Security of East-West Interface of SDN: A Review of Challenges, Solutions, and Future Directions

Hamad Alrashede
Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University (KAU), Jeddah, Saudi Arabia
halrashede0001@stu.kau.edu.sa (corresponding author)

Fathy Eassa
Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University (KAU), Jeddah, Saudi Arabia
feassa@kau.edu.sa

Abdullah Marish
Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University (KAU), Jeddah, Saudi Arabia
ammali@kau.edu.sa

Received: 17 March 2025 | Revised: 2 April 2025, 13 April 2025, and 15 April 2025 | Accepted: 19 April 2025

 DOI: https://doi.org/10.48084/etasr.10988

ABSTRACT

The east-west interface in Software Defined Networking (SDN) plays a crucial role in enabling inter-controller communication, which is vital for scalability, load balancing, and fault tolerance in distributed SDN environments. Despite its importance, this interface remains vulnerable to serious security threats, such as Man-in-the-Middle (MitM), unauthorized access, False Data Injection (FDI), and Distributed Denial-of-Service (DDoS) attacks. Unlike previous studies and reviews that focus broadly on SDN security, this paper presents a comprehensive review of the current security challenges and proposed solutions that are specific to the east-west interface. The literature is organized into five categories: cryptographic techniques, authentication and access control, blockchain-based mechanisms, Machine Learning (ML) approaches, and hybrid models. In addition, an analytical contribution is provided by introducing a threat-solution coverage matrix that maps each reviewed solution to the specific types of attacks it mitigates. This analysis highlights under-addressed vulnerabilities and uncovers critical research gaps. Future research directions are provided, including the adoption of zero-trust architectures and the need for standardized benchmarking protocols.

Keywords-east-west interface security; distributed SDN security; Software Defined Networking (SDN)

I. INTRODUCTION

SDN is transforming modern networking by decoupling the control plane from the data plane, resulting in programmable and flexible network architectures [1, 2]. The market value of SDN in 2023 was 34.29 billion dollars and is estimated to have a compound growth of 17.9% between 2023 and 2030 [3]. In distributed SDN environments, multiple controllers are deployed to enhance scalability, fault tolerance, and to avoid the single point of failure. The east-west interface plays a vital role in facilitating communication and synchronization between the distributed controllers, making it a key component of the SDN architecture [4]. However, the former is vulnerable to several security threats, including unauthorized access, MitM, DDOS, and FDI, which can compromise the security of the whole network [5-8]. Unfortunately, the currently available SDN controllers are vendor-specific, and lack both the agreed upon east-west protocols and the necessary security aspects [9-12]. Despite the growing relevance of the east-west interface, most security research focuses on north-south communication. To bridge this gap, the current review categorizes and critically analyzes existing security strategies focused on the east-west interface. In addition, a novel threat-solution mapping analysis is provided, exposing which threats are well-covered and which remain open, offering a research-driven roadmap for future work. The present study provides the following contributions:

- A taxonomy of the main security vulnerabilities that affect the east-west interface of SDN.
- A taxonomy of the existing security strategies, categorized into five key approaches.
- A comparative analysis of the current studies, highlighting the strengths, and limitations in each of them.
- A threat-solution mapping analysis that exposes which threats are well-covered and which remain open, offering a research-driven roadmap for future work.

II. REVIEW METHODOLOGY

The present study conducts a narrative literature review focused on securing the east-west interface of SDN. A systematic literature search was performed searching the IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink databases. The utilized keywords included "east-west SDN security," "inter-controller SDN attacks," "blockchain SDN," "machine learning SDN," and "SDN cryptographic methods." The initial search yielded 152 papers from which 64 relevant studies were selected based on the following inclusion criteria:

- Peer-reviewed journal articles from 2015 to 2025.
- Focus on the security of east-west or inter-controller communication.
- Quantitative or qualitative evaluation of the proposed methods.

III. EAST-WEST INTERFACE

In distributed SDN architectures, the east-west interface is critical for enabling communication between controllers to ensure synchronization, policy consistency, and network reliability, as presented in Figure 1. This interface is essential for maintaining a unified and efficient network infrastructure, particularly in large-scale or multi-domain environments [13-16]. The key functions associated with the east-west interface include:

- Exchange of topology updates:

Controllers share real-time information about network topology changes, ensuring that all controllers have an accurate and up-to-date view of the network. This is crucial for effective routing decisions and resource allocation [17].

- Coordination of traffic engineering policies:

The east-west interface helps controllers collaboratively manage and optimize the traffic flow across the network. This includes load balancing, congestion avoidance, and ensuring adherence to predefined service-level agreements [18, 19].

- Fault tolerance mechanisms:

By facilitating communication between controllers, the east-west interface supports redundancy and failover strategies. In the event of a controller's failure, other controllers can seamlessly take over, minimizing downtime and maintaining network stability [20].

The previous functions collectively contribute to the robustness and scalability of distributed SDN architectures, rendering the east-west interface a vital component for ensuring seamless inter-controller communication and overall network performance.

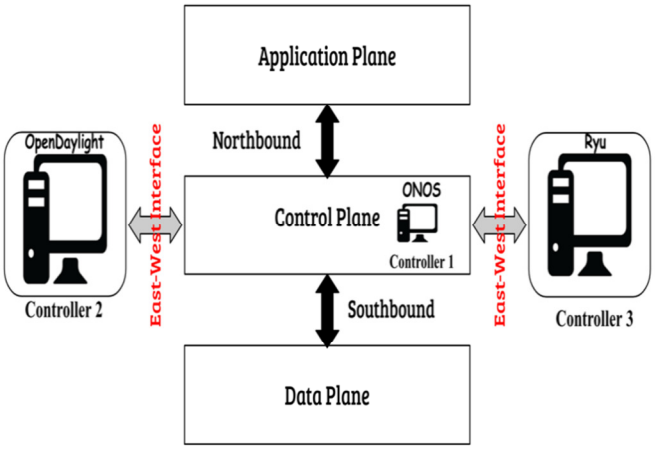

Fig. 1. The architectural role of the east-west interface within distributed SDN.

IV. SECURITY CHALLENGES IN EAST-WEST INTERFACE

Although the east-west interface in distributed SDN architectures is essential for inter-controller communication, it is susceptible to several vulnerabilities that can compromise network security and performance [21]. Figure 2 provides a taxonomy of the common security challenges encountered in the east-west interface, followed by an explanation for each one.

