

Article

Blockchain-Based Control Plane Attack Detection Mechanisms for Multi-Controller Software-Defined Networks

Abrar Alkhamisi ^{1,*}, Iyad Katib ¹  and Seyed M. Buhari ² ¹ King Abdulaziz University, Jeddah 21589, Saudi Arabia; iakatib@kau.edu.sa² University Teknologi Brunei, Bandar Seri Begawan BE1410, Brunei; ismail.buhari@utb.edu.bn

* Correspondence: aalkhamisi0034@stu.kau.edu.sa

Abstract: A Multi-Controller Software-Defined Network (MC-SDN) is a revolutionary concept comprising multiple controllers and switches separated using programmable features, enhancing network availability, management, scalability, and performance. The MC-SDN is a potential choice for managing large, heterogeneous, complex industrial networks. Despite the rich operational flexibility of MC-SDN, it is imperative to protect the network deployment with proper protection against potential vulnerabilities that lead to misuse and malicious activities on the MC-SDN structure. The security holes in the MC-SDN structure significantly impact network survivability and performance efficiency. Hence, detecting MC-SDN security attacks is crucial to improving network performance. Accordingly, this work intended to design blockchain-based controller security (BCS) that exploits the advantages of immutable and distributed ledger technology among multiple controllers and securely manages the controller communications against various attacks. Thereby, it enables the controllers to maintain consistent network view and accurate flow tables among themselves and also neglects the controller failure issues. Finally, the experimental results of the proposed BCS approach demonstrated superior performance under various scenarios, such as attack detection, number of attackers, number of controllers, and number of compromised controllers, by applying different performance metrics.

Keywords: multi-controller; software defined networks; security attacks; blockchain technology; attack detection



Citation: Alkhamisi, A.; Katib, I.; Buhari, S.M. Blockchain-Based Control Plane Attack Detection Mechanisms for Multi-Controller Software-Defined Networks. *Electronics* **2024**, *13*, 2279. <https://doi.org/10.3390/electronics13122279>

Academic Editor: Zbigniew Kotulski

Received: 25 April 2024

Revised: 2 June 2024

Accepted: 6 June 2024

Published: 11 June 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In the digital world, MC-SDN is emerging as a promising network paradigm that offers flexibility to manage the network infrastructure by clearly decoupling the data and control planes and managing the set of switches in a domain with multiple controllers [1]. The robust MC-SDN design provides a powerful architecture that offers scalability, flexibility, and failure resilience, making it a potential choice for large and complex network environments [2]. In the MC-SDN structure, each controller is responsible for managing a domain [3]. The capabilities of MC-SDN controllers are criticized for network availability, performance, and scalability. Thus, enabling multiple controllers is imperative for managing large-scale networks to improve the abovementioned issues, even though it increases network complexity and management [4]. Albeit, owing to the decoupling of planes with multi-controller structure, the MC-SDN applications are increasing day by day, and it is vulnerable to several types of attacks, such as Denial-of-Service (DoS), Man-in-the-middle, Flooding, and False Injection. Thus, paying attention to technological vulnerability challenges is paramount to applying proper solution strategies that effectively protect practical MC-SDN-based deployments [5,6]. In MC-SDN deployment, the distributed controller design spans several controllers to achieve scalability and attack resiliency. In this context, a compromised controller may greatly enhance the risk level of multiple controllers and switches. Hence, detecting such a vulnerable controller is crucial to protect the MC-SDN performance against various security attacks.

Blockchain is a powerful technology that detects the different MC-SDN attacks and prevents the controllers and switches from poor performance activities. In general, blockchain-based security models are highly influential solutions used to establish secure communication among controllers with immutable ledger data with different consensus, even in the presence of attackers [7–9]. However, an ingenious attacker can manipulate the immutable ledgers by getting hash knowledge series using sophisticated methods. Therefore, it is crucial to rate the blockchain controllers with a reward system to optimize the attack detection efficiency.

Therefore, the main research goal of the proposed BCS is to utilize the advantages of key enabling technologies such as blockchain to improve the security level of MC-SDN against various attacks in the control plane.

The main contributions of the proposed work are given as follows:

- The primary intention of the work is to maximize the MC-SDN security and efficiency against various attacks by utilizing the blockchain;
- The BCS improves the consistency and communication security among multiple controllers by incorporating reshaped Practical Byzantine Fault Tolerance (rPBFT) with a digit-coin assignment system. The BCS can also determine the malicious controllers affected by flow injection and man-in-the-middle attacks by providing equal priority to the genuine miners, resulting in high MC-SDN security;
- Finally, the experimental results demonstrate the superiority of the proposed BCS through MiniNet simulation. The simulation results are obtained in terms of diverse performance metrics.

The remaining part of the paper is organized as follows. Section 2 surveys the works related to controller security models of SDN and MC-SDNs. A detailed description of BCS design is provided in Section 3. Section 4 explains BCS experimental evaluation. Section 5 demonstrates the results of BCS. Finally, Section 6 concludes the paper.

2. Related Works

Recently, several works have been developed to provide SDN security using blockchain technology and have listed the advantages and limitations of the SDN strategies, especially from the security perspective, including DoS and illegal intrusion attacks on SDN control nodes. In [10], the flow-based traffic forwarding approach analyzes the security issues and lists possible loopholes in the SDN-blockchain environment, such as spoofing attacks, DoS attacks, hijacking attacks, latency issues, and privacy issues. This section reviews SDN security provisioning via blockchain-technology-based SDN security models.

A comprehensive review of security architecture platforms using SDN and blockchain technology is provided in [11]. Moreover, this study discusses the influence of blockchain technologies in protecting and securing the SDN architecture from the perspective of integrity, confidentiality, security, and availability. Blockchain-based lightweight security architecture (Bloc-Sec) [12] applies the Blake-256 hashing algorithm to authenticate all the IoT devices in the blockchain server. It applies the cuttlefish optimization algorithm to select the optimal Virtual Network Function (VNF). It securely stores the hashed flow rules in the VNF by invoking blockchain technology. Finally, the Bloc-Sec architecture employs the spiking dual fuzzy neural networks to leverage the packet classification through the packet header and content inspections. Some of the secure SDN architecture is designed only with specific DoS attacks in SDN, but still lacks data integrity-related attacks [13,14].

The SDN controller is responsible for dividing the data and control plane and controlling the SDN network activities without knowing the underlying structure. However, detecting malicious nodes or devices and securing SDN communication is prominent because it is vulnerable to insider threats. A hybrid network architecture [15] leverages the advantages of SDN and blockchain technology for the smart city. It comprises two parts, the core and edge networks, which inherit the power of the centralized and distributed network architectures. Moreover, it ensures security and privacy by modeling the Proof-of-Work (PoW) scheme without compromising the efficiency of the security mechanism. Blockchain

applications in smart communities were briefly studied in [16], which discussed the various secure transaction process models, communication infrastructure, and applications. However, implementing blockchain technology across multiple controllers and enabling inter and intra-controller communication across controllers are still not effectively solved.

The framework proposed in [17] combines the advantages of trust management and blockchain technology. Trust management and blockchain technology estimate the trust value for each node and establish the communication without a trusted party, respectively. It helps in providing data integrity to the communication. However, it incurs communication delays and unnecessary energy consumption. In addition, the combined framework of trust and blockchain technology tends to a communication workload due to modeling the security mechanism on all the network nodes and enabling the storage of all the data flow entries. Most SDN approaches deploy a single controller to ensure security for SDN. If any problem occurs with a single controller, the overall functionality of the SDN is degraded.

Most of the attackers mainly target the functionalities of the controller. Therefore, the security of the controller plays an important role in the success of SDNs. To solve those issues, a security model using blockchain technology was suggested by [18], which attempts to maintain consistency among instances of the SDN controller. It also executes the Open DayLight controller operational flow. Many works have suggested utilizing the advantages of blockchain entirely for securing the SDN [17–19]. The work in [20] addresses the security and privacy constraints in the vehicular IoT environment and transportation system in SDN-enabled 5G-VANET. It presents the scheduling procedures in the blockchain-based security model. Designing the blockchain-based security framework ensures secure vehicular IoT services with the advantage of the immutable and decentralized characteristics of the blockchain. The main problem with blockchain-based SDN security schemes is the unnecessary delay in the overall functionality.

In a multi-controller SDN structure, it is crucial to maintain a consistent network view among all controllers for performance enhancement. To accomplish the aim, Smart Block-SDN [21] identifies and isolates the rogue switches to provide secure network communication, guaranteeing efficient cluster-head selection. Moreover, it maintains the consistent tracking of the flow rules in the switches within the controller cluster through its layered architecture. The blockchain-based security framework for NorthBound Interface (BC-NBI) in [22] utilizes blockchain security features and automatically verifies the credentials of the controller and application through token-based authentication. The work in [23] presents a novel secure blockchain-enabled multi-controller Rule Enforcement Verification (BlockREV) for SDNs. It exploits the blockchain architecture to verify rule enforcements over a multi-controller blockchain environment. It ensures correctness in cross-domain forwarding of multi-controllers in SDN. It uses the most significant cryptographic primitives and address-based signature aggregation model to perform rule enforcement verification. Consequently, the work in [24] presents an Intelligent blockchain-based SDN (IB-SDN) security architecture to attain a global trust model among multiple domain controllers. Hence, the controllers upload the topological abstractions to the blockchain and manage it through smart contracts.

The design of lightweight blockchain architecture secures the application controller interface and prevents malicious activities with reduced packet overhead and processing time. The work in [25] presents a blockchain-enabled SDN framework to secure transactions that uses SDN and Network Function Virtualization against man-in-the-middle attacks. Albeit, the lightweight blockchain security models are prone to ingenious attack activities in massive heterogeneous SDN-based networks. The Blockchain-Based Multi Controller architecture for secure SDN (BMC-SDN) in [26] ensures security against multi-controller SDN control-plane attacks. Each SDN domain is managed by one master controller that communicates through blockchain with the masters of the other domains. The work in [27] includes blockchain-based architecture and intent-driven mechanisms to implement Intent-driven security SDNs (IS2N). Specifically, it presents a novel four-layer architecture of the IS2N with security capabilities. Furthermore, the work in [28] introduces blockchain-based

flow control consistency (B2-C2) for multi-controller SDNs. It incorporates blockchain and digital signatures into SDN infrastructure to assure consistency of flow control within MC-SDN. It can provide security against compromised controllers and switches, simultaneously maintaining a consistent network view among controllers. However, Ref. [28] failed to ensure entire network security.

