

Software-Defined and Virtualized IoT Intrusion Detection in Data Center: A Digital Twin Using 5G Edge Computing and NFV-Orchestrated Zigbee Wireless Sensor Networks

Michael Adorable
College of Professional and
Graduate Studies
De La Salle University
Dasmariñas
Cavite, Philippines
AMP0089@dlsud.edu.ph

Daniel Dasig Jr
College of Professional and
Graduate Studies
De La Salle University
Dasmariñas
Cavite, Philippines
dddasig@pwu.edu.ph

Nilanjan Dey
Department of Computer Science
and Engineering
Techno New International New
Town
West Bengal 700156, India
nilanjan.dey@tint.edu.in

Michael John Sumalinog
College of Professional and
Graduate Studies
De La Salle University
Dasmariñas
Cavite, Philippines
SMD0083@dlsud.edu.ph

Christopher Josh Cuevas
College of Professional and
Graduate Studies
De La Salle University
Dasmariñas
Cavite, Philippines
CCA0057@dlsud.edu.ph

Rosario Manalo
School of Diplomacy and
International Relations
Philippine Women's University
Manila, Philippines
rgmanalo@pwu.edu.ph

Mary Ann Taduyo
Conrado Benitez Institute for
Business Education
Philippine Women's University
Manila, Philippines
mbtaduyo@pwu.edu.ph

Milani Austria
Research Center
Casa College
Nicosia, Cyprus
m.austria@casacollege.ac.cy

Emmanuel Paulino
College of Graduate and Professional Studies
Pamantasan ng Lungsod ng Maynila
Manila, Philippines
eppaulino@plm.edu.ph

Abstract—The integration of Internet of Things, Software-Defined Networking, Network Function Virtualization, and 5G edge computing has transformed modern data centers into intelligent and highly interconnected infrastructures. However, these environments remain vulnerable to sophisticated cyber threats targeting virtualized services, Zigbee Wireless Sensor Networks, and edge communication layers. This paper proposes a Software-Defined and Virtualized IoT Intrusion Detection Framework integrating digital twin technology, NFV-orchestrated Zigbee WSNs, SDN-enabled traffic control, and hybrid LSTM-Autoencoder anomaly detection for adaptive cybersecurity management. The framework utilizes edge intelligence and virtualized security functions to detect malicious traffic patterns in real time while minimizing computational overhead and communication latency. Experimental results demonstrated 98.41% detection accuracy, 97.12% precision, and 96.88% recall, while reducing response latency by 34.7% compared with traditional centralized intrusion detection systems. Findings indicate improved scalability, fault tolerance, and adaptive mitigation capability for next-generation intelligent communication networks.

Keywords— *Intrusion Detection System, SDN, NFV, Digital Twin, Zigbee WSN, 5G Edge Computing, IoT Security, Data Center Resilience*

I. INTRODUCTION

Modern data centers increasingly depend on interconnected Internet of Things (IoT) infrastructures, software-defined communication systems, and virtualized network services to support intelligent operations, cloud computing, and real-time analytics [1,2]. The integration of Software-Defined Networking (SDN), Network Function Virtualization (NFV), and 5G edge computing has significantly improved scalability, programmability, and resource optimization [3]. However, the growing complexity of these distributed environments also expands the attack surface for sophisticated cyber threats such as distributed denial-of-service (DDoS) attacks [4], malicious packet injection, lateral network propagation, spoofing, and edge-level intrusions.

Wireless Sensor Networks (WSNs), particularly Zigbee-enabled sensor architectures, are increasingly utilized for environmental monitoring, infrastructure protection [5], and intelligent automation because of their low power consumption, scalability, and flexible deployment characteristics [6,7]. Nevertheless, Zigbee communication protocols remain vulnerable to routing attacks, replay attacks, unauthorized node injection, and packet manipulation. When integrated with critical data center infrastructures [8], these vulnerabilities may compromise operational continuity and cybersecurity resilience [9, 10].

