Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 06| 2025

Review Article **Received:** 15-05-2025| **Accepted:** 10-06-2025 | **Published:** 25-06-2025

Review of Secure Communication Systems for Cyber-Physical Systems and Industrial IoT

Sri Harsha Panchali[1], Usha Mohani kavirayani[2], Krishna Bhardwaj Mylavarapu[3], Jenitha Pilli[4], Prathik Kumar Jannu[5] and Javed Ali Mohammad[6]

[1]*Information Systems Engineer, CrowdStrike Inc*
[2]*Kent State University, MS in Computer Science*
[3]*MS in Computer Science, University of Illinois Springfield*
[4]*MS in Computer Science, University of Louisiana at Lafayette*
[5]*Computer Science Engineering, JNTU Hyderabad*
[6]*Masters in Data Science, New England College*

Abstract: Cyber-Physical Systems (CPS) and the Industrial Internet of Things (IIoT) have played a major role in the development of energy management, transportation, smart manufacturing, and other mission-dependent industrial applications. One need is real-time, continuous connection between the cyber and physical parts. However, its integration with various types of devices, obsolete industrial protocols and IP-based networks make it extremely vulnerable to exploitations. Therefore, the threats are able to eavesdrop, spoof, denial-of-service, and data manipulation attacks on secure communication architectures of IIoT and CPS, which in particular include core systems, architectural layers, and communication protocols, as well as security mechanisms. The characteristics of IIoT situations, dispositional formations of CPS, and the role of communications and networking technologies in the data exchange. Other significant security approaches led to the industrial environment like authentication, encryption, lightweight cryptography, secure management of keys, and use of middleware and gateways are a limited resource available within a system care of the real-time security-related constraints so that the stability and safety of the system may be ensured that there is a requirement of secure communication structures that are flexible and capable of predicting industrial uses.

Keywords: Cyber-Physical Systems (CPS), Industrial Internet of Things (IIoT), Secure Communication protocol, Industrial Network Security.

INTRODUCTION

The Internet of Things (IoT) framework has enabled easy communication among a massive number of interconnected objects that can sense, process, and exchange information through different networks. Communication forms the fundamental layer in systems using the IoT that is required in the data acquisition, coordination of devices, and delivery of services [Lv, W. *et al*., 2017; Sarkar, C. *et al*., 2014]. At that, it requires stable and effective communication techniques to ensure the flow of the data within the required time, the expandability of the system, and the interaction of the devices that are not concentrated in one location, particularly in the areas where real-time monitoring and regulation are needed.

Internet of Things (IoT) applications in the manufacturing, energy, transportation, and process automation industries make up what is known as the Industrial Internet of Things (IIoT) [Wu, M. *et al*., 2010]. Communication infrastructures of IIoT are equipped with the integration of different devices like sensors, actuators, programmable logic controllers, and supervisory systems through both the legacy industrial protocols and IP-based networks [Pathak, P. *et al*., 2015; Garg, S. 2019]. Such kinds of surroundings place very strict conditions on the communication such as latency, determinism, reliability, and availability [Raposo, D. *et al*., 2018]. As a result, communication architectures in IIoT have to be planned out in detail to be able to carry out the operations that are of a mission-critical nature and at the same time remain companionable with the existing industrial systems.

Cyber-Physical Systems (CPS) are a term for a very similar concept to the Internet of Things (IoT), which has opened up a lot of possibilities for multidisciplinary, where computational and networking components are merged very tightly with physical processes via control loops [Teslya, N., & Ryabchikov, I. 2017; Dobaj, J. *et al*., 2018]. In a scenario of IIoT, CPS are dependent on uninterrupted and reliable communication between the cyber and physical layers in order to keep the system stable and safe. If there is any interruption or attack on the communication, it will have an immediate impact on the physical processes which can result in system breakdowns or dangerous situations [Nerella, V. M. L. G. 2018; Malallah, S. *et al*., 2018]. Hence, the communication in IIoT

***Corresponding Author:** Sri Harsha Panchali

DOI- https://doi.org/10.5281/zenodo.19488312

systems with CPS as a core should be not only efficient but also resistant to errors and hostile actions.

With the adoption of IoT technology in cyber-physical systems (CPS), securing communication has been the main issue of concern [Xu, H. *et al*., 2018]. Different security architectures have been developed and implemented as a response to the security issues raised to prevent the communication channels from being attacked through denial-of-service assaults, replay attacks, spoofing, and eavesdropping [Olivier, F. *et al*., 2015; Sanchez-Iborra, R., & Cano, M. D. 2016]. These systems concentrate mainly on the establishment of trust between the entities that communicate with each other by means of the authentication mechanisms, on the protection of the data confidentiality as well as integrity by means of encryption techniques, and on the assurance of secure key distribution as well as management, there have been some improvements at the protocol level in terms of the security for the protocols that are commonly used in communications so as to be able to meet the limitations of the devices that have very few resources and the strict real-time requirements of the industrial environments.

Structure of the Paper

The paper is structured as follows: Section II presents the foundation of IIoT and cyber physical system. Section III presents architecture for CPS and IIoT. Section IV shows secure communication protocol and mechanism. Section V related Literature of review, Finally, Section VI concludes and future direction.

FOUNDATION OF IIOT AND CYBER-PHYSICAL SYSTEMS

The emergence of cyber-physical systems (CPS) and the Internet of Things (IoT) has created fascinating new opportunities for interdisciplinary research in two critical domains. A subset of the IoT, the Industrial Internet of Things (IIoT) links industrial machinery, sensors, actuators, control systems, and analytics platforms to increase automation, efficiency, safety, and predictability in industrial settings. This subset has made significant research findings and numerous advancements. Typically used in the manufacturing, energy, transportation, logistics, and utility sectors, it enables the acquisition, dissemination, and consultation of networked industrial equipment in real-time with the goal of optimizing operations and minimizing downtime.

Characteristics of IIoT

Superior Availability and Reliability

IIoT systems are supposed to be utilized in industrial processes of the mission critical nature where disruption may lead to severe financial damages, or even, security threats [Criado, J. *et al*., 2018]. In order to ensure continuous operation, they employ fault-tolerant architectures, redundancy, and failover.

