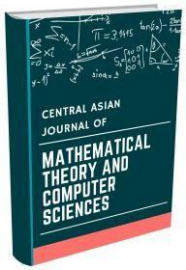

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 07 Issue: 02 | April 2026 ISSN: 2660-5309

Article

Enhancing Security in Software-Defined Networking: A Framework for Encryption

Mohammad Qassim Jawad[1], Hayder Talib Jawad Al-sammak[2]

1,2 University of Information Technology and Communication, Biomedical Informatics College, Baghdad, Iraq
* Correspondence: mohammad.Qassim2002@uortc.edu.iq

Abstract: Software-Defined Networking (SDN) will provide a higher network controllability and flexibility through decoupling of the control and data planes. Nonetheless, its centralized design presents security vulnerabilities and thus it is susceptible to threats like unauthorized access, data breaches and controller attacks. A secure SDN environment is achievable by having strong encryption, authentication and access control. Some of the protective measures that have been applied in this work are logging and security audit services, integration of the SSL/TLS and enforcing authentication of the graphical user interface (GUI). Also, encryptions are used based on cryptographic cipher like DES, AES and role-based authorization is done with the help of FortNOX to improve access controls. The suggested security model enhances the SDN controller by reducing possible threats and ensuring the entire system resiliency. Encryption methods coupled with access control measures provide a better level of data confidentiality and integrity lowering threats in SDN communication. These steps will help make SDN an environment that is more reliable.

Keywords: Network Security, Software-Defined Networking (SDN), SSL/TLS Encryption, Openflow Protocol, Role-Based Authorization, Authentication Mechanisms, AES, FortNOX.

Citation: Jawad M. Q., Al-sammak H. T. J. Enhancing Security in Software-Defined Networking: A Framework for Encryption. Central Asian Journal of Mathematical Theory and Computer Sciences 2026, 7(2), 155-165.

Received: 11th Dec 2025
Revised: 13th Jan 2026
Accepted: 26th Feb 2026
Published: 05th Mar 2026

1. Introduction

SDN has become more popular as a secure, well-managed, and flexible networking paradigm enhancing network programmability and control. In contrast to the conventional networking architecture, SDN brings about a centralized control model, in which data plane and control plane are decoupled.

This separation facilitates dynamic network set-up, automated traffic control so that network administrators can respond promptly to network changes besides maximizing resource utilization. The routing decisions are made by a centralized SDN controller, and distributed to the data-forwarding devices, e.g. switches and routers, by means of standardized protocols such as OpenFlow [1], [2].

Although SDN has many positive attributes in terms of scalability, efficiency and flexibility, security is also a significant issue. The flexibility of SDN which consists of its very programmability also creates gaps that are exploited by attackers. Network security may be compromised by unauthorized access, denial of service (DoS) attacks as well as configuration errors that result in data breaches, service failures as well as loss of integrity [3]. Given that the SDN controller will be the hub of network intelligence, any attack on it would be devastating, with the possible impact going across the whole network.

Also, the communication among the network elements should be encrypted to avoid man in the middle attacks and eavesdropping. In order to overcome these issues, SDN incorporates security surveillance devices, automatic threat mitigation systems and real-time network analyzing devices to track and prevent attacks effectively [3], [4]. The underlying structure of SDN as shown in Figure 1 puts emphasis on separation of control and data plane.

Though SDN was first applied in wired networks, the rising usage of mobile gadgets like Smartphones and tablets has created a massive traffic of wireless networks. The use of wireless Local Area Networks (WLANs) has become popular both at home, in business, and in the public areas to accommodate the growing connectivity needs [5]. The traditional WLANs are usually confronted with issues of smooth mobility, as well as load balancing of the clients, which SDN can overcome.

A client in an SDN enabled WLAN has a Lightweight Virtual Access Point (LVAP) with the unique Basic Service Set Identifier (BSSID). Such a design would facilitate a smooth transition process as the client will be able to get connected to another access point (AP) without having to reconnect to the connection manually. The LVAP mechanism enables SDN to dynamically handle AP associations without modifying the client device level unlike traditional handover mechanisms which create a network latency or packet loss. LVAPs can be moved between one AP and another without losing the current communication process and hence SDN has offered users with little service disruption thus making it an effective solution to the control of contemporary wireless networks [6].

These benefits notwithstanding, SDN security issues are a critical research field. There is high likelihood of SDN being an ideal target of cyber threats due to its centralized nature, requiring a well developed security mechanism for ensuring confidentiality, integrity, and availability of the network. This paper will explore SDN security issues, discuss its most important vulnerabilities, and suggest ways of improving its security system.