Although the multi-controller-based SDN effectively overcomes the single point of failure issues, there are three major concerns, such as controller coordination, network view consistency, and security are still not addressed by the conventional multi-controller SDN strategies. Sudden changes in the controller state significantly impact the new configuration of flow tables at other controllers in the MC-SDN structure. Inconsistencies among multiple controllers can shrink the performance of the infrastructure layer routing process. Also, the decentralized nature of MC-SDNs is vulnerable to different types of security attacks, that are false injection, a man in the middle, and compromised controllers. Hence, efficient security is needed to improve the performance of multi-controller SDNs ultimately. The BMC-SDN [26] effectively addresses the issues mentioned above by employing blockchain technology among the redundant controllers in a domain. However, in a scenario where multiple controllers are compromised, relying only on the monitored data from redundant controllers within a domain is not sufficient for robust decision-making. Therefore, a novel security strategy is needed to solve the compromised controller effectively, and also inconsistent network view problems. The main objective of the BCS is to ensure high security against such attacks when multiple controllers are compromised through blockchain's advantage in both inter and intra controllers while maintaining the flow consistency at each controller. Table 1 compares various blockchain-enabled SDN security solutions with their limitations.

Table 1. Comparison of blockchain-based SDN security models.

Ref.	Work	Controller	Algorithms	Limitations
[18]	Security model using blockchain technology	Single	Secure hashing	High Delay and not suitable for controller-compromised attacks
[21]	Smartblock-SDN	single	Clustering and distributed flow verification	Not suitable for real-world large-sized networks
[22]	BCNBI	Single	Fine-grained access control with trust evaluation	Not adaptable to distributed controller environment
[23]	BlockREV	Multi	The address-based aggregate signature scheme	High computation cost and high overhead
[24]	IB-SDN	Multi	Local and Global Reputation, voting mechanism	High complexity and not suitable for a compromised controller environment
[25]	Blockchain-enabled SDN Framework	Single	Controller authentication strategy	Lacks to ensure entire network security
[26]	BMC-SDN	Multi	Reputation mechanism	Accomplish poor performance in more than one compromised controller
[27]	IS2N	Multi	Security store network-level snapshots	High complexity
[28]	B2-C2	Multi	Blockchain and digital signature	High computation cost and high overhead

3. The Proposed Work

Although the conventional works utilize the MC-SDN structure to handle the single point of failure issues effectively, they may suffer due to inconsistent network view and district security attacks. Notably, when multiple numbers of controllers are compromised, there is a chance that an attacker can control a specific domain, which is a more serious problem in the MC-SDN structure. The existing BMC-SDN utilizes a redundant

controller structure with a blockchain advantage to solve such issues [26]. However, if an attacker compromises both the main and redundant controller of a domain to enhance its attack capabilities, the security of the entire network will be compromised. There is no effective existing solution, including BMC-SDN, to address multiple numbers of compromised controllers within a domain. Hence, it is crucial for a novel security solution to determine MC-SDN attacks even if the controllers of a domain have been compromised while maintaining a consistent network at each controller. Therefore, the proposed BCS aims to determine multiple MC-SDN security attacks with blockchain technologies under compromised controllers of a single domain. The features of blockchain technology make it a promising security strategy without sacrificing the performance level. The security design of BCS is shown in Figure 1. The BCS protects the controller communication against false injection, man-in-the-middle, and controller compromise attacks by enabling blockchain-based digital reputation.

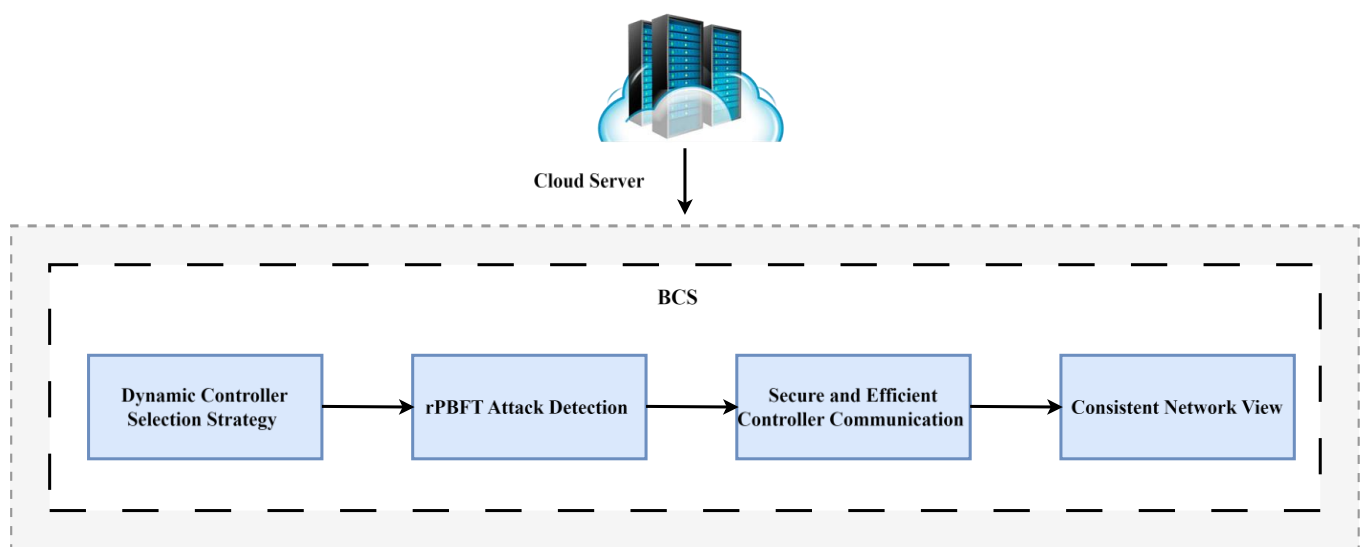


Figure 1. Overview of proposed BCS.

In this type, the BCS assigns the most suitable intra and inter-controllers to the main controller based on the digital reputation value estimated based on the sub-controller local reputation and blockchain history-based reputation. The tamper-resistance property of blockchain significantly improves the security and intra and inter-controller communication efficiency of MC-SDN against compromise, false-injection, and man-in-the-middle attacks. The BCS estimates a reputation value for the available controllers in the intra and inter-controller domain and selects the most suitable sub-controllers to monitor the behaviors of the main controller. As described in work [26], the proposed BCS constructs the multi-controller architecture. The proposed BCS differs from BMC-SDN [26] by assigning inter and intra-redundant controllers to the main controller. Thus, it effectively handles the main controller failure issues without increasing the burden of redundant controllers and cost. In the proposed BCS, the same sub-domain has multiple controllers that are not always active. Hence, only one main controller is active at a time, and the others only monitor the main controller activity at the same time. The main controller role is rotated among the intra-sub controllers based on network traffic over a particular period to handle the massive network data efficiently.

3.1. Control Plane Attack Model

Different types of threats are possible in a multi-controller SDN environment. The false injection, man-in-the-middle, and DoS are prominent as they damage the entire controller performance. For instance, any change in the state controller significantly affects

the performance of other controllers, resulting in inconsistent network view and SDN failures. The attack model for the MC-SDN control layer is shown in Figure 2.

- **False Injection:** An attacker spoofs the communication model of the controllers and injects false flow data, aiming to reduce the performance of the controller;
- **Man-in-the-Middle:** Attackers secretly intercept and relay the controller communications by exploiting any one of the methods. It leads to routing errors and creates routing loops, firewall leakages, and ineffective routing decisions;
- **Compromised Controllers:** An attacker compromises the controllers to obtain different topological views.

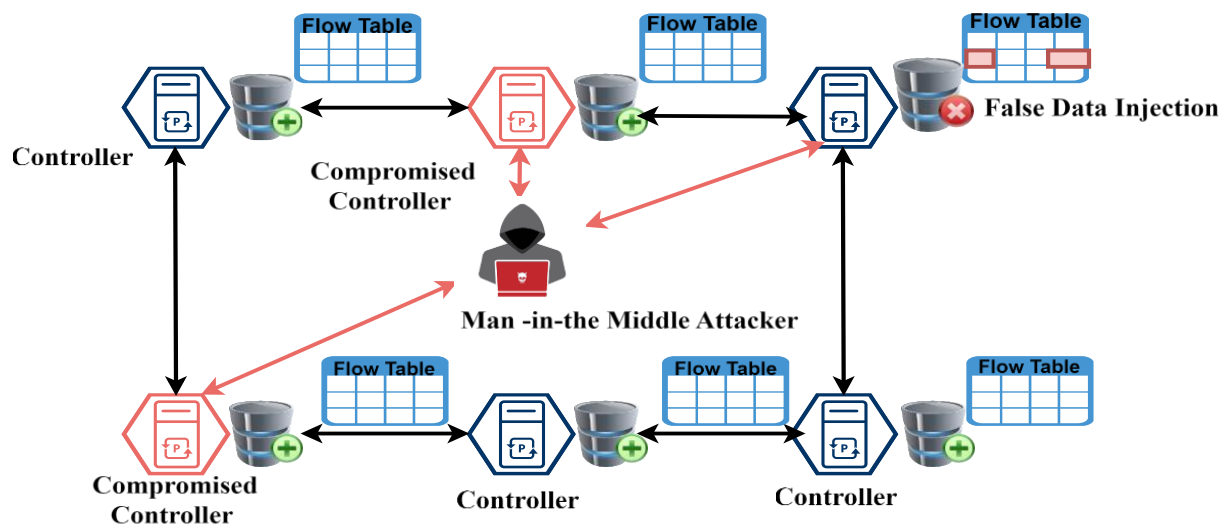


Figure 2. Attack model for the MC-SDN control layer.

3.2. Blockchain-Based Controller Security

The multi-controller SDN comprises several controllers that can work together to efficiently manage the traffic flow with a consistent network view over large-scale dynamic networks [26]. Sudden changes in the controller states should affect the performance of the new configuration flow of other controllers in the network, resulting in poor network performance. Also, the multi-controller SDNs are vulnerable to attacks such as false injection, a man in the middle, and compromised controllers. Thus, it ultimately impacts the entire performance of multi-controller SDN. Hence, efficient security is needed to protect the controllers against attacks and single-controller failure. Blockchain technology has proved as a promising security solution to mitigate MC-SDN security attacks, especially man-in-the-middle. Thus, it ultimately impacts the performance of multi-controller SDN. Detecting and mitigating the effects of attacks in an MC-SDN environment is crucial to maintaining the security and integrity of the multiple controllers. Also, efficient security is needed to protect the controllers against attacks and single-controller failure. To rectify the abovementioned issues and improve the security of multi-controller SDNs, this work intends to present a blockchain-enabled control plane security strategy named BCS. The main intention of the proposed BCS is to deliver distributed decentralized attack detection, providing strong security against multi-controller SDN systems by integrating the advantages of blockchain technology. The BCS design is explained in the following Figure 3, and it includes three mechanisms for the security of the multi-controller communication, the proposed model considers the work in [26] as a base model. Instead of assigning redundant controllers from the available controllers such as [26], the proposed BCS includes two redundant sub-controllers to the corresponding domain. Thus, it effectively handles the controller failure issues due to high load and optimizes the resource consumption among the controller without increasing the overhead.

