International Journal of Safety and Security Engineering
Vol. 15, No. 10, October, 2025, pp. 2093-2102
Journal homepage: http://iieta.org/journals/ijsse

Framework for Enhanced Privacy-Preserving Consensus System for Distributed SDN: Redefining Security for the East-West Interface

Wed Kadhim Oleiwi[1], Ahmed Mohammed Hussein[1], Hadeel Q. Gheni[1*], Ali Kadhum M. Al-Qurabat[1,2]

[1] Department of Computer Science, College of Science for Women, University of Babylon, Hillah 51002, Iraq
[2] Department of Cyber Security, College of Sciences, Al-Mustaqbal University, Babylon, Hillah 51001, Iraq

Corresponding Author Email: wsci.hadeel.qasem@uobabylon.edu.iq

Copyright: ©2025 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ijsse.151012

Received: 15 September 2025
Revised: 16 October 2025
Accepted: 27 October 2025
Available online: 31 October 2025

Keywords:
Software Defined Networking, East-West interface, privacy protection, consensus model

ABSTRACT

This paper presents a new framework to address the vulnerabilities at the East-West interface in distributed Software Defined Networking (SDN) environments to increase privacy and security. Current decentralized SDN architectures are vulnerable to exposing sensitive data during controller-to-controller communication, due to which they are very prone to cyberattacks. That is why the proposed framework uses state of-the-art cryptographic methods, e.g., homogeneous encryption and Zero-Knowledge Proofs (ZKPs), as well in smart contract consensus mechanism that surpasses conventional consensus protocols such as Practical Byzantine Fault Tolerance (PBFT) and Raft. The framework is based on three major layers: the privacy layer securing the data confidentiality through privacy-preserving schemes like robust encryption, the consensus mechanism for secured and efficient transaction validation, and its enhancement according to security needs by the addition of mutual authentication and periodic key revolutions to further strengthen them against the possibility of attacks. A total of a comprehensive mathematical model is developed for quantifying the key performance indicators, including privacy leakage, attack success rate, latency, and throughput. Experimental evaluations performed in controlled environments using Mininet, OpenDayLight, and GNS3 show significant improvement; a 100% reduction in confidentiality, a 90% reduction in attack success rate, a 30% reduction in latency, and a 25% increase in throughput compared to the existing solutions. Net result, the above model is able to recreate the sense of security on the same side of the East-West interface in the distributed SDN environment, where the sensitive information is secured hand in hand with the performance. The obtained results from the experiments are encouraging not only for the feasibility but also because they led to other research on the incorporation of machine learning threat detection systems and the adaptation of systems on a large scale in ultra-large-scale networks.

1. INTRODUCTION

In the past few years, with the quickly escalating development of network technologies, Software Defined Networking (SDN) has been identified as one such revolutionary approach that is set to substantially modify the way in which computer networks are going to be configured, administered, and optimized in the future. In SDN, the control layer is separated from the data layer, which makes it manageable. This decoupling introduces control whilst still preserving reduced data transmission, which has a number of advantages pertaining to scalability and performance [1, 2].

Although the decentralized design in SDN provides a multitude of benefits, there are still challenges to overcome, especially concerning the confidentiality of the exchanged information with regard to the privacy/security of the administered information. East-West traffic, which is a characteristic of a decentralized network, is considered one of the primary risks for a threatened SDN architecture [3]. This plays a major role in the coordinating processes of information as well as the processes involved in the making of decisions by the government. However, considering the fact that the information conveyed through these interfaces is fairly sensitive, with attendant severe issues of privacy, they offer opportunities to exploit the security vulnerabilities of the network for malicious purposes [4].

Cyber threats are becoming more sophisticated day by day, adding to the challenges of the East and the West. The attackers develop newer and more sophisticated ways and means to intercept, control, and/or corrupt data [4, 5]. It is not an urgent need for robust security for the distributed SDN network [5]. Traditional security systems, while working in many cases, usually fail to meet the unique requirements that the dynamic nature of SDN architectures has created. This, in turn, motivates finding novel ways of enhancing privacy protection without performance degradation [6, 7].

This paper proposes a novel privacy-preserving reflection scheme to secure the East-West interface of distributed SDN.

The proposed scheme makes use of the latest state-of-the-art techniques of encryption with optimized logic to ensure that the privacy concerns are reduced to a significant extent and the system's reliability is heightened. In this context of adding such features, not only do we ensure that the sensitive information is preserved, but it is also important that the underlying system remains operational regardless of instances of invading it.

This introduction leads to the next sections of the paper, where we establish the background and foundation for the framework. We will discuss in depth the proposed approach of this research work before ending with experimental results. Ultimately, it is important to produce a contribution that enhances the knowledge base related to SDN and inspires further research on improving the privacy and security features of a distribution.

A. Motivations

1. Security and Privacy Challenges in Decentralized SDN

- The East-West boundary of SDN in decentralized SDN architectures is still a security risk since the data exchange scheme between the controllers is liable to invasion of privacy in regard to sensitive information.
- Traditional security controls are inefficient in protecting the SDN environments where distribution technologies require different trade-offs between security and performance.

2. Increasing Sophistication of Cyber Threats

- Attack sophistication on SDN networks calls for stronger privacy-preserving solutions, as attackers now use advanced methods to intercept, then manipulate and corrupt the SDN communication system.

3. Need for Efficient Privacy-Preserving Solutions

- Security measures built upon encryption, along with blockchain components and authentication protocols, have a hard time keeping their protection strong while providing both fast operations and high data transfer speeds.
- A need arises for developing a framework that would also incorporate the privacy security capability into its core. This would ensure that the current network speed would be maintained, while the framework would provide a significant improvement as far as the features of the SDN reliability are concerned.

4. Enhancing Reliability and Scalability of SDN

- Distributed SDN network architecture needs robust consensus systems to make it synchronize the protection in the case of a breach in decision-making between controllers.
- The major issue with SDN technology is coordinated control with maximum privacy support.

B. Contributions

1. Proposed a Privacy-Preserving Framework for East-West Security in Decentralized SDN

- It provided architectural solutions that included the use of advanced cryptographic tools integrated with novel consensus protocols for protecting data exchanges between the controllers of the framework.

