A Secure Multicontroller SDN Blockchain Model for IoT Infrastructure

K. Janani and S. Ramamoorthy

Abstract IoT is making significant progress in a variety of fields, including health care, smart grids, supply chain, and so on. It also makes people's daily lives easier and improves their interactions with one another and their surroundings and environment. There is a variety of research on decentralized computing for IoT develops a decentralized IoT-based biometric facial recognition solution for COVID-19 lockdown cities. They propose a three-layer architecture (application layer, control layer, and data layer) and then create a blockchain framework on top of it to entirely restrict public movements. The software-defined network is the most widely utilized solution for establishing secure network interaction and building secure IoT infrastructures. They give a solid and dependable framework for dealing with dangers and issues like security, scalability, and confidentiality. This study provides a blockchain-based software-defined IoT framework for smart networks that are optimized for energy efficiency and security. Indeed, multicontroller SDN blockchain (MC-SDNBC) has been extensively used to manage vast-scale networks which are, though, subject to a variety of attacks, include false data injection, which causes regulator topology inconsistencies. Every software definition network domain is administered with a single master controller who communicates with both the masters of the other Internet via blockchain. The controller unit generates blocks of dynamic network modifications, which are subsequently evaluated by redundant controllers using a reputation technique given by the control system. The popularity system uses continuous and coupled reactive fading repute algorithms to score the controllers, for example, the voter's maker and block, during each voting activity. The analysis findings show that false flow rule insertion may be detected quickly and efficiently, keeping more secured IoT Systems.

Keywords IoT · MC-SDN · Blockchain · Security

K. Janani (✉) · S. Ramamoorthy
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, India
e-mail: jk6005@srmist.edu.in

S. Ramamoorthy
e-mail: ramamoos@srmist.edu.in

D. P. Agrawal et al. (eds.), *Cyber Security, Privacy and Networking*, Lecture Notes in Networks and Systems 370, https://doi.org/10.1007/978-981-16-8664-1_28

1 Introduction

According to a survey titled "State of IoT Security," attacks on the Internet of Things surged by 22% in the last quarter. According to the survey, some sectors, such as smart infrastructure, smart cities, healthcare, banking, and transportation, have the highest assault risk. Attacks are more complex and elevated by the day, which would be a cause for alarm. Blockchain, which has six main features decentralized, irreversible, transparent, autonomous, anonymity, and free software [1], has emerged as one of the modern approaches acknowledged by both research and industry in the last decade. Likewise, the Internet of Things (IoT) is a promising technology field in which many smart applications are being developed. IoT devices are implemented using actuators, intelligent devices, and sensors. The physical layer, network layer, and application layer are the three layers that make up the IoT system's core architecture [2].

Considering the worldwide health catastrophe COVID-19, businesses are eager to grow up work-from-home possibilities with heavy security and all focus specifically. As a result, remote management usage is more important than ever. Different heterogeneous devices are connected and communicated with each other in an IoT application [2]. Because the number of connected things to the Internet is increasing these days, managing and controlling IoT has become a difficult task. SDN steps in to provide the IoT network's adaptability and scalability without requiring existing implementations to change their design [3]. Because the majority of smart gadgets are low end, they are more vulnerable to attacks. There is a requirement for lightweight algorithm for cryptographic provision of a safe, and computing to create IoT-based communication services. The confidentiality, integrity, and availability (CIA) primary security purpose must be kept updated by the application. With the growing popularity of blockchain technology, increasing study has focused on the use of blockchains in conjunction with SDN, allowing untrustworthy persons to connect with others in a suitable area without the need for a trusted third party [4].