This analysis through a review of the available software-defined security solutions will aid in coming up with more robust SDN architecture that could resist emerging cyber threats [7], [8].

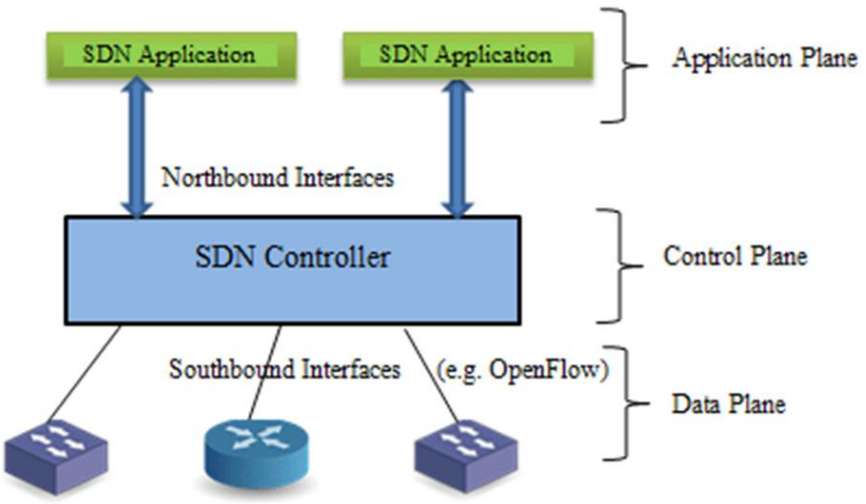

Figure 1. Structures of SDN.

2. Related Works

Over the past few years, various novel solutions were suggested to improve the security of Software-Defined Networking (SDN) in IoT and healthcare systems by utilizing

some of the most recent technologies including Machine Learning (ML), Blockchain, Quantum Key Distribution (QKD), and Edge Computing. The works are beneficial in the creation of secure SDN-based IoT systems, especially in the healthcare industry where data privacy and real-time communication are most important.

A particularly interesting article by [Ala Hamarsheh 2024] proposes the Enhanced SCAFFOLD protocol that is designed to protect IoT networks through the integration of SDN and Machine Learning (ML). The protocol employs ensemble classifiers, including the Support Vector Machines (SVMs), Random Forests, and Recurrent Neural Networks (RNNs), to identify anomalies in network flows that allow immediate response to security threats.

The protocol can selectively block the suspicious flows by using SDN control planes thus having minimal effect on the availability of the network. Although it is an effective way to approach the general IoT security issues, it is slightly constrained by the classical machine learning models, which are not aimed at addressing quantum threats that are gaining momentum in the field of cryptography today [9].

The next important input is the research of 2022 with the ability to create the BCNBI framework that serves to protect the northbound interface of SDN by using a blockchain technology. This implementation uses private/permissioned blockchain authentication, encryption and access control and a lightweight consensus algorithm reduce computational overhead.

The framework is a viable choice toward securing SDN-based healthcare systems because of the effectiveness of dealing with the threats of confidentiality, integrity and availability. Nevertheless, the scalability of blockchain-based systems is a weakness, even though currently, especially in IoT large-scale applications, the amount of data and transactions can saturate the conventional blockchain architecture [10].

To the contrary, [Mahdi and etal., 2022] proposes a hybrid quantum key distribution (QKD) protocol to protect SDN and network slicing OpenFlow communication channel. This hybrid key is the integration of classical and quantum key distribution methods, which makes authentication and security of the communications of the TLS protocol much stronger.

The solution has a strong protection against both classical and quantum computer attacks, which will become a future-proof system against new quantum threats. Yet, QKD protocols introduce further latency and computation complexity, which may become problematic in systems with low-latency and high-throughput connections like in healthcare IoT systems where real-time information transmission is essential [11].

Finally, authors suggested a secure architecture of SDN-based edge computing of IoT-enabled health-care systems. In this framework, a light-weight authentication methodology is applied, which guarantees authenticity on the communication between IoT devices and Edge servers such that only authorized devices will be able to share sensitive health data. The load balancing and efficient use of resources provided by the framework by means of the cooperation between several Edge servers with the help of an SDN controller is critical to the timely delivery of vital healthcare information.

The integration of Edge Computing is able to process information in real time at the source which greatly decreases latency and enhances efficiency within the network. This solution is especially the best to adopt the healthcare IT domain where data privacy, security, and real-time processing are paramount and unlike other frameworks where the main emphasis is placed on network security without taking into consideration performance optimization in resource-constrained settings [12].