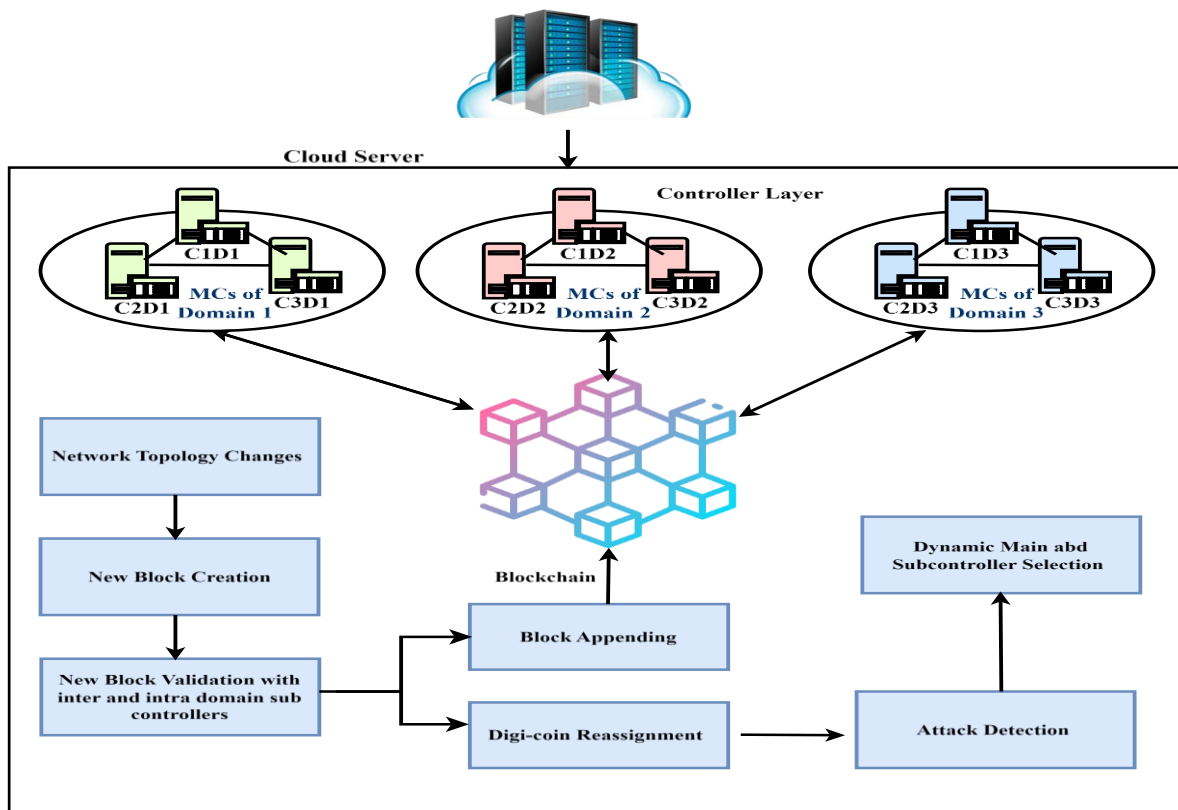


Figure 3. Design process of BCS for MC-SDN.

The blockchain system in BCS can yield security to intra and inter-controller communications and assist in maintaining a consistent network view at all controllers. More precisely, the multiple controllers in BCS architecture are becoming members of the blockchain network and establishing secure communication against attacks through the block creation and validation of immutable blockchain ledgers. The BCS includes three main mechanisms: digit-coin assignment, block validation with reputed rPBFT, and attack detection.

3.2.1. Digit-Coin Assignment in BCS

In a multi-controller SDN structure, the controllers establish communication whenever they observe changes in the network topology. In BCS, each controller receives digital coins based on the intra and inter-sub-controller monitoring data with blockchain after accomplishing topological changes. The BCS estimates the blockchain digit coins of main controllers, as demonstrated in Figure 4, with the assistance of the monitored data of both intra and inter-domain sub-controllers.

The BCS permits the nodes with high digit-coin to read and write the permissions of the proposed blockchain. During network initialization, each controller is considered a genuine node. After some rounds, the Genuity of the controllers is revised based on the digit-coin value. Thus, the proposed BCS can rectify the effects of compromised controllers in consensus participation. The main and sub-controllers of each domain are depicted in various colors. As shown in Figure 4, the controller C1D2 incurs flow changes and needs to update the corresponding changes to the main controllers C1D1 and C1D3 of other domains. Therefore, it inaugurates the digit-coin assignment system in which the monitored data of intra and inter-controllers are jointly considered with the blockchain historical data. The digit-coin system estimates the digit-coin of C1D2 (DC_{C1D2}) using Equation (1).

$$DC_{C1D2} = (\alpha \times (D_{C2D2} + D_{C3D2}))(\beta \times (D_{C1D1} + D_{C1D3}))(\gamma \times D_B) \quad (1)$$

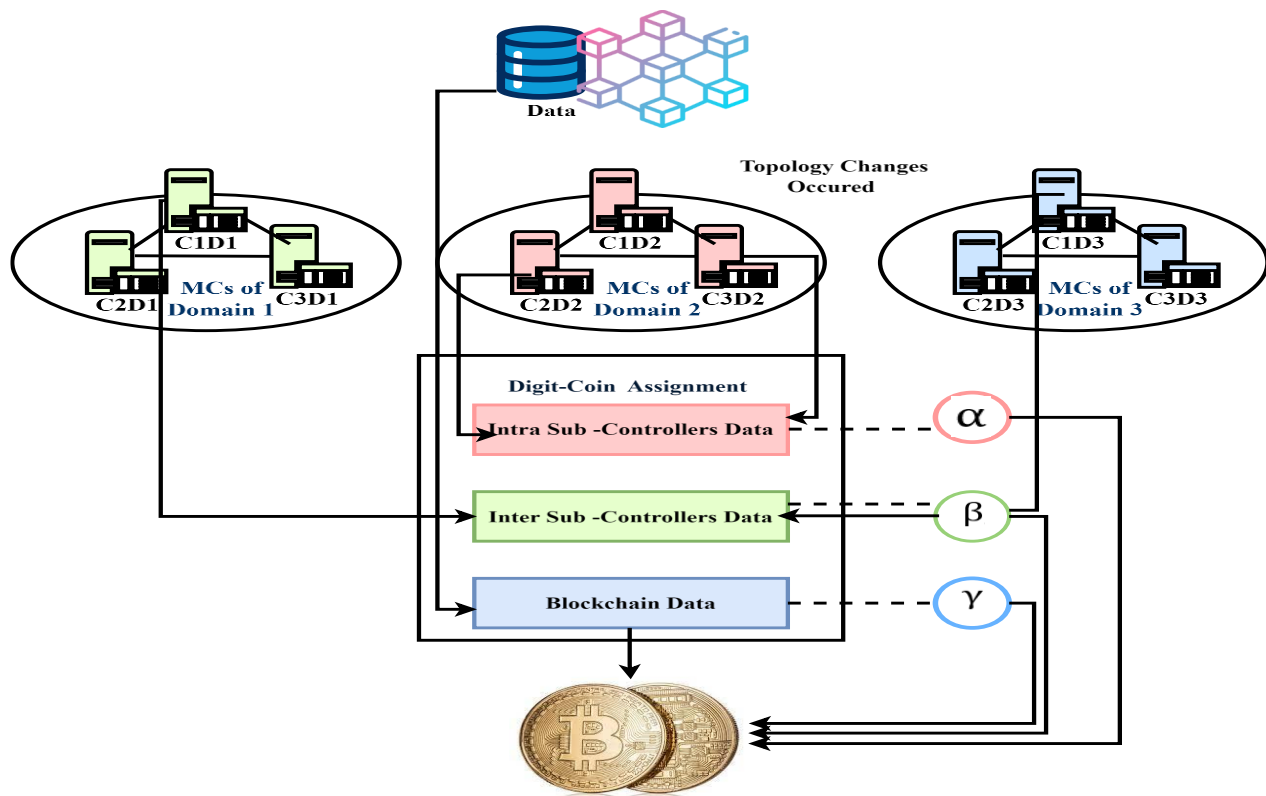


Figure 4. Digit-coin assignment of BCS.

In Equation (1), the factors α , β , and γ are weighting values of intra-sub-controller locally observed data. $(D_{C2D2} + D_{C2D2})$, inter sub-controller locally observed data $(D_{C1D1} + D_{C1D3})$, and blockchain historical data (D_B) . The summation value of weighting factors α , β , and γ equals 1. The BCS assigns dynamic weighting values between 0 to 1 based on the behavior of the intra and inter-controllers in previous communications. Moreover, the BCS provides the DC_{C1D2} to rPBFT consensus to validate its newly created block. Consequently, the BCS initiates the block validation using the reputed rPBFT process. The digit-coin assignment process is explained in the following Algorithm 1.

Algorithm 1 Digit-Coin-Assignment Process.

```

1: Input: Contract balance in terms of digit-coin
2: Output: Assign digit coins to controllers
3: BCS do
4:     Initiate the digit-coin Assignment process
5:     Verifies the contract balance
6: if the Contract does not have sufficient balance then
7:     Insufficient balance
8: else
9:     Check the Controller Address
10:    if the Controller Address is not valid then
11:        Invalid Address
12:    else
13:        Valid Address
14:        Assign Digit-coins Successfully

```

3.2.2. Block Validation with Reputed rPBFT

In the proposed BCS, the intra and inter-domain sub-controllers perform the consensus. These controllers are called miners and are responsible for blocking validation before

appending. The proposed BCS exploits the permissioned blockchain model with rPBFT to accomplish secure communication with minimum consensus delay among the controllers. Compared with other blockchain models such as public and permissionless, the customized consensus property and use case flexibility of permissioned blockchain make it highly adaptable to the MC-SDN environment. Initially, the controllers obtain a local topology view from their corresponding domain. By considering the opinions of optimally selected sub-controllers in block validation, the BCS neglects the contributions of attacks such as false injection, man-in-the-middle, and controller compromise in block creation, resulting in high accuracy of network consistent view. The proposed rPBFT is highly fit for a permissioned blockchain environment, compared to conventional PBFT, PoW, and PoS consensus mechanisms, as it assures fairness in consensus by providing equal chances to all benign miners during block generation.