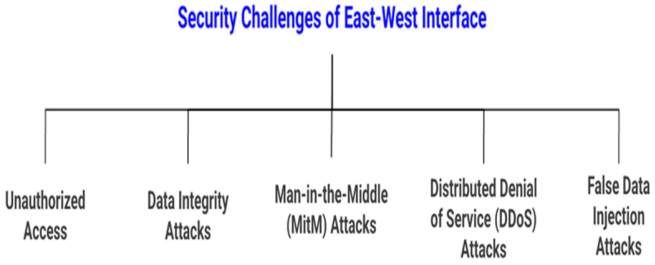

Fig. 2. A taxonomy of security challenges of east-west interface.

A. *Unathorized Access*

This type of attack occurs when an attacker gains illegal entry into the internal communication between SDN components, such as controllers, switches, and virtualized network functions [22]. Since SDN centralizes network control, unauthorized access to the controller can grant an attacker the ability to manipulate traffic flows, disrupt services, or launch further attacks, like MitM, DDoS, and FDI. This type of attack is particularly dangerous in east-west traffic, as it allows lateral movement within the network,

enabling the attacker to exploit vulnerabilities in multiple segments without detection. Common entry points involve weak authentication, misconfigured access controls, and insecure APIs [23, 24].

B. Data Integrity Attacks

Data integrity attacks pose a serious threat by allowing malicious actors to alter, delete, or inject false data into inter-controller communications [25]. Since SDN controllers rely on this interface to share critical network state information, any tampering with data can lead to incorrect routing decisions, network misconfigurations, and service disruptions. Attackers can exploit weak authentication, lack of encryption, or unsecured communication channels to modify control messages, manipulate flow rules, or introduce misleading network settings. Such attacks not only compromise network performance, but also create opportunities for adversaries to launch further exploits [26-28].

C. Man-in-the-Middle Attacks

An MitM attack occurs when an attacker intercepts and manipulates the communication between SDN controllers, switches, or other network elements operating within the same data plane [29]. Unlike north-south traffic, which involves external communication, east-west traffic in SDN deals with the lateral movements within the network, making it a prime target for attackers who seek to exploit vulnerabilities. Since SDN centralizes network control, an attacker gaining unauthorized access to the communication between controllers and switches can eavesdrop on sensitive data, inject malicious commands, or alter network flows, potentially causing large-scale disruptions. This attack can be facilitated through compromised switches, insecure APIs, or protocol vulnerabilities [30, 31].

D. Distributed Denial of Service attacks

A DDoS attack in the east-west interface involves an attacker leveraging compromised nodes within the network to overwhelm SDN controllers, switches, or internal services [32]. Unlike traditional DDoS attacks that target external-facing infrastructure (north-south traffic), east-west DDoS attacks exploit the lateral communication between the SDN components, leading to degraded network performance, increased latency, and potential system failure. Attackers can flood the SDN control plane with excessive requests, causing controller exhaustion, or disrupt the data plane by overloading switches with malicious traffic. Since SDN relies on centralized control, a successful DDoS attack on the controller can severely impact the entire network [32, 33].

E. False Data Injection

Through an FDI attack, the attacker injects manipulated or deceptive data into the network to alter its behavior and compromise decision-making processes [34, 35]. Since SDN separates the control plane from the data plane, attackers can target communication between switches and controllers, injecting false flow rules, modifying packet headers, or fabricating telemetry data. This can lead to incorrect routing, traffic redirection, or even facilitating other attacks, like MitM and DDoS. In east-west traffic, where communication occurs between internal SDN components, FDI attacks can spread laterally, compromising multiple devices without raising immediate suspicion.

V. EXISTING SOLUTIONS FOR EAST-WEST INTERFACE

A great amount of research has explored different approaches to enhancing the east-west interface security of SDN, ranging from cryptographic techniques to blockchain-based solutions. Figure 3 depicts a taxonomy of the existing studies, relevant to securing the east-west interface of SDN.

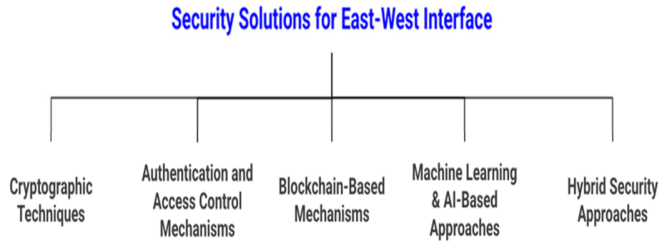

Fig. 3. A taxonomy of the existing security solutions for the east-west interface of SDN.

A. Cryptographic Techniques

Different cryptographic techniques have been proposed to secure the communication between the east-west interface of SDN. Authors in [36] identified Advanced Encryption Standard (AES), RSA, and hybrid encryption algorithms as the most effective cryptographic techniques for securing control plane communication in distributed SDN architectures. They emphasized that the hybrid coding method outperforms RSA alone in terms of security and speed, rendering it a robust solution for protecting data integrity and authenticity in SDN networks. The implementation of these algorithms addresses the security vulnerabilities associated with the separation of control and data planes. Authors in [37] proposed utilizing Elliptic Curve Cryptography (ECC) as the most effective cryptographic technique for securing control plane communication in distributed SDN architectures. ECC offers advantages, such as lower computational overhead, shorter key lengths, and enhanced resistance to attacks compared to other asymmetric encryption methods, like RSA. The introduced authentication mechanism, based on a Public Key Infrastructure (PKI) model, ensures efficient and secure communication between distributed controllers, effectively addressing security concerns in large networks. Authors in [38] introduced a multi-domain capable Identity-Based Cryptography (IBC) protocol to secure control plane communication in distributed SDN architectures. This approach aims to enhance the security of both east/west-bound and southbound communications, addressing the vulnerabilities present in current implementations. Although Transport Layer Security (TLS) is proposed for southbound communication, the need for a more robust solution, like IBC, is stressed to prevent malicious controllers from eavesdropping or manipulating network traffic effectively.

Authors in [39] presented elliptic curve encryption as an effective cryptographic technique for securing control plane communication in distributed SDN. This method addresses the security challenges associated with SDN's centralized controlling and data transfer channels, specifically the control and infrastructure layers. Unlike the existing Open-Flow protocols that depend on higher layer secure mechanisms, like TLS/SSL, the proposed architecture enhances security and efficiency by implementing elliptic curve cryptography, which is more suitable for the unique requirements of SDN environments. Authors in [40] proposed an efficient Zero-Knowledge Proof (ZKP)-based identification scheme as a cryptographic technique for securing control plane communication in SDN. This scheme ensures that only users who can prove their knowledge of a secret without revealing it can communicate with the controller, enhancing security. Additionally, the computation cost and efficiency of the proposed ZKP scheme were discussed compared to traditional methods, like Kerberos authentication, highlighting its effectiveness in securing SDN environments.

