made possible while scalability for data-intensive jobs is optimized. According to experiments, edge computing can drastically lower latency, enhancing system performance overall and facilitating the deployment of AI models at the edge [17][68][80][81].

3.3.8. Fog computing

Fog computing builds on cloud computing by enabling wireless, distributed devices to connect to networks and perform critical functions in industrial applications without external support. Fog nodes offer network connectivity, computing power, and storage, while IT infrastructure is used to deliver web services. These nodes can help with ML experiments, system optimizations, and failure forecasting. Fog computing increases the scalability and flexibility of industrial systems by reducing latency and facilitating local data processing and storage by reducing the distance between edge and cloud layers. By placing processing closer to end devices, fog computing enables edge platforms to handle data, allocate network resources, and carry out calculations similar to cloud services [16][68][81].

3.3.9. Cloud Computing

The enormous amount of data the IIoT generates must be managed, processed, analyzed, and stored using high-performance distributed computing platforms. By directly linking backend clouds to all devices and applications, cloud computing technologies supply the computation, network, and storage resources required for IIoT systems. Large corporations usually employ private clouds to provide security, privacy, and a competitive edge. These cloud services might be private, public, or hybrid. IIoT networks benefit from integrating cloud infrastructure with edge computing since it permits local data processing, lowers latency, and makes real-time data management more effortless. This combination optimizes resource utilization and system scalability, allowing for efficient ML activities and comprehensive analysis of large datasets [17][68][78][80].

3.3.10. Big Data Analytics

Due to latency and real-time constraints, IIoT systems create enormous data streams that must be processed and analyzed using high-performance computing, making it difficult to decide when, how, and where to handle the data. These systems provide for the smooth orchestration of analytics services by integrating many technologies to collect, store, manage, process, analyze, and actuate big data. While storage options include on-premise, in-network, and cloud locations, data-gathering technologies link to various sources, including sensors, smart devices, and HMI. While data analysis uses methods like ML, DL, and statistical analysis across several layers, data management and processing occur close to sensors, edge servers, and cloud centers. Despite their complexity, extensive data processing and analysis are essential for next-generation IIoT systems because actuator technologies enable interactions between devices and their surroundings. IIoT systems improve overall decision-making, energy performance, and operational efficiency by locally processing data within Industry 4.0 environments or manufacturing systems [68][80].

3.3.11. Artificial Intelligence

AI technologies ensure the autonomous and intelligent operation of IIoT systems, reducing human intervention and improving efficiency. By leveraging complex AI methods, such as multi-agent systems and conversational AI, IIoT becomes more self-sufficient. Intelligence is embedded across various layers, from sensors and devices to edge servers and cloud data centers, utilizing algorithms for search, optimization, and prediction. Integrating AI and ML into IIoT data processing boosts efficiency, competitiveness, and customer satisfaction. These technologies help analyze large amounts of data, including unstructured information, and enable real-time anomaly detection, enhancing system security and reliability. AI models in IIoT systems optimize industrial processes through predictive maintenance, defect prediction, and process optimization, improving operational efficiency and product quality control. Furthermore, AI techniques, like rule-based reasoning and reinforcement learning (RL), strengthen security and resilience by identifying and mitigating attacks on IIoT devices. In Industry 4.0, ML enables self-decision systems and automation solutions, while robotics fosters efficient digital development with minimal human involvement [17][77][78].

3.3.12. Augmented Reality and Virtual Reality

Augmented reality (AR) and virtual reality (VR) technologies are crucial in improving efficiency and reducing errors in industrial operations. AR helps workers during complex tasks like assembling and disassembling machinery, industrial products, and mission-critical systems by providing real-time guidance and monitoring workers and machines to minimize mistakes. It also delivers relevant information at the right moment to enhance performance. Conversely, VR allows users to visualize configurations and reconfigurations of IIoT systems before implementation, helping to reduce reconfiguration times and prevent plant shutdowns. AR and VR enable workers to perform tasks more accurately and efficiently, supporting Industry 4.0 initiatives by integrating virtual and real-world environments in industrial processes [77][78].

3.3.13. Robotics & Automation

Robotics and automation are key drivers of innovation in the IIoT, transforming industries by enhancing productivity, efficiency, and safety. By integrating robotics with IIoT technologies, organizations streamline operations and optimize processes through real-time data exchange. Robots with sensors, cameras, and IoT devices gather valuable insights into machine health and performance, enabling predictive maintenance and reducing downtime. These intelligent systems, including autonomous mobile robots, automated guided vehicles, and collaborative robots, work autonomously or alongside human operators to improve tasks like material handling, assembly, and inspection. IIoT also supports dynamic scheduling, inventory tracking, and quality control, all while reducing human error and increasing precision. Robotics and automation in hazardous environments minimize risks by monitoring safety conditions, while scalable and energy-efficient systems help companies adapt to changing demands. Remote monitoring and control further enhance efficiency, making managing large-scale operations across diverse locations easier.

3.3.14. Cybersecurity Solutions

The IIoT connects machines, devices, sensors, and systems to enable real-time data sharing and optimization, but its interconnected nature makes it vulnerable to cyberattacks, breaches, and disruptions. Protecting IIoT systems with cybersecurity solutions is crucial to safeguard sensitive data, critical infrastructure, and operational systems from threats. These solutions include device authentication, data encryption, network security, threat detection, and incident response, all designed to ensure confidentiality, integrity, and availability. Implementing regular software updates, secure design practices, and physical and supply chain security measures further strengthen the system. With continuous monitoring and adherence to industry standards, organizations can mitigate risks, maintain business continuity, and build trust with partners and customers while ensuring compliance and long-term success. Fig. 6 summarizes the enabling technologies in IIoT.

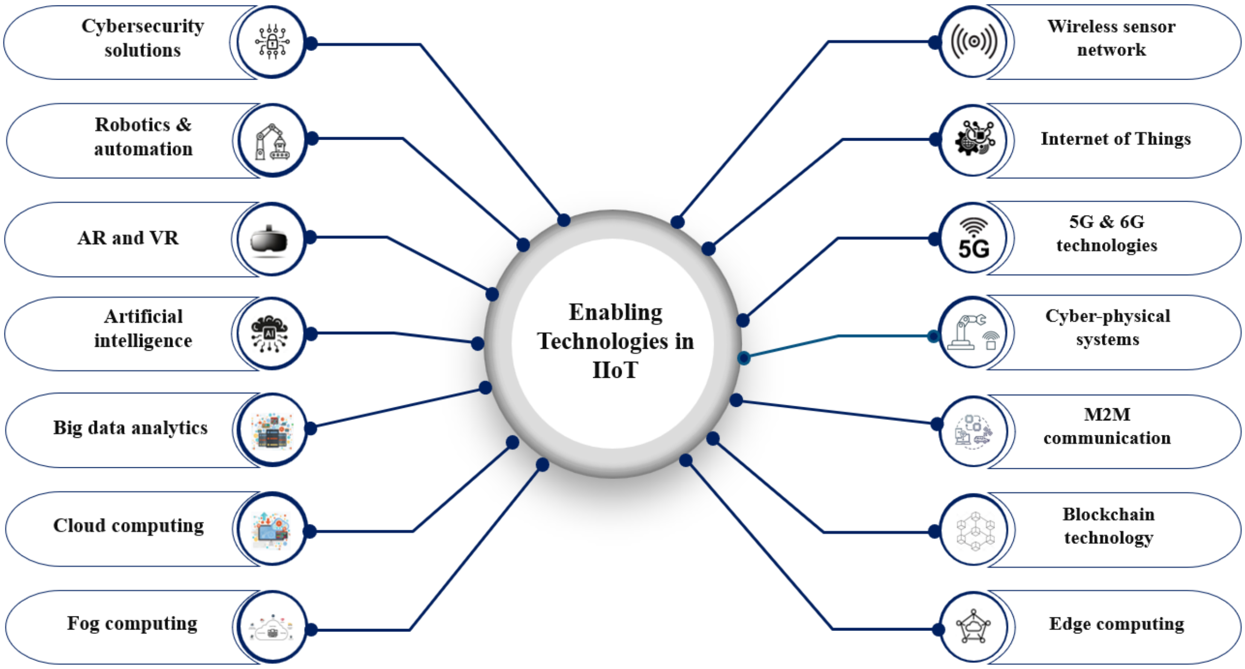

Fig. 6. Summary of the enabling technologies in IIoT.

3.4. IIoT Architecture

The IIoT architecture integrates various technologies to optimize industrial processes through connectivity, data analysis, and automation. This structured framework consists of multiple layers, each playing a distinct role in ensuring seamless data flow and operational efficiency. A widely used model includes layers for perception, network, edge computing, fog computing, cloud computing, processing, management, application, and security [13]. Fig. 7 depicts the main layers in the IIoT architecture.

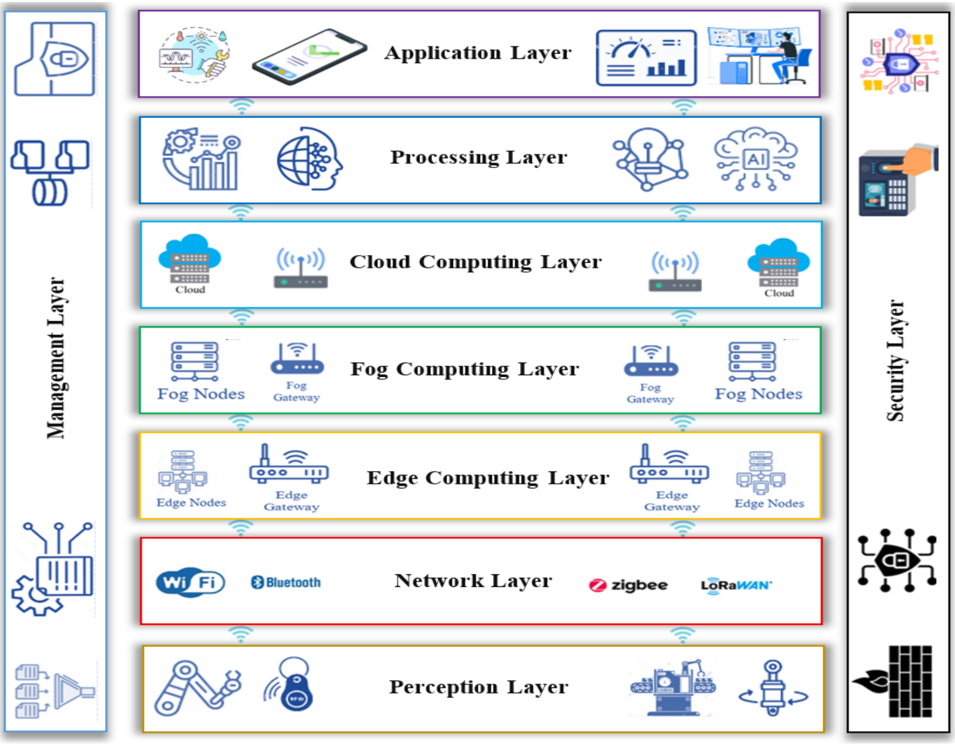

Fig. 7. Depicts the main layers in the IIoT architecture.

3.4.1. Perception layer

The perception layer forms the foundation of IIoT architecture by sensing, identifying, and capturing data from industrial devices [13]. This layer comprises various sensors, actuators, RFID tags, imaging devices, GPS modules, and edge computing devices that monitor environmental and operational parameters such as temperature, pressure, and machinery status [12]. Sensors collect real-time data, convert physical phenomena into digital signals, and transmit the information to the network layer for further processing [24]. Actuators, including LEDs, buzzers, and mechatronic devices, execute physical actions based on predictive models and control mechanisms [46]. This layer also integrates existing industrial digital systems, databases, and informatization systems, ensuring seamless connectivity between legacy and modern IIoT solutions [82]. Moreover, the perception layer enables industrial automation by supporting devices like industrial robots, automated guided vehicles, and transporter systems, which facilitate efficient monitoring, control, and optimization of production environments [32].

3.4.2. Network layer

The network layer facilitates secure and reliable data transmission between devices, sensors, networks, and servers using wired or wireless technologies like Ethernet, Wi-Fi, ZigBee, Bluetooth, and emerging 5G networks [13][46]. It enables seamless communication between the perception and processing levels through a range of protocols, including IPv4, IPv6, LPWAN, LoRa WAN, MQTT, and RFID [24][32][48]. As the IIoT advances, low-power wireless communication technologies like Bluetooth Low Energy (BLE) and ZigBee have become popular due to their efficacy. The network layer manages communication infrastructure, enables service discovery, and allows interoperability to provide dependable and high-capacity data transmission. Integrating security protocols and middleware ensures data integrity while satisfying industry-specific requirements such as M2M connectivity and high-bandwidth cloud communication [77]. Additionally, the transport layer organizes and mixes multiple application protocols, such as CoAP, MQTT, HTTP, and OPC UA, to facilitate flexible data flow [82]. The network layer, which serves as the basis for IIoT communication, connects different industrial parts and increases productivity through monitoring and intelligent production.

3.4.3. Edge computing layer

The edge computing layer, positioned between the device and cloud layers, processes data locally to reduce latency and bandwidth usage. The edge computing layer improves decision-making and system responsiveness by conducting real-time analytics and preliminary data processing close to the data source. This layer combines interrelated components to facilitate anomaly detection, intelligent decision-making, and real-time data processing. Fundamentally, Wi-Fi routers link edge servers, process local data, implement edge AI models, and communicate over the MQTT protocol. According to Joha et al. [9], these models carry out functions such as anomaly detection, data preparation, model deployment and analysis, and visualization.

3.4.4. Fog computing layer

Fog nodes—base stations, routers, switches, gateways, and specialized fog servers—are essential components that link endpoints to the cloud in IIoT fog computing. These nodes communicate extensively with one another to improve industrial processes, enabling tasks like establishing artifact traceability through data sharing without external help and improving algorithm performance through collaborative learning.

3.4.5. Cloud computing layer

Cloud-based systems are widely used for processing and storing data collected from IoT and IIoT devices due to their scalability and accessibility for data analysis and application development [48]. These platforms handle and store device-generated data via a data layer [13]. Cloud storage is crucial for IIoT due to its robust hardware and software capabilities. Cloud-stored data can be quickly evaluated or interpreted by AI or data-mining techniques. While recent innovations like fog computing help to reduce latency, specific manufacturing networks may use separate data centers or servers to store data based on their particular objectives and strategies [77].

3.4.6. Processing layer

The data processing and analytics layer, or the middleware layer, analyzes and processes data using cloud computing resources, advanced analytics, ML, and AI to extract actionable insights [48]. It ensures seamless communication between heterogeneous devices and software through APIs and protocols, supporting efficient data exchange [46]. This layer performs preprocessing, converts raw data into valuable information, and maintains the integrity and quality of data collected from lower layers [83]. It uses ML and DL to generate insights, optimize manufacturing performance, and enable predictive analysis, improving efficiency, production, and cost [24]. Applying techniques like data mining and statistical methods enhances IIoT performance, reduces resource consumption, and facilitates automated support, failure detection, and maintenance optimization, often relying on cloud-based resources to automate data collection and analysis cycles. Finally, the decision layer makes informed decisions based on the insights provided by this processing and analytics layer [13].

3.4.7. Management layer

The management layer in IIoT architecture is vital in overseeing the operation, control, and coordination of the entire IIoT ecosystem between the application and infrastructure layers. It manages and optimizes IIoT devices, systems, networks, and data flows, ensuring seamless performance. This layer utilizes cloud-based platforms for scalability, edge computing for local processing, and AI and ML for predictive maintenance and anomaly detection. It also incorporates automation tools for streamlining device configuration and monitoring. Key functions include device, network, data, security, resource management, system monitoring, diagnostics, service level management, and policy enforcement. The management layer facilitates integration and interoperability and supports analytics, ensuring adequate data handling and system optimization [13].

3.4.8. Application layer

The application layer in IIoT encompasses software solutions that convert processed data into actionable insights, optimize industrial operations, and support informed decision-making. It includes tools like predictive maintenance systems, quality control platforms, and dashboards for performance monitoring [48]. By offering services like actuator control, energy management, and remote monitoring, this layer interacts directly with end-user devices [12][13][24]. Through Internet-enabled devices, users can access cutting-edge applications in various industries, including smart manufacturing, healthcare, and agriculture [32]. The application layer links end nodes to the IIoT network and enables communication between devices and software. To operate correctly, IIoT systems rely on protocols like WebSockets, MQTT, CoAP, HTTP, and Secured MQTT. This layer also handles security issues and the increasing demand for real-world applications of AI, big data, and cloud-edge collaboration, which are critical to advancing industries’ intelligent and digital transformation [46][82].

3.4.9. Security layer

The security layer in IIoT architecture is crucial for protecting the entire IIoT ecosystem from cyber threats, unauthorized access, and data breaches. This layer ensures data and systems’ confidentiality, integrity, and availability by implementing various security measures, such as device authentication, encryption, network security, and endpoint protection. It employs technologies like public key infrastructure (PKI), multi-factor authentication (MFA), Transport Layer Security (TLS), and Advanced Encryption Standard (AES) to safeguard data. It also utilizes intrusion detection systems (IDS), firewalls, and secure communication protocols like MQTT to monitor and protect the network. Real-time monitoring, risk management, compliance, and incident response are critical components alongside secure software development practices. Advanced technologies such as Blockchain for data integrity, AI and ML for threat detection, and the Zero-trust security model enhance the overall defense, ensuring a robust and secure IIoT environment [77].

This modular and scalable layered architecture effectively implements IIoT systems, ensuring interoperability and efficient data management across industrial operations. It promotes seamless integration, allowing different components to work together efficiently while supporting growth and adaptability.

3.5. IIoT Applications

IIoT is revolutionizing industries by enhancing agility and responsiveness. Various IIoT applications have significantly improved resource efficiency, driving faster industry productivity growth. Below are the brief descriptions of the key applications of IIoT.

3.5.1. Predictive maintenance

IIoT uses sensors and analytics to monitor machinery and equipment instantly. By analyzing historical and live data, industries can predict failures before they happen, reducing downtime, cutting maintenance costs, and enhancing operational efficiency [84][85].

3.5.2. Smart Manufacturing

By integrating smart devices, electronics, and advanced communication methods, IIoT transforms traditional manufacturing into smart factories that boost production speed and flexibility. This transition enables highly adaptable and efficient production, replacing conventional methods with cutting-edge technologies. Smart factories incorporate innovations like augmented reality, simulations, and virtual prototypes, allowing machines to monitor their performance and adjust operations instantly. Through digital twins and CPS, manufacturers use real-time data to improve quality control, minimize waste, and enhance supply chain efficiency [77][86][87].

3.5.3. Asset tracking and management

Industries leverage IIoT to monitor assets across extensive facilities, including machinery, vehicles, and tools. RFID, GPS, and IoT sensors instantly track location, usage, and condition, preventing losses and optimizing resource allocation [88].

3.5.4. Energy management

IIoT optimizes industrial energy consumption by monitoring power usage in factories, plants, and warehouses. Smart grids, automated energy controls, and AI-driven analytics help reduce costs and lower carbon footprints by improving energy efficiency. Attaching IoT sensors to infrastructure allows businesses to track energy-consuming systems and implement automated solutions, such as turning off lights after a particular hour or when the building is empty. A robust IoT-based HVAC monitoring system efficiently manages heating, ventilation, and air conditioning energy use. As a key component of IIoT, industrial energy systems enhance the performance of new energy solutions and contribute to greater environmental security [32].

3.5.5. Supply chain and logistics optimization

IIoT improves supply chain management by enabling real-time tracking of raw materials, products, and shipments. With smart sensors and AI-driven insights, businesses can enhance inventory management, fleet tracking, route optimization, and warehouse automation. The intricate process of supply chain management covers a product's entire lifecycle. IIoT solutions provide essential transparency, control, and automation, allowing employees to monitor goods instantly, track storage conditions, optimize delivery routes, and quickly locate items in storage [3].

3.5.6. Industrial automation and robotics

Connected robots and automation systems enhance manufacturing, assembly, and packaging by enabling seamless communication between robotic arms, conveyor systems, and quality inspection tools through IIoT. This technology increases speed, precision, and flexibility while reducing overhead costs, boosting productivity, and improving employee satisfaction. By automating processes, IIoT minimizes human error and significantly enhances product quality. With this approach, IIoT supports highly dynamic automation across various industries, optimizing manufacturing, supply chain management, and logistics through real-time monitoring, predictive maintenance, and improved operational efficiency[48][77][89].

3.5.7. Worker safety and environmental monitoring

IIoT enhances workplace safety through wearable devices, real-time monitoring, and AI-based alerts. Smart sensors detect gas leaks, temperature fluctuations, air quality issues, and hazardous conditions, ensuring compliance with safety regulations and protecting workers. In high-risk industrial environments, operating heavy machinery poses grave dangers, but IIoT applications help prevent accidents. Sensors on workers monitor perspiration, working techniques, heart rate, and temperature to assess their well-being. A connected workforce strengthens workplace safety by tracking biometrics and hazard exposure and relaying that data to nearby workers. Implementing IIoT-based safety systems improves industrial efficiency by enhancing human resource management and reducing workplace accidents [77][90][91].

3.5.8. Remote monitoring and control

IIoT enables industries to remotely monitor and control operations, ensuring efficiency and operational continuity. With cloud-based platforms, supervisors can track machine performance, factory conditions, and security anywhere. Industrial IoT applications allow real-time adjustments to settings and equipment operations. For instance, if the system detects a gas leak, it can immediately trigger shutdown protocols to prevent hazards and costly damages. Remote control significantly cuts operational costs by reducing the need for on-site technicians. IIoT also enhances monitoring by replacing manual checks with sensors that detect anomalies and respond proactively [77][92].

3.5.9. Smart agriculture and farming

IIoT-powered smart sensors monitor soil conditions, weather patterns, crop health, and irrigation systems in agriculture. Automated machinery, including self-driving tractors and drones, optimizes farming operations to boost productivity and sustainability. By analyzing data, IIoT reduces waste and promotes sustainable farming practices [17].

3.5.10. Healthcare and pharmaceuticals

IIoT is revolutionizing the healthcare sector by ensuring precision, compliance, and operational efficiency in medical device manufacturing, pharmaceutical production, and hospital operations. It enables real-time tracking of medical supplies, remote patient monitoring, and automation of critical healthcare processes, significantly improving patient care and management systems. Integrating AI and ML, IIoT helps analyze patient data and predict health outcomes, fostering proactive health management. Applications such as patient-centered medical home care, medical equipment efficiency improvement, and telemedicine solutions benefit from IIoT, reducing costs and enhancing remote control of medical equipment. IIoT devices enable quick diagnosis, timely treatment decisions, and improved patient monitoring, while CPS and sensor devices provide real-time data to guide medical professionals. Additionally, IIoT-based doctor recommendation systems allow patients to access real-time information and book appointments with qualified doctors, further enhancing healthcare delivery [17][32].

3.5.11. Transportation and logistics

The IIoT transforms logistics and transportation by improving tracking, fleet management, and supply chain efficiency. It provides real-time vehicle location, condition, and performance data, ensuring better decision-making and optimized operations. Blockchain-enabled systems ensure secure data exchange, safeguarding against breaches and increasing stakeholder confidence. IoT technologies like RFID, autopilot systems, and computer vision enhance vehicle tracking and predictive capabilities, while advanced systems like BMW's iDrive use sensors to monitor road conditions and guide drivers. IIoT also enables mobile ticketing with NFC tags, monitors environmental conditions in food transport, and supports augmented maps for tourist information, ultimately boosting productivity and automation in logistics and transportation [17][32][77].

3.5.12. Smart grid

Smart grids enable bidirectional electricity transmission, facilitating coordination between power suppliers and consumers. IIoT automates smart grid operations by reducing fossil fuel use, increasing renewable energy adoption, and enhancing power utilization. It improves energy management by tracking production and consumption, facilitating cooperation among diverse renewable sources, and ensuring smoother grid integration. By leveraging real-time data, IIoT optimizes energy distribution, reduces operating costs, and strengthens grid stability while supporting demand response programs. Additionally, federated learning (FL) in IIoT networks enhances scalability and data privacy, safeguarding personal data and enabling intelligent energy management solutions [17][48][77].

3.5.13. Inventory monitoring

In industrial settings, IIoT-enabled inventory monitoring uses connected devices, sensors, and real-time data analytics to track and manage inventory efficiently. By placing sensors on products or pallets, businesses can monitor stock levels, location, condition, and movement while ensuring proper storage conditions through data on temperature, humidity, and environmental factors. RFID tags and barcode scanners work together to track and update the status of items as they move through warehouses or production lines. This real-time data offers valued insights into inventory levels, predicts demand, and optimizes stock replenishment. With automated stock refills and reduced human error, IIoT enhances accuracy, increases efficiency, and streamlines inventory management, saving businesses time and effort while improving operational performance [86][90].

3.5.14. Smart factory

Smart factories leverage IIoT technologies to connect machines and humans through operation, field, and mobile devices, with the primary goal being to deliver clients innovative products, services, and feedback. The key components of smart factories include intelligent machines, smart manufacturing, smart engineering, manufacturing IT, and cloud computing. Cloud computing and big data support the development of manufacturing processes, hardware, and software. Intelligent machines integrate autonomous systems, sensors, and communication devices to enable self-operability, maintenance, and awareness. Smart manufacturing combines CPS with IoT, automating processes for efficiency and responsiveness to customer needs. IIoT allows real-time monitoring of machines, fleets, and components, while innovative engineering uses big data analytics to optimize product design and development. Integrating IIoT into production processes boosts automation, resource efficiency, and predictive maintenance, ultimately improving productivity and reducing downtime [17][32].

3.5.15. Construction sector

Integrating IIoT in the construction sector is revolutionizing the industry by boosting productivity, enhancing safety, and streamlining resource management. IIoT links workers, machines, and equipment through wearable technology, smart sensors, and sophisticated monitoring systems, allowing for real-time data collecting and analysis. Thanks to this connectivity, construction companies can assess site conditions, keep an eye on worker safety, and monitor equipment performance. By adjusting operations independently, smart robots can minimize downtime and human mistakes. Predictive maintenance also reduces repair costs and minimizes interruptions by detecting possible problems before they become serious. By providing insightful information about progress, resource utilization, and material availability, IIoT also enhances project management by reducing delays and streamlining scheduling. IIoT enhances short-term project results and long-term sustainability by combining automation and data-driven insights to support safer, more cost-effective, and more efficient building operations [17].

3.5.16. Mining

The IIoT revolutionizes the mining industry by improving safety, efficiency, and productivity. By integrating smart sensors, wearable devices, and advanced monitoring systems, IIoT connects equipment, machinery, and personnel to enable real-time data collection and analysis. This connectivity allows mining companies to track equipment performance, monitor environmental conditions, and enhance worker safety. Sensors in equipment detect malfunctions or wear, enabling predictive maintenance that lessens downtime and repair costs. IIoT also provides insights into resource usage, energy consumption, and ore quality, helping optimize processes and minimize waste. With automation and remote-controlled systems, IIoT enables safer operations in hazardous environments, reducing risks to workers. Overall, IIoT drives operational efficiency, lowers costs, improves safety standards, and promotes sustainability in mining [17].

3.5.17. Advanced analytics

IIoT leverages connected devices and sensor data to enable informed, data-driven decision-making. IIoT facilitates advanced analytics like ML, predictive modeling, and AI by integrating real-time machinery, equipment, and operations data. These tools identify patterns, predict failures, and optimize performance, improving operational efficiency. For example, predictive maintenance models can forecast equipment failures, allowing for timely repairs and reducing costly downtime. IIoT-driven analytics also help optimize resource usage, minimize waste, and enhance sustainability. Industries such as manufacturing, energy, and mining can harness these insights to streamline processes, boost profitability, and drive continuous optimization across all business aspects [84][93].

4. CYBER THREATS AND ATTACKS IN IIoT

Despite widespread adoption in industrial control systems, IIoT remains vulnerable to cyberattacks that can severely impact organizations' reputations and finances. Table 2 briefly describes the most common security threats and attack methods in the IIoT environment.

TABLE II. BRIEFLY DESCRIBE THE MOST COMMON SECURITY THREATS AND ATTACK METHODS IN THE IIOT ENVIRONMENT.