The rPBFT utilizes a digit-coin assignment system to accomplish consensus fairness in the network. The three-stage process of rPBFT is pre-prepare, prepare, and respond. Most existing PBFT voting mechanisms only consider agreement and disagreement, which is insufficient for a practical MC-SDN environment. Therefore, the rPBFT utilizes fuzzy sets to optimize the digit-coin assignment process [29]. The fuzzy sets refer to the MC-SDN as U , then map the U to the fuzzy set interval $[0, 1]$. The fuzzy set is denoted as S . The digit-coin values of the controllers involved in block generation are evaluated based on the local monitoring information updated by the sub-controllers. Hence, all communication is performed via blockchain, which comprises immutable ledger technology. The fuzzy score of the main controller FS_{C1D2} is estimated using Equation (2).

$$FS_{C1D2} = [H_{SC}(u), 1 - M_{SC}(u)] \quad (2)$$

In the above-shown equation, the terms $H_{SC}(u)$ and $M_{SC}(u)$ represents the honest score level and malicious score level of digit-coins of the controller FS_{C1D2} respectively. The consensus process of rPBFT is shown in Figure 5. By converting the monitor values of sub-controllers as digit-coin scores in controller block validation, the rPBFT maximizes the consensus efficiency and improves the security level of the control layer in the BCS model.

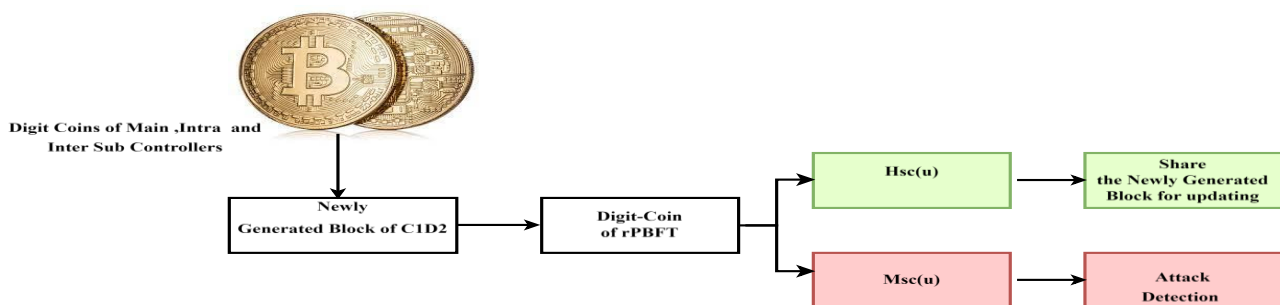


Figure 5. Digit-coin rPBFT consensus and block validation.

3.2.3. Attack Detection

The BCS determines the malicious controller based on the digit-coin and rPBFT consensus, referred to as additional security, as the blockchain offers fundamental security. The controller $C1D2$ can be in one of the following strategies, as shown in Equation (3).

$$C1D2 \sim \begin{cases} DC_{C1D2} \text{ and } FS_{C1D2} > 0.9, & C1D2 = \text{Honest} \\ DC_{C1D2} \text{ and } FS_{C1D2} \leq 0.9, & C1D2 = \text{Suspicious} \\ \text{Otherwise,} & C1D2 = \text{Malicious} \end{cases} \quad (3)$$

In the proposed BCS, the attack detection threshold of DC_{C1D2} and FS_{C1D2} are fixed between 0 to 1. As explained in Equation (3), the controller is honest when it obtains the digit-coin and consensus values DC_{C1D2} and FS_{C1D2} lies between 0.9 to 1. The controller

is considered suspicious when DC_{C1D2} and FS_{C1D2} lies between 0.5 to 0.9. Otherwise, the controller is compromised. Moreover, the BCS provides strong security against controller compromise through blockchain-enabled security. Algorithm 2 explains the process of BCS. The miners performed the validation process with rPBFT by determining the similarity between the data of the invalid block and its local data. Upon validation, the new block is appending with the chain, and the BCS distributes the newly created block to all controllers. By determining and eliminating the interaction of compromised controllers from block updating, the BCS neglects the effect of false injection and man-in-the-middle attacks. Moreover, it maintains a consistent network view at all controllers in BCS through efficient reputation and rPBFT block validation. Thus, it greatly impacts improving the security and performance efficiency of the MC-SDN data layer. By rotating the main controller role among the available sub-controllers in the corresponding domain, the proposed BCS enhances the controller utilization efficiency without impacting the security and performance of the network. Also, selecting intra and inter-domain sub-controllers for mining can minimize the controller failure issues due to high burden and optimize resource utilization.

Algorithm 2 Digital Reputation Estimation and Block Validation of BCS.

```

1: Input: Monitored information from C2D2, C3D2, C1D1, C1D3, and BN
2: Output: Digit-coin and Block validation
3: Main controller  $\leftarrow$  true
4: do while Main controller
5:     Generating new block according to topological changes
6:     BCS digit-coin system  $\leftarrow$  true
7:     do while BCS digit-coin system
8:         Initiates the digit-coin assignment process for C1D2
9:         Collects the monitored information from C2D2, C3D2, C1D1,
            C1D3, and BN
10:        Estimates the  $DCC1D2$  using Equation (2)
11:        Inputs the  $DCC1D2$  to rPBFT mining
12:        rPBFT  $\leftarrow$  true
13:        do while rPBFT
14:            Maps the  $DCC1D2$  as U sets
15:            Compute  $FSC1D2$  to main controller C1D2
16:            Obtain the honest and malicious score level using Equation (3)
17:            If ( $FSC1D2 > 0.9$  and  $FSC1D2 < 1$ )
18:                then C1D2 is trustworthy
19:            else if ( $FSC1D2$  lies between 0.5 to 0.9)
20:                then C1D2 is suspicious
21:            else if ( $FSC1D2 < 0.5$  and  $FSC1D2 > 0$ )
22:                then C1D2 is malicious
23:            end if
24:            rPBFT  $\leftarrow$  false
25:        end while
26:        BCS digit-coin system  $\leftarrow$  false
27:    end while
28:    Main controller  $\leftarrow$  false

```

4. Experimental Evaluation

The experimental model virtually creates the SDN in a simulated environment with the help of the Mininet emulator. There are two communication environments created using Mininet. Firstly, inter-controller communication is created to evaluate the performance of BCS. Ryu [30] is a Python-based OpenFlow virtual controller that bypasses the incoming network traffic over the connection with the SDN controller. Each domain has multiple controllers, enabling developers to manage, program, and control the applications through its interface. The controllers effectively maintain a consistent network view by enabling

blockchain-based communication environment creation. In the proposed model, a private blockchain assigns privileges to connect, send, and receive the flow information among the multi-controllers. In the simulated SDN, installed servers generate traffic flows across the multiple intermediate SDN switches. The configuration of the SDN devices or nodes relies on the applications executing on the Ryu controller through the OpenFlow. OpenFlow Ryu collects the statistical data from the SDN switches and devices. Hence, it is modeled as the firewall, switch, monitor, and router for the network traffic. The Ryu controller exploits the southbound Application Programming Interface (API) to establish the remote connection with Mininet, incorporating different hosts and switches. To design the processes involved in the proposed SDN research, the Ryu application development interface utilizes the Open vSwitch as the SDN switch for providing a switching stack for the virtualized environment. The proposed BCS approach is compared with existing IB-SDN [24] and BMC-SDN [26] to validate the effectiveness.

4.1. Implementation Parameters of BCS

The BCS security model is evaluated using Mininet, which creates virtual network support for implementation. The implementation parameters of BCS are shown in Table 2.

Table 2. Implementation parameters of BCS.

Parameters	Value
Simulator	MininetWiFi/PyEthereum
Type of SDN Controller	Ryu
Number of SDN Domain	5–20
Number of SDN main Controllers	5–20
Number of SDN Sub-Controllers	2 for each main controller
Blockchain Type	Permissioned Blockchain
Consensus Mechanism	Reshaped PBFT
Number of malicious Controllers	2 to 6
Type of SDN Nodes	OpenFlow Switches and Internet-enabled smart devices
Number of Switches	10 to 100
Number of SDN Nodes	10 to 500

The simulation environment creation is depicted in Figure 6.

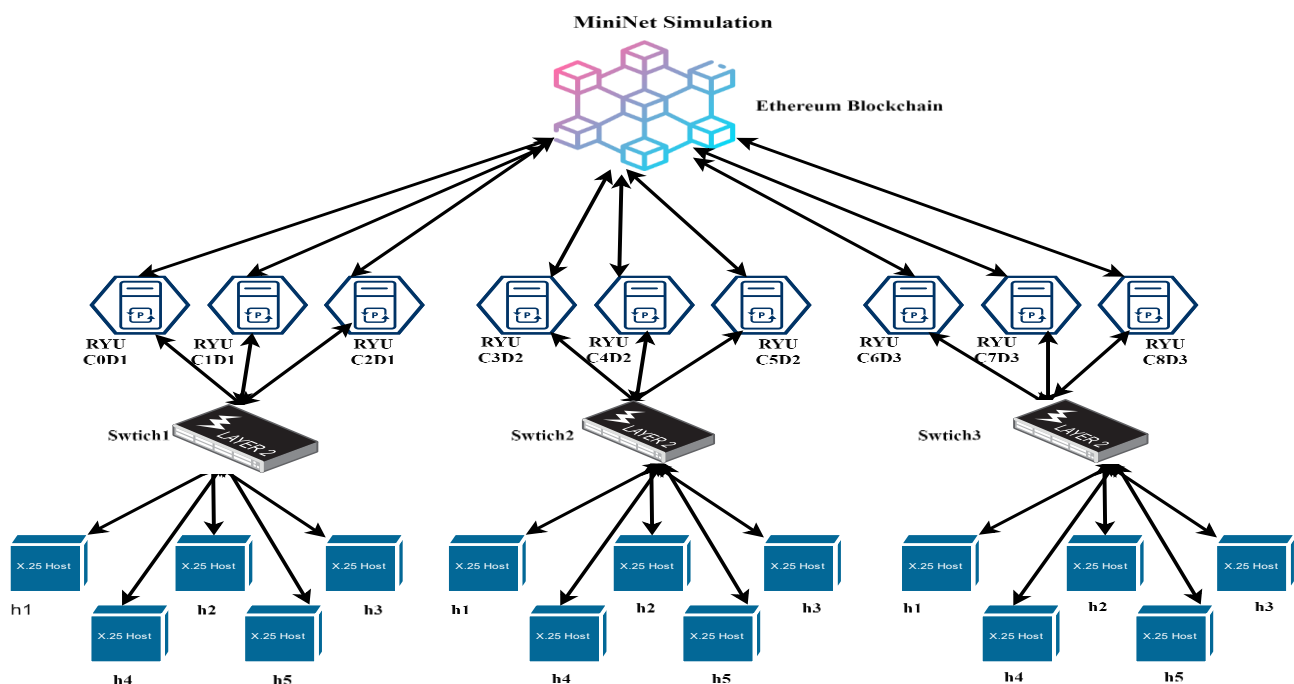


Figure 6. Simulation environment creation.

