ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may351

A New Era for Cyber-Physical Systems: Optimal Integration of AI, ML and Digital Twins

Manvendra Singh[1)] ; Amogh Ansh [2)]; Ananya Jain [2)];
Richa Dubey [2)]; Dr. Karthikeyan B [2)]

[1]School of Computer Science & Engineering (SCOPE)
[2]School of Electronics Engineering (SENSE),

Vellore Institute of Technology Vellore, India

Publication Date: 2025/05/16

Abstract: In an era where the interconnection between the digital and physical realms becomes increasingly complex, the security of cyber-physical systems (CPS) emerges as a crucial challenge. This paper undertakes a comprehensive analysis of journal articles on CPS security, examining the diverse methodologies proposed to fortify these systems against emerging threats. Emphasizing the role of advanced technologies such as artificial intelligence (AI), machine learning (ML), and blockchain, our study showcases their pivotal contributions to enhancing CPS resilience. Central to our analysis is the innovative integration of AI and ML with Digital Twins, a strategy that stands out for its ability to concurrently bolster security and operational efficacy. This study gives further detail a novel application of AI-enhanced Digital Twins, outlining a methodology for its practical implementation. Through this investigation, the aim is to enrich the scholarly dialogue on CPS security, advocating for the strategic use of technological advancements to create smarter, safer, and more efficient systems.

Keywords*: Cyber-Physical Systems (CPS), Artificial Intelligence (AI), Machine Learning (ML), Blockchain Technology, Digital Twins, CPS Security, AI-enhanced Security, Operational Efficiency, Technological Integration.*

How to Cite: Manvendra Singh; Amogh Ansh; Ananya Jain; Richa Dubey; Dr. Karthikeyan B (2025) A New Era for Cyber-Physical Systems: Optimal Integration of AI, ML and Digital Twins. *International Journal of Innovative Science and Research Technology*, 10(5), 204-210. https://doi.org/10.38124/IJISRT/25may351

I. INTRODUCTION

In the rapidly evolving digital age, the security of Cyber Physical Systems (CPS) stands as a critical concern that bridges the physical and cyber worlds. The integration of artificial intelligence (AI), machine learning (ML), and blockchain technology within these systems offers promising solutions to the multifaceted security challenges they face. This paper presents a comprehensive analysis of 15 journal articles, each contributing unique insights into methodologies for enhancing the security and efficiency of CPS. The selected articles span across various applications and technologies including blockchain for medical systems, AI and SDN (Software-Defined Networking) for IoT networks, safety and security risk management, and the innovative use of Digital Twins integrated with AI and ML for smart manufacturing and health monitoring.

Through a meticulous review, this research identifies the cutting-edge methodologies employed in current literature to address the vulnerabilities of CPS. It delves into the synergistic potential of integrating advanced technologies such as AI, ML, and blockchain to create resilient, efficient, and secure systems. The methodologies discussed range from blockchain-based frameworks for medical data privacy, AI-empowered security architectures for IoT, to Digital Twins augmented with AI for industrial 4.0 applications.

The analysis underscores a notable trend towards the harmonization of security and efficiency within CPS, highlighting the optimal integration of AI and ML technologies with Digital Twins as a particularly promising approach. This integration not only fortifies the security of CPS but also significantly enhances their operational efficiency and decision-making processes. The research culminates in a detailed discussion of an in-depth application of an AI-enhanced Digital Twin, proposing a step-by-step methodology for its implementation. This approach showcases a scalable, flexible, and intelligent solution to the challenges faced by modern CPS, marking a significant advancement towards smarter, autonomous industrial processes.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may351

By comparing the methodologies of the reviewed articles, this paper sheds light on the current state of research in the domain of Cyber Physical Security but also sets the stage for future explorations into the integration of emerging technologies for the advancement of CPS security and efficiency.

II. ANALYSIS OF PREVIOUS WORKS

[1] The paper presents an innovative framework to enhance the security and privacy of Medical Cyber-Physical Systems (MCPS) through blockchain technology. The authors investigate the security vulnerabilities present in medical cyber- physical systems and proposes a blockchain-based framework to address these challenges.

The main question revolves around how blockchain technology can be leveraged to provide a secure, private, decentralized, and efficient mechanism for managing medical data and ensuring the integrity and privacy of this information in a medical cyber-physical system. It distinguishes itself by focusing on a decentralized and privacy- preserving approach, contrasting with more centralized solutions present in existing literature.