Authors in [41] investigated hybrid Quantum Key Distribution (QKD) protocols to enhance SDN security. However, despite their innovative potential, QKD systems face practical deployment challenges due to their complexity, reinforcing the practicality of blockchain's decentralized nature. Authors in [42] presented QKD as an effective cryptographic technique for securing control plane communication in distributed SDN architectures. QKD leverages quantum mechanics principles, such as entanglement and superposition, to generate and distribute keys securely, ensuring confidentiality and privacy. The former is resistant to future technological advancements, making it an effective solution against potential cyber threats. QKD and SDN implementation can enhance security, protect against attacks, and maintain reliable network orchestration and data integrity.

B. Authentication and Access Control Mechanisms

Several studies have introduced authentication and access control approaches to mitigate the security challenges of east-west interface of SDN. Authors in [43] proposed a cryptographic key generation application that creates certificates for securing communication among SDN entities, including controller, switch, and application. TLS utilization was highlighted to ensure confidentiality, integrity, authentication, and authorization. Additionally, an integrated security module enhanced communication security by implementing Access Control Lists (ACL), hardening TLS configurations, and mitigating private key hijacking risks. This approach effectively addresses vulnerabilities in control plane communication within distributed SDN architectures. Authors in [44] presented a simple authentication mechanism using hash tables, cryptographic hash functions, and REST APIs to secure communications between access points and applications. They focused on preventing unauthorized access and certifying secure communication rather than detailing specific cryptographic techniques for the control plane. Authors in [45] introduced the Trust Enhanced Security (TES) for routing within the SDN. They integrated three distinct trust evaluation mechanisms to determine the most suitable trust level corresponding to varying network conditions. In order to validate its efficiency, a series of simulations was executed, with particular emphasis being placed on the identification of compromised switches. The simulation results indicate that the proposed framework adeptly detects and eliminates compromised nodes while concurrently ensuring the selection of secure routing paths. Authors in [46] focused on blockchain technology and smart contract utilization to enhance the security between SDN controllers. The proposed smart contracts embed SDN rules and are designed to prevent unauthorized access and DoS attacks, thereby ensuring secure communications within the distributed SDN environment. Authors in [47] employed a combination of theoretical analysis and practical case studies to explore the application of blockchain-based smart contracts within SDN for enhancing inter-domain communications.

C. Blockchain-based Mechanisms

Many researchers have explored blockchain-based solutions to enhance security at the east-west interface of SDN. Authors in [48] combined SDN and blockchain to bolster security in cloud IoT environments, particularly against MitM attacks. Blockchain ensures immutable transactions for device authentication and secure data sharing, complemented by smart contracts that enforce unchangeable transactions and device anonymity. SDN is utilized for traffic segmentation and dynamic policy enforcement, reducing MitM vulnerabilities through effective traffic inspection and access control. This approach not only prevents MitM attacks, but also enhances data integrity, confidentiality, and overall security in cloud-based IoT systems. Authors in [49] introduced the Controller-Block model, integrating blockchain with SDN to fortify security and privacy in cloud computing. This model employs a density-based block structure to establish a distributed architecture, mitigating single points of failure. By leveraging blockchain's distributed peer-to-peer networks, it facilitates secure communication among untrusted nodes, bolstering defenses against various attacks, including DDoS. Authors in [50] presented the Blockchain-based Multi-controller (BMC-SDN) architecture to secure the east-west interface across multi-domain environments. This architecture employs a reputation mechanism to assess controller reliability and prevent FDI attacks. However, its focus on specific threats limits its broader applicability to other security challenges. Authors in [51] introduced a blockchain-SDN architecture to secure cloud computing in smart industrial IoT settings, highlighting blockchain's adaptability but acknowledging gaps in providing a comprehensive security solution. Authors in [52] presented the Blockchain-based Controller against False Flow Rule (BCFR) injection to prevent specific attacks. However, their scope does not cover broader security concerns.

Authors in [53] proposed a Blockchain-based Controller Security (BCS) mechanism for Multi-Controller SDN (MC-SDN), leveraging immutable ledgers to enhance communication security among controllers. The experimental results demonstrated its efficacy in detecting attacks, with scalability issues in larger networks, though, remaining unaddressed. Authors in [54] integrated blockchain with the MC-SDN to prevent false flow rule injections. Nevertheless,

concerns about scalability and robustness in complex environments persist. Authors [55] explored blockchain's potential to reduce latency and gas consumption in SDN, while authors in [56] proposed a federated SDN east-west interface, using blockchain for decentralized security management. Authors in [57] presented a blockchain-based method for secure coordination between distributed SDN controllers, focusing on information exchange security, but omitting encryption and access control considerations.

D. Machine Learning and AI Approaches

Various articles have proposed ML and Artificial Intelligence (AI)-based approaches for the security of east-west interface in SDN. Authors in [58] employed an ML approach to detect possible security issues in the east-west communications. This method utilizes three classification algorithms for detecting DDoS attacks in SDN controllers: Extreme Gradient Boosting (XGBoost), Random Forest (RF), and Decision Tree (DT). The effectiveness of these techniques was evaluated using the CICDDoS2019 dataset. High accuracy scores were achieved, showcasing the specific techniques' ability to accurately identify DDoS attack types in the SDN environment. Authors in [59] introduced a hybrid Deep Auto Encoder with Random Forest (DAERF) classifier model specifically designed to enhance intrusion detection performance in a native SDN environment. This model is tailored to address the unique security challenges faced by the SDN networks. The proposed framework incorporates a three-layer protection mechanism for attack detection and prevention, which includes entropy-based detection, hybrid ML in the control layer, and proactive services monitoring in the application layer, thereby providing a comprehensive approach to security in SDN environments. ML techniques were proposed in [60] for the swift detection of attacks within SDN networks. Various methods were evaluated for detecting DDoS attacks, with the proposed ensemble method identified as the most precise. Authors in [61] introduced a method for detecting and mitigating DDoS attacks, utilizing SDN capabilities along with the sFlow-RT application. This approach allows for a real-time monitoring and analysis of network traffic to identify potential DDoS threats. The implementation of Policy-Based Flow Management (PBFM) through the SDN Controller was proposed to manage network flows effectively. This is achieved using the REST API, which helps ensure uninterrupted services during DDoS attacks, while it simplifies the management of mesh architecture-based networks.

