MALAYSIAN JOURNAL OF
CYBERSECURITY AND APPLICATIONS

A SURVEY ON CONTROL PLANE SECURITY APPROACHES IN SDN ENVIRONMENTS: ISSUES AND CHALLENGES

Mohammed Awwal Iliyasu[1,2], Azizol Abdullah[2*], Zurina Mohd Hanapi[2], Normalia Samian[2]

[1]Department of Computer Science, School of Science, Umaru Sanda Ahmadu College of Education, P.M.B 39 Minna, Nigeria.
[2]Department of Communication Technology and Networking, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia.

awwaliliyasu@gmail.com[1,2], azizol@upm.edu.my[2*], zurinamh@upm.edu.my[2], normalia@upm.edu.my[2]

ABSTRACT

The emergence of Software-Defined Networking as a transformative paradigm in network architecture offers enhanced flexibility and scalability through a centralized control system. This control plane is responsible for routine decisions and coordinating policies across the network, which makes it a prime target for malicious attacks. This study investigates recently proposed solutions for enhancing control plane security by analyzing their techniques, strengths and weaknesses through a systematic review. The reviewed security techniques were clustered into four key approaches: authentication and authorization, data encryption and secure communication, intrusion detection and prevention, and resilience and fault tolerance. The issues and challenges of the techniques were highlighted for each categorized approach. Future research directions are presented to serve as a baseline for further study.

Keywords: Software-Defined Networking; Control Plane Security Approaches; Control Plane Security Issues; Control Plane Security Challenges.

1. INTRODUCTION

Software Defined Networking (SDN) is an emerging networking architecture that separates the control plane from the data plane and enables programmable control over network resources through an Application Programming Interface (API). It has emerged as a leading networking architecture, streamlining network services and fostering innovation in communication. Due to central control feature of the control plane, it's responsible for coordinating the network services and logical decisions such as providing instructions to the data plane. The data plane, in turn, comprises network devices that follow these control instructions to forward data packets efficiently. This architectural transformation has yielded significant attention from both the network industries and academic domains [1].

SDN introduces a standardized and uniform API, which seamlessly incorporates programmable features into the network. The API resolves the inherent challenges of traditional networks such as inflexibility of network configuration and limited programmability across the network. It provides a flexible and manageable interface that can adapt to evolving requirements [2]. The SDN control plane offers a comprehensive view and management of the network topology, enabling dynamic upgrades and future enhancements of network functionalities.

Jammal et al. [3] assert that the controller and API features of the SDN network has led to its endorsement in academia and industry. This endorsement is crucial as security concerns have worsened in network environments, including cloud and peer to peer networks. Despite the benefits of SDN, it faces challenges in regards to its scalability, controller placement, latency and reliability. A notable drawback is the vulnerability to security attacks across SDN layers, which has emerged as a significant concern. Evolving security threats encompass issues such as flow rule consistency, controller vulnerabilities, legitimacy concerns, harmful applications and susceptible communication channels for northbound and southbound interfaces [4, 5].

The objective of this study is to investigate SDN control plane security measures proposed in the previous studies by scrutinizing relevant articles, evaluating their security measures and outlining the issues and challenges associated with the techniques used.

This study makes the following contributions:

- Present a taxonomy of control plane security approaches.
- Review control plane security techniques, analyzing their strengths and weaknesses.
- Clusters, examines and highlights the associated issues and challenges.
- Identifies future research trends based on the analysis of the existing studies.

This article is organized as follows: Section 1 provides an Introduction to the topic. Section 2 reviewed the background of SDN and its Architecture. Section 3 outlines the Research Method used in this study. Section 4 shows the Reviews and Discussions, consisting of a Taxonomy of SDN Control Plane Security Approaches, review on SDN Control Plane Security Approaches and analysis of the Issues and Challenges associated with these approaches. Finally, Section 5 concludes the paper with a summary and a future research direction.

1.1 Comparison of Related Surveys

In recent years, substantial research has been conducted to address the security challenges inherent in SDN control plane. For instance, Hirsi et al. [6] deliver an extensive analysis of security challenges and potential solutions within SDN, focusing on data and control planes security solutions. The authors thoroughly examined the traditional, AI-based and Moving Target Defense-based security solutions and highlighted future research directions. However, while their analysis of traditional techniques is comprehensive, it does not delve into resilience and fault tolerance reviews and it includes only few reviews on authentication and authorization solutions. Similarly, Bhuiyan et al. [7] provide a structured approach on vulnerabilities and attacks in SDN. The study includes detailed classifications and taxonomies of attacks and countermeasures, offering valuable insights into control plane attacks and practical guidance for enhancing security measures. Although their classification system may benefit from recent developments and emerging attack vectors that have evolved since their study, it did not delve into access control, data encryption and secure communication, intrusion detection and prevention, resilience and fault tolerance countermeasures, as these did not align with the attack solutions reviewed in their study.

Rahouti et al. [8] reviewed SDN's core functionalities and security challenges, categorizing solutions based on threats specific to different layers of the SDN infrastructure. This comprehensive review highlights key use cases and emerging research trends relevant to securing SDN environments. However, it has limited exploration of recent advances in resilience and fault tolerance techniques.

Further, Jimenez et al. [9] address security vulnerabilities and mitigation strategies across all layers and interfaces of the SDN architecture. The authors used Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege (STRIDE) threat modeling methodology and identified both existing issues and future research directions. Although their approach is methodical, it has not extensively captured the nuanced challenges and cutting-edge solutions that have emerged in the rapidly evolving field of SDN control plane security approaches, such as authentication and authorization, data encryption and secure communication, intrusion detection and prevention and resilience and fault tolerance.

Additionally, Aladaileh et al. [10] focus on the impact of Distributed Denial of Service (DDoS) attacks on SDN controllers, analyzing various detection techniques and comparing them based on technique, features and deployment locations within the SDN environment. While their study offers a valuable comparison of detection methods, specifically using the Intrusion Detection and Prevention approach, it did not address the broader spectrum of control plane security approaches.

In contrast, Nisar et al. [11] offer a comparative survey of SDN and traditional networking, exploring the OpenFlow protocol and analyzing SDN security threats and countermeasures. The authors also discussed the benefits of SDN and proposed future directions for enhancing SDN security solutions. Their survey focuses solely on authentication and authorization techniques and does not address other control plane security approaches.

Our study extends existing surveys by reviewing up-to-date techniques for securing the SDN control plane. We categorize the proposed techniques into approaches and reviewed various articles security measures; methods and their strengths. The issues and challenges associated with each approach is highlighted and future research trends were identified. Table 1 comparatively summarize our study and other related surveys as an overview of the state of the art in the SDN control plane security surveys.

Table 1: Comparison of related study

S.No.	Ref.	A	I	TSA	FR	Security Approaches				Latest Ref.				
						AA	DESC	IDP	RFT	2021	2022	2023	2024	2025
1	[11], 2020	√	↑	×	×	√	×	×	×	×	×	×	×	×
2	[10], 2020	√	↑	×	√	×	×	√	×	×	×	×	×	×
3	[9], 2021	√	√	×	√	↑	↑	↑	↑	√	×	×	×	×
4	[8], 2022	√	↑	×	√	√	√	√	↑	√	√	×	×	×
5	[7], 2023	√	√	×	√	√	×	×	×	√	√	×	×	×
6	[6], 2023	√	√	×	√	√	√	√	×	√	√	√	×	×
7	This study	√	√	√	√	√	√	√	√	√	√	√	√	√

√ indicates the topic is well covered, × is uncovered and ↑ partially covered.

Ref.: Reference, A.: Architecture of SDN, I.: Issues and Challenges of existing Security Approaches, TSA.: Taxonomy of SDN Security Approaches, FR.: Future Research, AA.: Authentication and Authorization, DESC.: Data Encryption and Secure Communication, IDP.: Intrusion Detection and Prevention, RFT.: Resilience and Fault Tolerance.

2. SOFTWARE DEFINED NETWORKING

SDN is an emerging network architecture that manages networks and their connections using a centralized control system (the controller) and a data plane for data transmission via communication channels. The control plane and data plane are segregated to expedite and simplify configuration of communication mediums for application and network services [12]. The dissimilarity between traditional and SDN networks lies in the control and data planes. Figure 1 depicts a traditional network and SDN architecture. In traditional network, the control and data planes are tightly integrated within a network device, while in an SDN, they are decoupled and a centralized controller manages the network's behavior.

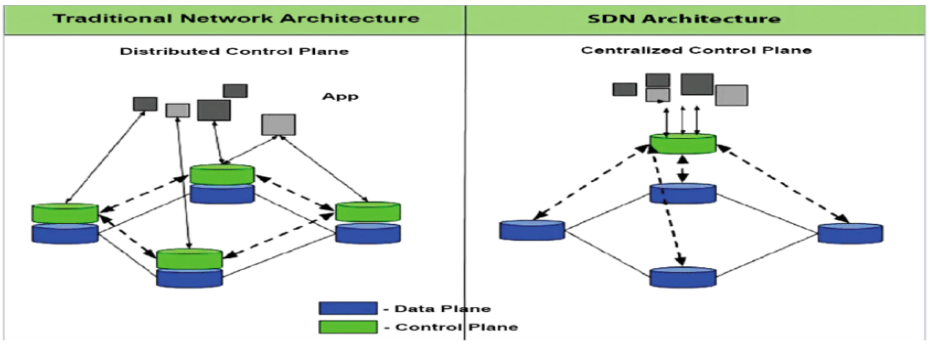

Fig. 1: Traditional and SDN Architectures [12]

In SDN, the separated control planes from traditional networks are integrated into a novel entity, the SDN controller, which is strategically centralized to manage the distinct data planes. This configuration enhances programmability for the development of network applications. The centralization of the network control system has resulted in cost effectiveness, enhanced network visibility, improved resource utilization efficiency and increased network performance [13]. SDN programmability is an innovative feature that offers dynamic initiation, control, modification and management of network behavior via an open interface such as OpenFlow. Additionally, it simplifies the centralized, intelligent management and control of each network device or component separately through the use of a software [14].

2.1 SDN Architecture

SDN architecture comprises three planes [15], also known as layers. Figure 2 presents these three layers: the data layer, control layer and application layer [2,16].