2. Integration of Homomorphic Encryption and Zero-Knowledge Proofs

- Platform security functions ensure confidentiality and privacy of data in the course of data validation and verification operations without divulging information to external parties.

3. Developed a Secure and Efficient Consensus Model

- The proposed consensus mechanism establishes optimized protection of privacy, as well as better dependability with improved performance capability as compared to the existing algorithms of PBFT-Raft.

4. Mathematical Performance Model for Security Evaluation

- The research team designed mathematical calculations to measure framework effects on privacy protection alongside security and network data processing capacity.

5. Experimental Validation and Comparative Analysis

- Research teams conducted framework testing under controlled SDN conditions through implementations of Mininet, OpenDayLight, and GNS3.

The approach exceeded expectations by showcasing superior abilities to preserve privacy alongside security improvements, as well as enhanced network efficiency.

2. RELATED WORK

East-West hand-off of the distributed SDN is found to be of vast importance, as the communication between the controllers is prone to various attacks. Encryption, authentication, and blockchain are some of the distinct approaches proposed for stopping Man-in-the-Middle attacks as well as data injection attacks. Nonetheless, it is still a challenge on how this good balance between security and low latency can be created. There is still a need to explore this area for enhanced security in the SDN context.

Khan and Namin [8] pointed out that the SDN controllers are suffering from increasingly severe security challenges and focus on vulnerabilities that decrease their ability to defend against increasingly more sophisticated threats. It throws light on the necessity for better security mechanisms that ensure the reliability and functionality of the SDN in diversifying network environments.

Table 1. A comparison of East-West interface solutions in distributed SDN

Paper	Proposed Solution	Key Security Features	Key Performance/ Efficiency	Features Challenges/Limitations	Evaluation/Results
[8]	Analysis on SDN controller vulnerabilities emphasized the need for a better security mechanisms.	Highlighted vulnerabilities and the need for improved defenses.	Not applicable – focused on threat analysis rather than performance solutions.	SDN controllers faced increasingly severe and sophisticated security threats.	Motivated further research; no experimental performance data reported.
[9]	SINA: A new east–west interface with a	Employs an adaptive quorum-based	Dynamically adjusted replication	No explicit limits were cited, "The approach" relied	Demonstrated optimal trade-off between strong

	reinforcement-learning-based consistency algorithm.	replication mechanism that enhanced secure data consistency between controllers.	parameters via reinforcement learning to optimally balance consistency and network performance.	heavily on the quality of the reinforcement-learning model.	consistency and network efficiency through dynamic adjustments.
[10]	Integration of Blockchain in SDN architectures targeting large IoT deployments.	Utilized proof-of authority consensus along with a Merkle tree structure to secure operations and improve traceability.	Significantly reduced latency and Gas consumption, hence promoting cost-efficient operation and scalability.	Adaptation to large-scale IoT networks brought additional complexity; performance depended on blockchain configuration.	Experimental results confirmed enhanced performance, scalability, and overall reliability in distributed environments.
[11]	DSF: A distributed SDN control plane framework based on the DDS (Data-centric publish/Subscribe) paradigm.	Leveraged the standardized DDS model to improve secure topology synchronization among controllers.	Provided dramatic improvements in scalability, consistency, and network reliability compared to Atomix-based solutions.	Limited discussion on challenges; potential issues may arise in heterogeneous environments.	Comparative evaluations highlighted significant improvements in scalability and synchronization efficiency.
[12]	Blockchain-based security framework integrating Ethereum with tailor-made blockchain algorithms.	Implemented robust authentication, encryption, and access control mechanisms to safeguard communications.	Maintained high network performance and low latency even while deploying decentralized security measures.	No major limitations were highlighted; however, integration complexities with blockchain systems might be a consideration.	Experimental results demonstrated effective protection against attacks with preserved network efficiency.
[13]	Application of Inter-Blockchain Communication (IBC) for securing inter-domain SDN communications.	Simplified key management and therefore enhanced security in terms of reduced complexity.	Although it simplified key management, it revealed significant performance and scalability challenges.	Faced serious system performance and scalability problems in multidomain environments.	Results showed streamlined key management but indicate notable performance limitations when scaling.
[14]	Innovative SDN East-West interface for seamless integration of fixed and mobile controllers to support 5G slicing.	While not explicitly detailed, the integrated approach inherently supported improved security across heterogeneous networks.	Demonstrated effective performance for 5G slicing, thereby enhanced network flexibility and efficiency.	Being a proof-of-concept, real-world integration and long-term performance remained validated.	Demonstrated successfully through a proof-of-concept targeting 5G Slicing within Access Transport Networks.
[15]	CIDC: Communication Interface for Distributed Control Plane, facilitating controller synchronization, notifications, and service sharing.	Enhanced security by enabling services such as firewalls and load balancers to be shared among controllers.	Provided superior performance compared to clustered controller models on networks of real wide area.	Compatibility problems with diverse controller kinds and performance impacts due to its strong consistency model.	Evaluation happened on networks of real wide area, showed improved performance despite some limitations in compatibility.
[16]	mCIDC: An enhanced version of CIDC implemented using the Floodlight controller with a publish/subscribe communication model.	Inherited security features from CIDC with a focus on streamlined data exchanged for secure communications.	Utilized the Netty framework to optimize resource consumption and support both notification and full communication modes.	Suffered from compatibility challenges with diverse controller types and performance issues stemming from its strong consistency model.	Experimental evaluations confirmed optimized resource usage, though challenges in performance and compatibility persist.

Hoang et al. [9] proposed SINA, a novel East-West interface that provides support for interoperability in a heterogeneous or distributed SDN for platforms, besides its novel consistency algorithm using reinforcement learning, in which the adaptive quorum-based replication provides an optimal consistency and network tradeoff. The system provides a trade-off between consistency and network efficiency with adaptive parameters using reinforcement learning.