E. Hybrid Security Methods

Authors in [62] introduced a novel integrated hybrid malware attack detection algorithm that combines three key methods: DDOS attack prevention, re-entrancy attack detection, and Byzantine fault tolerance detection, all integrated into a single cohesive architecture to enhance cybersecurity within blockchain systems. The proposed hybrid framework utilizes a detailed algorithmic approach that integrates SHA-256 and DSA to analyze and mitigate the three types of malware attacks, resulting in improved computational complexity and expedited execution within the network of nodes. Authors in [63] did not specifically address the most effective cryptographic techniques for securing control plane communication in distributed SDN architectures. Instead, they focused on creating a secure environment for networked control systems using cryptographic techniques to protect input and output data from malicious entities. The proposed methodology integrates cryptographic mechanisms with control algorithms, emphasizing the separation principle to meet both security and performance requirements in large-scale cyber-physical systems. Authors in [64] introduced a novel approach that integrates blockchain technology within SDN components to create a decentralized ledger, which enhances security, privacy, and trustworthiness of Device-to-Device (D2D) communication. This integration allows for transparent and verifiable records of communications among IoT devices. Smart contracts are utilized to enforce authentication rules, ensuring that only authenticated devices can access the network and engage in secure transactions. Additionally, the approach automates security policies to maintain tamper-resistant execution through cryptographic mechanisms that guarantee data integrity and authentic communication. Table I provides a summary of the different security approaches in the literature for protecting east-west interface, outlining their main contributions and limitations, while Figure 4 presents the distribution of the used mechanism.

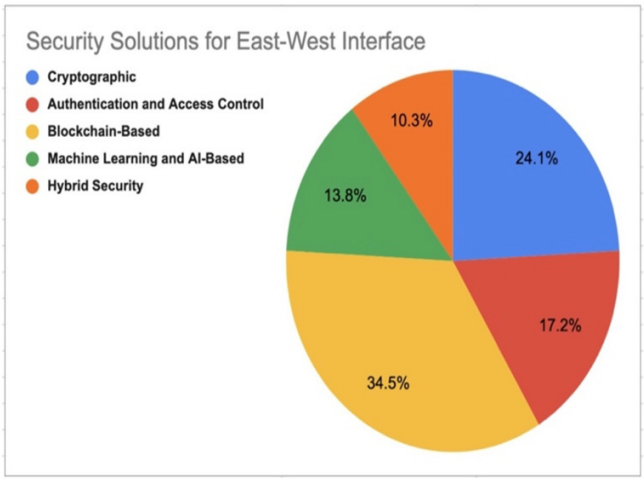

Fig. 4. Distribution of various mechanisms for securing east-west interface.

VI. DISCUSSION AND FUTURE DIRECTIONS

A. Reviewed Solution Analysis

Cryptographic methods, such as ECC, RSA, and AES, are widely used to secure inter-controller communication by ensuring confidentiality and data integrity. In [36–42], the advantages of ECC in distributed SDN were highlighted due to its low computational overhead and shorter key lengths, rendering it suitable for real-time environments. IBC [38] offers scalable key management in multi-domain scenarios, while QKD [41, 42] provides future-proof encryption. However, these techniques are generally limited in detecting dynamic threats, like DDoS or FDI. Furthermore, practical deployment challenges, particularly with QKD and IBC, restrict their widespread adoption in current infrastructures.

TABLE I. LITERATURE SUMMARY, CONTRIBUTIONS, AND LIMITATIONS

Reference	Approach	Contributions	Limitations
[36]	Proposes hybrid encryption for control plane security.	Identifies AES, RSA, and hybrid encryption as effective for securing control plane communication.	Limited to encryption techniques, does not address other security challenges.
[37]	Proposes ECC for control plane security.	Highlights ECC's advantages (lower overhead, shorter keys) and proposes a PKI-based authentication mechanism.	Focuses only on ECC, lacks comparison with other cryptographic methods.
[38]	Proposes IBC for multi-domain SDN security.	Enhances security for east-west-bound and southbound communications using IBC.	Limited discussion on IBC's scalability and performance.
[39]	Proposes elliptic curve encryption for SDN control plane.	Enhances security and efficiency for SDN control and infrastructure layers.	Focuses on elliptic curve encryption; lacks comparison with other methods.
[40]	Proposes ZKP for SDN control plane.	Enhances security by ensuring that only authenticated users can communicate with the controller.	Focuses on ZKP; lacks comparison with other cryptographic methods.
[41]	Investigates hybrid QKD for SDN security.	Explores QKD protocols for enhancing SDN security.	Practical deployment challenges due to complexity.
[42]	Proposes QKD for SDN control plane.	Enhances security using quantum mechanics principles for key distribution.	Limited to QKD; lacks comparison with other cryptographic methods.
[43]	Proposes cryptographic key generation and TLS for SDN communication.	Enhances communication security using TLS, ACLs, and private key protection.	Limited to TLS-based solutions; does not address other cryptographic techniques.
[44]	Proposes hash-based authenticationfor access points.	Uses hash tables and REST APIs to secure communication between access points and applications.	Focuses on authentication; does not address broader SDN security challenges.
[45]	Introduces TES for SDN routing.	Integrates trust evaluation mechanisms to detect compromised switches and ensure secure routing paths.	Limited to routing security; does not address other SDN vulnerabilities.
[46]	Uses blockchain and smart contracts for SDN controller security.	Prevents unauthorized access and DoS attacks using smart contracts.	Limited to particular attacks; scalability concerns are not addressed.
[47]	Explores blockchain-based smart contracts for SDN inter-domain communication.	Addresses scalability, interoperability, and smart contract complexity in SDN.	Focuses on theoretical analysis; lacks practical implementation.
[48]	Combines SDN and blockchain for cloud IoT security.	Prevents MitM attacks using blockchain for immutable transactions and SDN for traffic segmentation.	Limited to cloud IoT environments; scalability concerns are not addressed.
[49]	Proposes Controller Block model for SDN and blockchain integration.	Enhances security and privacy in cloud computing using blockchain-enabled P2P networks.	Focuses on cloud environments; lacks evaluation in other contexts.
[50]	Introduces BMC-SDN for multi-domain security.	Uses a reputation mechanism to prevent FDI attacks in east-west interfaces.	Does not address other threats, like MitM or privilege escalation.
[51]	Proposes blockchain-SDN for smart industrial IoT.	Emphasizes blockchain adaptability for securing cloud computing in industrial IoT.	Lacks comprehensive security solutions for broader SDN environments.
[52]	Introduces BCFR to prevent false flow rule injections.	Effectively addresses false flow rule injection attacks.	Limited to specific attack type; does not address other security challenges.
[53]	Proposes BCS for MC-SDN.	Enhances security among multiple controllers using Immutable ledger technology.	Scalability issues with increasing controllers and switches are not addressed.
[54]	Integrates blockchain with MC-SDN.	Prevents false flow rule injections using a reputation mechanism.	Scalability and robustness in higload, multi vendor environments remain untested.
[55]	Investigates blockchain for SDN east-west interface.	Reduces latency and gas consumption in SDN east-west communication.	Limited to performance aspects; lacks broader security evaluation.
[56]	Proposes blockchain for federated SDNs.	Showcases decentralized security management for east-west interfaces.	Does not address encryption or access control issues.
[58]	Uses ML for DDoS attack detection.	Evaluates XGBoost, RF, and DT for detecting DDoS attacks in SDN.	Limited to DDoS detection; does not address other attack types.
[59]	Proposes the DAERF model for intrusion detection.	Combines Deep AutoEncoder and RF for attack detection and prevention in SDN.	Focuses on intrusion detection; lacks broader security solutions.
[60]	Evaluates ensemble learning for DDoS detection.	Identifies ensemble learning as the most precise method for DDoS attack detection.	Limited to DDoS detection; does not address other attack types.
[61]	Uses SDN and sFlow-RT for DDoS detection and mitigation.	Implements PBFM for realtime DDoS threat mitigation.	Limited to DDoS attacks; scalability concerns are not addressed.
[62]	Introduces hybrid malware detection algorithm.	Combines DDOS prevention, reentrancy attack detection, and Byzantine fault tolerance for blockchain systems.	Limited to blockchain systems; lacks evaluation in SDN environments.
[63]	Focuses on securing networked control systems.	Integrates cryptographic mechanisms with control algorithms to protect data in cyber-physical systems.	Does not address other attack types of east- west interface.
[64]	Integrates blockchain with SDN for D2D communication.	Enhances the security, privacy, and trustworthiness of the IoT device communication using smart contracts.	Limited to IoT environments; scalability and performance are not evaluated.