Data Processing in Real Time

IIoT supports low-latency communication in real-time in processes such as automated quality control, industrial robotics [Patel, K. K. *et al*., 2016], predictive maintenance and so on. Real time analytics ensure timely responses to changes in operations.

Scalability and Interoperability

IIoT platforms enable smooth integration between heterogeneous devices and systems from various vendors by utilising open communication protocols (such as MQTT, OPC UA, and Modbus). They can manage thousands or millions of linked devices across extensive industrial operations because they are designed to scale effectively.

Security-First Design

IIoT uses strong cybersecurity measures, like security protocols, verification, intrusion detection, on top of safe firmware upgrades, to safeguard systems against cyber threats and unauthorised access because industrial infrastructure is so important.

Sturdiness and Integration of Edges

IIoT devices are designed to function dependably in challenging industrial settings, enduring vibration, dust, high temperatures, and electromagnetic interference. By processing data locally, edge computing capabilities are frequently integrated to lower latency, bandwidth consumption, and dependency on centralised cloud systems.

Architecture and Components of CPS

The term "cyber-physical system" (CPS) refers to a network of computer systems and physical components that are considered to work together

Publisher: SARC Publisher

intelligently [Koulamas, C., & Kalogeras, A. 2018]. Personalized healthcare, smart manufacturing, emergency response, smart transportation, energy supply and consumption, and homeland security are just a few of the vital areas that stand to benefit greatly from the new capabilities made possible by these intricately linked and integrated systems. Fig. 1 displays the CPS architecture.

Cyber-physical systems perform time-sensitive tasks with varied degrees of engagement with the environment, including human contact, by integrating computation, communication, sensing, and actuation with physical systems. In Fig. 1, see a CPS intellectual model. The purpose of displaying this diagram is to draw attention to the possible interconnections between various systems and devices in a SoS (such as a CPS infrastructure). A CPS can range from a single device to an entire network of interconnected devices, or it can be a system of systems (SoS) made up of numerous networks of interconnected devices. A device from one point of view might be a system from another, and vice versa; this pattern is recursive and perspective dependent. In the end, a CPS can't be complete without the decision flow and one of the information or action flows. While the action flow affects the real world, the information flow is a digital representation of the measurement of the physical world.

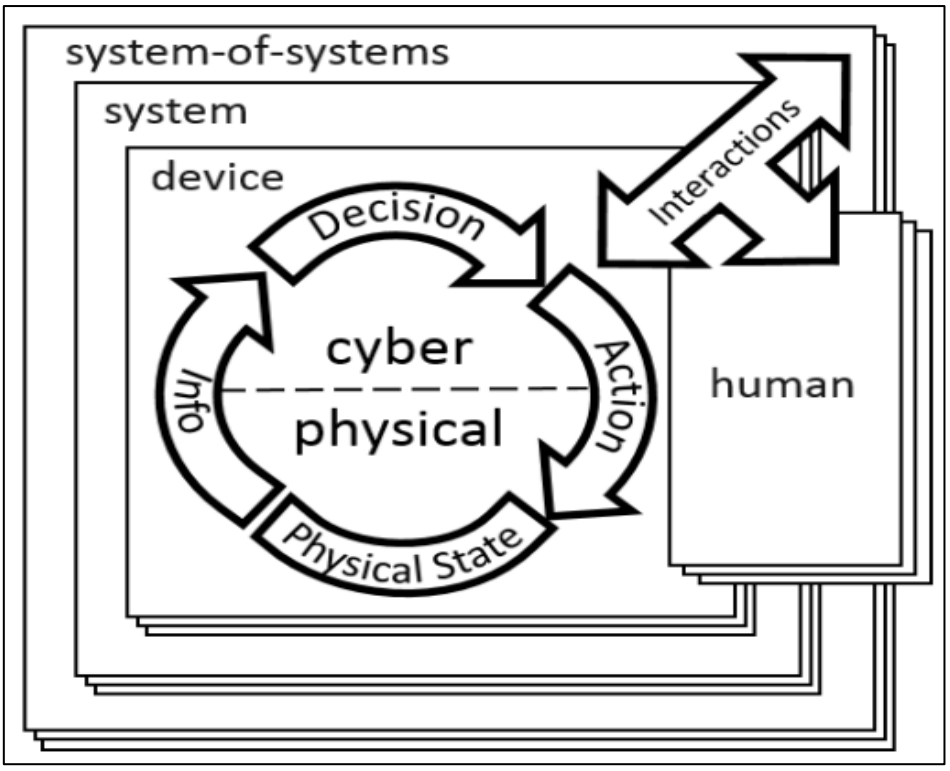

Fig 1: CPS Architecture

CPS Characteristics and Technologies

CPS rely on four distinct levels of key technology. Modern urban areas, electronic forms, intelligent power systems, etc. are CPS applications made possible by the interoperability of the numerous technologies in the layer stack, as shown in Fig. 2.