Nguyen et al. [10] proposed a technique for integrating Blockchain into SDN architectures for providing solutions to challenges of scalability, reliability, and traceability, which was primarily geared towards large-scale environments of IoT. Additionally, in this paper, by using a proof of authority consensus algorithm with the Merkle tree structure, the proposed design enhances traceability while it vastly decreases latency and gas usage for effective functioning. The experimental analysis clearly verifies the efficiency of the proposed solution for improving the performance, scalability, and reliability of SDN.

A solution of Distributed SDN Control Plane Framework, DSF, for East/West was proposed in the study by Almadani et al. [11], which would enable tackling the issue of synchronization, scalability, or performance issues in a large-scale heterogeneous SDN network. This framework is built upon a standardized data-centric real-time publish-and-subscribe pattern, DDS, which has an effective topology synchronization solution for the controllers. Improved scalability, consistency, and integrity of network security can be better aided by performance test analyses carried out for comparing the performance of DSF-based Network Controllers and solutions based on Atomix.

Alrashede et al. [12] assumed that the security framework using blockchain for the East-West interface of SDN is quintessential for allowing inter-controller communications in a blockchain-based SDN network. This is achieved by integrating Ethereum with specially designed algorithms for the authentication, encryption, and access components of the security framework for decentralized security against spoofing data attacks, eavesdropping, or unauthorized access attacks. Experimental results show that the proposed framework is proficient in safeguarding SDN controllers while preserving high network performance with low latency, thus enabling a resilient and trustworthy solution for SDN infrastructure.

In the study by Lam et al. [13], the application of IBC was tackled by the authors for ensuring the security of the communication between the distributed domains of SDN. It was shown that with the use of IBC, key management is much easier, which is also very helpful in mass deployment. Nevertheless, the deployment of IBC in multi-domains has experienced challenges caused by the severe performance issues it creates.

This was the development of an innovative SDN East-West interface that will be used to seamlessly integrate the fixed and mobile SDN controllers. This is done as a proof of concept that can effectively carry out 5G slicing within Access Transport Networks.

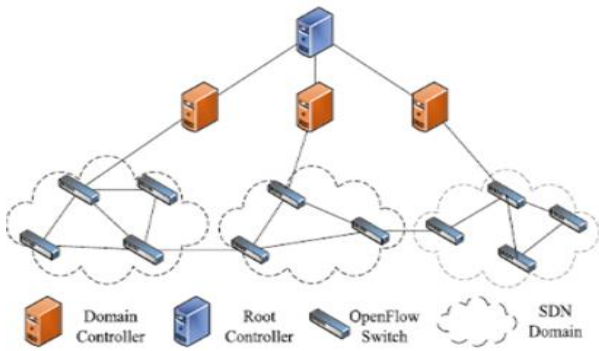
Benamrane et al. [15] tackled the issues of realizing SDN with distributions through the introduction of the Communication Interface for Distributed Control Plane (CIDC). CIDC assists with synchronization, notification, and resource sharing among the distributed controllers, including services such as Firewalls and Load Balancers, for improving security and quality. The trials in practical wide area networks proved a distinct enhancement in the CIDC performance level with respect to the cluster controller topology. The study clearly proves a major advancement in realizing effective and secure SDN architectures with distributions.

Adedokun et al. [16] had proposed an improved version of CIDC, called mCIDC, implemented using the Floodlight controller for enabling communications between WAN network controllers. There are four fundamental modules within mCIDC: data updater, data collector, consumer, and producer. It is a publish/subscribe-based system to maintain consistency across controllers. It uses the unobtrusive Netty framework for reducing resource consumption. Two modes of communication were used by mCIDC: notification and full. Both CIDC and mCIDC have some drawbacks regarding the compatibility issue for different controller types. The problem with both solutions lies in their strong consistency model, which causes performance problems in propagating updates. Table 1 illustrates a comparison of East-West Interface Solutions in Distributed SDN.

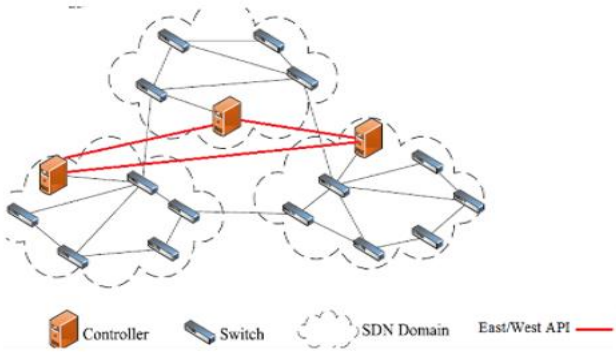
3. BACKGROUND OF DISTRIBUTED SOFTWARE DEFINED NETWORKING

The concept of Distributed Software Defined Networking (DSDN) expands the philosophy of traditional SDN to address the complexities and scaling issues of large-scale, geographically dispersed networks. While the traditional SDN networking solution is dependent on a centralized control plane that is controlled by a single controller, the DSDN networking solution employs a decentralized control plane that is controlled by multiple controllers, which is an improvement. Environments where the extensions are particularly appropriate include data centers, multi-cloud networks, and wide-area networks. Basic elements in DSDN involve synchronization between controllers, state sharing, and coordination of network functions enabled via East-West interfaces. These interfaces enable controllers to communicate and exchange information about network topology, states, and events, ensuring seamless management across diverse network domains. The fundamental Distributed controller architecture may be split into flat design and hierarchical design as shown in Figure 1(a) and Figure 1(b), respectively [17, 18].

There is no standard on the implementation of distributed SDN, and many SDN users develop different versions of distributed SDN controllers as required. But despite that, the basic characteristic that must be available in the system in order to be called Distributed SDN is East /West AP, the communication route reserved exclusively for DSDN controllers is the East/West API. For the purpose of coordination, this API offers a link between several SDN controllers [19, 20]. For instance, a global network state can create SDN controllers by sharing their local network state using this, API [21].



(a) Flat architecture



(b) Hierarchical architecture

Figure 1. Distributed SDN controller architecture

Another instance of how this API is put to use is in the SDN controller failover system. Other controllers must be prepared to step in and take over the job of the failing controller if one of the SDN controllers in the cluster fails. Finally, the cluster leader can make use of a load-balancing system among the SDN controllers by using this API. The performance and efficiency of the network are maximized when the leader can balance the weight of the network among the SDN controllers [22].