All these studies point to an array of methodologies of securing SDN-based networks in IoT and healthcare systems. Whereas Hybrid QKD provides the highest protection in

the future of quantum threats, Edge computing and load balancing in healthcare IoT offers the best performance optimization.

The security solutions based on blockchain are also able to provide solid data integrity and authentication, but can be limited regarding scalability, whereas the ML-driven attack detection frameworks can provide a powerful means of defense against general IoT settings but lack quantum-resilience features. Put in another way, these works are cumulative in terms of knowledge and practice of the safe and scalable solutions to the next generation healthcare IoT systems.

3. Security Analyses for SDN Environment

Software-Defined Networking (SDN) is slowly substituting conventional networking technologies because of its centralized control mechanism. Nevertheless, there are vulnerabilities in this centralized model that when compromised may affect the integrity, privacy and confidentiality of the system and end up reducing the efficiency and performance of the network. In order to counter false positive alerts, the current study offers a security analysis that seeks to implement a strong security in SDN by use of an alert correlation model and an attack graph [8].

The API programmability of the SDN is one of the main security issues that is open to concern. As much as they allow flexibility, they also make the network vulnerable to attacks as they make the vulnerabilities visible. Gaining of unauthorized access to the central controller may inject malicious codes into the system that will result in extensive harm to the network and data. Other layers, such as the control, application, and infrastructure layers, are also a threat to SDN [13], [14].

Application layer attacks usually include rules insertion which may introduce conflict whenever security specifications are not applied uniformly in various areas of SDN. Malicious code is also another issue that can affect program injection causing attacks where corrupted or lost data can occur.

The application layer attacks may take place in the control layer, where an attacker will have an illegal access to the application layer and obtain sensitive network information that may be exploited against the control layer. Also, the channel, controllers or communication between switches and controller may have Denial-of-Service (DoS) attacks and affect the network functions [15], [16].

There are also various threats to the infrastructure layer including DoS attacks where an attacker can flood the network with massive, frequent packets. This may flood the flow table and buffer flow thus causing delays and it may require the inclusion of new rules in the flow table. There is also risk of Man-in-the-Middle (MitM) attacks because communication between switches and the controllers is indirect.

MitM attackers will be able to redirect critical data and black hole attacks or data eavesdropping [13] may occur. The study uses an alert correlation model and attack graph to measure security to address such vulnerabilities. The alert correlation model is used to classify alerts and the attack graph is used to measure the capacity of the system to handle possible attack [17].

SDN is spreading with separation of control plane and data plane that provides a possibility to control the network more efficiently. This paper analyzes the issues and mechanisms used in attaining SDNs. Although wired and wireless SDN is being deployed in different industries to offer centralized traffic and network management, the distributed SDN networks are causing an architectural-level concern to the dependent network. Another problem that wireless SDN in particular experiences includes control of multiple network operators, users, and high monitoring overheads, compatibility, and security problems [18], [19].

The major issues with wireless SDN are some of the unauthorized users who attempt DoS attacks or that access points (APs) or switches interrupt the network traffic. Given that SDN is based on a central controller, the issues with the central controller may impact the whole network. Additionally, channel security implementation should not be done using SDN API which is susceptible to man-in-the-middle attacks [20].

Security and authentication of the servers are also essential, the vulnerabilities to breach of which in these domains may destabilize the whole system. There is a high risk of compromise in integrity, authentication, security, event detection, control plane consistency, and data consistency in wireless networking [17].

Regardless of these hurdles, there are great opportunities provided by wireless SDN, especially in the improvement of network security because real-time programmability and global monitoring is offered. The SDN centralized nature offers the opportunity to monitor as well as mitigate security risks. The functionality of the central controller can be spread over a number of servers in the network, and the visibility of the global network provides real-time monitoring of traffic so as to respond to the changing network security requirements [20].

4. SDN Architecture Impact on Network Security

The SDN architecture isolates data plane and the control plane to allow more flexibility in data forwarding. The protocol used to enable communication between network data and SDN controller is OpenFlow. The present paper discusses a number of SDN attributes that may be utilized to increase network security. The system is capable of identifying and responding to the emergent threats by changing flow tables in switches.

The basis of the suggested approach is in the analysis of the traffic patterns on the global and local levels. Frequent set analysis is one of the methods of the detection of potential threats. The local frequent set analyzer configured on SDN switching devices can be utilized to determine possible vulnerability so that it is possible to detect maliciously purposeful activity and implement the required countermeasures. The SDN controller also has a global frequent set analyzer.