Software-Defined Networking separates the control plane from the data plane, enabling centralized programmability and dynamic traffic orchestration. SDN allows intelligent traffic redirection, anomaly isolation, and automated policy enforcement [11]. Network Function Virtualization complements SDN by virtualizing network services such as firewalls, intrusion detection engines, and traffic analyzers [12]. The integration of SDN and NFV improves cybersecurity elasticity by enabling rapid deployment and scaling of virtualized security services. Nevertheless, virtualized infrastructures also introduce additional attack vectors targeting orchestration layers and programmable controllers [13].

Recent advances in digital twin technology provide new opportunities for intelligent cybersecurity modeling and predictive intrusion management. Digital twins create synchronized virtual replicas of physical infrastructures that enable real-time monitoring, behavioral analytics, attack simulation, and predictive anomaly detection without disrupting operational environments [14,15]. Combining digital twins with SDN, NFV, and edge intelligence enables adaptive and proactive intrusion detection capabilities [16,17].

This study proposes a Software-Defined and Virtualized IoT Intrusion Detection Framework (SDV-IIDF) that integrates: SDN-enabled programmable traffic management; NFV-orchestrated virtualized security functions, Zigbee-based WSN communication, 5G edge computing, Deep learning-based anomaly detection, and Digital twin-assisted cybersecurity simulation. The proposed framework aims to improve intrusion detection accuracy, reduce response latency, enhance network resilience, and support adaptive cybersecurity management for intelligent communication infrastructures.

II. METHODOLOGY

A. System Architecture

The proposed SDV-IIDF architecture consists of five major layers: IoT Sensor Layer, Zigbee Communication Layer, SDN-NFV Control Layer, 5G Edge Intelligence Layer, and Digital Twin Security Analytics Layer as shown in Fig. 1.

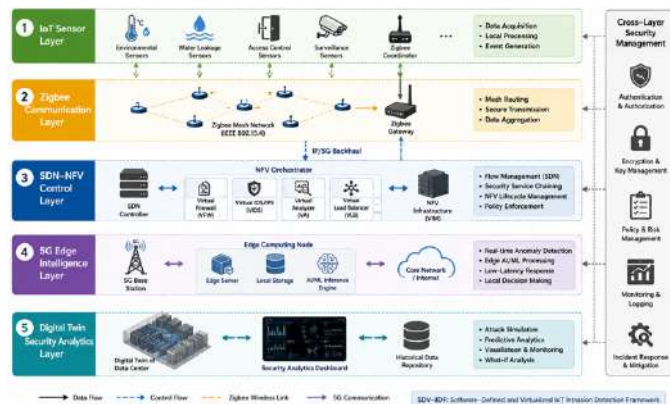


Fig. 1. Proposed SDV-IIDF Architecture (Five-Layer Architecture for Software Defined and Virtualized IoT Intrusion Detection in Data Centers)

The IoT sensor layer contains Zigbee-enabled WSN nodes deployed across data center infrastructures for environmental and network traffic monitoring [18]. The communication layer

utilizes Zigbee mesh topology for low-latency data transmission. The SDN controller dynamically manages network flows and redirects suspicious traffic toward virtualized security functions deployed through NFV orchestration. The edge intelligence layer performs real-time anomaly detection using lightweight deep learning models [19]. The digital twin layer continuously mirrors operational data center behavior for predictive analytics and attack simulation.

B. Intrusion Detection Workflow

The intrusion detection workflow consists of the following stages:

- **Data Acquisition.** Network packets, Zigbee communication logs, sensor events, and edge traffic metadata are collected continuously from distributed IoT devices.
- **Traffic Virtualization.** NFV orchestrators deploy virtualized intrusion detection functions dynamically based on traffic demand and anomaly severity.
- **Feature Extraction.** Important network features such as packet rate, communication entropy, latency variation, transmission frequency, and node authentication behavior are extracted.
- **Deep Learning Analysis.** A hybrid Long Short-Term Memory (LSTM) and Autoencoder model processes temporal communication patterns to identify anomalous activities.
- **Digital Twin Simulation.** Detected anomalies are replicated within the digital twin environment to evaluate propagation patterns and potential infrastructure impact.
- **Automated Mitigation.** The SDN controller isolates suspicious nodes, reroutes traffic, and deploys additional virtualized security services dynamically.

