Computer Science, Engineering and Technology
Vol: 1(1), March 2023
REST Publisher; ISSN: 2583-9179 (Online)
Website: https://restpublisher.com/journals/cset/
DOI: https://doi.org/10.46632/cset/1/1/19

Integrating IoT and Control Systems for Advanced Industrial Applications

***S. Gobinath, M. Chelliah, S. Suba, S. Priyadharshini**

Mahendra Engineering College, Namakkal, Tamil Nadu, India.
*Corresponding Author Email: gobinaths@mahendra.info

Abstract: *The integration of the Internet of Things (IoT) with control systems is transforming industrial applications by enabling automation, real-time monitoring, and intelligent decision-making. This study explores key enabling technologies such as wireless sensor networks, edge computing, and cloud-based control architectures. IoT-driven control systems enhance efficiency, reliability, and flexibility in industrial processes. The paper examines predictive maintenance, fault detection, and optimized resource utilization through IoT integration. Security challenges and solutions for ensuring robust industrial automation are discussed. Interoperability between IoT platforms and traditional control systems is explored. The study emphasizes scalable and resilient architectures for future industrial automation. Emerging trends such as digital twins and blockchain for secure IoT operations are analysed. Standardization efforts and regulatory considerations are reviewed. The findings demonstrate IoT's potential in revolutionizing industrial automation.*

Keywords: *Internet of Things, control systems, long short-term memory, Supervisory Control and Data Acquisition (SCADA) systems.*

1. INTRODUCTION

The way people view and interact with the world around us is changing due to the IoT, a technological revolution. This rapidly evolving field of information technology is transforming daily life by connecting an ever-growing number of systems and gadgets to the global network. They range from basic household gadgets like humidity sensors or thermometers to sophisticated industrial monitoring and control systems. Every aspect of life is impacted by the IoT, which presents both new possibilities and difficulties. The number of household gadgets having IoT capabilities has been steadily rising in recent years. An increasingly popular idea is the ”smart home,” in which every component—from the heating and lighting to the kitchen facilities and security systems—is linked into a single, cohesive network that allows for remote control and observation. This is just the beginning, though, as the IoT has enormous possibilities in a variety of economic sectors, including industry [1], transportation [2], medical services, and agriculture [3,4]. A key enabling technology of Industry [5], which includes the use of IoT in the industry, is the Industrial IoT (IIoT). In particular, the IIoT is used to link equipment and gadgets in industrial settings, with an emphasis on machine-to-machine interaction; any malfunction could result in high-risk losses, and IIoT data collection is significantly more extensive than IoT data collection [6]. Additionally, IIoT is seen as an analogous notion [7]. The conventional organisational frameworks are being altered by IIoT technologies, which are now offering more scalable systems with seamless data interchange [8]. This means that communications, software, and hardware must be arranged and dispersed according to functional architectures, which are the focus of study for the IIoT paradigms. For instance, the Platform Industrie 4.0 presented a three-dimensional map in 2015 called the Standard Architectural prototype for Industries. Similar to this, IoT-oriented designs are separated into tiers or layers that use IoT technology to share data. Numerous recent works examine current architectures and suggest novel ones. However, it is important to note two disadvantages in this context. In order to remedy the shortcomings of earlier architectures, new approaches and structures are created, which leads to a number of recommendations that once more produce diversity and misinterpretation [9]. This creates a paradox. However, these systems' level of abstraction and complexity works against their actual industrial use. ICSs are divided into two major categories. PLCs, detectors, actuators and other industrial machinery, resources, methods, and events are all monitored and managed by the hardware and software that make up the Operational Technology (OT) network. Conversely, workplaces, databases, and other traditional information-manipulation devices are part of the traditional IT network. The OT and IT networks were initially split up. However, both networks have been linked to enable process digitisation, creating significant susceptibility surfaces as a result of the so-called IT/OT Convergence. In the context of Cyber-Physical Systems (CPSs), which also include ICSs, the traditional CIA triad—Availability, Integrity, and Confidentiality—is viewed as being inverted, with Availability, Integrity, and