The Local Frequent Set Analyzer (LFSA) can mitigate the number of attacks [21] by inserting new rules to flow tables, particularly the Denial of Service (DoS) attacks by blocking malicious information packets. Access switch is more precise in controlling these attacks as compared to the aggregation switch. The proposed Distributed Flow Set Analyzer (DFSA) system makes use of SDN network facilities to identify a wide variety of network attacks, just as those already present in the IP networks.

4.1. Securing SDNs

This paper looks at some of the security threats whether internal or external as far as SDN architecture is concerned. The SDN functionality is centralized and this brings weaknesses of undermining the security and integrity of the SDN. The consequences of cyberattacks on SDN systems can be much more severe in comparison with the traditional ones. SDN layers have security concerns each of which consists of configuration errors. These concerns require proper attention otherwise security threats and attacks will occur.

A communication flooding attack, linking the controller and switch, has a potential to impact all 3 layers. The top layers may be affected by security threats associated with policy enforcement, and authorization attacks may lead to unauthorized access to the controller. Maintaining the security of every SDN component is essential in order to have a secure environment. Of particular concern is the protection of SDN controller that will control overall network activities. If the controller is compromised, the whole network would fail.

Flow encryption of SDN model is an effective technique of ensuring that malicious flows are not injected. Another important issue is the security of the SDN agent and its environment, and the main focus is on the threat isolation and threat detection. Firewalls, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS) have to be dynamically updated to provide security at every layer, and communication channels should be secured with the help of such measures as digital signature, integrity checking and secure coding.

4.2. Critical Analysis

The false positives are significantly reduced by alert correlation and when compared to original alerts, the alert correlation reduces false positives by about 64%. Using attack graphs and alert correlation techniques together will enable a security analysis to be done more effectively [8]. TLS is more secure than SSL between the control plane and data plane, but there are still a number of TLS/SSL implementations that are susceptible to man in the middle [1].

As TLS can fail to solve the security challenge in future, it is not necessarily the ideal choice. FortNOX is a role-based authorization system which could be the solution to the challenges of network resource authorization and authentication. The FortNOX deals with the failure of the controller to deal with inconsistent flow rules caused by various applications [7]. Nevertheless, role-based authorization cannot be used to handle the complexity of SDN, at least when it comes to resource or application isolation.

SDN firewalls conflict resolving also calls another concern, firewall authorization. The analysis of flow rules and entries and conflict resolution techniques is evaluated with the help of the analysis of the header space to define the effectiveness and efficiency of the suggested method [9], [10].

4.3. Control Plane Security in Network

FortNOX, which is a security enforcement kernel, implements role-based verification to control authorization of every OpenFlow (OF) application. Security in programming is critical, as it directly impacts communication between the control and application layers and their respective applications. FortNOX also addresses conflicts in the control layer and between the southbound and northbound interfaces by enforcing conflict resolution rules from various applications running on the network. FortNOX defines three common authorization roles in managing flow rules via the controller:

1. **OF Operator Role** – Imposes security policies.
2. **OF Security Role** – Adds flow constraints to counter live threat activities.
3. **OF Application Role** – Manages authorization of OpenFlow applications.

The basic FortNOX architecture is illustrated in Fig2.

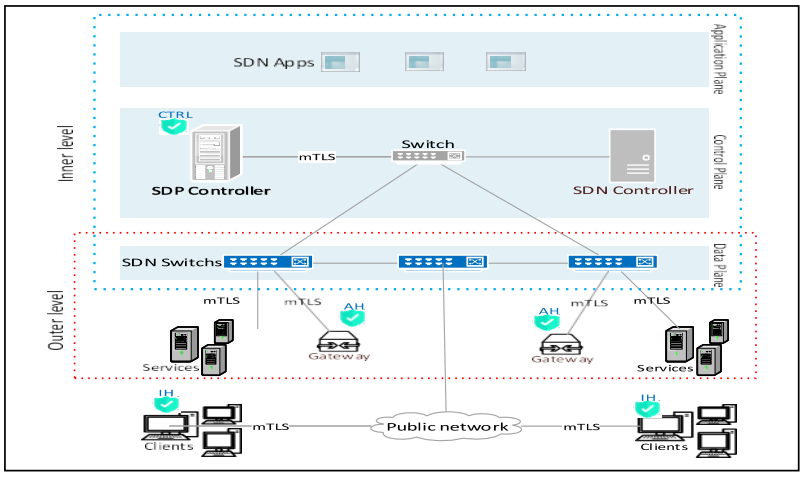

Figure 2. FortNOX Architecture.