4.2. Performance Metrics

The performance of BCS is evaluated using the following metrics:

- Attack Detection Rate: The percentage of successfully detected attacks to the total number of injected attacks.
- Consensus Delay: The amount of time taken to reach a consensus.
- Detection Time: The amount of time required to detect malicious controllers.

5. Experimental Results of BCS

Figure 7a plots the relationship between the number of controllers and attack detection time for a compromised controller attack (CCA) attack scenario. The results are obtained for different controller scenarios, such as 10, 20, and 30. The attack detection rate is increased by adjusting the controller density from 10 to 30. The main reason is that the number of CCA escalated, varying the number of controllers from low to high. Albeit the BCS strategy provides a strong defense against the compromised controllers, most of the controllers are attackers under high controller scenarios. Hence, the digit-coin value estimation accuracy may diminish due to the high numbers of comprised controllers. For example, the BCS accomplishes 92.86% and 89.32% of the attack detection rate for 10 and 30 controllers.

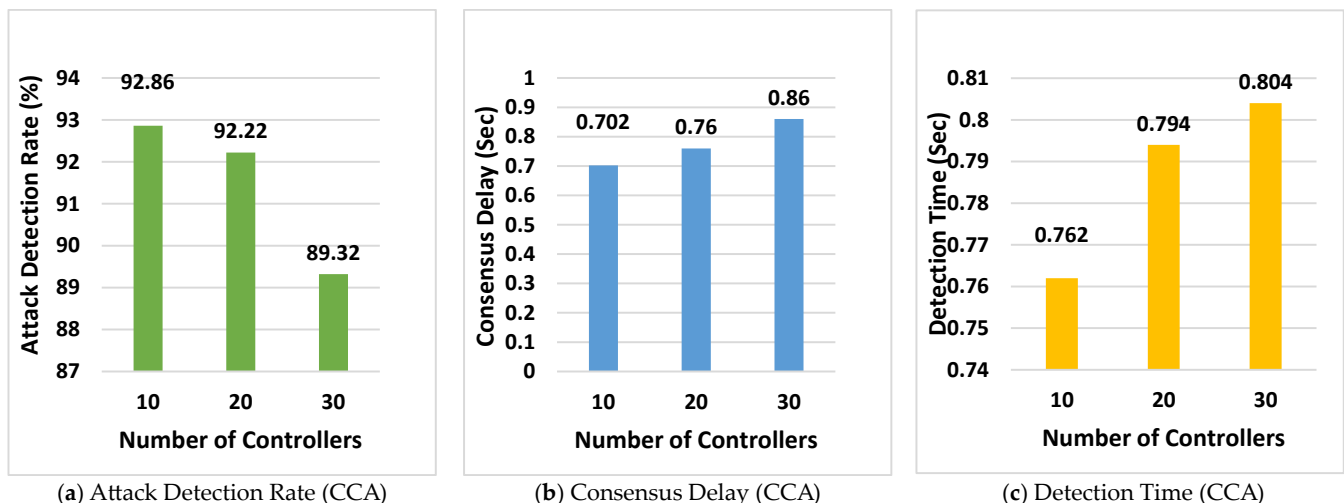


Figure 7. Compromised controller attack (CCA) performance metrics.

Figure 7b demonstrates the consensus delay results of the proposed BCS obtained for various controller scenarios with compromised controller attacks. The consensus delay escalates when the number of controllers varies from 10 to 30. The main reason is that many nodes compete to perform in the new block creation process, resulting in high consensus delay. Unlike fundamental PBFT, the proposed rPBFT provides an equal chance for miners to participate in consensus. For example, the consensus delay of the proposed BCS is 0.702 s for 10 controllers, and it varies by 0.86 for 30 controllers.

Figure 7c shows the relationship between the number of controllers and detection time for the CCA scenario. The BCS increases the detection time when varying the number of controllers from 10 to 30. This is caused because the percentage of CCA is high under 30 controller scenarios compared to 10 and 20 controller scenarios since the BCS needs adequate time to defend against the compromised controllers. For example, the BCS obtained 0.804 s of detection time for 30 controller scenarios.

Figure 8a illustrates the false injection attack (FIA) attack detection rate results of BCS obtained by varying the controller density from 10 to 30. The attack detection rate of BCS is decreased by varying the controller density from low to high. Under a low number of controller scenarios, the number of attackers is also minimal. Hence, the proposed model obtains accurate digit-coin values and quick rPBFT consensus. Thus, it improves the attack

detection rate compared to many attacker scenarios with more controllers. The increase in controllers also has an impact on the number of controllers. For instance, the proposed BCS incurs an 89.74% attack detection rate for 10 controllers. However, the proposed model minimizes the attack detection rate at a very low percentage by 2.16 under 30 controllers, compared with 10 controllers.

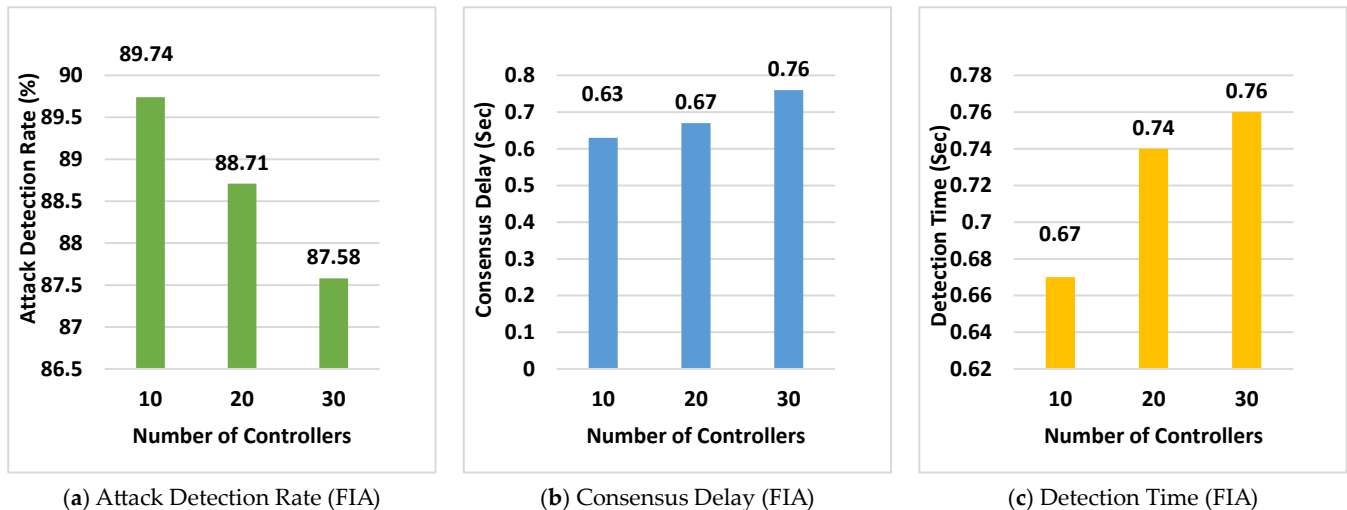


Figure 8. False injection attack (FIA) performance metrics.

Figure 8b compares the FIA consensus delay results of BCS obtained for the different number of controller scenarios. In the rPBFT, the consensus participation was decided according to the digit-coin value of nodes. The proposed model gives an equal chance to all the participants in the mining process. Thus, it accomplishes some delay in the consensus process, especially under many controllers. For example, the BCS obtained 0.63 s for 10 controllers. However, it varied by 20.63% when 30 controllers are present in the MC-SDN scenario.

Figure 8c depicts the detection time results of the FIA attack of BCS accomplished by varying the number of controllers from low to high. The detection time value was increased by adjusting the controller density from low to high. The proposed model considers 20% of controllers from the total controller density as attackers. Therefore, increasing the number of controllers also escalated the number of attackers in the network. Hence, the BCS needs significant time to detect such attackers in the MC-SDN scenario. For example, the BCS attained 0.67 and 0.76 s of detection time for 10 and 30 controller scenarios, respectively.

Figure 9a shows the attack detection rate results of BCS obtained for the Man-in-the-Middle Attack (MiMA) scenario. To analyze the attack detection efficiency of BCS, the number of controllers was varied from 10 to 30. The results demonstrate that the attack detection rate was reduced by varying the number of controllers from low to high. For example, the BCS incurred a 91.28% attack detection rate for 10 controllers, which is increased by 6.99% compared to the 30 controller scenarios. The main reason behind this is that the proposed model considers the digit-coin value and rPBFT consensus for attack detection in which the MiMA attacker contribution is high under many malicious scenarios.

The consensus delay results of the MiMA scenario are shown in Figure 9b. The BCS varies the number of controllers from 10 to 30 to obtain the consensus delay results. It increases the consensus delay by varying the number of controllers from low to high. For example, the BCS accomplishes 0.64 s of consensus delay for 10 controllers. Under the high number of controllers, the competing node density is also increased, resulting in maximum consensus delay. For example, the BCS decreases the consensus delay by 15.63% compared to the results obtained for 30 controllers.