S/No	Reference	Security threats and attacks	Description	Violated Security Principle							
				C	I	A	Au	AT	N	R	Ac
1	[33][35][94]	Privacy violation	The vast data generated by IIoT devices raises serious privacy concerns, especially in critical systems like smart grids and industrial control systems. Unauthorized access, weak authentication, and unsecured communications expose intellectual property, operational data, and employee privacy to cyber threats. Attackers can intercept unencrypted transmissions, manipulate industrial operations, and exploit excessive data collection without user consent. Poor data storage and retention policies make cloud platforms vulnerable to breaches, increasing the risk of leaks and permanent data loss. Privacy violations in IIoT compromise data confidentiality, exposing sensitive information without consent.	✓	✓	✓	✓	✓	✓	✓	✓
2	[32][33][37]	Data Breach	A data breach in IIoT happens when unauthorized individuals access sensitive information from interconnected industrial devices and networks. Many industrial systems are vulnerable to ransomware, malware, and data theft because they lack strong protection. Inadequate network segmentation puts critical infrastructure, such as ERP and SCADA platforms, at risk by enabling hackers to move between systems. Weak authentication, outdated firmware, and unencrypted data transmission provide hackers with entry points they can use. Inadequate network segmentation allows cybercriminals to move across IT and operational networks, potentially endangering critical infrastructure. Furthermore, unsecured remote access tools increase the risk of security breaches by allowing hackers to change systems, steal data, or impede business operations. Malicious actors could obtain private or sensitive information if sensitive data from digital twins is not sufficiently protected.	✓	✓	✓	✓	✓	✓	✗	✗
3	[36]	Reconnaissance attacks	Reconnaissance attacks in IIoT systems involve attackers gathering information about the target infrastructure, device configurations, and communication protocols to identify vulnerabilities. This process, typically the first step in a more complex intrusion, allows cybercriminals to understand the network layout, connected devices, and potential weaknesses. Attackers scan for open ports, services, and firmware versions, which may be exploited if known vulnerabilities exist. In IIoT environments, such attacks are more common due to devices' open and interconnected nature, which often have poor security practices like weak passwords or unencrypted communications. Poor authentication practices in systems	✓	✓	✓	✓	✓	✓	✗	✗

			like SCADA, where default or infrequently changed passwords are shared, make these environments particularly vulnerable to reconnaissance, as attackers can exploit such weaknesses to gain unauthorized access. While the immediate impact of reconnaissance attacks may be low, they lay the groundwork for more severe attacks like data breaches or system malfunctions.								
4	[17][31-33][38][39][81][95]	Malware and Ransomware attacks	Malware is malicious software that disrupts, damages, or gains unauthorized access to IIoT networks, devices, and control systems. It spreads through phishing emails, compromised software, or network vulnerabilities, leading to operational disruptions and data breaches. Ransomware, a severe malware type, encrypts critical data and demands a ransom, crippling industrial operations. Attackers exploit outdated software and weak security in IIoT systems to inject malware, steal information, or hijack control systems. These threats pose severe risks to industrial processes, causing financial losses, downtime, and compromised safety.	✓	✓	✓	✓	✓	✓	✓	✗
5	[17][21][22][32][33][35][46][81][96]	MitM attacks	MitM attacks in IIoT occur when attackers intercept and manipulate communication between devices, compromising data integrity and security. They exploit weak encryption, protocol vulnerabilities, or insecure network configurations to eavesdrop, alter messages, or inject malicious commands. Attackers can hijack IIoT communication through packet sniffing, session hijacking, or ARP spoofing, leading to false sensor readings, unauthorized control, or production disruptions. If they compromise the MQTT broker, they can control the entire IoT system. MitM attacks pose a serious threat by enabling data modification, fabrication, and unauthorized access, which can result in equipment failure and severe industrial damage.	✓	✓	✓	✓	✓	✓	✗	✗
6	[17][31-35][37][81][96][95]	DoS and DDoS attacks	DoS attacks threaten IIoT systems by overwhelming devices, networks, or services with excessive traffic, disrupting operations, and causing downtime. Attackers exploit vulnerabilities in communication protocols, weak authentication, and unsecured endpoints to degrade performance or trigger system failures. DDoS attacks amplify the impact by using botnets to flood IIoT networks, making monitoring and control nearly impossible. By leveraging techniques like SYN flooding, HTTP flooding, and signal jamming, attackers exhaust device resources and disrupt communication. Many IIoT devices lack strong security, allowing cybercriminals to hijack them into botnets that generate malicious traffic against industrial control servers, cloud platforms, and communication protocols like TCP and MQTT. As a result, DDoS attacks severely impact industrial automation, manufacturing, energy, and transportation networks, leading to financial losses, safety risks, and operational failures.	✓	✓	✓	✓	✗	✗	✓	✗
7	[21][31][33][81][95]	Supply chain attacks	Supply chain attacks in the IIoT exploit vulnerabilities in industrial systems by targeting hardware, software, or services at different supply chain stages. Cybercriminals insert malicious code, backdoors, or tampered components into firmware, software updates, or third-party applications before they reach end users. They compromise software repositories, development environments, or hardware during manufacturing and distribution, allowing unauthorized access, remote command execution, or data exfiltration once integrated into industrial networks. Attackers exploit weak cybersecurity practices among vendors or contractors with privileged access, using phishing attacks or insider threats to infiltrate critical infrastructure. These threats pose significant risks, mainly as IIoT integrates with Industry 4.0, increasing cybersecurity challenges. Adversaries can install backdoors, introduce defective chips, or use publicly available data to extract sensitive information via ML-based side-channel attacks.	✓	✓	✓	✓	✗	✓	✗	✗

8	[30][32][35]	Spoofing attack	A spoofing attack in the IIoT occurs when an attacker impersonates a trusted entity to manipulate or gain unauthorized access to an industrial system. By exploiting authentication, communication protocols, and network infrastructure vulnerabilities, attackers can spoof device identities such as IP addresses, MAC addresses, or unique credentials, allowing them to intercept, alter, or inject malicious data into the system, potentially causing incorrect decisions, equipment failure, or safety hazards. For example, an attacker could mimic a sensor in a smart factory to send falsified readings, disrupting operations. GPS spoofing, DNS, and ARP spoofing also pose significant risks, such as misleading location data in logistics or redirecting network traffic for eavesdropping and data theft. This attack can severely impact operational efficiency and security, with techniques like RFID spoofing exploiting inventory and equipment monitoring systems vulnerabilities.	✓	✓	✓	✓	×	✓	×	✓
9	[31][33][37]	Insider threats	Insider threats in the IIoT pose a significant risk to system security and functionality, as individuals with authorized access—such as employees, contractors, or trusted third parties—may misuse their position to compromise operations, steal sensitive data, or cause damage. These insiders can manipulate interconnected systems, alter sensor data, sabotage production processes, or cause downtime, leading to significant financial and reputational harm. The complexity of IIoT environments and traditional security measures' inability to detect insider actions make these threats hard to identify. Disgruntled employees may tamper with ICS or HMI systems, deliberately disrupting operations. Furthermore, privileged insiders with access to critical data, such as Digital Twins or physical assets, may abuse this power for personal gain or revenge, compromising security and integrity.	✓	✓	✓	✓	✓	✓	×	✓
10	[17][31][95][97][98]	Social engineering and phishing attacks	The IIoT enables seamless communication between devices, sensors, and control systems, but it also exposes systems to cyber threats like social engineering and phishing. These attacks manipulate individuals to reveal sensitive information or take actions that compromise security, leading to financial loss, reputation damage, and operational disruptions. Phishing is particularly harmful in IIoT environments, as attackers impersonate trusted figures to gain unauthorized access to ICS or HMI. Techniques such as deceptive emails, phone calls, and website forgeries target employees and vendors, risking control over critical systems.	✓	✓	✓	✓	✓	✓	×	✓
11	[32]	Side-channel attacks	Side-channel attacks in IIoT exploit unintended information leaks from power consumption, electromagnetic emissions, timing variations, or acoustic signals to gain unauthorized access or infer sensitive data. These attacks focus on the microarchitecture of processors to extract valuable information, such as cryptographic keys. Techniques like differential power analysis, electromagnetic analysis, and timing attacks allow attackers to deduce secret keys or manipulate industrial processes without direct system access.	✓	✓	✓	✓	×	✓	×	×
12	[17][38]	Botnet attacks	Botnet attacks target IIoT systems by exploiting weak authentication, outdated firmware, and unsecured communication channels. Infected devices are used to launch DDoS attacks, disrupt industrial operations, and cause financial losses through production delays and equipment malfunctions. Botnets also enable data exfiltration, espionage, ransomware attacks, and cryptojacking, leading to intellectual property theft, system slowdowns, and unauthorized control over industrial systems. In next-generation industrial CPS, attackers can exploit these devices to gain remote access, disrupt operations, and manipulate control commands. Additionally, security gaps at the boot stage make IIoT edge devices particularly vulnerable, allowing attackers to	✓	✓	✓	✓	✓	✓	✓	×

			capture devices during reboot and further compromise the system.								
13	[30][32][81]	Jamming attacks	Jamming attacks threaten IIoT security by disrupting wireless communication, leading to network failures, data loss, and reduced efficiency. Attackers use constant, reactive, deceptive, and random jamming techniques to interfere with industrial processes, causing production delays and safety risks. In smart factories and critical infrastructure, jamming can halt operations, trigger cascading failures, and enable further cyberattacks. A real-world case involved a former employee using a high-frequency jammer to disrupt communications between IIoT sensors and control systems, halting production and exposing vulnerabilities in the facility's security infrastructure.	✓	✓	✓	✓	✗	✗	✓	✗
14	[32][35][81]	Sleep deprivation attacks	Sleep deprivation attacks target battery-powered devices in IIoT networks by preventing them from entering low-power sleep modes, causing excessive energy consumption. Attackers achieve this by sending high volumes of unnecessary requests or exploiting network vulnerabilities, forcing devices to stay active and draining their batteries. In some cases, malicious code is executed to create infinite loops, or hardware modifications are made, keeping the devices continuously active. As a result, the devices' energy reserves deplete rapidly, leading to performance degradation, network congestion, and system failures. These attacks disrupt industrial operations by compromising data transmission, increasing maintenance costs, and causing potential downtime. They also harm system reliability by denying the power needed for IIoT devices to function correctly.	✓	✓	✓	✓	✓	✗	✓	✗
15	[32][33][81]	Replay attacks	Replay attacks threaten IIoT environments by intercepting and retransmitting legitimate data packets to deceive systems. Weak authentication and encryption allow attackers to reuse old messages to gain access, manipulate operations, or disrupt industrial processes. IIoT systems remain vulnerable due to legacy protocols and resource constraints, making secure encryption and key exchanges difficult. Attackers exploit these gaps by capturing and replaying network traffic, triggering unauthorized actions like altering sensor data or shutting down power grids.	✓	✓	✓	✓	✗	✓	✗	✗
16	[17][33][35][81]	Eavesdropping attacks	Eavesdropping attacks in IIoT involve attackers intercepting data transmitted between connected devices, sensors, controllers, and cloud systems. These attacks exploit wireless and wired communication vulnerabilities, targeting critical information such as operational commands, production data, and confidential business insights. The lack of strong encryption and secure authentication mechanisms in legacy systems, along with insecure wireless methods like unprotected Wi-Fi or Bluetooth, makes IIoT networks particularly vulnerable. Attackers use packet sniffers to capture and analyze network traffic without detection, often extracting sensitive information instantly, leading to system disruptions, data manipulation, financial losses, and risks to national security. In IIoT systems, which usually involve numerous transmitting devices, eavesdropping poses a significant threat to confidentiality and integrity, with attackers using traffic analysis to discern communication patterns and gain access to private information.	✓	✓	✓	✓	✓	✓	✗	✗
17	[32][35][81]	Sybil attacks	In a Sybil attack on IIoT networks, an attacker creates multiple fake identities or nodes to deceive the system and gain disproportionate influence over network operations. These counterfeit identities allow attackers to disrupt communication, inject false data, and manipulate decisions, leading to operational failures, financial losses, and compromised data integrity. For example, in smart grid environments, a Sybil attack can cause incorrect energy usage reports, resulting in power outages. The attack undermines consensus mechanisms and routing protocols	✓	✓	✓	✓	✗	✓	✗	✗

			by overwhelming legitimate nodes, causing network congestion, increased latency, or complete failure. Such disruptions can severely affect industries relying on real-time control and monitoring.								
18	[81][32]	Wormhole attacks	Wormhole attacks pose a severe security threat in IIoT networks by allowing attackers to create a low-latency communication link between two distant points, manipulating data transmission. Malicious nodes collaborate to capture packets at one location and tunnel them to another, bypassing normal routing mechanisms and distorting the network topology, which creates the illusion that two endpoints are closer than they are, disrupting network operations, misrouting data, and making the system more vulnerable to MitM or DoS attacks. IIoT systems, which rely on real-time communication for automation and control, are particularly vulnerable as wormhole attacks can delay or reroute critical data, leading to operational failures, safety hazards, or production downtime. These attacks can drain the batteries of intermediate legitimate nodes as the tunneled packets pass through them.	✓	✓	✓	✓	✗	✓	✗	✗
19	[81][32]	Malicious code injection attacks	Malicious code injection attacks in IIoT environments embed harmful code into IIoT systems, applications, or network components, exploiting vulnerabilities in ICS, SCADA systems, and edge computing devices. These attacks manipulate system behavior, gain unauthorized access, or disrupt operations using techniques like SQL injection, command injection, and cross-site scripting (XSS). Such attacks can compromise power grids, manufacturing plants, and water treatment facilities by altering sensor data, disrupting PLCs, or halting production lines. IIoT devices are more vulnerable due to their reliance on legacy systems with limited update capabilities, making it difficult to deploy security patches quickly. Malicious scripts can enter through unsecured APIs, outdated firmware, or misconfigured protocols, allowing attackers to exfiltrate sensitive data, install malware, or gain remote control, leading to operational failures or espionage. Exploiting vulnerabilities in debug modules or firmware upgrades, attackers can inject malicious code affecting individual devices and entire networks.	✓	✓	✓	✓	✓	✓	✓	✗
20	[32]	Fake node injection	Fake node injection occurs when attackers introduce counterfeit nodes that impersonate legitimate devices. These malicious nodes manipulate data, disrupt operations, and exploit system vulnerabilities. False information and illegitimate traffic can cause malfunctions, outages, and network congestion. Attackers exploit weak authentication or insecure protocols to control fake nodes, compromising IIoT system integrity, confidentiality, and availability.	✓	✓	✓	✓	✓	✓	✗	✓
21	[31][37][81][99]	Authorization and authentication attacks	Authentication and authorization attacks target access control mechanisms in IIoT systems. Attackers use credential stuffing, phishing, and brute force to bypass authentication, exploiting weak MFA. Once inside, they exploit authorization vulnerabilities to access sensitive resources, escalate privileges, or bypass access controls. These attacks can cause significant damage, including data theft, process disruptions, equipment damage, and safety hazards, highlighting the need for stronger security measures.	✓	✓	✓	✗	✗	✓	✗	✓
22	[17][100][101]	Advanced persistent threat attacks	APTs involve sophisticated cyberattacks that target specific networks for long-term infiltration. They exploit IIoT vulnerabilities, such as weak security in devices and centralized control systems, to remain undetected. APTs infiltrate IIoT networks through phishing, malware, exploiting known vulnerabilities, or compromising third-party vendors with access to industrial systems. Once inside, attackers conduct reconnaissance, escalate privileges, move laterally across the network, establish command and control, exfiltrate data, and disrupt	✓	✓	✓	✓	✗	✓	✓	✓

			operations. These attacks can steal sensitive data or disrupt critical operations, as seen with Stuxnet.								
23	[21][37]	IIoT device exploitation	Cyber attackers exploit IIoT devices by exploiting weak authentication, outdated firmware, and unpatched software. They manipulate data, disrupt operations, and cause cascading effects across connected systems. Attackers can seize control of critical systems like smart meters, remote cars, or aircraft, posing serious safety risks. IIoT devices' lack of security mechanisms makes them vulnerable to ransom demands and data exfiltration attacks.	✓	✓	✓	✓	✓	✓	✓	✗
24	[17][21][33]	Physical attacks	Physical attacks target critical infrastructure by sabotaging sensors, actuators, controllers, or network components, causing production disruptions and malfunctions. Attackers may alter system configurations or tamper with control systems like PLCs to trigger faulty processes. Damaging communication channels or stealing devices can result in data loss and unauthorized access.	✓	✓	✓	✓	✗	✓	✓	✓
25	[21][32]	Data interception and tampering	Malicious actors intercept and tamper with data in IIoT networks to compromise its integrity, confidentiality, and availability. They exploit weak encryption or security protocols to access sensitive operational data, such as control commands and sensor readings. Once intercepted, attackers manipulate or alter the data to disrupt operations, cause damage, or create safety risks. Attackers can also manipulate communication devices, RFID systems, and application data exchanged between servers and clients by altering POST requests.	✓	✓	✓	✓	✗	✓	✓	✗
26	[81]	Node capture attacks	In a node capture attack on IIoT, attackers physically seize a network node like a sensor or controller to compromise its functionality and extract sensitive data. They exploit hardware, software, or authentication vulnerabilities to reverse-engineer protocols, inject malicious instructions, or manipulate data, which grants long-term access, allowing attackers to monitor communications, disrupt processes, and impersonate devices. Attackers can also exploit trust between nodes, spread false data, and access sensitive assets, enabling further network-wide attacks.	✓	✓	✓	✓	✓	✓	✓	✗
27	[33][81]	Cross-site or malicious script attacks	Cross-site and malicious script attacks pose severe security risks to IIoT systems by injecting harmful code into web applications. Attackers exploit vulnerabilities to steal sensitive data, manipulate control systems, and disrupt industrial operations. In IIoT environments, where industrial machines and critical infrastructure connect through web interfaces, attackers can use malicious scripts to steal login credentials, redirect users to phishing sites, or gain unauthorized access to control systems. These scripts can hijack user credentials, redirect to phishing sites, or cause automation failures. Malicious code blends with legitimate scripts, making detecting and executing in any browser hard.	✓	✓	✓	✓	✗	✓	✓	✗
28	[33]	Impersonation attack	Impersonation attacks occur when attackers assume the identity of legitimate devices or users to access critical systems and data. They exploit communication channels by mimicking trusted entities like sensors or operators to bypass security measures. Attackers use spoofing, weak authentication, and stolen credentials to carry out these attacks. The complexity of IIoT networks, with their diverse and interconnected devices, increases the number of entry points available for exploitation.	✓	✓	✓	✓	✓	✓	✗	✗
29	[32]	Selective forwarding attacks	In an IIoT network, a selective forwarding attack occurs when an attacker filters or discards specific packets, disrupting data flow between devices like sensors, actuators, and gateways. This manipulation can corrupt transmissions, causing incorrect decisions, system failures, or safety risks. Attackers often remain undetected, as their actions resemble normal packet loss. These attacks are difficult to detect because they mimic normal packet losses, allowing attackers to stay hidden, especially in decentralized, wireless IIoT environments. An attacker can inject malicious code into a network node, preventing data	✓	✓	✓	✓	✗	✓	✗	✗

			from reaching its destination and compromising system reliability.								
30	[32][33]	Traffic analysis attack	A traffic analysis attack involves intercepting and examining communication metadata, like timing and frequency, instead of data content. Attackers can uncover critical operational details by analyzing traffic patterns, detecting vulnerabilities, and predicting actions. This method enables attackers to target specific systems and even manipulate operations. Unlike message interception, traffic analysis reveals the nature of communication without decrypting data.	✓	✓	✓	✓	×	✓	×	×
31	[32]	Routing information attacks	Routing information attacks exploit vulnerabilities in routing protocols to disrupt communication and compromise data integrity. Attackers inject false routing data, poisoning routing tables and rerouting traffic through malicious paths. Blackhole, MitM, and Sybil attacks further destabilize networks by dropping data, intercepting exchanges, or introducing fake nodes. These attacks can lead to system downtime, data loss, and manipulation of industrial processes, posing significant risks to IIoT systems.	✓	✓	✓	✓	✓	✓	×	×
32	[81]	SQL injection attacks	SQL injection (SQLi) is a cyberattack where malicious actors exploit vulnerabilities in SQL queries to access or alter a database. In the context of IIoT, attackers can target systems managing critical data like sensor readings or production workflows. By manipulating SQL queries, they can tamper with machine settings, alter real-time data, or compromise safety protocols, potentially causing severe disruptions in industrial operations. The lack of input validation in vulnerable systems allows attackers to inject malicious data, gain unauthorized access to sensitive information, modify database structures, or delete data. In IIoT environments, such attacks can lead to system failures, downtime, financial losses, and safety hazards, impacting the organization and its users.	✓	✓	✓	✓	✓	✓	×	✓
33	[21][38]	Firmware and software vulnerabilities	Firmware, the specialized software embedded in IIoT hardware devices, can harbor flaws due to outdated or poorly written code, weak encryption, or insecure communication protocols, enabling attackers to gain unauthorized access and compromise industrial networks. Similarly, software vulnerabilities in IIoT applications, such as control systems and monitoring tools, arise from coding errors, insufficient input validation, and weak user permission management. Legacy software further increases the attack surface, while inadequate patch management and weak authentication mechanisms make it easier for attackers to exploit weaknesses. The interconnected nature of IIoT devices amplifies the impact of these vulnerabilities, as a single compromised device can trigger widespread network failures. The lack of standardized update mechanisms and the long operational lifespans of industrial systems complicate secure, real-time updates.	✓	✓	✓	✓	×	✓	✓	×
34	[37]	Insecure communication	Insecure communication occurs when data exchange between connected devices, networks, and systems lacks proper security measures. This vulnerability arises when IIoT devices, such as machines, sensors, and controllers, communicate without encryption, allowing malicious actors to intercept and expose sensitive information. As a result, attackers can exploit unsecured channels to inject malicious code or tamper with data, leading to operational disruptions, incorrect decision-making, or even physical damage to industrial assets. In many cases, IIoT devices operate in remote environments with insufficient infrastructure to support advanced security protocols, making them prime targets for cyberattacks through weak points like insecure protocols, default passwords, or outdated software. Furthermore, insecure communication protocols can compromise data integrity between physical assets and their digital twins.	✓	✓	✓	✓	✓	✓	✓	×

35	[83][102]	Buffer overflow	A buffer overflow poses a security risk when a program or device attempts to store more data in a buffer than it can manage. IIoT systems, which rely on real-time data exchange and precise control of industrial processes, are particularly vulnerable to such attacks. When the excess data overflows, it can corrupt adjacent memory or execute malicious code, potentially allowing attackers to gain unauthorized access to ICS, resulting in taking control of machines, altering sensor readings, or disrupting critical processes. The interconnected nature of IIoT devices means that compromising one device could give attackers access to others, amplifying the attack's scope. These vulnerabilities are common in SCADA systems because they use programming languages like C, which lack type safety, and the continuous operation of devices, which can cause memory fragmentation over time. As a result, buffer overflow attacks can manipulate PLC instructions and sensor data, leading to system failures or safety hazards.	✓	✓	✓	✓	×	✓	✓	✓
36	[103][104]	Backdoor	A backdoor in Industrial IoT is a hidden access point allowing attackers to bypass security measures and control devices or networks undetected. Cybercriminals, insiders, or even manufacturers may introduce backdoors, either intentionally or unintentionally, during system design, production, or operation. Once in place, these vulnerabilities enable attackers to exploit system weaknesses, steal sensitive data, and disrupt critical industrial processes. The complexity and scale of IIoT networks, combined with outdated security practices and proprietary protocols, make them prime targets. Attackers use backdoors to evade authentication, execute malicious commands, and maintain persistent access, often without triggering security alarms. Some vendors in ICS include backdoor accounts for remote support and updates, unintentionally exposing SCADA data to potential threats. Backdoor malware poses an even greater risk by remaining dormant and undetectable while providing unauthorized access to manipulate operations and compromise infrastructure. The open and interconnected nature of IIoT further increases vulnerability, making backdoor attacks particularly dangerous due to their stealthy and persistent nature.	✓	✓	✓	✓	✓	✓	✓	×
37	[37]	Cross-domain data sharing	Cross-domain data sharing enables systems such as machinery, production lines, ERP, and supply chain management to exchange data seamlessly. By breaking down data silos, this integration enhances decision-making, operational efficiency, and innovation. For instance, sensors embedded in manufacturing equipment generate data that gives businesses a holistic view of operations when shared with inventory management or enterprise analytics platforms. This connectivity supports real-time monitoring, predictive maintenance, and optimized supply chain management while bridging the gap between operational technology and IT. However, ensuring compatibility between systems remains challenging due to differing data formats, protocols, and standards. Similarly, digital twins operate within a multi-stakeholder ecosystem, creating privacy risks as data may unintentionally reach unauthorized parties or be used beyond its original purpose.	✓	✓	✓	✓	✓	✓	×	×

Confidentiality (C), Integrity (I), Availability (A), Authentication (Au), Authorization (AT), Non-Repudiation (N), Resiliency (R), Accountability (Ac)

5. CYBERSECURITY IN IIoT

Protecting industrial networks from cyberattacks, unauthorized access, and vulnerabilities is crucial for cybersecurity. Cybersecurity encompasses a range of tools, security concepts, risk management strategies, processes, technologies, and best practices designed to safeguard digital systems, networks, financial and client data, operational procedures, and intellectual property from unauthorized access, breaches, and cyber threats while managing system access through effective procedures [105][106]. Cybersecurity aims to protect information from unauthorized disclosure, modification, or destruction by monitoring physical or cloud-based computer activities for system vulnerabilities and analyzing activity patterns. Its primary focus is intrusion detection, which helps ensure secure communication, user authentication, and authorization.

The global industrial cybersecurity market is valued at US$23.5 billion in 2024. From 2024 to 2031, it will expand at a CAGR of 8.2%, propelled by disruptive digital technologies and increased cyber-attacks. This rise is further accelerated by cyberattacks' growing sophistication and frequency [107]. Cybersecurity is used in many security domains, including network, application, information, operational, disaster recovery, operational continuity, and end-user training. It is also essential for risk analysis and management, preventing fraud and attacks [108]. It is vital to protecting industrial operations against disruptions, financial losses, and safety risks. To achieve successful IIoT cybersecurity, manufacturers, cybersecurity specialists, and lawmakers must collaborate to develop security frameworks and best practices. Industries can minimize security risks and optimize IIoT benefits by implementing robust cybersecurity protocols [109]. It is essential to guarantee protection throughout the whole lifecycle of an IoT-connected environment to avoid unwanted access, changes, or data loss. An IIoT security requirement model is required to identify problems and create solutions. It is usual practice to handle security in IIoT scenarios while evaluating security requirements carefully. By locating any weaknesses and implementing the necessary fixes, this technique contributes to the safety and integrity of systems. Some of the specifically mentioned security requirements for IIoT are described below:

- *Confidentiality*: This security principle shields private data from exposure or unwanted access, especially in IIoT systems that manage large data exchanges. This data frequently contains extremely sensitive information that could jeopardize access control and have catastrophic repercussions if compromised, such as access keys, device statuses, and commercial data. By safeguarding intellectual property, business secrets, and personal information, confidentiality is crucial to maintaining the integrity of IIoT systems [11][31][46].
- *Integrity*: This security mechanism verifies the authenticity of devices and the originality of data during transmission between IIoT devices, machines, and central database servers, ensuring that devices operate as intended. It is categorized as a primary security attribute in ISO/IEC 27000 and is closely related to safety. Integrity in IIoT systems ensures the accuracy and reliability of data, making it essential for decision-making and protecting against malicious attacks. Safeguarding data transmission between devices and software prevents alterations that could lead to process failures, system shutdowns, or security breaches. Effective strategies are needed to detect unexpected changes within the IIoT system [11][31][46].
- *Availability*: This security mechanism in IIoT systems ensures that devices and services remain operational and accessible when needed, preventing disruptions to critical infrastructure. It is crucial for maintaining the continuous functionality of IIoT systems, as downtime can lead to production delays, safety risks, and financial losses. Availability can be compromised by attacks such as DoS, particularly concerning IIoT systems with resource-constrained components. Security mechanisms designed to protect IIoT systems might reduce availability to mitigate cyber threats, but this can also impact safety in these environments, creating a balance between security and operational reliability [11][31][46].
- *Authentication*: This is a key security mechanism for verifying the identity of IIoT devices, ensuring they are what they claim to be. This process is crucial for preventing unauthorized devices from accessing the IoT network and protecting the authenticity of communication and the confidentiality and integrity of exchanged data. Lightweight MFA is essential in IIoT environments, where data security, quality of service, and factors such as low latency and limited computing resources must be considered. The mobility, scalability, and heterogeneity of IIoT devices also make it challenging to identify suspicious devices, and malicious devices can cause serious consequences. Therefore, a robust authentication mechanism maintains availability, resiliency, and safety in IIoT systems [11][46].
- *Authorization*: This security attribute ensures that access rights to devices and assets are managed, limiting access to privileged devices. Vulnerabilities can compromise these security controls, potentially exploiting IoT devices beyond their authorized privileges [11].
- *Non-repudiation*: This security property ensures that the sender of a message or digital transaction cannot deny sending or engaging in it. It proves communication and prevents individuals from disowning their actions, thereby maintaining trust and accountability in digital interactions. In the context of privacy, non-repudiation guarantees secure transmission by confirming the sender’s identity and bringing proof of delivery to the recipient. While not always considered critical for IIoT systems, non-repudiation is essential in certain areas, like payment systems, to prevent later denial of involvement in a transaction. IIoT security frameworks ensure that entities cannot deny their actions [11].
- *Recovery*: This security attribute ensures availability and safety in IIoT systems by focusing on security mechanisms that restore devices or services from a dead state to regular operation, either automatically or manually. A replica runs alongside the main components in critical applications, enabling recovery if the primary system fails due to vulnerabilities or security breaches. Incident response and recovery mechanisms are essential for safeguarding

critical IIoT infrastructure, with development relying on thorough risk estimation, vulnerability analysis, and understanding cascading impacts on assets. It is recommended that the replica system be physically isolated from the primary system and kept updated and maintained. [11]

Cybersecurity is critical in IIoT systems due to the increasing interconnectivity of devices, networks, and systems. One of the main justifications for strong cybersecurity is protecting sensitive data. Industrial trade secrets, operational data, and personal information are among the many types of data that IIoT systems gather and send. Organizations may preserve privacy and the integrity of critical data by implementing robust cybersecurity safeguards to stop theft, tampering, disclosure, and unauthorized access. Preserving operational continuity is another crucial element. Numerous IIoT implementations are essential in industrial and critical infrastructure contexts where interruptions could have dire repercussions. To maintain the stability and dependability of crucial services, cybersecurity guards against illegal access, manipulation, or disruption of IIoT devices and systems, guaranteeing seamless and continuous operations. Cybersecurity reduces monetary losses. Significant financial harm, such as financial fraud, intellectual property theft, system outages, or fines from the government for noncompliance, can be caused by cyberattacks on IIoT systems. Businesses can lower these financial risks and lessen the effect of cyber threats on their bottom line by putting strong cybersecurity procedures in place [48].

Furthermore, safeguarding user privacy is a significant issue. Sensitive data, including location, health, and personal habits, is frequently collected by IIoT devices. Secure data storage, user authentication, encryption, and other effective cybersecurity techniques guarantee that private data is kept private and shielded from unwanted access. Maintaining reputation and trust requires cybersecurity. An IIoT cybersecurity issue can harm trust in the technology and the companies using it. Businesses may improve their reputation and promote the ongoing adoption of IIoT solutions by showcasing a strong commitment to cybersecurity and earning the trust of users, clients, and partners. Safety is crucial in some IIoT applications, including ICS, medical equipment, or driverless cars. IIoT systems' cybersecurity flaws may result in accidents, bodily injury, or even fatalities. Strong security measures can be put in place by companies to reduce these dangers and contribute to community and individual safety. Lastly, it is imperative to address the changing threat scenario. Due to the frequent emergence of new attack channels, vulnerabilities, and advanced methodologies, cybersecurity threats are constantly evolving. To detect and manage these new dangers and reduce the possibility of harm, constant observation, threat intelligence, and prompt updates are crucial [48].

5.1. Overview of current security technologies in IIoT

Because of automation and widespread device connectivity, security in IIoT environments is crucial as the industrial sector transitions to a smart manufacturing era driven by 5G, AI, and cloud computing [86]. Security measures are essential to avoid losses and operational disruptions [115]. In addition to Blockchain techniques like Proof of Behavior Trust (PoBT) for quick block verification and ML techniques like Support Vector Machines (SVM) for attack detection and Q-learning for eavesdropping prevention, there are also lightweight encryption algorithms like Rivest–Shamir–Adleman (RSA), Data Encryption Algorithm (DES), and AES [116-118]. Firewalls, tokenization for device authentication, access control, and data auditing are further precautions [65].

Traditional security measures frequently fall short because IIoT networks are dynamic and decentralized. These systems must be secured using next-generation solutions that increase security, scalability, and resilience as cyber-attacks become more sophisticated. To tackle the unique challenges IIoT presents, AI, Blockchain, and quantum cryptography provide solid solutions that fortify existing security frameworks and introduce fresh ideas.

6. ARTIFICIAL INTELLIGENCE IN IIoT

The expansion of IIoT networks and their data are too significant for traditional security solutions to handle. However, AI-driven techniques improve cybersecurity across various industrial areas by processing and analyzing data rapidly. Artificial intelligence is the subset of computer science that develops intelligent robots, gadgets, and sensors to solve cognitive problems associated with human intellect. These systems can recognize patterns and images, learn, solve problems, detect their environment, and understand natural language [111][114][119]. AI enhances security by turning raw data into valuable intelligence. AI IIoT systems interact with their environment, analyze data, and make decisions independently or with a certain amount of autonomy to benefit society. These systems generate cognitive processes using mathematical formulas, computer models, and algorithms that mimic the functioning of the human brain. By instantly learning from enormous datasets, AI can spot patterns, predict future states, and spot anomalies without explicit programming for specific tasks. Thanks to ML, DL, NLP, RL, FL, and transfer learning (TL), AI can analyze enormous volumes of data collected by IIoT. By automating repetitious tasks, enhancing decision-making, and retrieving insightful data, these technologies ultimately improve work environments while saving time and money [112][120]. AI-driven security solutions are crucial to IIoT cybersecurity because of their rapid threat identification, assessment, and mitigation capabilities. By identifying and resolving complex cyber threats, ML, DL, NLP, RL, FL, and TL enhance IIoT cybersecurity. These AI algorithms analyze big datasets from multiple sources, spotting strange trends and anomalies that could indicate malicious behavior. These methods support anomaly detection, behavioral analysis, and neural networks while securing connections, detecting malware, and analyzing network data. AI strengthens IIoT systems, ensuring data availability, confidentiality, and integrity in increasingly complex environments. [47][52][121][122]. Fig. 8 summarizes the AI techniques for securing IIoT.

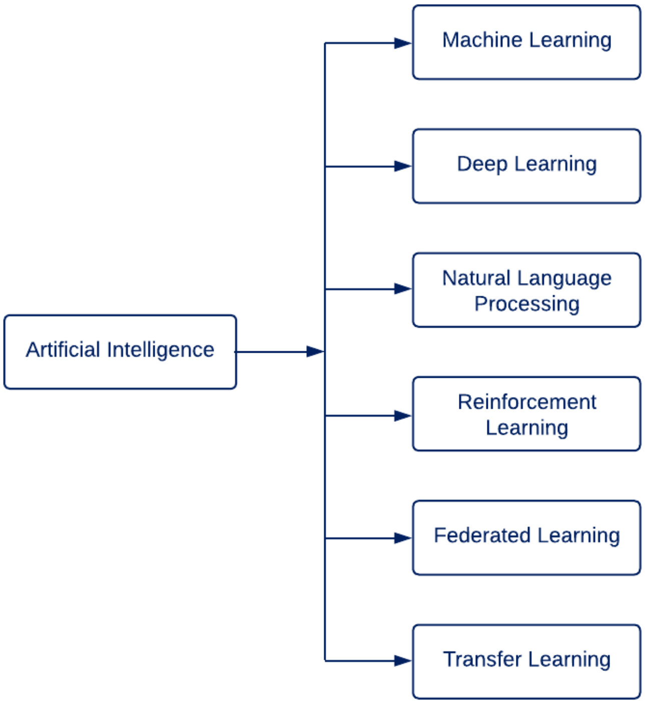

Fig. 8. Summary of AI techniques for securing IIoT

6.1. Machine learning

Machine learning generates statistical models and algorithms without explicit programming, enabling computers to learn from data independently, identify hidden patterns, and make predictions. ML employs complex statistical models and computational techniques to assess big datasets, enhance pattern identification and decision-making [110][111]. ML systems continuously improve performance by learning from training data through data mining, computational statistics, and mathematical optimization. As these systems process more data, they become more accurate predictors and can automate tasks previously done by humans. The four fundamental subcategories of ML—supervised, unsupervised, semi-supervised, and reinforcement learning—each provide distinct approaches to solving complex problems [112-114]. ML can be used to detect, prevent, and mitigate cyber threats. ML algorithms analyze large datasets to look for patterns and anomalies that could indicate hostile activity. While supervised learning models, which have been trained on prior attack data, identify known threats, unsupervised models detect new anomalies and provide preventative security measures. By spotting suspicious activity, clustering and classification techniques enhance network security, intrusion detection, and traffic monitoring. ML enhances cybersecurity through phishing detection, malware analysis, endpoint security, and identity and access management [121]. ML-driven security solutions keep up with the changes in cyber threats, increasing their efficacy in protecting infrastructure and digital assets. However, their effectiveness depends on various training datasets, which can provide difficulties when applied in the real world. ML algorithms reduce service interruptions in vital infrastructure like transportation networks, water systems, and power grids by analyzing past performance data and identifying early warning indicators of equipment failures. ML improves traffic control by anticipating traffic patterns, maximizing signal timings, and spotting anomalous traffic conditions to increase road safety. To identify and stop new cyber threats, ML-driven intrusion detection systems continuously learn from fresh data by examining network traffic and system logs for anomalies [122]. Supervised learning models like ensemble bag trees, K-nearest neighbors (KNN), decision trees (DT), SVM, and random forests (RF) identify cyber anomalies using labeled data in industrial environments [96]. At the same time, unsupervised techniques such as clustering and autoencoders detect threats without predefined labels. ML strengthens security frameworks by adapting to evolving attack scenarios, offering proactive defense mechanisms against sophisticated cyber threats [123].

