IJIE

INTERNATIONAL JOURNAL OF INTEGRATED ENGINEERING
ISSN: 2229-838X e-ISSN: 2600-7916

Vol. 18 No. 1 (2026) 202-214
https://publisher.uthm.edu.my/ojs/index.php/ijie

SDN Security in 6G: Future Technologies and Research Challenges

Abdinasir Hirsi[1,2], Lukman Audah[1]*, Adeb Salh[3], Mohammed A. Alhartomi[4], Nan Mad Sahar[1], Salman Ahmed[1]

[1] *Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, Parit Raja 86400, MALAYSIA*
[2] *Faculty of Engineering, Jamhuriya University of Science and Technology, Mogadishu, SOMALIA*
[3] *Faculty of Information and Communication Technology, University Tunku Abdul Rahman (UTAR), Kampar 31900, MALAYSIA*
[4] *Department of Electrical Engineering, University of Tabuk, Tabuk 71491, SAUDI ARABIA*

*Corresponding Author: hanif@uthm.edu.my & adebali@utar.edu.my
DOI: https://doi.org/10.30880/ijie.2026.18.01.015

Article Info

Received: 1 January 2026
Accepted: 30 March 2026
Available online: 17 April 2026

Keywords

SDN security, SDN attacks, Cybersecurity, SDN vulnerabilities, 6G, 6G SDN

Abstract

Sixth-generation (6G) wireless communication is expected to be launched by 2030, introducing advanced technologies to meet the demands of ultralow, intelligent, and highly secure networks. Software-defined networks (SDN) play a crucial role in enhancing 6G security by offering architectural flexibility, centralized intelligence, and programmable defenses that address the unique challenges of next-generation connectivity. However, securing these emerging technologies requires novel adaptive security solutions. Reliability and ultralow latency are fundamental to 6G, where security mechanisms play a pivotal role in ensuring trust and resilience. In this study, we explore the role of SDN in 6G, its emerging applications, security threats, and key technologies that enhance SDN security in 6G environments. Based on the review, nearly 95% of existing studies primarily focus on the control and application layers of SDN in 6G, while the role of the data plane remains largely underexplored and insufficiently addressed. Finally, we outline critical security challenges and future research directions. To the best of our knowledge, this is the first study to comprehensively summarize the applications, security challenges, and research directions for SDN security in 6G technologies.

1. Introduction

The exponential increase in mobile data traffic, as projected by the ITU and illustrated in Fig. 1, underscores the urgent need for scalable, secure, and intelligent network architectures [1]. Software-Defined Networking (SDN) has emerged as a transformative paradigm that decouples the control plane from the data plane to enable centralized control, programmability, and dynamic resource allocation. This shift enhances agility, automation, scalability, and positioning SDN as a key enabler of next-generation networks [2]. In 6G, SDN is expected to optimize network performance, enable intelligent traffic management, and strengthen multilayered security frameworks for complex distributed infrastructures. As shown in Table 1, 6G networks have introduced significant advancements over 5G, including spectrum expansion (up to 1 THz), ultra-reliable low-latency

communication (URLLC), and real-time data processing [1]. The integration of AI-driven automation, IoT proliferation, and edge computing will support emerging applications, such as extended reality (XR), autonomous systems, and space-air-ground integrated networks [3]. However, these innovations introduce greater architectural complexity and security risks, necessitating adaptive and intelligent frameworks to mitigate the evolving threats [1].

Although SDN enhances flexibility and programmability, its centralized control plane and dynamic nature pose security risks, including DDoS attacks, control plane hijacking, and adversarial AI threats [4]. Securing highly heterogeneous 6G environments requires advanced mechanisms, such as Zero-Trust Architecture (ZTA), blockchain-based trust management, AI-powered threat detection, Post-Quantum Cryptography (PQC), and secure network slicing. This study explores SDN's role of SDN in 6G, focusing on its applications in network automation, slicing, and intelligent traffic management while addressing critical security concerns and emerging protective technologies. It also examines open research challenges, such as cross-slice security risks, AI-driven adversarial threats, and resource-efficient security mechanisms, outlining future directions for developing adaptive SDN security frameworks for next-generation networks.

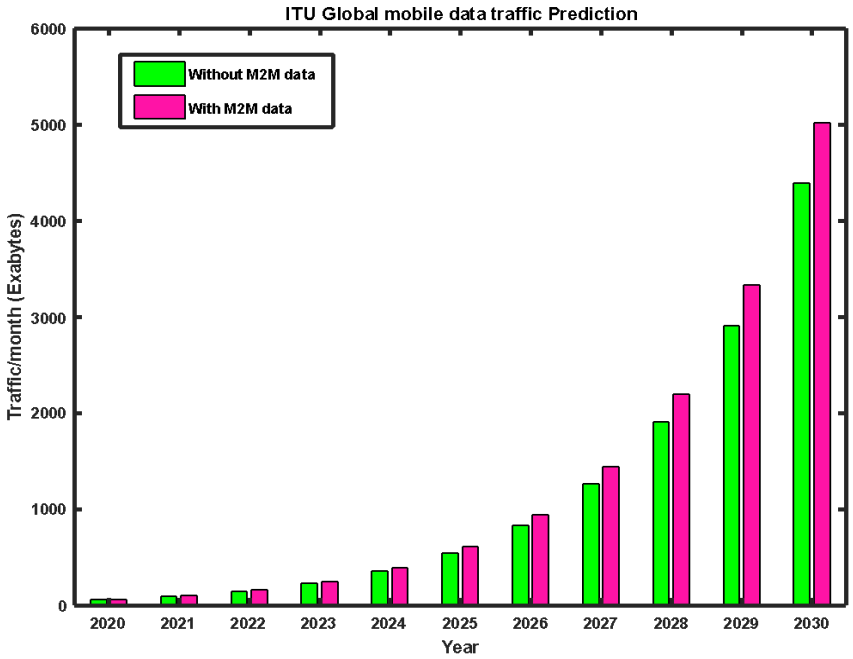

Fig. 1 *ITU global mobile data traffic prediction*

Table 1 *Key differences between 5G and 6G networks*

Feature	5G Networks	6G Networks
Frequency Band	3-300 GHz	Up to 1 THz
Uplink Speed	10 Gbps	1 Tbps
Downlink Speed	20 Gbps	1 Tbps
Network Reliability	10^{-5} Failure	1^{-9} Failure
User-Latency	0.5 ms	0.1 ms
C-Plane Latency	10 ms	1 ms
Data Traffic Density	10 Mbps/m^2	1-10 Gbps
Location Accuracy	10 cm in 2D	1 cm in 3D
AI-Integration Level	Partially	Fully

2. SDN in 6G: Opportunities and Applications

Security is a critical requirement in 6G networks because of their dense, heterogeneous, and software-defined architecture, as illustrated in Fig. 2. The integration of SDN controllers, relay nodes, small cells, machine-to-machine gateways, edge users, and massive Internet of Things devices significantly expands the attack surface

Int. Journal of Integrated Engineering Vol. 18 No. 1 (2026) p. 202-214

across both wireless and backhaul segments. Because the SDN controller centrally manages network operations, it represents a high-value target. A successful compromise can disrupt large-scale communication services and simultaneously affect multiple network domains. Furthermore, emerging 6G services, including ultralow-latency applications, device-to-device communication, edge computing, and artificial-intelligence-driven functions, demand stringent guarantees of confidentiality, integrity, availability, and trust management. In the absence of robust protection mechanisms across the application, control, and infrastructure layers, threats such as distributed denial-of-service attacks, signaling manipulation, device spoofing, and backhaul intrusion may severely degrade reliability and service continuity. Therefore, security in 6G networks must be intelligent, adaptive, and tightly integrated throughout the architecture to ensure resilient and trustworthy next-generation connectivity.