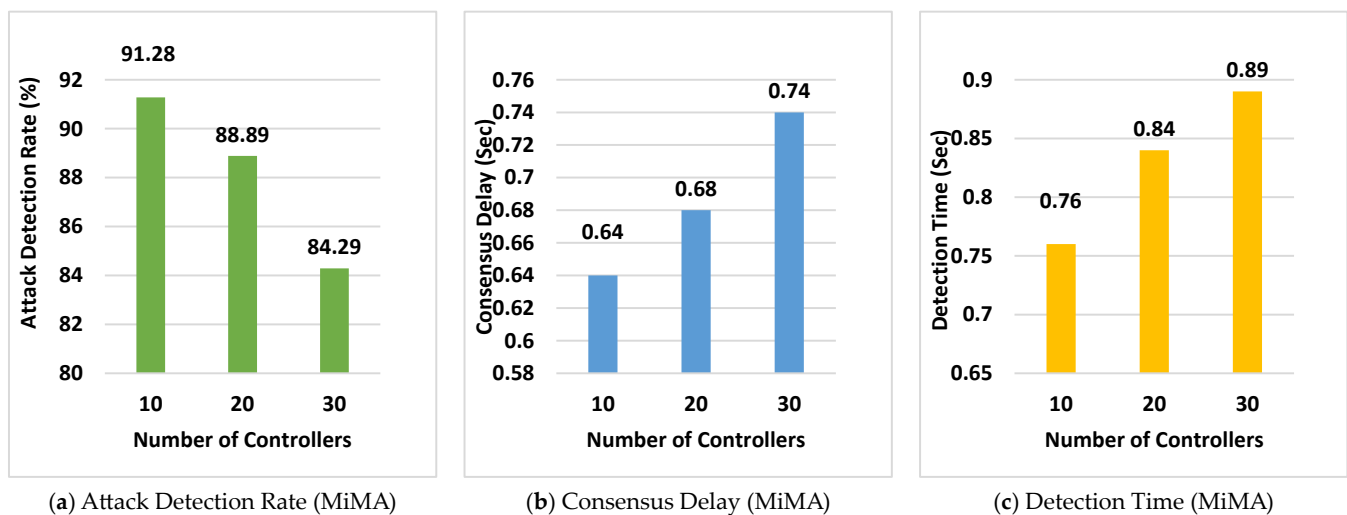


Figure 9. Man-in-the-Middle Attack (MiMA) performance metrics.

Figure 9c plots the detection time results obtained for MiMA under various numbers of controllers. The BCS improves the detection time when varying the number of controllers from 10 to 30. The reason is that the BCS has to defend against the high number of MiMA under a high controller scenario. Thus, it increases the detection time under a high number of controllers present compared to a low number of controller scenarios. For instance, the BCS attained 0.76 and 0.89 s of detection time, respectively, for 10 and 30 controllers.

Figure 10 portrays the attack detection rate results of BCS obtained for the number of attackers (NoA) = 3, 6, and 9. To evaluate the performance efficiency of the BCS security model under different scenarios, the number of controllers was varied from 10 to 30. The attack detection rate slightly increased with varying the number of domains and controllers from low to high. The reason is that the increasing number of domains also increased the number of controllers, resulting in efficient intra and inter-sub-controller monitoring. Thus, it increases the efficiency of digit-coin computation accuracy and improves the attack detection performance. The proposed BCS detects malicious behaviors based on three pieces of information: intra-sub-controller data, inter-sub-controller data, and blockchain data. The maintenance of digit-coin values as blockchain ledgers increases the security level of the proposed system. For example, the BCS accomplished 99.35% and 99.56% attack detection rates under 10 and 30 controllers, respectively, where NoA = 9.

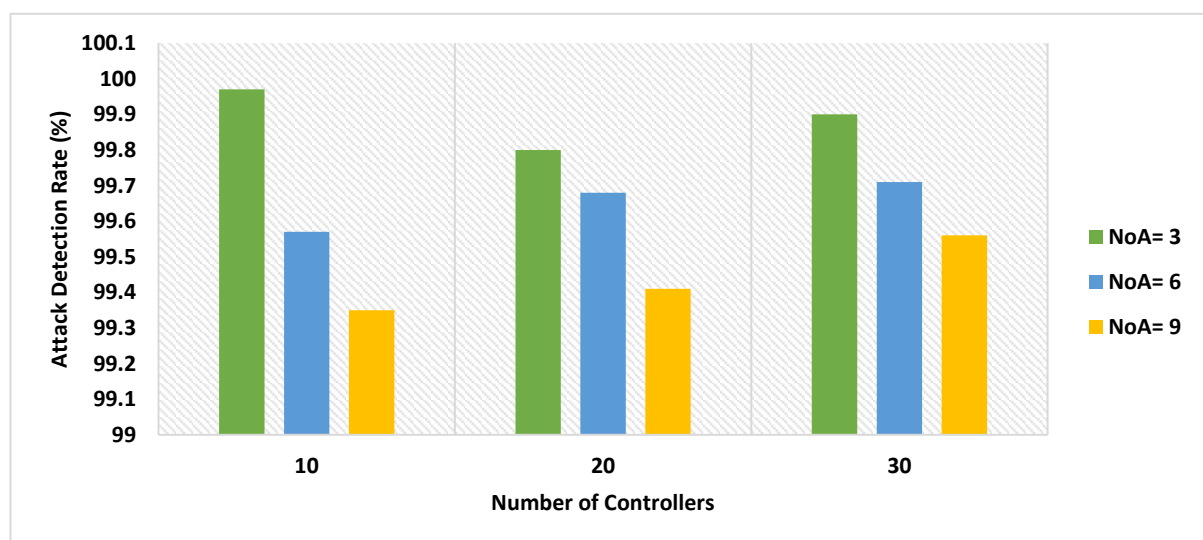


Figure 10. Number of controllers vs. attack detection rate.

The detection time of BCS is shown in Figure 11, and the numerical results are given. The results were obtained by varying the number of controllers from 10 to 30 under malicious controller scenarios 3, 6, and 9. The proposed system exploits the fuzzy-based rPBFT to detect malicious controllers, increasing the detection time when huge numbers of attackers and controllers are presented in the network. The proposed BCS includes different sub-controller monitoring and blockchain data to validate the newly generated blocks and attack detection. Hence, it provides strong security to the SDN even high number of attackers is presented in the network. The proposed model increases the detection time at an acceptable rate to provide strong security in the network. For example, the detection time of BCS is 0.56 and 1.3 s for the number of attackers, 3 and 9, respectively, when 30 SDN controllers are present in the network.

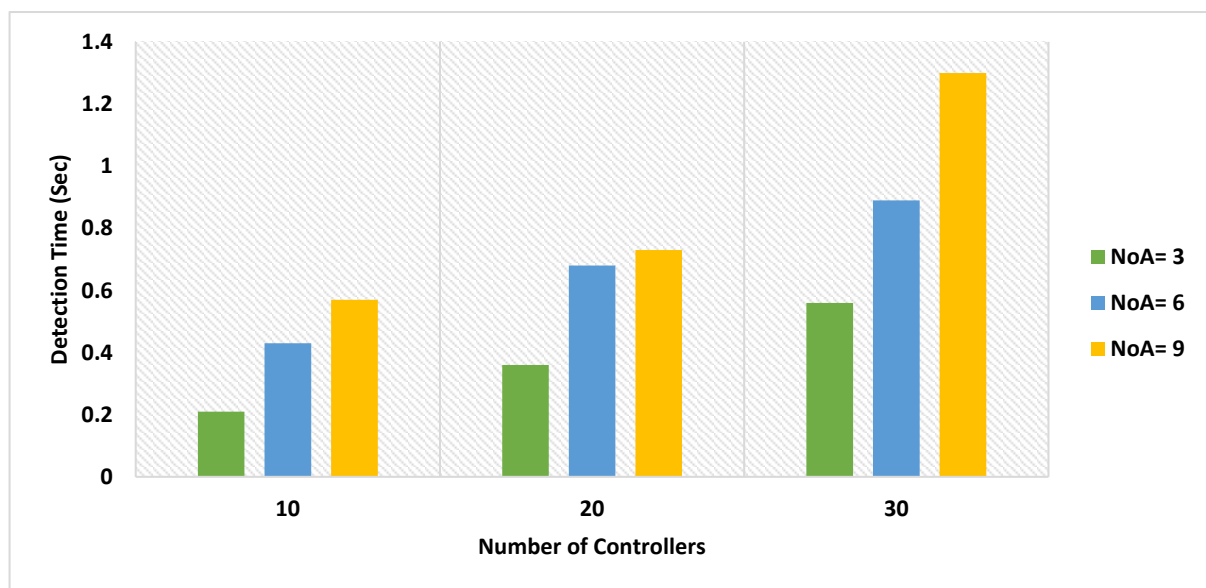


Figure 11. Number of controllers vs. detection time.

The consensus delay performance of rPBFT of BCS is demonstrated in Figure 12. Generally, the number of validators has some delay effect on the rPBFT consensus. The proposed model utilizes a digit-coin blockchain system where genuine miners are fairly involved in block creation and validation. Unlike fundamental PBFT, the rPBFT optimizes the miner selection process using digit-coin values. It selects an adequate number of genuine miners and performs equally to all the selected miner controllers during block validation. Thus, it minimizes the consensus delay and decreases overhead compared to existing PBFT. Also, it exploits various numbers of intra and inter-club-controllers in the consensus process, resulting in some consensus delays with secure mining. For example, the BCS accomplished 0.2 and 1.1 s of consensus delay for 1 and 5 validator scenarios, respectively.

Figure 13 portrays the attack detection rate of the proposed BCS, existing BMC-SDN, and IB-SDN. The proposed BCS model varies the number of attackers from 3 to 9 to show its superiority over existing BMC-SDN. Both models decrease the attack detection rate by adjusting the number of attackers from low to high. The reason is that both models consider the redundant controller monitoring information in attack detection, and most of the redundant controllers are malicious under the high malicious scenario. For instance, the proposed BCS accomplished a 99.54% and 99.14% attack detection rate for 3 and 9 attacker scenarios, respectively. However, the attack detection rate of the proposed BCS is better than the existing BMC-SDN and IB-SDN, as the proposed model includes the monitored data of both intra and inters controllers in attack detection. Unlike this, the existing BMC-SDN only includes the inter-controller reputation values for attack detection, resulting in a

minimum attack detection rate. The IB-SDN exploits global trust maintenance among the distributed controllers, and it is unable to minimize the compromised controller effect in the network. For example, the BCS enhanced the attack detection rate by 0.3% and 0.9% compared with existing BMC-SDN and IB-SDN, respectively, when nine attacker nodes were presented in the network.