Authentication and access control, include methods that verify identities and regulate inter-controller access. TLS-based encryption [43] combined with ACLs ensures secure communication. The REST API authentication [44] and TES [45] frameworks provide lightweight methods for access control. These approaches are effective in mitigating unauthorized access and MitM attacks, but they often lack mechanisms for real-time threat detection or adaptive response, making them less effective against DDoS and FDI attacks.

Blockchain technologies have gained popularity for their ability to provide immutable logs and decentralized authentication. Architectures, like BMC-SDN [50] and BCFR [52], use blockchain to secure east-west interfaces and prevent FDI. Blockchain-SDN integrations [46-57] also support inter-domain trust and resilience against MitM attacks. However, despite their potential, these solutions face latency, scalability, and energy efficiency challenges, particularly in resource-constrained or large-scale networks. Notably, only a few studies have evaluated performance trade-offs of blockchain at high traffic loads, leaving practical viability under-explored. ML and AI-based approaches [58-61] are promising for detecting and mitigating DDoS attacks in real time. Techniques, like XGBoost, RF, and Deep AutoEncoders have demonstrated high accuracy in anomaly detection using datasets, such as CICDDoS2019. These solutions offer adaptive learning and can detect evolving threats that static systems might miss. However, their effectiveness is often limited to known attack types, and training overheads can hinder real-time deployment. Moreover, most models are designed for north-south traffic and need further tailoring for east-west communication patterns.

Hybrid methods [62-64] integrate multiple techniques, such as combining cryptography with blockchain or AI, to provide layered security. These models offer higher threat coverage, as they leverage the complementary strengths of each technique. For example, authors in [64] combined smart contracts, cryptographic integrity checks, and blockchain logging for IoT-based SDN environments. However, hybrid systems introduce design and implementation complexity, require coordination between multiple modules, and may suffer from compatibility and integration issues across heterogeneous SDN deployments.

B. Threat-Solution Coverage Matrix

To uncover research gaps, the current study introduces a Threat-Solution Coverage Matrix that maps reviewed solutions to the specific threats they address. This allows for a visual identification of under-addressed security concerns, clearly demonstrating which types of security solutions address specific east-west interface threats in SDN. Figure 5 demonstrates that unauthorized access and MitM are covered across all solution types. It is observed that FDI and DDoS threats are under-addressed by cryptographic and access control methods, while hybrid solutions show promise but are relatively sparse. This matrix provides a structured lens to evaluate where new security mechanisms are most needed.

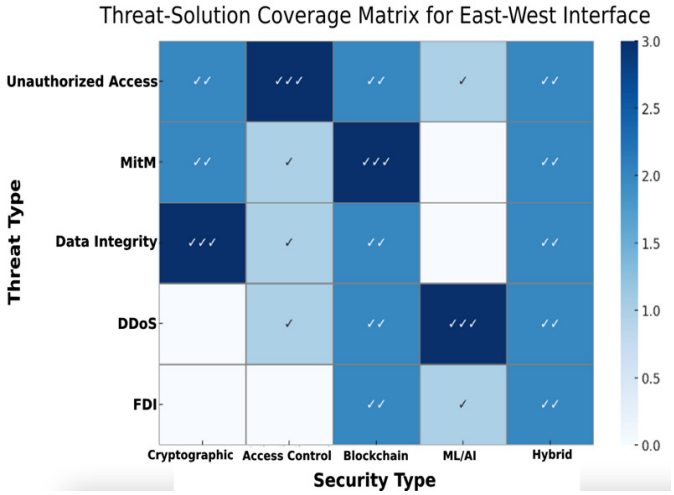

Fig. 5. Visualized threat-solution coverage matrix. Legend**:** ✓ = 1-2 studies, ✓✓ = 3-5 studies, ✓✓✓ = more than 5 studies.

C. Future Directions and Open Challenges

To enhance security in the east-west interface of SDN, it is essential to implement Zero-Trust architectures by adopting identity-centric frameworks for controller verification. Establishing standardized protocols for east-west communication is critical to ensure consistency and reliability across systems. The development of robust security testing tools, including benchmarks and simulation environments, is necessary for the effective evaluation of the emerging solutions. Furthermore, scalability and interoperability must be prioritized to guarantee that security mechanisms function seamlessly across heterogeneous SDN environments. Lightweight cryptographic schemes should be designed specifically for resource-constrained networks to maintain efficiency without compromising security. Finally, special attention should be given to techniques aimed at detecting FDI and insider threats, which are often subtle and difficult to identify.