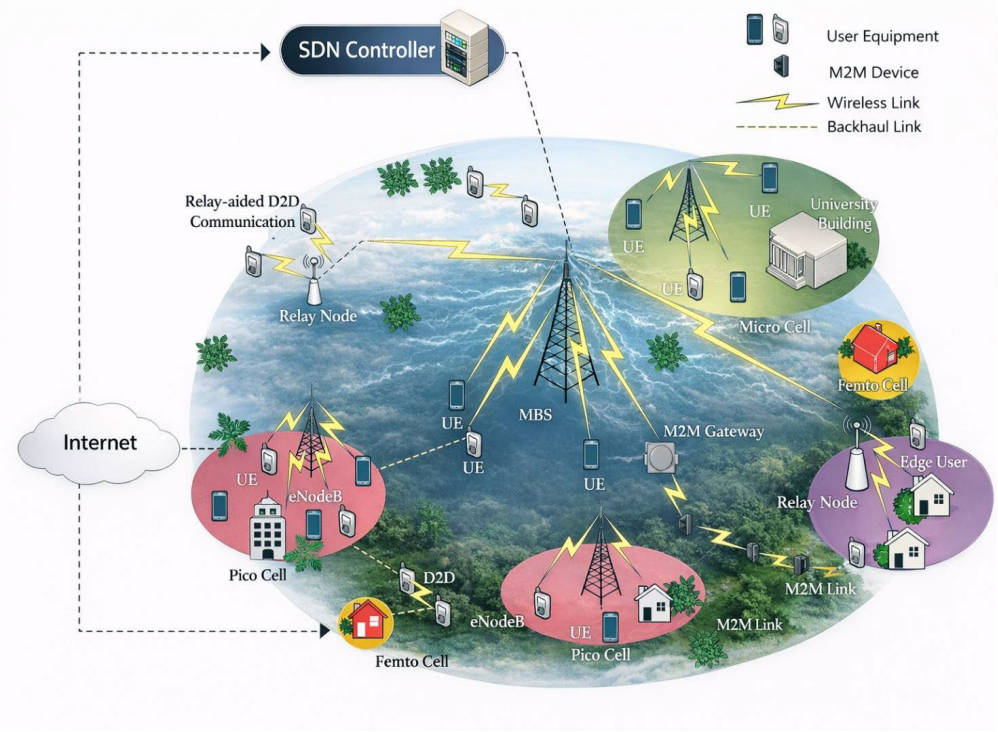

Fig. 2 *SDN-enabled 6G network architecture illustrating centralized control, heterogeneous cells, relay nodes, M2M communication, and integrated wireless and backhaul links*

This section discusses how SDN supports critical 6G features, such as ultra-low latency, intelligent resource allocation, and edge computing integration. It also explores emerging use cases enabled by SDN, including smart cities, autonomous vehicles, industrial automation, and non-terrestrial network integration.

2.1 Role of SDN in 6G

SDN is a cornerstone technology in the evolution of 6G networks, offering the flexibility, programmability, and centralized control required to meet the diverse and demanding requirements of next-generation communication systems. This section highlights how SDN supports critical 6G features.

- **Network Slicing:** SDN plays a vital role in enabling network slicing, which allows multiple virtual networks to operate on a shared infrastructure. This capability supports diverse applications, such as URLLC for critical use cases like autonomous driving and remote surgery [1]. SDN's centralized control enables real-time monitoring and management of network slices, ensuring efficient resource allocation and maintaining high service quality.
- **Ultra-Low Latency:** One of SDN's most significant contributions to 6G is its ability to optimize data routing, which reduces delays and achieves ultra-low latency. This is critical for applications such as AR and VR, where even small delays can degrade user experience. Additionally, SDN prioritizes traffic for latency-sensitive services, ensuring these applications receive sufficient bandwidth and low-latency paths even under heavy network load.
- **AI and Machine Learning Integration:** SDN provides an ideal platform for integrating AI and ML into 6G networks. These technologies enable real-time analysis of network conditions and predictive resource

management, allowing SDN to allocate resources dynamically and optimize performance across various applications. Moreover, SDN's programmability facilitates automated decision-making processes powered by AI, enhancing network efficiency and responsiveness without requiring manual intervention.

- **Dynamic Resource Allocation (DRA):** DRA is another key feature enabled by SDN. Its centralized control framework supports real-time adjustments to accommodate fluctuations in demand, ensuring efficient resource utilization. This capability also enables scalable resource management, allowing operators to adjust resources as needed for both high-demand and less intensive applications.
- **Edge Computing:** SDN is instrumental in supporting edge computing, which processes data closer to end-users to reduce latency and enhance service delivery. By integrating edge computing resources seamlessly into the network, SDN ensures latency-sensitive applications benefit from immediate data processing [1]. Additionally, SDN's real-time monitoring capabilities allow for intelligent load balancing across edge nodes, ensuring computational resources are utilized effectively.

2.2 Emerging Use Cases of SDN in 6G

Fig. 3 illustrates the pivotal role of SDN in enabling emerging 6G use cases through the integration of the application, control, and infrastructure layers in a unified architectural framework. In 6G environments, ultra-dense deployments, including pico cells, femto cells, relay nodes, machine-to-machine gateways, and massive base stations, generate highly dynamic and heterogeneous traffic from user equipment and machine-to-machine devices. This complexity necessitates flexible, programmable, and intelligent network management mechanisms. Furthermore, Logically centralized controllers within the control layer provide a global view of the network and enable dynamic configuration through southbound and east-west-bound interfaces. This facilitates the real-time optimization of wireless and backhaul links, efficient resource allocation, and adaptive traffic management across diverse service requirements.

In addition, by decoupling the control and data planes, SDN enhances scalability, reduces latency, and improves reliability across both the core and edge segments of the network. Consequently, it supports advanced 6G applications, including holographic communication, tactile Internet services, autonomous systems, massive Internet of Things orchestration, and artificial intelligence-driven network slicing. Overall, as shown in Fig. 3, Software Defined Networking serves as a foundational technology for the realization of adaptive and self-optimizing 6G ecosystems.