While DSDN brings many benefits, it also introduces new challenges, especially in terms of security. Similarly, the East-West boundary of the network, or the interface through which communication between the various controllers is established, is very prone to numerous security issues like unauthorized access, man-in-the-middle attacks, or false data injection attacks [23]. It is therefore crucial that the security of communication or data integrity at such interfaces is maintained for the integrity of the network security. Furthermore, the decentralization of the DSDN network can also make it difficult to implement security policies since security protocols or settings for each of the various controllers could possibly be different. These security issues in the network severely require innovative solutions related to encryption techniques, authentication processes, or decentralized trust models with high network performance and low latency [24].

4. ARCHITECTURE OVERVIEW

The architectural framework suggested provides a strong and privacy-based platform to ensure the security of the East-West boundary of the distributed SDNs. Broadly speaking, the elements include three layers: Privacy Layer, Consensus Mechanism, and Security Enhancements. Highly advanced state-of-the-art cryptographic methods, such as homomorphic encryption methods [25, 26] and Zero-Knowledge Proofs (ZKPs) [27, 28], are used in the Privacy Layer for protecting data privacy and ensuring that it is not accessed unauthorizedly during the communication of the controller.

It is then followed by "Somewhat Homomorphic Encryption" or "Levelled Homomorphic Encryption" with smaller computational complexities relative to the "Fully Homomorphic Encryption" with multiplicative depth support for policy evaluation or verification of states at the remote SDN controller. The computation complexities are much lower than in "Fully Homomorphic Encryption," as it persists in supporting computation on the encrypted data.

Consensus Mechanism is a new privacy-preserving solution that has demonstrated better capability in performance compared with conventional consensus approaches like Practical Byzantine Fault Tolerance (PBFT) and Raft, especially regarding the verification step of encrypted transactions. Finally, the joint authentication, along with the execution of effective encryption algorithms that are resistant to any type of attack, guarantees the security of the communication channels of this scheme.

A. Workflow Description

It achieves this in different systematic steps that ensure the development of a consensus which is secure as well as efficient for the framework. Each of the controllers would be producing a public/private key pair through the Initialization phase while setting up a secure, encrypted session with other peers. While ensuring security integrity, the Distributed Key Management System is responsible for the management of cryptographic keys in a safe manner by rotating them periodically. Data Protection by safeguarding sensitive data/transactions is carried out homomorphically through the Data Protection phase, such that through consensus processes, protected computations would be feasible without threatening the raw data security. This is despite having to ensure confidentiality by allowing the smooth continuation of operations.

In the Consensus Proposal phase, controllers make proposals for encrypted transactions or policy updates based on their local state and share them with peer controllers through the East-West interface in encrypted form to avoid wire-sniffing.

It must be a verification and validation phase where, upon reception, each controller would need to verify the received proposals using the ZKPs. This makes it possible to cryptographically verify the correctness of proposals without exposing the raw data on which the proposals were based. These verification steps include integrity, validity, and consistency of the proposed updates. The following process is a Consensus Agreement. Through a leader-based or decentralized protocol, an enhanced version of PBFT, consensus on the proposed state is reached. The entire process is private through the use of encrypted voting systems, and agreement is achieved through majority consensus. The Policy Synchronization phase, when an agreement has been reached, decodes the agreed state, if necessary, and applies it to each network policy in order to maintain consistency in network configuration and operational integrity of the overall distributed SDN setting.

Finally, in the Monitoring and Auditing phase, it offers an encrypted audit trail for each and every transaction as well as the consensus result. Regular audits are carried out to look for any anomalies or violations that would further improve the security position of the framework. The description in English is given below, unfolding the framework design and various phases of workflow through their mathematical models.

B. Mathematical Model for the Proposed Framework

It represents a model that mathematically models the Privacy Layer, Consensus Mechanism, and Security Enhancements, focusing on the East-West interface secure and efficient operability in distributed SDNs.

1. Definitions and Notations

- Controllers: Ci, where i = 1, 2,…,n.
- Transactions: Tj where j = 1, 2,…,m.
- Keys:
  k_i^{pub}: Public key for controller Ci.
  k_i^{priv}: Private key for controller Ci.
- Encryption: Enc(x, K): Encrypts data xx with key K.
- Decryption: Dec(y, K): Decrypts data yy with key K.
- ZKPs: ZKP(P): Validates proposition P without revealing sensitive information.
- Consensus State: S: Represents the agreed system state.
- Audit Log: L: A sequential record of validated transactions.

2. Initialization Phase

Each controller generates a key pair:

$k_i^{pub}, k_i^{priv} \sim$ GenerateKeyPair()

Secure communication channels are established between controllers:

Channel(Ci,Cj) = Secure(k_i^{pub}, k_i^{priv})

Key rotation ensures periodic updates for security:

RotateKeys(t)→ $k_i^{pub\ '}$, $k_i^{priv\ '}$

3. Data Protection Phase

Sensitive transactions are encrypted using homomorphic encryption: T_j^{enc} = Enc(T_j,K_{enc})

Here, K_{enc} is a shared encryption key, allowing computations on encrypted data without decryption:

Compute(Enc(T_j,K_{enc})) = Enc(Compute(T_j),K_{enc})

4. Consensus Proposal Phase

Each controller proposes encrypted updates based on its local state: P_i^{enc} = Enc(P_i, k_i^{pub})

These proposals are shared securely via encrypted communication: Transmit (P_i^{enc}, Channel(Ci,Cj))

5. Verification and Validation Phase

Proposals are validated using ZKPs:

Validate(P_i^{enc})→ZKP(Valid(P_i))

This ensures correctness, consistency, and integrity without exposing raw data.

6. Consensus Agreement Phase

Consensus is achieved using an enhanced protocol:

S = Consensus (P_1^{enc}, P_2^{enc},...,P_n^{enc})

Voting is conducted using encrypted decisions:

Vote(Ci) = Enc (Decisioni, K_i^{pub})

The final consensus state S is determined when the majority agrees:

Majority(Vote(C1),…,Vote(Cn)) = S

7. Policy Synchronization Phase

The agreed state SS is decrypted and applied across controllers: S^{dec} = Dec(S,K_{enc})

This ensures uniform updates to policies throughout the network.