VII. CONCLUSION

While notable advancements have been made in securing the northbound and southbound interfaces of Software Defined Networking (SDN), the east-west interface, which is responsible for the communication between distributed controllers, remains a critical, yet, unsecured component. This paper provides a comprehensive review and in-depth analysis of the current security landscape surrounding the east-west interface. The existing body of research is categorized into five major solution types: cryptographic techniques, authentication and access control mechanisms, blockchain-based methods, Machine Learning (ML) approaches, and hybrid models. A key contribution of this study is the introduction of a threat-solution coverage matrix, which highlights how well each type of solution addresses specific threats, such as Man-in-the-Middle (MitM), False Data Injection (FDI), and Distributed Denial-of-Service (DDoS) attacks. The analysis reveals that while the blockchain-based strategies are the most prevalent one, accounting for 34.5% of the reviewed solutions, only 13.8%

adopt hybrid models that combine multiple defense mechanisms. Furthermore, traditional cryptographic and access control methods often fall short in fully addressing evolving threats, like FDI and DDoS. These findings underscore the pressing need for unified and scalable security frameworks tailored to the east-west interface.

Future work should prioritize the development of zero-trust architectures, lightweight encryption protocols, and standardized evaluation benchmarks. As SDN technologies continue to evolve and scale across diverse environments, securing inter-controller communication will be fundamental to achieving resilient, adaptive, and trustworthy network infrastructures.

REFERENCES

[1] A. Liatifis, P. Sarigiannidis, V. Argyriou, and T. Lagkas, "Advancing SDN from OpenFlow to P4: A Survey," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 186:1-186:37, Jan. 2023, https://doi.org/10.1145/3556973.

[2] R. Chaudhary, G. S. Aujla, N. Kumar, and P. K. Chouhan, "A comprehensive survey on software-defined networking for smart communities," *International Journal of Communication Systems*, vol. 38, no. 1, 2025, Art. no. e5296, https://doi.org/10.1002/dac.5296.

[3] *Software Defined Networking Market, Industry Report, 2030*. Grand View Research, 2023.

[4] H. Alrashede, F. Eassa, A. Marish Ali, F. Albalwy, and H. Aljihani, "A Blockchain-Based Security Framework for East-West Interface of SDN," *Electronics*, vol. 13, no. 19, Jan. 2024, Art. no. 3799, https://doi.org/10.3390/electronics13193799.

[5] A. H. Janabi, T. Kanakis, and M. Johnson, "Survey: Intrusion Detection System in Software-Defined Networking," *IEEE Access*, vol. 12, pp. 164097–164120, 2024, https://doi.org/10.1109/ACCESS.2024.3493384.

[6] R. Basfar, M. Y. Dahab, A. M. Ali, F. Eassa, and K. Bajunaied, "Enhanced Intrusion Detection in Software-Defined Networking using Advanced Feature Selection: The EMRMR Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 19001–19008, Dec. 2024, https://doi.org/10.48084/etasr.9256.

[7] Huang, V.; Chen, G.; Zhang, P.; Li, H.; Hu, C.; Pan, T.; Fu, Q. "A Scalable Approach to SDN Control Plane Management: High Utilization Comes With Low Latency." IEEE Transactions on Network and Service Management, vol. 17, pp. 682–695, Sept. 2020.

[8] N. V. Oikonomou, D. V. Oikonomou, E. Stergiou, and D. Liarokapis, "Comprehensive Analysis of Software-Defined Networking: Evaluating Performance Across Diverse Topologies and Investigating Topology Discovery Protocols," *Journal of Engineering Research and Sciences*, vol. 3, no. 7, pp. 23–43, 2024, https://doi.org/10.55708/js0307003.

[9] R. S. Alsheikh, E. A. Fadel, and N. T. Akkari, "Distributed Software-Defined Networking Management:," *ARO-the Scientific Journal of Koya University*, vol. 12, no. 2, pp. 157–166, Sep. 2024, https://doi.org/10.14500/aro.11468.

[10] S. O. Sati, M. Sati, and M. Emshiheet, "Control Plane Scalability of Software Defined Networking," in *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, Manama, Bahrain, Jan. 2024, pp. 1830–1834, https://doi.org/10.1109/ICETSIS61505.2024.10459395.

[11] P. B. Bautista, J. Comellas, and L. Urquiza-Aguiar, "Evaluating Scalability, Resiliency, and Load Balancing in Software-Defined Networking," *Engineering Proceedings*, vol. 47, no. 1, 2023, Art. no. 16, https://doi.org/10.3390/engproc2023047016.

[12] M. Ali *et al.*, "Performance and Scalability Analysis of SDN-Based Large-Scale Wi-Fi Networks," *Applied Sciences*, vol. 13, no. 7, Jan. Art. no. 4170, 2023, https://doi.org/10.3390/app13074170.

[13] S. A. Darade and M. Akkalakshmi, "Load balancing strategy in software defined network by improved whale optimization algorithm," *Journal of High Speed Networks*, vol. 27, no. 2, pp. 151–167, Jul. 2021, https://doi.org/10.3233/JHS-210657.

[14] C. D. Bhowmik and T. Gayen, "Traffic aware dynamic load distribution in the Data Plane of SDN using Genetic Algorithm: A case study on NSF network," *Pervasive and Mobile Computing*, vol. 88, Jan. 2023, Art. no. 101723, https://doi.org/10.1016/j.pmcj.2022.101723.

[15] S. Xu, X. Wang, G. Yang, J. Ren, and S. Wang, "Routing optimization for cloud services in SDN-based Internet of Things with TCAM capacity constraint," *Journal of Communications and Networks*, vol. 22, no. 2, pp. 145–158, Apr. 2020, https://doi.org/10.1109/JCN.2020.000006.

[16] S. Ahmad and A. H. Mir, "SDN Interfaces: Protocols, Taxonomy and Challenges," *International Journal of Wireless and Microwave Technologies*, vol. 12, no. 2, pp. 11–32, Apr. 2022, https://doi.org/10.5815/ijwmt.2022.02.02.

[17] Z. Latif, K. Sharif, F. Li, M. M. Karim, S. Biswas, and Y. Wang, "A comprehensive survey of interface protocols for software defined networks," *Journal of Network and Computer Applications*, vol. 156, Apr. 2020, Art. no. 102563, https://doi.org/10.1016/j.jnca.2020.102563.

[18] O. Blial, M. Ben Mamoun, and R. Benaini, "An Overview on SDN Architectures with Multiple Controllers," *Journal of Computer Networks and Communications*, vol. 2016, no. 1, 2016, Art. no. 9396525, https://doi.org/10.1155/2016/9396525.

[19] J. Miguel-Alonso, "A Research Review of OpenFlow for Datacenter Networking," *IEEE Access*, vol. 11, pp. 770–786, 2023, https://doi.org/10.1109/ACCESS.2022.3233466.

[20] R. Firouzi and R. Rahmani, "A Distributed SDN Controller for Distributed IoT," *IEEE Access*, vol. 10, pp. 42873–42882, 2022, https://doi.org/10.1109/ACCESS.2022.3168299.