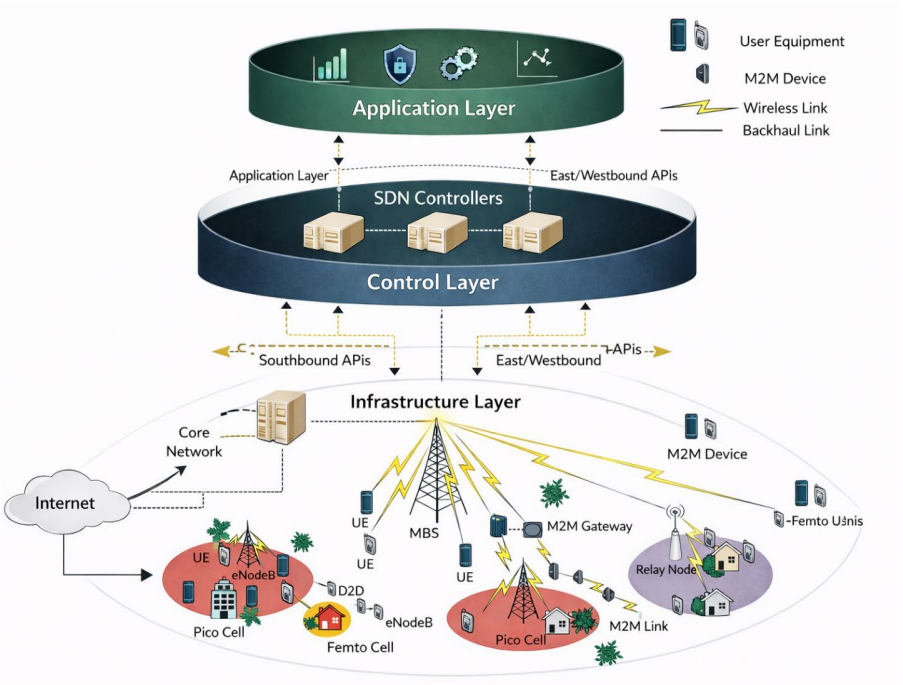

Fig. 3 *SDN-enabled 6G architecture showing application, control, and infrastructure layers with heterogeneous wireless components and API-based connectivity*

As 6G technology evolves, SDN is expected to play a transformative role in enabling diverse and innovative applications. This section explores some of the most promising use cases.

- **Smart Cities:** SDN has significant potential to enhance the infrastructure and services of smart cities. It enables dynamic traffic management by optimizing traffic flows and reducing congestion through real-time routing strategies. In energy management, SDN-powered smart grids can optimize energy distribution based on demand, promoting efficiency and sustainability. Additionally, SDN streamlines public safety measures by integrating surveillance systems and emergency response services, ensuring swift and coordinated responses to incidents.
- **Autonomous Vehicles:** In the context of autonomous vehicles, SDN facilitates seamless real-time communication between vehicles and infrastructure (V2I), enabling updates on road conditions, traffic signals, and potential hazards. It also supports cooperative driving through vehicle-to-vehicle (V2V) communication, allowing vehicles to coordinate maneuvers and improve traffic safety and flow. SDN's capability to create dedicated virtual networks ensures low-latency communication essential for safe and reliable autonomous vehicle operation.
- **Industrial Automation:** The integration of SDN in 6G networks offers significant advancements for industrial automation. SDN enhances smart manufacturing by interconnecting machines and systems, enabling real-time monitoring and predictive to optimize productivity. Its advanced analytics capabilities improve supply chain efficiency by enabling better resource allocation and operational visibility. Furthermore, SDN's low-latency connections enable remote operations, allowing experts to manage industrial processes from any location.
- **Integration with Non-Terrestrial Networks:** SDN simplifies the integration of non-terrestrial networks (NTNs), such as satellites, with terrestrial infrastructure, enabling seamless global connectivity across diverse environments. This capability is particularly valuable for disaster recovery scenarios, where NTNs can maintain critical communication links when terrestrial networks fail. Additionally, combining NTNs with SDN facilitates the deployment of IoT devices in remote areas, extending connectivity to underserved regions.

3. Security Challenges in SDN for 6G

Table 2 summarizes the security challenges in 6G.

3.1 Distributed Architecture and Scalability

In 6G-enabled SDN networks, distributed controllers enhance scalability but also introduce cyber risks such as synchronization issues, inter-controller trust gaps, and DDoS vulnerabilities. Unlike traditional centralized SDN, which relies on a single controller, distributed SDN requires secure coordination betweenen multiple controllers to maintain network integrity. Blockchain-integrated SDN (blockchain-SDN) has emerged as a decentralized solution that reduces single points of failure and improves trust [5]. However, the controller synchronization overhead can increase latency, causing performance bottlenecks. HybCon, a hybrid SDN-cloud architecture, leverages multipriority queuing to optimize path computation delays [6]. Similarly, ML-based SDN frameworks such as the EQUI-dispatcher model employ graph neural networks (GG-Rec-NNs) to improve controller workload balance and security [7]. In addition, SDN-based Ethernet architectures remain susceptible to broadcast traffic amplification, exacerbating congestion and security threats. A floodless SDN approach using a multistage security algorithm mitigates ARP-based attacks and minimizes excess broadcast traffic [2].

3.2 Diverse Threat Landscape in SDN Security for 6G

The 6G era introduced an expanded and more complex threat landscape for SDN, particularly with the integration of AI-powered cyberattacks, IoT-driven vulnerabilities, and distributed denial-of-service (DDoS) threats. These threats demand autonomous, AI-driven, and blockchain-enhanced security solutions to protect SDN-enabled 6G infrastructure. *Razaque et al.* [8] proposed Zero-trust models with AI-based anomaly detection will be essential in mitigating automated AI-driven attacks and ensuring real-time visibility across 6G network endpoints. Whereas, in [10] introduces a dual-layer closed-loop autonomous system that enables "self-protection against large-scale DDoS threats" by integrating "Digital Service Providers (DSPs)" and "Infrastructure Service Providers (ISPs)" to ensure real-time threat collaboration. Furthermore, the authors in [9] and [11] proposed "Deep Learning (DL)-Assisted Security Function Virtualization (SFV)" and "Software-Defined Security (SDS) architectures" to dynamically detect, localize, and neutralize security threats using AI-driven mechanisms.

3.3 Data Privacy and Trust in SDN for 6G Networks

Ensuring data privacy and trust in 6G-enabled SDN is critical due to increased network disaggregation, multi-stakeholder environments, and AI-driven automation [20]. *Latif et al.* [12] proposed a "blockchain-integrated SDN security method" that eliminates "proof of work (PoW)" and replaces it with public-private blockchain

mechanisms for trust-based authentication. Their results showed improved energy efficiency and throughput and reduced packet latency, making it viable for next-generation industrial networks. *Xiegler et al.* [13] highlights the need for automated closed-loop security operations, where "AI-driven privacy-preserving technique" and "quantum-safe security" ensure network-wide trustworthiness. Finaly *Lupez et al*. [14] introduces a "trust-driven privacy orchestration framework", where smart contracts and distributed ledgers track proof of transit and service execution transparency. RL-driven privacy-aware orchestration helps optimize the trust levels for different network entities.

