ISSN 2581 – 3781

AJCSE ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info

Asian Journal of Computer Science Engineering 2025;10(4):1-11

REVIEW ARTICLE

Secure Protocols for Industrial IoT Communication in Cyber-Physical Systems: A Review of Challenges and Defense Strategies

Deepak Mehta*

Department of Computer Sciences and Applications, Mandsaur University, Mandsaur, Madhya Pradesh, India

Received: 10-10-2025; Revised: 25-11-2025; Accepted: 05-12-2025

ABSTRACT

The fourth industrial revolution, or Industry 4.0, employs cutting-edge computer and networking technology to automate, rely on, and intelligently make production processes. This is achieved through the usage of the industrial internet of things (IIoT). Intelligent industrial ecosystems are made possible through the integration of sensing, computation, and actuation in cyber-physical systems (CPS). However, the confluence of IIoT and CPS in communication protocols and architectures exposes systems to risks such as denial-of-service attacks, man-in-the-middle assaults, and data breaches. These threats impair confidentiality, integrity, and availability; furthermore, they are caused by vulnerabilities. This paper explores the numerous challenges, potential threats, and solutions in the field of secure communication protocols for IIoT-enabled CPS by reviewing current practices in the field. It examines existing approaches, including transport layer security (TLS), Datagram TLS, IP security, constrained application protocol, message queuing telemetry transport-secure, and open platform communication-unified architecture, along with advanced techniques such as blockchain-based authentication, software-defined networking, semantic security ontologies, and federated learning. By analyzing their scalability, efficiency, and resilience, this review identifies research gaps and offers insights into building secure, trustworthy, and robust IIoT-CPS communication frameworks for Industry 4.0. The results could help academics and industry professionals improve industrial security designs and ensure the secure rollout of smart manufacturing ecosystems in the future.

Key words: Cyber-physical systems, encryption techniques, end-to-end security, industrial internet of things, industry 4.0, secure communication protocols.

INTRODUCTION

Industry 4.0 has revolutionized industrial environments by integrating cyber-physical systems (CPS) and the industrial internet of things (IIoT) to build smart, autonomous systems.[1] The IIoT allows for adaptive control, data interchange, and real-time monitoring by connecting equipment like sensors, actuators, and robots using sophisticated communication protocols.[2] The fundamental principles of Industry 4.0 are upheld by this integration, which incorporates digital-physical integration from beginning to finish, vertical integration inside industrial systems, and horizontal integration across value networks.[3]

Address for correspondence:
Deepak Mehta
E-mail: deepak.mehta@meu.edu.in

The CPS is a key component that permits this change because it unifies feedback-driven systems that combine computational parts with physical processes (such as sensing and actuation).[4] CPSs operate with minimal human intervention, capturing data via sensors such as Radio Frequency Identification (RFID) tags and transmitting it to cyber components, often deployed on cloud platforms, for intelligent decision-making and precise control. When implemented in industrial contexts, CPS evolves into Industrial CPS (I-CPS).[5] While I-CPS offers improved automation, scalability, and operational efficiency, its failure may cause severe consequences for system productivity and safety.[6]

The increasing integration of IIoT and CPS introduces significant security challenges. Denial-of-service (DoS)/distributed DoS (DDoS) attacks, replay attacks, data tampering, and privacy breaches are only some of the risks that systems in large-scale, heterogeneous, and resource-constrained networks confront.[7] Moreover, industrial environments impose strict real-time requirements where even minor delays in security operations can compromise reliability. Security concerns must therefore be prioritized, particularly because IIoT-enabled CPS is now central to critical sectors such as energy, healthcare, manufacturing, and national security.

To address these issues, researchers and practitioners have developed secure communication protocols and defense strategies tailored to IIoT environments. These approaches focus on minimizing vulnerabilities, preserving confidentiality, integrity, and availability (CIA), and ensuring interoperability across heterogeneous devices and networks.[8] This survey paper reviews the challenges and defense strategies in implementing secure protocols for IIoT communication in CPS, with a particular focus on building trusted, resilient, and efficient communication channels in the era of Industry 4.0. Various types of malwares pose significant security threats to Industrial IoT-enabled Cyber-Physical Systems, as summarized in Table 1.

Structure of the Paper

The structure of this paper is as follows: Section II presents the fundamentals of IIoT-driven CPS. Section III outlines secure protocols for IIoT in the context of the threat landscape. Section IV reviews security challenges in IIOT and CPS. Section V discusses research gaps, limitations, and emerging trends in secure protocol design. In Section VI, discusses potential avenues for further research.

FOUNDATIONS OF IIoT-DRIVEN CPS

The term "Industry 4.0" describes the most current phase of technical development in manufacturing and automation that has been put into place to boost efficiency and production. The IIoT and I-CPS are two significant viewpoints that emerge from Industry 4.0.[9] Entirely, I-IoT integrates cutting-edge IoT technology into manufacturing and industrial automation systems, enabling the identification and connection of numerous devices and equipment.[10] As an extension of conventional CPS, I-CPS means the integration of cyber and physical systems for automation, resilience, security, and command and control. While traditional CPS has expanded its use beyond its initial critical systems applications, such as power generation, transportation, and infrastructure, it remains an important tool in these fields. I-CPS, or industrial CPS, allows for more efficient and effective automation and production in the manufacturing sector.