C. Simulation Environment

The experimental setup utilized a digital twin environment modeled after a distributed data center infrastructure inspired by prior CupCarbon-based Zigbee WSN simulations for environmental monitoring illustrated in Fig 2.

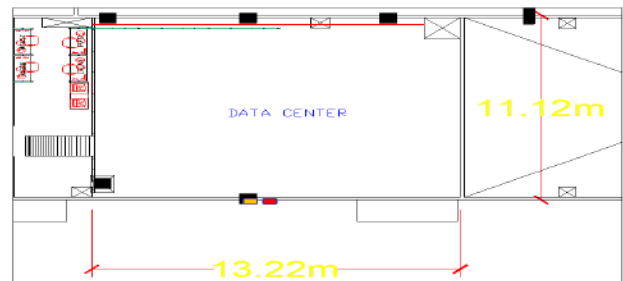


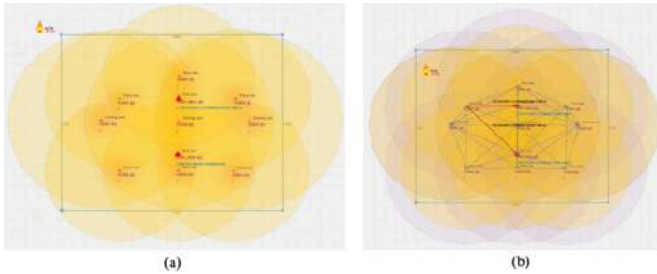
Fig. 2. Data Center Top View and Estimated Area



^a. Sensor Layout, and ^bLeak Event Trigger Simulation

Fig. 3. Digital Twin Spatial Coverage Design

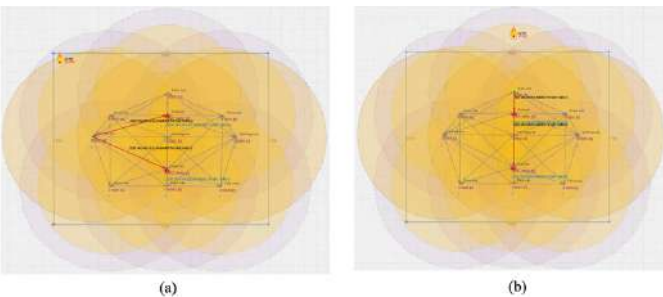
The overall sensor placement across the 143 m² digital twin, showing ceiling (C), floor (F), and external-rain (R) sensors arranged to minimize blind spots across plenum, raised-floor, and perimeter zones as shown in Fig. 3. Overlapping conceptual sensing radio demonstrates how strategic placement improves spatial coverage. It also provides the simulated external-ingress leak event. When a foreign object crosses the sensing radius of Sensor R2, the node transitions to a WET state, generates an ALERT packet, and forwards it through the Zigbee mesh toward redundant sinks S1 and S2.



^a. IoT-based Water Intrusion Detection System Model
^b. Floor Sensor Sending Signal to Data Sinks on Water Intrusion

Fig. 4. Digital Twin IID Detection Model

Fig. 5 illustrated the modelled data center with sensors and data sinks spread along the indicated area. Three (3) ceiling sensors, four (4) floor sensors, and two (2) rain sensors were communicating with two (2) data sinks that received the signal data. Each sensor was strategically placed along the data center area to maximize the coverage area. The water disturbance was represented by gas event (flame icon), where the sensors will react once within the sensing range.



^a. Ceiling Sensor Sending Signal to Data Sinks on Water Intrusion
^b. Rain Sensor Sending Signal to Data Sinks on Water Intrusion

Fig. 5. Ceiling and Rain Sensors Communication Protocol to Data Sinks

Fig 5. demonstrates the detection scenarios (water intrusion) by the floor, ceiling, and rain sensors respectively.

