Gradus Vol. 12, No. 2 (2025)
ISSN 2064-8014

Edge Computing Security in SDN-Enabled Industrial IoT Networks

Zsolt Csaba Johanyák[1,3,*] and **László Göcs**[2]

[1] Department of Information Technologies, GAMF Faculty of Engineering and Computer Science, John von Neumann University, Hungary
[2] Department of Information Technologies, GAMF Faculty of Engineering and Computer Science, John von Neumann University, Hungary
[3] Institute of Mechatronics and Vehicle Engineering, Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University, Hungary

https://doi.org/10.47833/2025.2.CSC.007

Keywords:
Software-Defined Networking,
Edge Computing,
Industrial Internet of Things,
Network Security

Article history:
Received: 13 October 2025
Revised: ... 2025
Accepted: ... 2025

Abstract: *The combination of Industrial Internet of Things (IIoT) with Software-Defined Networking (SDN) and Edge Computing (EC) provides industrial environments with enhanced flexibility and scalability and fast communication capabilities. However, the combination of these services also can lead to sophisticated security threats that impact every system element starting from basic IIoT devices up to SDN controllers and distributed edge servers. In this paper, a survey is conducted on SDN-enabled IIoT network security vulnerabilities and weaknesses that occur at each architectural level of edge computing systems. Our study enlists current security countermeasures that use lightweight cryptography and artificial intelligence-based intrusion detection systems and blockchain-based flow integrity verification methods and identifies knowledge deficits to direct future development of industrial security systems that provide both strong protection and fast response times.*

1. Introduction

The Industrial Internet of Things (IIoT) has experienced fast growth which requires all economical sectors to establish flexible network systems that can scale properly. Software-Defined Networking (SDN) supports the fulfillment of these requirements through its ability to separate control and data planes that allows centralized management and dynamic traffic steering and programmability [1] [2]. Edge Computing (EC) places computation and storage near IIoT devices, which decreases latency and solves bandwidth problems that occur in cloud-based systems [3]. The integration of SDN with EC provides industrial networks with both superior performance and detailed control capabilities. However, it also creates additional security risks.

SDN-enabled IIoT systems become vulnerable to security threats because attackers target their two main entry points, i.e. the centralized SDN controller and the distributed edge nodes. The control plane faces security threats from attackers who try to change flow rules and intercept data streams through edge servers they have compromised [4][5]. The perception layer (physical layer) of IIoT devices faces security risks because these devices do not have enough resources to implement standard security protocols [1]. An SDN-enabled IIoT system requires a complete security system, which defends all architectural levels starting from limited sensors up to edge data centers while maintaining real-time operational needs of industrial systems [1].

Research on SDN security has been focusing mainly on standard computer networks and IIoT security within cloud and edge computing systems [6] [7]. The current literature about SDN and edge computing integration for industrial IoT operations lacks sufficient detailed examination. Our main motivation stems from the idea that a targeted survey helps researchers and practitioners understand current security practices and system vulnerabilities that guide future research to create quick and dependable protection systems.

* Corresponding author: johanyak.csaba@nje.hu

The research reported in this paper evaluates all security threats and defense methods, which safeguard Industrial IoT networks that implement SDN technology with edge computing functionality. Section 2 classifies the main threats across the Industrial Perception Layer, the SDN-based Network Layer, and the Edge Data Center. Section 3 reviews state-of-the-art solutions, including lightweight cryptography, AI-driven intrusion detection, and blockchain-based integrity verification. Finally, Section 4 discusses open research challenges and outlines directions for developing holistic security frameworks that meet the performance and reliability demands of industrial applications.

2. Main security issues in SDN-Enabled Industrial IoT Networks

The combination of Industrial Internet of Things (IIoT) with Software-Defined Networking (SDN) and Edge Computing (EC) creates security challenges that exceed those of conventional networks [1]. SDN provides advantages through centralized control and programmability. However, its architectural design presents potential vulnerabilities to malicious attacks [1].