CPS for Smart Environments

The National Science Foundation's Helen Gil introduced CPS in 2006 as a means of connecting the physical and virtual realms by integrating networking, computation, and storage. In industrial environments, CPS enables the realization of Smart Factories through seamless interaction between physical processes and computational intelligence. Internet of Things (IoT) and IIoT, distributed computing, real-time embedded systems, industrial control systems, wireless sensor networks, fog, edge, cloud computing, Machine-to-machine (M2M) communication, and adjacent domains are all closely related.[11] Evolving from real-time systems, CPS emphasizes the interconnection of devices through Internet protocols, requiring interdisciplinary approaches to manage increasing interdependence between computational and physical elements.[12] The layered architecture of CPS comprises physical devices and communication interfaces at the foundation, a middleware layer linking CPS nodes, units, and systems, and a computation layer responsible for data collection, integration, processing, and interpretation using both batch and stream computing, are shown in Figure 1, thereby enabling secure and intelligent decision-making in complex industrial environments.

Architecture of IIoT

Smart grids and intelligent transport are two examples of the many uses made possible by the connectivity of physical components that make up CPS. Industrial CPS (I-CPS) is based on the idea of the IIoT, which expands the concept of the IoT beyond its consumer-oriented scope and into industrial domains. The IIoT does this by linking intelligent devices with control and management platforms, which in turn increases automation, efficiency, and productivity. In a typical three-layer architecture, the IIoT sees the following components: Sensors, actuators, industrial robots, and manufacturing equipment; the communication layer integrates networking technologies like WSANs, 5G, M2M, and software-defined networking (SDN) for large-scale connectivity; and the application layer supports smart factories, plants, and supply chains with real-time monitoring and control.[13] Collectively, these layers ensure interoperability, scalability, and efficient coordination in IIoT-enabled industrial systems, as illustrated in Figure 2.