[21] S. Ahmad and A. H. Mir, "Scalability, Consistency, Reliability and Security in SDN Controllers: A Survey of Diverse SDN Controllers," *Journal of Network and Systems Management*, vol. 29, no. 1, Nov. 2020, Art. no. 9, https://doi.org/10.1007/s10922-020-09575-4.

[22] V. Ganeshan and B. S. Manoj, "Beyond Traditional Boundaries: A Survey of Security Mechanisms in Software-Defined Networks," in *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*, Vellore, India, Oct. 2024, pp. 1–8, https://doi.org/10.1109/ic-ETITE58242.2024.10493728.

[23] M. Rahouti, K. Xiong, Y. Xin, S. K. Jagatheesaperumal, M. Ayyash, and M. Shaheed, "SDN Security Review: Threat Taxonomy, Implications, and Open Challenges," *IEEE Access*, vol. 10, pp. 45820–45854, 2022, https://doi.org/10.1109/ACCESS.2022.3168972.

[24] M. S. Farooq, S. Riaz, and A. Alvi, "Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review," *Electronics*, vol. 12, no. 14, Jan. 2023, Art. no. 3077, https://doi.org/10.3390/electronics12143077.

[25] G. Hessam, G. Saba, and M. I. Alkhayat, "A new approach for detecting violation of data plane integrity in Software Defined Networks," *Journal of Computer Security*, vol. 29, no. 3, pp. 341–358, May 2021, https://doi.org/10.3233/JCS-200094.

[26] Y. Maleh, Y. Qasmaoui, K. El Gholami, Y. Sadqi, and S. Mounir, "A comprehensive survey on SDN security: threats, mitigations, and future directions," *Journal of Reliable Intelligent Environments*, vol. 9, no. 2, pp. 201–239, Jun. 2023, https://doi.org/10.1007/s40860-022-00171-8.

[27] Z. A. Bhuiyan, S. Islam, Md. M. Islam, A. B. M. A. Ullah, F. Naz, and M. S. Rahman, "On the (in)Security of the Control Plane of SDN Architecture: A Survey," *IEEE Access*, vol. 11, pp. 91550–91582, 2023, https://doi.org/10.1109/ACCESS.2023.3307467.

[28] H. Y. I. Khalid and N. B. I. Aldabagh, "A Survey on the Latest Intrusion Detection Datasets for Software Defined Networking Environments," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13190–13200, Apr. 2024, https://doi.org/10.48084/etasr.6756.

[29] A. Sebbar, M. Boulmalf, M. Dafir Ech-Cherif El Kettani, and Y. Baddi, "Detection MITM Attack in Multi-SDN Controller," in *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, Marrakech, Morocco, Jul. 2018, pp. 583–587, https://doi.org/10.1109/CIST.2018.8596479.

[30] K. S. Goud and S. R. Gidituri, "Security Challenges and Related Solutions in Software Defined Networks: A Survey," *International*

Journal of Computer Networks and Applications, vol. 9, no. 1, Feb. 2022, Art. no. 22, https://doi.org/10.22247/ijcna/2022/211595.

[31] K. G. Yalda, D. J. Hamad, N. Tapus, and I. T. Okumus, "Security Issues in Software-Defined Networking (SDN) Environments," in *2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, Romania, Sep. 2024, pp. 1–8, https://doi.org/10.1109/RoEduNet64292.2024.10722112.

[32] A. O. M. Salih, "Exploring LDoS Attack Detection in SDNs using Machine Learning Techniques," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19568–19574, Feb. 2025, https://doi.org/10.48084/etasr.9424.

[33] L. F. Eliyan and R. Di Pietro, "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges," *Future Generation Computer Systems*, vol. 122, pp. 149–171, Sep. 2021, https://doi.org/10.1016/j.future.2021.03.011.

[34] A. T. Phu *et al.*, "Defending SDN against packet injection attacks using deep learning," *Computer Networks*, vol. 234, Oct. 2023, Art. no. 109935, https://doi.org/10.1016/j.comnet.2023.109935.

[35] Y. Suo, S. Chai, R. Chai, Z.-H. Pang, Y. Xia, and G.-P. Liu, "Security Defense of Large-Scale Networks Under False Data Injection Attacks: An Attack Detection Scheduling Approach," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1908–1921, 2024, https://doi.org/10.1109/TIFS.2023.3340098.

[36] S. Ghaly and M. Z. Abdullah, "Design and implementation of a secured SDN system based on hybrid encrypted algorithms," *TELKOMNIKA*, vol. 19, no. 4, pp. 1118–1125, Aug. 2021, https://doi.org/10.12928/telkomnika.v19i4.18721.

[37] S. B. Hashemi Natanzi and M. R. Majma, "Secure distributed controllers in SDN based on ECC public key infrastructure," in *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, Ras Al Khaimah, United Arab Emirates, Aug. 2017, pp. 1–5, https://doi.org/10.1109/ICECTA.2017.8252015.

[38] J.-H. Lam, S.-G. Lee, H.-J. Lee, and Y. E. Oktian, "Securing distributed SDN with IBC," in *2015 Seventh International Conference on Ubiquitous and Future Networks*, Sapporo, Japan, Jul. 2015, pp. 921–925, https://doi.org/10.1109/ICUFN.2015.7182680.

[39] L. A. Khalil Al Dulaimi, R. Badlishah Ahmad, N. Yaakob, and Q. M. Hussein, "A Secured OpenFlow Protocol Using Elliptic Curves Cryptographic for Software Defined Networks," *Journal of Physics: Conference Series*, vol. 1019, no. 1, Mar. 2018, Art. no. 012014, https://doi.org/10.1088/1742-6596/1019/1/012014.

[40] H. M. Alshameri and P. Kumar, "An Efficient Zero-Knowledge Proof Based Identification Scheme for Securing Software Defined Network," *Scalable Computing: Practice and Experience*, vol. 20, no. 1, pp. 181–189, Mar. 2019, https://doi.org/10.12694/scpe.v20i1.1473.

[41] S. S. Mahdi and A. A. Abdullah, "Improved Security of SDN based on Hybrid Quantum Key Distribution Protocol," in *2022 International Conference on Computer Science and Software Engineering (CSASE)*, Duhok, Iraq, Mar. 2022, pp. 36–40, https://doi.org/10.1109/CSASE51777.2022.9759635.

[42] M. H. Rempola, A. Smith, Y. Li, and L. Du, "Securing SDN Communication through Quantum Key Distribution," in *2024 IEEE Transportation Electrification Conference and Expo (ITEC)*, Chicago, IL, USA, Jun. 2024, pp. 1–5, https://doi.org/10.1109/ITEC60657.2024.10598919.