Confidentiality being ranked in order of significance. In this situation, dependability becomes the most important requirement since, in contrast to IT systems, where data confidentiality is the primary concern, availability is essential for an ICS because it can ensure fault tolerance and human safety. For example, data availability (e.g., core temperature) is more significant than secrecy in a nuclear plant setting [10]. One of the key elements of the digital data economy is the IoT. For instance, an IoT system's significance extends beyond the initial automation scenario that was envisioned. This is due to the fact that an IoT machine's wisdom is an additional value. The IoT database is sensors. Furthermore, industrial automation will be made possible by the cooperation of IoT sensors and actuators. Lastly, the data analysis of the sensors and actuators would eventually yield insightful information about the company. Material and nanotechnological advancements propelled sensor technology forward at previously unheard-of speeds, improving accuracy, lowering size and cost, and enabling the measurement or tracking of earlier unattainable artefacts. However, sensor technology is developing so quickly and efficiently that, within a year, a trillion of additional sensors will be installed. A sensor would be better described as a transducer. As a result, a particular physical effect is converted by the transducer into an electric momentum that controls a sensor's assessment. For other parts of the gadget, a microphone converts energy from vibrations (image wavelengths) into electrical power that corresponds to the source sound. Sensors are crucial to the creation of physical information. Sensors have been utilised in various fields in the past, but a computer is needed to access data via a computer network. Sensors are directly connected to the IoT network, much like computers. As machines are less sensitive to the flow of data than people, this concept has raised concerns.

2. LITERATURE REVIEW

Tucker., have described that another IoT use in smart factories is maintenance planning, which aims to minimise unscheduled downtime by anticipating possible equipment failures in machineries along with manufacturing equipment prior to happen. In smart factories, factory managers can use IoT to forecast possible equipment breakdowns and give maintenance schedules while minimising downtime by analysing data from sensors implanted in machinery [11]. Ashima et al., have stated that applications for IoT include asset tracking, inventory management, and energy management. Real-time manufacturing process tracking, assessment, and control are made possible by smart factories, which use IoT devices to establish an automated and networked environment [12]. According to Fernandez et al., to enhance blockchain usage in smart manufacturing processes, the incorporation of blockchain with the future cybersecure industries in relation to the industry 4.0 idea is investigated [13]. Durana et al., have conducted research on the IoT and arterial intelligence for sustainable automated manufacturing to develop Cyber-Physical production systems [14]. Xu et al., have stated that the IoT for manufacturing is being researched to improve the efficiency of smart factory technologies in the complex part production process [15]. Kovacova et al., have proposed that in order to develop assistance with decisions algorithms for automated factories that use the IoT, big data analysis for sustainable production is being researched [16]. According to Grabowska., to increase the productivity of part production, smart factories are being researched in the era of industry [17]. Kamble et al., have described that to boost the productivity of component production and create possibilities for the IoT in advanced manufacturing, Industry 4.0's smart manufacturing framework is being researched [18]. Zou et al., have proposed an additional hunting solution for an IT context is suggested. In order to identify APT techniques using synthesised analysis and data correlation, it was installed in an Ubuntu virtual machine. Logs, file configurations, and previously observed APT tactics are used as inputs by the software to detect APT tactics. A sorted list of APT tactics is then produced based on completeness. A different technique for detecting intrusions in industrial networks, known as spatiotemporal association analysis, was employed in an ICS. Feature mining and historical attack retrieval techniques between APT attack features were its main areas of research. The proposal identified anomalous APT attacks using a multi-feature SVM classification recognition technique. However, the solution doesn't specifically identify which of the numerous APT groups is launching the attack or go into the method employed in the attack that was discovered [19,20]. Baidhani et al., have provided a basic analogue version of a resilient nonlinear current mode control method for a pulse-width modulated DC-DC Cuk converter. The reduced-state sliding-mode current control technique serves as the foundation for the control scheme [21]. In contrast to traditional sliding-mode current controllers, Zhang et al., have suggested that controller doesn't need an output capacitor current sensor or two proportional-integral compensators. As a result, the actual implementation's expenses and complexity are reduced without compromising control performance. A production change optimisation model for a non-linear supply chain system in emergency situations is presented in the sixth paper [22]. There are manufacturers, suppliers, and retailers in a three-tiered, single-chain, nonlinear supply chain system. The supply chain system's optimisation model under unforeseen circumstances is created and utilised using the adaptive enhanced sliding mode controller. Numerical simulation experiments are used to confirm the efficiency of the suggested approach. Choi et al., have collected and examined datasets for ICS security research that same year, including various comparison tables to help determine which dataset was best for a given case study. The comparison was based on the assault vector technique. Some current datasets are purposefully ignored since they are not often utilised or do not contain attacks. Nevertheless, the latter may be helpful to investigate the behaviour of the ICS environment, even if it is not appropriate for anomaly detection tasks. Additionally, DEFCON23, one of the datasets that was presented, is no longer accessible [23]. Ani et al., have stated that the primary obstacles and the outcomes of a focus group with security specialists to identify pertinent design considerations and guidelines are highlighted in the authors' comprehensive survey with recommendations and best practices to assist in the construction of an ICS testbed