The implementation of multiple new technologies always creates additional security risks because their combined operation generates new security threats. The main difficulty in this paradigm stems from controlling the elevated complexity and heterogeneity that results from multiple IIoT devices and edge servers [1][3]. The need for quick product delivery together with network standardization limitations creates substantial security threats [2]. These core security issues can be systematically classified the underlying architecture layers they exploit, namely the Industrial Perception Layer (IPL), the Industrial Network Layer (INL)/SDN Control Plane, and the higher layers encompassing applications and data centers (Edge Data Center—EDC) [5].

2.1. Industrial Perception Layer (IPL) and Device Vulnerabilities

The IPL, also known as the perception layer or physical layer, functions as the base layer of IIoT systems which includes essential field devices such as sensors and actuators and controllers [1]. The devices in this layer face fundamental resource limitations because they have restricted processing capabilities and restricted memory and power resources (CPU, power consumption, and memory characteristics) which prevents them from running traditional security solutions based on Public Key Cryptography (PKC) [1]. Attacks targeting the IPL often exploit these constraints to get access to the devices or the collected data [2]. The typical threats at this level are presented below.

1. **Data Integrity and Availability Threats:** The exploitation of resource constraints enables the attackers to introduce incorrect or deceptive information disrupting the entire data collection and processing flow [1]. For example, battery-powered IoT platforms are vulnerable for tampering, i.e. represent physical security risks, which allow attackers to manipulate data and trigger system failures that could lead to dangerous industrial accidents [5].
2. **Physical-Layer Attacks:** These attacks target the physical hardware elements of IIoT systems. Examples include wireless IoT platform attacks, video and image attacks, and text data attacks that use adversarial methods to mislead NLP classification models [5].

2.2. Industrial Network Layer and SDN Control Plane Threats

The security of the INL and the centralized SDN control plane presents distinct and serious vulnerabilities. The centralized control architecture of SDN creates a Single Point of Failure (SPOF) risk because excessive traffic loads beyond controller capacity can lead to system efficiency and scalability problems in big networks [8][9]. Furthermore, the structure of SDN creates specific targets for cyberattacks as presented below.

1. **Implicit Trust and Centralization:** The centralized controller in SDN depends on an implicit trust relationship with edge switches for operation. Since the switches are essentially "dumb" devices that merely implement the flow rules sent to them, they do not verify the legitimacy of these rules . The SDN controller operates as a centralized system that handles sophisticated operations through flow content analysis and generates complex code that proves challenging to test and verify [4].
2. **Flow Rule Manipulation and Injection Attacks:** The main threat to SDN-enabled networks originates from the injection of fake flow rules. They modify OpenFlow routing rules leading to command and information misrouting [7].

3. **Network Propagation Risks:** The edge network becomes vulnerable to attacks that spread across all functional edge entities and through the entire communication network because of malicious traffic injection and eavesdropping on communication links [2].

2.3. Edge Data Center and Application Layer Threats

The combination of IIoT with edge computing systems creates security risks that affect data management and privacy, while attackers focus on the Edge Data Center (EDC) and application layer [1].

1. **Data and Privacy Breaches:** The security measures of edge servers usuall are weaker than those of central cloud servers, which makes data tampering more likely [1]. Additionally, cloud servers may act either curiously or maliciously, potentially extracting sensitive user information [10][11]. Remote devices face the risk of identity exposure because cloud storage of their data becomes insecure [6]. Sharing the huge volume of real-time data generated by IIoT devices among diverse heterogeneous applications and entities is a complicated challenge, particularly when limited edge device performance restricts the deployment of robust security techniques [1].

2. **Application and Malware Attacks:** The application plane experiences security threats that include application manipulation alongside information leakage, accountability issues, impersonation, and communication hijacking [7]. The application layer faces continuous challenges in malware detection and classification because the methods used for detection could fail to identify unknown malware samples [1][12]. Runtime malware injection attacks are also relevant concerns [1].