3.4 Control Plane Risks in SDN for 6G

In 6G SDN, the centralized control plane is increasingly vulnerable to sophisticated cyber threats, requiring robust security mechanisms. Many efforts have been made to explore controller risks to make top priorities. For example, *Soltani et al.* [15] proposed a "RAN Intelligent Controller (RIC)" in an Open RAN that plays a vital role in enhancing flexibility and efficiency. However, its programmability introduces new attack vectors, particularly, controller hijacking and data manipulation. *Eugster et al*. [16] reported that 6G SDN integrates multiple network technologies, leading to highly dynamic and complex control architectures. In addition, *Abdulqadder et al*. [17] network slicing in "SDN/NFV 6G" introduced security risks due to multi-tenant environments. However, there are still some challenges, including unauthorized access to slices, which leads to data leakage and service disruption.

3.5 AI-Powered Attacks in SDN for 6G

With the rise of AI-driven security mechanisms in SDN, attackers are leveraging AI techniques to create more sophisticated attacks. 6G SDN must adopt advanced AI-driven countermeasures to defend against AI-enhanced cyber threats. AI can be used for both security enhancement and attack automation as presented by *Ahammadi et al*. [18]. Currently, attackers employ adversarial AI techniques to manipulate SDN security policies. *Ko et al*. [19] discussed AI-powered DDoS attacks targeting SDN controllers. Nevertheless, *Pari et al.* [4] mentioned that AI methods are now used to detect flooding attacks in SDN environments. The authors proposed Multi-model AI frameworks that use ensemble learning to enhance the detection accuracy. However, this framework cannot distinguish legitimate high-traffic flows from malicious flooding attacks.

Table 2 *Summary of SDN security challenges in 6G*

Ref	Key Focus and Contribution	Security Objective	Mitigation Approach
[5]	Blockchain-SDN for IoT security; decentralized trust, reducing failure	Confidentiality, Integrity	Blockchain authentication
[6]	Multi-controller SDN for scalability; priority-based queueing for fast path	Availability, Scalability	Distributed control
[7]	ML-driven SDN controller load balancing using Graph Neural Networks	Integrity, Scalability	AI-based anomaly detection
[2]	Floodless SDN-based; multi-stage filtering for ARP attack prevention	Availability, Integrity	Traffic filtering
[8]	Blockchain-SDN trust model; VNF-SDN with blockchain threat filtration	Confidentiality, Integrity	Blockchain and filtering
[9]	AI-based SDN security; DL-assisted threat detection and mitigation	Availability, Integrity	AI-driven anomaly detection
[10]	Self-protecting SDN for DDoS; autonomous service layer mitigation	Availability, Scalability	Self-healing loops
[11]	AI-driven SDS for OT-IT security; anomaly detection	Confidentiality, Integrity	AI-powered SDS for IIoT/CPS
[12]	Blockchain-SDN trust model; decentralized authentication for SDN	Confidentiality, Integrity	P2P blockchain authentication
[13]	AI-enhanced SDN privacy; AI-driven trust and privacy preservation	Trust, Privacy, Security	AI-based closed-loop security

Int. Journal of Integrated Engineering Vol. 18 No. 1 (2026) p. 202-214

Ref	Key Focus and Contribution	Security Objective	Mitigation Approach
[14]	Intent-driven privacy in SDN; RL-based smart contracts for privacy	Privacy, Availability	Smart contracts, RL-based
[15]	Open RAN SDN risks; RIC vulnerabilities	Integrity, Availability	Zero Trust for SDN controllers
[16]	Robust SDN control; self-healing secure routing updates	Availability, Scalability	AI-driven anomaly detection
[17]	Secure SDN slicing; AI-based controller load balancing	Confidentiality, Integrity	Blockchain authentication
[18]	AI-based threats in SDN; adversarial ML attack risks	Confidentiality, Integrity	Adversarial AI detection
[19]	AI-powered DDoS detection; comparative AI model analysis	Availability, Integrity	RF-based ML detection
[20]	AI-driven network flooding detection; multi-model AI for SDN security	Availability, Scalability	Real-time AI-based defense

4. Emerging Technologies for Enhancing SDN Security in 6G

Security in SDN for 6G requires advanced solutions to address evolving cyber threats. As illustrated in Fig. 4, five key emerging technologies play a crucial role in enhancing SDN security. These technologies (see in Table 3) collectively enhance SDN security by providing proactive, intelligent, and scalable solutions to safeguard the next-generation networks.

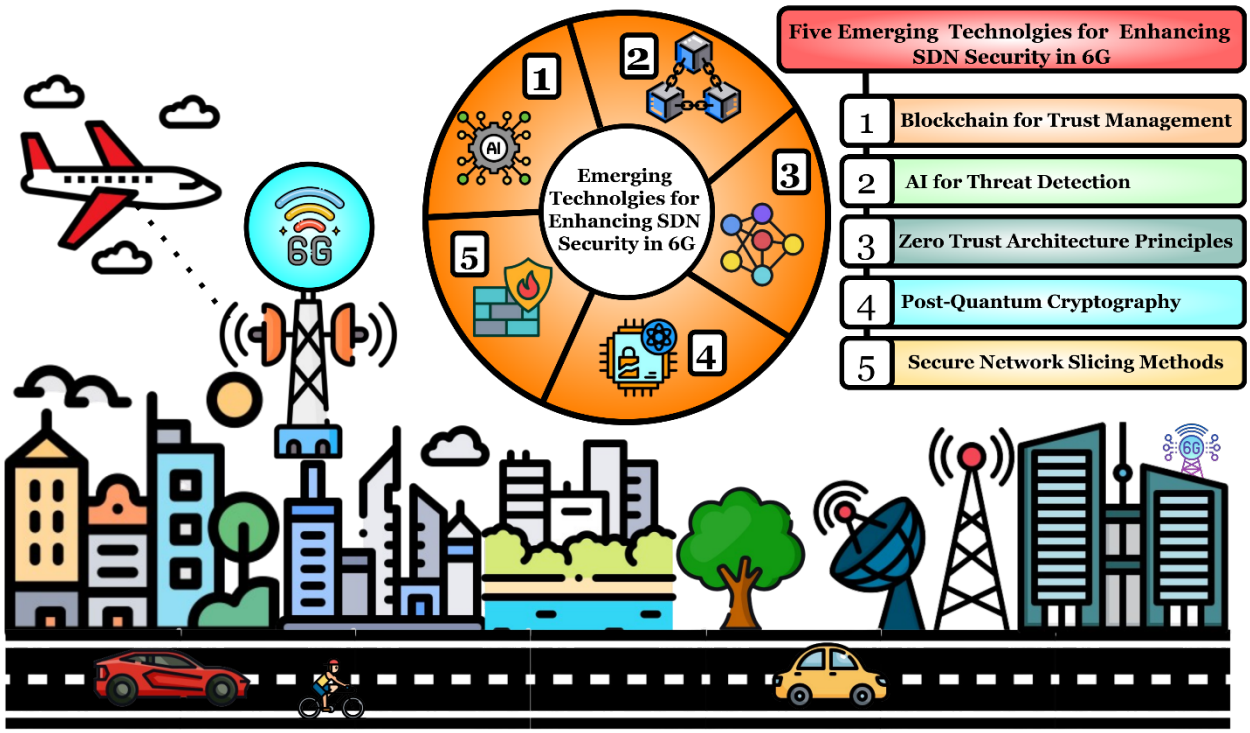

Fig. 4 *Overview of emerging technologies for enhancing SDN security in 6G*

4.1 Blockchain for Trust Management

The integration of blockchain with SDN enhances trust management, security, and resource efficiency in 6G IoT ecosystems. As hyperconnected environments introduce new security challenges, blockchain provides tamper-