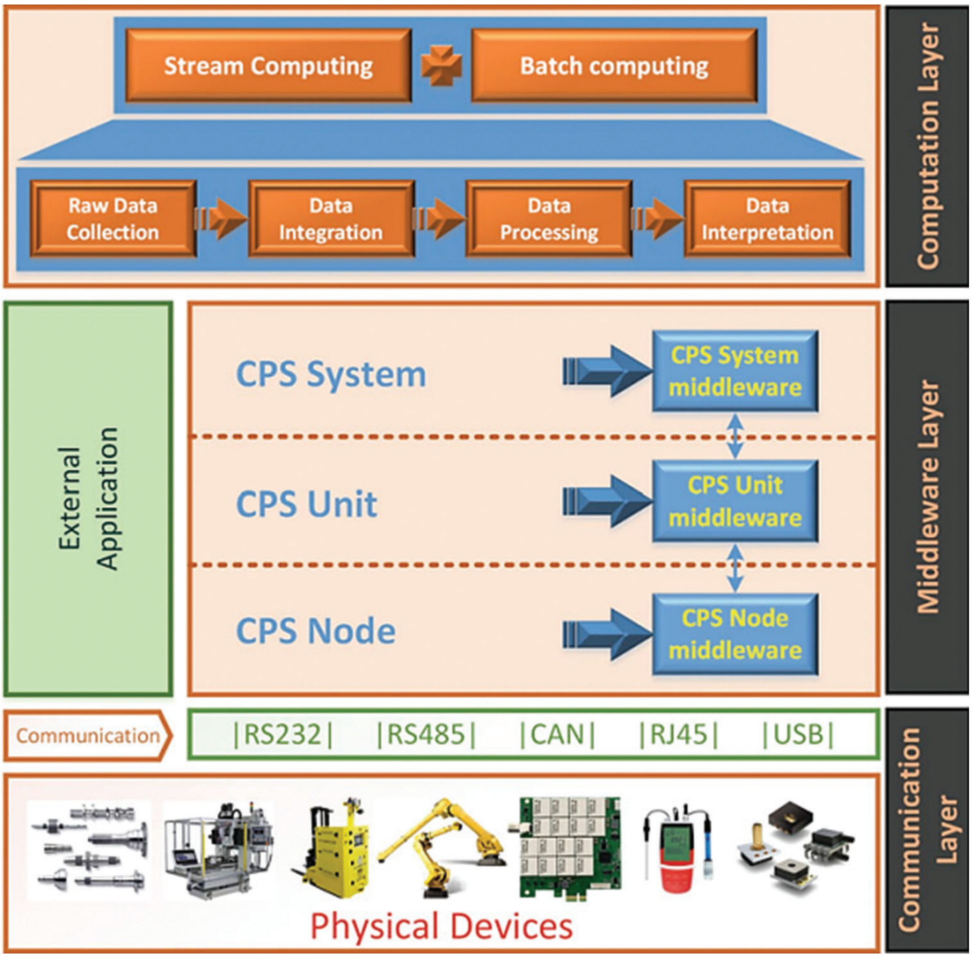

Figure 1: Cyber-physical systems architecture

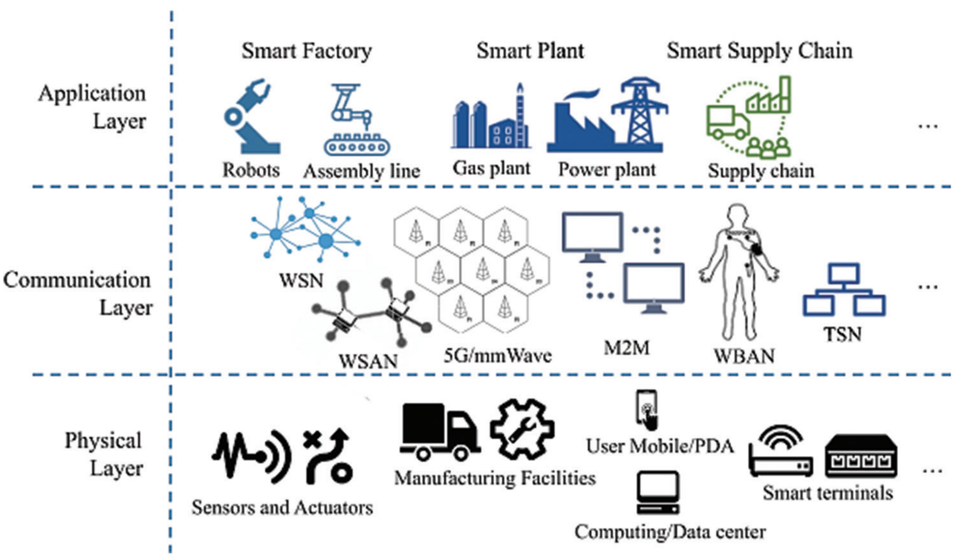

Figure 2: Industrial internet of things system architecture

Applications of IIoT in CPS

CPS benefits from the IIoT's increased monitoring capabilities, workplace optimization capabilities, and efficiency. Figure 3 shows some of its many uses, which include enhancing industrial performance and making smarter decisions through the use of automated control, intelligent data analysis, and interconnected equipment.[14] The applications of IIoT are depicted in Figure 4 and explained as follows:
Here are the applications of IIOT in CPS are as follows:

Table 1: Malware detection

Malware	Description
Worms	Their presence does not infringe upon any other programs. These entities not only exist, but also function autonomously and reproduce themselves.
Viruses	Although they can independently infect and parasitize other programs, they can self-replicate while doing so.
Trojans	They appear as legitimate software to conceal their true intentions and carry out harmful activities without the ability to replicate themselves.
Spyware	They enter into users' systems undetected and gather personal data without their knowledge or consent.
Ransomware	Their service encrypts users' sensitive data and then charges for decryption.
Backdoor	They work in a way that goes around the usual authentication process by using the covertly implanted communication connection path.

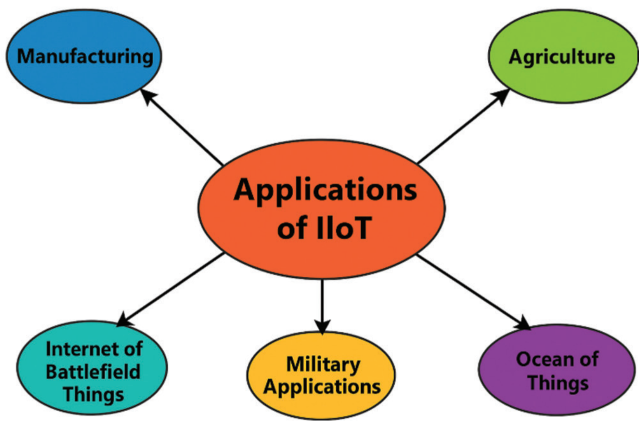

Figure 3: Applications of industrial internet of things

Manufacturing

IIoT transforms manufacturing by enabling real-time data collection from machines and production lines, improving efficiency and customer responsiveness. Insights derived from sensor data help optimize processes, reduce product waste, and accelerate response times, driving the vision of Industry 4.0 and Smart Factories.

Agriculture

Monitoring weather variables (such as precipitation, humidity, wind speed and direction, soil composition, temperature, and insect infestation) is just one of many possible agricultural applications for the IoT.[15] Improving farming processes, minimizing waste, and increasing crop yields and quality are all possible thanks to this data.

Military applications

IoT technologies are mostly employed in the military province for inspection, investigation, and other operations pertaining to combat. This makes use of several smart technologies suitable to the battlefield, such as sensors, robots, biometrics, and vehicles.

Internet of battlefield things

The IoT is a promising new technology that could revolutionize military operations by facilitating real-time monitoring of equipment, vehicles, and personnel as well as enhancing communication and coordination. The IoBT improves protection and efficiency by linking smart devices in combat zones.

Energy management

Energy Management IIoT plays a vital role in monitoring and optimizing energy consumption

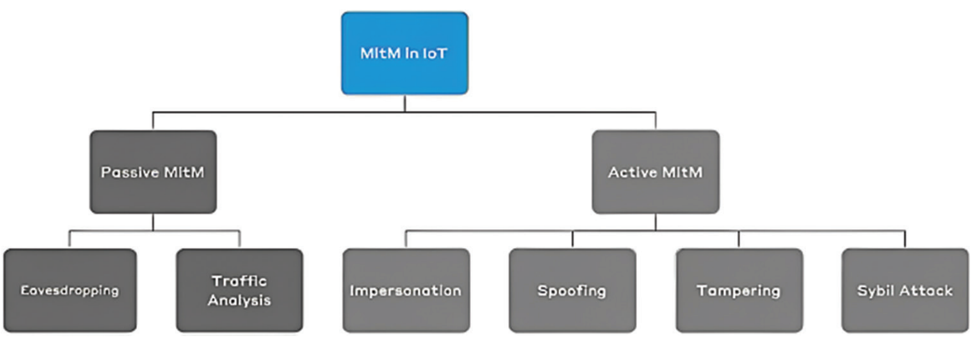

Figure 4: Passive and active man-in-the-middle attacks

in industrial plants, smart grids, and buildings. Real-time energy analytics enable predictive load management, reduction of wastage, and improved sustainability, contributing to cost savings and environmental efficiency.