3. **Prevalent Cyberattack Vectors:** The IIoT architecture has multiple security weaknesses which allow attackers to penetrate all architectural planes [5]. These include:

    - **Denial of Service (DoS) and Distributed DoS (DDoS) Attacks:** All system components experience operational disruptions and system functionality breakdowns from these attacks that occur worldwide [1][13].
    - **Ransomware and Malware:** Ransomware and various forms of malware are widespread global threats that can severely impact the critical components of industrial systems [5].
    - **Man-in-the-Middle (MITM) Attacks:** The lack of proper encryption and weak authentication protocols in IIoT systems makes them susceptible to Man-in-the-Middle (MITM) attacks and other routing attacks [7].

3. Security Solutions

The security solutions developed for SDN-Enabled Industrial Internet of Things networks need to handle the complex and diverse nature of these systems through advanced security measures that protect all three layers of the system, and the Edge Data Center [5]. The security of IIoT devices depends on Edge computing and Software-Defined Networking, which function as security foundations through centralized control and dynamic policy enforcement and localized computational resources for security operations that IIoT devices cannot perform alone [14]. The creation of a secure IIoT environment depends on combining Artificial Intelligence (AI) with Blockchain technology and strong architectural frameworks [5].

3.1. Architectural and Foundational Security Mechanisms

SDN and EC integration allows the creation of fundamental security frameworks. SDN enables network traffic monitoring through centralized control which supports IIoT security and resilience and dynamic segmentation and policy-based access control [14]. The centralized design of SDN controllers enables fast and efficient deployment of security protocols throughout the entire network [9]. The edge layer serves as an optimal position for IoT security solution deployment because it contains more resources than IoT devices which allows execution of security operations like Attribute-Based Access Control and Homomorphic Encryption [6]. Several architectural frameworks and design approaches have been proposed to implement these security capabilities, which can be categorized as follows.

1. **Policy-Driven Orchestration Frameworks:** The Policy-Driven Orchestration Frameworks use SDN to perform automated security management through the conversion of user-defined security policies into specific network configurations [14]. For example, security fusion mechanisms often

use the Interface to Network Security Function (I2NSF) framework coupled with Network Function Virtualization (NFV) [14].

2. **EdgeSec and Layered Designs:** The EdgeSec system and Layered Designs represent two architectural designs which implement complete security services through the Edge layer [6]. The security framework EdgeSec operates through six core modules that enable profile management, security analysis, protocol mapping, critical instruction simulation, interface management, and request processing [6]. This systematic approach enables organizations to implement security standards that apply to particular devices [6]. IEoT systems require hierarchical architectures to establish security because these architectures create logical device isolation from data centers while maintaining reliable data connections between each system layer [2].

3. **Hybrid Architectures:** The combination of cloud, edge, and fog computing systems in hybrid architectures produces better results through workload distribution for security operations [14] and enables scalable and energy-efficient anomaly detection [1].

3.2. Security Solutions for the Industrial Perception Layer (IPL)

The main challenge at the IPL is designing security solutions that work with the severe resource constraints (limited CPU, memory, and power consumption) of sensors, actuators, and controllers [1][2]. Because of these limitations, using traditionally intensive solutions like Public Key Cryptography (PKC) is generally not possible [1]. To solve these problems, the following methods focus on creating lightweight security measures and improving system architecture:

1. **Lightweight Cryptography and Authentication:** The solutions use fundamental cryptographic operations together with authentication methods that function well in systems with limited resources. One of the most suggested solution is AES encryption for secure session key exchange and Public Key Cryptography for device-SDN controller mutual authentication [14]. The implementation of Elliptic Curve Cryptography (ECC) and OAuth represents two often used alternative methods for authentication [14]. Furthermore, certificateless access control methods have also been proposed for IIoT [1].

2. **Intrusion Detection for Endpoints:** Machine learning techniques (e.g. Support Vector Machine (SVM) and Decision Tree models) deployed on edge nodes can help monitoring devices and secure the perception layer against unauthorized access and intrusions [5].

