CHAPTER 2

Literature Review

While SDN offers numerous benefits, its architecture also introduces new security challenges. Researchers have been actively exploring over the past decade towards securing the SDN networks. Several survey papers have been instrumental in outlining the security landscape of SDN, categorizing threats, and identifying potential research gaps. A foundational survey by Kreutz *et al.* [51] offers a comprehensive overview of SDN security challenges, categorizing them into threats to the data plane, control plane, and application plane. The study also points out that while SDN allows for easier deployment of security applications, it also necessitates robust security mechanisms to safeguard the controller and the data plane from being compromised by malicious clients.

2.1 Traditional OpenFlow rule integrity without blockchain

Giotis *et al.* [32] proposed a method that combines both the OpenFlow and sFLow to detect and mitigate anomalies in the SDN environment. In this method, sFlow is responsible for collecting statistics from the network components. However, their method often suffers from high costs and processing time due to heavy traffic loads. Another approach was introduced in [76], which involves maintaining a Global Flow Table (GFT) for the entire network. This approach computes the path for each flow and enables efficient searching for specific flows within the GFT, reducing the burden of suspicious flows. Similarly, Sasaki *et al.* [84] presented SDNSec, a solution based on symmetric-key cryptography to preserve the integrity of forwarding rules. Kurshid *et al.* [52] proposed VeriFlow, which acts as a tool to rigorously check for malicious OpenFlow rules installed at forwarding devices. These approaches focus on detecting malicious flow rules but may face scalability challenges when the network undergoes frequent changes. Kataoka *et al.* [49] maintained a trust list of IoT stakeholders to verify device authenticity, but relying on a central Trust List may present limitations.

In the past decades, researchers have been working in this direction to mitigate the DDoS attack [63, 58]. Ran *et al.* [78] proposed a solution based on confusable instance analysis by classifying the instances either into attack or not easy to distinguishable. Their method can reduce the number of abnormal instances. Another work is presented by Sayed *et al.* [85] that uses the Deep Learning method to detect the DDoS attack. Their method could reduce the false alarm rate. However, the result shows a degradation in the controller performance.

2.2 Blockchain in SDN Security

In recent years, blockchain technology has emerged as a promising solution for addressing some of the security challenges in SDN [67]. Characteristics of blockchain such as decentralized and immutable ledger can be leveraged to enhance the security of flow rule management, provide tamper-proof records of network transactions, and enable secure and transparent authentication processes. By integrating blockchain technology into SDN networks, it is possible to create a more secure and resilient network infrastructure. Blockchain can be used to ensure that flow rules are not tampered with, that control plane operations are transparent and auditable, and that user and device authentication processes are robust and trustworthy. As distributed networks are gaining popularity, efforts are being made by researchers to adopt Blockchain Technology for securing SDN-enabled networks. Blockchain has been widely adopted in various fields [54, 13, 100, 81, 64]. Blockchain has been effectively used in the field of IoT to preserve the privacy of IoT devices and data-sharing schemes [29]. In the healthcare sector, researchers are utilizing blockchain to preserve the privacy of patients and maintain electronic medical records (EMR) in the block.

2.2.1 Blockchain based solutions

In recent times, the utilization of blockchain technology has gained significant attention as an effective means to enhance the security of SDN networks and protect against flow modification attacks. Boukria *et al.* [17] proposed a blockchain-based trusted node acting as a firewall to retrieve flow information from forwarding elements and validate flow rules, but it lacks the validation of malicious flow rules. Bose *et al.* [16] introduced BlockSDSec, a virtual controller-based approach that detects malicious flows on forwarding elements by communicating with a blockchain network. Hu *et al.* [38] used Blockchain-as-a-Service (BaaS) to verify and insert flow rules on OpenFlow switches, primarily focusing on implementing a reward scheme for the verifier.

Weichen *et al.* [101] addressed the problem with a different approach by introducing a voting scheme to check whether the flow rule has been tampered with. Krishnamohan *et al.* [53] introduced BlockFlow and used the concept of switch version number to detect changes in the forwarding rules. However, their method is not economically well suited for a large network as the transaction cost will be higher due to the re-installation of flow rules.

2.2.2 Multicontroller architecture solutions

Janani and Ramamoorthy *et al.* [44] use multi-controller architecture to manage the false data injection on the IoT network. Each controller maintains one domain and the redundant controllers evaluate the network modifications. Rahman *et al.* [77] presented SmartBlockSDN, a robust mechanism to secure network communication by identifying and isolating the infected switches with optimized energy consumption. Sharma *et al.* [89] uses distributed SDN architecture (DistBlockNet) for IoT networks. They employ a distributed Blockchain network and a version number mechanism on flow tables to verify any changes made. However, this approach may suffer from high flow table update times if the response node has a low version. The work in [3] proposed a blockchain-based framework to secure SDN controllers and forwarding devices by recording on a distributed ledger, providing a tamper-resistant audit trail.