6.2. Deep learning

Deep learning automatically extracts features from large amounts of raw data using artificial neural networks with several processing layers. Without explicit programming, these networks improve performance, solve complex issues, and represent complex relationships [110][111]. Neural networks are used to process and analyze various types of data. DL design includes input, hidden, and output layers. Data travels through hidden levels for processing before arriving at the output layer. DL's layered structure makes it highly successful at processing high-dimensional data, enabling it to spot intricate patterns. DL removes manual feature engineering by automatically learning hierarchical features, but it still demands a lot of computing power despite its remarkable accuracy. Its application in data analysis, prediction, and decision-making has increased due to its ability to extract complex features from raw data [112][114]. DL has revolutionized cybersecurity by effectively evaluating enormous datasets and identifying intricate risks that conventional techniques frequently overlook. Recurrent neural networks (RNNs) and convolutional neural networks (CNNs) effectively identify sophisticated attack techniques and zero-day vulnerabilities. DL-based intrusion detection systems (IDS) employ designs such as gated recurrent units (GRU), bidirectional long short-term memory (BI-LSTM), and LSTM to identify cyber threats in industrial IoT contexts accurately [96][124]. DL enhances security in several domains, including user authentication, malware detection, phishing prevention, and network traffic anomaly detection. It can learn from enormous volumes of unstructured data, strengthening cybersecurity defenses, reducing false positives, and increasing detection rates. DL-powered security frameworks in AI-driven IIoT enhance public safety by identifying suspicious activity, identifying unauthorized access, and preventing security breaches. DL significantly improves intelligent urban environments by optimizing traffic control systems and enhancing cyber resilience. DL models predict traffic jams, improve vehicle flow, and optimize traffic light timings using information from traffic sensors and past patterns. These characteristics enhance urban mobility and reduce inefficient travel. Despite its advantages, DL deployment in IIoT and cybersecurity applications is not without its difficulties. Deep neural networks need a strong hardware infrastructure and much processing power to train and run. Since deep learning models frequently operate as "black boxes," it might be challenging to understand how they make decisions. Optimizing these models is crucial for maximizing their potential while addressing their limitations. Researchers can improve model transparency and performance by enhancing efficiency and balancing computational requirements [121][122][125].

6.3. Natural Language Processing

Natural language processing is a rapidly evolving field of AI that enables machines to comprehend, analyze, and alter human language [110][111]. Driven by the proliferation of online material, NLP employs techniques such as sentiment analysis to process and assess text effectively. Its two primary components are natural language generation (NLG), which enables machines to generate coherent text, and natural language understanding (NLU), which aids machines in understanding human language. Companies use supervised and unsupervised NLP algorithms to evaluate communication through emails, social media, and multimedia content. NLP technologies are essential to efficiently operating voice assistants, speech-to-text software, machine translation, and text production. These include ML-based strategies that find patterns in big datasets and rule-based tactics that rely on manually created rules. Because it retrieves valuable information from unstructured data, NLP is essential for speech recognition, machine translation, sentiment analysis, and text summarization. Language processing and data retrieval are improved by algorithms like named entity recognition (NER), tokenization, and word embeddings [112][114]. Modern cybersecurity tactics now require NLP because it helps companies identify, stop, and react to attacks. NLP assists in identifying phishing attempts, preventing social engineering attacks, and detecting malware by evaluating large amounts of communication data. It facilitates identity and access management, incident response automation, and behavioral analysis. By enabling quicker and more precise threat identification, these features strengthen IIoT cybersecurity defenses. NLP-driven developments will improve security protocols and give enterprises more powerful tools to protect their digital assets as cyber threats change [121].

6.4. Reinforcement learning

Reinforcement learning, a subfield of ML, allows agents to make decisions by interacting with their surroundings to receive or maximize rewards and penalties. Agents can identify the most effective tactics to optimize long-term gains by using this trial-and-error method [110][111]. RL agents adjust their behavior over time based on performance feedback rather than explicit instructions. Algorithm designers create reward systems that encourage desirable actions and discourage undesirable ones. This approach excels in decision-making, control, and optimization tasks that require sequential data acquisition. It includes model-based, value-based, and policy-based methods. Model-based RL builds a virtual representation of the environment for exploration, value-based RL optimizes decision-making by determining the best value function, and policy-based RL directly refines the agent's policy to maximize future rewards. Q-learning, Deep Q-Networks (DQN), SARSA, Dyna-Q, and Monte Carlo Methods are the most widely used RL algorithms [112][114]. RL handles dynamic and complex cybersecurity security challenges. It powers adaptive intrusion detection systems that evolve alongside emerging threats and optimizes resource allocation to address critical security risks efficiently. RL-driven threat intelligence platforms continuously analyze data from various sources, recognizing patterns to anticipate and mitigate potential cyberattacks. By integrating RL, organizations can enhance intrusion detection, network security, malware defense, access control, and incident response, strengthening their ability to protect digital assets. RL's role in cybersecurity will expand as cyber threats evolve, driving innovation and improving security strategies across industries. Beyond cybersecurity, RL supports industrial initiatives by optimizing urban transportation and energy management. For instance, RL algorithms analyze real-time traffic patterns to adjust signal timings, reducing congestion and improving traffic flow. By constantly learning from new data, RL helps transportation networks become more efficient, shortening travel times, enhancing road safety, and enabling cities to respond dynamically to changing conditions. These applications demonstrate RL's ability to tackle complex problems, continuously improving to create more adaptive and intelligent systems over time [121][122].

6.5. Federated Learning

Federated learning allows for collaborative training while maintaining privacy by training ML models on decentralized data instead of transferring it to a central server [110]. Because local servers or devices contribute to a standard model while maintaining data, this method is beneficial for IIoT scenarios. FL improves security and privacy by reducing data transit and centralization [31]. Enabling collaborative intelligence in IIoT systems to identify and stop cyberattacks guarantees safe industrial operations. Each IIoT device generates adversarial data by running a deep neural network locally to retrain the threat model. After the device gathers and synchronizes the trained gradient with further modifications, it is transmitted to a cloud server. The model converges across several transmission cycles to efficiently identify threats. FL is taking IoT ML beyond IIoT by allowing devices to train a single model while protecting consumers' private data. This decentralized method protects privacy when connected devices, such as wearable health data, location data from smart transportation systems, and security camera surveillance footage, produce sensitive data. FL lowers privacy risks and improves compliance with regulations like GDPR because it processes data locally. It decreases congestion and increases network efficiency by reducing data flows.

6.6. Transfer learning

Transfer learning in the IIoT refers to using knowledge from previously trained models that have been trained on data from one IIoT domain to improve performance in a different but related IIoT domain. Model deployment is expedited by utilizing patterns and features in comparable industrial contexts or activities and optimizing data consumption. TL allows models to quickly and accurately adapt to new, real-world industrial contexts, which is useful when labeled data is limited. TL is helpful for manufacturing process optimization, anomaly detection, and predictive maintenance since it minimizes the time and training data required for new tasks. Using pre-trained models to extract pertinent information from adjacent domains increases productivity and reduces the requirement for substantial additional data collection [122]. IIoT cybersecurity and industrial system performance are enhanced via TL. IIoT environments produce enormous volumes of heterogeneous data due to sensors, linked devices, and industrial processes. TL improves quality control, anomaly detection, and predictive maintenance while tailoring pre-trained models to specific industrial scenarios while increasing system accuracy and efficiency. It optimizes resource allocation, decreases downtime, and speeds up failure detection. By improving threat detection and response systems, it fortifies cybersecurity. Beyond IIoT, TL supports smart cities by enhancing security systems with quicker deployment and less data. It enhances traffic control and energy usage using pre-trained models adapted to new city problems. This results in more precise forecasts and better resource allocation [122].

6.7. Roles of AI in Securing IIoT

Artificial intelligence is essential to ensuring IIoT security in several ways, including:

6.7.1. Intrusion detection and prevention

Artificial intelligence- and ML-powered modern IDSs protect against cyberattacks by detecting anomalies and malicious behavior. They have an advantage over conventional security techniques due to their capacity to recognize zero-day threats. These systems use various ML techniques, such as DL architectures like CNN, RNN, and multilayer perceptrons, and classical models like Naïve Bayes, DT, RF, SVM, and gradient boosting [44][47]. However, the appropriate classifiers for this application are debatable. These systems get better over time as they adjust to new threats. For example, DL models increase the accuracy of identifying possible intrusions while decreasing false positives. IDS and IPS are better at detecting and stopping attacks because RL allows them to adjust to changing threats based on real-time data. RL can optimize configuration management and resource allocation while continuously altering detection and prevention rules and maintaining network security. Because AI-powered IDS monitor vast volumes of real-time data to identify unexpected threats, they are highly advantageous in industrial settings [121]. AI-based IDS uses ML and DL algorithms to identify new and established threat trends. The CNN approach examines network traffic to identify anomalies in time series. Cyber threat identification accuracy is increased by hybrid DL models that include supervised and unsupervised learning [126]. For example, AI-driven IDS may monitor SCADA systems for possible breaches in industrial automation and detect anomalous power consumption or unauthorized access in smart grids [48]. SVM aids in the prevention of cyber threats by detecting spoofing attempts and network intrusions [127]. This AI-based strategy enables early detection and a proactive response to changing security threats.

Some research studies that employed AI to prevent and detect intrusions in IIoT include. Kaur [20] developed an FL-based intrusion detection model for IIoT networks that only exchanges learning parameters with the central server to protect local data. The model uses GRUs to improve detection accuracy and capture temporal dependencies in network traffic. Deep RL improves FL aggregation by selecting high-quality IIoT devices while prioritizing data privacy and energy efficiency. Unlike previous methods, this approach considers non-IID data in modern IIoT datasets. Experimental results show that the framework outperforms FL and non-FL models in accuracy, precision, recall, F1-score, and receiver operating characteristics

(ROC). Rehman et al. [30] introduced a Fog-enabled FL-based IDS (FFL-IDS) that uses a CNN to address jamming and spoofing attacks in IIoT environments. The system enhances privacy, scalability, and real-time detection by combining FL and fog computing. It achieves high accuracy and efficiency through localized CNN training on edge devices and model aggregation at the fog layer. The Edge-IIoTset dataset achieved 93.4% accuracy, 91.6% recall, 88% precision, 87% F1 score, and 87% specificity for jamming and spoofing attacks. The system showed better robustness on the CIC-IDS2017 dataset, achieving 95.8% accuracy, 94.9% precision, 94% recall, 93% F1 score, and 93% specificity. Maddu [128] proposed an intrusion detection and mitigation framework for Software-Defined Networking (SDN)-based IIoT environments, using EfficientNet-B0 for domain-adapted feature extraction and incremental learning with Elastic Weight Consolidation to retain knowledge while adapting to new threats. The framework utilizes Simple Contrastive Learning (SimCLR) to generate robust embeddings, autoencoders for anomaly detection, and XGBoost for classifying known threats. Deep Q-Learning optimizes real-time mitigation, while Tiny-YOLO ensures low-latency anomaly detection in edge deployments. It achieves a detection accuracy of 96.8% on the CICIDS2017 dataset, with a precision of 95.4%, a recall of 94.7%, and an F1-score of 95.0% on the Bot-IoT dataset. The framework also demonstrates robustness over highly imbalanced datasets, with an AUC of 97.5% and a minimal false positive rate of 2.7%. Awad et al. [129] developed and evaluated a well-optimized IDS based on DL and ML techniques to enhance IIoT security. They used the Edge-IIoTset dataset to detect and mitigate 14 attack types across five threat groups: information collection, malware, DDoS, MitM, and injection attacks. Their experiments on the KNIME platform applied KNN, DT, and a neural network. The DT model achieved 100% accuracy, showcasing the approach's effectiveness. This study highlights a robust solution for securing industrial IoT networks.

Yang et al. [130] proposed an intrusion detection method that integrates an attention mechanism, Bidirectional GRUs (BiGRU), and an Inception-CNN to improve detection accuracy. The method utilizes a mixed sampling strategy for data resampling and applies denoising techniques to address noise introduced by hybrid sampling. The approach incorporates a feature selection method combining the Pearson correlation coefficient and RF to eliminate feature redundancy, enhancing the model's ability to capture crucial information from high-dimensional attack traffic. Experimental validation on widely recognized datasets (Edge-IIoTset, CIC-IDS2017, and CIC IoT 2023) confirms the effectiveness of the proposed method, highlighting its potential to improve intrusion detection in the security of IIoT networks. Yu et al. [44] proposed the DC-IDS for IIoT, an open-set solution based on deep RL. They modeled the open-set recognition problem in intrusion detection as a discrete-time Markov decision process and used a deep DQN to address it. Additionally, they introduced a conditional variational autoencoder into the value network of DQN. This approach divides the open-set recognition problem into two subproblems: fine-grained classification of known traffic and recognition of unknown attacks. DQN solves the known traffic classification, while the reconstruction error helps recognize unknown attacks, as it is generally higher for unknown attacks. Experiments on the TON-IoT dataset showed that the DC-IDS model outperforms previous methods, achieving better recognition of unknown attacks and more excellent model stability. Angelin and Priyadharsini [131] proposed a DL-based network IDS to identify attacks in IIoT environments. Their model enhances the effectiveness of Network IDS (NIDS) by combining CNN with AutoEncoder (AE) techniques. The autoencoder reduces data features, while CNNs automatically extract complex patterns and features from network traffic data. The hybrid model delivers strong performance on the Edge_IIoT dataset, achieving 92.34% accuracy, 91.69% precision, 90.28% recall, and an F1 score of 89.08%. Rehman et al. [30] introduced a Fog-enabled FL-based IDS (FFL-IDS) that leverages a CNN to address key limitations in IIoT network security. The framework enables multiple parties to train DL models while preserving data privacy and ensuring low-latency detection through fog computing. Validated on two datasets—Edge-IIoTset, designed for IIoT environments, and CIC-IDS2017, which features various network scenarios—the FFL-IDS achieved impressive results. On Edge-IIoTset, it reached 93.4% accuracy, 91.6% recall, 88% precision, 87% F1 score, and 87% specificity for jamming and spoofing attacks. CIC-IDS2017 showed even better robustness, with 95.8% accuracy, 94.9% precision, 94% recall, 93% F1 score, and 93% specificity.

Shan et al. [36] developed a clustered FL framework for IIoT intrusion detection (CFL-IDS) that leverages local models' evaluation metrics (EMs). They designed an intrusion detection model with dynamic focal loss (DFL) for edge nodes (ENs), enhancing performance in scenarios with imbalanced data by dynamically adjusting the focus on samples during loss minimization training. The time series of EMs from local models implicitly reflect ENs' data distributions, allowing clustering algorithms to group ENs with similar distributions and facilitate knowledge sharing. This process helps co-optimize a common model for these ENs. An intelligent cooperative model aggregation mechanism (ICMAM) adjusts the weight distribution of each local model, improving the benefits of FL and reducing the impact of subpar models. Experiments show that CFL-IDS demonstrates superior robustness and performance in handling data imbalance, non-IID scenarios, and resistance to poisoning attacks. Yalçın et al. [132] developed an AI-based IDS with high accuracy for SCADA security, examining potential cyberattacks against SCADA systems. They employed various AI methods, including KNN, quadratic discriminant analysis, adaptive boosting, gradient boosting, and RF, using different categories to build models with diverse parameters. They conducted comprehensive experiments on two distinct SCADA datasets to enhance model performance. The results showed that all models achieved test accuracy rates above 96.82%, with the XGB model outperforming others on the WUSTL-IIOT-2021 dataset, reaching an impressive accuracy of 99.99%. Attique et al. [133] propose an explainable and intelligent IDS for data-efficient intrusion detection in IIoT. Their framework integrates a Bidirectional Long-Short Term

Memory (BiLSTM) model with a self-adaptive attention mechanism that prioritizes critical data segments to detect security threats. This approach enhances learning from limited datasets by capturing significant features and temporal patterns, reducing the need for extensive training data. The IDS also improves transparency by incorporating Shapley Additive exPlanations (SHAP), increasing trust and interpretability. It achieves outstanding accuracy on CICIDS2017 (99.92%) and X-IIoTID (96.54%) benchmark datasets. Jyothi et al. [134] proposed an intelligent recognition system to detect cyberattacks in IIoT networks, addressing key challenges in the field. The system uses singular value decomposition to reduce data dimensions and improve detection performance. The SMOTE method is applied to prevent classification biases caused by overfitting or underfitting. The model, which uses ML and DL approaches to classify data for binary and multi-class scenarios, demonstrated a 99.98% accuracy rate, a 0.016% error rate reduction for multi-class classification, and a 0.001% error rate reduction for binary classification.

6.7.2. Anomaly and cyberattack detection and classification

By identifying time series data anomalies from normal behavior, anomaly detection uses statistical analysis to find possible risks [135]. By learning the expected behavior, these algorithms can identify variations that point to security vulnerabilities. This method successfully detects new threats that diverge from established attack patterns. Anomaly detection in the IIoT aids in spotting odd trends that may indicate cybersecurity threats, network outages, or device issues. AI-driven models use supervised and unsupervised learning approaches to assess real-time sensor data, identify patterns, and highlight problems. Supervised learning uses labeled datasets to teach AI models how to categorize anomalies based on past data. These models differentiate between risky and safe events using classification techniques. For example, manufacturing predictive maintenance systems use SVMs and RF algorithms to analyze sensor data and identify equipment flaws. Without using samples that have already been classified, unsupervised learning finds abnormalities in data. Autoencoders, k-means clustering, and numerous more algorithms can identify unknown or rare threats. For example, autoencoders can detect network intrusions by detecting normal traffic patterns and irregularities that point to malicious behavior [121]. DL models, such as RNNs and LSTM networks, examine sequential data to identify system flaws or degradation. These models can predict industrial equipment failures by monitoring sensor data like temperature and pressure. CNNs can be applied to visual data, such as camera feeds, to identify defects in manufacturing processes. These techniques enhance anomaly detection by continuously monitoring device operations and network behaviors, enabling the swift identification and mitigation of threats. For example, AI can detect unusual data spikes in network traffic, which may indicate DDoS attacks [122]. AI-based anomaly detection provides continuous monitoring and quick threat identification, offering enhanced protection against cybersecurity risks. It helps spot insider threats, zero-day attacks, and abnormal behavior that might signal a breach [48][121][136]. Real-time monitoring allows security teams to automate responses, reducing the time to neutralize threats. Technologies like Darktrace and IBM Watson use ML and DL to track network activity, detect deviations, and provide insights into emerging threats [137]. Principal component analysis (PCA) and DT detect anomalies by simplifying complex data and improving pattern recognition. These AI-driven solutions ensure robust defenses against evolving cyber threats in IIoT systems [138].

Notable research studies that employed AI in anomaly and cyberattack detection and classification include Zeng et al. [124], who introduced EvoAAE, an innovative automated adversarial DL-based unsupervised anomaly detection method designed to secure IIoT systems. EvoAAE optimizes the hyperparameters and neural architectures of adversarial variational autoencoders (VAE) by employing a generative adversarial network-based VAE to generate multivariate time series adversarially. The method uses particle swarm optimization with an efficient binary encoding strategy to evolve key elements in the VAE. Experimental results show that EvoAAE performs exceptionally well across four IIoT datasets from industrial control domains—secure water treatment, water distribution, Mars Science Laboratory, and power systems—achieving precision scores of 0.949, 0.8356, 0.972, and 0.981, recall scores of 0.971, 0.9214, 0.964, and 0.979, and F1-scores of 0.960, 0.8764, 0.968, and 0.980, respectively. Karim et al. [139] proposed the Bayesian ML with the Sparrow Search Algorithm for Cyberattack Detection (BMLSSA-CAD) technique, which enhances cyberattack detection in IIoT networks by normalizing input data using a min-max scaler and selecting optimal features with the Chameleon Optimization Algorithm (COA). It utilizes a Bayesian Belief Network (BBN) model, with hyperparameters optimized through the Sparrow Search Algorithm (SSA). The technique was tested on the UNSWNB51 and UCI SECOM datasets, achieving accuracy rates of 97.84% and 98.93%. Experimental results demonstrated that BMLSSA-CAD outperforms recent IIoT security approaches. Chen et al. [140] proposed an optimal DL model, MIX_LSTM, for anomaly detection in the IIoT. They first applied XGBoost for feature selection, retaining important features above a chosen threshold and reducing dimensionality to save computational resources. Next, they optimized the loss function to address issues such as imbalanced data, highly similar categories, and model training. In experiments on the UNSW-NB15 and NSL-KDD datasets, the MIX_LSTM model achieved 0.084 FAR, 0.984 AUC-ROC, and 0.988 AUC-PR on UNSW-NB15, and 0.028 FAR, 0.967 AUC-ROC, and 0.962 AUC-PR on NSL-KDD. The model outperformed traditional DL and ML models and existing technologies for detecting abnormal attacks in IIoT. Alkhafaji et al. [125] proposed a novel detection and classification model designed explicitly for IIoT environments, integrating Genetic Algorithms (GA) and DL to enhance cyber-attack detection. The GA optimizes feature selection from raw network data, extracting meaningful and relevant features, which the DL component then uses to build a robust model for accurately detecting and classifying cyber-attack patterns in IIoT devices. Experimentation with the

UNSW-NB 15 dataset, representing real-world IIoT network traffic, demonstrated the model's effectiveness in improving attack detection accuracy and adaptability. By combining GA and DL, the model achieved 98% precision, 96% accuracy, 94% recall, and 12% loss while reducing the feature set by over 50%, cutting processing time by half. This integrated approach enhances cybersecurity in IIoT systems, making them more secure and efficient.

Miryahyaei et al. [141] introduced the focal causal temporal CNN (FCTCNN), a cutting-edge deep binary neural network designed to address the challenges of imbalanced data in detecting rare attacks within IIoT systems. By transforming attack detection into a binary classification task, FCTCNN prioritizes minority attacks using a descending-order strategy within a tree-like structure, significantly reducing computational complexity. This approach outperforms existing methods in handling imbalanced data in rare attack detection for IoT security. Evaluations on various datasets, such as UNSW-NB15, CICIDS-2017, BoT-IoT, NBaIoT-2018, and TON-IIOT, show an accuracy exceeding 99%, proving the model's effectiveness in both detecting attacks and efficiently managing imbalanced IoT data. Kim et al. [142] proposed a DL method to train periodic data acquisition sequences, a common characteristic of IIoT. The trained model determines whether a packet sequence is normal, and the technique can be applied directly without additional analysis. This approach aims to prevent security threats by proactively detecting cyberattacks. The researchers collected a dataset from the Korea Electric Power Control System to validate the method. The model based on the application layer achieved an accuracy of 79.6%, while the transport layer-based model reached 80.9%. In both models, most false positives and false negatives occurred when abnormal packets appeared within a sequence. Arsalan et al. [143] introduced a one-dimensional CNN (1DCNN) algorithm for classifying cyberattacks in IIoT data. They began by preprocessing the data, removing NaN and duplicate values, before developing and training the 1DCNN on the Edge-IIoTset. The proposed architecture achieved an impressive 99.90% accuracy in classifying nine types of attacks. Through rigorous experimentation and validation, they demonstrated that their approach outperformed existing methods in detecting cyber threats. Idouglid et al. [123] introduced an advanced intrusion detection model to strengthen Industry 4.0 systems against evolving cyber threats by integrating ML and DL algorithms. The study used two primary benchmarking datasets—CIDDS and BoT-IoT—and four algorithms: MLP, KNN, XGBoost, and SVM. XGBoost emerged as the top performer on the CIDDS dataset, achieving exceptional accuracy (99.93%), precision (99.90%), F1-score (99.82%), and recall (99.82%), showcasing its ability to classify both benign and malicious instances effectively. MLP also demonstrated strong results with an accuracy of 99.26%. SVM and K-NN performed slightly less effectively, indicating areas for improvement. On the BoT-IoT dataset, all algorithms delivered outstanding results, with XGBoost again achieving near-perfect accuracy (99.99%) and excelling in threat detection.

6.7.3. Botnet attack classification and detection

Botnets are among the most advanced and dangerous cyberattacks. They can paralyze networks by deploying malware to exploit weaknesses in connected devices and networks. IIoT devices are especially susceptible to such attacks [50]. These botnets typically consist of compromised devices, or "bots," that cybercriminals remotely control to execute malicious activities like DDoS attacks, data theft, or disruption of industrial processes. Detecting and classifying these attacks is vital for preventing significant harm to industrial systems. Network traffic monitoring can help find abnormal patterns, such as odd traffic volumes, sudden spikes, or irregular communication behaviors that can point to botnet activity. To discover attack signatures and classify possible threats, AI-driven models are increasingly being utilized to classify these attacks according to their traffic irregularities and behavioral patterns. Real-time analysis, adaptive learning, and anomaly detection driven by AI improve detection accuracy and tackle issues brought on by the enormous number of IIoT devices and the dynamic nature of botnets. IIoT systems use anomaly detection, signature-based identification, and ML approaches to identify botnet attacks. Anomaly detection systems establish a baseline of typical device behavior to alert management to any notable anomalies, such as strange network traffic or irregular command patterns. Large data sets can be examined using ML and DL techniques, which spot complex attack patterns that conventional approaches overlook. SVM, K-NN, XGBoost, RF, and DT are effective methods for classifying botnet traffic. ML algorithms can distinguish between legitimate and botnet data by monitoring device actions over time. More sophisticated methods combine anomaly-based and signature-based algorithms with ML and DL to boost accuracy, reduce false positives, and expand scalability. In IIoT environments, AI-driven IDS use methods like LSTM networks and Autoencoders to monitor traffic and detect deviations. For example, an IDS using LSTM models in a smart factory can identify DDoS attacks by recognizing traffic spikes. In a smart energy grid, AI systems can detect abnormal data patterns in smart meters, isolating compromised devices to prevent further damage. Alrumaih and Alenazi [144] propose ERINDA, a novel framework to enhance industrial network resilience against DDoS attacks. It employs a two-phase approach that combines proactive monitoring and reactive response mechanisms. The framework monitors network traffic for anomalies and activates responses when an attack is detected, minimizing downtime. ns-3 simulations of a small-scale industrial network show that ERINDA recovers about 88% of normal throughput during a DDoS attack at 25% channel utilization, compared to a 77% reduction without ERINDA. ERINDA also restores packet delivery ratio and round-trip delay values to near-normal conditions under varying traffic loads. Hasan et al. [50] introduced a hybrid intelligent DL mechanism to protect IIoT infrastructure from complex and lethal multi-variant botnet attacks using LSTM-Deep Neural Networks (LSTM-DNN). They proposed a novel, flexible, adaptive hybrid DL algorithm combining DNN-LSTM. This mechanism underwent rigorous evaluation using the latest dataset, standard and extended performance metrics, and current DL benchmark algorithms, with cross-validation to ensure robust results. The approach successfully identified multi-variant sophisticated bot attacks with a 99.94% detection rate and achieved a speed efficiency of 0.066 milliseconds, demonstrating its promising performance. Mudassir et al. [145] proposed high-performing DL models for classifying botnet attacks that commonly target IIoT devices and networks. Their evaluation shows that models like the ANN, LSTM, and GRU can achieve up to 99% accuracy in detecting IIoT malware attacks.

6.7.4. Malware detection and classification

Malware is any program that disrupts or negatively impacts regular operations. New malware varieties appear daily, resulting in more complex and varied attacks. Cybersecurity is a significant concern because malware constantly changes, and security risks extend into industrial automation. IIoT systems need to be private and secure because cybercriminals target devices that are highly connected but susceptible [68]. ML algorithms examine how files and apps behave to find harmful activities. Patterns like file access sequences, network connections, and system modifications are found through behavioral analysis. By examining these traits, ML models can detect novel malware variants without depending on pre-existing signatures. To increase detection accuracy and adjust to new threats, ML models are constantly learning from fresh malware samples [48]. Supervised learning algorithms are trained on pre-existing malware datasets to categorize new malware according to resemblances to established threats [126]. Researchers have shown that the detection rates of malware in IoT devices were 99.7% and 99.9% for RF and KNN-based classification approaches, respectively. One study presented MARWIIoT, a genetic-KNN-based ML model to identify fraudulent activity in water-based industrial IoT situations. By enhancing malware identification, Q-learning improves IoT security [127]. DL is an effective cybersecurity method that simplifies malware detection by eliminating the requirement to extract features from images [146]. While CNNs and RNNs effectively assess data attributes and behaviors to detect dangerous software, traditional signature-based approaches find it challenging to keep up with emerging threats. CNNs successfully identify malicious code because they can identify spatial patterns in binary file structures. In contrast, RNNs analyze sequential data and spot network and system traffic irregularities, frequently pointing to malware activity. DL models concentrate on behavioral detection, identifying malware by its actions rather than examining a program's code. These algorithms are trained on enormous databases of safe and dangerous samples to find patterns of behavior linked to malware. By contrasting learned patterns with present actions, DL models can identify harmful activities after they have been trained [126]. By identifying patterns in big datasets of phishing emails, URLs, and malware samples, neural networks like CNNs and ANNs can reliably identify malware and phishing attacks. Similarly, SVMs and CNNs use attributes from URLs, email headers, and network data to categorize malware and phishing [138].

NLP also aids in the detection of malware by examining threats based on code and scripts. Using NLP techniques to identify linguistic patterns and directions within malicious programs, cybersecurity systems can differentiate between benign and malicious scripts. This feature is handy for identifying hidden scripts in documents and web pages and file-less malware. By identifying and reducing malware threats, RL significantly improves cybersecurity. Training RL models to recognize harmful activity and respond suitably to neutralize threats is feasible. For example, RL agents immediately monitor system operations and network traffic, identifying and halting harmful activity before it causes harm [121]. ML, DL, and behavioral analytics are used by AI-powered cybersecurity solutions to detect and mitigate malware threats in industrial IoT networks. Researchers have conducted numerous studies on AI applications for malware identification and categorization in IIoT. Ahmed et al. [147] developed a 5G-enabled system using DL to classify malware attacks on the IIoT. Their approach transforms malware data into grayscale images and applies a CNN to extract discriminative features. By integrating multiple layers, the model effectively differentiates various malware attacks. Experimental results showed that the system outperformed previous methods, achieving 97% accuracy on a benchmark dataset. Cha et al. [146] developed an intelligent anomaly detection system using malware image augmentation in an IIoT environment with a digital twin. Their system converts malware binaries into fixed-size images within the digital twin's virtual environment and generates new malware using an adversarial generative neural network. DL then analyzes these images for malware detection, achieving over 97% accuracy. The system augments or creates malicious code using generative neural networks to address data scarcity. Compared to seven previous models, it achieved an F1-score of 0.94, demonstrating its effectiveness.

6.7.5. Improve threat intelligence

Threat intelligence in the industrial IoT gathers, analyzes, and shares information about potential threats to IIoT networks and devices. Given how vital IIoT is to industry, energy, transportation, and healthcare, it is essential to have strong threat intelligence systems. These technologies are crucial for spotting, thwarting, and reacting to cyberattacks that can impair equipment, compromise data, or interfere with business operations. IIoT networks are susceptible to ransomware, malware, and APT. Effective threat intelligence combines real-time data collecting, predictive analytics, anomaly detection, and automated responses to safeguard IIoT infrastructures. A proactive, scalable, and flexible cybersecurity strategy must be implemented as these networks become more complicated and possible threats rise. IIoT threat intelligence is revolutionized by AI and ML, which improve decision-making abilities and automate critical processes. AI systems continuously scan device activity, network traffic, and system logs for any odd activity indicating a cyberattack. These systems detect anomalies, including odd sensor data or sudden spikes in network traffic, using supervised and unsupervised ML models.

To assist businesses in addressing vulnerabilities and taking preventative action before attacks happen, AI may also evaluate past threat data to forecast future attacks. AI immediately isolates infected devices, blocks malicious IPs, and starts system recovery when it detects risk [44]. AI-driven threat hunting helps cybersecurity professionals uncover hidden risks, identify suspicious trends, and investigate possible attacks by analyzing massive amounts of data. AI-based security solutions enhance stakeholder interaction and data exchange by combining smart cities' threat intelligence and incident management. These solutions promote a more cohesive approach to cybersecurity. By pulling pertinent information from various sources, including forums, security blogs, and social media platforms, techniques like NLP assist cities in rapidly learning about the most recent threats and vulnerabilities. Cities can respond to cyberattacks quickly and effectively by using the information acquired [122]. By examining past data and new trends, AI forecasts possible risks and helps businesses bolster their defenses before an attack. This proactive change greatly enhances cybersecurity by identifying and removing threats before they can do damage [136]. DL greatly enhances threat intelligence platforms by allowing them to examine vast amounts of unstructured data from several sources, including threat feeds, social media, and dark web forums. DL models can implement proactive protection measures and send out alarms by finding complex patterns and links in the data.