Publisher: SARC Publisher

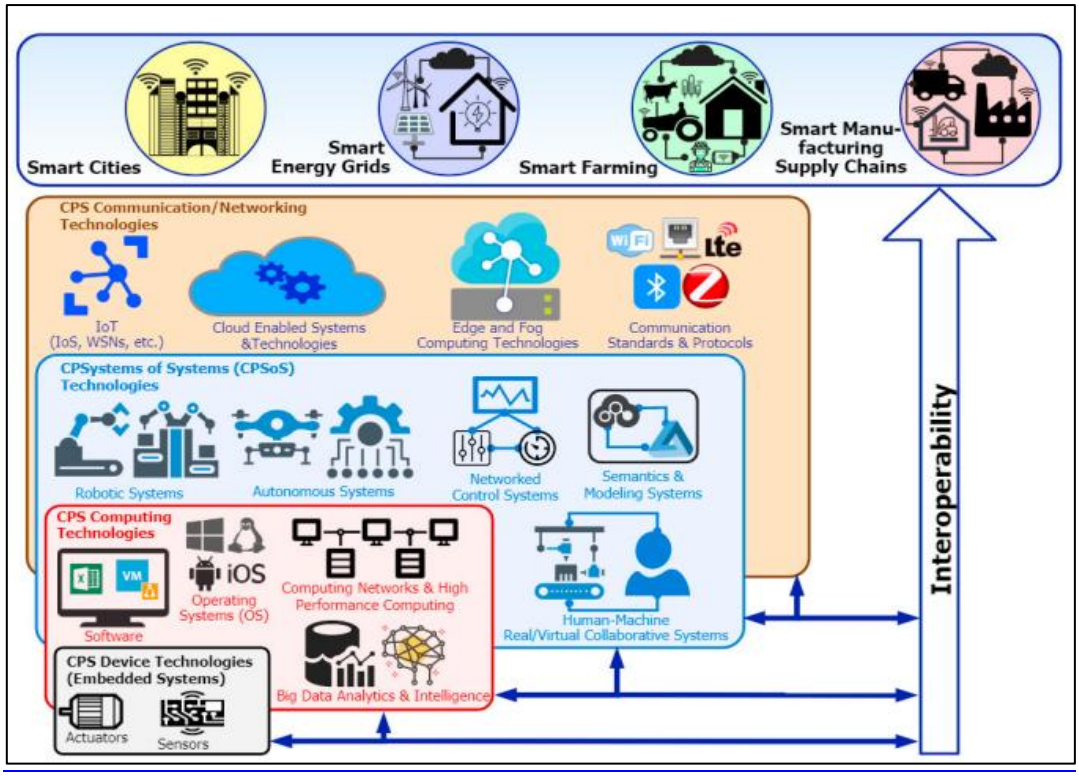

Fig 2: CPS Characteristic Technologies

Device Technologies

Device technologies make up any CPS's fundamental framework. They are the actual parts of the system that communicate with the outside world to gather information for analysis, control, and calculation. There are two main types: sensors that collect information about their surroundings (such humidity, temperature, etc.) and actuators that modify their surroundings using the processed data from those sensors. The hardware and software components of any CPS device technology form an embedded system.

- Hardware: This section relies on the interplay between mechanical and electrical parts to keep the device running smoothly. Shafts, rotors, gear systems, and electrical circuits like ICs, microcontrollers, microprocessors, Field Programmable Gate Arrays (FPGAs), etc. are all examples of mechanical components.
- Software: The software can be integrated into the hardware or run through an operating system. Common programming languages used for this process include assembly and C. Some examples of embedded operating systems are Contiki, TinyOS, and Mantis.

CPS Computational Technologies

The CPS characteristic technologies stack continues with computational technologies as the next level. They allow for the abstraction, analysis, and processing of data between other technologies and the CPS devices. Computational technologies also provide the foundation for the management, development, and improvement of architectures, system algorithms, and crucial concerns such as data processing, privacy, and security. It is made up of technologies such various operating systems, software, embedded computing, HPC, data analytics, and intelligence.

Cyber Physical System of Systems (CPSoS)

A CPS's distributed autonomous subsystems participate in ongoing, bidirectional communication across many networks, ensuring the successful implementation of CPSoS [Tao, F. *et al*., 2017]. Also required are appropriate systems to facilitate the development of effective human-machine interactions and collaborative structures. The aforementioned criteria for CPSoS deployment have been included in example works that use this architecture, which combines discrete event systems with continuous time ones.

Publisher: SARC Publisher

CPS Communication and Networking (CPS-ComNet) Technologies

CPS-ComNet technologies make it easier for data to move between the many systems and layers of the CPS technology stack. They make sure the CPS works well by allowing different communication protocols and standards to work together among the CPS technologies. Cloud computing, fog/edge computing, and the internet of things (IoT) have greatly improved how technology within and across CPS are networked and communicated.

Every layer of the computer stack makes use of CPS-ComNet technology. The CPS devices layer is connected to operational systems, software, data/intelligence algorithms, and WSANs (sensor/actuator networks that are either wireless or wired) through computer networks. The CPSoS layer is a multi-use area where edge, cloud, fog, and machine-to-machine (M2M) networks coexist.

Communication protocols and standards for CPS ComNet technologies

ComNet Technologies facilitated efficient and real-time information sharing between the cyber and physical elements through the use of standardized networking technologies [Kobara, K. 2016]. They let sensors, controllers, and control systems to talk to one another in a CPS environment, guaranteeing compatibility, fast response times, and secure data transfer. The CPS ComNet technologies that are able to communicate with one another are illustrated in Table I.

Table 1: CPS communication and networking protocols

Network Type	Com. Protocol	Features/Coverage	Freq./Data Rate	CPS App. Layer
Wired	UART	Low-power Up to 1km (standard dependent	Clock frequency of 77.6 MHz (baud rate 115200bps)/20kbps-20Mbps	WSANs, M2M
	SPI	Low-power Up to 100m	20MHz/20Mbps	WSANs, M2M
	I2C	Low-power Few meters	100kbps-3.4 Mbps	WSANs, M2M
	CAN	Up to 100m depending on the data rate	Up to 1Mbs	WSANs, M2M
	Ethernet	Local Area Networks (LANs) Max. of 100m	Up to 500MHz (cable dependent). 1–40Gbps (standard dependent)	WSANs, M2M
	ZigBee	Energy saving, Wireless LANs (WLANs) Up to 100m (standard dependent)	2.4 GHz/ 250 Kbps	WSANs, M2M
wireless	Bluetooth	Cable connection replacement. Up to 100m (version dependent)	2.4 GHz/ 1Mbps	WSANs, M2M
	Wi-Fi	Data networks, LAN, WLAN Up to 250 outdoors (standard dependent)	2.4–5 GHz/ 1 through to 150 Mbps (standard dependent)	WSANs, M2M, IoT (All)
	WiMAX	Metropolitan Area Network (MAN) Up to 56km	2–66 GHz/ 2–75 Mbps	WSANs, M2M IoT (All)
	Cellular 3G, 4G/LTE, 5G	Wide Area Networks (WANs), digital data packets	3G: 800–1900MHz 4G/LTE: 700–2500MHz	WSANs, M2M IoT (All)

Publisher: SARC Publisher

		1–several km (cell radius dependent)	5G/LTE: 600–6 GHz 5G/mmWave: 24–86 GHz	

SECURE ARCHITECTURE FOR IIOT AND CPS

The Industrial Internet of Things (IIoT) concept proposes a fully automated, transparent, and intelligent factory environment with the goal of enhancing production processes and overall efficiency. This goal can only be achieved if current hierarchical models evolve into completely linked vertical models [Liu, B. *et al*., 2019]. Cyber-attack vectors, standardization and interoperability concerns, and the IT/OT Industrial Control Systems (ICS) interface are only a few of the challenges that IIoT settings face due to their young. Further, the IIoT's machine-to-machine (M2M) communication uses cutting-edge communication models and technologies such as 5G, TSN Ethernet, and self-driving networks; thus, it calls for innovative and comprehensive approaches to provide the required data security levels. Fig. 3 shows the architecture of the IIoT and CPS.