[43] B. Yigit, G. Gur, B. Tellenbach, and F. Alagoz, "Secured Communication Channels in Software-Defined Networks," *IEEE Communications Magazine*, vol. 57, no. 10, pp. 63–69, Oct. 2019, https://doi.org/10.1109/MCOM.001.1900060.

[44] T. Mahboob, I. Arshad, A. Batool, and M. Nawaz, "Authentication Mechanism to Secure Communication between Wireless SDN Planes," in *2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, Islamabad, Pakistan, Jan. 2019, pp. 582–588, https://doi.org/10.1109/IBCAST.2019.8667157.

[45] N. S. Bülbül, O. Ermis, Ş. Bahtiyar, M. U. Çağlayan, and F. Alagöz, "Trust Enhanced Security for Routing in SDN," in *2022 1st International Conference on 6G Networking (6GNet)*, Paris, France, Jul. 2022, pp. 1–6, https://doi.org/10.1109/6GNet54646.2022.9830213.

[46] M. Almakhour, A. Wehby, L. Sliman, A. E. Samhat, and A. Mellouk, "Smart Contract Based Solution for Secure Distributed SDN," in *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, Apr. 2021, pp. 1–6, https://doi.org/10.1109/NTMS49979.2021.9432647.

[47] P. Ohri, S. G. Neogi, S. Sengupta, D. Arockiam, and S. K. Muttoo, "Blockchain-Based Smart Contract Architecture for Inter-Domain SDN Controller Communication," in *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, Mar. 2024, pp. 1–6, https://doi.org/10.1109/ICRITO61523.2024.10522419.

[48] K. U, T. Swetha, I. Sharma, R. Keerthana, V. Tejashwini, and G. G. Devarajan, "Enhancing Cloud IoT Security With Blockchain and SDN," in *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)*, Gautam Buddha Nagar, India, Feb. 2024, pp. 973–978, https://doi.org/10.1109/IC3SE62002.2024.10593053.

[49] K. Sibiya, M. Molefe, and B. Nleya, "A SDN Multi-Controller and Blockchain Enabled Authentication Framework for Cloud Computing," in *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Sydney, Australia, Jul. 2024, pp. 1–9, https://doi.org/10.1109/ICECET61485.2024.10698401.

[50] A. Derhab, M. Guerroumi, M. Belaoued, and O. Cheikhrouhou, "BMC-SDN: Blockchain-Based Multicontroller Architecture for Secure Software-Defined Networks," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, 2021, Art. no. 9984666, https://doi.org/10.1155/2021/9984666.

[51] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, "Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT," *Digital Communications and Networks*, vol. 9, no. 2, pp. 411–421, Apr. 2023, https://doi.org/10.1016/j.dcan.2022.11.003.

[52] S. Boukria, M. Guerroumi, and I. Romdhani, "BCFR: Blockchain-based Controller Against False Flow Rule Injection in SDN," in *2019 IEEE Symposium on Computers and Communications (ISCC)*, Barcelona, Spain, Jun. 2019, pp. 1034–1039, https://doi.org/10.1109/ISCC47284.2019.8969780.

[53] A. Alkhamisi, I. Katib, and S. M. Buhari, "Blockchain-Based Control Plane Attack Detection Mechanisms for Multi-Controller Software-Defined Networks," *Electronics*, vol. 13, no. 12, Jan. 2024, Art. no. 2279, https://doi.org/10.3390/electronics13122279.

[54] H. Eltaief, K. Thabet, and E. Kamel Ali, "Securing East-West Communication in a Distributed SDN," in *Hybrid Intelligent Systems*, 2023, pp. 1225–1234, https://doi.org/10.1007/978-3-031-27409-1_112.

[55] H. N. Nguyen, S. Souihi, H.-A. Tran, and S. Fowler, "A Blockchain-based SDN East/West Interface," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, Rio de Janeiro, Brazil, Sep. 2022, pp. 5759–5764, https://doi.org/10.1109/GLOBECOM48099.2022.10001381.

[56] S. C. Tollefson, "Utilizing Blockchain to Design an East/West Interface for Federated Software Defined Networks," M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 2018.

[57] W. Fan, S.-Y. Chang, S. Kumar, X. Zhou, and Y. Park, "Blockchain-based Secure Coordination for Distributed SDN Control Plane," in *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, Tokyo, Japan, Jun. 2021, pp. 253–257, https://doi.org/10.1109/NetSoft51509.2021.9492615.

[58] B. A. Almohagri, M. A. Saeed, H. M. Alazaby, and A. I. Mohammed, "Machine Learning Approach for Distributed Daniel of Service Attack Detection in SDNs," in *2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, Taiz, Yemen, Jul. 2023, pp. 01–07, https://doi.org/10.1109/eSmarTA59349.2023.10293527.

[59] L. Mhamdi and M. M. Isa, "Securing SDN: Hybrid autoencoder-random forest for intrusion detection and attack mitigation," *Journal of Network and Computer Applications*, vol. 225, May 2024, Art. no. 103868, https://doi.org/10.1016/j.jnca.2024.103868.

[60] M. M. Ahmed and H. Abdulkader, "An ensemble-based approach for effective distributed denial of service attack detection in software

defined networking," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 13, no. 2, pp. 2019–2026, Jun. 2024, https://doi.org/10.11591/ijai.v13.i2.pp2019-2026.

[61] S. Mani and M. J. Nene, "Preventing Distributed Denial of Service Attacks in Software Defined Mesh Networks," in *2021 International Conference on Intelligent Technologies (CONIT)*, Hubli, India, Jun. 2021, pp. 1–7, https://doi.org/10.1109/CONIT51480.2021.9498378.

[62] A. Sharma, D. Upadhyay, and S. Sharma, "Enhancing blockchain security: a novel approach to integrated malware defence mechanisms," *Engineering Research Express*, vol. 6, no. 2, Feb. 2024, Art. no. 025215, https://doi.org/10.1088/2631-8695/ad4ba7.

[63] Y. Yan, Z. Chen, and V. Varadharajan, "Control of Large-Scale Networked Cyberphysical Systems Using Cryptographic Techniques." arXiv, Aug. 20, 2020, https://doi.org/10.48550/arXiv.2002.03470.

[64] D. Das, U. Ghosh, N. Evans, and S. Shetty, "Blockchain-Enabled Secure Device-to-Device Communication in Software-Defined Networking," in *2024 IEEE International Conference on Communications Workshops (ICC Workshops)*, Denver, CO, USA, Jun. 2024, pp. 1450–1455, https://doi.org/10.1109/ICCWorkshops59551.2024.10615611.