The study concludes that the integration of blockchain technology into MCPS can significantly enhance the security, reliability, and privacy of medical data. The proposed framework not only addresses current security challenges but also provides a scalable and efficient solution for the management of medical cyber-physical systems.
While the proposed framework offers substantial improvements in security and privacy, the paper acknowledges the need for further research in several areas, including the scalability of blockchain solutions in larger MCPS environments, the integration of advanced cryptographic techniques for enhanced security, and the exploration of additional use cases within the healthcare sector.

[2] The paper addresses the critical need for robust security and energy efficiency in the IoT networks of cyber-physical systems, leveraging the synergistic integration of AI, blockchain, and Software-Defined Networking (SDN).

The methodology involves designing a security architecture that combines blockchain's decentralized security, SDN's flexible network management, and AI's predictive capabilities to detect and mitigate threats dynamically.

The study concludes that integrating AI, blockchain, and SDN presents a viable and effective strategy to fortify IoT networks against security threats while optimizing energy consumption. The proposed framework not only enhances the security posture of IoT networks but also contributes to the sustainability and resilience of cyber-physical systems.

The paper identifies areas for future research, including further exploration of the scalability of the proposed framework, the integration of more advanced AI algorithms for threat detection, and the development of more sophisticated consensus mechanisms for blockchain that balance security with energy efficiency.

[3] This research centres on the vulnerabilities of CPS in the modern era of smart living, questioning how multi-factor authentication and other robust security solutions can ensure the safety and integrity of CPS across various domains including smart homes, cities, and medical systems. It builds on prior work by exploring the unique challenges of CPS, differentiating itself through a comprehensive analysis of CPS's vulnerabilities and offering a survey of potential solutions that address these challenges in innovative ways.

The research employs a combination of literature review and analysis of existing technologies to present an overview of the current state of CPS security. It evaluates various strategies and solutions that have been proposed or implemented to enhance CPS security and identifies areas where further research is needed. The study concludes that the security of CPS is a multifaceted problem that requires a concerted effort from researchers, technologists, and policymakers.

It emphasizes the need for efficient, scalable, and reliable security mechanisms that can adapt to the evolving landscape of cyber threats facing CPS. The research highlights several areas for future investigation, including the scalability of security solutions, the integration of advanced cryptographic methods.

[4] This research builds on previous studies by focusing on the intersection of AI and CPS specifically within the construction sector, a niche that is sparsely explored. It extends existing knowledge on CPS and AI by applying their advantages to construction industry challenges, offering a novel perspective on intelligent system design for building environments.

The methodology involves designing a CPS- based system for measuring and controlling indoor environments in intelligent buildings. The system comprises four modules: detection, control, execution, and communication, utilizing multi-agent systems (MAS) to mimic human neuron connections for autonomous information access.

The integration of CPS and AI in the construction industry is viable and offers substantial benefits, such as improved indoor environment management through intelligent temperature control. The system's robustness and effectiveness in detecting and responding to environmental changes affirm the potential of AI and CPS to revolutionize the intelligent construction industry.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may351

While promising, the study acknowledges the need for further exploration, particularly in the system's responsiveness to broader environmental factors beyond temperature. Future research directions include enhancing system generalization and conducting comparative analyses to underscore the algorithm's advantages over existing solutions.

[5] The study introduces DEEP-FEL, a framework designed to address the privacy and security concerns in healthcare cyber-physical systems by leveraging decentralized federated learning.

The paper situates DEEP-FEL within the broader context of existing research on federated learning, edge computing, and privacy-preserving technologies. It contributes to the literature by proposing a novel integration that specifically addresses the unique security and efficiency needs of healthcare systems, emphasizing the importance of decentralized, efficient, and privacy-enhanced processing in this sensitive domain.

DEEP-FEL is designed as a hierarchical system that combines federated learning with edge computing to facilitate efficient and secure data processing close to the data sources. It incorporates differential privacy mechanisms to enhance data privacy. The research method involves the development of a theoretical framework, followed by an experimental evaluation using medical datasets to demonstrate the efficacy of DEEP-FEL in improving privacy and efficiency in healthcare applications.

The study concludes that DEEP-FEL effectively enhances the privacy and security of medical cyber- physical systems by leveraging federated learning and edge computing.