3. **Physical and Data Integrity Protection:** Physical and data integrity protection mechanisms can employ cooperative transmission methods to mitigate physical layer attacks, such as interference and eavesdropping [5]. Furthermore, lightweight hardware-based secure authentication schemes have proven to be a feasible solution for industrial equipment monitoring [1].

3.3. Securing the Industrial Network Layer and SDN Control Plane

Security solutions for the network and control layers mainly use the centralized intelligence of the SDN controller and add advanced detection systems to prevent attacks like Distributed Denial of Service and unauthorized flow rule injection, which are major threats to SDN architectures [12][7].

3.3.1 Intrusion Detection and DDoS Mitigation

Intrusion Detection Systems (IDS) and Intrusion Detection and Prevention Systems (IDPS) are crucial for the protection of the edge network and the control plane. To address protection requirements, modern IDPS implementations employ three key approaches: AI and machine learning-based detection mechanisms, real-time response systems leveraging Software-Defined Networking, and network resilience capabilities for infrastructure fault prediction.

1. **AI/ML-Based IDPS:** Advanced detection and prevention mechanisms are frequently achieved by deploying AI- and Blockchain-based solutions [1]. The combination of Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM) networks proved to be highly successful for detecting DDoS attacks and botnet attacks in distributed systems [1][12]. Security monitoring systems need to detect nonlinear dynamic industrial processes through modeling techniques to adapt to system changes. The identification process can be achieved for example through cloud-based

evolving fuzzy rule-based systems (FRB) that use on-line fuzzy learning and adaptive clustering and recursive algorithms to preserve model accuracy when system dynamics change [15].

2. **Real-Time Response Mechanisms:** The SDN controller operates with a centralized view that allows quick detection and response to security threats. SDN-based IDPS systems utilizing SVM machine learning models achieved 97% to 99% accuracy in simulated attacks against ICMP and TCP SYN floods [16]. SDN controllers can learn and analyze data traces to spot malicious data flows and dynamically assign flow rules to switches to block or slow down the flow.

3. **Network Resilience:** The real-time fault resilience of SDN enables network congestion and link failure prediction that are essential security elements for best path prioritization [17][7]. The SDN controller uses this capability to suggest backup paths that prevent communication failures and result in enhanced security [17].

3.3.2 Ensuring Flow Integrity with Blockchain

The use of blockchain technology ensures the protection of flow integrity in SDN systems. SDN systems are vulnerable to command misrouting attacks because attackers can inject harmful flow rules into the system [7]. Blockchain technology can be integrated to counter this threat by enforcing trust and providing an immutable, decentralized audit trail [4][18]. Blockchain-integrated approaches can be categorized into two primary implementations: edge-based verification systems that validate flows at network entry points, and comprehensive integrity checking mechanisms designed specifically for Industrial IoT environments.

1. **Edge Blockchain Verification:** Edge Blockchain as a Service (BaaS) provides a novel approach to verify flow through edge switches that can reduce attack opportunities [4]. This solution checks network policies against flow rules before creating new entries and keeps an unalterable log of flow insertion events [4].

2. **Blockchain-based Integrity Checking System (BICS):** Systems combining blockchain and SDN technologies can detect fraudulent flow rules in SDN-enabled IIoT environments [19]. The BICS approach demonstrated 100% detection accuracy for fraudulent flow rules while maintaining scalability in detection time [19].

3.4. Advanced Solutions for Data and Application Security (EDC)

The higher layers of solutions concentrate on protecting data integrity and privacy while securing applications that operate on distributed edge and cloud servers [1] and [2].

3.4.1 Data Integrity and Confidentiality

The security of data greatly depends on encryption methods, hashing techniques, and access control systems [7]. The security objectives can be achieved through two complementary mechanisms: encryption-based approaches that protect data confidentiality during transmission and sharing, and blockchain-enabled integrity verification systems that maintain verifiable records of data authenticity.