Blockchain is another sophisticated technology that can be combined with SDN-based IoT applications. Blockchain is a developing decentralized technology that can be integrated with SDN-based IoT systems. Every block of the process is continuously saved, and several blocks are chained together through controlling hash values. Using this blockchain technology will boost security and privacy. Several academics have made numerous recommendations for improving the performance of the network, but none of them can resolve the issue. Even though the Internet of Things, software-defined networks, and blockchain technologies are being merged to provide a better solution for smart infrastructure devices, those technologies also can enable dependable data transfer and interaction in networks. However, when these technologies are used, they add to the complexity. Many authors have explored many different solvents. A few of these technologies give a significant level of protection, but they are not a feasible approach [5].

A distributed blockchain-based SDN-IoT-enabled infrastructure for smart buildings is proposed in this paper. In this regard, smart buildings serve as a dependable domain for automatically controlling and managing temperature, security, light-

ing, and other building functions. Furthermore, SDN-based smart buildings include important factors such as goals, technique scope, target design (centralized network controller), networking devices, and resources configuration (homogeneous and heterogeneous). Security, energy efficiency, network monitoring, reliability, QoS, and delay reduction are some of the main goals. WiFi, LiFi, Zigbee, and Bluetooth are the communication technologies for SDN-enabled smart buildings [6].

To address the IoT security dilemma, we provide an infrastructure security that blends blockchain using a multicontroller software definition network. The key notion of the design and architecture is to allocate a set of controllers from each domain [7], which employs a large number of control systems to provide error detection, and our design focuses on ensuring safe and reliable inter-controller interactions. To achieve this purpose, the system design incorporates a controller unit and numerous controllers for each network domain. Each controller could be the owner in one domain, but it may be duplicated in another. The duplicate controllers select whether or not to validate the nodes of network architecture improvements generated by the control board. The design also includes a reputation system that uses constant and dynamic fading reputation algorithms to rate the controllers after every voting activity. Malicious master controls and duplicate controllers that offer false voting would be identified in this method. The following are the paper's primary achievements in further detail [8].

1. To secure inter-controller interaction, we present multicontroller block (MCB-SDN), IoT privacy issues design which combines software definition network and blockchain technology. Every domain is provided a special master device and several redundant controllers via MCB-SDN. The control systems are blockchain users; the master controller generates blocks, and the redundant directors monitor its activity (Fig. 1).
2. In MCB-SDN, we include a credibility process that rates controllers using one of two methods: (1) constant fading credibility, which allows the control system to forget past operational activities at a steady speed, or (2) simultaneous adaptive fading credibility, which ranks the console which uses various constants based also on device's credibility, gets in trouble, the faster good experiences fade away. On either side, the better the control behaves, the much more quickly unfavorable experiences fade away.
3. Analysis methods, including Mininet software products, ONOS, and multicontroller SDN-Chain, are used to execute the suggested MCB-SDN design. MCB-SDN archive low detection delay and it allows user to identify all maliciously inserted attacks. According to the findings the proposed MCB-SDN model provides dynamic nature of threat detection time to identify rogue in the network dynamic nature of the detection time to identify. Furthermore, the reputation approach provides for flexible detection time of rogue devices based on the network executive's needs.