[24]. The same authors published in the same years, offering intriguing rules for every ICS layer as well as a list of qualities to take into account while describing the goals, architecture, and evaluation procedure of a testbed. These studies are fascinating and provide a thorough understanding of the process of planning and assessing a testbed, they ignore datasets and IDSs, their needs, and their connections.

3. RESEARCH METHODOLOGY

The integration of IoT with industrial control systems is analyzed by exploring key enabling technologies, security challenges, and emerging trends. AI-driven adaptive control is examined to enhance automation and decision-making. Interoperability between IoT platforms and traditional control systems is assessed for seamless integration. The role of digital twins and blockchain in secure industrial automation is investigated. Security vulnerabilities and mitigation strategies are analyzed to improve system resilience. Standardization efforts and regulatory frameworks are reviewed for compliance and scalability. Cloud-based and edge computing architectures are studied for optimized resource utilization. Predictive maintenance and fault detection techniques are explored for operational efficiency. The impact of IoT-driven control systems on industrial reliability and flexibility is evaluated. Existing research and case studies are examined to identify best practices. A conceptual framework is proposed for scalable and resilient IoT integration.

4. IOT ARCHITECTURES FOR INDUSTRIAL CONTROL SYSTEMS

The integration of IoT with industrial control systems relies on structured architectures that ensure efficient data flow, real-time monitoring, and automation. A widely adopted framework is the three-tier IoT architecture, comprising the perception, network, and application layers. The perception layer includes sensors, actuators, and RFID systems that collect real-time industrial data. The network layer ensures seamless communication using technologies like industrial Ethernet, Wireless Sensor Networks (WSNs), and emerging Low-Power Wide-Area Networks (LPWAN) such as LoRa and NB-IoT. The application layer processes this data through cloud computing, edge computing, and AI-driven analytics for decision-making. Cloud-based architectures enable centralized control and historical data analysis, while edge computing enhances low-latency decision-making by processing data closer to the industrial equipment. Furthermore, IIoT relies on communication protocols such as OPC UA (for interoperability), MQTT (for lightweight IoT messaging), CoAP (for constrained devices), and Modbus/TCP (for legacy system integration). These frameworks facilitate the scalability and adaptability of IoT-driven industrial automation systems, ensuring seamless integration with existing industrial infrastructures. The IoT architecture is illustrated in figure 1.