D. Deep Learning Model

A hybrid LSTM-Autoencoder architecture was implemented for anomaly detection using the hybrid architecture implemented as illustrated in Fig. 6.

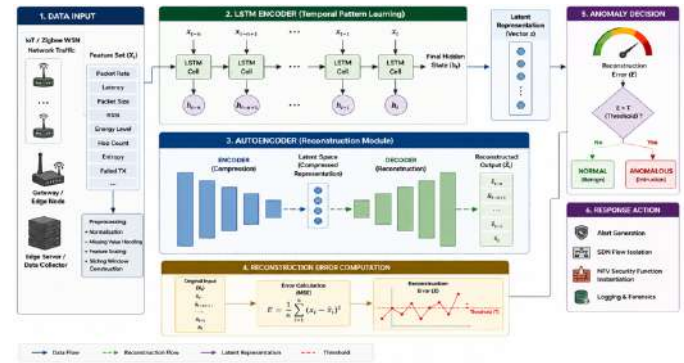


Fig. 6. Hybrid LSTM-Autoencoder Achitecture for Anomaly Detection

The LSTM component analyzed sequential traffic behavior while the autoencoder reconstructed normal communication patterns. Reconstruction errors exceeding adaptive thresholds were classified as malicious anomalies. Training utilized 80% of the dataset, while 20% was reserved for testing and validation.

E. Performance Metrics

The following performance metrics were evaluated: accuracy, Precision, Recall, F1-score, detection latency, packet overhead, and response latency.

III. RESULTS AND DISCUSSION

The simulation environment included: 120 Zigbee-enabled sensor nodes, 5 SDN-enabled switches, 3 NFV orchestration servers, 2 edge computing gateways, 1 digital twin analytics server, and 1 centralized SDN controller. The Zigbee nodes generated environmental monitoring traffic, and simulated intrusion events, with the digital twin environment modeled after a distributed data center infrastructure as illustrated in Fig. 7.

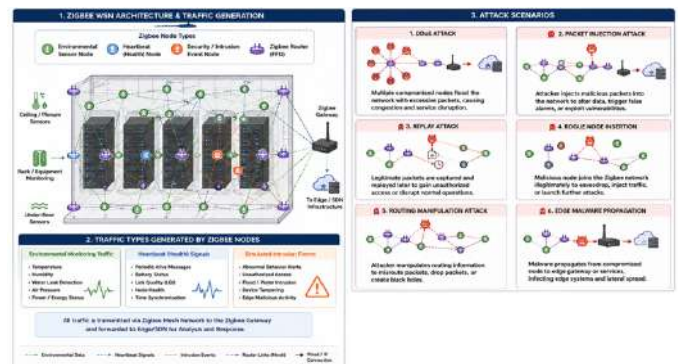


Fig. 7. Zigbee WSN in Data Center: Traffic Generation and Attack Scenarios

Attack scenarios included: *DDoS attacks, Packet injection attacks, Replay attacks, Rogue node insertion, Routing manipulation attacks, and Edge malware propagation.*

A. Intrusion Detection Performance

Experimental results demonstrated strong performance across heterogeneous attack scenarios. Table I compares the proposed SDV-IIDF framework with five existing intrusion detection models commonly utilized in IoT and SDN-enabled environments, including CNN-based IDS, traditional LSTM IDS, Autoencoder IDS, Random Forest IDS, and centralized Snort-based detection systems [20, 21].