1. **Encryption and Secure Data Sharing:** The paper [10] demonstrates that symmetric key encryption of IIoT data before transmission to third-party edge servers protects data confidentiality. For flexible sharing between authenticated parties, Proxy Re-Encryption (PRE) schemes, such as Identity-Based Proxy Re-Encryption (IBPRE), are adopted to securely transfer cryptographic file keys between data owners and other users via the blockchain [10].

2. **Blockchain for Data Integrity:** Before data outsourcing, devices compute a hash value of the data and upload this hash to the blockchain along with the encrypted keys [10]. The integrity of the data stored on the edge servers can be verified by recalculating the data hash and comparing it with the immutable hash value recorded on the blockchain [20]. The decentralized nature of blockchain technology enables trustful data storage with verifiable capabilities [18].

3.4.2 Access Control and Identity Management

The application layer requires authentication and authorization for proper operation [7]. New methods must manage heterogeneous devices and prevent unauthorized data access or application manipulation. These requirements can be addressed through three distinct approaches: standard-based mechanisms that define and enforce device behavioral profiles, zero-trust architectures that implement continuous verification and fine-grained access control, and blockchain-enabled identity management systems that establish trustworthy authentication and authorization.

1. **Manufacturer Usage Description (MUD):** The standard-based security mechanism MUD functions as a standard-based security mechanism to enhance security. It defines the expected network behavior of IIoT devices, allowing the SDN controller to translate MUD instructions into security policies (flow rules) for OpenFlow switches, thereby enforcing protective behavioral profiles and reducing the attack surface to only authorized nodes [18]. MUD automates node category identification and reduces operational costs in Smart Factory [18].

2. **Zero-Trust Architectures:** The integration of zero-trust architectures with SDN produces new solutions which implement zero-trust models to achieve fine-grained access control, dynamic network segmentation, and continuous authentication [14]. The proposed solution solves critical problems through its approach of dividing infrastructure components into separate logical domains [14].

3. **Blockchain for Identity/Trust:** The technology of blockchain serves multiple purposes in identity and trust management by enabling device authorization, credibility enhancement, device registration, and authentication functions [20]. An efficient Proof of Authentication (PoAh) consensus mechanism, built on a blockchain network, can be created to provide trustworthy authentication and trace endpoint activity [20].

3.4.3 Advanced Collaborative Techniques

Due to the complex nature of EC-SDN-IIoT systems their network protection demands distributed intelligence-based solutions. The development of intelligent security systems through deep learning and collaborative learning depends on formal modeling of sophisticated observation and cognitive processes, which needs an interdisciplinary method that uses AI, ML, and Cognitive Psychology [21]. The integration of Fuzzy Cognitive Maps (FCMs) with evolutionary computing approaches produces strong decision systems and control mechanisms for IoT sensor data through their capability to represent intricate concept relationships with weighted connections [22]. These intelligent security approaches are operationalized through two key methodologies: Federated Learning frameworks that enable collaborative model training while preserving data privacy, and integrated IT/OT convergence strategies that unify information and operational technology security measures.

1. **Federated Learning (FL):** The method of Federated Learning (FL) enables model training on decentralized IIoT data while protecting sensitive information. This approach provides both security and a resolution for privacy concerns [14]. FL combined with blockchain technology provides privacy-protected cyberattack detection for industrial edge environments.

2. **IT/OT Convergence Security:** Comprehensive cybersecurity strategies require the integration of IT and OT (Operational Technology) security measures, often leveraging technologies like AI, blockchain, and Digital Twins to improve real-time data protection [5].

4. Conclusions

The combination of Industrial Internet of Things, Software-Defined Networking and Edge Computing technology creates a major breakthrough for industrial automation systems and network control. The merging of physical and digital domains creates advanced security problems that require complete solutions that span all architectural levels.