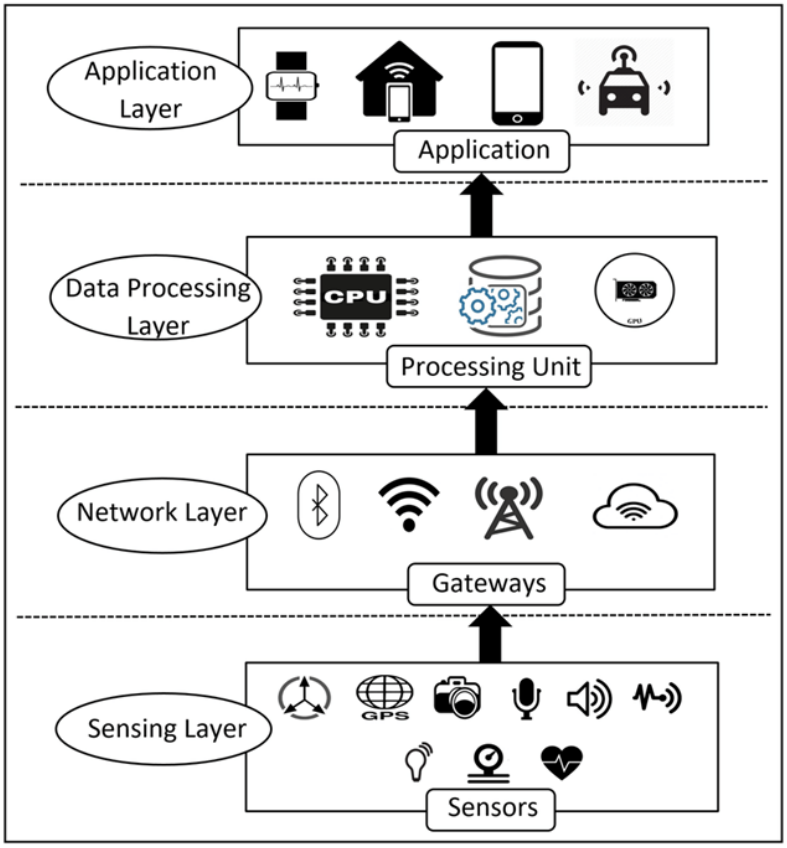

FIGURE 1. IoT architecture

5. ADAPTIVE CONTROL STRATEGIES USING AI AND MACHINE LEARNING

AI-driven adaptive control mechanisms enhance industrial automation by enabling dynamic process optimization, predictive maintenance, and intelligent decision-making. Reinforcement learning models are increasingly utilized in industrial control systems to dynamically adjust setpoints based on real-time sensor data, ensuring optimal performance in varying conditions. Predictive maintenance, a key IoT application, utilizes machine learning techniques such as random forests and Long Short-Term Memory (LSTM) networks to analyze temperature, vibration, and operational data for detecting early signs of equipment failures. Additionally, digital twins—virtual representations of physical systems—leverage real-time IoT sensor data to simulate and optimize industrial processes. Platforms such as Siemens MindSphere and GE Digital's Predix demonstrate the potential of digital twins in reducing downtime and improving asset management. By integrating AI-driven anomaly detection algorithms, industries can enhance operational efficiency while minimizing unplanned downtime in smart manufacturing environments.

6. IOT-DRIVEN PROCESS OPTIMIZATION IN INDUSTRIAL AUTOMATION

The deployment of IoT in industrial automation significantly improves process optimization, energy efficiency, and real-time monitoring. In smart manufacturing, AI-driven predictive quality control ensures defect detection in production lines before defects escalate into major quality issues. Automated material handling systems, integrated with IoT, enhance logistics efficiency using connected Automated Guided Vehicles (AGVs) that navigate industrial floors autonomously. Additionally, IoT-based energy management systems contribute to sustainable industrial operations by dynamically balancing power consumption through smart grid integration and AI-based load forecasting. Edge computing plays a key role in optimizing HVAC systems in industrial plants, reducing energy consumption by dynamically adjusting temperature and ventilation based on sensor data. The fusion of IoT, AI, and edge analytics thus enables industries to achieve higher productivity, reduced operational costs, and enhanced sustainability.