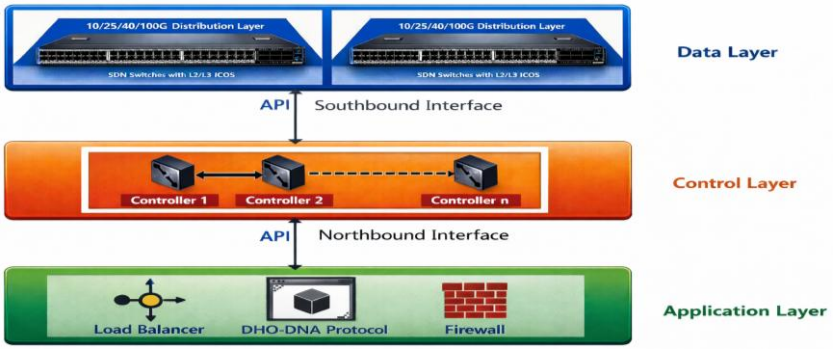

Fig. 2: SDN Architecture

2.1.1 Application Layer

The application layer hosts business-aligned applications that implement control logic to modify network behavior. Also known as the management layer, it provides services such as task scheduling, traffic control and system security [16] and serves as the execution platform for business and security applications. Applications implemented at this layer include intrusion prevention systems (IPS), firewalls, load balancers, access control systems, network virtualization and Intrusion Detection Systems (IDS) [17] [18]. These applications leverage the programmability and flexibility of the SDN architecture to dynamically control and adapt network behavior based on specific requirements and conditions.

2.1.2 Control Layer

The control layer consists of a central entity called the controller. It programs network resources, dynamically updates forwarding rules and enhances the flexibility and agility of network administration. This layer's overarching role is to oversee the operational aspects of the entire network, making decisions related to packet forwarding and routing. The controller communicates with the data layer via a southbound API. This controller function is implemented by various software platforms and frameworks, such as Floodlight, POX, NOX, Maestro and Jaxon [18].

2.1.3 Data Layer

The Data layer, also referred to as the forwarding or infrastructure layer in some literature, consists of network devices (e.g., switches) that forward, buffer and update packets based on instructions from the control layer. These switches contain modules dedicated to packet processing, which rely on rules received from the controller via the southbound interface. The southbound interface is the standardized communication link between the control and data layers. The separation of these layers allows network administrators to adjust security policies and network behavior easily through software, enabling the creation of agile networks that can meet evolving business requirements [16].

3.0 STUDY DESIGN

A systematic literature review was conducted following the PRISMA guidelines for the period from January 1, 2020, to December 31, 2025. The review activities were achieved by defining research questions, identifying the article inclusion and exclusion selection criteria, implementing search strategies and applying selection criteria.

3.1 Research Questions

1. What are the primary security approaches proposed for securing the SDN control plane in recent literature (2020-2025)?
2. What methods, strengths and weaknesses characterize the proposed techniques within each security approach?
3. What are the key issues and challenges associated with existing control plane security techniques?

4. How do the proposed techniques compare across different security approaches in terms of their effectiveness and applicability?
5. What future research directions are needed to address the identified gaps and challenges in SDN control plane security?

The first research question guides the identification and categorization of control plane security techniques into the four approaches presented in the taxonomy.

The second research question facilitates a detailed analysis of individual studies, resulting in tables that summarize each technique's security measures, methods, strengths and weaknesses.

The third research question addresses limitations, vulnerabilities and performance trade-offs in the surveyed literature, culminating in the "Issues and Challenges" analysis.

The fourth research question supports the comparative analysis and synthesis of findings, helping to highlight gaps and trends in the research landscape.

The fifth research question informs the derivation of future research trends from the analysis of existing studies limitations.

3.2 Inclusion and Exclusion Criteria

The study used four-point eligibility criteria presented in Table 2, to retrieve articles relevant to the study. The eligibility is based on inclusion and exclusion criteria used to retrieve and group the articles into their corresponding security approaches identified in the study.

Table 2: Inclusion and exclusion Criteria for article selection

Inclusion	Exclusion
Study focuses on control plane or controller-switch channel security	Study focuses on data plane, application plane, or northbound API security
Study proposes or implements a security technique, mechanism, or framework	Study is a review, survey, or non-technical overview paper lacking technical implementation or analysis
Full text is available in English	Full text is not in English or is inaccessible
Study is published between 2020–2026	Study is published before 2020 or after December 31, 2025

3.3 Information Sources

A manual literature search was conducted across major academic databases, including Science Direct, IEEE Xplore, Wiley and Springer. Table 3 depicts the information sources and their URLs.

Table 3: Information Sources

Platforms	URL
Science Direct	http://www.sciencedirect.com
IEEE Xplore	https://ieeexplore.ieee.org/Xplore/home.jsp
Wiley	https://onlinelibrary.wiley.com
Springer	http://www.springer.com

3.4 Search Strategy

A systematic search was conducted using a combination of keywords and Boolean operators across title, abstract and keyword fields. The primary search terms focused on three core concepts: (1) Software-Defined Networking, (2) control plane and (3) security.

The base search string was structured as follows:

("Software-Defined Networking" OR "SDN") AND ("control plane" OR "controller") AND ("security" OR "protection" OR "defense").

This string was adapted as needed for the search syntax of each database platform (Science Direct, IEEE Xplore, Wiley, Springer). Date filters were applied to restrict results to publications from January 1, 2020, onward and language filters were set to English only.

3.5 Study Selection Process

The study selection followed the four-stage PRISMA framework, as illustrated in Figure 3: (1) Identification of records through database searches; (2) Screening of titles and abstracts against inclusion/exclusion criteria; (3) Eligibility assessment via full-text review; and (4) Final inclusion of articles for qualitative synthesis. Duplicate records were removed prior to screening.

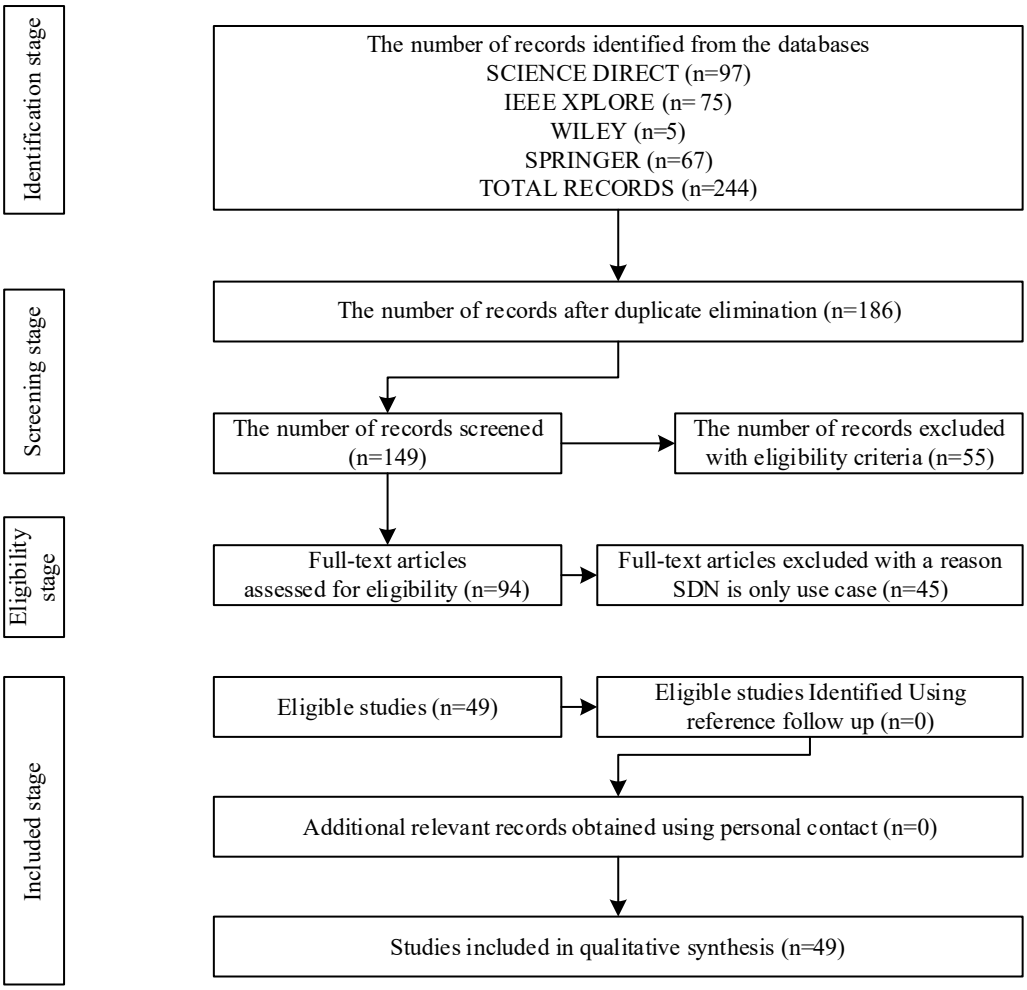

Fig. 3: The study workflow with PRISMA

3.6 Data Collection and Synthesis

Data from included studies were extracted using a standardized form capturing: publication details, security approach, specific techniques, methods, strengths, weaknesses and identified challenges. The extracted data were synthesized thematically according to the four security approaches identified in the taxonomy.

4.0 REVIEW AND DISCUSSIONS

This section presents the key contributions of this paper. We proposed a taxonomy for SDN control plane security approaches and categorized the reviewed articles within this taxonomy based on their techniques. The security measures, methods and respective strengths from these articles were analyzed and summarized. Furthermore, the issues and challenges associated with the techniques identified in the existing literature were clustered and examined.

4.1 Taxonomy of SDN Control Plane Security Approaches

The proposed taxonomy of SDN control plane security approaches is depicted in Figure 4 and classified into four broad areas. The taxonomy organizes key defensive strategies and countermeasures into coherent categories, mapping them to specific academic research. This classification serves as a framework for understanding the current research landscape and the evolution of security mechanisms intended to protect data, ensure system integrity and maintain operational availability in distributed and connected environments.
The taxonomy is hierarchically structured around a primary objective: Control Plans. This top-level category is subdivided into core Security Approaches. The taxonomy effectively structures the complex field of SDN control plane security into a logical framework. It synthesizes a wide body of academic literature, providing a valuable reference for understanding the current state of security strategies and for guiding the development of robust, multi-faceted defense mechanisms for critical and connected systems.