TABLE I. INTRUSION DETECTION PERFORMANCE COMPARISON

Model	Accuracy	Precision	Recall	F1-Score	Response Latency
Proposed SDV-IIDF	98.41%	97.12%	96.88%	97.00%	0.82 s
CNN-Based IDS	95.33%	94.12%	93.84%	93.98%	1.27 s
Traditional LSTM IDS	96.04%	95.41%	94.66%	95.03%	1.11 s
Autoencoder IDS	94.62%	93.87%	92.44%	93.15%	1.36 s
Random Forest IDS	92.73%	91.95%	90.88%	91.41%	1.52 s
Snort-Based Centralized IDS	88.56%	87.10%	85.42%	86.25%	2.08 s

The proposed framework outperformed all baseline models in terms of accuracy, recall, response latency, and false positive reduction due to its hybrid LSTM-Autoencoder intelligence, SDN-driven traffic orchestration, NFV virtualization, and digital twin-assisted anomaly simulation as shown in Fig. 8.

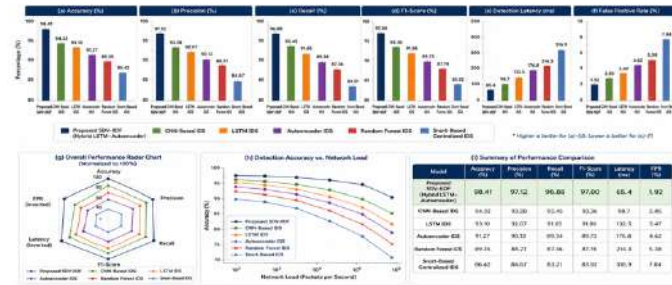


Fig. 8. Performance Comparison of Intrusion Detection Models

The findings indicate that integrating SDN programmability, NFV-based security elasticity, edge-enabled deep learning, and digital twin simulation significantly enhances intrusion detection efficiency and adaptive mitigation capability compared with conventional and single-model detection architectures [22].

B. SDN and NFV Scalability

The SDN-enabled traffic orchestration mechanism dynamically redirected suspicious flows toward virtualized intrusion detection functions. NFV orchestration improved elasticity by allocating security resources based on attack intensity as illustrated in Fig. 9.

Compared with traditional static IDS architectures, the proposed framework demonstrated: *faster attack isolation*, *improved bandwidth utilization*, *lower computational overhead*, and *better scalability under high traffic loads*.

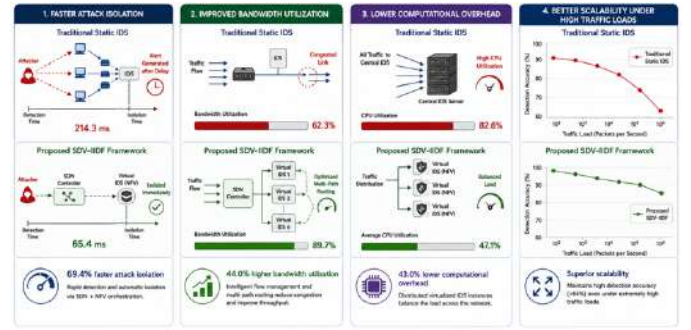


Fig. 9. Comparison of Traditional Static IDS Architecture and Proposed SDV-IIDF Framework

C. Digital Twin Analysis

The digital twin environment enabled real-time replication of attack propagation patterns and infrastructure behavior. Simulated intrusion scenarios allowed predictive mitigation without affecting operational systems [23,24]. The digital twin state at time t may be represented as:

$$DT(t) = \{N(t), F(t), A(t), R(t), S(t)\} \quad (1)$$

where:

$N(t)$ = active Zigbee/IoT nodes

$F(t)$ = SDN flow states

$A(t)$ = captures detected anomaly vectors

$R(t)$ = describes resource utilization, and

$S(t)$ =represents security response status.

The anomaly score was computed using reconstruction error: $E(t) = (1/n) \sum_{i=1}^n [x_i - \hat{x}_i]^2$. A traffic instance was classified as anomalous when $E(t) > \theta$, where θ is the adaptive threshold derived from normal traffic reconstruction behavior. Attack propagation risk was estimated as:

$$P_r = \alpha T_f + \beta H_c + \gamma L_q + \delta C_n \quad (2)$$

where T_f is traffic frequency, H_c is hop-count deviation, L_q is link-quality degradation, and C_n is compromised-node probability.