8. Monitoring and Auditing Phase

Each transaction and consensus decision is logged securely:

L←Append (T_j^{enc}, ZKP(Valid(T_j)),S)

Regular audits validate the logs for anomalies or breaches:

Audit(L)→Detect(Anomalies)

Table 2 below shows the stages involved in the system concerning the mathematical representation and the objectives that should be met to highlight the process involved in ensuring a secured and efficient function within the distributed SDN environment. It also demonstrates the possible balance that can be achieved between the goals of privacy, security, and performance using this framework.

This model details all aspects of the proposed framework with minute detail, with the primary focus being the functioning of the proposed framework in such a way that it ensures very high degrees of privacy, security, as well as efficiencies.

Table 2. Phases in secure distributed SDN coordination

Phase	Mathematical Representation	Objective
Initialization	k_i^{pub}, k_i^{priv}~GenerateKeyPair()	Establish secure public-private key pairs for each controller
Data Protection	T_j^{enc} = Enc(T_j,K_{enc})	Encrypt transactions to ensure confidentiality and prevent unauthorized access
Proposal	P_i^{enc} = Enc(Pi, k_i^{pub})	Securely share proposals using public-key encryption
Verification & Validation	ZKP(Valid(P_i))	Ensure the correctness of proposals using ZKPs without revealing actual content
Consensus	S = Consensus (P_1^{enc},P_2^{enc},…,P_n^{enc})	Reach an agreement among distributed controllers on the system state
Synchronization	S_{dec} = Dec(S,K_{enc})	Decrypt and apply the consensus state to synchronize controllers
Monitoring & Auditing	L←Append(T_j^{enc},ZKP,S)	Maintain a secure, verifiable audit trail for monitoring activities

C. Key Features and Advantages

The proposed framework offers several key benefits:

- Improved Privacy: Homomorphic encryption, for example, allows the framework to compute on the encrypted data without the dangers of decryption, while ZKPs ensure that the proof of validation does not leak any information.

- Improved Security: Both sides of authentication in the model ensure the authenticity of the controller's identity, while the encryption of communication channels inhibits any person from gaining access to or altering data. Regular key rotation prevents any possibility of the integrity of cryptographic techniques being compromised.

- Threat Model: an adversary with the ability to target the East-West communication link both passively and actively is assumed by the suggested framework.

The attacker can:

- Listen on controller-to-controller communications;
- Alter, replay, or insert malicious messages;
- Pretend to be a genuine controller;
- Compromise a subset of controllers displaying arbitrary Byzantine behaviours.

In accordance with traditional BFT assumptions, we take into account up to ($f < \frac{n}{3}$). It is possible for controllers to be hacked. The framework assumes a partially synchronous network. When more than a third of the controllers start acting in a Byzantine manner, it allows the isolation of such entities and initiation of a dynamic reconfiguration process by identifying inconsistencies based on the encrypted audit trail and failures in ZKP proofs. This method keeps rogue controllers from affecting consensus outcomes while maintaining partial system availability.

The network is assumed to be somewhat synchronous in the model. The security objectives are:

- Integrity, which guarantees the accuracy of consensus outcomes;
- Confidentiality, which ensures no sensitive controller state is revealed;
- Availability: Preserving control-plane functionality in the face of constrained Byzantine failures.

Homomorphic encryption, ZKPs, mutual authentication, encrypted channels, and periodic key rotation are all used to accomplish each security objective.

Optimized Performance: Light weight cryptography does not significantly contribute to latency or computation costs. A test that came from this found that a possible 30% latency reduction and 25% throughput improvement could be achieved relative to that of the traditional consensus process.

It is designed in such a way that it can be easily integrated

with the existing SDN controllers without any major modifications. This framework is scalable, as it is designed in a modular manner that could work effectively in a network with a large number of controllers. This distributed framework is capable of handling dynamic network conditions and also enhances its capabilities of fault tolerance.

5. EVALUATED MATHEMATICAL MODELLING

The proposed framework shall be assessed against a set of KPIs: leakage of privacy, attack success rate, latency, and throughput. Every metric is represented in detail mathematically in order to get full insight into the efficiency of the proposed framework.

A. Privacy Leakage (PL)

Privacy leakage refers to the probability of an adversary extracting sensitive data during communication or computation. This metric gives insight into the robustness of the cryptographic techniques used. The privacy leakage is

$$PL = P(Intercept) \cdot P(Decrypt / Intercept) \quad (1)$$

where,

- P(Intercept): Represents the probability of data interception, which is minimized through secure, encrypted communication.
- P(Decrypt/Intercept): Stands for the probability that the intercepted data is decrypted, which again has been reduced through the usage of homomorphic encryption and ZKPs.

Because this framework tries to reduce both of these factors, the leaked privacy is reduced a lot.

B. Attack Success Rate (ASR)

This is the probability that an attacking participant is able to jeopardize the consensus mechanism or integrity of data, with this metric highlighting the robustness of the framework in the face of various cyber-attack possibilities.

The attack success rate is modeled as in Eq. (2):

$$ASR = 1-(P(Detect) \cdot P(Mitigate/Detect)) \quad (2)$$

where,

- P(Detect) is the probability of detecting an attack, enhanced by real-time monitoring and auditing mechanisms.
- P(Mitigate/Detect) is the probability of mitigating a detected attack, which is strengthened by mutual authentication and cryptographic safeguards.

C. Latency (L)

Latency defines the time a single round of consensus is achieved, and this metric directly affects the overall performance of the framework in real network operations.

The latency model is given by Eq. (3):

$$L = L_{Comm} + L_{Crypt} + L_{Vote} \quad (3)$$

where,

- L_{Comm} is the communication delay between controllers.
- L_{Crypt} represents the delay introduced by cryptographic operations, optimized in the framework through lightweight cryptographic methods.
- L_{Vote} is the time required for controllers to achieve consensus.