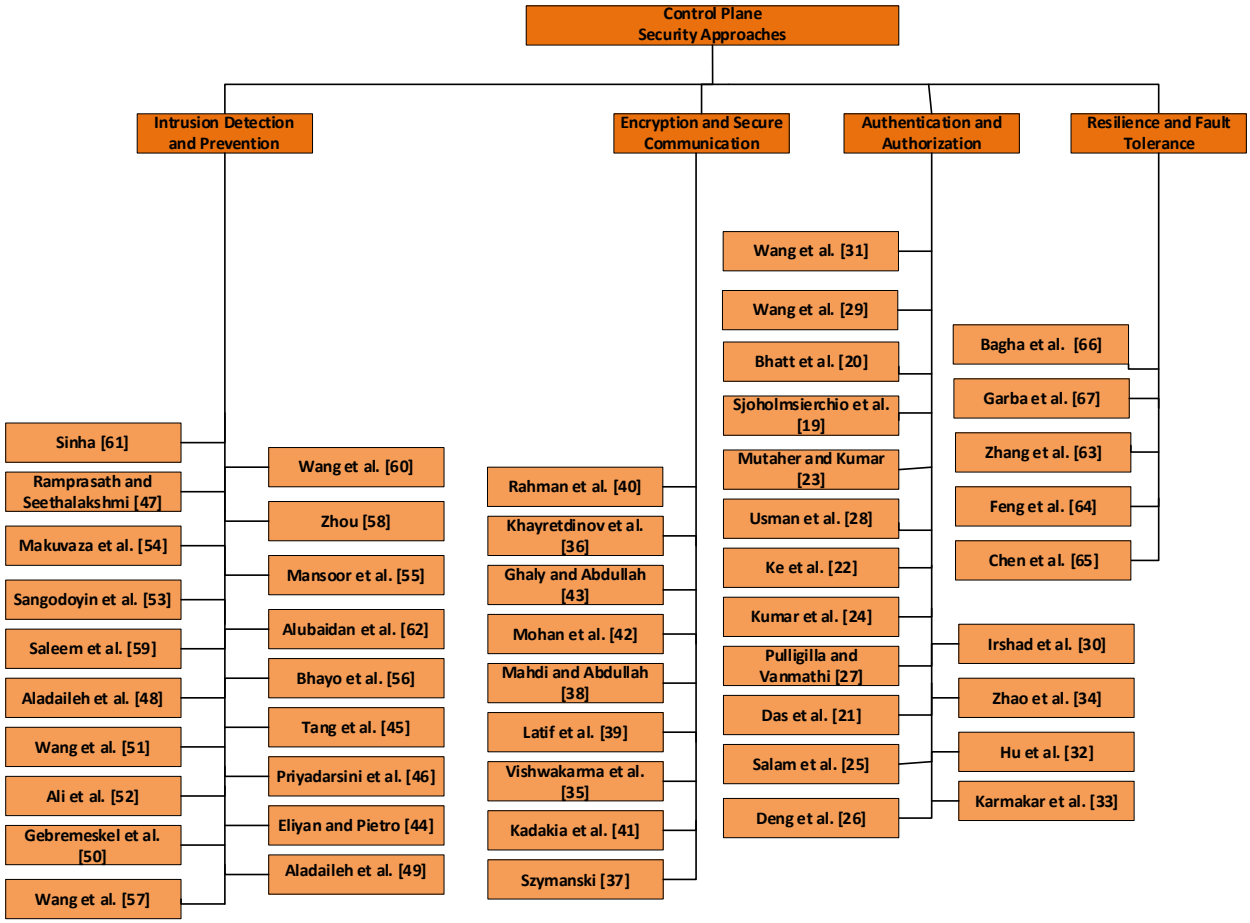

Fig. 4: Taxonomy of control plane security approaches

4.1.1 Authentication and Authorization

Authentication and Authorization approach focus on mechanisms that established and managed secured and authorized connections. In the realm of authentication and authorization within SDN control plane security, the reviewed articles address several authentication components, including controller, application and user authentication techniques.

4.1.2 Data Encryption and Secure Communication

Data encryption and secure communication are techniques for protecting data confidentiality and integrity using secured communication protocols. In this category, the reviewed papers include channel and data encryption techniques. The review covers proposed advancements in encryption algorithms, key management practices and the strength of the proposed techniques, offering a detailed examination of how these methods contribute to overall network security.

4.1.3 Intrusion Detection and Prevention

Intrusion detection and prevention focus on identifying and mitigating unauthorized access. This approach includes anomaly detection, signature-based detection and behavioral analysis. Anomaly detection involves identifying deviations from normal behavior that could indicate potential security breaches. articles in this area explore various techniques for detecting unusual patterns or activities that may signify an attack or intrusion. Signature-based detection focuses on using known attack patterns to identify malicious activities. This traditional method relies on predefined signatures of known threats. Furthermore, behavioral analysis research monitors the behavior of entities within the SDN to detect potential threats based on behavioral patterns rather than predefined signatures. This approach enhanced the development of sophisticated monitoring tools and algorithms to analyze and respond to emerging threats.

4.1.4 Resilience and Fault Tolerance

Resilience and Fault Tolerance focus on enhancing system reliability and robustness against failures and attacks. In this approach, the reviewed studies cover redundancy, failover mechanisms and DDoS mitigation. It addresses the effectiveness of different DDoS mitigation strategies and their impact on maintaining the resilience of SDN environments.

4.2 SDN Control Plane Security Approaches

This study reveals several proposed techniques used in securing the control plane of an SDN in the following categories.

4.2.1 Authentication and Authorization

Control plane authentication and authorization techniques are crucial for maintaining the security and integrity of network operations, given the control plane's central role in managing network policies and traffic flow. Effective techniques are used to prevent unauthorized access and ensure that network functions operate smoothly. Sjoholmsierchio et al. [19] introduced a per-message authentication strategy designed to defend against downgrade attacks, enhancing the robustness of control plane interactions. Bhatt et al. [20] proposed an authentication-based access and clustering approach to strengthen the control plane security by efficiently managing access and securing communication channels.

Reviews on controller authentication approach focuses on mechanisms that ensure only legitimate controllers can communicate with network devices, thus preventing unauthorized access and potential security breaches. Table 4 explores various authentication protocols and methods that effectively validate controller identities.

Table 4: Controller Authentication reviews

Reference	Security Measure	Method	Strength	Weaknesses
Das et al. [21]	Blockchain-enabled SDN security	Combined SDN and blockchain for 5G network security with controller authentication and smart contracts.	Improves network transparency, data security and user privacy.	Lack of security consensus algorithms; slow blockchain transaction speed.
Ke et al. [22]	Two-phase SDN authentication	Implemented a two-phase authentication scheme in an SDN gateway to protect user data.	Improves security, user data protection, with lower computing and high storage efficiency.	Inadequate in addressing virtual machine concerns; potentially vulnerable to spoofing attacks.
Mutaher and Kumar [23]	Kerberos authentication	Used the Kerberos protocol for host credential verification in SDN environments.	Enhances secure communication and protection against network attacks.	Single point of failure; reliance on a centralized authentication server may limit scalability.
Bhatt et al. [20]	Authentication and clustering	Integrated authentication-based access with clustering for control plane security.	Mitigates single point of failure and improved security through clustering.	Potential scalability issues; complexity in clustering management can introduce overhead.

Application Authentication approach allows only trusted applications to interact with the controller, thereby securing the communication channel between applications and the SDN controller. This involves exploring advanced authentication techniques and protocols to ensure the integrity and trustworthiness of applications interacting with the network. Table 5 summarizes articles proposing various application authentication techniques.

Table 5: Application Authentication reviews

Reference	Security Measure	Method	Strength	Weaknesses
Kumar et al. [24]	Blockchain-based authentication and intrusion detection	Utilized blockchain for secure communication and employed digital twin with deep learning for real-time intrusion detection.	Enhances low latency and real-time detection in Smart Grid networks.	Limited applicability outside Smart Grid networks; reliance on specific infrastructure may reduce versatility.
Salam et al. [25]	DC-IIoT authentication	Developed a DC-IIoT authentication protocol using a threshold-based approach for detecting cloning attacks.	Achieves resistance to various attacks with a good balance between security and efficiency.	Delay in response time due to algorithm complexity; potential difficulties in real-time applications.
Deng et al. [26]	Privacy-preserving authentication	Integrated PAS with SDN for VANETs, focusing on	Enhances anonymity and	Assumes the presence of

		trust models and authentication.	secure communication while preserving privacy in VANETs.	trusted entities, which may not always be realistic; limited adaptability to varied environments.

Node/User Authentication is another critical aspect of authentication reviewed, where research investigates methods to confirm the identities of nodes accessing the network. This includes exploring multi-factor authentication and other advanced user verification techniques, as summarized in Table 6.

Table 6: Node/User Authentication reviews

Reference	**Security Measure**	**Method**	**Strength**	**Weaknesses**
Sjoholmsierchio et al. [19]	Per-message authentication	Designed a per-message authentication mechanism to prevent TLS downgrade attacks.	Effectively mitigates TLS downgrade attacks with minimal overhead.	Potential trade-off between security and cost of the proposed derivatives; may not fully address all attack vectors.
Pulligilla and Vanmathi [27]	Optimization-based intrusion detection	Applied Rider-Sea Lion Optimized Neural Network with Rényi entropy for feature selection and intrusion detection.	Achieves 92.5% precision, 95.4% recall and 94% F-measure.	Limited to specific network environments; may require extensive training data for optimal performance.
Usman et al. [28]	Lightweight authentication for Unmanned Arial Vehicles (UAVs)	Developed ECC-based challenge-response authentication for UAV control planes.	Resolves packet drop issues and enhanced UAVs identity authentication security.	Delay in response time due to algorithm complexity; may not perform well in high-density UAVs environments.
Wang et al. [29]	Efficient authentication key agreement	Developed a key agreement scheme using NTRU, hash chains and CRT for secure handovers in integrated railway networks.	Outperformed other schemes in cost, overhead and performance, ensuring higher security.	Single point of failure; performance may degrade under high-load scenarios.
Irshad et al. [30]	Three-factor authentication for user access	Implemented mutual authentication in SDN controllers to control user access and secure the control plane.	Protects against CK-model attacks with a balance between security and computational efficiency.	Limited real-world validation and insufficient analysis of scalability, usability and controller compromise risks
Wang et al. [31]	Flexible Certificateless Signature-based (FCLS) authentication	Utilized fuzzy certificateless signatures with secret sharing and anonymous biometric identities for VANETs.	Improved error tolerance, efficient, privacy-preserving, flexible, no key escrow.	Biometric dependency, computational overhead, Hamming distance limits.