SECURE PROTOCOLS FOR IIoT COMMUNICATION

IIoT communication depends on secure methods to keep data sent private, error-free, and accessible (CIA).[16] Several widely adopted protocols provide varying levels of protection across different layers of the communication stack:

- Transport layer security (TLS): Provides end-to-end encryption and authentication over TCP-based connections, ensuring secure communication channels between IIoT devices and servers.
- Datagram transport layer security (DTLS): An adaptation of TLS designed for User Datagram Protocol (UDP), making it suitable for latency-sensitive and lightweight IIoT applications while maintaining confidentiality and integrity.
- IP security: Commonly employed for secure tunneling and VPNs in IIoT networks, it functions at the network layer to encrypt, authenticate, and verify the integrity of IP-based communications.
- Message queuing telemetry transport-secure (MQTT-S): A security-enhanced, lightweight publish/subscribe communications protocol designed for IIoT settings with limited bandwidth and resources.
- Constrained application protocol: Web transfer protocol enhanced for low-capacity devices and networks; typically DTLS or OSCORE-protected.
- Open platform communication: Industrial automation has embraced the unified architecture due to its built-in security features, which include authentication, encryption, integrity protection, and granular access control.

Communication Technologies used in IIoT

In IIoT, effective communication is the backbone that links sensors, machines, and control systems. These technologies bridge the perception layer with processing layers like edge or cloud, ensuring data flows quickly and reliably.[17] Depending on needs, devices connect directly through network protocols or through smart gateways. Common options include Wi-Fi, Ethernet, Bluetooth, NFC, low-power wide-area network (LPWAN), ZigBee, long-term evolution for machines (LTE-M), and narrowband (NB)-IoT, each suited for specific industrial scenarios.

- WiFi and Ethernet: A versatile and widely used wireless technology suitable for LAN/WAN environments, providing high-speed communication for industrial and office settings, and Ethernet, a reliable wired technology used in LAN/WAN networks, supporting stable communication between devices and compatibility across media types such as copper and fiber optics.
- Bluetooth: A lot of people use this wireless technology to set up personal area networks, which allow them to share data over relatively short distances.
- NFC: A wireless technology known as near field communications (NFC) allows for safe short-range communication between smart devices. Conventional wisdom holds that NFC has a communication range of roughly 10 cm.
- LPWAN: LPWAN is a radio technologies that enable long-distance communication. The most prominent LPWAN technologies are LoRa, Sigfox, and Nwave. Sending less data over greater distances is the usual use case for LPWANs, in contrast to other wireless technologies like Wi-Fi and Bluetooth.
- ZigBee: Based on IEEE 802.15.4, this protocol is widely applied in sensor networks, supporting low-data-rate communication with standards like ISA-100.11a and Wireless HART.
- LTE-M: A cellular-based LPWA technology that connects IoT devices, sensors, and actuators efficiently over wide areas.
- NB-IoT: A standards-based LPWA technology that improves power efficiency, spectrum usage, and capacity for large-scale IoT deployments in smart industries.

Key Models of Communication in IIoT

A system of networked sensors, devices, and systems used for monitoring, collecting, and analyzing data in industrial settings is called the IIoT. Reduced downtime and increased automation in industries like manufacturing, energy, and logistics are the end results of its principal objective of optimizing operating efficiency, increasing productivity, improving safety, and enabling predictive maintenance.[18] The key models include:

- M2M: Streamlines automation and real-time data transmission by allowing industrial machines and equipment to communicate directly with one another.
- Machine to cloud: Predictive maintenance and sophisticated analytics are made possible by industrial equipment communicating with computers in the cloud, which store, process, and analyze massive statistics.
- Machine to human: Facilitates human-machine interaction by means of interfaces; this permits control, monitoring, and adjustments in response to real-time feedback.
- Machine to enterprise: Streamlines business processes and improves decision-making by combining machine data with Enterprise Resource Planning (ERP) and Supply Chain Management (SCM) platforms.

Security Requirements in IIoT Communication

The IIoT is dependent on a wide-ranging ecosystem that includes sensors, networks, platforms for processing data (such as the cloud and the edge), and new technologies like LoRaWAN and NB-IoT. As a result, its security challenges extend beyond individual components to encompass the entire IIoT environment from physical device protection to secure communication, data storage, and application-level safeguards.[19] Addressing these challenges requires well-defined security requirements across the architecture, which include.