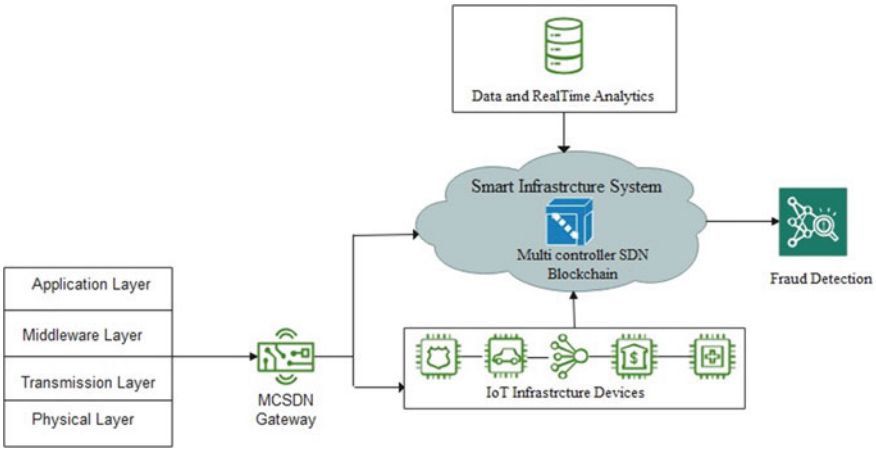

Fig. 1 IoT smart infrastructure layered MCB-SDN architecture

2 Literature Survey

This paper provides a decentralized IoT architecture idea that spans three IoT workflows: computation, storage, and networking in the form of P2P computation overlay, the Ethereum digital signature facilitated decentralized data for IoT entities. As our P2P Storage Overlay, IPFS enabled the widespread storage of IoT data, FL models, and application data. P2P network layers were used to oversee intra-domain and multi-communication using SDN controllers and SDN switches. By adhering to our architecture, we can make IoT computation private without exposing IoT data while preserving reliable IoT storage space and responsive IoT networking. Because we only suggested our architecture concept in this paper, implementing and evaluating it became our urgent future work [1].

To boost security in the cloud storage system, this study presented the Block-SDoTCloud architecture. We also used an SDN infrastructure to direct a distributed blockchain-based process that improved the security, scalability, dependability, confidentiality, and usability of cloud storage services for users. In addition, the writers have successfully performed numerous parameters. By analyzing various procedures, the suggested system provides multiple benefits such as higher throughput, faster response time, faster file transformation, and so on. Furthermore, there are a few restrictions in the proposed system; we did not consider any other assaults in the network layers other than DDoS with flooding attacks. Developers will be able to safely adapt this architectural concept to a variety of applications in the future, including clouds, edge, and mist computing. The system design model will thereafter include further SDN, blockchain, as well as other technologies [2]. In this study, we present a secure network framework that combines three systems: blockchain, SDN, edge, and cloud, for usage in the next phase of IoT ecosystems. The security management framework includes features that are state of the art for next-generation IoT.

The framework, for starters, makes use of blockchain technology. The results show that the proposed security architecture is suitable for fresh research issues in data confidentiality. As a result of the early identification of security breaches, there is less storage required and less delay, as well as a reduction in IoT resource usage and communication bandwidth use. Blockchain technology allows traveling IoT devices and the SDN server to communicate data. Finally, our findings suggest that the suggested security framework be implemented within the IoT network as a data confidentiality preserving element that detects and mitigates any single or collaborative security assaults by monitoring and researching the entire IoT device's traffic flow data.

In recent times, researchers and business verticals have become interested in IoT and IoT big data. While these two technologies actively make people's lives better, they also introduce new threat vectors for future cyber-attacks. IoT networks are an asset and highly heterogeneous when compared to conventional networks. Traditional security measures are inadequate for the IoT context due to these characteristics, necessitating an infrastructure, scalable, and effective security augmentation solution. We begin by examining the characteristics of IoT big data and possible security threats. Then, we present MC-SDNBC, an ID-based SDN security architecture. In this structure, we demonstrated the accuracy of intrusion detection and also overall performance in the presence and absence of our proposed network security using an SDN-specific dataset that models a real IoT environment and contains data recorded for common data assaults and also networks traffic. Our future research will entail expanding the dataset with new attack types and network topologies, as well as evaluating the proposed security strategy under these new network settings. We also want to include an interface for human specialists to interpret the security model, which would improve the model's validity even further [3, 4].