Hu et al. [32]	Representational State Transfer (REST) API access control and encryption	Utilized secure application management framework (SEAPP) with encrypted API registrations and risk-based authorization for SDN environments.	Provides secure application management with granular permissions, encrypted API calls and effective detection of malicious apps.	Relies heavily on the SEAPP framework and predefined risk models.
Karmakar et al. [33]	Fine-grained network access control	Developed a framework for enhancing Internet of Things (IoT) network access control and defending against malicious devices and attacks.	Improves network control and protection with a lightweight device authentication approach.	Lacks extensive validation in large-scale, heterogeneous IoT settings.
Zhao et al. [34]	Enhanced data protection and access control	Applied SASP with Attribute-Based Encryption (ABE) and Hierarchical Predicate ABE for securing vehicular social networks.	Boosts fine granularity, data integrity, stronger access control and recipient privacy through ciphertext re-randomization.	High computational cost, limited real-world experimentation.

4.2.2 Data Encryption and Secure Communication

To ensure the security of control plane in SDNs, robust encryption techniques are reviewed. Various methods have been proposed to fortify critical communication channels. For instance, encryption protocols leveraging elliptic-curve cryptography (ECC) and SHA-256 are employed to secure communication channels and ensure data integrity [35]. Encrypted labels in packet headers help in detecting and mitigating malicious traffic by dropping packets with invalid labels [36]. Advancements such as post-quantum cryptography and AI algorithms are being integrated into SD-WANs and D-switches to enhance network communication and security [37].
Channel encryption reviews focus on ensuring secure communication channels between controllers, applications and devices, often employing protocols such as TLS/SSL. This aspect of the research investigates how encryption can protect data as it travels across the network, securing it from interception and tampering. Table 7 depicts a summary of channel encryption articles proposed to secure communication channels, highlighting their contributions and effectiveness in securing SDN control plane.

Table 7: Communication Channel Encryption

Reference	Security Measure	Method	Strength	Weaknesses
Mahdi and Abdullah [38]	Hybrid classical and quantum key distribution	Combined classical and quantum key distribution with TLS for secure communication.	Enhances authentication, security and confidentiality.	TLS adaptation issues; single points of failure.
Latif et al. [39]	Distributed trust-based authentication and blockchain	Used distributed trust and private/public blockchains for communication security.	Improves security and energy efficiency.	Non-scalable; potential vulnerabilities in decentralized trust models.
Khayretdinov et al. [36]	Encrypted labels for traffic security	Used encrypted labels in packet headers to detect and mitigate malicious traffic.	Increases DoS attack mitigation effectiveness by 7.8 times.	Limited applicability in diverse industrial contexts; may not fully protect

				against advanced persistent threats.
Szymanski [37]	Post Quantum Cryptography (PQC) and AI	Integrated PQC and AI algorithms in Software-Defined Deterministic Wide Area Networks (SDD-WANs) for enhanced security.	Enhances flexibility, security and reliability in SDD-WANs.	Lack of empirical data and experimental validation in real-world scenarios; potential integration challenges with existing systems.
Rahman et al. [40]	Blockchain for data security	Integrated SDN and blockchain with sensor devices in 5G networks for remote patient health monitoring.	Enhances security and confidentiality with SDN, Blockchain and 5G technologies.	Limited to specific applications; potential overhead associated with integrating blockchain with existing infrastructures.
Kadakia et al. [41]	Encrypted two-tier control architecture	Combined encrypted nonlinear LMPC with encrypted linear controllers and used an ML-based cyberattack detector.	Improves cybersecurity for nonlinear processes with integrated ML-based attack detection.	Introduce latency in communication; complexity of implementation could hinder adoption.

Data encryption, on the other hand, involves protecting data both at rest and in transit within the control plane. Studies in this category explore various encryption techniques and strategies to safeguard sensitive information stored in network devices or transmitted across the network, as shown in Table 8.

Table 8: Data Encryption reviews

Reference	**Security Measure**	**Method**	**Strength**	**Weaknesses**
Mohan et al. [42]	Dynamic crypto key distribution and lightweight cryptography	Used SDN-enabled IoT and switches as fog nodes with performance assessment.	Reduces energy consumption by over 90% and enhances security.	Potential trade-offs between lightweight implementation and security robustness; limited scalability in larger networks.
Vishwakarma et al. [35]	ECC and SHA256 for data security	Integrated ECC and SHA256 in a Location-Based Service for Vehicles authentication and integrity.	Reduces computational cost, storage and communication overhead while preventing identity theft.	Non-Scalable; effectiveness can vary based on implementation context.

Ghaly and Abdullah [43]	Hybrid encryption (AES and RSA)	Implemented AES and RSA algorithms for data protection and authenticity.	Enhances security and efficiency with robust hybrid encryption methods.	Single point of failure; reliance on specific encryption methods limits flexibility in dynamic environments.

4.2.3 Intrusion Detection and Prevention

As network systems become increasingly vulnerable to Distributed Denial of Service (DoS) attacks, the need for advanced Intrusion Detection and Prevention (IDP) techniques has become paramount. Several IDP techniques are designed to enhance network security through sophisticated algorithms and innovative methodologies. Techniques such as entropy and proof of work, with predefined installation flow rules, have been introduced to control packet traffic during DoS attacks, effectively managing packet retransmission [44]. The Flow Table Overflow Protocol (FTOP) addresses Low-rate Flow Table Overflow (LFTO) attacks by utilizing advanced algorithms within distinct modules for prediction, detection, mitigation and prevention [45]. Additionally, the Trust-Based Controller Attack Detection (TCAD) model and the Risk-Based Attack Prevention (RAP) model leverage a game-theoretic approach to achieve 95% accuracy in detecting and filtering malicious traffic flows [46]. Table 8 provides a detailed review of these and other IDP techniques, highlighting their effectiveness and application in safeguarding network systems.
Anomaly detection involves identifying deviations from normal behavior that could indicate potential security breaches. Table 9 summarizes various techniques for detecting unusual patterns or activities that may signify an attack or intrusion.

Table 9: Anomaly Detection reviews

Reference	Security Measure	Method	Strength	Weaknesses
Eliyan and Pietro [44]	Sample entropy with proof-of-work	Combined entropy and proof-of-work with flow rule scheduling at SDN controllers.	Reduces control and retransmitted packets during DoS attacks.	Poor differentiation between legitimate and malicious traffic.
Ramprasath and Seethalakshmi [47]	Dynamic Access Control Lists (ACLs) for anomaly detection	Used dynamic ACLs, traffic categorization and Shannon entropy for detection and prevention.	Enhances SDN security and mitigates DoS attacks.	High controller overhead due to dynamic ACL updates.
Aladaileh et al. [48]	Dynamic Threshold and Rule-Based detection	Applied dynamic thresholds and rule-based methods for high-rate attack detection.	Detects high-rate DDoS attacks with low false positives.	Ineffective for multi-point distributed attacks.
Aladaileh et al. [49]	Entropy-based detection	Calculated entropy from packet headers and compares with thresholds.	Improves detection rates and reduces false positives.	Limited adaptability to evolving traffic patterns.
Gebremeskel et al. [50]	Entropy-based deep learning	Used chi-square test for feature selection in a deep learning model.	High accuracy and addresses model limitations.	High computational overhead and latency.
Wang et al. [51]	Supervised learning for DDoS	Trained and evaluated supervised learning	Promising detection results with	Requires labeled data; weak against

		algorithms for DDoS detection.	minimal resource requirements.	zero-day attacks.
Ali et al. [52]	ML/DL approaches for DDoS	Compared SVM, KNN, DT, MLP and CNN for DDoS detection.	High accuracy and reduced complexity.	Dataset-dependent performance.
Sangodoyin et al. [53]	Low-cost ML-based detection	Analyzed traffic patterns to detect and prevent DDoS attacks.	Enhances detection accuracy and speed with minimal expense.	Reduced scalability in dynamic environments .
Makuvaza et al. [54]	Deep Neural Network-based IDS	Developed a Deep Neural Network (DNN) model using CICIDS 2017 dataset for DDoS detection.	Achieves 97.59% accuracy with lower resource use.	Unable to detect unknown attacks.
Mansoor et al. [55]	Recurrent Neural Network-based prevention	Used Recurrent Neural Networks for data preprocessing and feature selection to detect attacks.	High accuracy, precision and F1-measure in DDoS detection.	High training and detection latency.
Bhayo et al. [56]	ML-based traffic profiling	Combined Naive Bayes, Decision Tree and SVM for DDoS detection.	Improves security and access control in SD-IoT networks.	Increased system complexity.

Signature-based detection focuses on using known attack patterns to identify malicious activities. This traditional method relies on predefined signatures of known threats. Table 10 presents signature-based reviews proposed to detect control plane attacks.

Table 10: Signature-Based Detection

Reference	**Security Measure**	**Method**	**Strength**	**Weaknesses**
Tang et al. [45]	Flow Table Overflow Protocol	Included prediction, detection, mitigation and prevention modules using random forest classifiers.	Prevents flow table overflow and mitigates LFTO attacks.	Limited scalability in large-scale, high-traffic SDN environments.
Wang et al. [57]	CC-Guard framework for DDoS	Framework with modules for attack detection, switch migration, anomaly detection and mitigation.	Provides real-time DDoS defense with high detection accuracy.	Increased framework complexity and controller overhead.
Zhou [58]	CNN-Bidirectional Long Short-Term Memory (BiLSTM) model	Integrated CNN and BiLSTM for DDoS detection with information entropy.	Reduces CPU usage and detection time, with improved accuracy.	Slower detection speed compared to entropy-based methods.
Saleem et al. [59]	Conditional privacy in VANETs	Used lightweight cryptographic primitives and random oracle model.	Improves performance and privacy for vehicle communications.	Limited applicability beyond VANET environments.
Wang et al. [60]	Collaborative defense framework	Used CD2P framework and DNN for hybrid attack detection.	Enhances cooperation between P4 switches and SDN controllers.	High computational cost due to

				DNN-based detection.
Sinha [61]	SynFloWatch for TCP-SYN-based attacks	Applied Tsallis entropy analysis and 3-way TCP handshake for detection.	Detects SYN-flood attacks with 25% higher accuracy and detailed insights.	Limited to TCP-SYN flooding attacks.