[6] This research positions itself within the discourse on digital agriculture, distinguishing its approach by focusing on the responsibilisation aspect. It aims to understand the relationships between the social, cyber, and physical components of agriculture and rural areas and outlines conditions for successful digital transformation, emphasizing design, access to technology, and navigating system complexity.

The paper introduces a socio-cyber-physical system framework that facilitates insight into the interactions among the social, cyber, and physical realms. This framework is used to explore digital transformation's moral responsibilities and accountability, focusing on the concept of responsibilisation.

The conclusion underscores the necessity of understanding the comprehensive effects of digital transformation in agriculture and rural areas. It emphasizes that digital transformation should not only focus on technological advancements but also on the socio-economic conditions that it influences. The framework proposed aids in the problematisation of digital transformation, facilitating a better grasp of moral responsibilities.

This work identifies the need for further research in several areas, including the scalability of digital solutions in agriculture, the integration of advanced technologies, and the development of more inclusive strategies that consider the socio-economic disparities in rural areas.

[7] This research contributes to the existing literature by proposing a novel approach that combines safety and security risk management practices. Unlike traditional methods that treat safety and security independently, this work advocates for a harmonized analysis to better reflect the intertwined nature of risks in CPS.

The methodology involves the development of Attack Route Models (ARM) to identify the root causes of cyber threats and their potential impacts on CPS. Additionally, it introduces a Cyber Security Prevention Route (CSPR) alongside the traditional Physical Safety Prevention Route (PSPR) to assess preventive measures. The integration of Safety Critical Variable Analysis (SCVA) with the bowtie method enables a comprehensive evaluation of both safety and security risks.

The study concludes that a harmonized approach to safety and security risk management significantly enhances the resilience of CPS against both physical and cyber threats. By systematically analysing and addressing these risks together, organizations can better protect their CPS infrastructure from diverse types of incidents.

The paper suggests further research in areas such as the scalability of the proposed framework, the effectiveness of different preventive measures in various CPS contexts, and the exploration of more sophisticated models to predict and mitigate combined safety and security risks.

[8]The study explores the incorporation of Human Digital Twins (HDT) into Human-Cyber- Physical Systems (HCPS), highlighting the transition from traditional human-physical systems to more integrated systems where humans, machines, and cyber systems interact seamlessly.

The proposed framework for HDT-driven HCPS consists of three main components: humans, the physical system, and the cyber system, with HDT acting as a bridge connecting these elements. The framework emphasizes the central role of humans in decision-making, interaction, and control, supported by real-time data flow between the physical and cyber systems.

The study identifies several key technologies crucial for enabling HDT-driven HCPS, including the Internet of Things (IoT), sensing, artificial intelligence (AI), cloud computing, and robotics. It details how these technologies facilitate sensing for humans and physical systems, computing and analysis for modelling and simulation, and control mechanisms for effective interaction between humans and machines.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may351

The paper discusses potential challenges such as data privacy, the synchronization between cyber and physical components, and the need for collaborative development across technical, legal, and political domains.

[9] The study proposes a small object detection model for digital twins (SOD-DT) that integrates a hybrid deep neural network model combining MobileNetv2, YOLOv4, and Openpose. This model is designed to accurately identify the real-time status of equipment, products, and operators.

A hybrid neural network architecture is constructed for feature extraction and object detection. The model leverages depth wise separable convolutions from MobileNetv2 integrated into YOLOv4 (referred to as YOLOv4-M2) for efficient feature extraction and small object detection. Additionally, the Openpose network, enhanced by features from YOLOv4-M2, is used for accurate long-distance human posture recognition.

The proposed SOD-DT model demonstrates superior performance in detecting small objects within complex manufacturing environments, as validated through experiments in various use cases. The model achieves higher detection accuracy and real-time performance compared to traditional methods, highlighting its potential to support the surveillance and optimization of equipment positioning, personnel distribution, and product trajectory in digital twins.

The research concludes that the integration of a hybrid deep learning model offers significant improvements in the detection of small objects for digital twins in smart manufacturing.

[10] The paper presents a multi-agent federated reinforcement learning (MA-FRL) algorithm that allows for secure and efficient incentive mechanisms. The methodology involves formulating the secure communication and data resource allocation problem as a Stackelberg game, modelling it as a partially observable Markov decision process, and then applying the MA-FRL algorithm to find efficient allocation policies.