proof identity verification, decentralized authentication, and secure communication channels. For instance, *Hameed et al*. [21] proposed "storing IoT device identities, public keys, and trust indices" on a blockchain to ensure immutability and tamper resistance. *Rahman et al.* [22] presented an optimized, energy-efficient blockchain-SDN framework designed for secure resource management in 6G environments. 6G introduces high-speed AI-powered network slicing, but trust issues arise owing to dynamic resource allocation and cross-slice security risks. *Alkawai* and *Yadav* [23] proposed a blockchain-based method for context-aware user authentication and handover management in 6G IoT networks. The framework reduces latency by 17.33% compared with existing blockchain security models. Furthermore, *Chelghoum et al*. [24] introduced a Collaborative IDS that utilizes AI-driven threat intelligence sharing across IoT nodes.

4.2 Artificial Intelligence (AI) for Threat Detection

AI plays a critical role in automating, optimizing, and enhancing threat detection in SDN-based 6G networks. *Khan et al*. [25] proposes a hybrid DL-based congestion control mechanism using "Long Short-Term Memory (LSTM)" and "Support Vector Machine (SVM)" to analyze real-time traffic patterns. The proposed technique achieved 93.23% accuracy in congestion and anomaly detection. In [26] an "intelligent zero-trust architecture (i-ZTA)" was introduced for 6G SDN networks, leveraging ML to dynamically evaluate risk and secure SDN components. Furthermore, authors in [27] presented an ML-powered SDN framework that monitored abnormal traffic fluctuations in multimedia streams. *Khalid et al*. [28] proposed "Deep Neural Networks (DNNs)" for joint multi-slice security management. To ensure resource integrity across slices, unauthorized breaches were prevented in 6G networks.

4.3 Zero-Trust Architecture (ZTA) in SDN for 6G

As 6G networks become more open and heterogeneous, ZTA has emerged as a critical security paradigm for SDN. *Ramez* and *Jahannath* [29] discussed i-ZTA, which is an AI-driven security framework designed for untrusted 5G/6G environments. It enables adaptive access control and reduces exposure to insiders and external threats. *Chen et al*. [30] proposed adaptive security across SDN control domains to counteract DDoS, malware, and zero-day exploits. The simulation results demonstrated improved resilience against cyber-attacks. *Enright et al*. [31] presented "digital forensic monitoring" for detecting and preventing insider attacks. The proposed model creates a self-learning ZTA system, making 6G networks more resilient to evolving cyber threats.

Table 3 *Emerging technologies for enhancing SDN security in 6G: layered framework approach*

Ref	Layer	Technology Used	Role in Trust Management	Advantages
[21]	Application	AI-based trust evaluation	Detects adversarial, Zero-day attack prevention	Improved adaptability, self-learning security
[22]	Control	Blockchain-enabled	Verifies SDN controller, Secure key management	Reduces unauthorized, Decentralized trust
[23]	Data	Secure flow-rule logging	Prevents rogue switch manipulation, Enforces trust	Ensures consistent SDN policies
[24]	Control	Blockchain-backed handover	Trust enforcement in cross-domain SDN slices	Seamless authentication, Enhances privacy
[25]	Control	Hybrid Deep Learning	Prevents network congestion attacks	93.23% accuracy, prevents overloading
[26]	Application	Zero Trust Architecture	Dynamic risk assessment	Real-time adaptive security policies
[27]	Control	QoE-based threat monitoring	Improves QoE-based security, mitigates cyber threats	Improves QoE-based security
[28]	Data	AI-driven traffic prediction	SLA security enforcement using GRU-DNN models	Optimized resource security reduces attacks
[29]	Application	I-ZTA architecture	Monitors security state and evaluates risks	Real-time security assurance

Ref	Layer	Technology Used	Role in Trust Management	Advantages
[30]	Control	Software-defined ZTA	Prevents malicious access behaviors	Elastic, scalable, and more resilient access
[31]	Network	ZTA with real-time detection	Enhances trust validation through AI-driven	Proactive and self-learning security
[32]	Control	Quantum Key Distribution	Provides quantum-safe SDN communication	Mitigates quantum threats in SDN
[33]	Application	PQC using NTRU algorithm	Enhances blockchain security for SDN services	Trust in multi-cloud SDN environments
[34]	Data	NSP with OVS	Enforces zero-touch security	Supports up to 2048 slices
[35]	Control	AI-native network slicing	Security management using AI	Autonomous threat mitigation

4.4 Post-Quantum Cryptography (PQC) in SDN for 6G

With the rise of quantum computing, traditional cryptographic methods, such as RSA and ECC, are becoming vulnerable to quantum attacks. The PQC provides quantum-resistant encryption to protect the SDN control and data planes in 6G networks. *Garcia et al*. [32] introduces "Quantum Key Distribution (QKD)" and "PQC" to enhance SDN security. It protects SDN controller authentication and secure routing protocols. *Zeydan et al*. [33] explored the integration of PQC into "blockchain-driven SDN" service orchestration. This method improves trust management across multiple cloud SDN domains. Limited research on PQC-SDN integration requires more studies on the impact of PQC overhead on SDN controller performance and hybrid cryptographic models combining classical, PQC, and QKD.

4.5 Secure Network Slicing in SDN for 6G

Network slicing is a fundamental security mechanism in 6G SDN that enables multitenant, multidomain network isolation to mitigate cyber threats [17]. *Escolar et al*. [34] proposed "Network Self-Protection (NSP)" with an "Open Virtual Switch (OVS)" that enables dynamic traffic isolation to separate legitimate and malicious flows. *Wu et al*. [35] discussed an "AI native network slicing framework" that leverages AI across the slicing lifecycle for real-time resource allocation and security enforcement. Further studies are required in this area first, Need for hybrid AI-PQC integration to secure slices against quantum-based cyber threats. Second, the Performance trade-offs in large-scale slice deployments require further exploration.

5. Research Challenges and Future Directions

Despite their transformative potential, SDN-driven 6G networks face critical security challenges because of their programmable nature, dynamic resource allocation, and AI-driven operations. Below are some of the key unresolved security challenges in SDN for 6G.