- Confidentially: Ensures protection against unauthorized access or disclosure of information. Mechanisms must secure device connections, safeguard stored data (data-at-rest), protect transmitted data (data-in-transit), and ensure analytical results delivered to end-users remain confidential.
- Integrity: Guarantees consistency, accuracy, and trustworthiness of IIoT data and services throughout their lifecycle. Mechanisms should detect and prevent unauthorized modifications such as insertion, deletion, or replay of data.
- Authentication: Verifies that entities in communication are legitimate. This involves authentication of devices ("things") and confirmation of data origin to prevent impersonation attacks.
- Authorization and access control: Prevents misuse of IIoT resources by ensuring only authorized devices and users can access networks, while edge devices enforce verification of access rights to collected data.
- Availability: Ensures IIoT resources remain accessible and operational at all times. Security mechanisms must mitigate or detect DoS and other disruptions that threaten system uptime.

SECURITY CHALLENGES AND DEFENSE STRATEGIES IN IIoT-ENABLED CPS

IIoT-enabled CPS face significant security challenges, including vulnerable components, legacy systems, increased interconnectivity, and human factors. These weaknesses expose industries to cyber risks such as man-in-the-middle attacks, DoS, and malware injection. Addressing these threats requires holistic approaches that integrate IT/OT security, robust protocols, and awareness to ensure reliability, availability, and resilience in smart industrial environments.

Security Challenges

Even with the significant benefits of adopting Industry 4.0 technologies and transforming critical infrastructure into smart systems, notable security challenges remain.[20] Consequently, industries must address several key security challenges, a few of which are outlined below:

Vulnerable components

Many IIoT devices were not designed with security-by-design principles, making them attractive targets for cyberattacks.[21] As systems transition from closed environments to interconnected CPS, vulnerabilities must be managed across IT, OT, and physical layers.

Increased interconnectivity

The attack surface grows in tandem with the increased connectivity across organizations, IT, and OT environments, which streamlines operations. Threats can develop in industrial control system (ICS) environments due to unsecured network connections, insecure technology deployment, and insufficient security policies.

Legacy systems

Outdated industrial systems often lack modern protection mechanisms. Integrating new IIoT devices with legacy hardware exposes hidden vulnerabilities, creating pathways for attackers.

Human factors

Employees remain a critical weak link in security. Lack of awareness about cyber risks, combined with threats such as phishing, makes human error a frequent entry point for attacks in industrial environments.

Attack Vectors in IIoT-Based CPS

Integrating CPS with the IIoT leaves them vulnerable to numerous attack vectors because of their extensive connectivity and limited resources. Many common entry points for attacks are:

Man-in-the-middle (MITM) attacks

MITM, also known as an on-path attack, occurs when an attacker positions themselves between two communicating parties to intercept or manipulate data exchanges.[22] These attacks threaten all three elements of the CIA triad: Confidentiality, integrity, and availability, along with authentication and authorization mechanisms. MitM in IoT, dividing into passive and active categories (Figure 4), highlights attacks like eavesdropping, spoofing, and tampering.

MITM attacks are generally categorized into two types:

- Passive MITM: Eavesdropping is a common method by which an attacker listens to communications in secret without changing them. Sensitive data such as login credentials or financial information can be stolen if traffic is not properly encrypted.
- Active MITM: The attacker performs more than just listen in on conversations; he or she actually inserts or changes messages in transit. Common examples include impersonation, spoofing, and data tampering.

DoS/DDoS

DoS attacks pose a major challenge in IoT and CPS environments, where resource-constrained devices are easily overwhelmed, making systems unavailable and reducing trust in transmitted data.[23] A variety of attacks can disrupt operations by taking advantage of vulnerabilities in networks. Some examples are denial-of-sleep, path-based DoS, jamming, wormhole, vampire, carousel, and stretch assaults.[24] DDoS is an even more destructive variant that employs a network of infected devices, or botnets, to overwhelm servers and networks with spam, wasting resources and interrupting regular communication. This kind of attack can severely harm industrial infrastructures.

Malware injection

Malware refers to malicious software designed to perform harmful activities on industrial systems, devices, or networks. In the context of ICS and CPS, malware can disrupt operations, render systems inoperable, or enable remote control by attackers, leading to severe consequences. Ransomware attacks are particularly critical, as they can paralyze industrial automation and control systems, compromise system integrity, and cause significant financial loss.[25] Beyond economic damage, malware infections in smart factories and industrial environments pose serious risks to safety, health, and the environment, making them one of the most dangerous threats in IIoT-enabled infrastructures.

Defence Strategies in IIOT-CPS

The increasing interconnection of devices in IIoT-enabled CPS introduces new vulnerabilities, making robust defense strategies essential to ensure data integrity, confidentiality, and system availability. A wide range of mechanisms has been proposed to counter these threats, focusing on intrusion detection, trust management, anomaly detection, access control, and privacy preservation, while also addressing the energy constraints of industrial devices.

1) Intrusion detection systems (IDS): IDS monitor IIoT networks for malicious activities.[26] Signature-based, anomaly-based, and hybrid IDS are used, with lightweight designs tailored for resource-constrained devices.
2) Blockchain-based trust management: Reduce dependency on centralized authority and single points of failure using blockchain's decentralized, tamper-proof records and smart contracts for secure access control.[27]
3) Artificial intelligence (AI)/machine learning (ML)-driven anomaly detection: ML and Deep Learning (DL) models detect abnormal behavior in real time,[28] enabling proactive defense against advanced persistent threats and 0-day attacks.
4) Access control and identity management: A lightweight identity scheme supports methods like capability-based access control, role-based access control, and attribute-based access control, which safeguard the IIoT from unauthorized access.
5) Secure data aggregation and privacy preservation: Homomorphic encryption, differential privacy, and secure multiparty computation protect sensitive industrial data while allowing analytics.
6) Energy-efficient security: Lightweight cryptography, energy-aware IDS,[29] and optimization strategies balance robust security with the limited resources of IIoT devices.