The study concludes that the proposed MA-FRL algorithm can significantly improve the incentive mechanism in federated learning settings for ICPS by ensuring secure communication and efficient data resource allocation. The algorithm allows for a decentralized, privacy-preserving approach to incentivizing device participation, demonstrating superior performance compared to baseline approaches.

The paper suggests areas for future research, including the exploration of more advanced privacy- preserving techniques within the MA-FRL framework, addressing scalability issues as the number of devices increases, and extending the application of the proposed algorithm to other domains beyond healthcare and industrial systems.

[11] The study investigates how Artificial Intelligence (AI) can be integrated with the Internet of Things (IoT) and Cyber-Physical Systems (CPS) to create secure smart wearable computing solutions for health monitoring. It focuses on addressing security risks and ethical issues within IoT and CPS, particularly when every piece of data and device is connected and accessible on the network, raising concerns about data misuse and privacy breaches.

The paper proposes an AI-enabled IoT-CPS framework to enable doctors to diagnose diseases in patients using data gathered from wearable sensors. It details a novel approach where AI algorithms are developed to identify disorders such as Diabetes, Heart Disease, and Gait Disturbances among patients.

The experimental results demonstrate that the proposed AI-enabled IoT-CPS algorithm out performs existing algorithms in detecting patient diseases and fall events in elderly people.

[12]The authors introduce a structured threat modelling approach for ICPS, aiming to predict and analyse cyber risks to protect industrial assets from potential cyber-attacks. This methodology involves classifying ICPS assets based on their criticality, analysing cybersecurity vulnerabilities, threats, risks, impacts, and countermeasures.

The methodology leverages meta-data extracted from the VueOne tool to automatically generate software code and hardware configurations that can be directly deployed on ICPS assets to counteract potential cyber-attacks.

The proposed solution was implemented on a Festo test rig prototype production line, showcasing the practical applicability and effectiveness of the methodology in a real-world setting. The work is particularly significant in the era of smart manufacturing, where the integration of digital and physical systems heightens the cybersecurity challenges. By addressing these challenges proactively through advanced threat modelling and mitigation techniques, the study contributes valuable insights and tools for securing ICPS against a backdrop of evolving cyber threats.

This research advances the field of smart manufacturing cybersecurity by providing a detailed framework for threat modelling that is both innovative and applicable to current industrial practices.

[13]The paper addresses the challenge of detecting operational failures in CPS by monitoring sensor measurements and actuator states to identify abnormal operation statuses. It highlights the difficulties in building effective anomaly detection models due to the complex dynamics of CPS and unknown sensor noise.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may351

➢ *NSIBF Framework:*

- Neural System Identification: Utilizes a neural network to model CPS dynamics as a dynamical state-space model, capturing system behaviour over time.
- Bayesian Filtering for Anomaly Detection: Applies Bayesian filtering on the identified state- space model to estimate the likelihood of observed sensor measurements over time, enabling robust anomaly detection.

The approach involves training a neural network to identify system dynamics, followed by Bayesian filtering for real-time anomaly detection.

➢ *Experiments and Findings:*

- Conducted qualitative and quantitative experiments on synthetic and real-world CPS datasets.
- Demonstrated that NSIBF outperforms state-of-the-art time series anomaly detection methods, showing considerable improvements in detecting anomalies in CPS.

The method's ability to accurately detect anomalies in noisy sensor data presents a significant advancement for enhancing the security and reliability of CPS.

[14] The proposed framework utilizes a two-level ensemble approach for attack detection and attribution. At the first level, an ensemble deep representation-learning model combined with a decision tree is developed for detecting attacks in imbalanced ICS environments. At the second level, an ensemble deep neural network is designed for attack attribution, aiming to identify the nature and source of detected attacks with precision. This methodology is evaluated using real-world datasets in gas pipeline and water treatment systems.

➢ *Findings and Contributions*

- The framework demonstrates superior performance in detecting and attributing cyber- attacks within IoT-enabled CPS compared to existing approaches, offering a promising solution to the nuanced challenges of ICS security.
- The paper contributes a novel approach to integrating deep representation learning with ensemble learning for enhanced security in ICS, highlighting the importance of tailored security solutions for IoT-enabled CPS.