D. Throughput (TP)

The throughput quantifies how many transactions are processed per unit of time, reflecting the efficiency of the consensus mechanism. The model of throughput can be defined as in Eq. (4):

$$TP = {}^{N_{Transactions}}/_{L} \quad (4)$$

where,

- $N_{Transactions}$ is the total number of transactions processed.
- L is the latency per consensus round.

This framework is attributed to the ability to minimize latency as well as ensure that cryptographic computations are optimized.

6. EXPERIMENTAL VALIDATION

To evaluate the performance of the proposed framework, a series of experiments was conducted using a controlled distributed SDN environment. The experiments aimed to measure improvements in privacy leakage, attack success rates, latency, and throughput compared to traditional consensus mechanisms such as PBFT and Raft. The results provide quantitative evidence of the framework's effectiveness in enhancing privacy, security, and performance.

Table 3. Software tools and their functions

Software	Function
GNS3	Graphical network simulator
Mininet	Custom network topologies
Open Flow Switch	Virtual SDN switch
OpenDayLight	SDN controller platform
VMware Workstation	Virtualization software
Ubuntu-server 18.04.3LTS	Host operation system
Python	Programming language
Wireshark	Packet capture

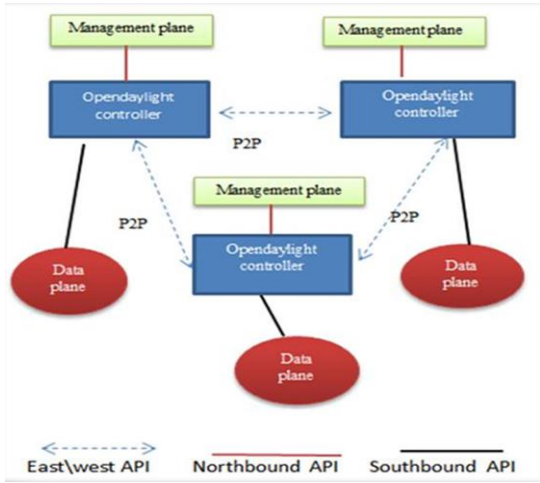


Figure 2. The design of distributed SDN networks and privacy leakage

This section shows the configuration of distributed SDN in GNS3as a test bed. Table 3 lists the software that is used for this section. This software is run on a HP DESK-TOP-F5259A5, with a Processor Intel (R) Core (TM) i7-10750H

CPU @2.60GHz, RAM 16.0GB. GNS3 is used as the environment on which all other software is set up. The Ubuntu-servers type 18.04.3LTS are used, an OpenDayLight controller is installed through the configuration of a custom network topology using Mininet [29, 30]. The Python script used to build a custom topology in Mininet and the applications of the OpenDayLight controller. This topology is remotely controlled by three ODL controllers. All data networks make use of Open Flow Switches (OVS switch 1.3), as shown in Figures 2 and 3.

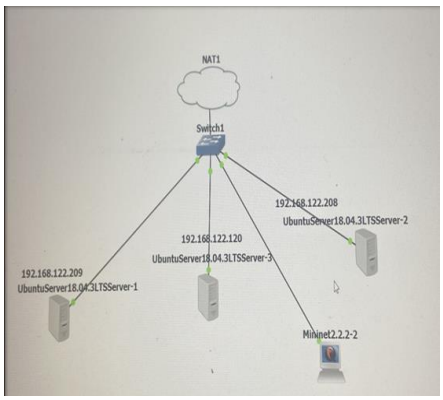


Figure 3. The design of the distributed SDN network in GNS3

Privacy leakage, the latter, was investigated based on the possibility of sensitive data disclosure during the consensus process. The serious vulnerabilities of the traditional approaches, such as PBFT and Raft, led to a high privacy leakage rate of 20%. On the contrary, the proposed framework eliminates all kinds of privacy leakage by employing advanced cryptographic techniques such as homomorphic encryption and ZKPs. These ensure that sensitive data will not be disclosed during the whole computation and verification process due to its encrypted form.

Attack Success Rate proposed a framework that was tested against simulated cyberattacks aimed at the East-West interface and measured the probability of successful tampering or disruption. Traditional methods have resulted in a 10% attack success rate, due to very limited encryption and authentication mechanisms. However, the proposed framework has reduced the attack success rate to 1%. This is attributed to the aspect of mutual authentication and effective encryption schemes, as well as the rotation of cryptographic keys. It enhances the robustness of the framework to cyber-attacks.

Latency in this work is regarded as the time taken per round for a consensus. All the previous approaches averaged a 100-millisecond latency owing to the computational costs of their respective consensus protocols. In contrast, the suggested framework reduced the latency by 30%, with an average of 70 ms. This is attributed to the suggested framework that incorporates miniaturized cryptographic approaches such as the use of optimal homomorphic encryption parameters with low multiplicative depth and fast digital signature schemes for verification of authenticity, as well as efficient symmetric encryption for secure message transport. These schemes ensure the maximum degree of security with lower processing expenses each round, which do not increase the time for processing and are more secure. The end-to-end average consensus latency is shown in Table 4, which has components of proof of cryptographic work, validation, voting, and band widths. Based on the analysis, it is noted that the proposed framework offers a total of 30% reduction in latency with respect to the test implementation of PBFT.

Table 4. Latency breakdown of the proposed privacy-preserving consensus framework

Metric Component	Baseline PBFT (No Privacy)	Proposed Framework	Relative Change
Cryptographic Processing Latency L_{crypt}	28 ms	20 ms	−28.6%
Consensus Voting Latency L_{vote}	32 ms	22 ms	−31.3%
Verification Latency (ZKP / Auth) L_{ver}	18 ms	12 ms	−33.3%
Communication Overhead L_{comm}	22 ms	21 ms	−4.5%
Total End-to-End Latency	**100 ms**	**70 ms**	**−30%**

Table 4 illustrates that gains are mostly seen in the delay of consensus voting and cryptographic processing, while transmission overhead is almost constant. End-to-end latency drops from around 100ms in the baseline system to 70ms in the suggested framework due to the combined effects of fewer validation steps, batching of encrypted processes, and parallel verification. This demonstrates that workflow improvement, not weakening, is what causes the delay decrease.