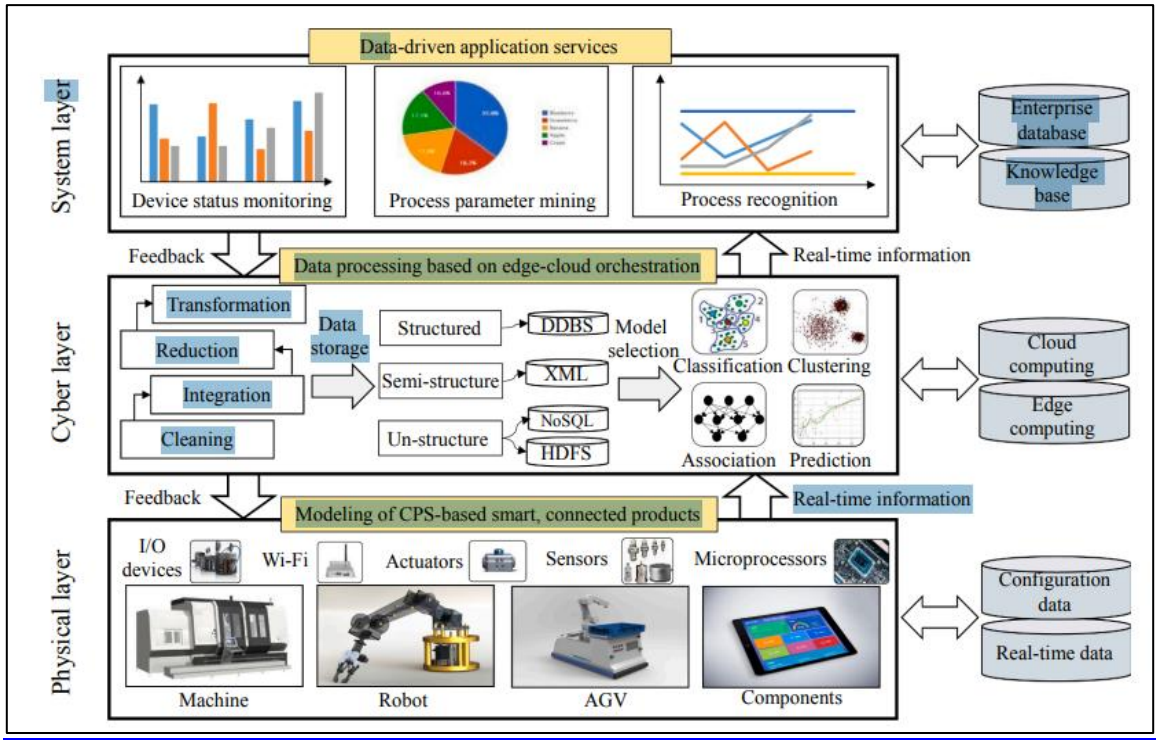

Fig 3: Architecture for CPS and IIoT

Physical layer

The physical layer details the setup of smart, linked objects that rely on CPS. Some of the parts that make up the hardware configuration are microprocessors, actuators, sensors, input/output devices, and a Wi-Fi module, and more. Machines, robots, AGVs, and other industrial equipment can be "retrofitted" with the characteristics of Industry 4.0—the ability to sense, compute, and communicate—after setup. Actually, at its core, the industrial Industrial equipment (e.g., machines, AGVs) on the shop floor can sense, transmit, and process data more easily with the appropriate hardware, which in turn can facilitate a reduction in production exceptions.

Cyber layer

The cyber layer is accountable for enhancing data quality and guaranteeing the efficacy and dependability of data analytics. This comprises data pretreatment (such as data cleansing, integration, reduction, and transformation). the first set of facts XML is used to define semi-structured data, which is then saved in DDBS or RDBMS. Unstructured data is stored and handled using Hadoop Distributed File System (HDFS) in addition to structured query language (NoSQL).

Publisher: SARC Publisher

System layer

Adopting data-driven application services such as process parameter mining, device status monitoring, and process recognition can cater to the demands of various stakeholders, including customers, manufacturers, suppliers, and service providers. Additionally, there is data stored in the background that is relevant to the application service's operation, including user requests, satisfaction levels, and rules.

Common Security Threats of CPS in IIoT

Unauthorised access, where hackers use lax authentication to take control of devices, and data breaches, where private industrial data is stolen, are frequent security risks in IoT and IIoT environments. While ransomware and malware disrupt processes or demand payment for restoration, denial-of-service (DoS) attacks can overwhelm networks and cause operational downtime. Malicious control can be undertaken using vulnerabilities in old firmware or software and man-in-the-middle (MitM) attacks can be used to intercept and modify communications. Moreover, the functionality of the systems can be altered or lead to the leaking of data by physical manipulation of sensors or devices. These threats highlight the importance of strong security measures to protect the key infrastructure and industrial operations against cyber-attack. Cyber-Physical Systems (CPS) are susceptible to numerous security risks that compromise the data integrity, safety, and functionality. Monitoring of unauthorised communication channels resulting in exposure of private operational data is referred to as eavesdropping and data interception. Denial-of-service (DoS) attacks target computer resources and network denial of service and disrupt real-time control processes. Spoofing and identity attacks occur when attackers assume the identity of trusted devices or users with the aim of loading malicious information or instructions, which can lead to perilous behaviour. Insider threats are the cases whereby authorised members are found to deliberately or negligently use their access to fight the systems or disclose confidential data. CPS environments require strict access control procedures, intrusion detection, high-level encryption, and authentication in order to combat these threats.