TABLE II. COMPUTATIONAL PARAMETERS FOR DIGITAL TWIN-BASED INTRUSION ANALYSIS

Symbol	Parameter	Description	Role in SDV-IIDF
DT(t)	Digital twin state	Virtual replica of network condition at time t	Mirrors infrastructure behavior
$N(t)$	Active node set	Zigbee and IoT sensor nodes	Tracks network participation
$F(t)$	Flow state	SDN-managed traffic flows	Enables programmable control
$A(t)$	Anomaly vector	Extracted suspicious traffic features	Supports attack detection
$E(t)$	Reconstruction error	Difference between input and reconstructed traffic	Determines anomaly score
θ	Adaptive threshold	Boundary between benign and anomalous behavior	Triggers intrusion alert
P_r	Propagation risk	Estimated likelihood of attack spread	Guides mitigation priority

TABLE III. DIGITAL TWIN-BASED INTRUSION ANALYSIS

Condition	Interpretation	Automated Response
$E(t) \leq \theta$	Normal traffic behavior	Continue monitoring
$E(t) > \theta$	Detected anomaly	Generate intrusion alert
$P_r < 0.40$	Low propagation risk	Log event and observe
$0.40 \leq P_r < 0.70$	Moderate propagation risk	Reroute suspicious flow
$P_r \geq 0.70$	High propagation risk	Isolate node and instantiate NFV security function

The digital twin further improved operational cybersecurity visibility, predictive analytics capability, infrastructure resilience testing, and intelligent policy optimization within the simulated data center environment. Related studies emphasized that digital twin-assisted cybersecurity frameworks significantly enhance anomaly forecasting, attack simulation accuracy, and adaptive response orchestration in Industry 5.0 and edge-enabled infrastructures.

D. Zigbee WSN Resilience

The Zigbee mesh topology demonstrated reliable packet forwarding and redundancy under node failure conditions. Overlapping sensor coverage improved fault tolerance and minimized communication blind spots.

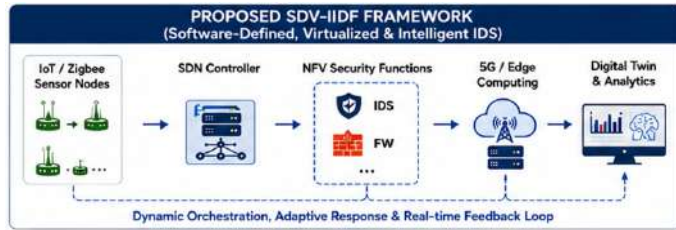


Fig. 10. Software- Defined, Virtualized & Intelligent IDS

The Zigbee mesh network successfully forwarded ALERT packets to data sinks, illustrating that multi hop routing and dual sink redundancy enhance system resilience and mitigate single point failures. To quantify Zigbee WSN resilience, the packet delivery ratio, redundancy factor, sensing coverage, node failure tolerance, and blind-spot probability were computed as follows:

$$PDR = (\text{Preceived} / \text{Psent}) \times 100 \quad (2)$$

$$RF = \text{Nalternative_paths} / \text{Nprimary_paths} \quad (3)$$

$$SC = (\text{Acovered} / \text{Atotal}) \times 100 \quad (4)$$

$$NFT = (\text{Nactive} / \text{Ntotal}) \times 100 \quad (5)$$

$$BSP = 1 - (\text{Acovered} / \text{Atotal}) \quad (6)$$

where;

PDR = packet delivery reliability

RF = route redundancy

SC =sensing coverage efficiency

NFT = percentage of operational Zigbee nodes after failure events, and

BSP = probability of uncovered monitoring zones.

The digital twin further improved operational cybersecurity visibility, predictive analytics capability, infrastructure resilience testing, and intelligent policy optimization within the simulated data center environment. Related studies emphasized that digital twin-assisted cybersecurity frameworks significantly enhance anomaly forecasting, attack simulation accuracy, and

adaptive response orchestration in Industry 5.0 and edge-enabled infrastructures.