Our analysis reveals that security threats in these integrated environments span three critical layers: the Industrial Perception Layer, the Industrial Network Layer with SDN Control Plane, and the Edge Data Center with application layer components. At IPL, resource-constrained devices face data integrity threats, physical-layer attacks, and authentication challenges that traditional security methods cannot adequately address. The centralized nature of SDN architectures creates single points of failure and

vulnerabilities to flow rule manipulation attacks, while edge computing introduces additional data privacy and application security concerns.

The security solutions studied in this survey prove that multiple defense systems are needed to protect sophisticated environments. Lightweight cryptography and authentication mechanisms demonstrate potential solutions to IPL limitations, while AI/ML-based intrusion detection systems can effectively protect the network and control layers. The technology of blockchain proves useful for maintaining unalterable audit records and preserving flow integrity in SDN systems. The management of distributed security requirements receives additional capabilities through advanced techniques which include federated learning and zero-trust architectures.

Although a wide range of literature can be found related to this topic thre are still research gaps, which the recent discoveries have not managed to resolve. For example, the performance impact of security solutions on real-time industrial operations requires further investigation. Besides, security systems today focus on individual protection layers without building comprehensive defense systems that address threats, which affect multiple security layers.

Future research needs to create complete security frameworks that protect all architectural layers at once. Quantum-safe cryptographic implementations for resource-constrained IIoT devices have become a vital emerging field. The combination of artificial intelligence and machine learning with blockchain security systems enables the development of adaptive protection systems, which detect and counter new threats as they emerge.

The security of SDN-enabled Industrial IoT networks at the edge will stay a vital research and development focus because industrial systems advance toward increased automation and network connectivity. The survey results identify vital solutions to current security challenges while showing the need for continuous advancement of industrial infrastructure protection systems.

References

[1] B. Alotaibi, "A survey on industrial internet of things security: Requirements, attacks, AI-based solutions, and edge computing opportunities," *Sensors*, vol. 23, no. 17, p. 7470, Aug. 2023. DOI: 10.3390/s23177470

[2] P. Li, J. Xia, Q. Wang, Y. Zhang, and M. Wu, "Secure architecture for industrial edge of things(IEoT): A hierarchical perspective," *Computer Networks*, vol. 251, p. 110 641, Sep. 2024. DOI: 10.1016/j.comnet.2024.110641

[3] S. S. Jazaeri, S. Jabbehdari, P. Asghari, and H. Haj Seyyed Javadi, "Edge computing in SDN-IoT networks: A systematic review of issues, challenges and solutions," *Cluster Computing*, vol. 24, no. 4, pp. 3187–3228, Dec. 2021. DOI: 10.1007/s10586-021-03311-6

[4] J. Hu, M. Reed, N. Thomos, M. F. AI-Naday, and K. Yang, "Securing SDN-controlled IoT networks through edge blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2102–2115, Feb. 2021. DOI: 10.1109/JIOT.2020.3017354

[5] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi, "Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions," *Sensors*, vol. 25, no. 1, p. 213, Jan. 2025. DOI: 10.3390/s25010213

[6] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A survey of edge computing-based designs for IoT security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 195–202, May 2020. DOI: 10.1016/j.dcan.2019.08.006

[7] A. Rahdari et al., "Security and privacy challenges in SDN-enabled IoT systems: Causes, proposed solutions, and future directions," *Computers, Materials & Continua*, vol. 80, no. 2, pp. 2511–2533, 2024. DOI: 10.32604/cmc.2024.052994

[8] A. Singh, R. Salam, and D. S. Gupta, "Network resilience and secure confidentiality in industrial-IoT through software-defined networking," in *2024 15th international conference on computing communication and networking technologies (ICCCNT)*, Kamand, India, Jun. 2024, pp. 1–6. DOI: 10.1109/ICCCNT61001.2024.10725705

[9] F. Keti and O. M. Ghazal, "A review of the security challenges mitigation in IoT systems via the utilization of SDN technology," in *2023 international conference on engineering, science and advanced technology (ICESAT)*, Mosul, Iraq, Jun. 2023, pp. 1–6. DOI: 10.1109/ICESAT58213.2023.10347320