4.4. Transport Layer Security Protocol

The goal of using Transport Layer protocol to secure SDN is to safeguard the privacy of data that is transmitted between control plane and the data via internet. [10], [12]. The server must authenticate itself to the client for managing authentication, and the client must use the private keys to authenticate itself to the server. The information is encrypted with the use of cypher suites, which are used to create such keys. The outgoing messages are subjected to message authentication code (MAC), which is validated at the recipient end. Fig. 3 illustrates how TLS functions fundamentally.

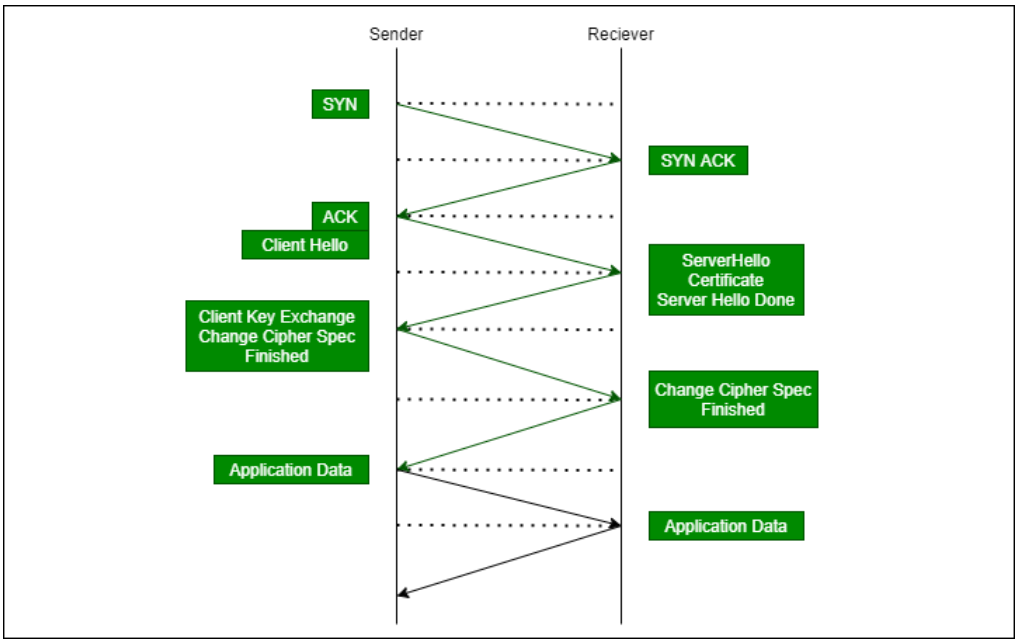

Figure 3. TLS functions fundamentall.

4.5. Encryption of Data

Using encryption, complete security is achieved. In the case where the data is transferred from a place to another, it is of a highest level of vulnerability. Encryption protects sensitive data, like an individual's personal information, throughout data transfer. Data that is encrypted helps to preserve data integrity by alerting those who receive it to potential corruption or cyberattacks. It helps to protect privacy and lessens the likelihood that both criminals and law enforcement monitoring.

Advanced Encryption Standard: AES can be defined as symmetric block cipher that is used for encrypting and decrypting sensitive data in order to secure secret information. Encryption converts data into cipher text, whereas decryption returns the cipher text back to text. It is used in software and hardware to shield digital information—including video, audio, and other types of data—from unauthorized users. Since it's a security protocol,

uses, including financial transactions, e-business, encrypted data storage, and wireless communications, are frequently made use of it. Because AES often encrypts each block in the same way, it is challenging to implement in software because it balances security and performance. Fig. 4 illustrates how AES functions fundamentally.

Data Encryption Standard: Symmetric block ciphers like Data Encryption Standard, or DES, are used. It generates 64-bit cipher text as the output after receiving a 56-bit key as

input and 64-bit plain text. The same algorithm is used in both decryption and encryption for DES. The key is extracted in the opposite order. With regard to encryption, an attack on a 56-bit key is not feasible. But because the 56-bit key size is too little, DES is insecure. DES is extremely slow algorithm, such that Triple DES (3-DES) [12].