LITERATURE OF REVIEW

This section reviews secure communication approaches in IIoT-based CPS, with emphasis on privacy-preserving intrusion detection, semantic security ontologies, blockchain-assisted authentication, and SDN-enabled lightweight intrusion detection.

Saheed and Chukwuere provide a novel approach to preserving user privacy in CPS-IIoT cyber-attack detection using agglomerative clustering and Bidirectional Long Short-Term Memory (BiLSTM) integrated with scaled dot-product attention. Particularly designed for CPS-IIoT environments, suggested solution has agglomerative clustering and a scaled dot product attention mechanism. These mechanisms adaptively modify their emphasis to prioritize crucial features within the CPS-IIoT network traffic data, providing additional computational resources to data segments that are likely to include abnormalities and patterns that indicate security issues. They evaluated the performance of proposed model by conducting experiments on two relevant datasets: University of New South Wales (UNSW)-NB15 and a novel IIoT dataset named X-IIoTID.[30]

Jarwar *et al.* offer a thorough evaluation by conducting a systematic study of ontologies and important security properties necessary for simulating the safety of IIoT settings. Academic papers, ontologies for semantic security, and cybersecurity standards are all part of a comprehensive review. Based on findings, uniform security ontologies designed for IIoT may be built around key security concepts and attributes. They also investigate the possibility of incorporating ontologies into the Industry 5.0 model, which prioritises sustainability, resilience, and human-centeredness. Although ontologies provide the ability to represent structured data, they do not yet adequately address the specific security requirements of Industry 5.0, which are characterised by increased collaboration and adaptability.[31]

Belay *et al*. propose DTKD-Fed, a novel semi-supervised DDoS detection framework that integrates digital twin technology with federated knowledge distillation. By leveraging digital twins as virtual replicas of IoT devices, the proposed method enables continuous learning and decentralized model training without requiring labeled data or sharing raw data. The DTKD-Fed framework enhances real-time anomaly detection and mitigates DDoS attacks while maintaining data privacy.[32]

Gyamfi *et al.* propose a novel IIoT network security using federated blockchain (FB) and ML-based verification. Multi-access Edge Computing (MEC) optimizes the FB model to ensure data integrity and confidentiality between the IIoT's local network cluster and external devices. Data within the local network cluster is secured with public-key cryptography. The ML-based verification model ensures legitimate key-pair updates and device joining in MEC-assisted IIoT. This approach outperforms conventional security solutions in scalability, data privacy, and adaptability to IIoT network changes. Present a detailed implementation and evaluate its

Table 2: Summary of literature on secure protocols for IIoT communication in CPS

References	Study on	Approach	Key findings	Challenges	Future direction
Saheed *et al*. (2025)	Privacy-preserving cyber-attack detection for CPS-IIoT	Pearson correlation + agglomerative clustering + BiLSTM with scaled-dot product attention; evaluated on UNSW-NB15 and X-IIoTID using a CPS-IIoT testbed	Very high detection performance on UNSW-NB15 (Acc 99.60%, AUC 100%, Precision 100%, Recall 97.98%, F1 98.23%); X-IIoTID used as realistic IIoT benchmark	Potential generalisability to unseen IIoT protocols/devices; computational cost of attention & clustering in real-time CPS	Validate on larger, heterogeneous IIoT deployments; optimize for real-time/edge deployment and resource constraints
Jarwar *et al*. (2025)	Systematic review of security ontologies for IIoT	Systematic literature review of semantic ontologies and standards for IIoT security	Identifies key security concepts/attributes and gaps in existing ontologies; finds limited alignment with Industry 5.0 goals (human-centricity, resilience, sustainability)	Lack of standardized, security-by-design ontologies; poor semantic mapping and sociotechnical coverage	Develop holistic, standardized IIoT security ontologies addressing socio-technical aspects and Industry 5.0 requirements
Belay *et al*. (2025)	Semi-supervised DDoS detection for IoT	DTKD-Fed: digital twin + federated knowledge distillation; semi-supervised, privacy-preserving, decentralized learning	Demonstrates high detection accuracy and scalability without sharing raw data; continuous learning using digital twins	Complexity of maintaining accurate digital twins; communication/ compute overhead in federated setup	Improve twin fidelity and efficiency; test in large-scale, real-world IIoT deployments and heterogeneous networks
Gyamfi *et al*. (2024)	IIoT security using federated blockchain & ML verification	MEC-assisted federated blockchain for key management + ML verification for device joining/key updates	Enhances data integrity/ confidentiality and scalability; ML verification reduces illegitimate key updates	Overhead of blockchain/MEC integration; latency and resource demands on constrained IIoT devices	Lightweight blockchain primitives, optimized MEC orchestration, and energy-aware ML verification for constrained devices
Irshad *et al*. (2023)	SDN-enabled IIoT 3-factor authenticated key exchange	Cryptographic three-factor authentication with SDN controller mediation; formal/informal security analysis	Proven secure under analysis; favorable trade-off between security features and computational overhead (simulation results)	Centralization risk (SDN controller as attractive target); deployment complexity in heterogeneous IIoT	Decentralized/resilient controller architectures, hardware-friendly implementations, and real-world testbed validation
Attkan *et al*. (2022)	IoT security mechanisms, authentication, and integration with blockchain & AI	Systematic survey of trending technologies and traditional key security mechanisms	Provides a comprehensive review of authentication methods and session key management; highlights integration of blockchain and AI for enhanced cybersecurity in IoT	Heterogeneity of IoT edge devices; diverse storage formats; need for highly secure mutual authentication	Development of standardized secure authentication protocols; adoption of AI and blockchain for scalable IoT security; addressing interoperability of heterogeneous devices