The study concludes that the proposed two-level ensemble framework significantly improves the security of IoT-enabled CPS by enabling more accurate detection and attribution of cyber-attacks. It calls for further research into refining this approach, exploring its scalability, and adapting it to various ICS contexts to ensure wide applicability and effectiveness.

[15] The paper discusses the transformation of the industrial sector towards full digitalization and integration, known as Industry 4.0, where Cyber- Physical Systems (CPS) play a crucial role.

Defined as a virtual representation of a physical asset enabled by data and simulators for real-time prediction, optimization, monitoring, controlling, and decision-making, Digital Twins embody the cyber-physical integration within Industry 4.0.

The adaptation of Digital Twin in Industry 4.0 is closely linked with recent advances in Information and Communication Technology (ICT), such as 5G, Edge, and Fog computing. These technologies provide the necessary communication link with low end-to-end latency, low jitter, and localization awareness essential for industrial services. AI, particularly through Machine Learning (ML) algorithms, plays a critical role in automating and enhancing Digital Twins by developing expertise in specific tasks and optimizing beyond human capability.

The integration of Digital Twins with computing and network infrastructure presents challenges such as effectively using real-time data streams, optimal allocation of computing resources, and building Digital Twins that benefit from heterogeneous RAT resources. AI agents are proposed as solutions to these challenges, leveraging ML algorithms to exploit existing data sources with context information at both the application and infrastructure levels.

The experiment involves predicting the next movements using real data from the Digital Twin and comparing the performance of different ML-based algorithms. The results highlight the potential benefits of integrating AI with Digital Twins for enhancing remote control operations.

In conclusion, the integration of Digital Twins with AI represents a significant advancement towards achieving smarter, autonomous industrial processes in Industry 4.0. AI agents, supported by ML algorithms, offer promising solutions to the challenges faced by Digital Twins in terms of automation, optimization, and smartification.

III. OPTIMAL CPS INTEGRATION

Among the reviewed methodologies, the integration of AI and ML technologies with Digital Twins for enhancing Cyber-Physical Systems (CPS) security and efficiency represents a particularly promising and cutting-edge approach. This approach facilitates real-time prediction, optimisation, monitoring, controlling, and decision-making in industrial processes, embodying the cyber-physical integration within Industry 4.0.

The combination of Digital Twins with AI and ML algorithms represents a holistic approach that not only addresses the cybersecurity aspects but also enhances operational efficiency and decision-making processes. AI and ML algorithms can process vast amounts of data generated by CPS, identifying patterns and anomalies that human operators might miss. As CPS become increasingly complex and integrated with emerging technologies like

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may351

IoT, 5G, and edge computing, the flexibility and scalability offered by Digital Twins, coupled with the advanced analytics of AI, ensure that security measures can evolve in tandem with new challenges and threats. The experimental results highlighted in the article demonstrate the potential benefits of integrating AI with Digital Twins, including enhancing remote control operations and optimising industrial processes beyond human capabilities.

IV. IN-DEPTH APPLICATION

Implementing an AI-enhanced Digital Twin for a specific CPS would involve several key steps:

- Develop a comprehensive Digital Twin of the physical system, accurately reflecting its components, operations, and data flows.
- Incorporate real-time data streams from the physical system into the Digital Twin, utilizing IoT sensors and devices for data collection.
- Employ ML algorithms to analyse historical and real-time data, identifying patterns, predicting system behaviours, and detecting anomalies.
- Use the Digital Twin to simulate various operational scenarios and cyber threats, applying AI models to predict outcomes and identify vulnerabilities.
- Leverage the insights gained from AI analysis and Digital Twin simulations to inform decision-making, optimizing system performance and enhancing security measures.
- Implement a feedback loop where the system continuously learns from new data, improving the AI models' accuracy and the Digital Twin's effectiveness over time.

This approach represents a significant advancement towards achieving smarter, autonomous industrial processes, offering a scalable, flexible, and intelligent solution to the challenges faced by modern CPS.

V. CONCLUSION

Our comprehensive review of 15 journal articles on the security of cyber-physical systems (CPS) underscores a significant shift towards the integration of advanced technologies such as artificial intelligence (AI), machine learning (ML), and blockchain to address the complex security challenges these systems face. Among the methodologies explored, the fusion of AI and ML with Digital Twins emerges as the most promising, offering a holistic approach to enhancing both the security and operational efficiency of CPS.