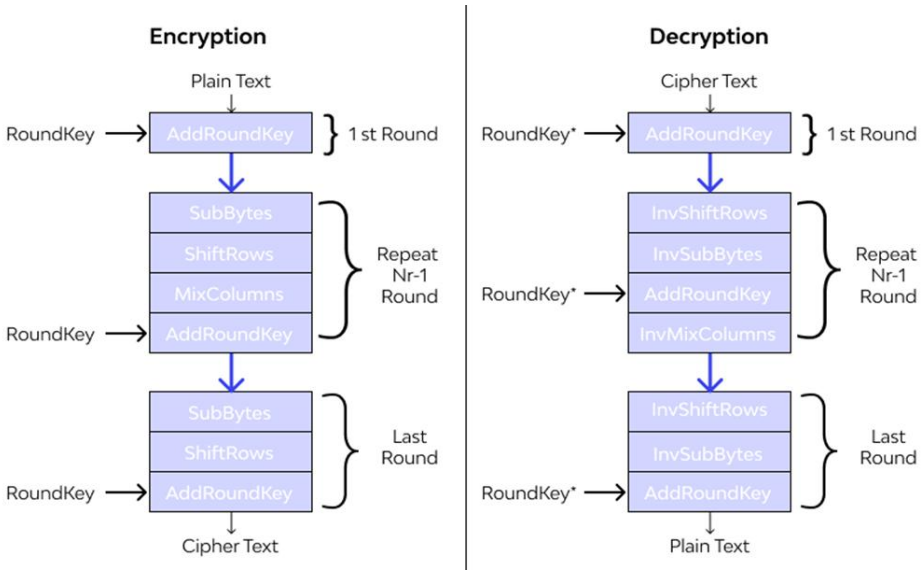

Figure 4. AES Workflow.

5. Discussion of Results

TLS (Transport Layer Security) is an essential technology in guaranteeing integrity of data, encryption and authentication of data during secure network communications. TLS works by establishing a secure connection between the client and the server and by securing the information used by the two parties as it moves through the networks that may be insecure, such as the internet. There are also cases where certain problems are encountered during a session, in such cases TLS records the alerts and timestamps such problems to be analyzed later giving a detailed audit trail of security.

TLS protocol has two main layers that include the record layer and the handshake layer. When combined, they offer a secure method of communication between the client and server. Public key cryptography is utilized alongside these layers, and it makes use of record and hand shake mechanisms, to make a secure connection. The handshake process is initiated by the client when initiating some connection and the server responds by providing required data for mutual authentication. This will guarantee that the client and the server will have trust before sharing sensitive information.

In the process, the client and the server communicate using various cryptographic keys to form a secure communication channel. Notably, the authentication key of the client will be stored to be used in the future, which will make the system more efficient in terms of continued interaction. The functionality of these keys and the increased security provisions of TLS aid in securing the data transmission by reducing the risks involved in the MitM attacks whereby attackers may aim to intersect or modify the communication between client and server.

TLS uses timestamps as one of the main security options. These timestamps monitor the entry point of every packet across the network, which is used to identify any delay, packet loss, and any other performance problem. Timestamps can be especially helpful in determining and minimizing data loss by determining the time delays of packet trades because network switches do not normally exchange metadata. This guarantees a higher level of data delivery and improves the level of security of the communication process.

After the authentication is done and the identity of the client verified with a Certificate Authority (CA) certificate, then the secure connection established. But, as such authentication process guarantees that data is being sent in a secure manner, it does not always guarantee that the content of the data is being secured. To achieve full security in

data, extra encryption measures, including AES and DES (Data Encryption Standard), encryption measures are used.

Under DES encryption, the data is segmented into 64-bit blocks and every block is encrypted with a different cryptography key. The blocks are encrypted and finally the ciphertext is made up of the combined encrypted blocks. On the contrary, AES employs the same key in encryption and decryption, which makes the algorithm more efficient and secure than the other algorithms whereby the encryption process has to be reversed in the decryption process.

In the framework of SDN, FortNOX, a network security implementation kernel of OpenFlow (OF) networks, is an important component of a secure data communication. FortNOX role is to assigns each device on the network with individual security rules or key. When a device attempts to be provided with access to information, the system cross-checks with the device's key matches the expected key. When the key is correct, the access is enabled and when it is wrong an error will be triggered and no one can access the network.

In this way, FortNOX, along with TLS and encryption methods like AES and DES, provides a robust security model for SDN environments, ensuring that data integrity, confidentiality, and authentication are maintained throughout the network.