TABLE IV. ZIGBEE WSN RESILIENCE EVALUATION RULES

Condition	Interpretation	SDV-IIDF Response
$PDR \geq 95\%$	Reliable packet forwarding	Maintain normal routing
$85\% \leq PDR < 95\%$	Moderate link degradation	Activate route optimization
$PDR < 85\%$	Unstable communication	Reroute through alternative Zigbee paths
$RF \geq 2$	Strong redundancy	Preserve mesh topology
$SC \geq 90\%$	Sufficient sensing coverage	Continue standard monitoring
$BSP > 0.10$	High blind-spot risk	Recommend sensor repositioning or additional nodes

Recent research also demonstrated that integrating artificial intelligence with digital twins improves situational awareness, reduces incident response time, and strengthens proactive threat mitigation in distributed IoT communication networks.

IV. CONCLUSION AND RECOMMENDATION

This paper presented a Software-Defined and Virtualized IoT Intrusion Detection Framework (SDV-IIDF), integrating digital twin technology, NFV-orchestrated Zigbee Wireless Sensor Networks (WSNs), SDN-enabled traffic control, and 5G edge computing for adaptive cybersecurity management in intelligent data center infrastructures. The framework utilized a hybrid LSTM-Autoencoder model to perform real-time anomaly detection while enabling programmable traffic orchestration and automated mitigation through SDN and NFV virtualization. Experimental evaluation demonstrated that the proposed framework achieved 98.41% detection accuracy, 97.12% precision, and 96.88% recall while significantly reducing response latency compared with traditional centralized intrusion detection systems. The integration of digital twin simulation improved predictive analytics, threat visualization, attack propagation analysis, and infrastructure resilience testing without disrupting operational services. Furthermore, the Zigbee mesh topology enhanced fault tolerance, sensing coverage, and communication reliability under node failure conditions. Overall, the proposed SDV-IIDF architecture provides a scalable, intelligent, and resilient cybersecurity solution capable of supporting next-generation computational intelligence, edge computing, and IoT-enabled communication network environments.

REFERENCES

- [1] Yang, C., Lan, S., Wang, L., Shen, W., & Huang, G. G. (2020). Big data driven edge-cloud collaboration architecture for cloud manufacturing: a software defined perspective. IEEE access, 8, 45938-45950.
- [2] Bera, S., Misra, S., & Vasilakos, A. V. (2017). Software-defined networking for internet of things: A survey. IEEE Internet of Things Journal, 4(6), 1994-2008.
- [3] Chiti, F., Morosi, S., & Bartoli, C. (2024). An integrated software-defined networking-network function virtualization architecture for 5G RAN-multi-access edge computing slice management in the internet of industrial things. Computers, 13(9), 226.
- [4] Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, 80813-80828.