Additionally, unstructured content from forums, dark websites, and social media is handled and examined via NLP. NLP models provide insightful information, track threat actors, and identify new threats by extracting pertinent information from text data. For instance, monitoring hacker forums for conversations regarding vulnerabilities or possible attacks may yield early warning signs, enabling security teams to address these dangers proactively. When cybersecurity workers actively look for indications of malicious activity within a network rather than just responding to warnings, RL is helpful for automated threat hunting. It is possible to train RL models to investigate intricate network setups and spot indications of intrusion. RL models increase the effectiveness of threat-hunting and decrease the time required to detect and respond to cyber-attacks by rewarding agents for correctly recognizing threats and penalizing false positives [121]. Many businesses use AI to improve IIoT threat intelligence. For example, IBM's QRadar Advisor with Watson integrates AI-powered threat data to evaluate IIoT attack trends and produce automated security reports. Darktrace uses AI-powered cybersecurity solutions that act as the immune system of an IIoT network, identifying abnormalities in regular network activity and taking autonomous action to thwart attacks immediately. Palo Alto Networks' IoT Security platform continuously monitors the condition of linked devices in IIoT networks using AI to spot unusual activity and stop harmful activities like malware and DDoS attacks. Cisco’s Cyber Vision platform integrates advanced threat intelligence to provide real-time monitoring of industrial devices and systems, using AI algorithms to detect unidentifiable attacks through traditional methods. A study by Bibi et al. [51] introduced a self-learning, multivector threat intelligence and detection mechanism to protect IIoT systems. The ConvLSTM2D model, which self-optimizes and scales well to counter evolving IIoT threats, is powered by a computational unified device architecture. They evaluated a state-of-the-art dataset with 21 million attack occurrences against benchmark algorithms and existing DL models. According to the results, the model delivers excellent detection accuracy without compromising speed efficiency. Comprehensive performance metrics and benchmark comparisons validate its effectiveness in threat intelligence and detection.

6.7.6. APT detection and classification

APT uses vulnerabilities in IIoT networks to obtain illegal access, carry out espionage, interfere with business operations, or harm vital infrastructure. These attacks employ complex tactics such as zero-day exploits, lateral movement, privilege escalation, and advanced evasion techniques. In IIoT networks, APTs target SCADA systems and move through stages of methodical attacks inside the core network. In IIoT contexts, these systems are the main hardware elements that make monitoring and managing industrial core processes possible. Four main characteristics set APTs apart from regular cyberattacks: careful preparation, deliberate execution, multi-stage deployment, and persistent infiltration. Traditional security methods are ineffective because attackers move slowly and deliberately to evade discovery. The increasing threat posed by APTs is illustrated by several high-profile incidents, such as the Shamoon malware attack on Saudi Aramco, the Stuxnet attack on Iran's nuclear reactor, and campaigns by organizations like Sauron, CopyKittens, Volatile Cedar, and ShellCrew. Some attacks employ masking techniques or encrypted communications to avoid detection [148]. Because of their stealth and complexity, APTs are difficult for traditional cybersecurity techniques to identify. In IIoT contexts, AI employs ML and DL to recognize attack patterns, spot irregularities, and act fast to thwart APTs. AI improves IIoT security by reducing risks, guaranteeing operational resilience, and continuously learning from network traffic and threat signatures. AI gradually identifies malicious activity and enhances security by tracking and categorizing network traffic, endpoints, and device interactions. AI can teach ML algorithms to identify typical IIoT system behavior patterns. Once it has established a baseline for typical behavior, the system could locate variations that might point to an ongoing attack. Even when attackers conceal or encrypt their actions, AI-driven traffic analysis can distinguish between benign and dangerous transmissions. Neural networks can detect suspicious event sequences that indicate an attack by simulating intricate linkages inside network activity. Because RNNs are so good at analyzing time-series data, they are especially helpful in identifying APTs that use data exfiltration and extended reconnaissance. For example, AI models can track the smart plant's interactions between sensors and PLCs. If an attacker compromises a sensor and issues unlawful commands, AI-driven systems can detect deviations and sound an alarm.

Moreover, ML models can differentiate between regular network traffic and APT-related actions, such as data exfiltration to distant servers. Even when attackers use encryption, AI can identify timing, frequency, and anomalies in data flow patterns. Assume AI associates a sudden increase in traffic directed at a particular IIoT device with known attack indicators from threat intelligence streams. It might take protective measures after determining the circumstance as an APT. IIoT settings can enhance security, detect sophisticated cyber threats, and reduce the risks posed by APTs using AI-driven analysis. Javed et al. [148] developed an intelligent APT detection and classification system to enhance IIoT security. After pre-processing, they applied multiple ML algorithms, including DT, RF, SVM, logistic regression (LR), gaussian Naive Bayes, bagging, extreme gradient boosting, and Adaboost, to the KDDCup99 dataset. Their comparative analysis identified Adaboost as the best performer, achieving 99.9% accuracy, 100% recall, and a 0.012s execution time. The system outperformed state-of-the-art techniques, demonstrating its effectiveness in detecting APT attacks.

6.7.7. Prevention of data leakage

Data leakage in the industrial IoT refers to the unauthorized or unintentional exposure of sensitive industrial data. The interconnected nature of IIoT environments makes them particularly vulnerable to data leaks, which can stem from weak security configurations, insider threats, insecure communication protocols, weak authentication, and access controls, misconfigured cloud and edge storage, compromised devices, supply chain vulnerabilities, and vulnerabilities in cloud storage or edge devices. When organizations fail to mitigate these risks, they face serious consequences such as intellectual security breaches, operational disruptions, property theft, regulatory non-compliance, and financial damage. AI is preventing data leakage within IIoT by leveraging ML algorithms, anomaly detection models, and security frameworks to maintain data integrity, confidentiality, and availability. AI-powered systems can detect and prevent data leaks while providing advanced protection mechanisms. ML models can analyze historical data to establish a baseline for regular network activity and system behavior. By continuously monitoring IIoT environments, AI-driven anomaly detection systems can identify deviations and trigger alerts when devices or sensors exhibit unusual data transmission patterns, signaling potential data exfiltration. AI also enhances security by optimizing encryption methods and managing access controls dynamically. Adaptive algorithms assess data sensitivity and apply appropriate encryption schemes while adjusting access privileges based on user roles, behaviors, and risk profiles. For example, AI can detect unauthorized access attempts to critical industrial data or attempts to bypass encryption protocols, triggering automated security responses such as enforcing encryption or restricting access. AI-driven data loss prevention systems enhance security by utilizing NLP and context analysis to scan data streams for sensitive information. These systems inspect communication channels between IIoT devices to prevent the unauthorized transmission of classified data. AI-powered data loss prevention can prevent accidental leaks of proprietary product designs or sensor readings in manufacturing environments by flagging unapproved file-sharing activities or insecure data transmissions. By integrating with threat intelligence platforms, AI can predict and identify vulnerabilities within IIoT networks. Analyzing global cyber threat data allows AI to correlate network activity with emerging threats and proactively apply patches or countermeasures before data leaks occur. For instance, AI-based systems can anticipate and mitigate sophisticated attacks such as MitM or DoS attacks that threaten IIoT data. If an AI system detects an exploit targeting industrial protocols, it can immediately trigger a protective response. Deploying AI at the network's edge enhances security by enabling real-time data analysis and decision-making on IIoT devices or local gateways. This method lessens the risk of data leakage during transmission by eliminating the need to send sensitive data to centralized servers. For example, Edge AI in a smart factory can analyze sensor data locally and apply security measures such as anonymizing or encrypting sensitive information before transferring it to a central database or cloud service. AI-powered intrusion detection and prevention systems (IDPS) significantly improve traditional security measures by incorporating ML to detect previously unseen attack patterns. In IIoT environments, AI-driven IDPS can identify subtle threats to system integrity or data leakage attempts that conventional signature-based methods might overlook. For example, an AI-powered IDPS can recognize when an IIoT device exhibits behavior consistent with remote attacker control, signaling a potential data breach. The system can then trigger an automated response, such as disconnecting the compromised device or rerouting its data to a secure channel.

AI enhances IIoT security by proactively identifying and mitigating risks through edge computing, real-time processing, and RL. By continuously adapting to evolving cyber threats, AI-driven security solutions provide robust protection against data leakage, ensuring the reliability and resilience of industrial systems. Miao et al. [149] proposed a DL-based anti-leakage method to secure power business data interactions between the state grid business platform and third-party platforms. Their approach integrates named entity recognition, regular expressions, and a Decoding-enhanced BERT with disentangled attention (DeBERTa)-Bidirectional LSTM (BiLSTM)-Conditional Random Field (CRF) model. The DeBERTa model extracts pre-trained features, BiLSTM captures sequence context semantics, and CRF ensures globally optimal tag sequences. This method identifies privacy-sensitive information in structured and unstructured power business data. Experiments on the CLUENER 2020 dataset show an F1 score of 81.26%, effectively reducing data leakage risks.

6.7.8. Phishing detection

Since IIoT devices are connected to business networks and ICS, hacked credentials or malware infestations can result in financial losses, security risks, and production disruptions. AI-driven approaches improve phishing detection in IIoT by using ML techniques, NLP, and pattern recognition. Attackers use phishing techniques to trick operators, employees, or even automated systems into downloading malware, disclosing personal information, or allowing unauthorized access [150]. According to Lamina et al. [151], these technologies increase the accuracy and efficacy of identifying and halting phishing attempts. AI-powered systems analyze communication patterns, spot suspicious behavior, and immediately stop hostile activities. Fake emails, dubious URLs designed to collect credentials, and phony login websites may be identified using ML models trained on historical phishing data. AI-powered NLP algorithms examine email content and spot phishing attempts that trick clients with false language, social engineering techniques, or urgent messages. Phishing threats in IIoT environments are identified using behavioral analytics. AI analyzes user login attempts, device interactions, and data access requests to discover irregularities. For instance, a device inadvertently connects to illegal endpoints, or a worker tries to access critical system settings from an unknown place. After that, the AI system provides a warning and limits access. AI also fortifies authentication procedures by spotting brute-force login attempts and credential stuffing, which frequently occur after phishing attacks. Threat intelligence systems driven by AI enhance phishing detection by monitoring global attack trends over time. By examining known phishing domains, malicious URLs, and attack patterns, these systems block fraudulent websites before users or IIoT devices engage in proactive interactions. AI also filters phishing emails via secure email gateways, preventing employees from clicking on harmful links or accessing infected content. Edge AI improves phishing security in IIoT systems by managing threat detection locally on IIoT gateways and devices. This solution reduces the need for cloud-based detection methods and reaction time. For example, the AI-powered security module of an industrial gateway can immediately identify phishing attempts and examine incoming data packets, preventing malware infections before they can compromise critical systems. NLP techniques explore the characteristics of email text, and ML models examine the material and architecture of websites to identify bogus sites. ML prevents data breaches and protects user information by quickly and accurately detecting phishing scams.

DL models examine web page properties, URLs, and email content to detect phishing attempts. These algorithms, which NLP enhances, identify manipulative techniques and misleading language patterns in phishing emails. By examining visual components and website architecture, DL algorithms protect against phishing attacks by distinguishing authentic websites from fraud. NLP methods search email communications for odd formatting, ambiguous hints, and questionable linguistic patterns. NLP models, for instance, may identify minute variations in email grammar, word choice, and structure that point to phishing attempts. Critical information is protected, and NLP prevents data breaches by filtering suspicious emails before recipients see them. NLP also guards against social engineering scams. Conversational data includes things like voice recordings and chat logs. NLP algorithms look for indications of manipulation. Emotion detection and sentiment analysis help spot coercive or dishonest social engineering techniques. NLP helps security staff identify and stop possible abuse by warning them about suspicious contacts [121]. Tamal et al. [152] used supervised ML (SML) classifiers and the optimal feature vectorization approach to create a reliable phishing detection system. They extracted 41 ideal characteristics from a massive dataset of 2,74,446 URLs (134,500 phishing and 139,946 real). After cleaning and dimensionality reduction, they evaluated 15 SML methods based on various standards. Random forests outperformed the others with an accuracy of 97.52%, precision of 97.50%, and AUC of 97%. The model offers a strong, portable tool for thwarting phishing efforts.

6.7.9. Behavioral analysis

Behavior analysis finds abnormalities by systematically observing and evaluating user or device activities and comparing them to typical behavior patterns. This approach enhances risk detection and raises the accuracy of recognizing potential threats by considering certain contextual factors. However, developing an exact standard requires vast knowledge and experience. Insider risks are the focus of User and Entity Behavior Analytics (UEBA) solutions, which prioritize this strategy [135]. AI improves IIoT systems' behavioral analysis skills. IIoT may enhance operations, safety, and efficiency while identifying irregularities that point to cyber threats like insider attacks by using AI tools to monitor, analyze, and forecast complex industrial behaviors. ML models discover irregular behavior in employees, machines, and equipment. Traditional monitoring systems rely on predefined criteria, whereas AI-driven systems may learn from data and notice minute abnormalities. AI can analyze sensor data from a manufacturing facility's pumps, motors, and turbines. By comprehending the typical operating patterns, the system can identify anomalies, like odd vibrations or temperature changes, that could point to an imminent failure or malfunction. Early detection makes proactive maintenance and less unplanned downtime possible [85][122][153]. Using sensor data and prior maintenance records, AI models can anticipate when machines will likely break down based on their behavior. Uptime is increased, and expenses are decreased when maintenance is done proactively (repairing before failure) rather than reactive (repairing after failure). AI might, for example, evaluate the behavior of workers and assembly line robots in a smart factory to find inefficiencies that can be fixed to maximize output and resource use without compromising quality. AI optimizes processes using real-time data, which lowers energy use in industrial settings. AI models identify areas where energy consumption may be reduced by analyzing machine and system energy use patterns. By examining the energy consumption of various equipment, AI can improve power distribution or suggest scheduling adjustments to reduce energy usage during off-peak hours, for example, in a large manufacturing facility. AI also continuously observes and assesses employee behavior to predict safety threats. By evaluating trends like location and movement, AI can identify high-risk circumstances, such as workers approaching unsafe places or neglecting safety regulations. For example, wearables with AI capabilities can follow workers' whereabouts at chemical companies, detect aberrant activity, and trigger alarms to reduce the frequency of accidents. By combining sensor data and visual systems, AI can also instantaneously assess how objects or processes behave, allowing quicker detection of flaws or departures from quality norms. AI-powered vision systems that identify soldering or component placement problems and promptly identify defective goods for inspection inspect production lines in the electronics manufacturing industry. AI watches IIoT supply chain activities to find trends and inefficiencies. AI in the automotive sector forecasts supply chain interruptions by examining component supplier behavior, transportation delays, and machine performance, allowing businesses to proactively modify inventory levels or rearrange production runs to avert possible problems.

AI is used by collaborative robots to evaluate and enhance HMI, resulting in safer and more effective teaming. For example, AI can modify a robot's speed or course according to a worker's vicinity to avoid safety risks while preserving productivity. By examining how assets and vehicles behave, AI improves fleet and asset management, improving logistics, reducing fuel consumption, and averting issues. AI-powered UEBA systems also help detect sophisticated attacks and insider threats by detecting deviations from normal activity patterns. For instance, in the logistics industry, AI systems track the speed and path of delivery trucks and notify fleet management of inefficiencies so that corrective action can be taken. ML algorithms can detect suspicious activity or illegal access attempts by learning user behavior patterns to establish baseline profiles and identify deviations, improving the accuracy of IDS [48]. AI also monitors user and object behavior to identify anomalies pointing to security flaws. By modeling user behavior over time, LSTM networks can identify frequent patterns and anomalies that may indicate malicious activity; by continuously analyzing login times, access patterns, and transaction patterns, these networks aid in detecting security breaches. NLP enhances UEBA by creating user and entity behavior profiles through the analysis of written interactions, such as emails and chat messages; if variations are observed, such as when an employee uses informal language when they typically use formal language [121], ML can detect subtle signs of compromise by analyzing device activity over time, and ML models can identify abnormal activity that may indicate a security risk by examining how devices interact with the network and each other. For example, a smart thermostat showing unusual data access patterns or communicating with unknown external servers could be flagged as a potential compromise, prompting a security review.

6.7.10. Incident response management

Incident response is a key element of cyber resilience, focused on swiftly identifying, analyzing, and minimizing the impact of cyber threats. AI automates incident response, enabling faster detection and resolution of cyber incidents. AI technologies can autonomously identify and address threats, minimizing the damage caused by cyberattacks. By utilizing AI, organizations improve their ability to respond to security breaches and recover efficiently. AI-driven systems enhance security by instantly detecting anomalies like unauthorized access attempts or malware infections. By reducing the need for human interaction, these technologies improve an organization's security posture and enable faster responses [135]. Moreover, AI tools that analyze massive amounts of security data from SIEM systems correlate patterns and events to identify potential threats, reducing the likelihood of human error and speeding up the time between discovery and remediation [137]. ML techniques improve incident response and enable timely and effective organization-wide responses by automating the process. Using ML algorithms, automated response systems evaluate security warnings, correlate events, and initiate real-time responses. These systems significantly increase the speed and efficacy of incident management by streamlining event evaluation, setting priorities, and coordinating response actions [44]. AI facilitates automated decision-making and response coordination, enabling detection and response during cyber emergencies. Based on past performance, RL agents evaluate the seriousness of security incidents and suggest the best course of action. These AI models continuously enhance response tactics by simplifying procedures and reducing the workload for security professionals. By incorporating AI into cybersecurity frameworks, companies may automate processes such as fixing vulnerabilities, starting countermeasures, and isolating compromised systems, ensuring a more efficient and adaptable response to evolving threats and significantly reducing reaction times [48][154].

6.7.11. Vulnerability/risk assessment and management

Risk assessment is crucial in enhancing cyber resilience as it helps prioritize cybersecurity threats based on their likelihood and potential consequences. This procedure is streamlined by ML techniques, which use data-driven approaches to detect, identify, and address cyber threats effectively. Various ML-based risk assessment techniques use event data, contextual information, and threat intelligence to forecast and quantify cyber threats. These methods use RL to build models that calculate the likelihood and seriousness of particular threats. On the other hand, labeled datasets are used to train supervised learning models such as regression, RF, and gradient-boosting machines to create predictive models for potential risks. Clustering and anomaly detection can unearth concealed patterns and anomalies in data, even without previously labeled data, which raises questions regarding potential hazards. RL is not frequently used for risk assessment, although it can reduce threats and alter safety precautions. Organizations can use these ML-driven frameworks to manage resources, prioritize security efforts, and develop plans for mitigating threats and vulnerabilities [44]. AI has significantly improved vulnerability management in IIoT systems by efficiently finding patterns in massive amounts of data. These systems pose security concerns because of their complexity, scalability, and wide range of connected devices. ML monitors odd or malevolent activities in system logs, device actions, and network traffic. An industrial facility's IIoT system may include anomalies that AI may identify, such as unusual pressure or temperature measurements, that could indicate a security compromise. Examining device configurations, historical occurrences, and external threat intelligence also forecasts vulnerabilities and assesses the probability of exploiting them. Predictive models recommend preventive steps, such as patching schedules, to minimize hazards before they worsen [48]. Moreover, AI automates vulnerability management by prioritizing and responding to attacks in IIoT systems. To guarantee that the most urgent problems are fixed first, ML algorithms assess vulnerabilities according to their operational impact, criticality, and exploitability. AI can, for example, prioritize less essential parts of a smart grid over flaws in the central management system. AI can also mimic attacks through automated penetration testing tools to find weaknesses that conventional scans might overlook. As demonstrated by connected car systems that highlight odd sensor data, AI continuously tracks device behavior, identifying abnormalities that may indicate security breaches. It can swiftly isolate affected devices, stop attackers, and implement mitigations through automated incident response, reducing the time needed to address attacks and improving the general security of IIoT systems [122].

6.7.12. Cloud Security

AI enhances cloud security for IIoT environments by improving threat detection, risk management, and automated incident response. IIoT systems produce vast amounts of data that must be processed, stored, and analyzed securely in the cloud. AI-powered security solutions examine real-time network traffic, device behavior, and access patterns to identify malware infections, data breaches, and illegal access. ML models set baselines for typical behavior and highlight anomalies that might be signs of a cyberattack. AI, for example, can spot anomalous login attempts or patterns of data exfiltration, allowing businesses to stop problems before they become more serious. AI-driven predictive analytics evaluate vulnerabilities and possible attack pathways by examining past security events, system configurations, and external threat intelligence. By using proactive firewall rule updates, MFA, and zero-trust designs, these insights assist enterprises in enhancing security. AI automates security monitoring and compliance enforcement, reducing human error that leads to cloud security breaches. AI-powered tools that continuously monitor cloud configurations identify and recommend changes for issues like unsecured storage or excessive access permissions. Automated compliance monitoring lowers the likelihood of compliance infractions by guaranteeing adherence to legal requirements and security best practices. AI enhances authentication and authorization by analyzing user behavior and contextual factors in identity and access management. It can enforce MFA or temporarily block access if it detects a strange login attempt from an unfamiliar device or location. This adaptive security method protects private data stored in the cloud and stops unwanted access. AI-driven threat intelligence systems, which collect and analyze data from various sources to identify emerging risks, further enhance cloud security. These systems can detect indications of compromise and predict possible attack paths by fusing threat intelligence with cloud operations, enabling companies to lower risks before they become dangerous. Furthermore, incident response and mitigation are improved by AI-driven security automation, which decreases the impact of cyber threats. AI is used by security orchestration, automation, and response technologies to identify, stop, and eliminate threats with little assistance from humans. AI can, for instance, immediately isolate an IIoT device, start an investigation, and block questionable IP addresses if it notices an unusual spike in data flow from the device. By detecting security vulnerabilities in code, monitoring application behavior, and spotting security issues during development and deployment, AI improves cloud application security when integrated into DevSecOps processes. AI-driven solutions for preventing data loss monitor data flows, recognize vital information, and establish access limits or encryption to avoid unintentional data disclosure. Organizations rely increasingly on AI to improve cloud resilience, automate security enforcement, and boost threat detection as cyber threats grow [121].

6.7.13. Security analytics

AI is transforming security analytics in the IIoT by enhancing real-time threat detection, prevention, and response. IIoT connects machines, sensors, and systems in industrial environments, enabling seamless data exchange and increasing exposure to cyber threats. AI-powered security analytics address this challenge by learning from historical data to identify patterns in device behavior. AI initiates notifications for possible breaches when the device deviates from its typical behavior. Even in situations with few predefined rules, ML models are highly effective at identifying abnormalities and cyberattack trends. AI-driven systems, for instance, track sensor data like pressure and temperature in a smart factory. AI can help stop malfunctions or cyberattacks by identifying anomalous spikes and flagging them for investigation. It also improves predictive maintenance by evaluating IIoT data to find security threats that might cause operational failures. AI reduces downtime and enhances system resilience by identifying early indicators of cyber interference. Predictive maintenance technologies, for example, analyze sensor data in production to identify anomalous wear patterns connected to hacking efforts. AI can detect abnormalities quickly and start countermeasures if an attacker tries interfering with a turbine. AI streamlines threat intelligence analysis by analyzing vulnerability reports, attack signatures, and system logs. It uses NLP and ML to link data sources and identify new dangers. A power plant, for example, can monitor worldwide cyber threats using AI-driven security analytics. If AI discovers a weakness in an IIoT protocol, it can assess the plant's vulnerability and recommend security fixes. Besides intelligence and detection, AI also automates network monitoring, real-time threat response, and access control. AI systems analyze IIoT network data to identify attacks like DDoS attacks or illegal access attempts. For example, AI detects unusual spikes in traffic in smart grids and isolates affected systems to prevent widespread disruption. AI-powered behavioral biometrics increase security by regularly confirming individuals based on interaction patterns. AI monitors operator behavior in critical manufacturing settings, spotting any anomalies that would indicate unauthorized access. It automates encryption, patch management, and vulnerability scanning to protect sensitive data. By integrating with existing security systems, AI enhances threat detection, speeds up response times, and reduces human error, boosting IIoT security and resilience [48].

6.7.14. Network traffic analysis

AI-driven network traffic analysis enhances security in the IIoT by detecting anomalies, identifying cyber threats, and automating threat responses instantly. ML models establish baseline patterns of normal network behavior by analyzing historical and real-time data. These models detect nonconformities such as unusual data transmission spikes, unauthorized connections, or abnormal access patterns, which may indicate cyberattacks like malware infections, intrusion attempts, or data exfiltration. For instance, in a smart factory, AI continuously monitors traffic between IoT-enabled robots and the central control system. Suppose it detects an unusual increase in data packets sent from a PLC, possibly indicating an unauthorized attempt to extract sensitive production data. In that case, the system triggers an alert and isolates the affected device to prevent data breaches. AI strengthens traditional IDPS by analyzing massive network traffic data and identifying sophisticated attack patterns. Unlike rule-based security systems, AI-driven IDPS can detect previously unknown threats, including zero-day attacks, by recognizing subtle behavioral anomalies. For example, AI-based IDPS monitors traffic between a power plant's ICS and external communication points. If AI detects an unusual command sequence on SCADA systems—potentially originating from an APT—it can automatically block the malicious traffic and alert security teams. AI enhances deep packet inspection (DPI) by scanning network traffic instantly for suspicious content, such as malicious payloads or unauthorized protocol usage. For example, AI-driven DPI might detect an encrypted payload transmission from an IIoT controller to an external entity in an industrial water treatment facility. Since such transmissions are uncommon in normal operations, AI flags the activity for further inspection, uncovering a covert data exfiltration attempt. By leveraging predictive analytics, AI forecasts security threats based on past incidents, real-time data feeds, and external cyber threat intelligence. This proactive approach helps IIoT security teams mitigate risks before they escalate into full-scale attacks. AI also facilitates automated network segmentation, ensuring that IIoT devices communicate only within authorized zones and initiating countermeasures like blocking malicious IP addresses or isolating compromised devices. For example, in a manufacturing plant, AI detects a compromised IoT sensor attempting to connect with an unauthorized external server. The system instantly segments the affected network zone, preventing the attacker from moving laterally while security teams investigate the breach. Moreover, AI continuously refines security policies based on evolving threats and network behavior. Unlike static security rules, AI-driven models update themselves by learning from new attack vectors, making IIoT networks more resilient against emerging cyber threats. Clustering algorithms and deep neural networks enhance network traffic classification, improving threat detection accuracy while reducing response time [121][138].

6.7.15. Identity and access management

By implementing intelligent, flexible, and automated security measures that safeguard vital assets and industrial networks, AI improves identity and access management (IAM) in the IIoT. The enormous scale and complexity of IIoT environments, where thousands of devices, sensors, and users interact, are too much for traditional IAM systems to manage. AI-driven IAM solutions tackle these issues using ML, behavioral analytics, biometric authentication, anomaly detection, and automation [121]. These technologies reduce the possibility of unauthorized access, enforce access control regulations, and improve identity verification. AI enhances identity verification by combining cutting-edge authentication techniques like behavioral biometrics, MFA, and biometric recognition. Password-based authentication is insufficient in IIoT environments because of the risk of credential theft; AI-powered facial recognition, voice recognition, and fingerprint scanning offer a safe substitute. AI improves MFA by enabling adaptive authentication by analyzing user behavior patterns. The system initiates extra authentication procedures to confirm the user's identity if it notices a login attempt from an unfamiliar device or location. AI maximizes access control by modifying permissions according to user roles, device health, and network conditions. In contrast to static policies, AI-driven Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) AI improve security by detecting anomalies and monitoring them instantly. By analyzing login history, access patterns, and device interactions, it can detect suspicious activities like privilege escalation, credential misuse, or lateral movement within the network. AI also strengthens IAM by automating compliance processes, improving encryption techniques, and optimizing device authentication. When it detects abnormal behavior, like an engineer trying to access unauthorized systems, it immediately alerts administrators and blocks the access attempt. AI further improves security by enabling just-in-time access control, which grants temporary permissions only when necessary and then revokes them afterward to minimize the attack surface and prevent excessive access privileges. AI-driven IAM systems generate real-time access logs and audit reports, ensuring compliance with industry regulations such as NIST, IEC 62443, and GDPR. These systems also detect policy violations and recommend corrective actions, such as revoking excessive permissions or updating expired security credentials. Furthermore, AI enhances encryption by optimizing cryptographic algorithms and key management processes, making encryption more secure and efficient. AI-based encryption systems analyze encrypted data patterns to detect weaknesses and strengthen encryption protocols when necessary. In device authentication, AI employs biometric recognition, contextual authentication, and adaptive access control to verify device legitimacy and prevent unauthorized network access. By integrating AI-driven access controls, encryption, and authentication mechanisms, organizations can enhance their security posture, protect confidential data, and mitigate insider threats and cyberattacks [155][156].

6.7.16. Endpoint security

Traditional security methods struggle to protect IIoT endpoints due to their large-scale deployment, diverse hardware configurations, and real-time operational requirements. AI enhances IIoT endpoint security by providing intelligent threat detection, automated response mechanisms, adaptive authentication, and continuous monitoring to prevent cyber threats, malware infections, and unauthorized access. ML and DL models analyze endpoint behavior, detect anomalies, and identify emerging cyber threats, surpassing traditional signature-based security solutions. AI-driven behavioral analysis monitors endpoint operations, including command execution and device communication patterns, to identify deviations that could indicate cyber threats. For example, AI can locate an ICS acting strangely, like sending unexpected directives to PLCs, and initiate an investigation before damage is done. AI-driven predictive threat intelligence looks at cybersecurity patterns and historical attack trends to prevent potential threats. At the same time, DL algorithms detect and stop advanced malware, like APTs and polymorphic versions. AI enhances endpoint authentication and access management through adaptive authentication, biometric verification, and role-based access controls. Adaptive authentication automatically adjusts security parameters based on contextual risk factors, including user behavior and device type. For instance, an AI-based security system in a power plant can recognize when an operator logs in with a strange device and request additional verification before permitting access. Biometric and behavioral authentication methods, such as voice and facial recognition, further prevent credential theft by verifying user identities before allowing access to critical systems. AI also enforces just-in-time access control by granting temporary privileges only when necessary and automatically rescinding them when the task is completed, reducing insider threats and privilege abuse. AI, for example, can allow temporary contractors to access HVAC systems with IIoT capabilities while ensuring their login credentials expire following maintenance. AI-driven endpoint security solutions continuously track device behavior, generate real-time notifications, and automate issue actions. SIEM systems with AI capabilities analyze massive amounts of endpoint data to find dangers and send alerts. AI, for instance, can identify unauthorized connections between a compromised IoT sensor and an external command-and-control server, triggering immediate security measures. AI also automates incident responses by segregating compromised endpoints, blocking malicious IP addresses, and installing security patches without human intervention. Automating regulatory reporting, detecting violations, and enforcing security requirements enhances compliance management. AI-powered encryption secures data in transit and at rest by dynamically adjusting cryptographic key strength based on real-time threats. AI also detects insecure communication channels, enforces encryption protocols, and ensures data integrity by identifying unauthorized modifications or tampering attempts. ML and DL are crucial in endpoint security, as they examine application and process behaviors to detect indicators of compromise, such as abnormal file access patterns or unauthorized network connections [121].

7. BLOCKCHAIN TECHNOLOGY IN IIoT

Industries integrating IIoT devices face significant challenges, including security risks, data integrity concerns, interoperability issues, and the need for trust among stakeholders. Blockchain technology provides a secure solution by offering a decentralized, transparent, and tamper-resistant framework for data management. Tyagi [48], Tian and Huang [157], and Kumar et al. [158] described Blockchain technology as a secure, immutable distributed ledger and computing system that logs transactions in a sequential chain of blocks connected by hash values. A Blockchain consists of interconnected blocks, each with a data record. Cryptographic techniques encrypt and authenticate the contents in each block to stop unwanted changes or manipulation [159]. Safe data operations and decentralized processing are made possible by smart contracts. Blockchain technology divides data among several networked computers, or nodes, that are running specialized software to maintain data consistency [160]. Because the system retains information across numerous nodes and binds each block to the one before, it is difficult for an attacker to change or remove data. By safely storing and verifying sensitive data, Blockchain upholds confidence in the decentralized network [160]. Each block includes transactions and essential information required to construct the hash for the current block, like a date and the previous block's hash. The block structure comprises a body with the transactions and a header with metadata [25]. Fig. 9 illustrates the structure of Blockchain blocks and the Merkle tree [160].