Behavioral analysis research monitors the behavior of entities within SDN to detect potential threats based on behavioral patterns rather than predefined signatures. This approach involves developing sophisticated monitoring tools and algorithms to analyze and respond to emerging threats. Table 11 summarizes recent behavioral analysis techniques used for identifying threats.

Table 11: Behavioral Analysis

Reference	Security Measure	Method	Strength	Weaknesses
Priyadarsini et al. [46]	Trust-Based and Risk-Based models	Utilized game theory for trust calculation and attack prevention.	Achieves 95% accuracy in attack detection and prevention.	Requires adaptation to new attack patterns and improved time efficiency.
Alubaidan et al. [62]	Machine learning techniques	Used Logistic Regression, SVM, KNN, Random Forest and LSTM for attack detection.	Excellent detection with reduced computational overhead.	Dataset-dependent performance and limited zero-day attack detection.

4.2.4 Resilience and Fault Tolerance

In network systems, ensuring the resilience and fault tolerance of control planes is crucial for maintaining continuous operation and stability, even in the event of component failures. Distributed Data Backup and Recovery (DDBR) with a secret key sharing technique facilitates rapid data recovery on backup controllers, significantly improving fault management and network availability in SD-WAN environments [63]. Additionally, the controller replacement technique has been employed to secure, optimize and reduce the operational costs of controllers in multi-domain SDN environments [64]. Table 12 depicts resilience and fault tolerance approach, including articles that utilize DDoS mitigation, failover and redundancy techniques.

Table 12: Resilience and Fault Tolerance reviews

Reference	Security Measure	Method	Strength	Weaknesses
Chen et al. [65]	Three-stage overload control (statistical, TCP handshake, correction).	Used Network Function Virtualization for DDoS attack defense.	Effective against brute force attacks; maintains quality services.	Lack of real-world cloud validation.
Zhang et al. [63]	Distributed data backup and secret key sharing.	Divided and stored SD-WAN controller data in switches.	Enhances fault management and network availability.	No practical deployment or scalability evaluation.
Feng et al. [64]	Controller replacement using the Baguette algorithm.	Secured and cost-effective controller deployment in SDN.	Optimizes performance, security and reduces costs.	Limited implementation in cloud environments.

Bagha et al. [66]	ELA-RCP algorithm for control plane reliability.	Hybrid Spider Optimization Algorithm and queueing-based greedy algorithm.	Improves reliability, energy efficiency and performance.	Insufficient real-world SDN validation.
Garba et al. [67]	Real-time DDoS detection with machine learning and SNORT.	Trained models on network traffic for attack detection.	Achieves 99% accuracy in classifying traffic.	Dataset-dependent; limited real-time deployment testing.

4.3 Issues and Challenges of Control Plane Security Approaches

This study examined the issues and challenges associated with several proposed techniques used to enhanced the SDN control planes. These issues are presented in the following sub sections.

4.3.1 Issues and Challenges of Authentication and Authorization Approach

Authentication and authorization are crucial in any Internet of Things (IoT) environment within a Software-Defined Networking (SDN) framework. They prevent adversaries from launching attacks that could compromise a controller or the entire network, through the control plane. Several studies have aimed to strengthen authentication security for IoTs to address the vulnerabilities of the SDN control plane. For example, a per-message authentication technique has been designed to mitigate downgrade attacks, though this comes with a trade-off between security and implementation cost [19]. Additionally, clustering and authentication-based access methods have been integrated to enhance controller security. This approach addresses the single point of failure vulnerability through clustering and improves network authentication security, but it struggles with control partitioning and redundancy in a multi-controller setup [20].

A blockchain-enabled SDN framework has been proposed that integrates a controller authentication scheme and smart contract addressing to tackle security challenges in 5G networks. However, the consensus mechanism lacks a security algorithm, rendering it vulnerable to attacks and the complexity of the technique affects transaction speed, leading to slower blockchain transactions [21]. Another approach involves a lightweight challenge-response authentication using the Elliptic Curve Diffie-Hellman protocol, aimed at resolving packet drop issues during transmission and strengthening control plane security through identity authentication in UAVs [28]. However, two-factor authentication using email-based and SMS-based OTPs, implemented after users input their username and password, is vulnerable to SIM swap, Signal System 7 (SS7) and SMTP attacks. A two-phase authentication scheme has been integrated into an SDN gateway to protect user data in fog nodes. Nevertheless, this approach does not address data security during transmission between fog nodes and IoTs, which affects the integrity and reliability of data during transmission [22]. Lastly, a Privacy-Preserving Authentication technique has been proposed to secure communication and preserve privacy in vehicle networks. This approach relies on an assumed trust model that may not always be realistic, indicating the need for real-world validation of its integrity [26].

Furthermore, a Dynamic Access Control List was designed to detect anomalies and prevent traffic flooding within a network. This approach has improved the security of sensitive data by classifying traffic for more effective detection and mitigation of DoS attacks [47]. However, this approach couldn't detect and prevent other types of attacks jeopardizing the network and its data.

4.3.3 Issues and Challenges of Data Encryption and Secure Communication Approach

Mohan et al. [42] proposed a lightweight cryptographic function using dynamic crypto key distribution to secure SDN and its switches as fog nodes. Classical and quantum key distribution protocols are used with TLS to secure communication channels [38]. Clustering structures with a blockchain-based architecture are employed to secure SDN communication channels [39].

Encryption techniques also face challenges such as energy consumption and weak response times due to algorithm complexity or architectural design. Elliptic-Curve Cryptography (ECC) and SHA-256 are used to authenticate and

secure communication channels and data integrity. This approach has improved performance by reducing computational cost, storage consumption, communication overhead and consensus delay. However, it is inadequate for diverse network conditions, as it primarily focuses on vehicle networks. Extending it to other applications, such as smart industries and healthcare, may encounter challenges related to varying traffic conditions and channel reliability in cellular networks. Additionally, Ghaly and Abdullah [43] proposed AES and RSA as a hybrid encryption approach to protect data integrity during communication and verify the authenticity of data sources. While this approach effectively addresses several security challenges facing SDN, it trades off security for network performance, resulting in weak response times during communication.

4.3.4 Issues and Challenges of Intrusion Detection and Prevention Approach

Proof of work combined with flow rule installations is used as an entropy technique to control and coordinate packets. This approach effectively manages packet transmission during DoS attacks but cannot differentiate between legitimate and illegitimate traffic, posing a high risk to control systems during requests [44]. The FTOP detects and mitigates LFTO attacks, successfully preventing flow table overflow. However, this approach has limited exploration of the complexities involved in detecting and mitigating flow table overflow in large-scale SDN networks with high traffic and intricate topologies [45]. The TCAD model and the RAP model are used to detect and filter malicious traffic flows. These models have achieved 95% accuracy in attack detection and prevention across various scenarios. The TCAD model needs enhancement to address new attack patterns and the RAP model requires optimization for time complexity efficiency [46].

A Dynamic Threshold algorithm is employed to design a new rule-based detection mechanism for DDoS attacks. This approach effectively detects high-rate attacks with a low false positive rate when targeting a single point. However, it struggles with low detection rates and high false positive rates when attackers simultaneously target multiple points [48]. The CNN-BiLSTM model, proposed for DDoS attack detection using information entropy and deep learning, has reduced CPU utilization and improved detection efficiency compared to previous studies [58]. However, machine learning models generally exhibit slower detection speeds compared to entropy-based methods. Makuvaza et al. [54] proposed a DNN-based Intrusion Detection System (IDS) to detect and prevent DDoS attacks. This IDS achieved a 97.59% detection accuracy and consumed fewer resources and time. Nonetheless, signature-based detection remains vulnerable to new anomaly attacks, meaning it cannot detect attacks not included in the signature database.

4.3.5 Issues and Challenges of Resilience and Fault Tolerance Approach

A three-stage overload control approach has been proposed to detect and protect against DDoS attacks. This approach includes statistical identification, in-depth TCP handshake verification and identification of legitimate flows [65]. Zhang et al. [63] proposed a DDBR method and a secret key sharing technique to enhance fault management and network availability. Additionally, Feng et al. [64] improved multi-domain security through controller replacement, utilizing the Baguette algorithm to replace some controllers in a Software-Defined Networking (SDN) environment. However, these approaches require practical implementation and evaluation in a cloud environment, which limits the validation of the proposed enhancements and performance claims from these studies.

4.4 Summary of Emerging Issues and Challenges in Control Plane Security Approaches

This section summarized the existing control plane security approaches issues and challenges reviewed. The review reveals that while various approaches have been proposed to address authentication, access control, data encryption and secure communication, intrusion detection and resilience, each approach comes with inherent limitations and trade-offs as summarized in Table 13.

Table 13: Summary of Control Plane Security Issues and Challenges

Approach	Issue Count	Issues	Percentage (%)
Authentication & Authorization	16	Trade-off between security and implementation cost. Control partitioning and redundancy issues. Consensus mechanism lacks security algorithm. Slower blockchain transactions. Vulnerability to SIM swap, SS7 and SMTP attacks. Integrity issues in fog nodes and IoTs. Assumed trust model may not always be realistic. Limited detection and prevention capabilities for attacks beyond DoS.	32.7%
Data Encryption & Secure Communication	9	High energy consumption. Weak response times due to algorithm complexity. Inadequacy for diverse network conditions. Trade-off between security and network performance.	18.4%
Intrusion Detection & Prevention	19	Cannot differentiate between legitimate and illegitimate traffic. Limited exploration of complex SDN topologies. Needs enhancement for new attack patterns. Requires optimization for time complexity efficiency. High false positive rate in multi-target attacks. Slow detection speed in ML-based models.	38.8%

Approach	Issue Count	Issues	Percentage (%)
		Signature-based detection vulnerable to new anomaly attacks.	
Resilience & Fault Tolerance	5	Requires real-world validation in cloud environments.	10.2%
Total	49		100%

Note: Percentages are rounded to one decimal place; totals may not equal 100% due to rounding.