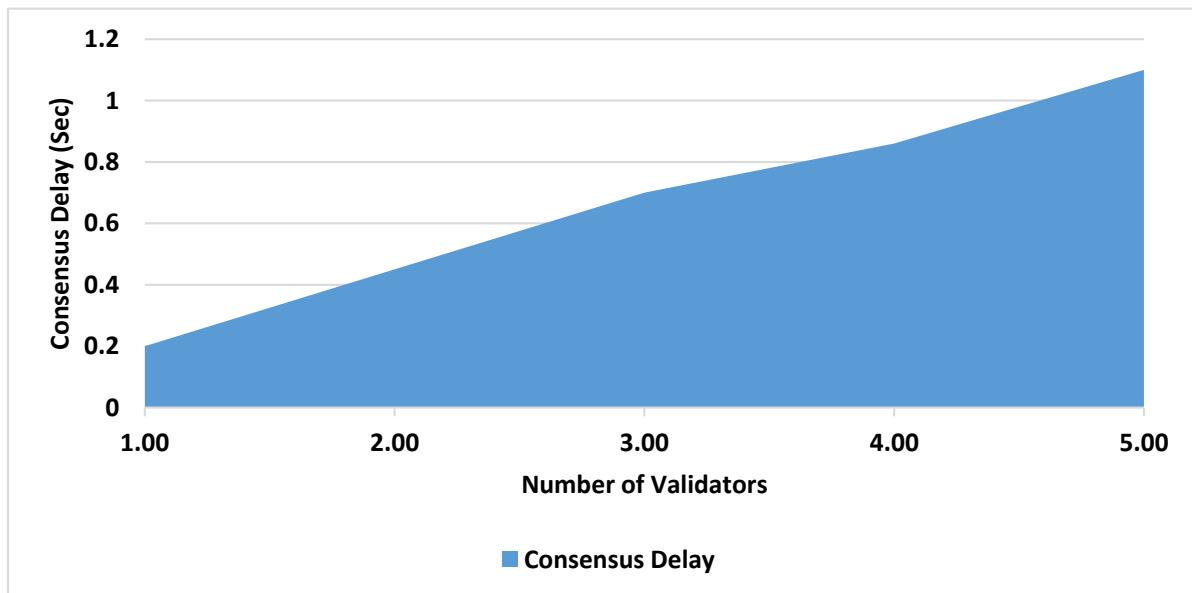


Figure 12. Number of validators vs. consensus delay.

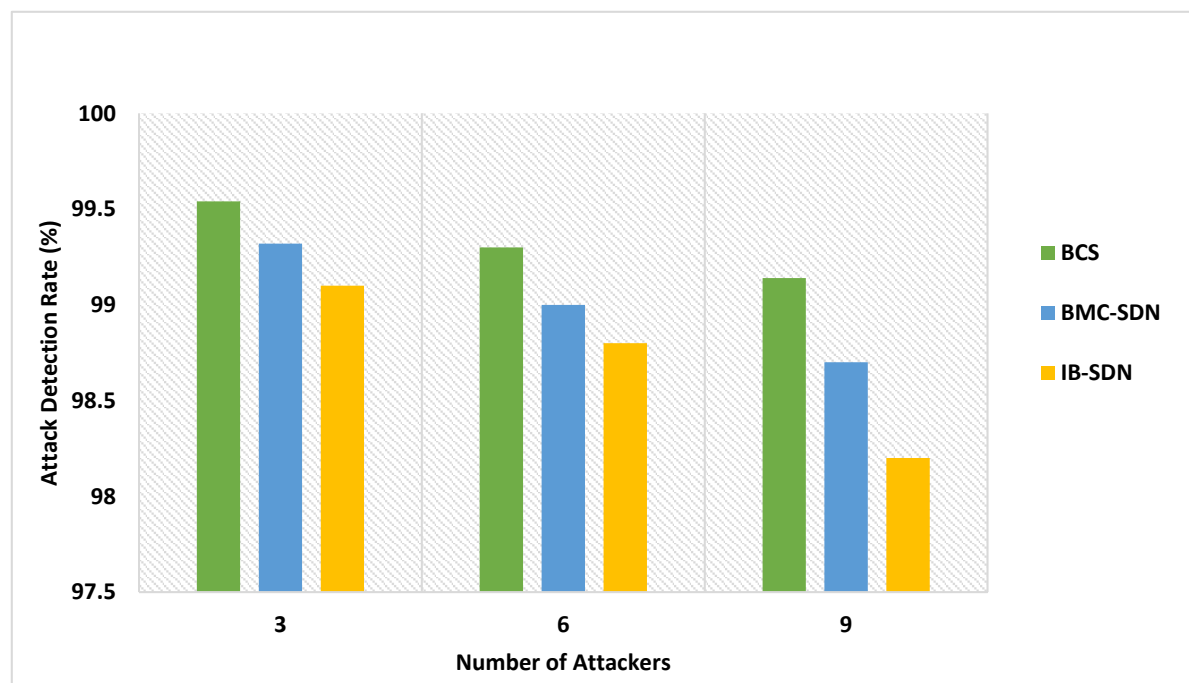


Figure 13. Number of attackers vs. attack detection rate.

Figure 14 illustrates the comparison of attack detection rate results of BCS, BMC-SDN, and IB-SDN. To show the superiority of BCS under multiple numbers of compromised controllers, the number of compromised controllers is varied from 1 to 3. The results demonstrate that all three works decreased the attack detection rate when adjusting the number of compromised controllers from low to high. For instance, the proposed BCS decreased the attack detection rate by only 0.4% by adjusting the compromised controller number from 1 to 3. However, it was minimal when compared with the attack detection rate results of BMC-SDN and IB-SDN. The reason is that the proposed model includes the advantage of inter and intra-controller monitoring strategy in the reputation estimation of the main controller. Although the BMC-SDN also includes the redundant controller structure to mitigate the compromised controller effect, it fails when multiple numbers of controllers within a domain are compromised. The IB-SDN fails to provide defense against compromised controller scenarios. For instance, the BCS minimized the compromised controller effects while improving the attack detection rate by 5.7% and 13.9% compared with BMC-SDN and IB-SDN, respectively, when three compromised controllers were present in the scenario.

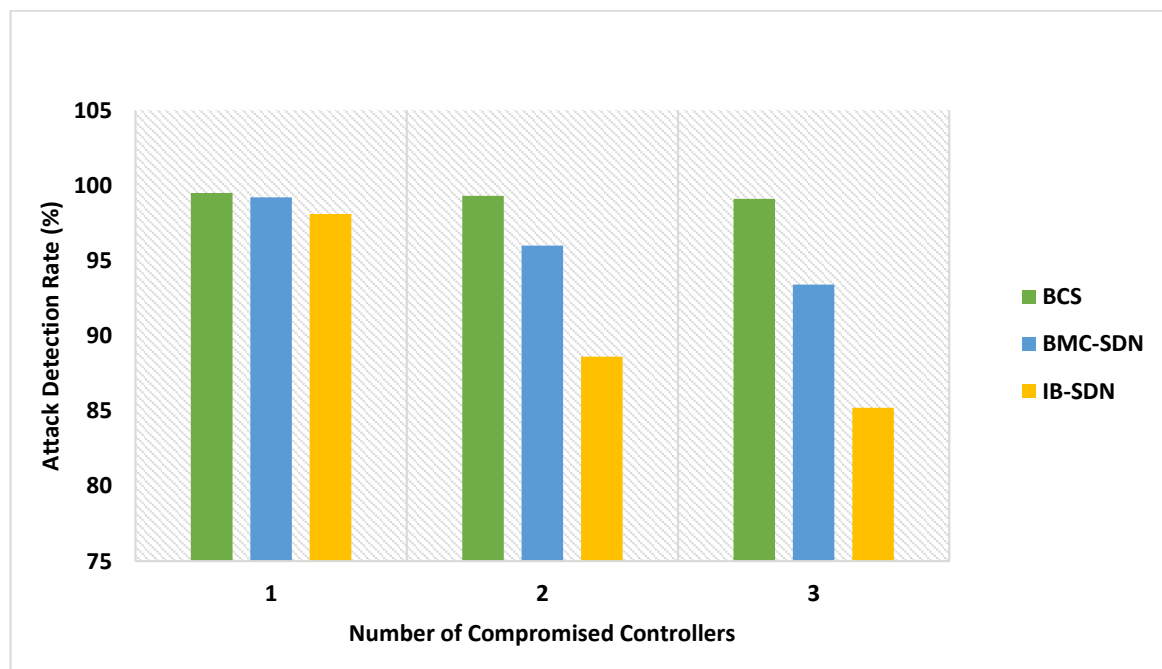


Figure 14. Number of compromised controllers vs. attack detection rate.

Figure 15 compares the attack detection time results of the proposed BCS, existing BMC-SDN, and IB-SDN obtained by varying the number of attackers from low to high. The attack detection time increased when adjusting the number of attackers from 3 to 9. The reason is that the attack detection models perform the computation for huge nodes. For example, the proposed BCS attained 0.12 and 0.23 s of attack detection time for 3 and 9 attackers, respectively. However, the reshaped PBFT provides fair consensus options to the genuine miners selected using blockchain and sub-controller data and neglects the participation of malicious nodes in the consensus process, resulting in quick validation. Thus, it also diminishes the attack detection time of BCS compared with the existing BMC-SDN and IB-SDN. For example, the proposed BCS minimized the attack detection time by 6% and 15% more than BMC-SDN and IB-SDN, respectively, when nine attackers were present in the scenario.

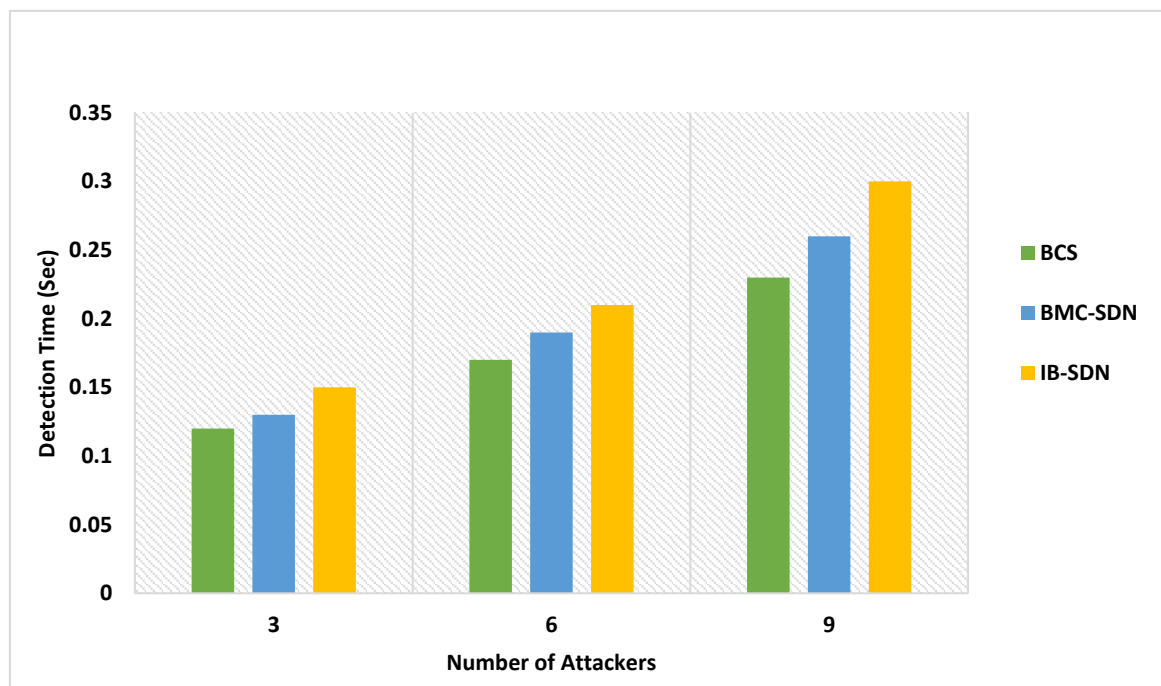


Figure 15. Number of attackers vs. detection time.