Single point of failure, denial of service attacks, as well as the lack of identification between both the application and the controller were all addressed in this study. We were able to tackle the aforementioned concerns by distributing the SDN control plane across numerous devices while maintaining it logically centralized. Furthermore, blockchain assisted in resolving the common issues that arise when attempting to employ a multicontroller architecture, like device-to-device state synchronization workload is distributed evenly among all processors. A database containing flow entries cannot be changed. For vulnerability analysis and analysis, a record of neural impulses is kept [9]. This research helps ease protection doubts against SDN and encourages industrial adoption of this technology by network engineers by proposing a solution to the security problems discovered in SDN utilizing blockchain. A topology finding mechanism could be added to the smart contract to advance this research. Devices are now added manually via the immediately respond application. Network switches, on the other hand, could be expected to access themself, as well as the details of surrounding switches, to a list of linked switches in the smart contract when they link to a control layer. The switch can then be approved and added to the topology by the application layer. In the long run, the difficulty bomb function outlined in the previous section might cause mining blocks to take longer and longer to mine, potentially leading to a phenomenon known as the ice age. Even if after Ethereum uses the proof of stake method, this will no longer be an issue [5].

The smart infrastructure network and sensor devices connected in the building need to be more secure to monitored the infrastructures like roads, banks, hospital, buildings, fire service, power supply system, traffic management, gas supply system, homes, digital library, conference hall, etc., the backbone of the smart infrastructure in the ICT transaction with smartly creating physical infrastructure. This ICT infrastructure has a communication protocol like Wi-Fi, fiber optics, hotspot as service-oriented information system [6]. The smart infrastructure is highly efficient, safe and fault-tolerant, and secure as considered to high-level infrastructure which are all physical infrastructure hardware, software, middleware as its overall components. Suppose there is a lot of energy consumption, high maintenance costs, and many abnormal situations [8]. This means this ICT communication gives better ideas and gives solutions to management immediately reflected in smart cities. The use of IoT devices gives an integrated solution that can work and identify the huge amount of data which will higher the operational and power consumption of smart infrastructure (SI). The advantage of SI following: high efficiency, decision making, low-cost operation, more resource gathering, less capital and operational cost structure and management, and risk identification and sustainability [8].

Smart environment monitor system using wireless communication network of ZigBee IoT protocol collects the complete real-time environment information, and here, they started basic monitoring system network connected the street lights as route and taxi's as a node, next dynamically assigned the network every node is allotted with an address as only one identity in the network [10]. The computer design management simulation result is true and can meet the gathered information to structure the terminal in the form of a transaction according to the settings. The multiple sensors added from various intranet devices support multi-functional smart cities based on streetlight and taxis [11]. The multi wireless sensor network model designed with multiple nodes perform different kind of function of the node. Every node divided into a base station, cluster headers, and bash nodes as per their capabilities, which give facilitate an organized and group of the nodes [12]. The hybrid blockchain model is proposed here, connected multi-WSN network model far better, according to various capabilities and energy of various nodes, private and public blockchain delivered in-between cluster header and base station like hybrid network model structured [13].

This paper provides a generic classification of IoT attacks in the latest papers based upon IoT privacy and security, using this technology increased data transaction and networking over the Internet. As per new state-of-art software-based managed devices is called software denied network (SDN) which can fluctuate to conduct a customer's necessary. This attempts to give the taxonomy of previous IoT security threats, and their answers are SDN using the deep learning algorithms [14]. This is also suggested as the primary task of an IoT system to collect data from the devices which is classified into three categories: IoT wireless network, authentication, data aggregation, and validation here remove the cross-layer malicious attack, Bayesian algorithm data validity, neural network are used deep learning [15].

