Abstract

Software-Defined Networking (SDN) has emerged as a transformative technology that decouples the control and data planes, enabling centralized network management, dynamic configuration, and improved efficiency. The key enabler of SDN is the OpenFlow protocol, which dictate how traffic should navigate through the network. The separation of control plane from the forwarding devices introduce significant flexibility and programmability, but it also brings a set of challenges that need to be addressed to ensure network security. Key challenges in SDN networks include maintaining flow rule integrity, mitigating the risk of a single point of failure, ensuring cross-domain flow integrity, and securely authenticating users within the network. Flow tables being one of the major component of SDN architecture, the attacker try to exploit the flow tables and maliciously modify the existing flow rules. This create a potential vulnerability where malicious actors can deceive security applications, leading to the installation of malicious flow rules on OpenFlow switches. Further, the centralized nature of the SDN control plane, where a single controller or a small set of controllers manage the entire network, introduces the risk of a single point of failure. Additionally, in large-scale networks, particularly those spanning multiple administrative domains, maintaining flow integrity across domain boundaries is a significant challenge as each domain may have its own policies, protocols, and security requirements. Further, an unauthorized access to the control plane could allow an attacker to manipulate flow rules and compromise the entire network.

In recent years, blockchain technology has emerged as a promising solution for addressing some of the security challenges in SDN. Their characteristics 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. Therefore, this thesis is aimed at enhancing the security and resilience of SDN through the integration of blockchain smart contracts. This thesis addresses these challenges through four key contributions.

First, we propose a blockchain-based mechanism to ensure the integrity of flow rules in OpenFlow switches, preventing unauthorized modifications and enhancing the security of SDN networks through a spcialized blockchain agent which performs continuous flow verification. Our threat model addresses three main risks: flow modification attacks, false flow insertion attacks, and flow deletion attacks. Using blockchain smart contracts, we streamline the flow verification process to protect against malicious alterations. The proposed model targets only the affected flow rules for reinstallation, thus significantly reduces both the verification delay and the associated overhead on the SDN controller. The performance analysis shows that the proposed method achieved significant reduction in execution time compared to BlockFlow [53], BlockSDSec [16], and FRChain [101] by 52.36%, 48.62%, and 35.67% respectively. Overall, our findings affirm that the proposed method offers a practical and effective solution for safeguarding against malicious manipulation of flow rules in single controller SDN network.

Second, we design a distributed controller architecture that mitigates the risk of single points of failure by implementing a consensus-based approach, where the failure of the master controller is determined only if more than one-third of controllers vote for it. This approach significantly enhances the fault tolerance and reliability of the SDN control plane. Further, the equal controllers perform a consensus process considering the response time and resource utilization of all equal controllers to appoint a new master controller. This architecture ensures increased resilience by incorporating a mechanism that dynamically selects the equal controller with optimal performance as a master controller in the event of failure. The experimental result shows that the proposed model significantly enhances the responsiveness of network service availability by providing a minimum update time compared to existing methods.

Third, we address the challenge of cross-domain flow integrity by developing a blockchain-based multi-stage proposal verification in multi-domain SDN networks, implemented through smart contracts. This method ensures that flow modification proposals undergo three security checks before a final decision is made (digital signature, selecting the non-rogue controllers, and voting consensus). Additionally, we introduced an adaptive policy enforcement mechanism designed to proactively address potential security threats by isolating infected network components and inserting proactive flow rules to mitigate threats before they escalate. The multi-stage security effectively detects and mitigates threats from rogue or malicious controllers. The experimental results validate the effectiveness of our approach in maintaining network stability, even in the face of attacks like DDoS, rogue controller activities, and replay attacks.

Finally, we introduce a blockchain-based authentication scheme using specialized tokens tailored for SDN-IoT networks, providing a scalable and secure method for managing user and device identities, ensuring that access permissions are verifiable and resistant to unauthorized access. These tokens, created by network peers, serve as identification for users or devices in subsequent system interactions. Smart contracts can revoke tokens upon unsuccessful authentication attempts to prevent attacks on the system. Experimental results indicate that the proposed system effectively resists tested attack scenarios, demonstrating a high level of security.

The findings of this thesis contribute to the advancement of secure SDN architectures, offering practical solutions that integrate blockchain technology to address the pressing challenges in modern network environments.