6. Conclusions

MC-SDN demonstrates potential advantages in data centers and enterprise network environments due to its scalability, fault tolerance, efficient network management, and performance. However, the compromised controllers in this environment have widespread implications and severe performance issues. The proposed BCS security model offers security against multiple compromised controllers and other security attacks at the controller level. The blockchain-based security model of BCS is implemented among the SDN controllers to detect attacks against controllers, especially in multiple numbers of compromised controller environments. By enabling the main controllers of every domain as sub-controllers to their preceding and succeeding domains, the BCS minimizes the impact of multiple compromised controllers and failure issues, thereby improving consistency among controllers. The rPBFT consensus with the digit-coin system mitigates compromised controllers' behaviors and improves flow table maintenance efficiency at all controllers. By eliminating the impact of multiple numbers of compromised controllers within a domain through inter and intra-controller structure, the BCS maintains a consistent network view among all controllers and improves the flow table update accuracy. Maintaining a consistent network view at the controller level also enhances efficiency at the infrastructure level. Finally, the evaluation results prove the superiority of BCS by improving the attack detection rate when varying the number of controllers and attackers under different network scenarios. For instance, the proposed BCS enhanced the attack detection rate by 5.7% and 13.9% compared with BMC-SDN and IB-SDN, respectively, even when an attacker could compromise three numbers of controllers within a domain. Thus, the BCS extremely minimizes the multiple compromised controller effects while maintaining a high attack detection rate. The notable enhancements demonstrated by the BCS have a significant advantage in the MC-SDN environment specifically large data centers and enterprise networks.

Some of the future directions of BCS are as follows:

- Future work plans to extend the BCS security model to cover the rest of security planes such as infrastructure, northbound, and southbound.
- Future work aims to improve the flexibility and integration capabilities and facilitate interoperability among distinct blockchain platforms exploited within MC-SDNs.

- BCS will be extended as an adaptive security framework that leverages immutable records of blockchain technology to dynamically respond against evolving real-time threat landscapes.
- BCS can exploit the advantage of blockchain to construct a secure, shared distributed repository of intelligence about threat information, where each controller can securely access threat information and improve their contribution to network consistency.
- Proposing a blockchain-enabled secure controller communication approach can enhance controller coordination and ensure that all controllers in the network can operate with similar trust levels.

Author Contributions: Methodology, A.A.; Software, A.A.; Validation, A.A.; Resources, A.A.; Writing—original draft, A.A.; Supervision, I.K. and S.M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hu, T.; Guo, Z.; Yi, P.; Baker, T.; Lan, J. Multi-controller Based Software-Defined Networking: A Survey. *IEEE Access* **2018**, *6*, 15980–15996. [\[CrossRef\]](#)
2. Blial, O.; Ben Mamoun, M.; Benaini, R. An Overview on SDN Architectures with Multiple Controllers. *J. Comput. Netw. Commun.* **2016**, *2016*, 9396525. [\[CrossRef\]](#)
3. Hu, T.; Yi, P.; Zhang, J.; Lan, J. Reliable and load balance-aware multi-controller deployment in SDN. *China Commun.* **2018**, *15*, 184–198. [\[CrossRef\]](#)
4. Yu, T.; Hong, Y.; Cui, H.; Jiang, H. A survey of Multi-controllers Consistency on SDN. In Proceedings of the 2018 4th International Conference on Universal Village (UV), Boston, MA, USA, 21–24 October 2018; pp. 1–6.
5. Maleh, Y.; Qasmaoui, Y.; El Gholami, K.; Sadqi, Y.; Mounir, S. A comprehensive survey on SDN security: Threats, mitigations, and future directions. *J. Reliab. Intell. Environ.* **2023**, *9*, 201–239. [\[CrossRef\]](#)
6. Bhuiyan, Z.A.; Islam, S.; Islam, M.; Ullah, A.B.M.A.; Naz, F.; Rahman, M.S. On the (in)Security of the Control Plane of SDN Architecture: A Survey. *IEEE Access* **2023**, *11*, 91550–91582. [\[CrossRef\]](#)
7. Indrason, N.; Saha, G. Exploring Blockchain-driven security in SDN-based IoT networks. *J. Netw. Comput. Appl.* **2024**, *224*, 103838. [\[CrossRef\]](#)
8. Fan, W.; Chang, S.Y.; Kumar, S.; Zhou, X.; Park, Y. Blockchain-based secure coordination for distributed sdn control plane. In Proceedings of the 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), Tokyo, Japan, 28 June–2 July 2021; pp. 253–257.
9. Ahmad, S.; Mir, A.H. Securing centralized sdn control with distributed blockchain technology. *Comput. Sci.* **2023**, *24*, 5–30. [\[CrossRef\]](#)
10. Li, W.; Meng, W.; Liu, Z.; Au, M.H. Towards blockchain-based software-defined networking: Security challenges and solutions. *IEICE Trans. Inf. Syst.* **2020**, *103*, 196–203. [\[CrossRef\]](#)
11. Alharbi, T. Deployment of Blockchain Technology in Software Defined Networks: A Survey. *IEEE Access* **2020**, *8*, 9146–9156. [\[CrossRef\]](#)
12. Abdulqadder, I.H.; Zhou, S.; Zou, D.; Aziz, I.T.; Akber, S.M.A. Bloc-sec: Blockchain-based lightweight security architecture for 5G/B5G enabled SDN/NFV cloud of IoT. In Proceedings of the 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 28–31 October 2020; pp. 499–507.
13. Goksel, N.; Demirci, M. Dos attack detection using packet statistics in sdn. In Proceedings of the 2019 International Symposium on Networks, Computers and Communications (ISNCC), Istanbul, Turkey, 18–20 June 2019; pp. 1–6.
14. Phan, T.V.; Park, M. Efficient Distributed Denial-of-Service Attack Defense in SDN-Based Cloud. *IEEE Access* **2019**, *7*, 18701–18714. [\[CrossRef\]](#)
15. Sharma, P.K.; Park, J.H. Blockchain based hybrid network architecture for the smart city. *Future Gener. Comput. Syst.* **2018**, *86*, 650–655. [\[CrossRef\]](#)
16. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Kumar, N.; Choo, K.K.R.; Zomaya, A.Y. Blockchain for smart communities: Applications, challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *144*, 13–48. [\[CrossRef\]](#)
17. Li, W.; Tan, J.; Wang, Y. A framework of blockchain-based collaborative intrusion detection in software defined networking. In *Network and System Security*; Springer: Cham, Switzerland, 2020; pp. 261–276.
18. Lokesh, B.; Rajagopalan, N. A Blockchain-based security model for SDNs. In Proceedings of the 2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2–4 July 2020; pp. 1–6.

19. Barka, E.; Dahmane, S.; Kerrache, C.A.; Khayat, M.; Sallabi, F. STHM: A Secured and Trusted Healthcare Monitoring Architecture Using SDN and Blockchain. *Electronics* **2021**, *10*, 1787. [CrossRef]
20. Xie, L.; Ding, Y.; Yang, H.; Wang, X. Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs. *IEEE Access* **2019**, *7*, 56656–56666. [CrossRef]
21. Rahman, A.; Islam, M.J.; Montieri, A.; Nasir, M.K.; Reza, M.M.; Band, S.S.; Pescapè, A.; Hasan, M.; Sookhak, M.; Mosavi, A. Smartblock-sdn: An optimized blockchain-sdn framework for resource management in IoT. *IEEE Access* **2021**, *9*, 28361–28376. [CrossRef]
22. Algarni, S.; Eassa, F.; Almarhabi, K.; Algarni, A.; Albeshri, A. BCNBI: A Blockchain-Based Security Framework for Northbound Interface in Software-Defined Networking. *Electronics* **2022**, *11*, 996. [CrossRef]
23. Li, P.; Guo, S.; Wu, J.; Zhao, Q. BlockREV: Blockchain-Enabled Multi-Controller Rule Enforcement Verification in SDN. *Secur. Commun. Netw.* **2022**, *2022*, 7294638. [CrossRef]
24. Zeng, Z.; Zhang, X.; Xia, Z. Intelligent Blockchain-Based Secure Routing for Multidomain SDN-Enabled IoT Networks. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 5693962. [CrossRef]
25. Das, D.; Banerjee, S.; Dasgupta, K.; Chatterjee, P.; Ghosh, U.; Biswas, U. Blockchain enabled sdn framework for security management in 5g applications. In Proceedings of the 24th International Conference on Distributed Computing and Networking, Kharagpur, India, 4–7 January 2023; pp. 414–419.
26. Derhab, A.; Guerroumi, M.; Belaoued, M.; Cheikhrouhou, O. BMC-SDN: Blockchain-based multicontroller architecture for secure software-defined networks. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 984666. [CrossRef]
27. Song, Y.; Feng, T.; Yang, C.; Mi, X.; Jiang, S.; Guizani, M. IS2N: Intent-Driven Security Software-Defined Network with Blockchain. *IEEE Netw.* **2023**, *38*, 118–127. [CrossRef]
28. Medury, L.; Kandah, F. B2-C2: Blockchain-based Flow Control Consistency for Multi-Controller SDN Architecture. In Proceedings of the 2024 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 6–8 January 2024; pp. 1–6.
29. Ekel, P.; Queiroz, J.; Parreiras, R.; Palhares, R. Fuzzy set based models and methods of multicriteria group decision making. *Nonlinear Anal. Theory Methods Appl.* **2009**, *71*, e409–e419. [CrossRef]
30. The Ryu. Available online: <https://ryu-sdn.org/> (accessed on 14 July 2023).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.