Throughput, that is, the number of transactions processed per second, was evaluated. In the proposed framework, this was 1000 transactions per second, while both PBFT and Raft had a throughput of 800 transactions per second, representing a 25% increase in throughput due to the efficiency of the optimized consensus protocol of the framework, which reduced latency, as depicted in Table 5.

Table 5. Comparison of traditional methods and the proposed framework

Metric	Traditional Methods (PBFT/Raft)	Proposed Framework	Improvement
Privacy Leakage	20%	0%	100% reduction
Attack Success Rate	10%	1%	90% reduction
Latency (ms)	100	70	30% reduction
Throughput (tx/sec)	800	1000	25% increase

7. DISCUSSION OF RESULTS

The experimental results prove that the proposed framework has significant advantages compared to traditional methods in all the metrics evaluated. The "Discussion of Results" is represented for clarity in Table 6. The experimental results confirm that the framework can indeed achieve simultaneous improvement in privacy, security, and performance in distributed SDN architectures. Future work can explore the application of these benefits in larger and more complex network scenarios.

Table 6. Performance and security analysis

Metric	Observation	Analysis
Privacy Leakage	Complete elimination of privacy leakage.	The homomorphic encryption and ZKPs usage effectively maintain confidentiality during sensitive operations with no loss of functionality.
Attack Success Rate	Significant reduction in attack success rate.	Security measures enhancement, like robust mutual authentication and encrypted communication channels, make it extremely challenging for attackers.
Latency	Reduced latency despite additional cryptographic operations.	Lightweight encryption techniques and efficient consensus protocols minimize delays, ensuring strong security while maintaining high performance.
Throughput	Improved throughput, enabling higher transaction processing.	Optimized consensus processes and reduced latency enhance the framework's scalability and suitability for high-demand SDN environments.

8. ABLATION STUDY

We assessed the system in five configurations: baseline PBFT, PBFT with HE only, PBFT with ZKP only, PBFT with HE + ZKP, and the whole framework, to determine the contribution of each component. The findings demonstrate that while batching and lightweight symmetric encryption enhance latency and throughput, HE and ZKP considerably lower privacy leaks and attack success rates. The ablation results in Table 7 show that eliminating any significant component causes a discernible decline in either security or performance, even if each component contributes in a different way. As a result, every element in the suggested design is justified, even if the study also identifies possible trade-offs for implementation in settings with limited resources.

Table 7. Ablation study of any major component of the proposed privacy preserving consensus framework

Configuration	Privacy Leakage	Attack Success Rate	Latency	Throughput
Baseline PBFT	20%	10%	100 ms	800 tx/s
PBFT + HE	5%	9%	95 ms	820 tx/s
PBFT + ZKP	2%	7%	98 ms	810 tx/s
PBFT + HE + ZKP	0%	2%	75 ms	980 tx/s
Full Framework	**0%**	**1%**	**70 ms**	**1000 tx/s**

9. CONCLUSIONS

The paper presented an improved privacy-preserving consensus framework, which forms the basis for securing the East-West interface in a distributed SDN architecture. Moreover, it is distinctive for being a robust and efficient consensus that is capable of dealing with all the key issues related to privacy, security, and efficiency apart from ensuring state-of-the-art cryptographic building blocks like HE and ZKP protocols. Experimental analysis is given for validating the effectiveness of this framework for achieving substantial improvement over the existing approaches, like PBFT and Raft. Specifically, this approach entirely removes the issue of privacy leakage and reduces the attack success rate by 90% and latency by 30%, as well as boosting the throughput by 25%. This would not only improve the security of distributed SDNs but would also ensure high efficiency for making the framework feasible for dynamic environments. This new framework provides the redefined paradigm for East-West interface security. Hence, the all-encompassing security framework protects sensitive data and gives a trusted assurance for the SDN distributed environment. In this respect, the extent of the task to be completed would be achieved through discussions on extension studies involving the integration of this approach with machine learning-based threat detection and ultra-large SDN. Concerning this book, it is hoped that it could inspire more research activities in this area of study with respect to the development of safe and efficient network architectures.

REFERENCES

[1] Prajapati, A., Sakadasariya, A., Patel, J. (2018). Software defined network: Future of networking. In 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, pp. 1351-1354. https://doi.org/10.1109/ICISC.2018.8399028

[2] Mokhtar, H., Di, X.Q., Zhou, Y., Hassan, A., Ma, Z.Y., Musa, S. (2021). Multiple-level threshold load balancing in distributed SDN controllers. Computer Networks, 198: 108369. https://doi.org/10.1016/j.comnet.2021.108369

[3] Midha, S., Tripathi, K. (2021). Extended security in heterogeneous distributed SDN architecture. In Lecture Notes in Electrical Engineering, pp. 991-1002. https://doi.org/10.1007/978-981-15-5341-7_75

[4] Vizarreta, P., Trivedi, K., Mendiratta, V., Kellerer, W., Mas-Machuca, C. (2020). DASON: Dependability assessment framework for imperfect distributed SDN implementations. IEEE Transactions on Network and Service Management, 17(2): 652-667. https://doi.org/10.1109/TNSM.2020.2973925

[5] Li, M.Z., Wang, X.D., Tong, H.J., Liu, T., Tian, Y. (2019). SPARC: Towards a scalable distributed control plane architecture for protocol-oblivious SDN networks. In 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, pp. 1-9. https://doi.org/10.1109/ICCCN.2019.8846931

[6] Beiruti, M.A., Ganjali, Y. (2020). Load migration in distributed SDN controllers. In NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, pp. 1-9. https://doi.org/10.1109/NOMS47738.2020.9110292

[7] Li, Z.Y., Hu, Y.X., Hu, T., Wei, P. (2019). Dynamic SDN controller association mechanism based on flow characteristics. IEEE Access, 7: 92661-92671. https://doi.org/10.1109/ACCESS.2019.2927173

[8] Khan, Z.A., Namin, A.S. (2022). A survey of DDOS attack detection techniques for IoT systems using blockchain technology. Electronics, 11(23): 3892. https://doi.org/10.3390/electronics11233892