We analyzed the issues and challenges affecting the control plane security techniques proposed in recent years, based on their approaches and revealed the approaches needing more security attention in Figure 5.

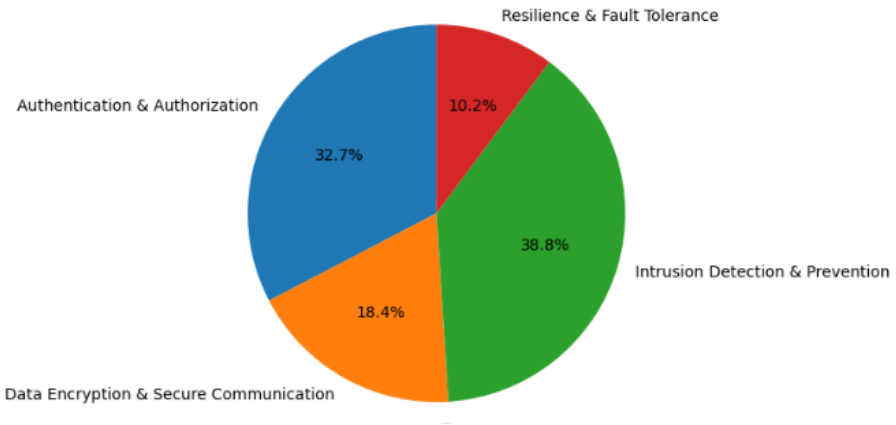

Figure 5: Analysis on Security Approaches Issues and Challenges

The analysis shows that Intrusion Detection and Prevention accounts for approximately 38.8% of the total identified security issues, representing the highest proportion among all categories. This is closely followed by Authentication and Authorization, which contributes 32.7%, indicating that both areas face significant security challenges and are highly susceptible to threats affecting system performance and control plane operations. Data Encryption and Secure Communication represent 18.4% of the reported security issues, reflecting a moderate level of vulnerability that still requires focused attention. In contrast, Resilience and Fault Tolerance accounts for only 10.2%, suggesting comparatively fewer security challenges in this category.

Overall, these findings emphasize the need for further research and the development of robust security mechanisms, particularly in Authentication and Authorization and Intrusion Detection and Prevention, to effectively mitigate security threats and enhance the overall reliability and security of the system.

5.0 Conclusion

This study presents a comprehensive survey on SDN control plane security approaches and clustered the approaches into authentication and authorization, data encryption and secure communication, intrusion detection and prevention and resilience and fault tolerance techniques. For each approach, we reviewed articles that propose techniques to mitigate or address existing security issues. The techniques strengths, issues and challenges are presented to serve as baseline for future studies. It's crucial to maintain a proactive stance through continuous research, collaboration and knowledge-sharing to effectively address the dynamic landscape of security threats in the SDN control plane. Ongoing research should focus on developing standardized security protocols, robust authentication mechanisms and adaptive security measures to detect and mitigate the evolving threats faced by SDN control planes. Further studies are required to strengthen security, enable real-time evaluations and enhance their applicability in dynamic, real-world scenarios, considering the challenges posed by simulations analyses.

5.1 Future Research Trends

1. Blockchain-enabled SDN frameworks face challenges related to consensus mechanisms and transaction speed [21]. Future research could focus on developing robust security algorithms for consensus mechanisms to mitigate vulnerabilities and enhance the resilience of the blockchain against various attacks. Additionally, blockchain transactions can be optimized by exploring more efficient consensus algorithms or hybrid approaches that combine blockchain with other secure communication techniques. Integrating advanced cryptographic methods and scalable solutions could also improve the overall efficiency of the blockchain in 5G and other IoT environments.
2. Clustering and Authentication-Based access techniques improve controller security and address single points of failure, issues such as control partitioning and redundancy in multi-controller setups remain problematic [20]. Future research should focus on developing advanced clustering techniques that dynamically adjust to network changes, enhance partitioning strategies and minimize redundancy. Investigating adaptive algorithms for load balancing and controller failover mechanisms can improve the reliability and efficiency of multi-controller SDN environments.
3. The use of lightweight challenge-response authentication protocols, such as Elliptic Curve Diffie-Hellman, offers potential benefits in terms of securing data during transmission [28]. Future research should focus on enhancing this protocol's performance through exploring alternative cryptographic techniques. The techniques should offer a balance between security and computational efficiency. Future research should focus on hybrid authentication schemes that integrate multiple cryptographic techniques to provide robust security while maintaining low overhead.
4. Two-phase authentication scheme in SDN gateways enhances security, issues related to data security during transmission between fog nodes and IoTs need to be addressed [22]. Future research should focus on developing end-to-end encryption methods and secure transmission protocols that will protect data integrity and confidentiality during transmission. Investigating secure communication channels and implementing advanced cryptographic techniques for data-in-transit will enhance the robustness of authentication schemes in SDN environment.
5. Privacy-preserving authentication techniques for vehicle networks, rely on assumed trust models that may not always reflect real-world scenarios [26]. Future research should focus on validating these techniques under realistic conditions and diverse threat models. Exploring practical implementation challenges, conducting field trials and assessing the techniques effectiveness in real-world environments will provide insights into their reliability and potential areas for improvement.
6. The vulnerabilities associated with email-based and SMS-based OTPs, such as SMTP, SIM swap and Signal System 7 attacks, highlight the need for more secure secondary authentication methods [28]. Research should focus on developing alternative two-factor authentication mechanisms that are resistant to these attacks. Potential areas include the use of hardware tokens, biometric authentication, or more secure app-based solutions. Evaluating these methods effectiveness and usability in IoT environments will significantly improve authentication security.
7. Dynamic Access Control Lists (ACLs) is potential in detecting anomalies and mitigating traffic flooding, particularly against DoS attacks [47]. Future research should focus on extending the capabilities of dynamic ACLs to detect and prevent a wider range of attack vectors, including sophisticated multi-vector attacks and emerging threats. This will involve integrating advanced machine learning algorithms to improve anomaly detection and classify malicious traffic more accurately. Additionally, exploring adaptive ACL mechanisms that can dynamically adjust policies in response to evolving threat landscapes will enhance the overall security posture of IoT networks.
8. Policy-Based Access Control (PBAC) systems are crucial for managing permissions and protecting data [47]. Further study can be carried out on integrating PBAC with advanced security measures, such as real-time threat intelligence feeds and behavioral analytics. This integration will enhance the system's ability to adapt to emerging threats and enforce more granular access policies. PBAC can be combined with encryption technologies, secure multi-party computation and blockchain for policy enforcement to improve data integrity and confidentiality.
9. Given the limitations of dynamic ACLs and traditional access control techniques, hybrid approaches that integrate both techniques will provide more robust security solutions [47]. Future research should focus on developing hybrid access control models that leverage the strengths of dynamic ACLs, policy-based control and emerging technologies like Holochain. These models will offer enhanced flexibility, scalability and security. Investigating the integration of hybrid approaches with automated response systems and adaptive security protocols will further improve the resilience of IoT networks against various threats.

10. Proof of Work (PoW) and flow rule integration is used for managing packet transmission during DoS attacks, but its inability to distinguish between legitimate and illegitimate traffic poses risks [44]. Future research should focus on enhancing PoW mechanisms to incorporate packet classification and traffic analysis techniques that can differentiate between legitimate and malicious traffic more effectively. This will involve integrating machine learning algorithms or advanced statistical methods to better identify and filter out malicious traffic while allowing legitimate packets to access network resources unimpeded. Exploring hybrid approaches that combine PoW with other entropy techniques will improve the overall network security and its performance.
11. FTOP is effective in mitigating LFTO attacks but it faces limitations in large-scale SDN networks [45]. Future research should focus on how FTOP can be adapted and scaled to handle high traffic volumes and complex network topologies. This involves developing enhanced detection mechanisms that can efficiently identify and manage flow table overflows in high-traffic environments. Exploring distributed FTOP implementations or integrating FTOP with other network management strategies will address scalability issues and improve its applicability to large-scale networks.
12. Dynamic Threshold algorithm is effective against high-rate DDoS attacks at single points but struggles with multi-point attacks [48][48]. Future research should focus on developing advanced rule-based detection mechanisms that can handle distributed attack scenarios more effectively. This will involve creating adaptive threshold algorithms that adjust in real time based on traffic patterns and attack characteristics. Additionally, integrating multi-point detection techniques and leveraging collaborative filtering across multiple network nodes can improve detection rates and reduce false positives in complex attack scenarios.
13. Supervised learning techniques are effective in detecting flooding DDoS attacks but face challenges such as high resource consumption and slow response times [58]. Future research should explore optimizing the technique to improve its efficiency. This may involve developing more lightweight models, optimizing training processes, or utilizing hardware acceleration to speed up detection.
14. Signature-based Intrusion Detection Systems (IDS) are effective but vulnerable to new and future potential anomaly attacks because they cannot detect attacks not included in the signature database [54]. Future research should focus on developing hybrid IDS approaches that combine signature-based detection with anomaly detection techniques. This involves incorporating real-time anomaly detection and behavioral analysis to identify novel threats. Additionally, exploring adaptive and self-learning IDS systems that can update their signatures and detection rules based on evolving attack patterns could improve their resilience to new and emerging threats.
15. To provide a more robust defense against network disruption attacks, integrating overload control mechanisms with fault management and backup solutions should be considered. Future research should explore the synergies between the three-stage overload control approach and distributed data backup and recovery techniques [63, 65]. This includes developing an integrated framework that combines attack detection, traffic management and fault tolerance to enhance network resilience.
16. Several proposed techniques in this study, including the three-stage overload control approach and the DDBR technique, require practical implementation and evaluation in cloud environments. Future research should focus on deploying these techniques in cloud settings to assess their performance, scalability and impact on network availability. This includes conducting performance benchmarks, stress tests and real-world case studies to validate the effectiveness. Additionally, studying how these techniques interact with cloud-specific challenges, such as elastic scaling and multi-tenancy, could provide valuable insights into their practical applicability.