2.2.3 Multi-domain SDN solutions

As SDN has been increasingly adopted across multiple domains, the security of flow modification requests has emerged as a critical concern. To tackle these security challenges, researchers have investigated a variety of solutions, including conventional network security measures, sophisticated cryptographic methods, and the application of blockchain technology [28, 42, 57]. Multi-domain SDN introduces additional complexities, such as the need for inter-domain trust, the potential for cross-domain attacks, and the difficulty of achieving consensus across diverse and potentially heterogeneous controllers. The work presented in [68] integrates the Ethereum Smart Contract to enhance the automation of access control in a multi-SDN environment. Another work is presented in [8] that uses a concept called digit-coin to provide permission to the controller to perform the task. This digit-coin value is updated if the controller is found to be compromised to avoid participation in the consensus. The authors in [101] proposed a security scheme to preserve forwarding rule integrity through the voting process. They allow 1/3 of the nodes to be compromised for the completion of voting. However, their scheme is limited to small networks.

Recent studies have begun to address these challenges by proposing more sophisticated trust models and incorporating adaptive security mechanisms. For example, in [6] proposed a trust-based framework for SDN that creates trust between the controller and the network application based on Subjective Logic Reasoning (SLR). Similarly, the work in [22] explored the use of a reputation mechanism on controllers to separate the malicious nodes.

2.2.4 Authentication solutions

Authentication is an essential part of any secure system. The conventional forms of authentication, such as those relying on passwords, two-factor authentication, and Public Key Infrastructure (PKI), are reliant on a central server, which could become a failure point for the entire system [10]. Recently, Blockchain-based solutions have been adopted by many researchers. Li *et al.* [55] designed an authentication and data protection mechanism where the identity of the devices is registered on the blockchain. They perform the data integrity by checking the hash value with the root hash. A decentralized authentication scheme (DecAuth) is presented in [66] to identify the devices using Ethereum Blockchain. However, due to the use of a public blockchain, the system requires a longer time to reach a consensus. Ali *et al.* [5] presented a cross-domain authentication for an IoT network where it uses the recent concept of Blockchain SC. Shashidhara *et al.* [90] introduced a decentralized authentication scheme using blockchain to ensure the safety of the network. Another user authentication mechanism is presented in Khan and Nanda *et al.* [50] known as HetNet for SDN-5G network. Blockchain stores the hashed flow rules and user credentials.

With the development of SC, token-based authentication is increasing nowadays as it eliminates the need for a central authority to manage and secure user data. The SC allows the creation of digital tokens which can be used to authenticate the users in the network. The work presented in [74] utilizes the ERC tokens to authenticate users in the smart home. The token encapsulates the user's access right information for the IoT devices. Dewangan *et al.* [23] presented work on token-based access control to patient data.

Table 2.1: Summary of works presented in literature for OpenFlow rule security in Software-Defined Network

Ref.	**Year**	**Work**	**Method**	**Mitigation**	**Limitation**
[52]	2012	VeriFlow	State management	Flow installation	Undergoes frequent changes
[32]	2013	sFlow	Entropy Based Detection	Anomaly Mitigation	Suffers from high cost and processing time
[84]	2016	SDNSec	Symmetric-key cryptography	False rule injection	Key management issue
[76]	2017	GFT	Global Flow table	False rule injection	Accessing a large flow table is troublesome
[49]	2018	TrustList	Central Trust List	False rule injection	Single point of failure
[53]	2020	BlockFlow	Flow checking	DDoS attack	Limited attack detection
[22]	2021	BMC-SDN	Reputation mechanism	False rule injection	No dynamic policy
[101]	2021	FRChain	Voting mechanism	Modification	Limited scalability
[8]	2024	BCS	DigitCoin	False injection, MITM	High computation
[62]	2024	B2-C2	Digital signature	Rogue devices	Small networks
[91]	2024	SecureFlow	Data driven ensemble	IDS	High overhead
[79]	2024	P4-SDN	Fuzzy rule based	Malicious switch	Limited attack detection
[93]	2024	FTODefender	Classification model	Overflow attack	High latency
[9]	2024	FedSec	Federated learning	DDoS	Single domain work

We present a summary of the literature review in Table 2.1 regarding the OpenFlow rule security using blockchain highlighting the major limitations in their work. In summary, many works have been proposed in the literature using different approaches. However, these solutions possess a few pitfalls to satisfy the performance requirements for SDN applications. These solutions further lack preventive measures after the detection of the attack and deployment of the actual SDN platform. Further, we observed that blockchain is used for the mere storage of flow rules. However, the distributed architecture of blockchain can also be used to improve the SDN controller security and make the network more agile. The transparency of blockchain allows the network peers to share the data without any trusted authority. Moreover, the data shared on the network can be traced back if any malicious activity is detected on the SDN network. Therefore, in this thesis, we take full advantage of blockchain to design a robust security system to protect the flow table from malicious attacks.

Therefore, in this thesis, we aim to address these gaps by proposing novel solutions for enhancing the security and resilience of SDN networks, with a particular focus on ensuring flow rule integrity, improving distributed controller coordination, and integrating blockchain for secure user and device authentication.