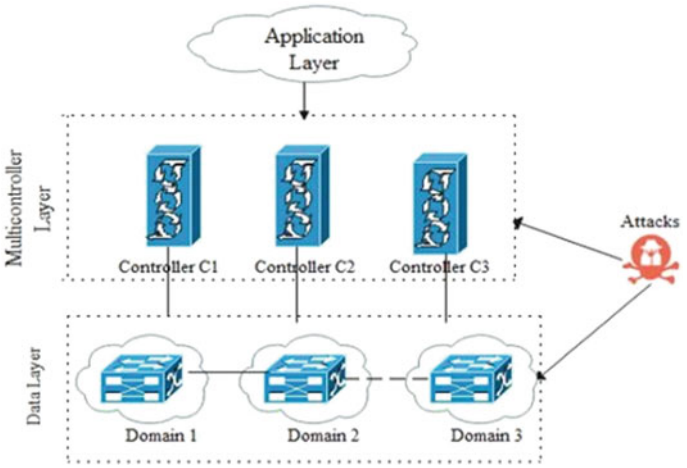

Fig. 2 General multicontroller SDN system

3 Proposed Method

Multiple and dispersed controllers in an SDN network. The application, control, and data layers make up the overall SDN controller. The application layer is made up of programs that tell the actuators about their network architecture and source nodes' regulations. The control layer is made up of *N* control systems that are spread over the network. Devices established in *N* separate domains are found in the data layer. One master controller controls every domain, but every controller unit includes multiple child or duplicate controllers. The controller unit serves as a duplicate controller for multiple domains in addition to its main function. In a distributed system, the controllers. The global view of the network is maintained by multicontroller SDN (Fig. 2). MC-SDN [16] is proposed to manage large-scale and multidomain systems, with each operator accountable with one domain. There have been two types of techniques in MC-SDN: vertical and horizontal. The Openflow [17] handles the southbound connection between both the controller and forwarding devices, such as switches, in verbal leadership by informing switching devices where to get off. The device's communication with the apps is managed by the network layer. Controllers transmit network information topology via their east–west connections in information exchange.

The network manager and network software's key concern is keeping the SDN controllers synced and shared significant network information to make the best routing informed choices. Microcontroller SDN, but on the other hand, might be vulnerable to a variety of vulnerabilities, involving false data insertion, in which a hacked controller provides fake flows to other controllers. To address this problem, we offer a security infrastructure that combines blockchain with MCB-SDN (Fig. 3).

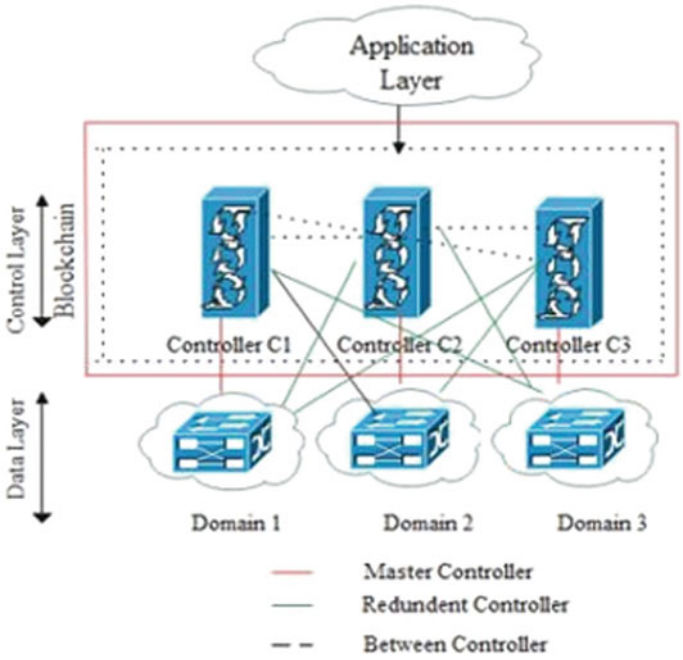

Fig. 3 Proposed MCB-SDN system

The architecture's core concept is to assign a collection of actuators to each domain. Unlike [18], which uses a large number of controllers for high availability, our design is focused on guaranteeing safe and reliable inter-controller interaction. The proposed framework includes a controller unit and multiple controllers for each virtual network to achieve this goal. Inside one domain, every controller could be the owner, because in other domains, it can be duplicated. The controller unit generates blocks of dynamic network changes, and the duplicate devices decide to choose whether or not authenticate them. The design also includes a popularity system that uses continuous and adaptive fading repute algorithms to rate the controllers during each voting activity.