ACKNOWLEDGEMENT

This study was supported by the Geran Putra IPS (GP-IPS9788400). The authors would like to express their gratitude to Universiti Putra Malaysia (UPM) for its valuable assistance.

APPENDIX

The acronyms used in this study are listed in Table 14.

Table 14: List of acronyms

ABE	Attribute-Based Encryption	PAS	Privacy-Preserving Authentication Scheme
BiLSTM	Bidirectional Long Short-Term Memory	PQC	Post-Quantum Cryptography
CK-model	Cramer-Krawczyk Model	RBSLO	Rider-Sea Lion Optimized Neural Network
CNN	Convolutional Neural Network	REST API	Representational State Transfer Application Programming Interface
DC-IIoT	Distributed Control for Industrial Internet of Things	SASP	Security-Aware Service Provisioning
DDBR	Distributed Data Backup and Recovery	SDNShield	Software-Defined Networking Shield
DL	Deep Learning	SD-WAN	Software-Defined Wide Area Network
ECC	Elliptic Curve Cryptography	SEAPP	Secure Application Management Framework for SDN
ELA-RCP	Enhanced Load-aware Resilient Control Plane	SHA256	Secure Hash Algorithm 256-bit
HP-ABE	Hierarchical Policy Attribute-Based Encryption	SNORT	Network Intrusion Detection System
KNN	K-Nearest Neighbors	SOA	Service-Oriented Architecture
LBSV	Lightweight Blockchain-Based Security Protocol	SVM	Support Vector Machine
LSTM	Long Short-Term Memory	TLS	Transport Layer Security
ML	Machine Learning	TSallis	Tsallis Entropy
NTRU	N-th Degree Truncated Polynomial Ring Unit	VANETs	Vehicular Ad Hoc Networks

REFERENCES

[1] M. S. Farooq, S. Riaz and A. Alvi, "Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review," Jul. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/electronics12143077.

[2] N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Pérez-Díaz and M. Zareei, "Towards security automation in Software Defined Networks," Feb. 01, 2022, *Elsevier B.V.* doi: 10.1016/j.comcom.2021.11.014.

[3] M. Jammal, T. Singh, A. Shami, R. Asal and Y. Li, "Software defined networking: State of the art and research challenges," Oct. 29, 2014, *Elsevier B.V.* doi: 10.1016/j.comnet.2014.07.004.

[4] A.-W. Alhasan and S. Wei, "Predicting DDoS Anomaly Patterns in SDN Controller using Hidden Markov Model," 2020.

[5] C. Farnell, E. Soria, J. Jackson and H. A. Mantooth, "Cyber protection of grid-connected devices through embedded online security," in *2021 IEEE Design Methodologies Conference, DMC 2021*, Institute of Electrical and Electronics Engineers Inc., Jul. 2021. doi: 10.1109/DMC51747.2021.9529935.

[6] A. Hirsi Abdi, A. Salh, M. A. Alhartomi, H. Rasheed, S. Ahmed and A. Tahir, "Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI and MTD Approaches to Security Solutions", doi: 10.1109/ACCESS.2023.0322000.

[7] Z. A. Bhuiyan, S. Islam, M. 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, doi: 10.1109/ACCESS.2023.3307467.

[8] M. Rahouti, K. Xiong, Y. Xin, S. K. Jagatheesaperumal, M. Ayyash and M. Shaheed, "SDN Security Review: Threat Taxonomy, Implications and Open Challenges," 2022, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2022.3168972.

[9] M. B. Jimenez, D. Fernandez, J. E. Rivadeneira, L. Bellido and A. Cardenas, "A Survey of the Main Security Issues and Solutions for the SDN Architecture," 2021, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2021.3109564.

[10] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, Y. W. Chong and Y. K. Sanjalawe, "Detection Techniques of Distributed Denial of Service Attacks on Software-Defined Networking Controller-A Review," *IEEE Access*, vol. 8, pp. 143985–143995, 2020, doi: 10.1109/ACCESS.2020.3013998.

[11] K. Nisar *et al.*, "A survey on the architecture, application and security of software defined networking: Challenges and open issues," Dec. 01, 2020, *Elsevier B.V.* doi: 10.1016/j.iot.2020.100289.

[12] A. A. Bahashwan, M. Anbar and N. Abdullah, "New architecture design of cloud computing using software defined networking and network function virtualization technology," in *Advances in Intelligent Systems and Computing*, Springer, 2020, pp. 705–713. doi: 10.1007/978-3-030-33582-3_66.

[13] N. S. Shaji and R. Muthalagu, "Survey on security aspects of distributed software-defined networking controllers in an enterprise SD-WLAN," *Digital Communications and Networks*, Sep. 2023, doi: 10.1016/j.dcan.2023.09.004.

[14] X. Etxezarreta, I. Garitano, M. Iturbe and U. Zurutuza, "Software-Defined Networking approaches for intrusion response in Industrial Control Systems: A survey," Sep. 01, 2023, *Elsevier B.V.* doi: 10.1016/j.ijcip.2023.100615.

[15] M. A. Iliyasu, A. Abdullah, Z. M. Hanapi and N. Samian, "A survey on Control Plane Security Approaches in Software Defined Networks," Institute of Electrical and Electronics Engineers (IEEE), Dec. 2025, pp. 1–8. doi: 10.1109/iccr67387.2025.11292437.

[16] A. Bhardwaj, R. Tyagi, N. Sharma, A. Khare, M. S. Punia and V. K. Garg, "Network intrusion detection in software defined networking with self-organized constraint-based intelligent learning framework," *Measurement: Sensors*, vol. 24, Dec. 2022, doi: 10.1016/j.measen.2022.100580.

[17] K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj and P. Chinnasamy, "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques," in *2021 International Conference on Computer Communication and Informatics, ICCCI 2021*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021. doi: 10.1109/ICCCI50826.2021.9402517.

[18] K. Dhamecha and B. Trivedi, "SDN Issues A Survey," *Int. J. Comput. Appl.*, vol. 73, no. 18, pp. 30–35, Jul. 2013, doi: 10.5120/12843-0195.

[19] M. Sjoholmsierchio, B. Hale, D. Lukaszewski and G. Xie, "Strengthening SDN Security: Protocol Dialecting and Downgrade Attacks," in *Proceedings of the 2021 IEEE Conference on Network Softwarization: Accelerating Network Softwarization in the Cognitive Age, NetSoft 2021*, Institute of Electrical and Electronics Engineers Inc., Jun. 2021, pp. 321–329. doi: 10.1109/NetSoft51509.2021.9492614.

[20] C. Bhatt, V. Sihag, G. Choudhary, P. V. Astillo and I. You, "A multi-controller authentication approach for SDN," in *2021 International Conference on Electronics, Information and Communication, ICEIC 2021*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021. doi: 10.1109/ICEIC51217.2021.9369825.

[21] D. Das, S. Banerjee, K. Dasgupta, P. Chatterjee, U. Ghosh and U. Biswas, "Blockchain Enabled SDN Framework for Security Management in 5G Applications," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jan. 2023, pp. 414–419. doi: 10.1145/3571306.3571445.

[22] C. Ke, Z. Zhu, F. Xiao, Z. Huang and Y. Meng, "SDN-Based Privacy and Functional Authentication Scheme for Fog Nodes of Smart Healthcare," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17989–18001, Sep. 2022, doi: 10.1109/JIOT.2022.3161935.

[23] H. Mutaher and P. Kumar, "Security-enhanced SDN controller based kerberos authentication protocol," in *Proceedings of the Confluence 2021: 11th International Conference on Cloud Computing, Data Science and Engineering*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 672–677. doi: 10.1109/Confluence51648.2021.9377044.

[24] P. Kumar, R. Kumar, A. Aljuhani, D. Javeed, A. Jolfaei and A. K. M. N. Islam, "Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity," *Solar Energy*, vol. 263, Oct. 2023, doi: 10.1016/j.solener.2023.111921.

[25] R. Salam, P. K. Roy and A. Bhattacharya, "DC-IIoT: A Secure and Efficient Authentication Protocol for Industrial Internet-of-Things Based on Distributed Control Plane," *Internet of Things (Netherlands)*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100782.

[26] X. Deng, T. Gao, N. Guo, J. Qi and C. Zhao, "PAS: Privacy-Preserving Authentication Scheme Based on SDN for VANETs," *Applied Sciences (Switzerland)*, vol. 12, no. 9, May 2022, doi: 10.3390/app12094791.

[27] M. kumar Pulligilla and C. Vanmathi, "An authentication approach in SDN-VANET architecture with Rider-Sea Lion optimized neural network for intrusion detection," *Internet of Things (Netherlands)*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100723.

[28] M. Usman, R. Amin, H. Aldabbas and B. Alouffi, "Lightweight Challenge-Response Authentication in SDN-Based UAVs Using Elliptic Curve Cryptography," *Electronics (Switzerland)*, vol. 11, no. 7, Apr. 2022, doi: 10.3390/electronics11071026.

[29] Y. Wang, W. Zhang, X. Wang, M. K. Khan and P. Fan, "Security Enhanced Authentication Protocol for Space-Ground Integrated Railway Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 1, pp. 370–385, Jan. 2024, doi: 10.1109/TITS.2023.3307453.

[30] A. Irshad, G. A. Mallah, M. Bilal, S. A. Chaudhry, M. Shafiq and H. Song, "SUSIC: A Secure User Access Control Mechanism for SDN-Enabled IIoT and Cyber-Physical Systems," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 16504–16515, Sep. 2023, doi: 10.1109/JIOT.2023.3268474.

[31] L. Wang, J. Xu, B. Qin, M. Wen and K. Chen, "An efficient fuzzy certificateless signature-based authentication scheme using anonymous biometric identities for VANETs," *IEEE Trans. Dependable Secure Comput.*, 2025, doi: 10.1109/TDSC.2024.3392470.

[32] T. Hu *et al.*, "SEAPP: A secure application management framework based on REST API access control in SDN-enabled cloud environment," *J. Parallel Distrib. Comput.*, vol. 147, pp. 108–123, Jan. 2021, doi: 10.1016/j.jpdc.2020.09.006.