Attack Type	Information	Mitigation
DDOS Attacks		
HTTP Floods	The attack is generated by sending HTTP GET or POST requests to cause denial on the target webserver.	Track abnormal traffic on the server and implement progressive challenges that can help mitigate the sudden surge of traffic.
DNS Amplification	The attack is generated by turning initially small DNS queries into a much larger payload. Thus taking down the DNS server which enables the resolution of Domain Name.	Rate Limiting or Blocking attacking DNS servers and opening DNS recursive relay servers.
UDP Flood	The attack is generated by connecting random ports with large numbers using the UDP protocol.	Rate limiting the ICMP Responses.
SYN Flood	The attack is generated by exploiting the common TCP three-way handshake.	IPS service should help in detecting and blocking abnormal SYN attacks.
NTP Amplification	The attack is generated by exploiting publically available Network Time Protocol Servers.	Disable NTP server responses to requests from outside the network, enabling rate limiting, and restricting access to trusted clients.
Defacement Attacks		
External Defacement	External defacement involves unauthorized modification or alteration of a target's publicly accessible website or web page to convey messages, spread propaganda, or protest against specific organizations or ideologies.	Implement strict access controls and monitoring mechanisms to detect and prevent unauthorized alterations to the website. Regularly scan and backup website content to quickly restore in case of defacement
Compromised Account Takeover		
Credential Stuffing	Hackers systematically test stolen username and password combinations across multiple platforms and services to gain unauthorized access to accounts usually sourced through Stealer Logs	Enforce strong password policies, implement multi-factor authentication, and monitor for suspicious login attempts to detect and prevent credential stuffing attacks. Enable Visibility over Stealer Logs
Email Accounts	Hacktivists engage in unauthorized access and control of compromised email accounts, often showcasing their access without further escalation.	Secure email accounts with strong passwords, enable two-factor authentication, and educate users about phishing risks to prevent unauthorized access.
Social Media Accounts	Hacktivists target social media accounts for unauthorized access and control to spread their messages, ideologies, or protests.	Secure social media accounts with strong passwords, enable two-factor authentication, and closely monitor for unusual activities to prevent unauthorized access.
SQL Injection		
SQL Injection	Malicious SQL code is inserted through input fields to manipulate databases and access sensitive data, where targets are sourced using G-Dorks Use of Automated tools such as SQLMap	Use parameterized queries, employ web application firewalls, keep systems updated, conduct security assessments, and educate developers on secure coding practices.

Although the proposed architecture can protect the SDN outer level, more challenges still exist to secure inner level, mainly SDN Controller. In general, SDN Controller is hidden by default and invincible against flooding attacks due to SDN architecture. In other words, it is impossible to attack the SDN Controller directly unless metadata has been sniffed which isn't possible especially in the new proposed architecture as a result of the TLS connection. In addition to that, there is a number of simple solutions that can be traded such as the management of a firewall at the controller to block all of the inbound traffic except SDN switches.

From a different perspective, there remains a chance for indirect attacks to take over the controller. For example, a DoS attack can be established by the randomly requesting of anonymous servers through one the SDN switches connected to the controller. Even though those requests will end up in a null route or

6. Conclusion

The advent of Software-Defined Networking (SDN) has addressed the growing need for networks that are adaptable, reliable, well-managed, and secure. However, the division of control plane and data plane in SDN has introduced new vulnerabilities that make it more susceptible to various attack vectors compared with the traditional networks. These vulnerabilities pose significant risks to the network's consistency, availability, confidentiality, authenticity, and integrity. As a result, SDN networks face challenges that could have severe impacts on their overall performance and security.

This paper has addressed various solutions for mitigating these security issues providing underlying challenges and risks SDN has been exposed to in both the wired and wireless network. Specifically, Wireless SDN (WSDN) has all the same vulnerabilities as the traditional SDN architectures, and there are some more complications associated with the utilization of wireless media.

Nevertheless, studies have focused on the opportunities of leveraging the benefits of a centralized SDN framework, like real time programmability and the capability of global traffic monitoring. All these characteristics can boost the security of the network and make SDN networks more resilient.

Although SDN brings about new security issues, it also provides a high degree of prospects of solving modern networking issues, particularly in conjunction with advanced security measures. Due to the constant development of SDN technologies, the research and development of security mechanisms will be necessary to overcome risks and achieve the maximum potential of SDN in terms of providing secure, reliable, and flexible networks.

REFERENCES

[1] M. Blessing and J. Olusegun, "The Impact of Software-Defined Networking (SDN) on Traditional Network Architectures : Opportunities and Challenges Author : Moses Blessing Date : 28 th August, 2024," no. August, 2024.

[2] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing," *PLoS One*, vol. 18, no. 6 June, pp. 1–20, 2023, doi: 10.1371/journal.pone.0287291.