4 Methodology

The proposed MC-SDNBC structure is defined in detail in section. The goal of MC-SDNBC is to defend that SDN controller of the previously mentioned multiSDN architecture. In the face of the many vulnerabilities mentioned in Sect. 3, BMC-SDN leverages blockchain to safeguard controller interaction in this way. The control

layer is safeguarded by blockchain. All devices are users of a public blockchain, and devices interact with one another through this network. At MC-SDNBC, we place a premium on information security. The control layer traffic directed towards east-west interface. We evaluate our research in [9] for the integrity of interaction between sensors and control layer components. The number of controllers within the system is denoted by N. We choose a central server controller and M redundant units for each domain, $2 < N \leq M$. Inside the event that the controller unit fails, the duplicate controllers take over. If it is the only redundant regulator available, a duplicate controller cannot substitute several parent controllers. The duplicate controller which will take over the role of a control system is chosen based on its characteristics. The redundant control system with the shortest ID is chosen more accurately. Furthermore, M duplicates controllers in the same database monitor the respective master device's behavior and contribute to the consensus of evaluating the master device's blocks of data.

4.1 Trusted MCB-SDN Node

In MCB-SDN, the authorized node has written and read on the blockchain, privileges. All parent operators are regarded as trustworthy data. They will understand and develop new blocks from blockchain adding a new external element to the equation the data layer's message triggers the creation of a new block. When a control board gets new information from its own property's data layer controllers, such as a based on flow notification, it builds a new block having sufficient information and distributes it to the redundant processors for confirmation. All managers in the network have access to the approved block. As a result, each microcontroller can create a global network model that is identical. The duplicate managers are in charge of the consensus process.

(a) **Trust Multicontroller** if Ri is less than 0.8. The miners assess and take into account the data sent by the controller in this situation.
(b) **Uncertainty Multicontroller** if Ri = 0.8 and 0.4. The evidence provided by the controller is analyzed in this situation; however, the miners do not consider that (Fig. 4).

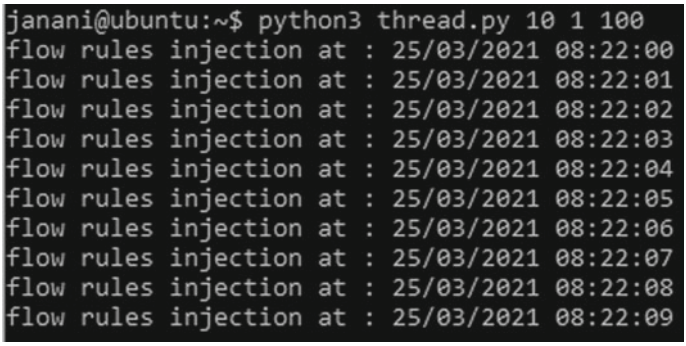

Fig. 4 Attack experiment

4.2 Reputation and Consensus MCB-SDN Mechanism

The controllers of this group are known as miners. They are in charge of ensuring that freshly produced blocks are valid. The latest defective block is distributed to the miners once the controller unit introduces a new block. The miners begin the system testing by analyzing the outcomes included in the faulty block to their personal information. The miners get the same application as the control system and respond with the required information. They may, for example, create the same flow rule in response to a certain flow rule request. As a result, the miner may compare the two blocks and approve the new one appropriately after it has been validated, the new node will be uploaded to the blockchain. Malicious controllers could include miners who disagree with the consensus and the control board whose block has still not been confirmed. The following popularity technique can be used to calculate the recognition of the rogue controller. The reputation theory is modeled as such an added step of defense for the SDN controller [19], so the overall system. This strategy is centered on the management of controller reputation. Every controller (Ci) must have a reputation (Ri) value, which is distributed through the chain by all miners. Reputation (Ri) is a number that ranges from 0 to 1 ($0 \leq \text{Ri} \leq 1$). Every controller in this system can be in one of three states, based on its reputation score Ri.