This paper not only highlights the current state of research within the field but also proposes a detailed methodology for implementing an AI-enhanced Digital Twin, marking a pivotal step towards smarter and more autonomous industrial processes. Through our analysis, we advocate for a continued exploration of these integrations, emphasizing their potential to revolutionize the security and functionality of CPS in the digital age. Our findings contribute to the academic discourse on CPS security, suggesting a forward path that leverages recent technological innovations for the advancement of secure and efficient systems.

REFERENCES

[1]. A. K. Tyagi, S. U. Aswathy, G. Aghila and N. Sreenath, “AARIN: Affordable, accurate, reliable and innovative mechanism to protect a medical cyber-physical system using blockchain technology,” *International Journal of Intelligent Networks*, pp. 175-183, 2021.

[2]. S. A. Latif, F. B. X. Wen, C. Iwendi, L.-l. F. Wang, S. M. Mohsin, Z. Han and S. S. Band, “AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems,” *Computer Communications*, pp. 274-283, 2022.

[3]. A. K. Tyagi and N. Sreenath, “Cyber Physical Systems: Analyses, challenges and possible solutions,” *Internet of Things and Cyber-Physical Systems*, pp. 22-33, 2021.

[4]. Z. Lv, D. Chen, R. Lou and A. Alazab, “Artificial intelligence for securing industrial-based cyber–physical systems,” *Future Generation Computer Systems*, pp. 291-298, 2021.

[5]. Z. Lian, Q. Yang, W. Wang, Q. Zeng, M. Alazab, H. Zhao and C. Su, “DEEP-FEL: Decentralized, Efficient and Privacy- Enhanced Federated Edge Learning for Healthcare Cyber Physical Systems,” *IEEE Transactions on Network Science and Engineering*, 2022.

[6]. K. Rijswijk, L. Klerkx, M. Bacco, F. Bartolini, E. Bulten, L. Debruyne, J. Dessein, Scotti and G. Brunori , “Digital transformation of agriculture and rural areas: A socio-cyber-physical system framework to support responsibilisation,” pp. 79-90, 2021.

[7]. Z. ji, S.-H. Yang, Y. Cao, Y. Wang, C. Zhou, L. Yue and Y. Zhang, “Harmonizing safety and security risk analysis and prevention in cyber-physical systems,” *Process Safety and Environmental Protection*, pp. 1279-1291.

[8]. B. Wang, H. Zhou, G. Yang, X. Li and H. Yang, “Human Digital Twin (HDT) Driven Human-Cyber-Physical Systems: Key Technologies and Applications,” 2022.

[9]. X. Zhou, X. Xu, W. Liang, Z. Zeng, S. Shimizu, L. T. Yang and Q. Jin, “Intelligent Small Object Detection for Digital Twin in Smart Manufacturing With Industrial Cyber- Physical Systems,” pp. 1377-1385, 2022.

[10]. M. Xu, J. Peng, B. Gupta, J. Kang, Z. Xiong, Z. Li and A. A. A. El-Latif, “Multi-Agent Federated Reinforcement Learning for Secure Incentive Mechanism in Intelligent Cyber-Physical Systems,” *IEEE Internet of Things Journal*, 2021.

[11]. L. K. Ramasamy , F. Khan, M. Shah, B. V. V. S. Prasad, C. Iwendi and C. Biamba, “Secure Smart Wearable Computing through Artificial Intelligence-Enabled Internet of Things and Cyber-Physical Systems for Health Monitoring,” *Sensors*, 2022.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25may351

[12]. M. Jbair, B. Ahmad, C. Maple and R. Harrison, "Threat modelling for industrial cyber physical systems in the era of smart manufacturing," *Computers in Industry*, 2022.
[13]. C. Feng and P. Tian, "Time Series Anomaly Detection for Cyber-physical Systems via Neural System Identification and Bayesian Filtering," in *27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*, 2021.
[14]. A. N. Jahromi, H. Karimipour, A. Dehghantanha and K.-K. Raymond Choo, "Toward Detection and Attribution of Cyber- Attacks in IoT-enabled Cyber-physical Systems," *IEEE Internet of Things Journal*, 2021.
[15]. M. Groshev, C. Guimara˜es, J. Mart´ın-Pe´rez and A. de la Oliva, "Towards Intelligent Cyber-Physical Systems: Digital Twin meets Artificial Intelligence," *IEEE Communications Magazine*, pp. 14-20, 2021.