[3] Y. Su, D. Xiong, K. Qian, and Y. Wang, "A Comprehensive Survey of Distributed Denial of Service Detection and Mitigation Technologies in Software-Defined Network," *Electron.*, vol. 13, no. 4, 2024, doi: 10.3390/electronics13040807.

[4] Z. G. Al-Mekhlafi, M. A. Al-Shareeda, S. Manickam, B. A. Mohammed, and A. Qtaish, "Lattice-Based Lightweight Quantum Resistant Scheme in 5G-Enabled Vehicular Networks," *Mathematics*, vol. 11, no. 2, pp. 1–17, 2023, doi: 10.3390/math11020399.

[5] M. A. Al-shareeda *et al.*, "NE-CPPA: A New and Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks (VANETs)," *Appl. Math. Inf. Sci.*, vol. 14, no. 6, pp. 957–966, 2020, doi: 10.18576/amis/140602.

[6] C. Serôdio, J. Cunha, G. Candela, S. Rodriguez, X. R. Sousa, and F. Branco, "The 6G Ecosystem as Support for IoE and Private Networks: Vision, Requirements, and Challenges," *Futur. Internet*, vol. 15, no. 11, pp. 1–32, 2023, doi: 10.3390/fi15110348.

[7] A. H. Abdi *et al.*, "Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI, and MTD Approaches to Security Solutions," *IEEE Access*, vol. 12, no. March, pp. 69941–69980, 2024, doi: 10.1109/ACCESS.2024.3393548.

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

[9] A. Hamarsheh, "An Adaptive Security Framework for Internet of Things Networks Leveraging SDN and Machine Learning," *Appl. Sci.*, vol. 14, no. 11, 2024, doi: 10.3390/app14114530.

[10] S. Algarni, F. Eassa, K. Almarhabi, A. Algarni, and A. Albeshri, "BCNBI: A Blockchain-Based Security Framework for Northbound Interface in Software-Defined Networking," *Electron.*, vol. 11, no. 7, pp. 1–27, 2022, doi: 10.3390/electronics11070996.

[11] S. S. Mahdi and A. A. Abdullah, "Enhanced Security of Software-defined Network and Network Slice Through Hybrid Quantum Key Distribution Protocol," *Infocommunications J.*, vol. 14, no. 3, pp. 9–15, 2022, doi: 10.36244/ICJ.2022.3.2.

[12] J. Li *et al.*, "A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System," *IEEE Access*, vol. 8, pp. 135479–135490, 2020, doi: 10.1109/ACCESS.2020.3011503.

[13] 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, no. August, pp. 91550–91582, 2023, doi: 10.1109/ACCESS.2023.3307467.

[14] S. N. Mjeat, M. Yousif, S. Bader, O. Mohammed, and A. H. Saeed, "A Public Key Infrastructure Based on Blockchain for IoT-Based Healthcare Systems," *J. Cybersecurity Inf. Manag.*, vol. 15, no. 1, 2025, doi: 10.54216/jcim.150118.

[15] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, "A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges," *J. Inf. Intell.*, vol. 2, no. 6, pp. 455–513, 2023, doi: 10.1016/j.jiixd.2023.12.001.

[16] M. A. Al-Shareeda and S. Manickam, "Man-in-the-Middle Attacks in Mobile Ad Hoc Networks (MANETs): Analysis and Evaluation," *Symmetry (Basel).*, vol. 14, no. 8, 2022, doi: 10.3390/sym14081543.

[17] R. Bukhowah, A. Aljughaiman, and M. M. H. Rahman, "Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions," *Electron.*, vol. 13, no. 6, 2024, doi: 10.3390/electronics13061031.

[18] M. A. Al-shareeda *et al.*, "Proposed Efficient Conditional Privacy-Preserving Authentication Scheme for V2V and V2I Communications Based on Elliptic Curve Cryptography in Vehicular Ad Hoc Networks," in *Advances in Cyber Security*, M. Anbar, N. Abdullah, and S. Manickam, Eds., Singapore: Springer Singapore, 2021, pp. 588–603.

[19] M. Q. Jawad and M. Yousif, "Improving Video Streaming Quality and Network Efficiency through Data Distribution Services," vol. 1, no. 01, pp. 97–107, 2025.

[20] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms," *Sensors*, vol. 24, no. 2, 2024, doi: 10.3390/s24020713.

[21] A. Ataalla, M. Al-yousif, and A. S. Bader, "A Hybrid GA-GWO Method for Cyber Attack Detection Using RF Model," *J. Cybersecurity Inf. Manag.*, vol. 15, no. 1, 2025, doi: 10.54216/jcim.150117.