Unique Security Challenges in Industrial Environments

Industrial settings are unique integrating the outdated systems presents security concerns, specialised equipment, and ongoing requirements of the operations. Many SCADA systems and industrial control systems (ICS) were originally not designed to resist cybersecurity and their vulnerability to modern attacks is an open field [Rúbio, E. M. *et al*., 2018]. The need to ensure high availability exposes the systems to unpatched vulnerabilities due to downtime reduction on occurrence of security updates. The conditions in harsh locations, remote areas, and the use of heterogeneous vendors create more challenges in monitoring and threat mitigation. In addition, physical processes can now be directly impacted by cyber threats since there is an overlap of information technology (IT) and operational technology (OT) which increases the attack surface. Supply chain risks, insider threats and regulatory compliance are other complexities that add to the protection of industrial environments.

Real-World Security Incidents

The severe consequences of cyberattacks on the critical infrastructure are exhibited by real security breaches in the cyber-physical and Internet of Things networks. Among them is the Stuxnet worm (2010) which exploited zero-day vulnerabilities in SCADA systems to attack the nuclear facility in Iran and physically destroy centrifuges without being detected [Mosterman, P. J., & Zander, J. 2016]. The other example is the 2015 Ukrainian power grid attack where hackers broke into the control systems and caused a serious power outage that impacted over 230,000 people. Through ransom and file encryption, the internet services across the globe are experiencing an unsecured huge distributed denial-of-service (DDoS) assaults are being caused by attacks on the internet of things (IoT). Ongoing monitoring, secure software design, and timely patching, as well as solid authentication process, are essential as these attacks demonstrate that CPS and IoT vulnerabilities can be exploited in espionage, sabotaging, and massive disruption. The lessons of these cases point to the necessity of active, multi-layered, and robust cybersecurity in the industrial and Internet of Things environments to be able to overcome the evolving threats.

Publisher: SARC Publisher

SECURE COMMUNICATION PROTOCOL AND MECHANISM

Secure communication scheme in IIoT and CPS is to ensure data between networks, controllers and devices is available, confident and integral. Considering the variety of the industrial and Internet of Things protocols, these architectures follow a tiered strategy, combining intrusion detection, access control, encryption, and authentication on various levels. To safeguard both IP-based and non-IP-based communications, network segmentation, secure gateways, and protocol-specific security enhancements (such as secure Modbus and KNX/IP over TLS) are put into place.

Secure Industrial Communication Protocols

Secure Industrial Communication Protocols refer to communication standards that are implemented in industrial facilities and come with security features to ensure the safe exchange of data among the various sensor, controller, and supervisory systems that are part of Industrial IoT (IIoT) and Cyber-Physical Systems (CPS). Until 2019, most widely used protocols like OPC UA, Secure DNP3, and Modbus Security improved the security of the standard industrial communication by introducing features that allow secure authentication, encrypted data transmission, and integrity verification [Wang, L., & Wang, G. 2016]. These protocols were created to fulfill industrial demands such as reliability, real-time operation, and interoperability and, at the same time, protect against security risks in the digital realm, including hacking, data corruption, and eavesdropping.

Key Components

- Authentication and Access Control: This provides the means for the verification of communicating devices and users through certificate-based authentication and also ensures the control of privileges via role-based access control mechanisms.
- Encryption and Data Integrity: It secures the communication data with the help of encryption methods (e.g., TLS/SSL) to ensure the confidentiality of the data and also to stop any kind of tampering, during data transmission

Lightweight Cryptography for Resource-Constrained Devices:

Cryptography with Lightweight Algorithms Simple cryptographic algorithms such as Ascon, PRESENT, and SPECK are employed due to the fact that many IIoT and CPS devices have limited processing power, storage, and energy. Such algorithms are ideal in latency-sensitive and battery-powered applications since they reduce a computational and energy overhead and still have good security properties.

Secure Key Management in IIoT/CPS

Secure communications necessitate efficient key management. Among these tasks are the generation, distribution, storage, rotation, and revocation of secure keys. Hardware security modules, trusted platform modules, and public key infrastructure all work together to prevent cryptographic keys from being leaked or altered by unauthorized parties.

Secure Middleware and Gateways

Intrinsic security bases include middleware and gateways, which make connections among dissimilar networks and devices. They are forced to implement access controls, protocol validation, encrypted channels of data and mutual authentication. They also make sure that the industrial ecosystems are end-to-end secure since they serve as intrusion detection points, provide network segmentation and secure information flow between the IT and operational technology (OT) worlds.

Cryptographic and Authentication Mechanisms

Cryptographic and Authentication Mechanisms are imperative components which assist in ensuring the security of the communication between the IIoT and Cyber-Physical Systems (CPS) [Kim, J. H. 2017]. They also guarantee trusted communication between devices and systems as well as safeguarding the sensitive industrial information besides offering the customary encrypted means of cryptography such as the symmetric encryption (AES) to cover solitary information security; the asymmetric encryption methods (ECC and RSA) to handle identity verification and secure key exchange. authentication methods like RBAC, PKI, and certificate-based authentication were extensively employed to verify the authenticity of devices and users. These methods made it difficult for

Publisher: SARC Publisher

unauthorized access, impersonation, and data tampering to occur while also being compatible with legacy industrial systems and satisfying the requirements of real-time operations

Encryption and Key Management: Are powered by the duo of symmetric and asymmetric cryptographic algorithms together with securely implemented key distribution mechanisms that make industrial communications confidentiality and integrity guaranteed.

Authentication and Authorization: Confirm identity of the device and user through the use of digital certificates coupled with access control policies that limit the system access to trusted entities.

LITERATURE OF REVIEW

The reviewed works explore secure communication and system reliability in Industrial IoT (IIoT) and Cyber physical system are used in technique and Table II in key approach, challenges, Limitation and future work are discussed below:

Karaagac, Verbeeck and Hoebeke (2019) there has been very little time for the idea of the IoT. A vast array of sensors, machines, and Internet-connected gadgets are brought together by it, allowing them to exchange data and work in tandem. Here take a look at two potential standards for interoperability in these two areas—OPC Unified Architecture and the Lightweight Machine-to-Machine (LwM2M) protocol and how they relate to one another and the integration of the two domains. It also delves into a scalable and effective way to integrate and interoperate across domains utilising Docker containers [Karaagac, A. *et al*., 2019].

Vakaloudis and O'Leary (2019) introducing the Internet of Things (IoT) in industrial settings efficiently requires a multidisciplinary approach and the implementation of baby stages to keep disturbance to a minimum. From the first sensor node all the way to the end user interface, solution considers the software and hardware components of the system as a whole while solving this challenge [Vakaloudis, A., & O'Leary, C. 2019].