- Ensuring low-latency, real-time decision making while securing inter-controller communication remains a major challenge [41].
- AI is both an enabler and a threat to 6G networks. Attackers can exploit AI-driven SDN mechanisms by launching adversarial ML-based evasion [21], [38]-[40].
- AI-powered malware and polymorphic attacks can manipulate SDN policies in real time, leading to traffic redirection, or network hijacking [36], [37].
- SDN relies on secure key exchanges that can be compromised by quantum-enabled cryptanalysis [3], [41]-[44].
- Multitenant network slicing in 6G increases the risk of cross-slice, unauthorized, and traffic eavesdropping [45]-[49].
- Attackers can exploit resource-constrained edge devices, launch edge-based DDoS attacks [50]-[55].

Future studies on SDN security in 6G should focus on building secure and resilient SDN-driven 6G ecosystems. The key potential areas are as follows.

- Development of self-learning AI models that enable predictive threat detection in SDN environments [56].
- PQC algorithms are tailored for SDN-based authentication and encryption [57].

- QKD for SDN controllers to establish tamper-proof, quantum-resistant key exchanges [58].
- ZTNS techniques that restrict unauthorized movement between slices [59].
- Blockchain-based decentralized trust management to secure inter-controller authentication and policy enforcement [60].

6. Conclusion

This review confirms that Software-Defined Networking (SDN) is a foundational enabler for achieving the stringent performance requirements of 6G, particularly ultra-low latency targets of 0.1 ms at the air interface and below 1 ms end-to-end. The surveyed studies consistently demonstrate that centralized control, intelligent traffic engineering, AI-driven optimization, blockchain-assisted trust management, and programmable data planes collectively enhance resource allocation efficiency and dynamic network adaptability. These capabilities are essential for supporting emerging 6G use cases, such as the tactile Internet, holographic communications, massive IoT, and autonomous systems. However, despite these advancements, several critical challenges remain. Scalability is a primary concern because managing thousands of heterogeneous nodes through centralized SDN controllers may introduce control plane bottlenecks and latency overhead. Security vulnerabilities, controller reliability, inter-domain orchestration, and limited exploration of data plane intelligence further complicate practical deployment. Notably, the majority of existing research concentrates on the control and application layers, whereas the data plane, particularly programmable and AI-assisted forwarding mechanisms, remains underexplored. From our perspective, SDN-enabled 6G networks must move toward distributed intelligent architectures that combine centralized orchestration with edge-level autonomy. Integrating AI-native control, programmable hardware acceleration, zero-trust security frameworks, and scalable controller federation is essential. Therefore, SDN in 6G should not only be viewed as a latency optimization tool but also as a holistic architectural paradigm requiring cross-layer innovation to ensure resilience, scalability, and trustworthiness in next-generation networks.

Acknowledgement

This work was supported by the Ministry of Higher Education (MOHE) through Fundamental Research Grant Scheme under Grant FRGS/1/2022/TK07/UTHM/02/25.

Conflict of Interest

Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: Abdinasir Hirsi: ***Conceptualization of this study, Methodology, Software, Investigation, Writing original draft, Formal analysis, Visualization, Conceptualization, Validation, writing, review and editing****. Lukman Audah:* ***Supervison, Project administration, Conceptualization, review and editing****. Adeb Salh:* ***Reviewing original draft, Data curation, supervision****. Mohammed Alhartomi:* ***Ensuring data integrity and quality****. Nan Mad Sahar:* ***Ensurin ethical standards and approvals are met.*** *Salman Ahmed:* ***Modification for the final layout.***

References

[1] S. Elmeadawy and R. M. Shubair, “6g wireless communications: Future technologies and research challenges,” in 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA), 2019, pp. 1–5.

[2] M. N.Munther, F. Hashim, N. A. A. Latiff, K. A. Alezabi, and J. T. Liew, “Scalable and secure sdn based ethernet architecture by suppressing broadcast traffic,” Egyptian Informatics Journal, vol. 23, no. 1, pp. 113126, 2022.

[3] A. Hirsi et al., "Deep Learning for Enhanced DDoS Detection in Software-Defined Networks: A Review," 2025 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarang, Indonesia, 2025, pp. 286-291, doi: 10.1109/ISemantic67418.2025.11292030.

[4] S. Neelavathy Pari, E. C. Ritika, B. Ragul, and M. Bharath, “Ai-based network flooding attack detection in sdn using multiple learning models and controller,” in 2023 12th International Conference on Advanced Computing (ICoAC), 2023, pp. 1–7.

[5] M. J. Islam, A. Rahman, S. Kabir, M. R. Karim, U. K. Acharjee, M. K. Nasir, S. S. Band, M. Sookhak, and S. Wu, “Blockchain-sdn-based energy-aware and distributed secure architecture for iot in smart cities,” IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3850–3864, 2021.

[6] D. A. Chekired, M. A. Togou, and L. Khoukhi, "Hybcon: A scalable sdn based distributed cloud architecture for 5g networks," IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 550–563, 2021.

[7] A. Ashraf, Z. Iqbal, M. A. Khan, U. Tariq, S. Kadry, and S.-o. Park, "Scalable offloading using machine learning methods for distributed multi-controller architecture of sdn networks," The Journal of Supercomputing, vol. 78, no. 7, pp. 10191–10210, 2022.

[8] A. Razaque, J. Yoo, G. Bektemyssova, M. Alshammari, T. T. Chinibayeva, S. Amanzholova, A. Alotaibi, and D. Umutkulov, "Efficient internet-of-things cyberattack depletion using blockchain-enabled software-defined networking and 6g network technology," Sensors, vol. 23, no. 24, p. 9690, 2023.

[9] M. A. Rahman and M. S. Hossain, "A deep learning assisted software defined security architecture for 6g wireless networks: Iiot perspective," IEEE Wireless Communications, vol. 29, no. 2, pp. 52–59, 2022.

[10] P. Benlloch-Caballero, Q. Wang, and J. M. A. Calero, "Distributed dual layer autonomous closed loops for self-protection of 5g/6g iot networks from distributed denial of service attacks," Computer Networks, vol. 222, p. 109526, 2023.

[11] A. Rahman and M. S. Hossain, "A deep learning assisted software defined security architecture for 6g wireless networks: Iiot perspective," IEEE Wireless Communications, vol. 29, no. 2, pp. 52–59, 2022.

[12] S. A. Latif, F. B. X. Wen, C. Iwendi, F. W. Li-Li, 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, vol. 181, pp. 274–283, 2022.

[13] V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, "Security and trust in the 6g era," IEEE Access, vol. 9, pp. 142314–142327, 2021.

[14] J. A. Alonso-Lupez, L. A. M. Hern´ andez, S. P. Arteaga, A. L. S. Orozco, L. J. G. Villalba, A. Pastor, and D. L. Garc´ ıa, "Level of trust and privacy management in 6g intent-based networks for vertical scenarios," in 2022 1st International Conference on 6G Networking (6GNet), 2022, pp. 1–4.