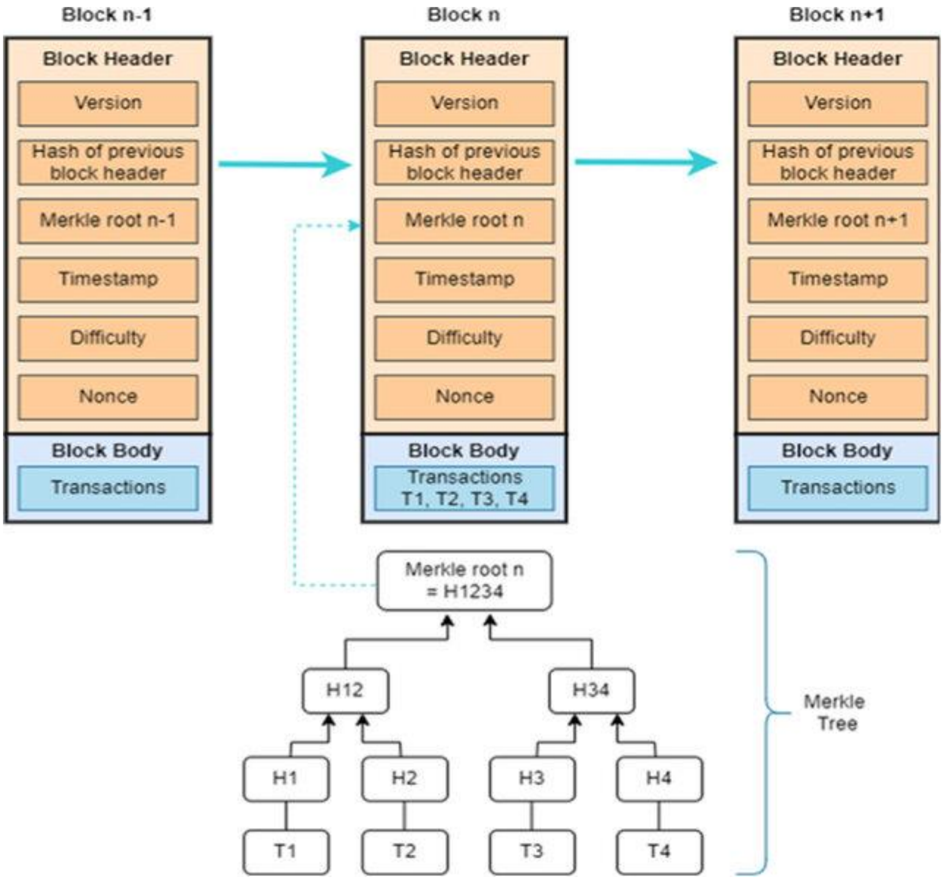

Fig. 9. Illustrates the structure of Blockchain blocks and the Merkle tree [160].

Blockchain technology increases the security and anonymity of digital transactions by employing cryptographic techniques to build an infinitely growing collection of records called blocks. The base of the chain is the first brick. Each block is identifiable by its cryptographic hash, including its predecessor's hash, to guarantee immutability. A peer must create a cryptographic hash connecting a new block to the one before it to add it [160][161]. Both the body and the block header are required for any new block. Important details, including the version number, timestamp, target hash bit, nonce, hash of the preceding block, and Merkle root, are all contained in the block header [162]. The block body includes additional elements, such as timestamps and transaction metadata. Before being added to the chain, a new block must be timestamped and hashed so all Blockchain users can track and validate the information to ensure data continuity. The timestamp in the block header records the publication time, and transaction verification is made easier by the Merkle tree root. In addition to digitally signing and grouping transactions to guard against tampering, a distributed electronic database guarantees consensus and verification. Data consistency across all ledger copies is ensured by this decentralized method [162][163]. An attacker's identity is void if they try to change a previous block, rendering the Blockchain useless. Changing one block and updating the headers of every succeeding block is nearly complicated. However, a Blockchain fork may occur if several nodes produce legitimate blocks simultaneously. The Blockchain accepts the most extended fork and rejects others to preserve a single canonical version. Every block header contains details unique to a consensus method that controls the validation of new blocks [164].

Blockchain maintains and verifies transactions or data points in IIoT networks as a distributed ledger, guaranteeing transparency and guarding against manipulation. Before adding it to the chain, the network verifies the information in each block, such as sensor readings and machine statuses. Blockchain technology protects against unwanted changes in the massive volumes of data produced by IIoT sensors and devices while facilitating safe, quick data sharing. Every device connects to a Blockchain node; each transaction or occurrence is documented as a block. The decentralized framework enables Trustless device interactions by doing away with the central authority responsible for data verification. Proof of Work (PoW) and Proof of Stake (PoS) are used on the Blockchain to validate and record accurate data. Blockchain can also store crucial industrial transaction data to increase security. The Blockchain's Universally Unique Identifier (UUID) is a thin storage presence and can identify data files. The InterPlanetary File System (IPFS) is a peer-to-peer file distribution system that effectively uses storage resources on network nodes. By adding IPFS, Blockchain can expand its storage capacity [157].

The SecureArchi-IIoT operational architecture uses Blockchain technology to increase the security and privacy of IIoT operations. Superior protection and confidentiality are provided by smart contracts and a reputation-based behavioral penalty mechanism that regulates operational permits and increases security efficiency [17]. Public, private, consortium, hybrid, and sidechain Blockchains are among the different types of Blockchains. Unlike private Blockchains, which are permissioned and usually controlled by a single institution, public Blockchains are open and decentralized, enabling everyone to participate. When using consortium Blockchains, multiple businesses oversee the Blockchain. Hybrid Blockchains combine the finest aspects of private and public Blockchains, making some data private and others publicly accessible. This approach balances the advantages of public visibility and privacy to provide flexibility in regulating data disclosure. Sidechain Blockchains enhance interoperability by facilitating asset transfers across different Blockchains [159–161]. Decentralization, immutability, autonomy, non-repudiation, democratization, transparency, integrity, traceability, tamper-proofing, anonymity, pseudonymity, programmability, persistency, auditability, automation, privacy, and confidentiality are some of the characteristics that make Blockchain a dependable, effective, safe, and popular choice for IIoT systems [159][161][163][165].

Blockchain-based smart contracts are self-executing agreements with terms built right into the code. When specific criteria are met, these contracts—used on decentralized Blockchain networks like Ethereum—automatically carry out, manage, or record actions [160]. The contract implements the agreed-upon activities without intermediaries once the prerequisites are satisfied. By providing a decentralized, visible, and unchangeable ledger that guarantees tamper-proof execution, smart contracts improve security. Once engaged, they validate the criteria of the code and then automatically carry out the required actions. Fraud and manipulation are less likely to happen since they are decentralized [160]. Platforms, including Ethereum, Binance Smart Chain (BSC), Solana, Cardano, and Polkadot, support smart contracts used in many sectors. In decentralized finance (DeFi), they enable automated lending, borrowing, and trading, while in supply chains, they ensure the transparency and authenticity of goods. Healthcare applications use them for secure patient data management, and real estate benefits from automated property transfers and escrow services [164].

Cryptography is key to Blockchain technology's ability to provide transaction security, integrity, and privacy. Symmetric and asymmetric encryption restrict data access to the designated recipients. Merkle trees, hashing, and digital signatures all increase security. Hashing converts extensive data sets into unique, fixed-length hash keys that appear random, do not collide, and prevent input retrieval. Even little changes to the input result in entirely new hashes. Merkle trees efficiently verify large data sets by arranging transaction hashes into a binary hierarchy, where each node hashes its child nodes. Tamper detection is made possible because any modified transaction modifies the final hash, or Merkle root, that is contained in the block header. Digital signatures use asymmetric cryptography to safeguard Blockchain transactions further. Clients encrypt a transaction hash using their private key to generate a digital signature. The transaction is subsequently verified by network peers utilizing the client's public key [159][160].

The algorithms that make up a Blockchain consensus protocol manage the network's operations. It allows scattered nodes to agree on the validity of transactions in a decentralized network. They achieve this by ensuring all users concur with the present state of the Blockchain and safely confirming transactions. These protocols define how new blocks are added, how transactions are validated and stored, and how network security is preserved. Their primary goals are guaranteeing participant consensus and stopping malevolent nodes from convincing legitimate nodes to approve fraudulent transactions [159]. These algorithms are crucial for preserving security, decentralization, and consistency without depending on a centralized authority. Various consensus systems offer distinct principles and trade-offs by tackling scalability, energy efficiency, and security issues. They are essential for maintaining a standard view of the ledger, stopping fraud, and protecting the integrity and dependability of the Blockchain. PoW, PoS, Delegated Proof of Stake (DPoS), Proof of Authority (PoA), and Byzantine Fault Tolerance (BFT) are notable consensus algorithms [159][160][162].

Numerous Blockchain frameworks, such as Quorum, IOTA, Exonum, Ethereum, Hyperledger Fabric, TRON, Multichain, OpenChain, and Bitcoin, have become more well-known. These platforms cater to various businesses and provide a range of capabilities [159]. The six layers of an application, contract, incentive, consensus, network, and data comprise a basic Blockchain architecture. Time-stamped blocks protected by cryptographic methods, including chain structures, Merkle (hash) trees, and hash functions, are part of the data layer. The network layer controls distributed networking protocols, data propagation, and verification. While the incentive layer describes reward systems for participating nodes, the consensus layer offers a variety of algorithms for Blockchain applications. The application layer concentrates on Blockchain-based commercial applications, while the contract layer specifies programming methods utilized in Blockchain [159].

7.1.Integration of Blockchain technology into IIoT systems

By improving transparency, efficiency, and security across the supply chain, integrating Blockchain technology with the IIoT is consistent with Industry 4.0 ideals. IIoT sensors collect data on emissions, energy consumption, and other environmental factors. Blockchain’s decentralized and tamper-resistant ledger ensures data integrity across connected devices, eliminating the need for intermediaries. This streamlined approach enhances data exchange while reducing operational costs. In IIoT networks, Blockchain strengthens cybersecurity by preventing unauthorized access and data manipulation. Smart contracts further enhance automation by enforcing predefined rules without human intervention, increasing reliability and reducing errors in industrial processes. Supply chain management significantly benefits from Blockchain integration, enabling real-time tracking of goods, ensuring product authenticity, and improving stakeholder accountability [55]. Blockchain supports predictive maintenance by securely recording sensor data. This capability allows businesses to optimize equipment performance, reduce downtime, and improve efficiency. By combining Blockchain with IIoT, industries can create more secure, efficient, and autonomous ecosystems. This integration fosters innovation, enhances operational resilience, and drives the future of smart manufacturing and industrial automation. Blockchain's secure and decentralized ledger ensures transparent and tamper-proof data storage. Each block links to the previous one and includes a timestamp, forming a safe and verifiable information chain [55]. Fig. 10 illustrates how Blockchain integrates into IIoT systems [166].

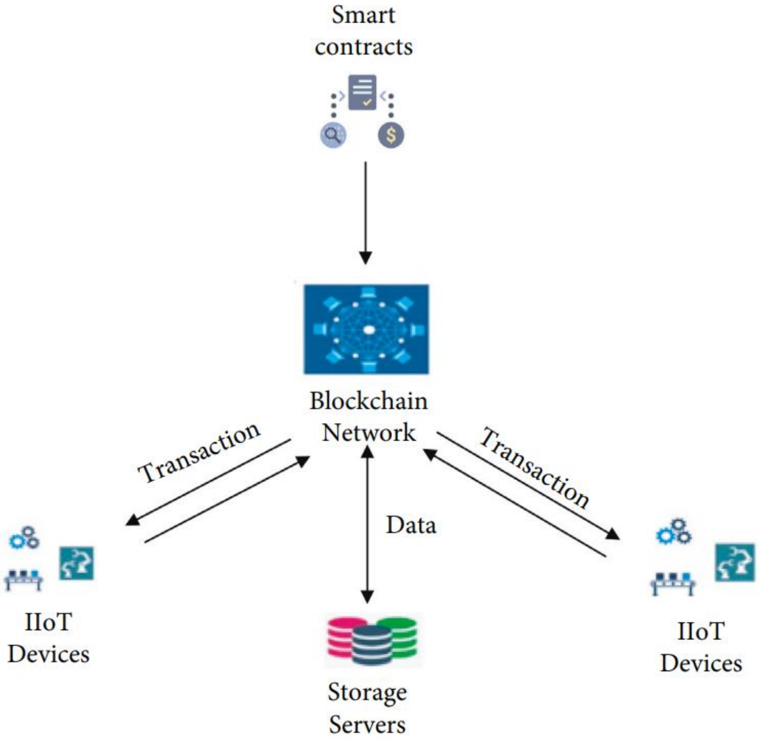

Fig. 10. Illustrates the integration of Blockchain into IIoT systems [166].
Fig. 11.

In the IIoT ecosystem, which includes perception, network, control, Blockchain service, and application layers across domains like manufacturing, the Blockchain service layer is crucial in enabling secure and decentralized data sharing, auditing, and trust among stakeholders. This layer links to both on-chain and off-chain Blockchain networks and includes smart contracts, transaction management, and support for Blockchain services. Verifier nodes protect the on-chain network by confirming transactions and preserving the Blockchain's integrity. Using a credit consensus approach and a directed acyclic structure, researchers have created a secure Blockchain design that protects data secrecy by giving misbehaving nodes more power and good nodes less. Studies that combine Blockchain with edge frameworks to enhance security, task monitoring, latency, and resource efficiency have neglected system performance [66].

According to Tian and Huang [157], Blockchain technology has several benefits, including decentralization, traceability, immutability, and ease of collaboration. Blockchain's smart contract design can safeguard IIoT operations such as commerce and transportation. A UUID can effectively identify data files, making them portable and appropriate for storage on a Blockchain. Additionally, security is improved by putting crucial industrial transaction data on the Blockchain. The IPFS increases the storage capacity of the Blockchain and optimizes the storage resources of network nodes [157]. Blockchain offers a ground-breaking way to share data safely in the IIoT while maintaining data security and privacy. Its distributed and unchangeable structure guards against data manipulation by hackers. Stakeholders can access and exchange trustworthy data because of its consensus process and data auditing features, improving transparency and trust. Blockchain nodes must store and process every transaction data as data volume increases, dramatically increasing the processing and storage power required [167][168].

7.2.Applications of Blockchain Technology in IIoT

Below is a brief explanation of the primary applications of Blockchain in IIoT security.

7.2.1. Secure device authentication and identity management

Blockchain improves decentralized identity management for IIoT devices by enabling secure authentication independent of a central authority and guarding against identity theft, spoofing, and illegal access. The Blockchain ensures that only authorized devices can connect to the network by giving each device a distinct digital identity [54]. Storing encrypted identity information eliminates the need for centralized identity providers, reduces the risk of identity theft and unwanted access, and gives individuals control over their data [48]. By employing cryptographic techniques to provide trust and authentication in IIoT communication, Blockchain reduces the likelihood of impersonation by allowing devices to securely identify and authenticate themselves without needing a centralized authority [48]. By giving each device a distinct cryptographic identity stored on a Blockchain, IBM's Hyperledger Fabric, for example, has effectively handled device IDs in IIoT scenarios and ensured that only authorized entities communicate with the network.

7.2.2. Data integrity and tamper-resistant storage

Blockchain improves the security and integrity of IIoT data by keeping transaction logs on an immutable ledger and guarding against unwanted changes. To ensure dependability, each network user must approve any modifications to the data. Each transaction is stored as a block that cannot be deleted once put, protecting data throughout transmission [48]. Blockchain avoids breaches and limits access to authorized parties by encrypting and distributing data throughout the network rather than depending on centralized servers. Its decentralized ledger structure links each block to the previous one, making data manipulation nearly impossible and ensuring a trustworthy source of truth across the supply chain [55]. For example, Siemens, a German manufacturing firm, leverages Blockchain to secure IIoT sensor data in industrial automation, protecting machine logs from tampering and enhancing predictive maintenance and operational reliability.

7.2.3. Secure communication and data exchange

Blockchain enhances encrypted and authenticated communication between IIoT devices, reducing vulnerabilities like MitM attacks and enabling direct peer-to-peer interactions without intermediaries. Utilizing advanced encryption techniques establishes secure channels that protect transmitted data from eavesdropping or interception, ensuring confidentiality. Blockchain’s cryptographic capabilities safeguard sensitive data, preserving its integrity and privacy across the supply chain [48]. Participants have control over their data, sharing it selectively within the network [55]. For instance, Chronicled, a Blockchain-based supply chain company, employs Blockchain to secure communication in pharmaceutical IIoT applications, preventing counterfeit drugs by maintaining transparent and verified transaction records.

7.2.4. Smart contracts for automated security protocols

Smart contracts enable IIoT devices to perform defined security procedures independently, ensuring compliance with security regulations by enforcing access control, detecting irregularities, and alerting users in the event of a breach. Blockchain-based smart contracts increase the security and integrity of contractual agreements by reducing the likelihood of fraud or manipulation because they are self-executing and self-enforcing. The decentralized Blockchain framework guarantees the reliability of smart contract execution [48]. These contracts can also automate compliance with sustainability standards, such as energy use, waste management, and emissions, by triggering warnings or penalties when criteria are met or violated [55]. Additionally, smart contracts reduce the possibility of malicious intent or human error by automating rules and behaviors throughout the IoT network [54]. By autonomously starting activities based on predefined events, self-executing smart contracts combined with IIoT data can streamline industrial processes and eliminate manual involvement [53]. Smart contracts in IIoT pipeline monitoring systems can automatically initiate shutdowns upon anomaly detection in industries such as oil and gas, lowering safety and environmental concerns.

7.2.5. Supply chain security and traceability

Blockchain enhances IIoT-based supply chain systems by providing end-to-end traceability, ensuring secure data exchange, and preventing counterfeiting. It boosts supply chain security and transparency by enabling the tracking and verification of products and components, safeguarding authenticity, and preventing tampering [48]. For instance, Walmart and IBM have teamed up to utilize Blockchain and IIoT sensors to track food products instantly, improving food safety and minimizing contamination risks.

7.2.6. Decentralized access control and authorization

Traditional access control models depend on centralized databases, which expose them to cyber-attacks. Blockchain-based access control decentralizes trust, offering more substantial and more resilient security. For instance, the Energy Web Foundation leverages Blockchain in smart grids to securely manage energy resource access, facilitating safe transactions between decentralized power producers and consumers.

7.2.7. Resilient cybersecurity against DDoS attacks

Due to their interconnected nature, IIoT networks are vulnerable to DDoS attacks. Blockchain mitigates these attacks by decentralizing Domain Name System (DNS) services and validating traffic sources, making it harder for attackers to manipulate domain ownership. By storing domain ownership information on the Blockchain, the system becomes more resistant to malicious interference [48]. For example, Xage Security, a startup, integrates Blockchain into IIoT cybersecurity frameworks to protect industrial systems from DDoS and ransomware attacks, distributing authentication processes across multiple nodes to enhance security.

7.2.8. Decentralization

Centralized databases are susceptible to single points of failure and security breaches, while Blockchain's decentralized structure removes these risks. Blockchain distributes data across multiple nodes, ensuring that the rest of the network stays secure in case of a compromise of a single node, preserving continuous data availability [55]. This decentralized approach removes the dependence on a central authority, making IoT networks less susceptible to failures and reducing the risk of unauthorized access or data manipulation [54].

7.2.9. Immutable audit trails

Traditional audits in supply chain management are often time-consuming and resource-intensive. Blockchain streamlines the auditing process by providing easy access to relevant information on a distributed ledger, minimizing the risk of errors, and enabling real-time audits [55]. Its immutable and tamper-proof nature makes it ideal for creating reliable audit trails, as it records security events like system changes, access attempts, or data breaches, ensuring transparency and supporting forensic analysis [48]. Moreover, Blockchain preserves the integrity and reliability of IoT data by creating permanent records of all transactions or data exchanges, which cannot be altered or deleted [54].

7.2.10. Consensus mechanisms

Blockchain consensus mechanisms, such as PoW and PoS, validate and verify IIoT transactions, ensuring that only legitimate data is added to the Blockchain. By requiring a collective agreement among nodes, these mechanisms prevent malicious actors from injecting fraudulent information into the communication stream. This consensus ensures that all participants maintain a consistent and transparent view of the data, ultimately enhancing trust and security [48][54].

7.2.11. Traceability and accountability

Blockchain enables end-to-end product traceability across the supply chain by recording every transaction and event related to manufacturing, delivery, and distribution. This traceability helps identify the sources of environmental impact, making it easier to hold parties accountable for sustainability issues [55]. Blockchain ensures accountability and compliance by providing a transparent and auditable trail of all transactions, which is especially crucial in industries where these factors are critical [54]. In the context of IoT, Blockchain traces every data transaction, device interaction, or command back to its origin. It also records communication transactions within IIoT networks, creating an immutable audit trail that supports forensic analysis and helps identify and address security breaches or unauthorized activities [48].

7.2.12. Transparency

Blockchain technology enhances industrial IoT by offering a secure, decentralized, and transparent framework for managing data, ensuring security, and automating processes. It creates new business models, boosts operational efficiency, and builds trust among stakeholders in IoT ecosystems [54]. Blockchain enables supply chain traceability and end-to-end visibility, allowing any network member to access an immutable, transparent record of each transaction—from the initial procurement to the delivery of the finished product. This transparency minimizes waste, ensures compliance with environmental regulations, and helps identify inefficiencies [55].

7.2.13. Distributed threat intelligence

Distributed threat intelligence uses decentralized networks to share and analyze security data across stakeholders in the IoT ecosystem. By integrating Blockchain technology, IIoT systems securely and transparently exchange real-time threat information without relying on a central authority. This approach ensures that the data remains immutable, tamper-resistant, and accessible to authorized parties, enabling organizations to quickly detect, mitigate, and respond to security threats. Blockchain-based distributed threat intelligence fosters trust among network participants, reduces the risk of cyberattacks, and strengthens the security of critical industrial infrastructure. Organizations can collaborate instantly by storing and sharing threat information on the Blockchain, enhancing their ability to detect and address emerging threats [48].

7.2.14. Distributed and decentralized network

Blockchain technology enhances security, transparency, and collaboration in IIoT by creating a decentralized and distributed network. This structure enables secure data sharing and storage across nodes without a central authority. In IIoT, Blockchain ensures that sensor data, operational insights, and threat intelligence remain immutable, transparent, and resistant to tampering. It facilitates real-time, peer-to-peer exchanges of information, improving decision-making speed and accuracy while strengthening network security. By removing single points of failure, Blockchain makes it more difficult for cyberattacks to compromise system integrity, enabling trusted, auditable, and secure interactions within IIoT ecosystems for more resilient and efficient industrial operations [48].

7.2.15. Secure device registration

Blockchain enhances industrial IoT device registration security by authenticating, verifying, and securely adding devices to the network. Leveraging Blockchain's decentralized nature, it creates a transparent, immutable ledger to store each device's unique identifier, like a serial number or cryptographic key, which ensures that only legitimate devices can interact with the IIoT system, establishing a chain of trust for secure communication and data sharing. Blockchain's cryptographic features protect registration data from tampering, making any changes auditable and traceable. Blockchain helps prevent spoofing, impersonation, and unauthorized access by preventing unauthorized devices from joining, creating a reliable foundation for secure communication across IIoT networks [48].

7.2.16. Zero-trust networks

When IIoT is integrated with Blockchain, zero-trust networks enhance security by ensuring no device or user is trusted by default, even within the network perimeter. In this model, every device, user, and communication request undergo continuous authentication, verification, and authorization before gaining access or performing any action. Blockchain strengthens this process by offering a decentralized, immutable ledger to record and validate each transaction and device interaction, ensuring that only authorized entities can access sensitive data or resources. By combining Blockchain's cryptographic features with zero-trust principles, IIoT networks become more resilient to attacks, as every action is scrutinized accurately and auditable, preventing unauthorized access, reducing internal threat risks, and reinforcing the security of IIoT systems. Blockchain also supports the creation of decentralized, trustless networks, allowing organizations to establish peer-to-peer connections and validate the integrity and authenticity of network participants without relying on a central authority [48].

7.2.17. Incident response and forensics

Blockchain technology enhances incident response and forensics in IIoT by providing a tamper-proof, decentralized ledger that records all interactions and transactions within the network. This immutable nature enables detailed, auditable tracking of device interactions, communications, and events, making it easier to analyze incidents. In a security breach, Blockchain helps trace the attack's origin, identify compromised devices or users, and examine the sequence of events. Its transparency ensures that forensic teams have critical, unaltered data to understand the attack's scope and impact. By incorporating Blockchain into incident response, organizations can improve detection, response, and recovery, all while preserving the investigation's integrity and strengthening overall IIoT security [48].

7.2.18. Threat detection and analytics

Blockchain enhances threat detection and analytics in IIoT by securely and transparently recording device interactions and transactions across the network. Its decentralized nature allows real-time data from IIoT devices to be captured in a tamper-proof ledger, making it easier to identify anomalies, threats, and malicious activities. Analyzing these Blockchain-based records helps detect unusual behavior, such as unauthorized access, abnormal communications, or system malfunctions. Blockchain's transparency also enables efficient monitoring of device health and security status, facilitating the rapid identification of vulnerabilities and compromised assets. Integrating Blockchain with threat detection systems strengthens the ability to proactively address security risks while providing reliable historical data for investigation and response, ultimately enhancing the overall security of IIoT networks. Furthermore, patterns and anomalies can be identified by aggregating and analyzing security data from multiple Blockchain sources, enabling proactive threat detection and response [48].

7.2.19. Reduced fraud and counterfeiting

Blockchain significantly reduces fraud and counterfeiting in IIoT by providing a secure, transparent, and immutable record of device interactions and transactions. It logs every movement or transaction in a decentralized, tamper-proof ledger, making it impossible for malicious actors to alter or forge data, ensuring the traceability of products, parts, and components from origin to endpoint and preventing counterfeit goods from entering the supply chain. Instantly, stakeholders can verify the authenticity of devices, parts, and services, quickly identifying and resolving fraudulent activities. By maintaining an unchangeable and transparent transaction record, Blockchain builds trust, protects the integrity of IIoT systems, and mitigates fraud risks [55].

7.2.20. Security against cyber threats by encryption and consensus

Blockchain strengthens security in IIoT by using encryption and consensus mechanisms to protect data from cyber threats. Encryption secures data transmitted between devices, ensuring confidentiality and integrity by making it immutable and resistant to unauthorized access. The consensus mechanism, where multiple nodes validate transactions, prevents the single entity from controlling or manipulating the data. This approach makes it nearly impossible for malicious actors to alter the data or take control of the network, significantly enhancing the cybersecurity of the supply chain [55].

7.2.21. Tokenization of assets

Tokenization of assets in IIoT involves converting physical or digital assets into digital tokens recorded and secured on the Blockchain. This process allows real-world assets, like machinery, equipment, or raw materials, to be represented as tokens that can be easily tracked, traded, or transferred. Blockchain's transparency, security, and immutability ensure these tokens are securely managed, reducing the risk of fraud or unauthorized transactions. By streamlining asset management, tokenization enhances traceability, improves efficiency, and enables fractional ownership or sharing of assets across the network. Blockchain simplifies the tokenization of physical and digital assets, providing electronic representations for each supply chain item, which helps track the origin and movement of assets and ensures that only authorized entities can access and modify the corresponding digital records [55].

7.2.22. Decentralized automation

Decentralized automation in IIoT leverages Blockchain's distributed ledger technology to enable autonomous decision-making and operations without relying on a central authority. Using smart contracts and decentralized applications (dApps), IIoT devices and systems can execute predefined tasks and agreements automatically when specific conditions are met, eliminating intermediaries, enhancing efficiency, and ensuring transparency and security. Blockchain provides a secure, immutable record of actions, improving traceability and building participant trust. By distributing control across the network, decentralized automation increases system reliability, reduces single points of failure, and enhances resilience. This integration makes IIoT systems more autonomous, minimizing manual intervention, improving operational efficiency, and lowering risks [54].

Some notable research studies that used Blockchain technology to secure IIoT include the following. Wang et al. [165] present a Blockchain-assisted lightweight revocable anonymous authentication scheme in IIoT. They design a fast, secure authentication method using Okamoto's protocol and elliptic curve cryptography to ensure data anonymity and traceability. A two-level key derivation algorithm, combined with Blockchain technology, addresses pseudonym management, enabling devices to generate and revoke pseudonyms independently. Security analysis confirms that the scheme meets security goals and resists common attacks. Performance evaluations show that the approach achieves low computational and communication overheads, outperforming related solutions. Ababio et al. [5] introduced a Blockchain-assisted FL framework to address trust, data security, and model accuracy challenges in IIoT. Deploying AI models on edge devices and using FL ensures data privacy while enabling collaboration. Blockchain secures data management and enhances transparency, while explainable AI improves model interpretability. The framework boosts security, privacy, and scalability for self-optimizing digital twins in IIoT environments. Real-world evaluation shows its effectiveness in optimizing industrial operations, offering a scalable, secure, and efficient solution for dynamic, resource-constrained IIoT infrastructures. Dildar et al. [169] proposed an end-to-end security mechanism for industrial IoT using Blockchain for authentication, authorization, and data integrity without relying on a central authority. The mechanism uses smart contracts to enforce security policies and allows real-time rule changes in response to suspicious behavior. A lightweight cryptographic scheme that minimizes data management overhead was introduced to ensure compatibility with various devices. The hybrid Blockchain approach combines the strengths of private and public implementations, providing high security and scalability. Tong et al. [168] proposed a Blockchain-based data sharing and privacy protection scheme for the IIoT, combining weighted threshold secret sharing, zero-knowledge proof, and attribute-based encryption. They use weighted threshold secret sharing to assign attribute values and enable flexible permission combinations, ensuring secure and flexible data access for terminal members. A non-interactive zero-knowledge proof protocol was employed to pre-authenticate data accessors, preventing unauthorized access. It also uses IPFS for distributed encrypted data storage, alleviating Blockchain storage pressure.

Wang et al. [43] proposed a Blockchain-based certificateless conditional anonymous authentication (BCCA) scheme for IIoT, optimizing authentication efficiency by using an elliptic curve design to avoid the time-consuming bilinear pairing operation. They introduced a precomputation strategy to prepare essential materials in advance and implemented one-time verification for batch signatures to reduce latency. Random verification checksums protect against key recovery attacks, while a mix of long-term and short-term secrets addresses temporary secret leakage. Simulation results confirm that the scheme offers both security and computational cost benefits. Wang et al. [170] introduced a Blockchain-based lightweight message authentication for edge-assisted cross-domain IIoT. They developed a Blockchain-enabled, edge-assisted authentication framework that enhances efficiency by reducing redundant interactions between entities. The proposed lightweight authentication algorithm ensures message security with minimal computational overhead, making it ideal for multi-receiver cross-domain IIoT. Security analysis confirms the scheme's resilience against various attacks under the random oracle model. Performance evaluations show that the approach achieves low computational and communication overheads, outperforming related schemes. Wang et al. [171] proposed a lightweight and secure data-sharing scheme for Blockchain-enabled cross-domain IIoT, enabling authorized smart devices to access data anonymously. Devices can generate pseudonyms dynamically without requiring domain authorization centers, reducing storage overhead and workload. The scheme combines broadcast encryption and proxy re-encryption, ensuring flexible data sharing and privacy protection. Security proofs and analyses confirm its robustness against attacks. Performance evaluations show that the scheme achieves low computational and communication overheads, outperforming related approaches. Aljuhani et al. [172] proposed a DL-integrated Blockchain framework to secure IIoT networks. They design a private Blockchain for secure communication among IIoT entities, using session-based mutual authentication and key agreement mechanisms. The proof-of-authority consensus mechanism verifies transactions and block creation based on miner voting over the cloud server. They introduce a DL-based IDS combining CSAE, ABiLSTM networks, and a softmax classifier to detect cyberattacks. Performance analysis with ToN-Edge-IIoTset data sets demonstrates superior intrusion detection, confirming the framework's effectiveness.