7. INTEROPERABILITY BETWEEN IOT AND TRADITIONAL ICS

The integration of IoT with traditional Industrial Control Systems (ICS) presents significant challenges due to differences in communication protocols, data formats, and real-time processing requirements. Traditional ICS, including Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), and Distributed Control Systems (DCS), were originally designed as isolated, deterministic systems with minimal connectivity to external networks. In contrast, IoT-based systems rely on open communication protocols, cloud computing, and real-time analytics, creating compatibility issues when merging the two technologies. Achieving seamless interoperability between IoT and ICS requires protocol conversion, middleware solutions, and standardized frameworks to ensure reliable and secure data exchange. Key Aspects of IoT-ICS Interoperability

1. Communication Protocol Bridging
2. Edge Computing for Real-Time Processing
3. Middleware for Data Standardization
4. Cybersecurity Considerations
5. Legacy System Retrofitting

8. LATENCY ANALYSIS IN IOT-INTEGRATED INDUSTRIAL CONTROL SYSTEMS

One of the major challenges in integrating IoT with industrial control systems (ICS) is the end-to-end latency, which affects real-time decision-making. The total system delay can be broken down as follows:

$$T_{\text{total}} = T_{\text{sense}} + T_{\text{network}} + T_{\text{process}} + T_{\text{actuate}}$$

where:

- T_{sense} = Time taken by sensors to capture data.
- T_{network} = Delay due to transmission over industrial networks.
- T_{process} = Processing delay at the edge/cloud server for analytics.
- T_{actuate} = Time for control signals to reach actuators.

To model network delay, let us assume an M/M/1 queuing model, where sensor data packets arrive at rate λ

and are processed at rate μ. The average queuing delay is given by:

$$T_{\text{network}} = \frac{1}{\mu - \lambda}$$

where:

- λ = Packet arrival rate (packets per second).
- μ = Packet processing rate.

For real-time control applications, it is crucial to minimise T_{network} by reducing network congestion. Edge computing significantly reduces T_{process} since computation happens closer to the industrial site instead of relying on cloud services. The improvement in latency is given by:

$$\Delta T = T_{\text{cloud}} + T_{\text{edge}}$$

where ΔT represents the latency reduction achieved by edge computing.

9. PREDICTIVE MAINTENANCE MODEL USING MACHINE LEARNING

IoT-based predictive maintenance relies on statistical modelling of failure probabilities. A widely used method is the Weibull failure distribution, given by:

$$P(T \leq t) = 1 - e^{-(t/\eta)^{\beta}}$$

where:

- $P(T \leq t)$ = Probability of failure before time t.
- η = Characteristic life parameter.
- β = Shape factor (indicates failure rate trends).

For industrial machinery, sensor-based degradation models can be expressed as:

$$D(t) = D_0 + \alpha t + \epsilon$$

where:

- $D(t)$ = Degradation at time t.
- D_0 = Initial degradation level.
- α = Degradation rate (can be estimated using ML models).
- ϵ = Random noise.

10. ENERGY OPTIMISATION IN IOT-DRIVEN SMART FACTORIES

Industrial IoT (IIoT) plays a key role in optimising energy consumption by dynamically managing machine power usage. The total energy consumption in an industrial plant can be modelled as:

$$E_{\text{total}} = \sum_{i=1}^{N} P_i \cdot t_i$$

where:

- P_i = Power consumption of machine i.
- t_i = Operational time of machine i.
- N = Total number of machines.

The goal is to minimise energy consumption while ensuring operational efficiency. The optimisation problem can be formulated as:

$$\min \sum_{i=1}^{N} P_i \quad \text{subject to} \quad \sum_{i=1}^{N} P_i \leq P_{\text{max}}$$

where P_{max} is the total allowable power consumption.