SDN: Software-defined networking, NB: Narrowband, ML: Machine learning, AI: Artificial intelligence, CPS: Cyber-physical systems, IIoT: Industrial internet of things

performance using a realistic IoT testbed, showing improved network security while maintaining the performance and scalability of MEC-assisted IIoT systems.[33]

Irshad *et al.* propose a novel SDN-supported approach to three-factor authenticated key exchange (SUSIC) for the IIoT ecosystem. If an SDN-enabled controller node is used to conduct mutual authentication, then a registered user can access real-time data from a physical IIoT environment using the SUSIC database. Following thorough official and informal security testing, the scheme was found to be secure. Simulation findings and performance evaluations also point to a more favourable compromise between security features and computational overheads. Several innovative applications have arisen as a result of the convergence of CPSs with the rapidly expanding information and communication technology sector. These include smart grids, public safety, intelligent transportation, smart logistics, and remote healthcare.[34]

Attkan and Ranga delve into the topic of classic key security measures while methodically surveying current trending technologies from the perspective of IoT security. Integrating the IoT, blockchain technology, and authentication based on AI in cybersecurity is the subject of this article's thorough and high-quality research. Because it helps its users live better lives and stay up with technical developments in the cyber-physical world, the IoT has been getting a lot of attention recently. There is a wide variety of underlying technologies and storage file types utilised by the IoT edge devices. To communicate data securely, these devices must first authenticate each other using highly secure methods of mutual authentication.[35]

Table 2 summarizes the literature review by outlining the purpose, methodology, main results, obstacles, and suggested next steps for each study.

CONCLUSION AND FUTURE WORK

Secure protocols for IIoT communication in CPS have been critically examined, highlighting their central role in enabling trusted and resilient Industry 4.0 ecosystems. While IIoT-enabled CPS accelerate automation and intelligence, they remain highly exposed to multifaceted threats stemming from vulnerable components, legacy infrastructures, human-centric weaknesses, and increased interconnectivity. Attack vectors such as man-in-the-middle, DoS, and malware injection directly compromise confidentiality, integrity, and availability, necessitating robust defense mechanisms. Recent advances, including privacy-preserving intrusion detection, semantic security ontologies, blockchain-assisted authentication, federated learning, and SDN-enabled anomaly detection, demonstrate strong potential by enhancing scalability, data confidentiality, and adaptability across heterogeneous industrial environments. Nonetheless, limitations such as computational overhead, latency constraints, semantic misalignment, and centralization risks continue to challenge secure protocol design, particularly in resource-constrained IIoT settings.

Future research should prioritize the development of lightweight, real-time, and adversarially robust security protocols tailored for IIoT-CPS. Key directions include resilient SDN controllers, energy-efficient blockchain integration, standardized semantic ontologies aligned with Industry 5.0, and adaptive intrusion detection optimized for edge and fog deployment. Large-scale validation across heterogeneous industrial testbeds will be critical to ensure practical applicability, resilience, and long-term sustainability of next-generation secure industrials ecosystems.