Gore *et al*. (2019) industrial plants make a positive impact on businesses by improving data visualization and decision-making. This includes water, oil-gas, and chemical plants. Gathering information from plant-based sensor devices and transmitting it over the internet for either local or remote control and monitoring is a common use case for the IIoT. The Internet of Things (IoT) usually uses low-power wireless communication at the local level to gather data from sensor devices and a gateway that is connected to the internet. This data can be used for either local or remote control and monitoring. Bluetooth low energy (BLE) and a gateway working together, allows for the local communication and monitoring of sensor devices in an industrial plant, as well as their connection to Internet-based services and applications [Gore, R. N. *et al*., 2019].

Sen and Jayawardena (2019) Generating vast amounts of data are IoT and CPS. A well-functioning cyber-communication infrastructure is crucial to the success of these three; improving the cyber-communication internetwork's performance entails optimizing network procedures and ensuring the cyber-network's security. Given the increasing number of cyberattacks on large-scale physical infrastructures and industrial hardware, it is critical to prioritize the development of more robust and efficient data transfer protocols in order to boost the Internet's overall performance [Sen, S., & Jayawardena, C. 2019].

Xu *et al*. (2018) the incorporation of smart computing and network technologies into mainstream manufacturing and production is at the heart of the industrial revolution. Building an IIOT to allow for the interconnection of different processes and devices is also a part of this revolution. Distinct from the IoT in consumer use, the Industrial Internet of Things (IIoT) has many unique characteristics. Some of these challenges include the fact that networking technologies like 5G, machine-to-machine communication, and the IIoT's second computing dimension are required for IIoT applications. In addition, there are strict command and control requirements that IIoT applications must meet [Xu, H. *et al*., 2018]

Choi *et al*. (2017) Cyber-Physical Systems (CPS) contain certain distinguishing features, such as the fact that digital commands can be physically observed and verified, and that the number of possible combinations of commands is limited and finite. An increase of CPSs necessitates durable, maintenance-free solutions to mitigate cyber threats. It is possible to manage and maintain

Publisher: SARC Publisher

cyber-physical systems using TDA, a conceptual framework for system engineering, without constantly updating security patches or fixing vulnerabilities [Choi, S. *et al*., 2017].

Table 2: Literature Review on Industrial Iot and Cyber-Physical System in Secure Communication

Authors	Key Approach	Methodology	Challenges Addressed	Limitations	Future Work
Karaagac, Verbeeck & Hoebeke (2019)	Cross-domain integration of IoT and industrial systems using OPC UA and LwM2M	Proposed an efficient and scalable integration framework using Docker containers to enable interoperability between OPC UA and LwM2M	Interoperability between heterogeneous industrial IoT standards; scalability of cross-domain communication	Focused mainly on protocol-level integration; limited evaluation in large-scale real industrial deployments	Extend validation to real-world industrial environments; performance evaluation under large-scale and heterogeneous networks
Vakaloudis & O'Leary (2019)	Holistic end-to-end IoT adoption in industrial environments	Stepwise, multidisciplinary system design approach covering sensors, gateways, software, and user interfaces	Risk minimization and disruption during industrial IoT adoption; system integration complexity	Incremental approach may slow down full-scale deployment; lacks quantitative performance metrics	Development of automated deployment tools; integration with advanced analytics and AI-driven decision systems
Gore *et al*. (2019)	Industrial IoT data acquisition using BLE and gateways	Utilized Bluetooth Low Energy (BLE) for local sensor communication and gateways for Internet connectivity	Efficient low-power data acquisition; local monitoring and control in industrial plants	BLE range and scalability limitations; potential interference in harsh industrial environments	Exploration of alternative low-power wireless technologies; enhanced gateway intelligence and edge analytics
Sen & Jayawardena (2019)	Secure and optimized cyber-communication infrastructure for IoT and CPS	Optimal network design and cybersecurity measures for optimal network performance	Cybersecurity threats targeting industrial infrastructure; network performance bottlenecks	Mainly conceptual and analytical; limited implementation details	Design of adaptive security frameworks; real-time intrusion detection for CPS and IIoT systems
Xu *et al*. (2018)	Infrastructure planning and development for the IIoT	Survey and analysis of IIoT networking (5G, M2M), computing paradigms (cloud, edge, hybrid)	Meeting strict QoS, reliability, and control requirements in industrial systems	Broad survey nature; lacks experimental validation	Practical implementation of hybrid cloud–edge architectures; optimization of 5G-enabled IIoT systems
Choi *et al*. (2017)	Trusted Dynamic	Proposed a conceptual	Reducing cyber risks without	Conceptual framework with	Prototype implementation;

Publisher: SARC Publisher

	Adaptation (TDA) for CPS security	system engineering framework enabling resilient and maintenance-free CPS operation	frequent patching; resilience of CPS	limited empirical validation	integration of TDA with real-world IoT, ICS, and drone systems

CONCLUSION AND FUTURE WORK

Secure communication is a critical security component of the safe and reliable IIoT and CPS because these systems combine digital intelligence and physical industrial activities. It is noted in the review that the communication architectures of the IIoT and CPS context have to not only address the high demands of real-time performance, availability, and reliability but also achieve the utmost protection against the dynamic cyber threats. The deployment of a variety of devices, industrial protocols of the past, and modern IP-based networks significantly increase the scale of attack, which in turn makes the traditional security mechanisms ineffective Communications security protocols, strong authentication and access control systems, encryption, lightweight cryptography of limited resource devices, and effective key management are the conditions to safety of information, reliability of system, and data secrecy. On top of that, secure gateways and middleware are also very important for easing interoperability and at same time, they enforce end-to-end services across the IT to the OT domains. Despite the high advancement, the challenges of scalability, interoperability, legacy systems, and dynamic threat landscape the future IIoT and CPS installations must adhere to the adaptive, scalable, and interoperable security architectures that are flexible to satisfy the demands of the business world. Achieving the next-generation industrial system with durable and future-ready secure communication infrastructures will be difficult lacking state-of-the-art tools such as blockchain, AI, and edge computing.