Using Lagrange multipliers, the Lagrangian function becomes:

$$\mathcal{L}(P, \lambda) = \sum_{i=1}^{N} P_i + \lambda \left(P_{\text{max}} - \sum_{i=1}^{N} P_i \right)$$

11. REAL-TIME IOT-ICS INTEROPERABILITY MODEL

Interoperability between IoT platforms and legacy ICS is crucial for smooth industrial automation. Middleware solutions, such as IoT gateways, enable protocol translation between modern IoT devices and traditional PLCs/SCADA systems. Consider an IoT-enabled industrial process where a sensor updates data at rate λ per second, and a legacy PLC can process commands at rate μ. If $\lambda > \mu$, a bottleneck occurs. The probability of a backlog forming in the system follows a Poisson queuing model:

$$P(n) = \frac{(\lambda/\mu)^n e^{-\lambda/\mu}}{n!}$$

where:

- $P(n)$ = Probability of n unprocessed sensor messages in the queue.

For seamless integration, industrial IoT middleware must dynamically buffer and prioritise sensor updates, using FIFO (First-In-First-Out) or priority-based scheduling. The queueing time can be estimated as:

$$T_{\text{queue}} = \frac{\lambda}{(\mu - \lambda)\lambda}$$

By optimising T_{queue}, industrial systems ensure low-latency, real-time control even when integrating legacy ICS with IoT.

12. CONCLUSION

The integration of IoT with traditional ICS enhances real-time monitoring, predictive maintenance, and adaptive control, driving industrial automation toward greater efficiency and scalability. Key technologies such as wireless sensor networks, edge computing, and AI-driven decision-making enable seamless data processing and automation. However, interoperability challenges arise due to differences in communication protocols, data formats, and real-time processing requirements. Middleware solutions and protocol converters help bridge this gap, ensuring smooth integration with legacy systems. Cybersecurity threats associated with IT/OT convergence necessitate robust security measures, including blockchain authentication and encryption. Additionally, digital twins and blockchain improve system modelling and secure data management. Standardization efforts and retrofitting strategies play a vital role in facilitating IoT-ICS adoption. Optimized resource utilization and AI-driven automation further enhance industrial performance. Cloud and edge computing frameworks ensure low-latency decision-making and improved efficiency. Scalable and resilient architectures enable future-ready industrial automation. Interoperability and security remain key challenges for seamless IoT integration. Intelligent control algorithms optimize system operations dynamically. Future research should focus on developing unified standards and AI-driven optimizations to maximize automation potential. IoT-driven ICS revolutionizes industry by minimizing downtime and enhancing operational flexibility.

REFERENCES

[1]. Hu, Y.; Jia, Q.; Yao, Y.; Lee, Y.; Lee, M.; Wang, C.; Zhou, X.; Xie, R.; Yu, F.R. (2024). Industrial Internet of Things Intelligence Empowering Smart Manufacturing: A Literature Review. IEEE Internet Things J. 11, 19143–19167.

[2]. Agarwal, V.; Sharma, S. (2020). IoT based smart transport management system. In Proceedings of the International Conference on Advanced Informatics for Computing Research, Gurugram, India, 26–27 December 2020; Springer: Berlin/Heidelberg, Germany; pp. 207–216.

[3]. Ioannides, M.G.; Stamelos, A.P.; Papazis, S.A.; Stamataki, E.E.; Stamatakis, M.E. (2024). Internet of Things-Based Control of Induction Machines: Specifics of Electric Drives and Wind Energy Conversion Systems. Energies 17, 645.

[4]. Zeng, F.; Pang, C.; Tang, H. (2024). Sensors on Internet of Things Systems for the Sustainable Development of Smart Cities: A Systematic Literature Review. Sensors 24, 2074.

[5]. Mrabet, H.; Alhomoud, A.; Jemai, A.; Trentesaux, D. (2022). A Secured Industrial Internet-of-Things Architecture Based on Blockchain Technology and Machine Learning for Sensor Access Control Systems in Smart Manufacturing. Appl. Sci. 12, 4641.

[6]. Babayigit, B.; Abubaker, M. (2023). Industrial Internet of Things: A Review of Improvements Over Traditional SCADA Systems for Industrial Automation. IEEE Syst. J. 18, 120–133.