[10] Y. Gao, Y. Chen, X. Hu, H. Lin, Y. Liu, and L. Nie, "Blockchain based IIoT data sharing framework for SDN-enabled pervasive edge computing," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5041–5049, Jul. 2021. DOI: 10.1109/TII.2020.3012508

[11] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," en, *Future Generation Computer Systems*, vol. 78, pp. 680–698, Jan. 2018, ISSN: 0167739X. DOI: 10.1016/j.future.2016.11.009

[12] S. K. Poorazad, C. Benzaïd, and T. Taleb, "Blockchain and deep learning-based IDS for securing SDN-enabled industrial IoT environments," in *GLOBECOM 2023 - 2023 IEEE global communications conference*, Kuala Lumpur, Malaysia, Dec. 2023, pp. 2760–2765. DOI: 10.1109/GLOBECOM54140.2023.10436839

[13] Y. Zhou, G. Cheng, and S. Yu, "An SDN-Enabled Proactive Defense Framework for DDoS Mitigation in IoT Networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5366–5380, 2021, ISSN: 1556-6013, 1556-6021. DOI: 10.1109/TIFS.2021.3127009

[14] S. R. Mishra, B. Shanmugam, K. C. Yeo, and S. Thennadil, "SDN-Enabled IoT Security Frameworks—A Review of Existing Challenges," en, *Technologies*, vol. 13, no. 3, p. 121, Mar. 2025, ISSN: 2227-7080. DOI: 10.3390/technologies13030121

[15] S. Blazic, D. Dovzan, and I. Skrjanc, "Cloud-based identification of an evolving system with supervisory mechanisms," in *2014 IEEE International Symposium on Intelligent Control (ISIC)*, Juan Les Pins, France: IEEE, Oct. 2014, pp. 1906–1911, ISBN: 978-1-4799-7406-1. DOI: 10.1109/ISIC.2014.6967642

[16] N. Mazhar, R. Saleh, R. Zaba, M. Zeeshan, M. Muzaffar Hameed, and N. Khan, "R-IDPS: Real time SDN-based IDPS system for IoT security," *Computers, Materials & Continua*, vol. 73, no. 2, pp. 3099–3118, 2022. DOI: 10.32604/cmc.2022.028285

[17] A. Savaliya, R. H. Jhaveri, Q. Xin, S. Alqithami, S. Ramani, and T. A. Ahanger, "Securing industrial communication with software-defined networking," *Mathematical Biosciences and Engineering*, vol. 18, no. 6, pp. 8298–8313, 2021. DOI: 10.3934/mbe.2021411

[18] N. N. Josbert, M. Wei, P. Wang, and A. Rafiq, "A look into smart factory for Industrial IoT driven by SDN technology: A comprehensive survey of taxonomy, architectures, issues and future research orientations," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 5, p. 102 069, Jun. 2024. DOI: 10.1016/j.jksuci.2024.102069

[19] A. Derhab et al., "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, p. 3119, Jul. 2019. DOI: 10.3390/s19143119

[20] S. Asaithambi, S. Nallusamy, J. Yang, S. Prajapat, G. Kumar, and P. S. Rathore, "A secure and trustworthy blockchain-assisted edge computing architecture for industrial internet of things," *Scientific Reports*, vol. 15, no. 1, p. 15 410, May 2025. DOI: 10.1038/s41598-025-00337-3

[21] C. Pozna and R.-E. Precup, "Aspects concerning the observation process modelling in the framework of cognition processes," *Acta Polytechnica Hungarica*, vol. 9, no. 1, pp. 203–223, 2012.

[22] J. Vaščák, L. Pomšár, P. Papcun, E. Kajáti, and I. Zolotová, "Means of IoT and Fuzzy Cognitive Maps in Reactive Navigation of Ubiquitous Robots," en, *Electronics*, vol. 10, no. 7, p. 809, Mar. 2021, ISSN: 2079-9292. DOI: 10.3390/electronics10070809