REFERENCES

1. Lv, W., Meng, F., Zhang, C., Lv, Y., Cao, N., & Jiang, J. "A general architecture of IoT system." 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC). Vol. 1. IEEE, (2017).
2. Sarkar, C., SN, A. U. N., Prasad, R. V., Rahim, A., Neisse, R., & Baldini, G. "DIAT: A scalable distributed architecture for IoT." IEEE Internet of Things journal 2.3 (2014): 230-239.
3. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. "Research on the architecture of Internet of Things." 2010 3rd international conference on advanced computer theory and engineering (ICACTE). Vol. 5. IEEE, (2010).
4. Pathak, P., Shrivastava, A., & Gupta, S. "A survey on various security issues in delay tolerant networks." J Adv Shell Program 2.2 (2015): 12-18.
5. Garg, S. "Predictive analytics and auto remediation using artificial inteligence and machine learning in cloud computing operations." Available at SSRN 5267117 (2019).
6. Raposo, D., Rodrigues, A., Sinche, S., Sá Silva, J., & Boavida, F. "Industrial IoT monitoring: Technologies and architecture proposal." Sensors 18.10 (2018): 3568.
7. Teslya, N., & Ryabchikov, I. "Blockchain-based platform architecture for industrial IoT." 2017 21st conference of open innovations association (FRUCT). IEEE, (2017).
8. Dobaj, J., Iber, J., Krisper, M., & Kreiner, C. "A microservice architecture for the industrial Internet-of-Things." Proceedings of the 23rd European Conference on Pattern Languages of Programs. (2018).
9. Nerella, V. M. L. G. "Automated cross-platform database migration and high availability implementation." Turkish Journal of Computer and Mathematics Education (TURCOMAT) ISSN 3048 (2018): 4855.
10. Malallah, S., Zalah, Y., & Karne, R. "An Analysis of the Advanced Encryption Standard and Threats Associated." (2018).
11. Xu, H., Yu, W., Griffith, D., & Golmie, N. "A survey on industrial Internet of Things: A cyber-physical systems perspective." Ieee access 6 (2018): 78238-78259.

Publisher: SARC Publisher

12. Olivier, F., Carlos, G., & Florent, N. "New security architecture for IoT network." Procedia Computer Science 52 (2015): 1028-1033.
13. Sanchez-Iborra, R., & Cano, M. D. "State of the art in LP-WAN solutions for industrial IoT services." Sensors 16.5 (2016): 708.
14. Criado, J., Asensio, J. A., Padilla, N., & Iribarne, L. "Integrating cyber-physical systems in a component-based approach for smart homes." Sensors 18.7 (2018): 2156.
15. Patel, K. K., Patel, S. M., & Scholar, P. "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges." International journal of engineering science and computing 6.5 (2016).
16. Koulamas, C., & Kalogeras, A. "Cyber-physical systems and digital twins in the industrial internet of things [cyber-physical systems]." Computer 51.11 (2018): 95-98.
17. Tao, F., Cheng, J., & Qi, Q. "IIHub: An industrial Internet-of-Things hub toward smart manufacturing based on cyber-physical system." IEEE Transactions on Industrial Informatics 14.5 (2017): 2271-2280.
18. Kobara, K. "Cyber physical security for industrial control systems and IoT." IEICE TRANSACTIONS on Information and Systems 99.4 (2016): 787-795.
19. Liu, B., Zhang, Y., Zhang, G., & Zheng, P. "Edge-cloud orchestration driven industrial smart product-service systems solution design based on CPS and IIoT." Advanced Engineering Informatics 42 (2019): 100984.
20. Rúbio, E. M., Dionísio, R. P., & Torres, P. M. B. "Industrial IoT devices and cyber-physical production systems: Review and use case." International Conference on Innovation, Engineering and Entrepreneurship. Cham: Springer International Publishing, (2018).
21. Mosterman, P. J., & Zander, J. "Industry 4.0 as a cyber-physical system study." Software & Systems Modeling 15.1 (2016): 17-29.
22. Wang, L., & Wang, G. "Big data in cyber-physical systems, digital manufacturing and industry 4.0." International Journal of Engineering and Manufacturing (IJEM) 6.4 (2016): 1-8.
23. Kim, J. H. "A review of cyber-physical system research relevant to the emerging IT trends: industry 4.0, IoT, big data, and cloud computing." Journal of industrial integration and management 2.03 (2017): 1750011.
24. Karaagac, A., Verbeeck, N., & Hoebeke, J. "The integration of LwM2M and OPC UA: An interoperability approach for industrial IoT." 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE, (2019).
25. Vakaloudis, A., & O'Leary, C. "A framework for rapid integration of IoT Systems with industrial environments." 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE, (2019).
26. Gore, R. N., Kour, H., Gandhi, M., Tandur, D., & Varghese, A. "Bluetooth based sensor monitoring in industrial iot plants." 2019 International Conference on Data Science and Communication (IconDSC). IEEE, (2019).
27. Sen, S., & Jayawardena, C. "Analysis of network techniques and cybersecurity for improving performance of big data IoT and cyber-physical communication internetwork." 2019 IEEE International Conference on Industrial Technology (ICIT). IEEE, (2019).
28. Xu, H., Yu, W., Griffith, D., & Golmie, N. "A survey on industrial Internet of Things: A cyber-physical systems perspective." Ieee access 6 (2018): 78238-78259.
29. Choi, S., Chavez, A., Torres, M., Kwon, C., & Hwang, I. "Trustworthy design architecture: Cyber-physical system." 2017 International Carnahan Conference on Security Technology (ICCST). IEEE, (2017).
30. Gupta, A. K., Polu, A. R., Narra, B., Buddula, D. V. K. R., Patchipulusu, H. H. S., & Vattikonda, N. "Leveraging deep learning models for intrusion detection systems for secure networks." Journal of Computer Science and Technology Studies 6.2 (2024): 199-208.
31. Narra, B., Buddula, D. V. K. R., Patchipulusu, H., Vattikonda, N., Gupta, A., & Polu, A. R. "The integration of artificial intelligence in software development: Trends, tools, and future prospects." Available at SSRN 5596472 (2024).
32. Achuthananda, R. P., Bhumeka, N., Dheeraj Varun Kumar, R. B., Hari Hara, S. P., & Navya, V. "Evaluating machine learning approaches for personalized movie recommendations: A comprehensive analysis."