[15] S. Soltani, A. Amanloo, M. Shojafar, and R. Tafazolli, "Intelligent control in 6g open ran: Security risk or opportunity?" IEEE Open Journal of the Communications Society, vol. 6, pp. 840–880, 2025.

[16] P. Eugster, "Toward robust control for 6g networks," IEEE Network, vol. 38, no. 3, pp. 254–260, 2024.

[17] I. H. Abdulqadder and S. Zhou, "Sliceblock: Context-aware authentication handover and secure network slicing using dag-blockchain in edge-assisted sdn/nfv-6g environment," IEEE Internet of Things Journal, vol. 9, no. 18, pp. 18079–18097, 2022.

[18] A. Ahammadi, W. H. Hassan, and Z. A. Shamsan, "An overview of artificial intelligence for 5g/6g wireless networks security," in 2022 International Conference on Cyber Resilience (ICCR), 2022, pp. 1–6.

[19] K.-M. Ko, J.-M. Baek, B.-S. Seo, and W.-B. Lee, "Comparative study of ai-enabled ddos detection technologies in sdn," Applied Sciences, vol. 13, no. 17, p. 9488, 2023.

[20] A. F. Samatar, A. Hirsi, A. M. Omar, and M. J. Abdiaziz, "Investigating ddos attack mitigation strategies and simulation tools using gns3," in 2024 FORTEI-International Conference on Electrical Engineering (FORTEI-ICEE), 2024, pp. 142–147.

[21] S. Hameed, S. A. Shah, Q. S. Saeed, S. Siddiqui, I. Ali, A. Vedeshin, and D. Draheim, "A scalable key and trust management solution for iot sensors using sdn and blockchain technology," IEEE Sensors Journal, vol. 21, no. 6, pp. 8716–8733, 2021.

[22] A. Rahman, M. J. Islam, A. Montieri, M. K. Nasir, M. M. Reza, S. S. Band, A. Pescape, M. Hasan, M. Sookhak, and A. Mosavi, "Smartblock sdn: An optimized blockchain-sdn framework for resource management in iot," IEEE Access, vol. 9, pp. 28361–28376, 2021.

[23] L. M. Alkwai and K. Yadav, "Blockchain-based secure 5g/6g communication for internet of things devices in consumer electronic systems," IEEE Transactions on Consumer Electronics, vol. 70, no. 3, pp. 63276338, 2024.

[24] M. Chelghoum, G. Bendiab, M. A. Labiod, M. Benmohammed, S. Shiaeles, and A. Mellouk, "Blockchain and ai for collaborative intrusion detection in 6g-enabled iot networks," in 2024 IEEE 25th International Conference on High Performance Switching and Routing (HPSR), 2024, pp. 179–184.

[25] S. Khan, A. Hussain, S. Nazir, F. Khan, A. Oad, and M. D. Alshehri, "Efficient and reliable hybrid deep learning-enabled model for congestion control in 5g/6g networks," Computer Communications, vol. 182, pp. 31–40, 2022.

[26] K. Ramezanpour and J. Jagannath, “Intelligent zero trust architecture for 5g/6g networks: Principles, challenges, and the role of machine learning in the context of o-ran,” Computer Networks, vol. 217, p. 109358, 2022.

[27] A. A. Barakabitze and R. Walshe, “Sdn and nfv for qoe-driven multimedia services delivery: The road towards 6g and beyond networks,” Computer Networks, vol. 214, p. 109133, 2022.

[28] A. Khalid, R. G. Anand, and A. Malviya, “A development of dynamic end-to-end slicing network along with the offline sla-method integrated with deep learning for 5g/6g networks,” in 2024 1st International Conference on Innovative Sustainable Technologies for Energy, Mechatronics, and Smart Systems (ISTEMS), 2024, pp. 1–5.

[29] K. Ramezanpour and J. Jagannath, “Intelligent zero trust architecture for 5g/6g networks: Principles, challenges, and the role of machine learning in the context of o-ran,” Computer Networks, vol. 217, p. 109358, 2022.

[30] X. Chen, W. Feng, N. Ge, and Y. Zhang, “Zero trust architecture for 6g security,” IEEE Network, vol. 38, no. 4, pp. 224–232, 2024.

[31] M. A. Enright, E. Hammad, and A. Dutta, “A learning-based zero-trust architecture for 6g and future networks,” in 2022 IEEE Future Networks World Forum (FNWF), 2022, pp. 64–71.

[32] C. R. Garc´ıa, S. Rommel, J. J. V. Olmos, and I. T. Monroy, “Enhancing the security of software defined networks via quantum key distribution and post-quantum cryptography,” in International Symposium on Distributed Computing and Artificial Intelligence. Springer, 2023, pp. 428–437.

[33] E. Zeydan, J. Baranda, and J. Mangues-Bafalluy, “Post-quantum blockchain-based secure service orchestration in multi-cloud networks,” IEEE Access, vol. 10, pp. 129520–129530, 2022.

[34] A. M. Escolar, J. B. Bernabe, J. M. A. Calero, Q. Wang, and A. Skarmeta, “Network slicing as 6g security mechanism to mitigate cyber-attacks: the rigourous approach,” in 2024 IEEE 10th International Conference on Network Softwarization (NetSoft), 2024, pp. 387–392.

[35] W. Wu, C. Zhou, M. Li, H. Wu, H. Zhou, N. Zhang, X. S. Shen, and W. Zhuang, “Ai-native network slicing for 6g networks,” IEEE Wireless Communications, vol. 29, no. 1, pp. 96–103, 2022.

[36] A. Hirsi, L. Audah, A. Salh, N. M. Sahar, S. Ahmed, and M. A. Alhartomi, “Ddos anomaly detection in software-defined networks: An evaluation of machine learning techniques for traffic classification and prediction,” in 2024 International Conference on Future Technologies for Smart Society (ICFTSS), 2024, pp. 100–105

[37] A. Hirsi, M. A. Alhartomi, L. Audah, A. Salh, N. M. Sahar, S. Ahmed, G. O. Ansa, and A. Farah, “Comprehensive analysis of ddos anomaly detection in software-defined networks,” IEEE Access, vol. 13, pp. 23 013–23 071, 2025.

[38] Alsalem, T., & Amin, M. (2023). Towards Trustworthy IoT Systems: Cybersecurity Threats, Frameworks, and Future Directions. Journal of Cyber Security and Risk Auditing, 2023(1), 3–18. https://doi.org/10.63180/jcsra.thestap.2023.1.2

[39] Almedires, M. A., Elkhalil, A., & Amin, M. (2025). Adversarial Attack Detection in Industrial Control Systems Using LSTM-Based Intrusion Detection and Black-Box Defense Strategies. Journal of Cyber Security and Risk Auditing, 2025(3), 4–22. https://doi.org/10.63180/jcsra.thestap.2025.3.2

[40] Alshuaibi, A., Arshad, M. W., & Maayah, M. (2025). A Hybrid Genetic Algorithm and Hidden Markov Model-Based Hashing Technique for Robust Data Security. Journal of Cyber Security and Risk Auditing, 2025(3), 42–56. https://doi.org/10.63180/jcsra.thestap.2025.3.6

[41] A. H. Abdi and H. Rasheed, "Performance Analysis of Outdoor Massive MIMO on Ultra-High Frequency Bands (73 GHz and 100 GHz)," 2022 International Symposium on Networks, Computers and Communications (ISNCC), Shenzhen, China, 2022, pp. 1-6, doi: 10.1109/ISNCC55209.2022.9851799.