4.3 Attack MultiController

If Ri is < 0.4, this microcontroller's communication traffic is disregarded by the until managed services intervenes, and others will be affected. SDN controller (Ci) reputation is regularly updated when Ri (0:5), and then when Ri 0:4 and Ri 0:8, it transitions to a doubtful and reliable state, accordingly.

4.4 The Consensus Ci Is Evaluated by the Miner Controllers Based on the Consensus Outcome

If a consensus is established, the master device's block will be validated, and also its reputation score may rise. If a consensus cannot be established, the master device's block will be not be confirmed, reducing the value of its repute. The reputation of miners that share the majority opinion viewpoint will improve. Miners whose views differ from the majority will also have their image tarnished [20].

4.5 The Amount of Ri Is Calculated in the Following Way

Throughout each time frame, we calculate the repute of regulator Ci (RPi) (or observation interval). RPi is defined as Pi/TPi, with Pi is alot of quality participations made by manager Ci in blockchain activities and TPi seems to be the overall lots of successful participations made by control Ci (creation and validation of blocks).

4.6 Both Good and Negative Memories Are Remembered at the Same Pace When the Fixed Fading Factor Is Used. Let Us Have a Look at This Link Scenario

If the controller is reliable and then begins to act deliberately, the positive experience will be gradually lost, and the controller's detection rate will indeed belong. If the microcontroller is also not malicious and starts behaving well, the unfavorable past will eventually be forgotten, and the controller's redemption time would belong. If the controller is reliable and then begins to act deliberately, the positive experience will be swiftly forgotten, and the device's detection rate will indeed be short. If indeed the device is malicious then begins to behave well, the negative past will be swiftly forgotten, and also, the controller's redemption time will indeed be quick [21]. Throughout this case, the control system might take advantage of the consensus mechanism and behave maliciously also for the duration of the season, and once the situation of the smart contract becomes suspect or malicious, it will be terminated. The controller would be able to take action. We can see by the examples above that employing a fixed fading factor has various drawbacks [22]. To address this problem, we propose employing varying fading factors based on the controller's trustworthiness.

5 Results and Discussions

IoT Infrastructure for Implementation we use the following elements to construct the blockchain-based secure multicontroller architecture in this section (Fig. 6).

a. **SDN Control**: The SDN controller is implemented with the open network operating system. It provides the control plane that allows a domain to be deployed with many controllers. The number of SDN domains is 3, the number of duplicate controllers is 2, the switching frequency is (10–100), and the number of connections is (10–450).
b. **Blockchain**: Multi-communication BC is a technology that allows you to store information to construct a private blockchain, and we use multichannel, an open-source platform.
It can regulate who can connect, transmit, and receive transactions, as well as create flows and blocks by assigning rights to nodes. The multichain Web sample, a basic Web application for multichain blockchains, is used to view each distributed consensus node [23].
c. **Mininet**: It generates a wireless machine on a single computer that supports OpenFlow and consists of switches and actual apps. It contains the source code which we used to develope MCB-SDN [20]. It generates a wireless machine on a single computer that supports OpenFlow and consists of switches and actual apps. It contains the code which we deployed MCB-SDN to implement. In furthermore, we use postman and other tools to develop our strategy, an option that enables you to submit and handle HTTP requests. SecureCRT, a network management and end-user access software, is used. Our approach is based on Python and certain libraries such as HTTP BasicAuth and Requests, which identify and communicate with the REST APIs for SDN ONOS devices as needed. JSON can be used to serve data that has been handled also by control [21]. Data Structure: The most essential ONOS Stores are ONOS control systems that have used data stores as their true shared data structure. The entire network keep store is among the shared stores, which includes the flow database and the host warehouse. The remaining distributed stores are categorized as software [24, 25] (Figs. 5 and 6).