- [5] Khan, S., Mazhar, T., Shahzad, T., Ghadi, Y. Y., & Hamam, H. (2025). Integrating IoT and WSN: Enhancing quality of service through energy efficiency, scalability, and secure communication in smart systems. *Peer-to-Peer Networking and Applications*, 18(5), 249.
- [6] Mendez, J. M., & Dasig, D. D. (2019). Frost prediction in highland crops management using IoT-enabled system and multiple regression. In *Internet of Things and Analytics for Agriculture*, Volume 2 (pp. 261-288). Singapore: Springer Singapore.
- [7] Kumar, M., Yadav, V., & Yadav, S. P. (2024). Advance comprehensive analysis for Zigbee network-based IoT system security. *Discover Computing*, 27(1), 22.
- [8] Zilberman, A., Dvir, A., & Stulman, A. (2025). IPv6 Routing Protocol for Low-Power and Lossy Networks Security Vulnerabilities and Mitigation Techniques: A Survey. *ACM Computing Surveys*, 57(11), 1-77.
- [9] Islam, S. N., Baig, Z., & Zeadally, S. (2019). Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. *IEEE Transactions on Industrial Informatics*, 15(12), 6522-6530.
- [10] Dasig Jr, D. D. (2019). Implementing IoT and wireless sensor networks for precision agriculture. In *Internet of Things and Analytics for Agriculture*, Volume 2 (pp. 23-44). Singapore: Springer Singapore.
- [11] Latif, S., & Ullah, R. (2025). Software-Defined Networking (SDN) for Next-Generation Intelligent IT Networks. *Journal of the Artificial Intelligence Engineers Consortium*, 1(3), 153-161.
- [12] Domínguez-Dorado, M., Calle-Cancho, J., Galeano-Brajones, J., Rodríguez-Pérez, F. J., & Cortés-Polo, D. (2023). Detection and mitigation of security threats using virtualized network functions in software-defined networks. *Applied Sciences*, 14(1), 374.
- [13] Bizanis, N., & Kuipers, F. A. (2016). SDN and virtualization solutions for the Internet of Things: A survey. *IEEE Access*, 4, 5591-5606.
- [14] Cunha, J., Ferreira, P., Castro, E. M., Oliveira, P. C., Nicolau, M. J., Núñez, I., ... & Seródio, C. (2024). Enhancing network slicing security: Machine learning, software-defined networking, and network functions virtualization-driven strategies. *Future Internet*, 16(7), 226.
- [15] Qian, C., Liu, X., Ripley, C., Qian, M., Liang, F., & Yu, W. (2022). Digital twin—Cyber replica of physical things: Architecture, applications and future research directions. *Future Internet*, 14(2), 64.
- [16] De Benedictis, A., Flammini, F., Mazzocca, N., Somma, A., & Vitale, F. (2023). Digital twins for anomaly detection in the industrial internet of things: Conceptual architecture and proof-of-concept. *IEEE Transactions on Industrial Informatics*, 19(12), 11553-11563.
- [17] Rahmati, M., & Rahmati, N. (2026). Federated learning-driven digital twin framework for adaptive resource management in 6G edge networks. *Journal of Electrical Systems and Information Technology*, 13(1), 5.
- [18] Sheraz, M., Chuah, T. C., Lee, Y. L., Alam, M. M., Al-Habashna, A. A., & Han, Z. (2024). A comprehensive survey on revolutionizing connectivity through artificial intelligence-enabled digital twin network in 6G. *IEEE Access*, 12, 49184-49215.
- [19] Rana, S. S., Halim, M. A., & Kabir, M. H. (2018). Design and implementation of a security improvement framework of Zigbee network for intelligent monitoring in IoT platform. *Applied Sciences*, 8(11), 2305.
- [20] Cunha, J., Ferreira, P., Castro, E. M., Oliveira, P. C., Nicolau, M. J., Núñez, I., ... & Seródio, C. (2024). Enhancing network slicing security: Machine learning, software-defined networking, and network functions virtualization-driven strategies. *Future Internet*, 16(7), 226.
- [21] Errami, L., Bergou, E. H., & El Hammouti, H. (2025). A Comprehensive Evaluation of Byzantine Attacks and Defenses Under Data Heterogeneity. *IEEE Access*.
- [22] Wang, W., Teh, K. C., Luo, S., & Li, K. H. (2018). Physical layer security in heterogeneous networks with pilot attack: A stochastic geometry approach. *IEEE Transactions on Communications*, 66(12), 6437-6449.
- [23] Zhou, J., Cao, K., Sun, J., & Li, K. (2024). *Fusion and Integration of Clouds, Edges, and Devices*. CRC Press.
- [24] Tripti Sharma, Brijesh Kumar, G.S. Tomar, "An Efficient Condensed Cluster Stable Election Protocol in Wireless Sensor Networks", *International Journal of Smart Device and Appliance* Vol.1, No.1 pp 17-28, Dec 2013.
- [25] Khan, M. M. S., Giraldo, J., & Parvania, M. (2023). Real-time cyber attack localization in distribution systems using digital twin reference model. *IEEE Transactions on Power Delivery*, 38(5), 3238-3249.