[42] Maayah, M. (2025). Framework for Node Detection in Cloud Computing: A Multi-Metric Approach Integrating Security, Availability, and Latency Factors. Journal of Cyber Security and Risk Auditing, 2025(4), 238–256. https://doi.org/10.63180/jcsra.thestap.2025.4.4

[43] A. Hirsi et al., "HSF: A Hybrid SVM-RF Machine Learning Framework for Dual-Plane DDoS Detection and Mitigation in Software-Defined Networks," in IEEE Access, vol. 13, pp. 112303-112323, 2025, doi: 10.1109/ACCESS.2025.3583712.

[44] A. H. Abdi, L. Audah, A. M. Omar and M. J. Abdiaziz, "Design and Simulation of a Secured Enterprise Network Architecture for All Departments at East Africa University (EAU), Somalia," 2024 4th International Conference of Science and Information Technology in Smart Administration (ICSINTESA), Balikpapan, Indonesia, 2024, pp. 552-557, doi: 10.1109/ICSINTESA62455.2024.10747898.

[45] W. Feng, C. Liu, B. Cheng, J. Chen and Z. Wan, "An End-Host-Importance-Aware Secure Service-Enabled Hybrid SDN Deployment," in IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 2056-2070, June 2023, doi: 10.1109/TNSM.2022.3208695.

[46] A. Hirsi et al., "Hybrid CNN-LSTM Model for DDoS Detection and Mitigation in Software-Defined Networks," in IEEE Transactions on Network and Service Management, vol. 23, pp. 2507-2527, 2026, doi: 10.1109/TNSM.2026.3662819.

[47] J. H. Cox, R. Clark and H. Owen, "Leveraging SDN and WebRTC for Rogue Access Point Security," in IEEE Transactions on Network and Service Management, vol. 14, no. 3, pp. 756-770, Sept. 2017, doi: 10.1109/TNSM.2017.2710623.

[48] Q. Ren et al., "SDN-ESRC: A Secure and Resilient Control Plane for Software-Defined Networks," in IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2366-2381, Sept. 2022, doi: 10.1109/TNSM.2022.3163198.

[49] B. Yuan et al., "Toward Automated Attack Discovery in SDN Controllers Through Formal Verification," in IEEE Transactions on Network and Service Management, vol. 21, no. 3, pp. 3636-3655, June 2024, doi: 10.1109/TNSM.2024.3386404.

[50] S. Deng, L. Chen and X. Gao, "Manipulating Sensitive Match Fields to Poison Applications in SDN," in IEEE Transactions on Network and Service Management, vol. 21, no. 2, pp. 2413-2425, April 2024, doi: 10.1109/TNSM.2023.3337434.

[51] M. Girdhar, K. Park, W. Su, J. Hong and C. -C. Liu, "Cybersecurity Enhancement in Digital Substations: Hidden Markov Model-Based Smart Cyber Switching and Threat Response," in IEEE Access, vol. 13, pp. 217022-217037, 2025, doi: 10.1109/ACCESS.2025.3648339.

[52] G. Yang et al., "Real-Time DDoS Attack Detection in SDN Based on En-CNN and OptiLGBM," in IEEE Access, vol. 13, pp. 161453-161471, 2025, doi: 10.1109/ACCESS.2025.3608205.

[53] S. Rekik and S. Mehmood, "A Hybrid Graph Neural Network and Neural ODE Model to Intrusion Detection in Dynamic Network Topologies," in IEEE Access, vol. 13, pp. 198201-198227, 2025, doi: 10.1109/ACCESS.2025.3635385.

[54] A. Hirsi, L. Audah, A. Salh, N. M. Sahar, M. A. Alhartomi and S. Ahmed, "Detecting Low-Rate DDoS Attacks in SDN Using Ensemble Machine Learning Techniques," 2024 IEEE 22nd Student Conference on Research and Development (SCOReD), Selangor, Malaysia, 2024, pp. 299-304, doi: 10.1109/SCOReD64708.2024.10872742.

[55] Ö. Durmuş, F. Atasoy and M. Türkoğlu, "Comparative Detection of DDoS Attacks on Software-Defined 5G Network Data Using Deep Neural Networks and Machine Learning Methods," in IEEE Access, vol. 13, pp. 194657-194676, 2025, doi: 10.1109/ACCESS.2025.3631396.

[56] W. Ren, Y. Sun, H. Luo and M. Guizani, "SILedger: A Blockchain and ABE-based Access Control for Applications in SDN-IoT Networks," in IEEE Transactions on Network and Service Management, vol. 18, no. 4, pp. 4406-4419, Dec. 2021, doi: 10.1109/TNSM.2021.3093002.

[57] S. M. Shamim, Y. Kodera and Y. Nogami, "GAN-Based IDS System for Imbalanced Datasets in SDN Environments With Offline and Real-Time Traffic Analysis," in IEEE Access, vol. 13, pp. 190786-190806, 2025, doi: 10.1109/ACCESS.2025.3629710.

[58] J. Polónio, J. Moura and R. N. Marinheiro, "Toward Automatic Detection and Mitigation of High-Risk Cybersecurity Vulnerabilities at Networked Systems," in IEEE Access, vol. 13, pp. 181957-181976, 2025, doi: 10.1109/ACCESS.2025.3622497.

[59] N. Sun, X. Li, H. Zheng, Y. Zhao and Y. Guo, "Dynamic Upgrade to SDN From a Global Perspective: Model and Its Heuristic Solutions," in IEEE Transactions on Network and Service Management, vol. 20, no. 4, pp. 4751-4764, Dec. 2023, doi: 10.1109/TNSM.2023.3278877.

[60] D. Zhou, X. Ji, W. You, H. Qiu, Y. Zhao and M. Xu, "Intent-Based Automatic Security Enhancement Method Toward Service Function Chain," in IEEE Transactions on Network and Service Management, vol. 23, pp. 1043-1060, 2026, doi: 10.1109/TNSM.2025.3635228.

[61] U. H. Morshidi, “Bandwidth Enhancement of 5G Parallel Coupled Line Band Pass Filter Using Patterned Ground Structure Technique”, IJIE, vol. 12, no. 6, pp. 87–93, Jun. 2020.

[62] N. S. Mohd Suhaimi and N. M. . Mahyuddin, “Review of Switched Beamforming Networks for Scannable Antenna Application towards Fifth Generation (5G) Technology”, IJIE, vol. 12, no. 6, pp. 62–70, Jun. 2020.