[7]. Nakagawa, E.Y.; Antonino, P.O.; Schnicke, F.; Capilla, R.; Kuhn, T.; Liggesmeyer, P. (2021). Industry 4.0 reference architectures: State of the art and future trends. Comput. Ind. Eng. 156, 107241.

[8]. Ladegourdie, M.; Kua, J. (2022). Performance Analysis of OPC UA for Industrial Interoperability towards Industry 4.0. Internet Things 3, 507–525.

[9]. Bader, S.R.; Maleshkova, M.; Lohmann, S. (2019). Structuring reference architectures for the industrial Internet of Things. Future Internet 11, 151.

[10]. Filkins, B.; Wylie, D.; Dely, A. J. (2019). SANS 2019 State of OT / ICS Cybersecurity Survey. SANS Institute, no. June.
[11]. Tucker, G. (2021). Sustainable product lifecycle management, industrial big data, and internet of things sensing networks in cyber-physical system-based smart factories. J. Self Govern. Manag. Econ. 9, 9–19.
[12]. Ashima, R.; Haleem, A.; Bahl, S.; Javaid, M.; Mahla, S.K.; Singh, S. (2021). Automation and manufacturing of smart materials in Additive Manufacturing technologies using Internet of Things towards the adoption of Industry 4.0. Mater. Today: Proc. 45, 5081–5088.
[13]. Fernandez-Carames, T.M.; Fraga-Lamas, P. (2019). A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. IEEE Access 7, 45201–45218.
[14]. Durana, P.; Perkins, N.; Valaskova, K. (2021). Artificial intelligence data-driven internet of things systems, real-time advanced analytics, and cyber-physical production networks in sustainable smart manufacturing. Econ. Manag. Financ. Mark. 16, 20–30.
[15]. Xu, X.; Han, M.; Nagarajan, S.M.; Anandhan, P. (2020). Industrial Internet of Things for smart manufacturing applications using hierarchical trustful resource assignment. Comput. Commun. 160, 423–430.
[16]. Kovacova, M.; Lewis, E. (2021). Smart factory performance, cognitive automation, and industrial big data analytics in sustainable manufacturing internet of things. J. Self Govern. Manag. Econ. 9, 9–21.
[17]. Grabowska, S. (2020). Smart factories in the age of Industry 4.0. Manag. Syst. Prod. Eng. 28, 90–96.
[18]. Kamble, S.S.; Gunasekaran, A.; Ghadge, A.; Raut, R. (2020). A performance measurement system for industry 4.0 enabled smart manufacturing system in SMMEs-A review and empirical investigation. Int. J. Prod. Econ. 229, 107853.
[19]. Zou, Q.; Singhal, A.; Sun, X.; Liu, P. (2020). Automatic recognition of advanced persistent threat tactics for enterprise security. In Proceedings of the 6th International Workshop on Security and Privacy Analytics, pp. 43–52.
[20]. Wang, X.; Liu, Q.; Pan, Z.; Pang, G. (2020). APT attack detection algorithm based on spatio-temporal association analysis in industrial network. Journal of Ambient Intelligence and Humanized Comp., pp. 1–10.
[21]. Al-Baidhani, H.; Kazimierczuk, M.K. (2023). Simplified Nonlinear Current-Mode Control of DC-DC Cuk Converter for Low-Cost Industrial Applications. Sensors 23, 1462.
[22]. Zhang, J.; Wu, Y.; Li, Q. (2023). Production Change Optimization Model of Nonlinear Supply Chain System under Emergencies. Sensors 23, 3718.
[23]. Choi, S.; Yun, J. H.; Kim, S. K. (2019). A comparison of ICS datasets for security research based on attack paths. Springer International Publishing, vol. 11260 LNCS. [Online]. Available: http://dx.doi.org/10.1007/978-3-030-05849-4_12
[24]. Ani, U. P. D.; Watson, J. M.; Green, B.; Craggs, B.; Nurse, J. R. (2020). Design considerations for building credible security testbeds: Perspectives from industrial control system use cases. Journal of Cyber Security Technology, pp. 1–49.