Publisher: SARC Publisher

J Contemp Edu Theo Artific Intel: JCETAI-115 (2024).
33. Waditwar, P. "The Intersection of Strategic Sourcing and Artificial Intelligence: A Paradigm Shift for Modern Organizations." Open Journal of Business and Management 12.06 (2024): 4073-4085.
34. Bitkuri, V., Kendyala, R., Kurma, J., Mamidala, J. V., Attipalli, A., & Enokkaren, S. J. "A Survey on Blockchain-Enabled ERP Systems for Secure Supply Chain Processes and Cloud Integration." International Journal of Technology, Management and Humanities 10.04 (2024): 126-135.
35. Mamidala, J. V., Bitkuri, V., Attipalli, A., Kendyala, R., Kurma, J., & Enokkaren, S. J. "Machine Learning Approaches to Salary Prediction in Human Resource Payroll Systems." Journal of Computer Science and Technology Studies 6.5 (2024): 341-349.
36. Waditwar, P. "AI for Bathsheba Syndrome: Ethical Implications and Preventative Strategies." Open Journal of Leadership 13.03 (2024): 321-341.
37. Attipalli, A., Kendyala, R., Kurma, J., Mamidala, J. V., Bitkuri, V., & Enokkaren, S. J. "Privacy Preservation in the Cloud: A Comprehensive Review of Encryption and Anonymization Methods." International Journal of Multidisciplinary on Science and Management IJMSM 1.1 (2024).
38. Tamilmani, V., Maniar, V., Singh, A. A., Kothamaram, R. R., Rajendran, D., & Namburi, V. D. "A Review of Cyber Threat Detection in Software-Defined and Virtualized Networking Infrastructures." International Journal of Technology, Management and Humanities 10.04 (2024): 136-146.
39. Singh, A. A. S., Kothamaram, R. R., Rajendran, D., Deepak, V., Namburi, V. T., & Maniar, V. "A Review on Model-Driven Development with a Focus on Microsoft PowerApps." International Journal of Humanities, Science Innovations and Management Studies 1.1 (2024): 43-56.
40. Padur, S. K. R. "AI-augmented platform engineering: Redefining developer experience through autonomous, self-optimizing enterprise systems." International Journal of Science, Engineering and Technology (2024).
41. Gangineni, V. N., Tyagadurgam, M. S. V., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., & Chalasani, R. "AI-Powered Cybersecurity Risk Scoring for Financial Institutions Using Machine Learning Techniques (Approved by ICITET 2024)." Journal of Artificial Intelligence & Cloud Computing (2024).
42. Sagili, S. R., Goswami, C., Bharathi, V. C., Ananthi, S., Rani, K., & Sathya, R. "Identification of Diabetic Retinopathy by Transfer Learning Based Retinal Images." 2024 9th International Conference on Communication and Electronics Systems (ICCES). IEEE, (2024).
43. Sagili, S. R., & Kinsman, T. B. "Drive dash: Vehicle crash insights reporting system." 2024 International Conference on Intelligent Systems and Advanced Applications (ICISAA). IEEE, (2024).
44. Padur, S. K. R. "Securing Oracle Integration Cloud ERP ecosystems, zero trust architecture, data governance, and compliance automation." International Journal of Science, Engineering and Technology 12.4 (2024): 10-5281.
45. Sagili, S. R., Chidambaranathan, S., Nallametti, N., Bodele, H. M., Raja, L., & Gayathri, P. G. "NeuroPCA: Enhancing Alzheimer's disorder Disease Detection through Optimized Feature Reduction and Machine Learning." 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT). IEEE, (2024).
46. Sagili, S. R., Veeranjaneyulu, K., Puli, B., Sundaramoorthy, P., Murugadoss, R., & Keerthana, N. V. "Advancing Cervical Cancer Identification using Generative-based Adversarial Networks: An Integrative Learning Methodology." 2025 6th International Conference for Emerging Technology (INCET). IEEE, (2025).
47. Routhu, K. K. "Beyond Automation: AI-Powered Employee Engagement Journeys in Oracle HCM Cloud." KOS Journal of AIML, Data Science, and Robotics 1.1 (2024): 1-6.
48. Routhu, K. K. "The future of HCM: Evaluating Oracle's and SAP's AI-powered solutions for workforce strategy." Journal of Artificial Intelligence, Machine Learning & Data Science 2.2 (2024): 2942-2947.

Publisher: SARC Publisher

49. Sannapureddy, R., Nadella, V. M., & Nelavelli, S. "Edge–Cloud Continuums for Latency-Sensitive Tasks." International Journal of AI, BigData, Computational and Management Studies 5.4 (2024): 189-201.
50. Arigela, A. K., Brahmareddy, A., Sreenivas, T. S., Selvan, M. P., Venu, N., & Lal, D. K. "Optimizing Energy Efficiency and Latency in IoT Devices Through AI-Based Adaptive Protocols in Fog-Edge Computing Environments." Congress on Smart Computing Technologies. Singapore: Springer Nature Singapore, (2024).
51. Nadella, V. M. "Al-Native 6G Network Management." American International Journal of Computer Science and Technology 6.1 (2024): 23-37.
52. Sannapureddy, R., Nadella, V. M., & Nelavelli, S. "Edge–Cloud Continuums for Latency-Sensitive Tasks." International Journal of AI, BigData, Computational and Management Studies 5.4 (2024): 189-201.
53. Arigela, A. K., Brahmareddy, A., Sreenivas, T. S., Selvan, M. P., Venu, N., & Lal, D. K. "Optimizing Energy Efficiency and Latency in IoT Devices Through AI-Based Adaptive Protocols in Fog-Edge Computing Environments." Congress on Smart Computing Technologies. Singapore: Springer Nature Singapore, (2024).
54. Nadella, V. M. "Al-Native 6G Network Management." American International Journal of Computer Science and Technology 6.1 (2024): 23-37.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Panchali, H., kavirayani, U. M., Mylavarapu, K. B., Pilli, J., Jannu, P. K. & Mohammad, J. A. “Review of Secure Communication Systems for Cyber-Physical Systems and Industrial IoT” *Sarcouncil Journal of Engineering and Computer Sciences* 4.6 (2025): pp 349-362.

Publisher: SARC Publisher