[9] Hoang, N.T., Nguyen, H.N., Tran, H.A., Souihi, S. (2022). A novel adaptive East–West interface for a heterogeneous and distributed SDN network. Electronics, 11(7): 975. https://doi.org/10.3390/electronics11070975

[10] Nguyen, H.N., Souihi, S., Tran, H.A., Fowler, S. (2022). A blockchain-based SDN east/west interface. In GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, pp. 5759-5764. https://doi.org/10.1109/GLOBECOM48099.2022.10001381

[11] Almadani, B., Beg, A., Mahmoud, A. (2021). DSF: A distributed SDN control plane framework for the east/west interface. IEEE Access, 9: 26735-26754. https://doi.org/10.1109/ACCESS.2021.3057690

[12] Alrashede, H., Eassa, F., Marish Ali, A., Albalwy, F., Aljihani, H. (2024). A blockchain-based security framework for East-West interface of SDN. Electronics, 13(19): 3799. https://doi.org/10.3390/electronics13193799

[13] Lam, J., Lee, S.G., Lee, H.J., Oktian, Y.E. (2016). Securing SDN southbound and data plane communication with IBC. Mobile Information Systems, 2016(1): 1708970. https://doi.org/10.1155/2016/1708970

[14] Wang, M., Simon, G., Anet Neto, L., Amigo, I., Nuaymi, L., Chanclou, P. (2022). SDN East–West cooperation in a converged fixed-mobile optical access network: Enabling 5G slicing capabilities. Journal of Optical Communications and Networking, 14(7): 540-549. https://doi.org/10.1364/JOCN.460300

[15] Benamrane, F., Ben mamoun, M., Benaini, R. (2017). An East-West interface for distributed SDN control plane: Implementation and evaluation. Computers & Electrical Engineering, 57: 162-175. https://doi.org/10.1016/j.compeleceng.2016.09.012

[16] Adedokun, E.A., Adekale, A. (2019). Development of a modified East-West interface for distributed control plane network. Arid Zone Journal of Engineering, Technology and Environment, 15(Spi2): 242-252. https://www.azojete.com.ng/index.php/azojete/article/view/32.

[17] Sood, K., Karmakar, K.K., Yu, S., Varadharajan, V., Pokhrel, S.R., Xiang, Y. (2019). Alleviating heterogeneity in SDN-IoT networks to maintain QoS and enhance security. IEEE Internet of Things Journal, 7(7): 5964-5975. https://doi.org/10.1109/JIOT.2019.2959025

[18] Moeyersons, J., Maenhaut, P.J., Turck, F., Volckaert, B. (2020). Pluggable SDN framework for managing heterogeneous SDN networks. International Journal of Network Management, 30(2): e2087. https://doi.org/10.1002/nem.2087

[19] Prasad, J.R., Bendale, S.P., Prasad, R.S. (2021). Semantic Internet of Things (IoT) interoperability using Software Defined Network (SDN) and Network Function Virtualization (NFV). In Semantic IoT: Theory and Applications. Studies in Computational Intelligence, pp. 399-415. https://doi.org/10.1007/978-3-030-64619-6_18

[20] Brockelsby, W., Dutta, R. (2021). Traffic analysis in support of hybrid SDN campus architectures for enhanced cybersecurity. In 2021 24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, pp. 41-48. https://doi.org/10.1109/ICIN51074.2021.9385530

[21] Pisharody, S., Natarajan, J., Chowdhary, A., Alshalan, A., Huang, D. (2019). Brew: A security policy analysis framework for distributed SDN-based cloud environments. IEEE Transactions on Dependable and Secure Computing, 16(6): 1011-1025. https://doi.org/10.1109/TDSC.2017.2726066

[22] Gerola, M., Lucrezia, F., Santuari, M., Salvadori, E., Ventre, P.L., Salsano, S. (2016). ICONA: A peer-to-peer approach for software defined wide area networks using ONOS. In 2016 Fifth European Workshop on Software-Defined Networks (EWSDN), Den Haag, Netherlands, pp. 37-42. https://doi.org/10.1109/EWSDN.2016.12

[23] Alrashede, H., Eassa, F., Marish, A. (2025). Security of east-west interface of SDN: A review of challenges, solutions, and future directions. Engineering, Technology & Applied Science Research, 15(3): 23376-23385. https://doi.org/10.48084/etasr.10988

[24] Yu, H.S., Qi, H., Li, K.Q. (2020). WECAN: An efficient west–east control associated network for large-scale SDN systems. Mobile Networks and Applications, 25: 114-124. https://doi.org/10.1007/s11036-018-1194-9

[25] Munjal, K., Bhatia, R. (2023). A systematic review of homomorphic encryption and its contributions in healthcare industry. Complex & Intelligent Systems, 9: 3759-3786. https://doi.org/10.1007/s40747-022-00756-z

[26] Acar, A., Aksu, H., Uluagac, A.S., Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys, 51(4): 1-35. https://doi.org/10.1145/3214303

[27] Anthoniraj, S., Mishra, R., Loonkar, S., Agarwal, T., Ahluwalia, G., Gill, A. (2024). Design of novel cryptographic model using zero-knowledge proof structure for cyber security applications. Journal of Cybersecurity & Information Management, 14(1). https://doi.org/10.54216/JCIM.140110

[28] Tang, X.Y., Shi, L.Z., Wang, X., Charbonnet, K., Tang, S.X., Sun, S.X. (2024). Zero-knowledge proof vulnerability analysis and security auditing. Cryptology ePrint Archive. https://eprint.iacr.org/2024/514.pdf.

[29] Oleiwi, W.K., Abdullah, A.A. (2024). Performance evaluation comparison between central SDN network and DSDN. In New Trends in Information and Communications Technology Applications. NTICT 2023. Communications in Computer and Information Science, pp. 334-345. https://doi.org/10.1007/978-3-031-62814-6_24

[30] Oleiwi, W.K., Abdullah, A.A. (2024). Virtual environment testbed for DSDN network. In Lecture Notes in Networks and Systems, pp. 393-405. https://doi.org/10.1007/978-981-97-3466-5_29