Zhang et al. [85] introduced a lightweight, secure, and trustworthy stateless Blockchain-based identity management architecture for IIoT. By combining cryptographic accumulators with Blockchain, they created a proof that maintains a constant length despite identity changes, ensuring the complete concealment of identity information. The authors also designed a stateless Blockchain structure and proposed new consensus, identity modification, and verification algorithms. They presented a comprehensive threat model and security analysis of the system. Experimental results show a time cost of 130.25 ms and a Blockchain size of 100.13 MB, enhancing portability and efficiency for IIoT applications. Sohail et al. [173] proposed a secure, incentive-based data-sharing framework for IIoT systems using Blockchain technology. Blockchain ensures secure, tamper-resistant data storage and sharing by utilizing a distributed ledger to prevent unauthorized access. They design a security protocol that leverages elliptic curve cryptography (ECC) and applies the Shapley value for fair revenue distribution. They conduct extensive simulations using AVISPA and Scyther to evaluate security, proving the protocol's resilience against adversarial attacks. The experiments demonstrate that the framework ensures fairness in revenue distribution among participants. Chen et al. [174] introduced Blockchain and Coded Computing-based Secure Edge Learning (BCC-SEL) for industrial IoT. They developed a coded edge learning framework using Lagrange Coded Computing (LCC) to efficiently utilize idle nodes during training. An incentive mechanism based on Blockchain rewards and punishes participating clients, while cosine-similarity detection ensures robustness. The approach reduces computational consumption and guarantees accuracy, with experimental results showing a 4.19% accuracy margin. Cao et al. [175] introduced a Blockchain-based distributed IoT architecture to enhance security and efficiency in smart factories. Their scheme employs a federated Blockchain to establish trust across domains, ensuring secure device connections. Security analysis confirms that the scheme offers integrity, mutual authentication, scalability, and resistance to four types of attacks. Efficiency experiments demonstrate the scheme's feasibility, improving performance as peer nodes increase. This approach boosts equipment security and supports the digital transformation of smart factories, fostering a more efficient and reliable future. Yao et al. [176] introduced SecureArchi-IIoT, a Blockchain-based architecture to enhance security and privacy in IIoT operations. They designed smart contracts that meet industrial demands and developed an operational control policy for precise permissions management. A reputation-based punishment mechanism enhances security. The prototype was implemented in a private IIoT environment, proving its feasibility. Experimental results show that SecureArchi-IIoT surpasses traditional architectures in security and privacy while maintaining acceptable real-time performance. Zainudin et al. [177] introduced a permissioned Blockchain-based system for collaborative and decentralized cyber threat detection in digital twin (DT)-enabled IIoT networks. They developed a context-aware intrusion detection model (C-NIDS) that uses factorized and grouped convolution structures to detect adversarial attacks in virtual and physical environments. A verifiable off-chain aggregation technique with RSA-based digital signatures ensures reliable and tamper-proof model aggregation with minimal transaction time. The system achieved 99.50% accuracy with a lightweight model structure (4634 parameters, 0.0088 MFLOPs) and a transaction time of 0.0244 seconds. The proposed BCFed-DT model outperforms existing methods in both accuracy and efficiency.

8. QUANTUM CRYPTOGRAPHY IN IIoT

Strong cryptographic solutions must be implemented as IIoT develops to secure industrial networks and guarantee dependable operations in vital infrastructure. Cryptography safeguards data by encrypting it into ciphertext and decrypting it back into plaintext as transmitted over a network. According to Mammeri [178], cryptography is the art and science of safely hiding messages and data, especially private information, to prevent unwanted access. Thanks to cryptography, only the intended receivers can access sensitive information, guaranteeing its safe storage and transmission over unsecured networks. It shields data against unwanted disclosure or modification while confirming user and message authenticity [178]. By assuring data secrecy, cryptographic systems defend against malevolent attackers [179]. Additionally, they guard against unwanted access to protected data and preserve the integrity of messages [60]. Cryptographic techniques are essential to ensure the secure communication and storage of images taken by IoT camera sensors. The best way to stop illegal access to data that is kept and sent is to use encryption. Encryption transforms readable (plain) text into unreadable (cipher) text, whereas decryption restores the original content. Cryptographers use both symmetric and asymmetric encryption to protect data. Symmetric encryption is sufficient since it only requires one key for encryption and decryption and is also a secure key-sharing method. By eliminating the requirement for shared secret keys and employing a key pair—a public key for encryption and a private key for decryption—asymmetric encryption increases security. Both tactics guard against unauthorized access to personal information [180]. Because they guarantee data confidentiality, integrity, and authentication, traditional cryptographic approaches are essential for safeguarding IIoT systems. By utilizing a single shared key for encryption and decryption, symmetric encryption techniques such as Data Encryption Standard (DES), Triple DES (3DES), and AES offer quick and effective protection. For IIoT devices operating in dispersed contexts, asymmetric encryption techniques like ECC and RSA offer secure key exchange and authentication. Data integrity is preserved by cryptographic hash functions like SHA-256, which provide fixed-size hash values that identify unwanted changes.

During transmission, the integrity and validity of messages are ensured using hash-based message authentication codes (HMACs) and other MACs. Digital signatures based on asymmetric cryptography protect against spoofing and guarantee non-repudiation by validating IIoT devices and data sources. While these techniques provide basic security, IIoT applications occasionally require low-power cryptographic solutions to accommodate resource-constrained edge devices. Researchers consistently improve these techniques to balance security and performance [17][181]. To address the shortcomings of conventional cryptography, researchers have developed lightweight encryption algorithms that reduce secret key sizes and encryption rounds. These methods protect tiny datasets, such as device statuses, temperature readings, raw data, numerical values, and outputs from ICS. However, encrypting gathered images takes a long time because these methods rely on block encryption across multiple rounds to achieve the necessary security level [180]. As the industrial IoT expands and quantum computing advances, conventional encryption techniques like DES, 3DES, AES, RSA, and ECC risk becoming obsolete. These techniques are vulnerable to quantum attacks, which can decrypt data more quickly because they rely on mathematical complexity. Quantum cryptography provides a secure alternative by using quantum mechanics to provide communication channels unaffected by the most powerful quantum computers.

Wazid et al. [57] and Nita and Mihailescu [60] define quantum cryptography as an advanced branch of cryptography that applies the principles of quantum mechanics to secure communication channels. Because quantum cryptography uses the principles of quantum mechanics to protect communication and information transfer, it is naturally resistant to hacking and eavesdropping. It uses quantum bits (qubits) and their unique properties to establish secure channels for key distribution. The core principles that enable this security include Heisenberg's uncertainty principle, quantum entanglement, superposition, and the no-cloning theorem.

- Heisenberg's uncertainty principle states that measuring a quantum particle's momentum and position simultaneously with absolute precision is impossible. Quantum cryptography leverages this principle to create secure communication channels. This principle secures quantum key distribution by ensuring unauthorized access disturbs the quantum state, revealing potential security threats.
- Quantum entanglement is another fundamental principle that enables secure long-distance communication. When two or more quantum particles become entangled, their states remain strongly correlated regardless of the distance separating them. Changing one particle affects its entangled counterpart instantly. This property allows quantum cryptography to establish secure connections between communicating parties. Any attempt to measure or intercept entangled particles disturbs their state, alerting users to potential eavesdropping. Entanglement ensures that only the intended recipient can access the information, reinforcing the security of quantum key distribution.
- Superposition enhances the efficiency and security of quantum communication. Unlike classical bits, which exist in either a 0 or 1 state, qubits can exist in multiple states simultaneously until measured. This property enables the encoding of information in a way that increases computational power and security. By harnessing superposition, quantum systems can process and transmit information more efficiently than classical systems. This property strengthens encryption by making it significantly harder for attackers to determine the transmitted data without introducing detectable disturbances.
- The no-cloning theorem further ensures the security of quantum cryptography by preventing the exact duplication of an unknown quantum state. This principle prevents Eavesdroppers from making complete copies of transmitted quantum information. Errors would be introduced by any illicit attempt to reproduce quantum states, revealing the existence of an intruder. By blocking eavesdropping efforts, the no-cloning theorem guarantees that cryptographic keys stay safe while being transmitted.

These principles ensure that attempting to measure or intercept quantum states will alter their characteristics, warning authorized users of any security flaws [56][57][60][64][182]. Quantum cryptography ensures that encryption keys are spread even when they do not encode data. A fundamentally secure key exchange method impervious to classical and quantum-based attacks is offered using concepts from quantum mechanics. Quantum cryptography provides an answer as quantum computing develops by guaranteeing unbreakable security in key distribution.

8.1.Quantum key distribution

A QKD uses quantum mechanics to establish secure communication channels [60][183]. Unlike traditional encryption methods that rely on mathematical algorithms, QKD offers unconditional security by utilizing the uncertainty principle and the no-cloning theorem. For the communicating parties to identify eavesdropping, these principles make sure that any attempt to measure or intercept quantum states breaches them [56][58][63][184]. QKD improves security in quantum industrial applications by protecting vital operational parameters across production sites. Securely exchanging encrypted communications between senders and recipients ensures dependable communication. The main actors are the source and the destination [56]. QKD creates a secure communication mechanism at the network layer by allowing both parties to generate and share a shared key for message encryption and decoding [185]. The rise of different QKD protocols and applications, like Key-as-a-Service (KaaS), has attracted much interest from academia and industry. By integrating QKD into optical networks, KaaS provides secure key distribution across virtual optical networks, allowing network operators to employ quantum-based security solutions more efficiently. In addition to communication security, it is crucial for industrial applications and quantum computing networks, especially in Industry 4.0, where safeguarding private security information is crucial. It is a reliable option for protecting sensitive data in various businesses since it can identify and stop eavesdropping. [57][182]. Beyond QKD, quantum cryptography uses quantum-resistant encryption to protect data from classical and quantum attacks. These encryption techniques are divided into two primary groups: purely quantum encryption, which uses just quantum states for encryption and decryption, and QKD-based encryption, which combines QKD with traditional cryptographic algorithms. Traditional encryption techniques are increasingly under threat from developments in quantum computing, but quantum cryptography offers a secure, future-proof alternative. Since quantum cryptography exploits quantum phenomena like entanglement and superposition to ensure the confidentiality, integrity, and validity of conveyed data, it is an important development in secure communication [62]. Researchers have developed numerous QKD approaches, and each has unique characteristics. These consist of Twin-field QKD, Coherent-one-way (COW) QKD, Continuous-variable QKD (CV-QKD), and the protocols BB84, E91, and SARG04 [62].

8.2.Applications of Quantum Cryptography in IIoT

Quantum cryptography is gaining traction in the IIoT sector due to the increasing need for robust security in environments where connected devices and systems are susceptible to cyber threats. Below are brief descriptions of the key applications of quantum cryptography in IIoT.

8.2.1. Quantum key distribution

Quantum key distribution allows two parties to safely exchange cryptographic keys via potentially insecure channels using quantum mechanics concepts. It ensures data integrity and confidentiality by shielding industrial equipment against MitM attacks and eavesdropping. Industries can safeguard critical operational data and enhance supply chain management, predictive maintenance, and real-time monitoring by incorporating QKD into IIoT networks [59][61][62][184][186-188]. For instance, by facilitating secure key exchanges, QKD almost eliminates the possibility of hackers intercepting or changing communication between control systems and factory machines in an IIoT system.

8.2.2. Quantum-resistant encryption

Since conventional encryption techniques like RSA and ECC are susceptible to quantum-based threats, especially those that use Shor's algorithm to crack public-key cryptography, quantum-resistant encryption in the IIoT focuses on protecting networks from quantum computer attacks. Researchers are developing post-quantum cryptography (PQC) techniques to counter these threats, such as multivariate polynomial, lattice-, hash-, code-, and isogeny-based cryptography. These quantum-safe encryption methods ensure data integrity, confidentiality, and authentication across IIoT systems, protecting critical infrastructure such as energy grids, transportation networks, and smart factories. Integrating quantum-safe encryption into IIoT requires low processing overhead, compatibility with existing security protocols, and defense against classical and quantum adversaries. Quantum-resistant algorithms, for example, can shield vital data in smart grids, such as control signals and energy consumption patterns, from potential quantum-enabled attacks [59][62][187][188].

8.2.3. Quantum random number generation

Using quantum physics, QRNG in industrial IoT generates random numbers required for secure communications, cryptographic protocols, and system operation. Unlike classical random number generators that rely on deterministic algorithms, QRNGs use quantum processes such as photon polarization or quantum fluctuations to provide unpredictable randomness that is almost hard to duplicate or predict. By offering a strong basis for applications like secure authentication, data encryption, and defense against cyberattacks, QRNG improves cybersecurity in IIoT systems, where safe data interchange and system integrity are essential. QRNGs are perfect for creating cryptographic keys and protecting massive sensor networks in industrial settings like smart factories and driverless cars because they leverage the inherent unpredictability of quantum physics to provide a higher level of security than traditional pseudo-random techniques. With solutions based on the core ideas of quantum physics, quantum cryptography continues to transform digital security as it develops [187][188].

8.2.4. Securing communication in autonomous systems

Quantum cryptography, especially QKD, uses quantum mechanics to identify eavesdropping attempts and secure communication in autonomous IIoT systems. Protecting sensitive data and preserving operational integrity are essential in IIoT contexts where networked devices function independently. Secure key exchanges and data encryption that withstand traditional computational attacks are made possible by quantum cryptography, which offers a strong defense against hacking and illegal access. Secure communication channels are essential for autonomous systems like robots and drones, and quantum cryptography protects against manipulation and eavesdropping. For instance, in an autonomous warehouse, where robots communicate to transport goods, quantum cryptography safeguards the communication between robots and the central management system, protecting operational data such as movement patterns and inventory details [59][118][186][188][189].

8.2.5. Quantum authentication protocols

Quantum authentication protocols in the IIoT secure communication and ensure data integrity by using QKD to establish encryption and authentication keys, protecting against eavesdropping and MitM attacks. These protocols enhance the security of industrial networks, where sensitive data is transmitted, by adding a layer of protection against emerging cybersecurity threats. By leveraging quantum states, they authenticate devices, ensuring only authorized devices can access the network [59][186]. Quantum-resistant algorithms can future-proof IoT systems against powerful quantum computers [64]. In systems using biometric data for authentication, such as fingerprint or iris scans, quantum ML optimizes the recognition process, improving security by detecting anomalies that make spoofing more difficult. In IIoT-enabled healthcare facilities, quantum authentication ensures that only authorized medical devices can exchange data with hospital systems, reducing the risk of unauthorized access and malicious attacks [64].

8.2.6. Post-quantum cryptography for legacy IIoT systems

Post-quantum cryptography (PQC) focuses on developing cryptographic techniques to protect legacy IIoT systems from potential quantum computer threats. As existing protocols like RSA and ECC are vulnerable to quantum attacks, integrating quantum-resistant algorithms into these systems is essential for ensuring long-term security. This transition upgrades or replaces existing cryptographic protocols with PQC alternatives. These alternatives rely on mathematical problems that quantum computers struggle with, like lattice-based cryptography. Mostly, lattice-based algorithms present a viable remedy for the shortcomings of conventional cryptography techniques. The transition to PQC necessitates careful planning to meet system resource limitations, performance constraints, and backward compatibility to ensure a seamless integration without interfering with vital operations [187]. PQC can be implemented to protect data transfer between vintage devices and newer quantum-secure systems, avoiding a complete infrastructure upgrade in industries like oil and gas, where IIoT systems are frequently antiquated and lack quantum-resistant characteristics.

8.2.7. Quantum-enhanced sensor networks

The IIoT's quantum-enhanced sensor networks use quantum technology to improve sensor performance in industrial settings. These networks increase measurement accuracy, lower noise, and facilitate safe data transfer by utilizing concepts like superposition and entanglement. Because quantum sensors are more sensitive and accurate than classical ones, they are perfect for fault detection, precision monitoring, and optimization in the industrial, energy, and logistics sectors. These sensors make processes more dependable, effective, and secure by identifying the slightest changes in physical variables like temperature, pressure, and magnetic fields. Quantum sensors offer exact measurements in settings that need close environmental monitoring, such as chemical industry or aerospace, while guaranteeing that the data is secured and safeguarded using quantum cryptography techniques [188].

8.2.8. Eavesdropping detection

Unauthorized parties intercepting conversations, known as eavesdropping, can result in identity theft or data breaches. Secure communication is ensured by quantum cryptography, which uses quantum mechanics to identify and stop illegal data interception. Secure key exchange is made possible by protocols like QKD and BB84, which detect eavesdropping attempts by altering the quantum state of the communication channels. Both parties are made aware of the existence of an intruder by this observation-based disruption. Using quantum cryptography techniques safeguards data confidentiality and integrity when IIoT devices transmit sensitive information over potentially insecure networks, protecting against malevolent attacks and unwanted access. When unauthorized measurements are made, QKD protocols—like BB84—are built to identify such efforts by adding detectable mistakes. MitM attacks are similarly prevented by quantum cryptography [61][62][184][186].

8.2.9. Mitigating DoS attacks

Incorporating QKD into IIoT networks establishes encryption keys resistant to conventional DoS attack routes. Moreover, PQC and other quantum-resistant techniques improve defense against classical and quantum DoS attacks. By ensuring data confidentiality, availability, and integrity, these quantum-based solutions lessen the effect of DoS attacks on vital IIoT infrastructure. By incorporating quantum cryptography into secure communication protocols, secure channels are created, reducing the possibility of an attacker overloading the system. Ultimately, quantum-secure systems increase service availability and network resilience, making it harder for DoS attacks to interfere with business operations.

8.2.10. Quantum-enhanced jamming resistance

IIoT networks are susceptible to jamming attacks, in which malicious actors purposefully obstruct communication channels to impede network functionality. Techniques with quantum enhancements can make wireless networks more resilient to these kinds of attacks. These include quantum cryptography techniques, which secure the control channels of IIoT networks and make it difficult for adversaries to target specific frequencies for jamming, and quantum signal processing techniques, which enable more effective detection and mitigation of jamming signals than classical methods, guaranteeing uninterrupted communication in hostile environments [188].

8.2.11. Quantum ML for anomaly detection

Quantum ML (QML) combines quantum computing with ML techniques to analyze big datasets more effectively than traditional approaches. QML can uncover tiny anomalies that regular techniques might miss by quickly processing data and exploring high-dimensional spaces more efficiently using quantum algorithms like quantum SVM or quantum neural networks. Because of its increased processing capacity, QML is particularly useful in cybersecurity, fraud detection, and system monitoring—areas where detecting uncommon or unforeseen incidents is crucial to preserving stability and security. QML identifies irregularities and possible security breaches in IIoT network security [64][188]. Fig. 11 summarizes the applications of quantum cryptography in securing IIoT.

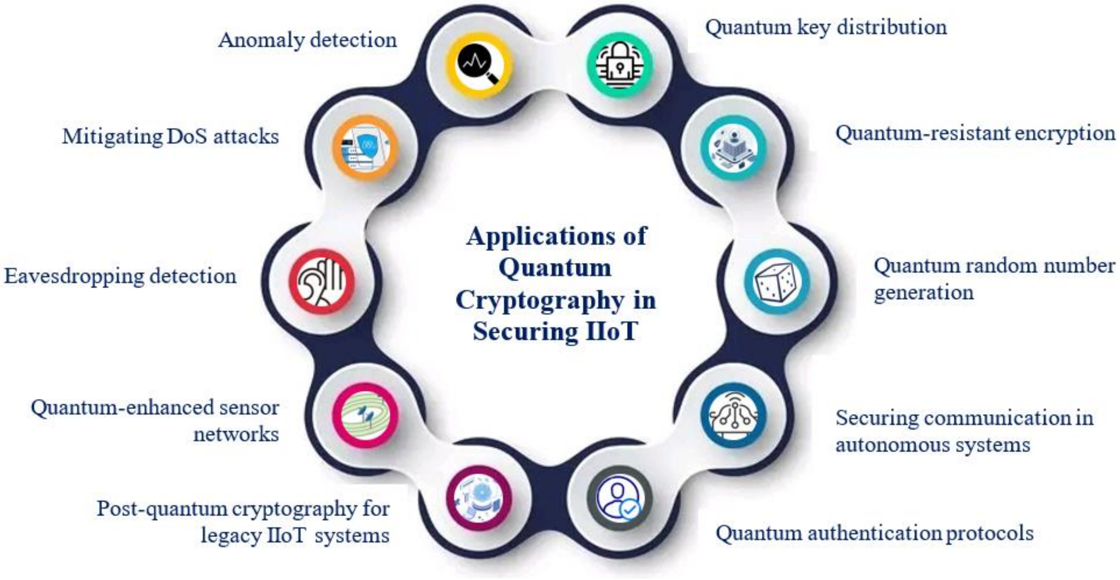
Anomaly detection
Quantum key distribution
Mitigating DoS attacks
Quantum-resistant encryption
Applications of Quantum Cryptography in Securing IIoT
Eavesdropping detection
Quantum random number generation
Quantum-enhanced sensor networks
Securing communication in autonomous systems
Post-quantum cryptography for legacy IIoT systems
Quantum authentication protocols

Fig. 12. Summary of the applications of quantum cryptography in securing IIoT.
Fig. 13.

Some notable research studies implementing quantum cryptography in securing industrial IoT include the following. Li et al. [190] developed a quantum cryptography encryption and decryption program for industrial control systems, leveraging QKD and invisible state transfer algorithms to secure data transmission. They built a simulation test environment for the system's upper and lower computers and deployed quantum algorithms on embedded systems and PCs. The tests demonstrated that quantum cryptography effectively enhances the AES key scheme. The encryption and decryption process took less than 61.8 seconds, meeting real-time requirements. Thus, quantum cryptography is well-suited to protect field-level data in ICS. Prajwal et al. [191] proposed a lightweight, quantum-safe authentication protocol for IIoT applications, utilizing Quantum Physical Unclonable Functions (qPUF). The protocol employs one-way hash functions and geometric threshold secret sharing, ensuring secure communication without storing keys in non-volatile memory, thus resisting quantum attacks. Formal verification with Scyther confirmed its resilience to various known attacks. Implemented on NodeMCU, it demonstrated low communication and computation costs, making it ideal for resource-constrained IIoT devices. The protocol provides robust security, including mutual authentication, forward secrecy, and protection against replay and DoS attacks. Bhattacharya et al. [192] proposed a dual-layered quantum ML architecture using quantum neural networks (QNN) to detect cryptojacking attacks in IIoT networks. The first layer, a QNN detection layer, applies a weighted sum on time, frequency, and network traffic, modeled as a multi-objective optimization solved by the quantum approximate optimization algorithm. The second filtration layer uses a quantum metric to filter anomalies based on set thresholds. Using the CSECIC-IDS 2018 dataset augmented with live IIoT data, the model was evaluated for various metrics such as convergence rate, attack detection time, and precision. With 60 nodes, the model achieved 11.84 KBps throughput, a 23.44%

improvement over baseline models, and an accuracy of 0.97 in classifying malign and benign requests. Kannadasan [193] introduced a quantum-assisted security framework to protect 5G nodes in massive machine-type communications for IIoT applications. The framework combines QKD with ML-based attack detection to address security challenges in 5G-enabled IIoT environments. Simulation results show a 99.7% success rate in detecting and mitigating quantum-level attacks. It also achieves a 40% reduction in latency compared to classical security approaches. This framework offers strong resilience against classical and quantum-based attacks, making it a reliable solution for securing IIoT infrastructure.

Xu et al. [194] introduced a secure cross-layer device authentication framework with quantum encryption for 5G-enabled IIoT in Industry 4.0. The system uses random hash coding on multidomain physical-layer resources to encode device identifiers securely. It employs a quantum walk-based privacy-preserving protocol to ensure high-level privacy controlled by physical resource usage. Key components include access control, AMD, device authentication, channel estimation, and small data delivery. The study also derives the upper bound of decoding errors, formulates a nonconvex integer programming problem, and demonstrates how the system achieves high privacy, scalability, and low latency under attack. Singamaneni et al. [195] introduced a dynamic QKD algorithm to secure critical public infrastructure and IIoT cyber-physical systems. Dynamic, chaotic quantum key generation is improved using their unique multi-state qubit representation, which has low computational overhead and high efficiency. The proposed QKD algorithm creates chaotic qubits for session-based dynamic keys, ensuring secure communication and distribution of sensitive IIoT data. The study demonstrated key exchange between IIoT devices without attacks and proves the model's superior security against quantum threats. It also reduces qubit transmission and key exchange rates while improving error-rate measurement for detecting snooping. Ahmad et al. [196] proposed a secure Industrial IoT architecture using true random numbers generated by a QRNG. The FireConnect IoT node from CITRIOT demonstrates a proof of concept for a quantum-safe network where a cloud-based quantum device generates random keys. They implemented QRNG on actual quantum computers and simulators, comparing the results with pseudo-random numbers from a classical computer. The scheme proves the feasibility of providing high-quality random numbers in a distributed network.

9. SYNERGISTIC INTEGRATION OF AI, BLOCKCHAIN, AND QUANTUM CRYPTOGRAPHY FOR SECURING IIoT

Integrating AI, Blockchain, and quantum cryptography transforms industrial IoT security by enhancing data integrity, securing communications, and automating threat detection. This convergence enables industries to implement robust, scalable, and future-proof security solutions. These technologies create a highly secure, resilient, and autonomous framework for IIoT systems, ensuring stronger protection against emerging cyber threats. Below are some key synergies that demonstrate their combined potential.

- *Real-time threat detection and autonomous response*: AI analyzes vast IIoT data to detect real-time anomalies and suspicious activities. Blockchain maintains data integrity by recording events on an immutable ledger, while quantum cryptography secures communication channels against interception. Together, these technologies enable AI to autonomously identify and respond to threats while ensuring all actions remain verifiable and secure.

- *Decentralized identity management and authentication*: Blockchain ensures that only authorized IIoT devices connect to the network by providing decentralized, tamper-proof identities. AI monitors and analyzes device behavior, detecting and flagging any irregularities for further investigation. Quantum cryptography secures device communications, preventing identity spoofing and MitM attacks.

- *Blockchain-verified data integrity for predictive maintenance*: AI-powered predictive maintenance algorithms depend on accurate data to predict potential failures. By using Blockchain to securely record sensor data and equipment status in a tamper-proof ledger, these systems add an extra layer of verification for the data that AI relies on. Quantum cryptography further protects the communication between IIoT devices, reporting critical sensor data and ensuring its integrity during transmission.

- *Secure data sharing and collaboration*: AI analyzes data from multiple IIoT devices to detect patterns or trends that may signal potential security threats. Blockchain enables secure and transparent data sharing among stakeholders, such as manufacturers, vendors, and service providers, without centralizing sensitive information. At the same time, quantum cryptography ensures the privacy and protection of shared data, safeguarding it from eavesdropping, even in multi-party collaboration scenarios.

- *Smart contracts for secure automation and device management*: Smart contracts on the Blockchain autonomously execute secure transactions when predefined conditions are met, such as shutting down a compromised device. AI monitors the network to detect when these conditions are triggered and initiates the corresponding smart contract actions. Meanwhile, quantum cryptography ensures that all communications regarding these automated actions remain encrypted, safeguarding them from tampering or interception by unauthorized parties.

- *Enhanced supply chain traceability and security*: AI predicts disruptions and vulnerabilities in the IIoT-powered supply chain, while Blockchain tracks every process step, from raw material procurement to delivery, ensuring data immutability and transparency. Quantum cryptography secures data exchanges and communications throughout the supply chain, protecting sensitive business information and preventing cyber-attacks.
- *Quantum-resistant encryption for future-proof security*: Quantum cryptography safeguards IIoT systems from the threat of quantum computers that could compromise traditional encryption methods like RSA or ECC. AI adapts to emerging threat patterns instantly, while Blockchain securely stores encrypted data and ensures its integrity over time. Together, these technologies strengthen the resilience of IIoT networks against future cryptographic risks.
- *Secure communication between distributed IIoT devices*: Blockchain enables secure and decentralized data exchange between IIoT devices, while AI monitors this data to detect anomalies and predict potential malfunctions or security breaches. Quantum cryptography safeguards communication between IoT devices, protecting them from quantum-level threats and strengthening the overall integrity of the IIoT network.
- *AI-powered threat intelligence with immutable Blockchain logs*: AI gathers threat intelligence from network traffic and IIoT device behavior to predict potential attacks. Blockchain records these insights, making them immutable and preventing any modification or deletion of threat data. Quantum cryptography ensures the secure transmission of these threat intelligence reports and predictive models, safeguarding them from interception by malicious actors.
- *Multi-layered security for critical IIoT infrastructure*: Combining AI, Blockchain, and quantum cryptography creates a multi-layered security framework to protect critical IIoT infrastructure. AI analyzes data instantly and provides predictive insights, while Blockchain ensures data integrity and secures transactions. Quantum cryptography safeguards the confidentiality of sensitive communications. Together, these technologies form a robust and adaptive security architecture that can effectively respond to evolving threats in the IIoT landscape.

AI, Blockchain, and quantum cryptography enhance IIoT security by addressing different aspects of the security challenge. Their integration strengthens IIoT networks, making them more secure, adaptable, and resilient to future threats. These technologies offer a comprehensive, multi-faceted approach to safeguarding IIoT systems.

10. CHALLENGES AND LIMITATIONS

Integrating AI, Blockchain, and quantum cryptography offers a promising approach to securing the IIoT, but real-world deployment faces several limitations and challenges. Below are some of these limitations and challenges:

- *Technological limitations*: QKD, in particular, is still in its infancy and has not been widely used in the business world. Challenges such as photon loss in fiber-optic cables and a restricted transmission range hinder its practical use in industrial IoT applications. The lack of universal standards for integrating AI, Blockchain, and quantum cryptography into IIoT security frameworks also causes interoperability issues between devices and networks. IIoT devices also face computational power, memory, and battery life limitations. Running complex AI models, Blockchain consensus mechanisms, or quantum-safe encryption algorithms on edge devices is challenging.
- *Computational and performance bottlenecks*: AI-driven security mechanisms require extensive data processing, which can introduce delays in IIoT networks. Similarly, computationally intensive Blockchain consensus mechanisms, such as Proof-of-Work, are unsuitable for real-time IIoT applications. Integrating AI for anomaly detection, Blockchain for data integrity, and quantum cryptography for encryption adds to processing time, resulting in higher latency for critical IIoT operations. These technologies, including quantum cryptographic operations and AI-based security models, demand significant computational power, which can quickly deplete the battery life of IIoT devices. Moreover, Blockchain's cryptographic hashing and consensus mechanisms further worsen this issue.
- *Scalability challenges*: Traditional Blockchain networks struggle with low transaction throughput, making them inefficient for managing large volumes of IIoT transactions. Storing IIoT device data on these networks causes rapid ledger growth, demanding significant storage and computational resources, often impractical for lightweight IIoT devices. Implementing quantum cryptographic solutions at scale requires a robust quantum communication infrastructure, which is costly and not yet widely accessible.
- *Interoperability and integration issues*: IIoT environments involve various devices, protocols, and communication standards, making integrating AI, Blockchain, and quantum cryptography across these heterogeneous systems challenging. Combining AI models, Blockchain frameworks, and quantum cryptographic protocols requires significant adaptation. However, compatibility issues often arise due to differences in programming languages, hardware, and network architectures.
- *Security and privacy risks*: AI-driven security solutions face vulnerabilities from adversarial attacks, where attackers manipulate input data to deceive AI models, causing false positives or false negatives in threat detection.

While quantum cryptography improves security, future quantum computers could compromise current Blockchain encryption schemes (e.g., RSA, ECC), undermining Blockchain-based IIoT security. Smart contracts used for automated IIoT security enforcement may contain bugs or vulnerabilities that attackers could use to gain illegal access or manipulate data. Blockchain's immutability conflicts with privacy regulations like GDPR, which require data modification and deletion capabilities. AI-driven analytics depend on vast IIoT data, raising concerns about exposing sensitive information. Although quantum cryptography offers secure communication, it does not inherently address data privacy at the storage or application level.

- *Regulatory and ethical constraints*: AI, Blockchain, and quantum cryptography deployment in IIoT security must adhere to GDPR and CCPA data protection laws. Blockchain's immutable nature challenges regulations requiring data deletion, like the "right to be forgotten." AI-powered security systems can introduce biases, potentially leading to unfair or inaccurate threat detection and risk assessments in IIoT environments. Many quantum cryptographic technologies face export control laws restricting their availability in certain regions.
- *Energy consumption*: The combination of these technologies creates high energy demands. Blockchain consensus mechanisms (e.g., Proof of Work) consume significant energy, quantum cryptography relies on complex mathematical operations, and AI models need continuous training and inference. As a result, energy efficiency becomes a critical concern, especially in edge computing environments.
- *High implementation costs*: Adopting AI, Blockchain, and quantum cryptography can be costly for IIoT industries, e.g., small and medium enterprises, due to the high demands for specialized hardware, software, and skilled professionals. These advanced security mechanisms often create a significant financial burden, making it challenging for such businesses to implement them.
- *Lack of skilled workforce*: Integrating AI, Blockchain, quantum cryptography, and IIoT security demands expertise in all three areas. However, a significant shortage of professionals with skills across these domains makes it challenging for organizations to implement and maintain these technologies effectively.

Ongoing research, technological advancements, and industry collaboration are essential to creating a secure, scalable, and efficient framework for IIoT security. While integrating AI, Blockchain, and quantum cryptography offers a strong foundation for securing IIoT networks, addressing current limitations in technology, computation, scalability, security, and regulation is crucial. Future research will be key to overcoming these challenges and enabling the widespread adoption of secure IIoT networks.

11. FUTURE RESEARCH DIRECTIONS AND RECOMMENDATIONS

IIoT systems enhance predictability, detect anomalies, and enable near-real-time decision-making by leveraging AI, Blockchain, and quantum cryptography. However, integrating these technologies is complex, and to solve these problems and build on previous developments, more research is needed in several crucial areas. The following are a few of the future research studies.