[33] K. K. Karmakar, V. Varadharajan, S. Nepal and U. Tupakula, "SDN-Enabled Secure IoT Architecture," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6549–6564, Apr. 2021, doi: 10.1109/JIOT.2020.3043740.

[34] Y. Zhao, H. Yu, Y. Liang, M. Conti, W. Bazzi and Y. Ren, "A Sanitizable Access Control with Policy-Protection for Vehicular Social Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 3, pp. 2956–2965, Mar. 2024, doi: 10.1109/TITS.2023.3285623.

[35] L. Vishwakarma, A. Nahar and D. Das, "LBSV: Lightweight Blockchain Security Protocol for Secure Storage and Communication in SDN-Enabled IoV," *IEEE Trans. Veh. Technol.*, vol. 71, no. 6, pp. 5983–5994, Jun. 2022, doi: 10.1109/TVT.2022.3163960.

[36] R. Khayretdinov, D. Dautov, A. Vulfin, K. Mironov and A. Frid, "Secure data exchange system in software-defined networks of energy complex facilities," in *Proceedings - ICOECS 2021: 2021 International Conference on Electrotechnical Complexes and Systems*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 58–63. doi: 10.1109/ICOECS52783.2021.9657256.

[37] T. Szymanski, "An Ultra-Reliable Quantum-Safe Software-Defined An Ultra-Reliable Quantum-Safe Software-Defined Deterministic Internet of Things (IoT) for Data-Centers, Cloud Deterministic Internet of Things (IoT) for Data-Centers, Cloud Computing and the Metaverse Computing and the Metaverse," *, Cloud Computing and the Metaverse Computing and the Metaverse*, 2023, doi: 10.36227/techrxiv.22680520.v1.

[38] S. S. Mahdi and A. A. Abdullah, "Improved Security of SDN based on Hybrid Quantum Key Distribution Protocol," in *Proceedings of the 2nd 2022 International Conference on Computer Science and Software Engineering, CSASE 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 36–40. doi: 10.1109/CSASE51777.2022.9759635.

[39] S. A. Latif *et al.*, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Comput. Commun.*, vol. 181, pp. 274–283, Jan. 2022, doi: 10.1016/j.comcom.2021.09.029.

[40] A. Rahman *et al.*, "Internet of medical things and blockchain-enabled patient-centric agent through SDN for remote patient monitoring in 5G network," *Sci. Rep.*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-55662-w.

[41] Y. A. Kadakia, A. Suryavanshi, A. Alnajdi, F. Abdullah and P. D. Christofides, "Integrating machine learning detection and encrypted control for enhanced cybersecurity of nonlinear processes," *Comput. Chem. Eng.*, vol. 180, Jan. 2024, doi: 10.1016/j.compchemeng.2023.108498.

[42] K. V. M. Mohan, S. Kodati and V. Krishna, "Securing SDN Enabled IoT Scenario Infrastructure of Fog Networks From Attacks," in *Proceedings of the 2nd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1239–1243. doi: 10.1109/ICAIS53314.2022.9742727.

[43] S. Ghaly and M. Z. Abdullah, "Design and implementation of a secured SDN system based on hybrid encrypted algorithms," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 19, no. 4, pp. 1118–1125, Aug. 2021, doi: 10.12928/TELKOMNIKA.v19i4.18721.

[44] L. F. Eliyan and R. Di Pietro, "DeMi: A Solution to Detect and Mitigate DoS Attacks in SDN," *IEEE Access*, vol. 11, pp. 82477–82495, 2023, doi: 10.1109/ACCESS.2023.3301994.

[45] D. Tang, Z. Zheng, K. Li, C. Yin, W. Liang and J. Zhang, "FTOP: An Efficient Flow Table Overflow Preventing System for Switches in SDN," *IEEE Trans. Netw. Sci. Eng.*, pp. 1–13, Jul. 2024, doi: 10.1109/tnse.2023.3297650.

[46] M. Priyadarsini, P. Bera, S. K. Das and M. A. Rahman, "A Security Enforcement Framework for SDN Controller Using Game Theoretic Approach," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 2, pp. 1500–1515, Mar. 2023, doi: 10.1109/TDSC.2022.3158690.

[47] J. Ramprasath and V. Seethalakshmi, "Secure access of resources in software-defined networks using dynamic access control list," *International Journal of Communication Systems*, vol. 34, no. 1, Jan. 2021, doi: 10.1002/dac.4607.

[48] M. A. Aladaileh, M. Anbar, A. J. Hintaw, I. H. Hasbullah, A. A. Bahashwan and S. Al-Sarawi, "Renyi Joint Entropy-Based Dynamic Threshold Approach to Detect DDoS Attacks against SDN Controller with Various Traffic Rates," *Applied Sciences (Switzerland)*, vol. 12, no. 12, Jun. 2022, doi: 10.3390/app12126127.

[49] M. A. Aladaileh *et al.*, "Effectiveness of an Entropy-Based Approach for Detecting Low- and High-Rate DDoS Attacks against the SDN Controller: Experimental Analysis," *Applied Sciences (Switzerland)*, vol. 13, no. 2, Jan. 2023, doi: 10.3390/app13020775.

[50] T. G. Gebremeskel, K. A. Gemeda, T. G. Krishna and P. J. Ramulu, "DDoS Attack Detection and Classification Using Hybrid Model for Multicontroller SDN," *Wirel. Commun. Mob. Comput.*, vol. 2023, pp. 1–18, Jun. 2023, doi: 10.1155/2023/9965945.

[51] S. Wang *et al.*, "Detecting flooding DDoS attacks in software defined networks using supervised learning techniques," *Engineering Science and Technology, an International Journal*, vol. 35, Nov. 2022, doi: 10.1016/j.jestch.2022.101176.

[52] T. E. Ali, Y. W. Chong and S. Manickam, "Comparison of ML/DL Approaches for Detecting DDoS Attacks in SDN," *Applied Sciences (Switzerland)*, vol. 13, no. 5, Mar. 2023, doi: 10.3390/app13053033.

[53] A. O. Sangodoyin, M. O. Akinsolu, P. Pillai and V. Grout, "Detection and Classification of DDoS Flooding Attacks on Software-Defined Networks: A Case Study for the Application of Machine Learning," *IEEE Access*, vol. 9, pp. 122495–122508, 2021, doi: 10.1109/ACCESS.2021.3109490.

[54] A. Makuvaza, D. S. Jat and A. M. Gamundani, "Deep Neural Network (DNN) Solution for Real-time Detection of Distributed Denial of Service (DDoS) Attacks in Software Defined Networks (SDNs)," *SN Comput. Sci.*, vol. 2, no. 2, Apr. 2021, doi: 10.1007/s42979-021-00467-1.

[55] A. Mansoor, M. Anbar, A. A. Bahashwan, B. A. Alabsi and S. D. A. Rihan, "Deep Learning-Based Approach for Detecting DDoS Attack on Software-Defined Networking Controller," *Systems*, vol. 11, no. 6, Jun. 2023, doi: 10.3390/systems11060296.

[56] J. Bhayo, S. A. Shah, S. Hameed, A. Ahmed, J. Nasir and D. Draheim, "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," *Eng. Appl. Artif. Intell.*, vol. 123, Aug. 2023, doi: 10.1016/j.engappai.2023.106432.

[57] J. Wang, L. Wang and R. Wang, "A Method of DDoS Attack Detection and Mitigation for the Comprehensive Coordinated Protection of SDN Controllers," *Entropy*, vol. 25, no. 8, Aug. 2023, doi: 10.3390/e25081210.

[58] H. Zhou, "A Cooperative Detection of DDoS Attacks Based on CNN-BiLSTM in SDN," *International Journal of Future Computer and Communication*, pp. 27–36, Jun. 2023, doi: 10.18178/ijfcc.2023.12.2.600.

[59] M. A. Saleem *et al.*, "Provably Secure Conditional-Privacy Access Control Protocol for Intelligent Customers-Centric Communication in VANET," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1747–1756, Feb. 2024, doi: 10.1109/TCE.2023.3324273.

[60] Y. C. Wang and P. Y. Su, "Collaborative Defense Against Hybrid Network Attacks by SDN Controllers and P4 Switches," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 2, pp. 1480–1495, Mar. 2024, doi: 10.1109/TNSE.2023.3324329.

[61] M. Sinha, "SynFloWatch: A Detection System against TCP-SYN based DDoS Attacks using Entropy in Hybrid SDN," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jan. 2024, pp. 359–364. doi: 10.1145/3631461.3631463.

[62] H. Alubaidan, R. Alzaher, M. AlQhatani and R. Mohammed, "DDoS Detection in Software-Defined Network (SDN) Using Machine Learning," *International Journal on Cybernetics & Informatics*, vol. 12, no. 04, pp. 93–104, Jul. 2023, doi: 10.5121/ijci.2023.120408.

[63] Y. Zhang, C. Xu and G. M. Muntean, "A Novel Distributed Data Backup and Recovery Method for Software Defined-WAN Controllers," in *2021 IEEE Global Communications Conference, GLOBECOM 2021 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/GLOBECOM46510.2021.9685291.

[64] W. Feng, L. Chuanchang, C. Bo and C. Junliang, "Secure and cost-effective controller deployment in multi-domain SDN with Baguette," *Journal of Network and Computer Applications, , ,* vol. 2021, no. 102969, p. 178, 2021.

[65] K. Y. Chen *et al.*, "SDNShield: NFV-Based Defense Framework Against DDoS Attacks on SDN Control Plane," *IEEE/ACM Transactions on Networking*, vol. 30, no. 1, pp. 1–17, Feb. 2022, doi: 10.1109/TNET.2021.3105187.

[66] M. Abedini Bagha, K. Majidzadeh, M. Masdari and Y. Farhang, "ELA-RCP: An energy-efficient and load balanced algorithm for reliable controller placement in software-defined networks," *Journal of Network and Computer Applications*, vol. 225, May 2024, doi: 10.1016/j.jnca.2024.103855.

[67] U. H. Garba, A. N. Toosi, M. F. Pasha and S. Khan, "SDN-based detection and mitigation of DDoS attacks on smart homes," *Comput. Commun.*, vol. 221, pp. 29–41, May 2024, doi: 10.1016/j.comcom.2024.04.001.