REFERENCES

1. Pivoto DG, De Almeida LF, Da Rosa Righi R, Rodrigues JJ, Lugli AB, Alberti AM. Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. J Manuf Syst 2021;58:176-92.
2. Patel R. Optimizing communication protocols in industrial IoT edge networks: A review of state-of-the-art techniques. Int J Adv Res Sci Commun Technol 2023;4:503-14.
3. Agrawal N, Kumar R. Security perspective analysis of industrial cyber physical systems (I-CPS): A decade-wide survey. ISA Trans 2022;130:10-24.
4. Chalapathi GS, Chamola V, Vaish A, Buyya R. Industrial internet of things (IIOT) applications of edge and fog computing: A review and future directions. Adv Inf Secur 2021;83:293-325.
5. Patel R. Security challenges in industrial communication networks: A survey on ethernet/Ip, controlnet, and devicenet. Int J Recent Technol Sci Manag 2022;7: 54-63.
6. Gerodimos A, Maglaras L, Ferrag MA, Ayres N, Kantzavelou I. IoT: Communication protocols and security threats. Internet Things Cyber Phys Syst 2023;3:1-13.
7. Shah V. An analysis of dynamic DDoS entry point localization in software-defined WANs. Int J Adv Res Sci Commun Technol 2024;4:442-55.
8. Chandu HS. Enhancing manufacturing efficiency: Predictive maintenance models utilizing IoT sensor data. Int J Sci Adv Res Technol 2024;10:58-66.
9. Wollschlaeger M, Sauter T, Jasperneite AJ. The future of industrial communication. IEEE Ind Electron Mag 2017;1:17-27.
10. Seetharaman KM. Internet of things (IoT) applications in SAP: A survey of trends, challenges, and opportunities. Int J Adv Res Sci Commun Technol 2021;3:499-508.
11. Shah V. Networking challenges in IoT to deployment of TCP/IP to 6LoWPAN for next Gen network system. KOS J Sci Eng 2024;1:1-8.
12. Cengiz K, Ozyurt B, Singh KK, Sharma R, Topac T, Chatterjee JM. The Role of IoT and Narrow Band (NB)-IoT for Several Use Cases. Berlin: Springer; 2021.
13. Pahune S. Data Collection and Performance Evaluation using a TK1 Board Major: Computer Engineering. United States: University of Memphis Digital Commons; 2019.
14. Patel N. Sustainable smart cities: Leveraging IoT and data analytics for energy efficiency and urban development. J Emerg Technol Innov Res 2021;8: 313-9.
15. Jaidka H, Sharma N, Singh R. Evolution of IoT to IIoT: Applications & challenges. SSRN Electron J 2020:1-6.
16. Mathur S, Gupta S. An Energy-Efficient Cluster-based Routing Protocol Techniques for Extending the Lifetime of Wireless Sensor Network. In: 2023 International Conference on the Confluence of Advancements in Robotics, Vision and Interdisciplinary Technology Management (IC-RVITM). IEEE; 2023. p. 1-6.
17. Latif S, Driss M, Boulila W, Huma ZE, Jamal SS, Idrees Z, *et al*. Deep learning for the industrial internet of things (IIoT): A comprehensive survey of techniques, implementation frameworks, potential applications, and future directions. Sensors (Basel) 2021;21:7518.
18. Alfahaid A, Alalwany E, Almars AM, Alharbi F,

Atlam E, Mahgoub I. Machine learning-based security solutions for IoT networks: A comprehensive survey. Sensors (Basel) 2025;25:3341.
19. Tan SF, Samsudin A. Recent technologies, security countermeasure and ongoing challenges of industrial internet of things (IIoT): A survey. Sensors (Basel) 2021;21:6647.
20. Abeck S, Schneider M, Quirmbach JP, Klarl H, Urbaczek C, Zogaj S. A Context Map as the Basis for a Microservice Architecture for the Connected Car Domain. Lecture Notes in Informatics (LNI). Vol. 294. In: Proceedings-Series of the Gesellschaft Fur Informatik; 2019. p. 125-38.
21. Bilipelli AR. AI-driven intrusion detection systems for large-scale cybersecurity networks data analysis: A comparative study. TIJER Int Res J 2024;11:a922-8.
22. Fereidouni H, Fadeitcheva O, Zalai M. IoT and man-in-the-middle attacks. Secur Priv 2025;8:1-19.
23. Arora S, Khare P, Gupta S. AI-Driven DDoS Mitigation at the Edge: Leveraging Machine Learning for Real-Time Threat Detection and Response. In: 2024 International Conference on Data Science and Network Security (ICDSNS). IEEE; 2024. p. 1-7.
24. Ghali AA. Artificial Intelligence and Bioinspired Computational Methods. Vol. 1225. Berlin: Springer; 2020.
25. Kim H, Lee K. IIoT malware detection using edge computing and deep learning for cybersecurity in smart factories. Appl Sci 2022;12:7679.
26. Rao D, Waoo AA, Singh MP, Pareek PK, Kamal S, Pandit SV. Strategizing IoT network layer security through advanced intrusion detection systems and AI-driven threat analysis. J Intell Syst Internet Things 2024;24:195-207.
27. Pandya S. Innovative blockchain solutions for enhanced security and verifiability of academic credentials. Int J Sci Res Arch 2022;6:347-57.
28. Thangaraju V. Enhancing web application performance and security using AI-driven anomaly detection and optimization techniques. Int Res J Innov Eng Technol 2025;9:205-12.
29. Prajapati N. Review of quantum computing advances and their impact on modern cryptographic security. Int J Innov Sci Res Technol 2025;10:2023-35.
30. Saheed YK, Chukwuere JE. CPS-IIoT-p2attention: Explainable privacy-preserving with scaled dot-product attention in cyber-physical system-industrial IoT network. IEEE Access 2025;13:81118-42.
31. Jarwar MA, Watson J, Ali S. Modeling industrial IoT security using ontologies: A systematic review. IEEE Open J Commun Soc 2025;6:2792-821.
32. Belay MA, Rasheed A, Rossi PS. Digital Twin Knowledge Distillation for Federated Semi-Supervised Industrial IoT DDoS Detection. In: 2025 IEEE Symposium on Computational Intelligence in Security, Defence and Biometrics Companion (CISDB Companion); 2025. p. 1-5.
33. Gyamfi E, Ansere JA, Kamal M, Mir S, Bonsu KA. Adaptive Federated Blockchain-Powered Security for MEC-Assisted Industrial IoT Ecosystems. In: 2024 19th International Conference on Emerging Technologies (ICET); 2024. p. 1-6.
34. Irshad A, Mallah GA, Bilal M, Chaudhry SA, Shafiq M, Song H. SUSIC: A secure user access control mechanism for SDN-enabled IIoT and cyber-physical systems. IEEE Internet Things J 2023;10:16504-15.
35. Attkan A, Ranga V. Cyber-physical security for IoT networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex Intell Syst 2022;8:3559-91.