- *AI-driven quantum cryptography*: Future studies should examine how AI algorithms might improve the functionality and usefulness of quantum cryptography protocols in IIoT settings. It should specifically look at how AI might improve the distribution and management of real-time quantum keys, guaranteeing scalable and reliable security for IIoT networks.
- *Decentralized AI-based threat detection and response mechanisms*: Creating decentralized AI models for IIoT network anomaly detection and predictive threat responses is critical. These models can use Blockchain's security characteristics to guarantee data integrity and transparency. This study will investigate methods for making AI-driven reactions both autonomous and auditable to improve the dependability and credibility of threat mitigation in IIoT contexts.
- *Secure data marketplaces for IIoT devices powered by Blockchain*: It is necessary to investigate the creation of Blockchain-based systems that allow IIoT devices to safely communicate data with other devices or third parties, enabling reliable transactions. Using smart contracts to secure and validate shared data while investigating AI's function in confirming data quality before exchange.
- *Quantum-resistant Blockchain protocols for IIoT networks*: Investigate how quantum-resistant Blockchain algorithms can secure IIoT devices and networks against quantum computing threats. Make current Blockchain technologies, such as proof of stake and proof of work, quantum-safe while preserving their scalability and usefulness in business contexts.
- *AI-powered Blockchain consensus algorithms for enhanced IIoT security*: AI can potentially improve Blockchain consensus mechanisms in IIoT networks by providing adaptive models that optimize security, lower energy

consumption, and improve scalability. AI can instantaneously adjust consensus methods by dynamically predicting network conditions, ensuring dependable performance and efficient resource utilization. This method lessens the computational burden related to conventional consensus procedures while preserving the security and dependability of IIoT systems.

- *Federated learning for a secure, privacy-preserving IIoT with Blockchain*: Future studies should examine how FL and Blockchain integration could improve industrial IoT systems' security and privacy. FL protects personal information while enabling the training of decentralized AI models across devices. Blockchain offers a safe, unhackable ledger for documenting and confirming data transfers and model revisions. By combining FL with Blockchain, IIoT devices can collaborate to train models in a decentralized architecture while preserving data integrity, transparency, and resilience to cyberattacks.
- Future research should examine the use of AI and quantum cryptography for zero-knowledge proofs in the IIoT to assess device behaviors and transactions while maintaining data privacy. It should also investigate using quantum cryptography to defend these proofs against quantum attacks. It should also examine how AI might optimize proof generation and verification, increasing IIoT systems' efficiency.
- *Scalability of AI and Blockchain solutions in large-scale IIoT environments*: Future research might investigate the scalability problems that arise when integrating AI, Blockchain, and quantum cryptography in large-scale IIoT networks. It can also examine how Blockchain scaling solutions like sharding and sidechains can be used with AI-powered threat management systems to increase security and productivity in industrial settings.
- *Post-quantum AI for IIoT infrastructure security*: AI algorithms used for IIoT security will significantly impact future advancements in quantum computing. Future research must look at developing quantum-resistant AI models and integrating quantum cryptography to adapt AI to remain secure and effective in a post-quantum environment. These advancements allow IIoT infrastructures to maintain robust security against emerging quantum threats.
- *Post-quantum cryptography standards*: The NIST is developing and standardizing post-quantum cryptographic algorithms to replace current cryptographic standards in IIoT networks. These new algorithms will ensure long-term security against the threats posed by quantum computing.
- *Quantum-enhanced ML for security*: Quantum computing enhances ML algorithms for threat detection and security analysis by processing vast data at unprecedented speeds. This capability improves the ability to identify threats and mitigate risks in IIoT systems, enabling faster and more effective security measures.

By exploring future research directions, researchers can improve the security of IIoT systems, ensuring these vital networks operate safely and efficiently. These directions focus on addressing the complex security challenges associated with the digital transformation of industries.

12. CONCLUSIONS

Integrating AI, Blockchain, and quantum cryptography offers a transformative approach to enhancing the security, reliability, and efficiency of the IIoT. As IIoT systems become more complex and interconnected, conventional security mechanisms struggle to keep pace with evolving cyber threats, latency constraints, and concerns around data integrity. This study examines how the convergence of these advanced technologies can create a robust security framework for IIoT ecosystems. The synergy of these technologies offers a comprehensive, future-ready solution for securing IIoT systems. Technological constraints, performance snags, scalability problems, and interoperability issues are some difficulties in integrating these technologies. Risks regarding security and privacy, ethical and legal limitations, energy use, high implementation expenses, and a lack of qualified personnel must all be addressed. Notwithstanding these difficulties, the potential of Blockchain, AI, and quantum cryptography working together promises to protect IIoT infrastructures from advanced cyberattacks. Together, they build a trust-based ecosystem that guarantees data availability, confidentiality, and integrity—all essential for protecting industrial operations. Adopting this comprehensive security framework will be crucial to determining the direction of IIoT as research and innovation advance. It will promote broad adoption in the transportation, energy, manufacturing, and healthcare sectors. In conclusion, the fusion of AI, Blockchain, and quantum cryptography in IIoT security necessitates collaborative efforts from academia, industry, and policymakers. This interdisciplinary approach forms a formidable security paradigm, mitigating risks while enhancing efficiency and trust. Standardization, regulatory frameworks, and cross-sector partnerships will be pivotal in unlocking the full potential of these technologies. Furthermore, addressing interoperability between legacy IIoT systems and these emerging technologies is necessary for seamless deployment. Future work should focus on developing lightweight AI models, improving Blockchain consensus mechanisms to increase transaction throughput, and advancing quantum-safe cryptographic techniques for real-world feasibility. Organizations can build resilient, intelligent, and future-ready IIoT security systems by addressing current challenges and leveraging ongoing advancements. While obstacles remain, continuous progress in these fields will enable the practical implementation of this framework, paving the way for a more secure and resilient IIoT infrastructure in the digital age.

Conflicts of Interest

The authors declare no conflict of interest.

Funding

This research received no external funding.

Acknowledgment

We sincerely appreciate the reviewers’ insightful feedback and constructive suggestions, which played a crucial role in shaping this work. We also thank our friends for their patience, understanding, and unwavering support throughout this journey. Their encouragement made this study possible.

References

[1] P. K. Dutta, S. M. El-kenawy, G. Ali, and K. Dhoska, “An Energy Consumption Monitoring and Control System in Buildings using Internet of Things,” *Babylonian Journal of Internet of Things*, vol. 2023, pp. 38–47, 2023. https://doi.org/10.58496/BJIoT/2023/006

[2] M. M. Mijwil, I. Bala, G. Ali, M. Aljanabi, M. Abotaleb, R. Doshi, . . . E.-S. M. El-Kenawy, “Sensing of Type 2 Diabetes Patients Based on Internet of Things Solutions: An Extensive Survey,” In K. K. Hiran, R. Doshi, and M. Patel (Eds.), *Modern Technology in Healthcare and Medical Education: Blockchain, IoT, AR, and VR* (pp. 34-46). IGI Global, 2024. doi:10.4018/979-8-3693-5493-3.ch003

[3] X. Mu, and M. F. Antwi-Afari, “The applications of Internet of Things (IoT) in industrial management: a science mapping review,” *International Journal of Production Research*, vol. 62, no. 5, pp. 1928–1952, 2024. https://doi.org/10.1080/00207543.2023.2290229

[4] T. Gaber, J. B. Awotunde, S. O. Folorunso, S. A. Ajagbe, and E. Eldesouky, “Industrial internet of things intrusion detection method using machine learning and optimization techniques,” *Wireless Communications and Mobile Computing,* vol. *2023,* pp. 1–15, 2023. https://doi.org/10.1155/2023/3939895

[5] I. B. Ababio, J. Bieniek, M. Rahouti, T. Hayajneh, M. Aledhari, D. C. Verma, and A. Chehri, “A Blockchain-Assisted federated learning framework for secure and Self-Optimizing digital twins in industrial IoT,” *Future Internet,* vol. 17, no. 1, pp. 1–20, 2025. https://doi.org/10.3390/fi17010013

[6] K. Hassini, and M. Lazaar, “Enhancing Industrial-IoT cybersecurity through generative models and convolutional neural networks,” In *Lecture notes in networks and systems* (pp. 543–558). Springer, 2024. https://doi.org/10.1007/978-3-031-74491-4_41

[7] I. Bala, M. M. Mijwil, G. Ali, and E. Sadıkoğlu, “Analyzing the Connection Between AI and Industry 4.0 from a Cybersecurity Perspective: Defending the Smart Revolution,” *Mesopotamian Journal of Big Data*, vol. 2023, pp. 63–69, 2023. https://doi.org/10.58496/mjbd/2023/009

[8] S. Thapar, D. Mishra, and R. Saini, “Secure transmission in NOMA-Enabled industrial IoT with Resource-Constrained untrusted devices,” *IEEE Transactions on Industrial Informatics,* vol. 20, no. 1, pp. 411–420, 2024. https://doi.org/10.1109/tii.2023.3263276

[9] M. I. Joha, M. M. Rahman, M. S. Nazim, and Y. M. Jang, “A Secure IIoT Environment That Integrates AI-Driven Real-Time Short-Term Active and Reactive Load Forecasting with Anomaly Detection: A Real-World Application,” *Sensors,* vol. 24, no. 23, pp. 1–33, 2024. https://doi.org/10.3390/s24237440

[10] S. Lee, and S. Park, “Mobility-Assisted Digital Twin Network Optimization over Industrial Internet of Things,” *Applied Sciences,* vol. 14, no. 19, pp. 1–13, 2024. https://doi.org/10.3390/app14199090

[11] M. A. Jarwar, J. W. C. FREng, and S. Ali, “Modelling Industrial IoT Security Using Ontologies: A Systematic Review,” *IEEE Open Journal of the Communications Society*, pp. 1–34, 2025. https://doi.org/10.1109/ojcoms.2025.3532224

[12] H. H. Azeez, M. Sharbaf, B. Zamani, and S. Kolahdouz-Rahimi, “Applying pattern language to enhance IIoT system design and Integration: From Theory to practice,” *Information*, vol. 15, no. 10, pp. 1–23, 2024. https://doi.org/10.3390/info15100595

[13] V. R. Kebande, and R. A. Ikuesan, “Standardizing Industrial Internet of Things (IIoT) forensic processes,” *Security and Privacy,* vol. 8, no. 1, pp. 1–17, 2025. https://doi.org/10.1002/spy2.485

[14] F. T. Fera, and C. Spandonidis, “An Artificial Intelligence and industrial Internet of Things-Based framework for sustainable hydropower plant operations,” *Smart Cities,* vol. 7, no. 1, pp. 496–517, 2024. https://doi.org/10.3390/smartcities7010020

[15] S. Banerjee, P. Kumari, and T. Maity, “Development of MQTT Protocol-Based Sensor Data Subscription Using Raspberry-Pi as a Server Mode for IIoT Application,” *2024 IEEE International Conference on Smart Power Control and Renewable Energy (ICSPCRE),* Rourkela, India, 19-21 July 2024, pp. 1–5. https://doi.org/10.1109/icspcre62303.2024.10675281

[16] E. Villar, I. M. Toral, I. Calvo, O. Barambones, and P. Fernández-Bustamante, “Architectures for Industrial AIoT Applications,” *Sensors,* vol. 24, no. 15, pp. 1–30, 2024. https://doi.org/10.3390/s24154929

[17] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi, “Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, threats, and future directions,” *Sensors,* vol. 25, no. 1, pp. 1–42, 2025. https://doi.org/10.3390/s25010213

[18] T. Zvarivadza, M. Onifade, O. Dayo-Olupona, K. O. Said, J. M. Githiria, B. Genc, and T. Celik, “On the impact of Industrial Internet of Things (IIoT) - mining sector perspectives,” *International Journal of Mining Reclamation and Environment,* vol. 38, no. 10, pp. 771–809, 2024. https://doi.org/10.1080/17480930.2024.2347131

[19] L. S. Vailshery, ‘‘Number of internet of things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033,” Statista. Retrieved February 12, 2025, from https://www.statista.com/aboutus/our-research-commitment/2816/lionel-sujay-vailshery (accessed March 8, 2025)

[20] A. Kaur, "Intrusion Detection Approach for Industrial Internet of Things Traffic using Deep Recurrent Reinforcement Learning Assisted Federated Learning," *IEEE Transactions on Artificial Intelligence, vol.* 6, no. 1, pp. 1–13, 2025. https://doi.org/10.1109/tai.2024.3443787

[21] R. Sinha, P. Thakur, S. Gupta, and A. Shukla, "Development of lightweight intrusion model in Industrial Internet of Things using deep learning technique," *Discover Applied Sciences,* vol. 6, no. 7, pp. 1–15, 2024. https://doi.org/10.1007/s42452-024-06044-4

[22] N. Alenezi, and A. Aljuhani, "Intelligent intrusion detection for industrial internet of things using clustering techniques," *Computer Systems Science and Engineering,* vol. 46, no. 3, pp. 2899–2915, 2023. https://doi.org/10.32604/csse.2023.036657

[23] K. M. Alalayah, F. S. Alrayes, J. S. Alzahrani, K. M. Alaidarous, I. M. Alwayle, H. Mohsen, I. A. Ahmed, and M. A. Duhayyim, "Optimal deep learning based intruder identification in industrial internet of things environment," *Computer Systems Science and Engineering*, vol. 46, no. 3, pp. 3121–3139, 2023. https://doi.org/10.32604/csse.2023.036352

[24] A. H. Eyeleko, and T. Feng, "A critical overview of industrial internet of things security and privacy issues using a Layer-Based Hacking scenario," *IEEE Internet of Things Journal,* vol. 10, no. 24, pp. 21917–21941, 2023. https://doi.org/10.1109/jiot.2023.3308195

[25] A. Shahidinejad, and J. Abawajy, "Efficient provably secure authentication protocol for multidomain IIOT using a combined Off-Chain and On-Chain approach," *IEEE Internet of Things Journal,* vol. 11, no. 9, pp. 15241–15251, 2024. https://doi.org/10.1109/jiot.2023.3347677

[26] M. N. Jamil, O. Schelén, A. A. Monrat, and K. Andersson, "Enabling industrial internet of things by leveraging distributed Edge-to-Cloud Computing: Challenges and opportunities," *IEEE Access,* vol. 12, pp. 127294–127308, 2024. https://doi.org/10.1109/access.2024.3454812

[27] A. N. Alvi, B. Ali, M. S. Saleh, M. Alkhathami, D. Alsadie, and B. Alghamdi, "Secure computing for Fog-Enabled Industrial IoT," *Sensors,* vol. 24, no. 7, pp. 1–21, 2024. https://doi.org/10.3390/s24072098

[28] P. Dini, L. Diana, A. Elhanashi, and S. Saponara, "Overview of AI-Models and Tools in embedded IIoT Applications," *Electronics*, vol. 13, no. 12, pp. 1–33, 2024. https://doi.org/10.3390/electronics13122322

[29] A. Mehmood, A. Shafique, N. Kumar, and M. N. Bhutta, "Data security in the Industrial Internet of Things (IIoT) through a triple-image encryption framework leveraging 3-D NEAT, 1DCJ, and 4DHCFO techniques," *Computers & Electrical Engineering*, vol. 118, pp. 1–27, 2024. https://doi.org/10.1016/j.compeleceng.2024.109354

[30] T. Rehman, N. Tariq, F. A. Khan, and S. U. Rehman, "FFL-IDS: a FOG-Enabled Federated Learning-Based Intrusion Detection System to counter jamming and spoofing attacks for the industrial internet of things," *Sensors,* vol. 25, no. 1, pp. 1–34, 2024. https://doi.org/10.3390/s25010010

[31] V. Demertzi, S. Demertzis, and K. Demertzis, "An overview of privacy dimensions on the industrial Internet of things (IIoT)," *Algorithms*, vol. 16, no. 8, pp. 1–32, 2023. https://doi.org/10.3390/a16080378

[32] M. S. Farooq, M. Abdullah, S. Riaz, A. Alvi, F. Rustam, M. A. L. Flores, J. C. Galán, M. A. Samad, and I. Ashraf, "A survey on the Role of Industrial IoT in Manufacturing for Implementation of smart Industry," *Sensors,* vol. 23, no. 21, pp. 1–38, 2023. https://doi.org/10.3390/s23218958

[33] A. K. Mishra, and M. Wazid, "Design of a cloud-based security mechanism for Industry 4.0 communication," *2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC),* Jalandhar, India, 26-28 May 2023, pp. 337–343. https://doi.org/10.1109/icsccc58608.2023.10176702

[34] O. Aouedi, T. Vu, A. Sacco, D. C. Nguyen, K. Piamrat, G. Marchetto, and Q. Pham, "A survey on intelligent Internet of Things: applications, security, privacy, and future directions," *IEEE Communications Surveys & Tutorials,* pp. 1–56, 2024. https://doi.org/10.1109/comst.2024.3430368

[35] J. Cecílio, and A. Souto, "Security Issues in Industrial Internet-of-Things: Threats, Attacks and Solutions," *2024 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0 & IoT)*, Firenze, Italy, 29-31 May 2024, pp. 458–463. https://doi.org/10.1109/metroind4.0iot61288.2024.10584217

[36] Y. Shan, Y. Yao, X. Zhou, T. Zhao, B. Hu, and L. Wang, "CFL-IDS: An effective clustered federated learning framework for industrial internet of things intrusion detection," *IEEE Internet of Things Journal,* vol. 11, no. 6, pp. 10007–10019, 2024. https://doi.org/10.1109/jiot.2023.3324302

[37] B. Soudan, " Cybersecurity of digital twins in industrial IoT environments," *2024 Advances in Science and Engineering Technology International Conferences (ASET),* Abu Dhabi, United Arab, 03-05 June 2024, pp. 1–6. https://doi.org/10.1109/aset60340.2024.10708640

[38] M. Adil, A. Farouk, H. Abulkasim, A. Ali, H. Song, and Z. Jin, "NG-ICPS: Next generation Industrial-CPS, Security Threats in the era of Artificial Intelligence, Open challenges with future research directions," *IEEE Internet of Things Journal,* vol. 12, no. 2, pp. 1343–1367, 2025. https://doi.org/10.1109/jiot.2024.3486659

[39] P. R. Agbedanu, S. J. Yang, R. Musabe, I. Gatare, and J. Rwigema, "A scalable approach to internet of things and industrial internet of things security: Evaluating Adaptive Self-Adjusting Memory K-Nearest Neighbor for Zero-Day attack detection," *Sensors*, vol. 25, no. 1, pp. 1–35, 2025. https://doi.org/10.3390/s25010216

[40] S. H. Mekala, Z. Baig, A. Anwar, and S. Zeadally, "Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions," *Computer Communications,* vol. 208, pp. 294–320, 2023. https://doi.org/10.1016/j.comcom.2023.06.020

[41] R. Ullah, A. Mehmood, M. A. Khan, C. Maple, and J. Lloret, “An optimal secure and reliable certificateless proxy signature for industrial internet of things,” *Peer-to-Peer Networking and Applications*, vol. 17, no. 4, pp. 2205–2220, 2024. https://doi.org/10.1007/s12083-024-01654-6

[42] M. Shahin, M. Maghanaki, A. Hosseinzadeh, and F. F. Chen, “Advancing Network Security in Industrial IoT: A Deep Dive into AI-Enabled Intrusion Detection Systems,” *Advanced Engineering Informatics*, vol. 62, pp. 102685, 2024. https://doi.org/10.1016/J.AEI.2024.102685

[43] X. Wang, W. Wang, C. Huang, P. Cao, Y. Zhu, and Q. Wu, “Blockchain-Based certificateless conditional anonymous authentication for IIoT,” *IEEE Systems Journal*, vol. 18, no. 1, pp. 656–667, 2024. https://doi.org/10.1109/jsyst.2023.3345370

[44] S. Yu, R. Zhai, Y. Shen, G. Wu, H. Zhang, S. Yu, and S. Shen, “Deep Q-Network-Based Open-Set intrusion detection solution for industrial internet of things,” *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 12536–12550, 2024. https://doi.org/10.1109/jiot.2023.3333903

[45] T. Le, Y. E. Oktian, and H. Kim, “XGBOOST for Imbalanced Multiclass Classification-Based Industrial Internet of Things Intrusion Detection Systems,” *Sustainability*, vol. 14, no. 14, pp. 1–21, 2022. https://doi.org/10.3390/su14148707

[46] Y. F. Liu, S. C. Li, X. H. Wang, and L. Xu, “A review of hybrid cyber threats modelling and detection using artificial intelligence in IIoT,” *Computer Modeling in Engineering & Sciences*, vol. 140, no. 2, pp. 1233-1261, 2024. https://doi.org/10.32604/cmes.2024.046473

[47] M. Schmitt, “Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection,” *Journal of Industrial Information Integration*, vol. 36, pp, 1–12, 2023. https://doi.org/10.1016/j.jii.2023.100520

[48] A. K. Tyagi, “Blockchain and artificial intelligence for cyber security in the era of internet of things and industrial internet of things applications,” In *Advances in computational intelligence and robotics book series* (pp. 171–199). IGI Global, 2023. https://doi.org/10.4018/979-8-3693-0659-8.ch007

[49] A. Yazdinejad, M. Kazemi, R. M. Parizi, A. Dehghantanha, and H. Karimipour, “An ensemble deep learning model for cyber threat hunting in industrial internet of things,” *Digital Communications and Networks*, vol. 9, no. 1, pp. 101–110, 2023. https://doi.org/10.1016/j.dcan.2022.09.008

[50] T. Hasan, J. Malik, I. Bibi, W. U. Khan, F. N. Al-Wesabi, K. Dev, and G. Huang, “Securing industrial internet of things against botnet attacks using hybrid deep learning approach,” *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2952–2963, 2023. https://doi.org/10.1109/tnse.2022.3168533

[51] I. Bibi, A. Akhunzada, and N. Kumar, “Deep AI-Powered cyber threat analysis in IIoT,” *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7749–7760, 2023. https://doi.org/10.1109/jiot.2022.3229722

[52] M. Humayun, N. Tariq, M. Alfayad, M. Zakwan, G. Alwakid, and M. Assiri, “Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive survey,” *IEEE Access*, vol. 12, pp. 25469–25490, 2024. https://doi.org/10.1109/access.2024.3365634

[53] B. Pimentel, and R. Pinto, “A Blockchain Approach Towards Secure Industrial Internet of Things Management,” *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*, Aveiro, Portugal, 12-27 October 2023, pp. 1–6. https://doi.org/10.1109/wf-iot58464.2023.10539412

[54] V. P. Patil, and S. Ohatkar, “Blockchain for IoT/Industrial IoT applications,” *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, Pune, India, 17-19 October 2024, pp. 1–7. https://doi.org/10.1109/icbds61829.2024.10837075

[55] M. Soori, F. K. G. Jough, R. Dastres, and B. Arezoo, “Blockchains for industrial Internet of Things in sustainable supply chain management of industry 4.0, a review,” *Sustainable Manufacturing and Service Economics*, vol. 3, pp. 1–18, 2024. https://doi.org/10.1016/j.smse.2024.100026

[56] P. Radanliev, “Artificial intelligence and quantum cryptography,” *Journal of Analytical Science and Technology*, vol. 15, no. 4, pp. 1–17, 2024. https://doi.org/10.1186/s40543-024-00416-6

[57] M. Wazid, A. K. Das, and Y. Park, “Generic Quantum Blockchain-Envisioned Security Framework for IoT Environment: Architecture, Security Benefits and Future Research,” *IEEE Open Journal of the Computer Society*, vol. 5, pp. 248–267, 2024. https://doi.org/10.1109/OJCS.2024.3397307

[58] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, “Securing IoT devices: A novel approach using Blockchain and quantum cryptography,” *Internet of Things*, vol. 25, pp. 1–16, 2024. https://doi.org/10.1016/j.iot.2023.101019

[59] S. T. Whyte, “Quantum Cryptography and its Implications in Cybersecurity: Securing Communication in the Quantum Era,” *American International Journal of Computer Science and Information Technology*, vol. 9, no. 3, pp. 16–28, 2024. https://doi.org/10.5281/zenodo.13709957

[60] S. L. Nita, and M. I. Mihailescu, Cryptography and Cryptanalysis in Java: Creating and Programming Advanced Algorithms with Java SE 21 LTS and Jakarta EE 11 (2nd ed.). Berkeley, CA: Apress , 2024. https://doi.org/10.1007/979-8-8688-0441-0

[61] D. R. Ojha, “Quantum computing: Potential impacts on cryptography and data security,” *Journal of Durgalaxmi*, vol. 3, no. 1, pp. 87–106, 2024. https://doi.org/10.3126/jdl.v3i1.73848

[62] S. K. Sahu, and K. Mazumdar, “State-of-the-art analysis of quantum cryptography: applications and future prospects,” *Frontiers in Physics*, vol. 12, no. 1–13, 2024. https://doi.org/10.3389/fphy.2024.1456491

[63] C. G. Kinyua, “The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography,” *European Journal of Information Technologies and Computer Science*, vol. 5, no. 1, pp. 1–10, 2025. https://doi.org/10.24018/ejcompute.2025.5.1.146

[64] V. Rishiwal, U. Agarwal, M. Yadav, S. Tanwar, D. Garg, and M. Guizani, “A New Alliance of Machine Learning and Quantum Computing: Concepts, Attacks, and Challenges in IoT Networks,” *IEEE Internet of Things Journal*, 1–22, 2025. https://doi.org/10.1109/JIOT.2025.3535414

[65] M. Mahmood, and J. Abdul-Jabbar, “Securing Industrial Internet of Things (Industrial IoT)- A Reviewof Challenges and Solutions,” *Al-Rafidain Engineering Journal (AREJ)*, vol. 28, no. 1, pp. 312–320, 2023. https://doi.org/10.33899/RENGJ.2022.135292.1196

[66] V. R., Kebande, and A. I. Awad, “Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions,” *ACM Computing Surveys*, vol. 56, no. 5, pp. 1–37, 2024. https://doi.org/10.1145/36350

[67] T. L. Narayana, C. Venkatesh, A. Kiran, C. B. J, A. Kumar, S. B. Khan, A. Almusharraf, and M. T. Quasim, “Advances in real time smart monitoring of environmental parameters using IoT and sensors,” *Heliyon*, vol. 10, no. 7, pp. e28195, 2024. https://doi.org/10.1016/J.HELIYON.2024.E28195

[68] S. F. Ahmed, M. S. B. Alam, M. Hoque, A. Lameesa, S. Afrin, T. Farah, M. Kabir, G. Shafiullah, and S. Muyeen, “Industrial Internet of Things enabled technologies, challenges, and future directions,” *Computers & Electrical Engineering*, vol. 110, pp. 1–16, 2023. https://doi.org/10.1016/j.compeleceng.2023.108847

[69] OpenAI. “ChatGPT [Large language model],” ChatGPT. https://chatgpt.com (accessed February 26, 2025)

[70] K. Li, Y. Zhang, Y. Huang, Z. Tian, and Z. Sang, “Framework and capability of industrial IoT infrastructure for smart Manufacturing,” *Standards*, vol. 3, no. 1, pp. 1–18, 2023. https://doi.org/10.3390/standards3010001

[71] H. Alshahrani, A. Khan, M. Rizwan, M. S. A. Reshan, A. Sulaiman, and A. Shaikh, “Intrusion Detection Framework for industrial internet of things using software defined network,” *Sustainability*, vol. 15, no. 11, pp. 1–18, 2023. https://doi.org/10.3390/su15119001

[72] G. Beniwal, and A. Singhrova, “A systematic literature review on IoT gateways,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 9541–9563, 2022. https://doi.org/10.1016/J.JKSUCI.2021.11.007

[73] S. Mujawar, A. Deshpande, A. Gherkar, S. E. Simon, and B. Prajapati, “Introduction to Human-Machine Interface,” In M. Rishabha, S. Sonali, B. Prajapati, & S. K. Singh (Eds.), *Human Machine Interface: Making Healthcare Digital* (pp. 1–23). John Wiley & Sons, 2023. https://doi.org/10.1002/9781394200344.CH1

[74] M. Mowbray, M. Vallerio, C. Perez-Galvan, D. Zhang, A. Del Rio Chanona, and F. J. Navarro-Brull, “Industrial data science - a review of machine learning applications for chemical and process industries,” *Reaction Chemistry and Engineering*, vol. 7, no. 7, pp. 1471–1509, 2022. https://doi.org/10.1039/d1re00541c

[75] G. Czeczot, I. Rojek, D. Mikołajewski, and B. Sangho, “AI in IIoT Management of Cybersecurity for Industry 4.0 and Industry 5.0 Purposes,” *Electronics*, vol. 12, no. 18, pp. 1-15, 2023. https://doi.org/10.3390/electronics12183800

[76] S. Sujitha, K. S. Vinod, V. S. Dechamma, J. Likitha, R. M. Prajwal, and R. Jayanth, “Study of Interfacing PLC With HMI for Industrial Applications,” *2023 Second International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 02-04 March 2023, pp. 343–346. https://doi.org/10.1109/icears56392.2023.10084927

[77] M. Alabadi, A. Habbal, and X. Wei, “Industrial Internet of Things: requirements, architecture, challenges, and future research directions,” *IEEE Access*, vol. 10, pp. 66374–66400, 2022. https://doi.org/10.1109/access.2022.3185049

[78] N. Hasan, and M. Alam, “Role of machine learning approach for industrial internet of things (IIoT) in cloud environment-a systematic review,” *International Journal of Advanced Technology and Engineering Exploration*, vol. 10, no. 108, pp. 1391–1416, 2023. https://doi.org/10.19101/ijatee.2023.10101133

[79] V. K. V. V. Bathalapalli, S. P. Mohanty, C. Pan, and E. Kougianos, “QPUF: Quantum Physical Unclonable Functions for Security-by-Design of Industrial Internet-of-Things,” *2023 IEEE International Symposium on Smart Electronic Systems (iSES)*, Ahmedabad, India, 18-20 December 2023, pp. 296–301. https://doi.org/10.1109/ises58672.2023.00067

[80] G. Gokilakrishnan, V. M, A. Dhanamurugan, A. Bhasha, R. Subbiah, and A. H, “A review of applications, enabling technologies, growth challenges and solutions for IoT/IIoT,” *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*. Coimbatore, India, 17-18 March 2023, pp. 2241-2250. https://doi.org/10.1109/icaccs57279.2023.10112825

[81] B. Alotaibi, “A survey on industrial Internet of Things Security: requirements, attacks, AI-Based solutions, and edge computing opportunities,” *Sensors*, vol. 23, no. 17, pp. 1–49, 2023. https://doi.org/10.3390/s23177470

[82] Z. Xing, Y. Lan, Z. Sun, X. Yang, H. Zheng, Y. Yu, and D. Yu, “IoT OS Platform: Software infrastructure for Next-Gen industrial IoT,” *Applied Sciences*, vol. 14, no. 13, pp. 1–25, 2024. https://doi.org/10.3390/app14135370

[83] M. Wang, Y. Sun, H. Sun, and B. Zhang, “Security Issues on Industrial Internet of Things: Overview and challenges,” *Computers*, vol. 12, no. 12, pp. 1–27, 2023. https://doi.org/10.3390/computers12120256

[84] I. T. Christou, N. Kefalakis, J. K. Soldatos, and A. M. Despotopoulou, “End-to-end industrial IoT platform for Quality 4.0 applications,” *Computers in Industry*, vol. 137, pp. 103591, 2022. https://doi.org/10.1016/J.COMPIND.2021.103591

[85] K. Zhang, C. K. M. Lee, and Y. P. Tsang, “Stateless Blockchain-Based lightweight identity management architecture for industrial IoT applications,” *IEEE Transactions on Industrial Informatics*, vol. 20, no. 6, pp. 8394–8405, 2024. https://doi.org/10.1109/tii.2024.3367364

[86] J. Kim, J. Park, and J. H. Lee, “Analysis of Recent IIoT Security Technology Trends in a Smart Factory Environment,” *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Bali, Indonesia, 20-23 February 2023, pp. 840–845. https://doi.org/10.1109/ICAIIC57133.2023.10067004

[87] M. Soori, B. Arezoo, and R. Dastres, “Internet of things for smart factories in industry 4.0, a review,” *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 192–204, 2023. https://doi.org/10.1016/J.IOTCPS.2023.04.006

[88] F. Hadi Masmali, S. J. Miah, and N. Noman, "Different Applications and Technologies of Internet of Things (IoT)," In *Lecture Notes in Networks and Systems* (Vol. 464). Springer Nature, 2023. https://doi.org/10.1007/978-981-19-2394-4_5

[89] R. D. S. G. Campilho, and F. J. G. Silva, "Industrial Process Improvement by Automation and Robotics," *Machines*, vol. 11, no. 11, pp. 1-5, 2023. https://doi.org/10.3390/MACHINES11111011

[90] P. Kantanavar, and S. Rajendran, "Industrial Internet of Things: Architecture and Its Applications," In *Internet of Things* (1st ed., pp. 1–20). Taylor & Francis, 2023. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003226888-18/industrial-internet-things-architecture-applications-pratibha-kantanavar-sindhu-rajendran

[91] G. Karacayılmaz, and H. Artuner, "A novel approach detection for IIoT attacks via artificial intelligence," *Cluster Computing*, vol. 27, no. 8, pp. 10467–10485, 2024. https://doi.org/10.1007/S10586-024-04529-W/TABLES/1

[92] H. V. Krishna, and K. R. Sekhar, "Enhancing security in IIoT applications through efficient quantum key exchange and advanced encryption standard," *Soft Computing*, vol. 28, no. 3, pp. 2671–2681, 2024. https://doi.org/10.1007/s00500-023-09585-9

[93] A., Presciuttini, and A. Portioli-Staudacher, "Applications of IoT and Advanced Analytics for manufacturing operations: a systematic literature review," *Procedia Computer Science*, vol. 232, pp. 327–336, 2024. https://doi.org/10.1016/J.PROCS.2024.01.032

[94] S. Li, S. Zhao, G. Min, L. Qi, and G. Liu, "Lightweight Privacy-Preserving scheme using homomorphic encryption in industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14542–14550, 2022. https://doi.org/10.1109/jiot.2021.3066427

[95] A. Alnajim, S. Habib, M. Islam, S. Thwin, and F. Alotaibi, "A comprehensive survey of cybersecurity threats, attacks, and effective countermeasures in industrial internet of things," *Technologies*, vol. 11, no. 6, pp. 1–26, 2023. https://doi.org/10.3390/technologies11060161

[96] S. Soliman, W. Oudah, and A. Aljuhani, "Deep learning-based intrusion detection approach for securing industrial Internet of Things," *Alexandria Engineering Journal*, vol. 81, pp. 371–383, 2023. https://doi.org/10.1016/j.aej.2023.09.023

[97] K. Jayasudha, and T. N. Anitha, "Unraveling the impact of social engineering on organizations," In *Social Engineering in Cybersecurity: Threats and Defenses* (pp. 70–84). Taylor & Francis, 2024. https://doi.org/10.1201/9781003406716-5

[98] V. Bharath, H. L. Gururaj, B. C. Soundarya, and L. Girish, "Introduction to social engineering," In *Social Engineering in Cybersecurity: Threats and Defenses* (pp. 1–25). Taylor & Francis, 2024. https://doi.org/10.1201/9781003406716-1

[99] H. Alasmary, "RDAF-IIOT: Reliable Device-Access Framework for the Industrial Internet of Things," *Mathematics*, vol. 11, no. 12, pp. 1–21, 2023. https://doi.org/10.3390/math11122710

[100] C. Gan, J. Lin, D. Huang, Q. Zhu, and L. Tian, "Advanced Persistent Threats and their defense Methods in Industrial Internet of Things: a survey," *Mathematics*, vol. 11, no. 14, pp. 1–23, 2023. https://doi.org/10.3390/math11143115

[101] A. Saxena, and S. Mittal, "Advanced Persistent Threat Datasets for Industrial IoT : A Survey," *2023 Second International Conference on Informatics (ICI),* Noida, India, 23-25 November 2023, pp. 1–6. https://doi.org/10.1109/ici60088.2023.10421181

[102] N. K. Pandey, K. Kumar, G. Saini, and A. K. Mishra, "Security issues and challenges in cloud of things-based applications for industrial automation," *Annals of Operations Research*, vol. 342, no. 1, pp. 565–584, 2023. https://doi.org/10.1007/s10479-023-05285-7

[103] M. M. Khan, A. Buriro, T. Ahmad, and S. Ullah, "Backdoor malware detection in industrial IoT using machine learning," *Computers, Materials & Continua*, vol. 81, no. 3, pp. 1–10, 2024. https://doi.org/10.32604/cmc.2024.057648

[104] N. Subramanian, S. N. Bushra, G. Shobana, and S. Radhika, "Backdoor Attacks Prediction in IIoT Network using Optimal Double Mask Region Convolution Model," *IETE Journal of Research*, vol. 70, no. 5, pp. 4801–4814, 2024. https://doi.org/10.1080/03772063.2023.2230174

[105] G. Ali, M. M. Mijwil, B. A. Buruga, M. Abotaleb, and I. Adamopoulos, "A Survey on Artificial Intelligence in Cybersecurity for Smart Agriculture: State-of-the-Art, Cyber Threats, Artificial Intelligence Applications, and Ethical Concerns," *Mesopotamian Journal of Computer Science*, vol. 2024, pp. 71–121, 2024. https://doi.org/10.58496/MJCSC/2024/007

[106] G. Ali, M. M. Mijwil, B. A. Buruga, and M. Abotaleb, "A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech," *Iraqi Journal For Computer Science and Mathematics*, vol. 5, no. 3, pp. 45–91, 2024. doi:https://doi.org/10.52866/ijcsm.2024.05.03.004

[107] V. Bali, "Industrial Cybersecurity Market Report 2025 (Global Edition)," In Cognitive Market Research (No. CMR648420). Cognitive Market Research, 2024. Accessed: Feb. 21, 2025. [Online]. Available: https://www.cognitivemarketresearch.com/industrial-cybersecurity-market-report?srsltid=AfmBOooZFNN_H2NAyXEmkyS2sEQNEFfYDKY6watfFfMPhPbZ0y3Jz-OO

[108] G. Ali, and M. M. Mijwil, "Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles," *Mesopotamian Journal of CyberSecurity,* vol. 4, no. 2, pp. 20–62, 2024. https://doi.org/10.58496/MJCS/2024/006

[109] G. Bravos, A. J. Cabrera, C. Correa, D. Danilovic, N. Evangeliou, G. Ezov, Z. Gajica, D. Jakovetic, L. Kallipolitis, M. Lukic, J. Mascolo, D. Masera, R. Mazo, I. Mezei, A. Miaoudakis, N. Milosevic, W. Oliff, J. Robin, M. Smyrlis, . . . D. Vukobratovic, "Cybersecurity for Industrial Internet of Things: architecture, models and lessons learned," *IEEE Access*, vol. 10, pp. 124747–124765, 2022. https://doi.org/10.1109/access.2022.3225074

[110] G. Ali, R. Wamusi, M. M. Mijwil, M. Sallam, J. Ayad, and I. Adamopoulos, "Securing the Internet of Wetland Things (IoWT) Using Machine and Deep Learning Methods: A Survey," *Mesopotamian Journal of Computer Science*, vol. 2025, pp. 17–63, 2025. https://doi.org/10.58496/mjcsc

[111] G. Ali, M. M. Mijwil, I. Adamopoulos, and J. Ayad, "Leveraging the Internet of Things, Remote Sensing, and Artificial Intelligence for Sustainable Forest Management," *Babylonian Journal of Internet of Things*, vol. 2025, pp. 1–65, 2025. https://doi.org/10.58496/BJIoT/2025/001

[112] M. M. Mijwil, O. Adelaja, A. Badr, G. Ali, B. A. Buruga, and P. Pudasaini, "Innovative Livestock: A Survey of Artificial Intelligence Techniques in Livestock Farming Management," *Wasit Journal of Computer and Mathematics Science*, vol. 2, no. 4, pp. 99–106, 2023. https://doi.org/10.31185/wjcms.206

[113] G. Ali, and W. Robert, "Machine Learning for Temperature Analysis in Ouagadougou: A Random Forest Perspective," *EDRAAK*, vol. 2024, pp. 101-105, 2024. https://doi.org/10.70470/EDRAAK/2024/012

[114] G. Ali, M. M. Mijwil, I. Adamopoulos, B. A. Buruga, M. Gök, and M. Sallam, "Harnessing the Potential of Artificial Intelligence in Managing Viral Hepatitis," *Mesopotamian Journal of Big Data*, vol. 2024, pp. 128–163, 2024. https://doi.org/10.58496/MJBD/2024/010

[115] K., Wu, and J. Chen, "Implementing Robust Security Measures in Cloud Infrastructure: Strategies, Best Practices, and Emerging Trends," *Engineering Advances*, vol. 3, no. 4, pp. 337–341, 2023. https://doi.org/10.26855/EA.2023.08.012

[116] S. Chaudhary, and P. K. Mishra, "DDoS attacks in Industrial IoT: A survey," *Computer Networks*, vol. v236, pp. 110015, 2023. https://doi.org/10.1016/J.COMNET.2023.110015

[117] J. Ayad, G. Ali, W. Ullah, and W. Robert, "Encryption of Color Images utilizing cascading 3D Chaotic Maps with S-Box Algorithms," *SHIFRA*, vol. 2023, pp. 95-107, 2023. https://doi.org/10.70470/SHIFRA/2023/011

[118] N. Mishra, S. K. Hafizul Islam, and S. Zeadally, "A survey on security and cryptographic perspective of Industrial-Internet-of-Things," *Internet of Things*, vol. 25, pp. 101037, 2024. https://doi.org/10.1016/j.iot.2023.101037

[119] M. M. Mijwil, M. Abotaleb, G. Ali, and K. Dhoska, "Assigning Medical Professionals: ChatGPT's Contributions to Medical Education and Health Prediction," *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol. 2024, pp. 76–83, 2024. https://doi.org/10.58496/MJAIH/2024/011

[120] A.-H. Al-Mistarehi, M. M. Mijwil, Y. Filali, M. Bounabi, G. Ali, and M. Abotaleb, "Artificial Intelligence Solutions for Health 4.0: Overcoming Challenges and Surveying Applications," *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol. 2023, pp. 15–20, 2023. https://doi.org/10.58496/mjaih/2023/003

[121] M. Paramesha, N. L. Rane, and J. Rane, "Artificial Intelligence, Machine Learning, and Deep Learning for Cybersecurity Solutions: A review of Emerging Technologies and applications," *Partners Universal Multidisciplinary Research Journal (PUMRJ)*, vol. 1, no. 2, pp. 84–109, 2024. https://doi.org/10.5281/zenodo.12827076

[122] J. Ali, S. K. Singh, W. Jiang, A. M. Alenezi, M. Islam, Y. I. Daradkeh, and A. Mehmood, "A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks," *Computer Communications*, vol. 229, pp. 1–27, 2025. https://doi.org/10.1016/j.comcom.2024.108000

[123] L. Idouglid, S. Tkatek, K. Elfayq, and A. Guezzaz, "Next-gen security in IIoT: integrating intrusion detection systems with machine learning for industry 4.0 resilience," *International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering*, vol. 14, no. 3, pp. 3512–3521, 2024. https://doi.org/10.11591/ijece.v14i3.pp3512-3521

[124] G. Zeng, Y. Yang, K. Lu, G. Geng, and J. Weng, "Evolutionary adversarial autoencoder for unsupervised anomaly detection of industrial internet of things," *IEEE Transactions on Reliability*, pp. 1–15, 2025. https://doi.org/10.1109/tr.2025.3528256

[125] N. Alkhafaji, T. Viana, and A. Al-Sherbaz, "Integrated genetic algorithm and deep learning approach for effective Cyber-Attack detection and classification in industrial Internet of things (IIoT) environments," *Arabian Journal for Science and Engineering,* pp. 1–25, 2024. https://doi.org/10.1007/s13369-024-09663-6

[126] M. Ozkan-Okay, E. Akin, Ö. Aslan, S. Kosunalp, T. Iliev, I. Stoyanov, and I. Beloev, "A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions," *IEEE Access*, vol. 12, pp. 12229–12256, 2024. https://doi.org/10.1109/access.2024.3355547

[127] A. K. Abed, and A. Anupam, "Review of security issues in Internet of Things and artificial intelligence-driven solutions," *Security and Privacy*, vol. 6, no. 3, pp. 1–18, 2022. https://doi.org/10.1002/spy2.285

[128] N. M. Maddu, "Integrated Intrusion Detection and Mitigation Framework for SDN-Based IIOT networks using lightweight and adaptive AI techniques," *Journal of Information Systems Engineering & Management,* vol. 10, no. 9s, pp. 456–472, 2025. https://doi.org/10.52783/jisem.v10i9s.1244

[129] O. F. Awad, L. R. Hazim, A. A. Jasim, and O. Ata, "Enhancing IIoT Security with Machine Learning and Deep Learning for Intrusion Detection," Malaysian Journal of Computer Science, vol. 37, no. 2, pp. 139–153, 2024. https://doi.org/10.22452/mjcs.vol37no2.3

[130] K. Yang, J. Wang, and M. Li, "An improved intrusion detection method for IIoT using attention mechanisms, BiGRU, and Inception-CNN," *Scientific Reports*, vol. 14, no. 1, pp. 1–24, 2024. https://doi.org/10.1038/s41598-024-70094-2

[131] J. A. B. Angelin, and C. Priyadharsini, "Deep Learning based Network based Intrusion Detection System in Industrial Internet of Things," *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT),* Bengaluru, India, 04-06 January 2024, pp. 426–432. https://doi.org/10.1109/idciot59759.2024.10467510

[132] N. Yalçın, S. Çakır, and S. Ünaldı, "Attack detection using artificial intelligence methods for SCADA security," *IEEE Internet of Things Journal,* vol. 11, no. 24, pp. 39550–39559, 2024. https://doi.org/10.1109/jiot.2024.3447876

[133] D. Attique, W. Hao, W. Ping, D. Javeed, and P. Kumar, "Explainable and Data-Efficient deep learning for enhanced attack detection in IIoT ecosystem," *IEEE Internet of Things Journal,* vol. 11, no. 24, pp. 38976–38986, 2024. https://doi.org/10.1109/jiot.2024.3384374

[134] E. V. N. Jyothi, M. Kranthi, S. Sailaja, U. Sesadri, S. N. Koka, and P. C. S. Reddy, "An Adaptive Intrusion Detection System in Industrial Internet of Things(IIoT) using Deep Learning," *2024 1st International Conference on Innovative Sustainable Technologies for Energy, Mechatronics, and Smart Systems (ISTEMS),* Dehradun, India, 26-27 April 2024, pp. 1–6. https://doi.org/10.1109/istems60181.2024.10560245

[135] D. Jagli, R. Temkar, L. Nakirekanti, and A. Bhatt, "The role of artificial intelligence in cyber security," *Journal of Electrical Systems,* vol. 20, no. 3, pp. 5283–5291, 2024. https://doi.org/10.52783/jes.6327

[136] G. F. Asere, K. A. Nuga, and M. Medugu, "The role of Artificial intelligence in Cybersecurity: Understanding the dynamics, impacts, and remediations," *Journal of Computer, Software and Program*, vol. 2, no. 1, pp. 1–9, 2025. https://doi.org/10.69739/jcsp.v2i1.120

[137] N. A. Folorunso, N. T. Adewumi, N. A. Adewa, N. R. Okonkwo, and N. T. N. Olawumi, "Impact of AI on cybersecurity and security compliance," *Global Journal of Engineering and Technology Advances*, vol. 21, no. 1, pp. 167–184, 2024. https://doi.org/10.30574/gjeta.2024.21.1.0193

[138] L. Ofusori, T. Bokaba, and S. Mhlongo, "Artificial intelligence in cybersecurity: a comprehensive review and future direction," *Applied Artificial Intelligence*, vol. 38, no. 1, pp. 1–47, 2024. https://doi.org/10.1080/08839514.2024.2439609

[139] F. K. Karim, J. Varela-Aldás, M. K. Ishak, A. Aljarbouh, and S. M. Mostafa, "Modeling of Bayesian machine learning with sparrow search algorithm for cyberattack detection in IIoT environment," *Scientific Reports*, vol. 14, no. 1, pp. 1–26, 2024. https://doi.org/10.1038/s41598-024-79632-4

[140] Z. Chen, Z. Li, J. Huang, S. Liu, and H. Long, "An effective method for anomaly detection in industrial Internet of Things using XGBoost and LSTM," *Scientific Reports,* vol. 14, no. 1, pp. 1–23, 2024. https://doi.org/10.1038/s41598-024-74822-6

[141] M. Miryahyaei, M. Fartash, and J. A. Torkestani, "Focal Causal Temporal Convolutional Neural Networks: Advancing IIoT Security with Efficient Detection of Rare Cyber-Attacks," *Sensors*, vol. 24, no. 19, pp. 1–26, 2024. https://doi.org/10.3390/s24196335

[142] S. Kim, W. Jo, H. Kim, S. Choi, D. Jung, H. Choi, and T. Shon, "Two-Phase industrial control system anomaly detection using communication patterns and deep learning," *Electronics*, vol. 13, no. 8, pp. 1–17, 2024. https://doi.org/10.3390/electronics13081520

[143] M. Arsalan, M. Mubeen, M. Bilal, and S. F. Abbasi, "1D-CNN-IDS: 1D CNN-based intrusion Detection system for IIOT," *2024 29th International Conference on Automation and Computing (ICAC)*, Sunderland, United Kingdom, 28-30 August 2024, pp. 1–4. https://doi.org/10.1109/icac61394.2024.10718772

[144] T. N. Alrumaih, and M. J. Alenazi, "ERINDA: A novel framework for Enhancing the Resilience of Industrial Networks against DDoS Attacks with adaptive recovery," *Alexandria Engineering Journal*, vol. 121, pp. 248–262, 2025. https://doi.org/10.1016/j.aej.2025.02.042

[145] M. Mudassir, D. Unal, M. Hammoudeh, and F. Azzedin, "Detection of Botnet Attacks against Industrial IoT Systems by Multilayer Deep Learning Approaches," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–12, 2022. https://doi.org/10.1155/2022/2845446

[146] H. Cha, H. Yang, Y. Song, and A. R. Kang, "Intelligent Anomaly Detection System through Malware Image Augmentation in IIoT Environment Based on Digital Twin," *Applied Sciences*, vol. 13, no. 18, pp. 1–21, 2023. https://doi.org/10.3390/app131810196

[147] I. Ahmed, M. Anisetti, A. Ahmad, and G. Jeon, "A multilayer deep learning approach for malware classification in 5G-Enabled IIoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1495–1503, 2023. https://doi.org/10.1109/tii.2022.3205366

[148] S. H. Javed, M. B. Ahmad, M. Asif, S. H. Almotiri, K. Masood, and M. A. A. Ghamdi, "An intelligent system to detect advanced persistent threats in industrial internet of things (I-IoT)," *Electronics*, vol. 11, no. 5, pp. 1–25, 2022. https://doi.org/10.3390/electronics11050742

[149] W. Miao, X. Zhao, Y. Zhang, S. Chen, X. Li, and Q. Li, "A Deep Learning-Based method for preventing data leakage in electric power industrial internet of things business data interactions," *Sensors*, vol. 24, no. 13, pp. 1–20, 2024. https://doi.org/10.3390/s24134069

[150] D. Kiseki, V. Havyarimana, D. Zabagunda, W. Wail, and T. Niyonsaba, "Artificial Intelligence in Cybersecurity to Detect Phishing," *Journal of Computer and Communications*, vol. 12, pp. 91-115, 2024. doi: 10.4236/jcc.2024.1212007.

[151] O. A. Lamina, W. A. Ayuba, O. E. Adebiyi, G. E. Michael, O. D. Samuel, and K. O. Samuel, "AI-Powered Phishing Detection and Prevention," *Path of Science*, vol. 10, no. 12, pp. 4001–4010, 2024. https://doi.org/10.22178/pos.112-7

[152] M. A. Tamal, M. K. Islam, T. Bhuiyan, A. Sattar, and N. U. Prince, "Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning," *Frontiers in Computer Science*, vol. 6, pp. 1–19, 2024. https://doi.org/10.3389/fcomp.2024.1428013

[153] D. O. Ofoegbu, K. S. Osundare, O. S. Ike, C. G. Fakeyede, O. B. Ige, and C. Author, "Data-Driven Cyber Threat Intelligence: Leveraging Behavioral Analytics for Proactive Defense Mechanisms," *Computer Science & IT Research Journal*, vol. 4, no. 3, pp. 502–524, 2023. https://doi.org/10.51594/CSITRJ.V4I3.1501

[154] J. Uzoma, O. Falana, C. Obunadike, and E. S. Obunadike. "Using Artificial Intelligence for Automated Incidence Response in Cybersecurity," *International Journal of Information Technology (IJIT)*, vol. 1, no. 4, pp. 1-32, 2023.

[155] D. Garabato, C. Dafonte, R. Santoveña, A. Silvelo, F. J. Nóvoa, and M. Manteiga, "AI-based user authentication reinforcement by continuous extraction of behavioral interaction features," *Neural Computing and Applications*, vol. 34, no. 14, pp. 11691–11705, 2022. https://doi.org/10.1007/S00521-022-07061-3/TABLES/6

[156] S. Selvarajan, G. Srivastava, A. O. Khadidos, A. O. Khadidos, M. Baza, A. Alshehri, and J. C. Lin, "An artificial intelligence lightweight Blockchain security model for security and privacy in IIoT systems," *Journal of Cloud Computing Advances Systems and Applications*, vol. 12, no. 1, pp. 1–17, 2023. https://doi.org/10.1186/s13677-023-00412-y

[157] H. Tian, and G. Huang, "Research on Distributed secure storage framework of industrial internet of things data based on Blockchain," *Electronics*, vol. 13, no. 23, pp. 1–20, 2024. https://doi.org/10.3390/electronics13234812

[158] K. S. Kumar, J. A. Alzubi, N. Sarhan, E. M. Awwad, V. Kandasamy, and G. Ali, "A secure and efficient Blockchain and distributed Ledger technology-based optimal resource management in digital twin beyond 5G networks using hybrid energy valley and levy Flight Distributer Optimization algorithm," *IEEE Access*, vol. 12, pp. 110331–110352, 2024. https://doi.org/10.1109/access.2024.3435847

[159] S. B. Kahyaoglu, and V. Tecim, "Exploring Blockchain Applications: Management Perspectives," In *CRC Press eBooks* (1st ed.). CRC Press, 2024. https://doi.org/10.1201/9781003389552

[160] D. Dutta, and P. Govindaraj, "Exploring Blockchain: technological foundations, applications, and security concerns," *Engineering Research Express*, vol. 7, pp. 1–15, 2025. https://doi.org/10.1088/2631-8695/ada2de

[161] A. Denis, A. Thomas, W. Robert, A. Samuel, S. P. Kabiito, Z. Morish, M. Sallam, G. Ali, and M. M. Mijwil, "A Survey on Artificial Intelligence and Blockchain Applications in Cybersecurity for Smart Cities," *SHIFRA*, vol. 2025, pp. 1-45, 2025. https://doi.org/10.70470/SHIFRA/2025/001

[162] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "Blockchain integration in the era of industrial metaverse," *Applied Sciences*, vol. 13, no. 3, pp. 1–29, 2023. https://doi.org/10.3390/app13031353

[163] L. A. C. Ahakonye, C. I. Nwakanma, and D. Kim, "Tides of Blockchain in IoT Cybersecurity," *Sensors*, vol. 24, no. 10, pp. 1–27, 2024. https://doi.org/10.3390/s24103111

[164] S. Latif, Z. Idrees, Z. E. Huma, and J. Ahmad, "Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, pp. 1–37, 2021. https://doi.org/10.1002/ett.4337

[165] F. Wang, J. Cui, Q. Zhang, D. He, and H. Zhong, "Blockchain-Assisted flexible revocable anonymous authentication in industrial internet of things," *IEEE Transactions on Network Science and Engineering*, pp. 1–16, 2025. https://doi.org/10.1109/tnse.2024.3503996

[166] S. K. Dwivedi, P. Roy, C. Karda, S. Agrawal, and R. Amin, "Blockchain-Based Internet of Things and Industrial IoT: A Comprehensive survey," *Security and Communication Networks*, vol. 2021, pp. 1–21, 2021. https://doi.org/10.1155/2021/7142048

[167] W. Robert, A. Denis, A. Thomas, A. Samuel, S. P. Kabiito, Z. Morish, and G. Ali, "A Comprehensive Review on Cryptographic Techniques for Securing Internet of Medical Things: A State-of-the-Art, Applications, Security Attacks, Mitigation Measures, and Future Research Direction," *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol. 2024, pp. 135–169, 2024. https://doi.org/10.58496/MJAIH/2024/016

[168] W. Tong, L. Yang, Z. Li, X. Jin, and L. Tan, "Enhancing security and flexibility in the industrial internet of things: Blockchain-Based data sharing and privacy protection," *Sensors*, vol. 24, no. 3, pp. 1–27, 2024. https://doi.org/10.3390/s24031035

[169] M. S. Dildar, A. S. Khan, I. A. Abbasi, R. Shaheen, K. A. Ruqaishi, and S. Ahmed, "End-to-end security mechanism using Blockchain for Industrial Internet of Things," *IEEE Access*, vol. 13, pp. 20584–20598, 2025. https://doi.org/10.1109/access.2025.3535821

[170] F. Wang, J. Cui, Q. Zhang, D. He, C. Gu, and H. Zhong, "Blockchain-Based lightweight message authentication for Edge-Assisted Cross-Domain industrial internet of things," *IEEE Transactions on Dependable and Secure Computing,* vol. 21, no. 4, pp. 1587–1604, 2024. https://doi.org/10.1109/tdsc.2023.3285800

[171] F. Wang, J. Cui, Q. Zhang, D. He, and H. Zhong, "Blockchain-Based secure Cross-Domain data sharing for Edge-Assisted industrial internet of things," *IEEE Transactions on Information Forensics and Security,* vol. 19, pp. 3892–3905, 2024. https://doi.org/10.1109/tifs.2024.3372806

[172] A. Aljuhani, P. Kumar, R. Alanazi, T. Albalawi, O. Taouali, A. K. M. N. Islam, N. Kumar, and M. Alazab, "A Deep-Learning-Integrated Blockchain framework for securing industrial IoT," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 7817–7827, 2023. https://doi.org/10.1109/jiot.2023.3316669

[173] M. N. Sohail, A. Anjum, I. A. Saeed, M. H. Syed, A. Jantsch, and S. Rehman, "Optimizing industrial IoT data security through Blockchain-Enabled Incentive-Driven Game theoretic approach for data sharing," *IEEE Access*, vol. 12, pp. 51176–51192, 2024. https://doi.org/10.1109/access.2024.3382571

[174] Y. Chen, X. Lin, H. Xu, S. Liao, J. Guo, and C. Zou, "Leveraging Blockchain and Coded Computing for Secure Edge Collaborate Learning in Industrial IoT," *2024 33rd International Conference on Computer Communications and Networks (ICCCN)*, Kailua-Kona, HI, USA, 29-31 July 2024, pp. 1–6. https://doi.org/10.1109/icccn61486.2024.10637571

[175] Z. Cao, X. Wen, S. Ai, W. Shang, and S. Huan, "A decentralized authentication scheme for smart factory based on Blockchain," *Scientific Reports*, vol. 14, no. 1, pp. 1–12, 2024. https://doi.org/10.1038/s41598-024-76065-x

[176] P. Yao, B. Yan, T. Yang, Y. Wang, Q. Yang, and W. Wang, "Security-Enhanced Operational Architecture for decentralized industrial Internet of Things: a Blockchain-Based approach," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 11073–11086, 2024. https://doi.org/10.1109/jiot.2023.3329352

[177] A. Zainudin, M. A. P. Putra, R. N. Alief, D. Kim, and J. Lee, "Blockchain-aided collaborative threat detection for securing digital twin-based IIoT networks," *ICC 2024 - IEEE International Conference on Communications*, Denver, CO, USA, 09-13 June 2024, pp. 4656–4661. https://doi.org/10.1109/icc51166.2024.10622717

[178] Z. Mammeri, Cryptography: Algorithms, Protocols, and Standards for Computer Security (1st ed.). John Wiley & Sons, Inc, 2024.

[179] H. Yin, Y. Li, H. Deng, W. Zhang, Z. Qin, and K. Li, "An Attribute-Based keyword search scheme for multiple data owners in Cloud-Assisted industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 4, pp. 5763–5773, 2023. https://doi.org/10.1109/tii.2022.3192304

[180] M. Alawida, "A novel image encryption algorithm based on cyclic chaotic map in industrial IoT environments," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 8, pp. 10530–10541, 2024. https://doi.org/10.1109/tii.2024.3395631

[181] Z. A. Shaikh, F. Hajjej, Y. D. Uslu, S. Yüksel, H. Dınçer, R. Alroobaea, A. M. Baqasah, and U. Chinta, "A New Trend in Cryptographic Information Security for Industry 5.0: A Systematic review," *IEEE Access*, vol. 12, pp. 7156–7169, 2024. https://doi.org/10.1109/access.2024.3351485

[182] V. A. Telsang, M. S. Kakkasageri, and A. D. Devangavi, "Edge Computing Devices Authentication using Quantum Computing," *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Kamand, India, 24-28 June 2024, pp. 1–6. https://doi.org/10.1109/ICCCNT61001.2024.10725671

[183] S. Chaitrasree, and G. A. Srinidhi, "Quantum Cryptography for Enhanced Cyber Security – A Review," *International Journal of Enhanced Research in Science, Technology & Engineering*, vol. 13, no. 10, pp. 1–20, 2024.

[184] M. Hasan, "Quantum Cryptography for Secure Communications and the Enhancement of U.S. Cybersecurity in the Quantum Age," *Advances in Social Sciences Research Journal*, vol. 11, no. 10, pp. 1–9, 2024. https://doi.org/10.14738/assrj.1110.17764.

[185] B. Senapati, and B. S. Rawal, "Quantum communication with RLP quantum resistant cryptography in industrial manufacturing," *Cyber Security and Applications*, vol. 1, pp. 1–8, 2023. https://doi.org/10.1016/j.csa.2023.100019

[186] A. Green, J. Lawrence, G. Siopsis, N.A. Peters, and A. Passian, "Quantum Key Distribution for Critical Infrastructures: Towards Cyber-Physical Security for Hydropower and Dams," *Sensors*, vol. 23, no. 24, pp. 1-24, 2023. https://doi.org/10.3390/s23249818

[187] S. Sonko, K. I. Ibekwe, V. I. Ilojianya, E. A. Etukudoh, and A. Fabuyide, "Quantum Cryptography and U.S. Digital Security: A Comprehensive Review: Investigating the Potential of Quantum Technologies in Creating Unbreakable Encryption and Their Future in National Security," *Computer Science & IT Research Journal*, vol. 5, no. 2, pp. 390–414, 2024. https://doi.org/10.51594/csitrj.v5i2.790

[188] N. A. Samson, "Quantum computing and wireless networks security: A survey," *GSC Advanced Research and Reviews*, vol. 20, no. 03, pp. 199–230, 2024. https://doi.org/10.30574/gscarr.2024.20.2.0308

[189] G. Nagar, and A. Manoharan, "The Rise of Quantum Cryptography: Securing Data Beyond Classical Means," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 04, no. 05, pp. 6329-6336, 2024. https://doi.org/10.56726/irjmets24238

[190] H. Li, Y. Dong, Y. Zhang, and H. Wang, "Exploration of Quantum Cryptography Security applications for industrial control systems," *Applied Mathematics and Nonlinear Sciences,* vol. 9, no. 1, pp. 1–14, 2024. https://doi.org/10.2478/amns-2024-1711

[191] C. P. Prajwal, A. S. Mohan, D. N. Reddy, and K. Nimmy, "Quantum-Safe Authentication Protocol leveraging qPUF for Industrial Internet of Things," *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT),* Kamand, India, 24-28 June 2024, pp. 1–8. https://doi.org/10.1109/ICCCNT61001.2024.10725580

[192] P. Bhattacharya, A. Kumari, S. Tanwar, I. Budhiraja, S. Patel, and J. J. P. C. Rodrigues, "Quant-Jack: Quantum Machine Learning to Detect Cryptojacking Attacks in IIoT Networks," *2024 IEEE International Conference on Communications Workshops (ICC Workshops),* Denver, CO, USA, 09-13 June 2024, pp. 865–870. https://doi.org/10.1109/ICCWORKSHOPS59551.2024.10615371

[193] K. Kannadasan, "Next Generation: Quantum-Enhanced Security for 5G Node Protection in Massive Machine-Type Communications for IIoT Applications. *Multidisciplinary Journal for Applied Research in Engineering and Technology (MJARET)*," vol. 4, no. 2, pp. 11–15, 2024. https://doi.org/10.54228/mjaret0624009

[194] D. Xu, K. Yu, and J. A. Ritcey, "Cross-Layer Device Authentication With Quantum Encryption for 5G Enabled IIoT in Industry 4.0," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6368–6378, 2022. https://doi.org/10.1109/TII.2021.3130163

[195] K. K. Singamaneni, G. Dhiman, S. Juneja, G. Muhammad, S. A. Alqahtani, and J. Zaki, "A Novel QKD Approach to Enhance IIOT Privacy and Computational Knacks," *Sensors*, vol. 22, no. 18, pp. 1–18, 2022. https://doi.org/https://doi.org/10.3390/s22186741

[196] S. F. Ahmad, M. Y. Ferjani, and K. Kasliwal, "Enhancing Security in the Industrial IoT Sector using Quantum Computing," *2021 28th IEEE International Conference on Electronics, Circuits, and Systems, ICECS 2021 - Proceedings,* PP. 1-18. https://doi.org/10.1109/ICECS53924.2021.9665527