5.1 The Performance Calculations Are Used to Assess BMC-Performance SDNs in This Category

a. **Execution Time**: It denotes by (T_{Total}) the amount of time it takes to move a circulation on the blockchain. It is the whole of three factors linked to the number of hosts and switches inside the system: (1) consensus time, (2) block sending time, and (3) information transfer time.

$$\text{TimeTotal} = \text{TimeConsensus} + \text{TimeSent} + \text{TimeUpdate} \quad (1)$$

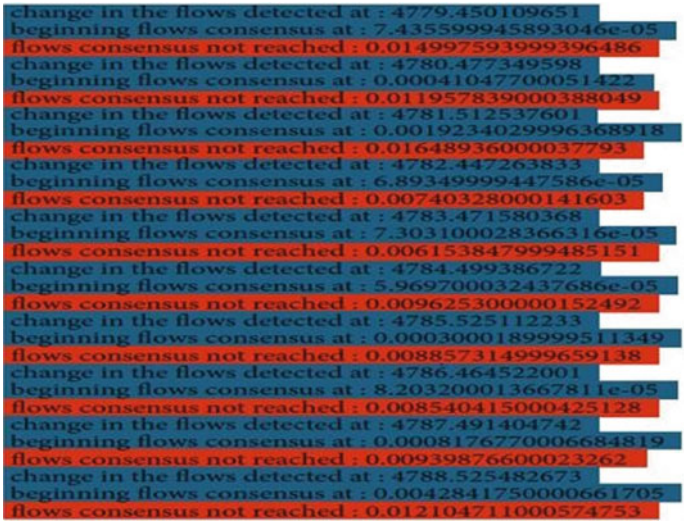

Fig. 5 Thread detection experiment

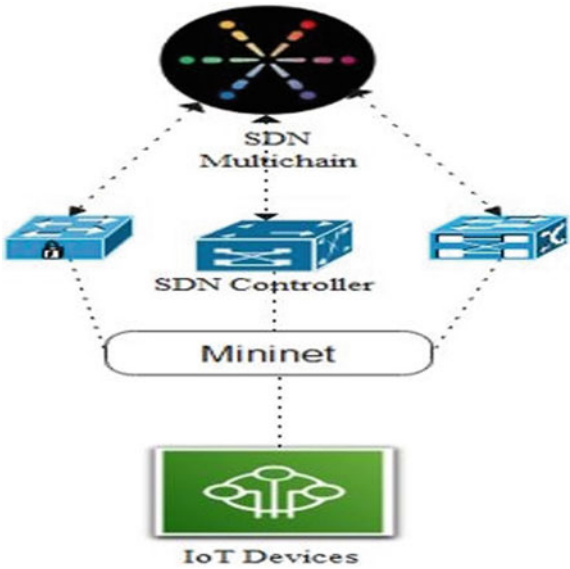

Fig. 6 Implementation of MC-SDNBC architecture

Table 1 No of attack versus DR

Total no of attacks	DR (%)
10	100
20	100
30	100
40	100
50	100
60	100
70	100
80	100
90	100
100	100

b. **Detection Rate** (DR): This is the number of threats multiplied by the number of attacks. **Detection Time** (DT). It keeps track of how long it takes to detect rogue controllers. **Detection Time**(DT): It keeps track of how long it takes to detect rogue controllers. We insert false flows to the regulator to test the robustness of our MC-SDN method, as portrayed inflows are identified as malicious in Figs. 4 and 5 and notified to the admin by creating a record to the logs giving information of the identified anomaly. Table 1 shows the prediction accuracy versus the number of injected threats. As seen in Tables 2, 3 and Figs. 7, 8 MC-SDNBC provides a detection rate of 100%, meaning that all injected threats were effectively recognized in the system. The duplicate devices have seen the same Internet also as a control system, and the fake flow supplied also by masters is detected by the duplicates during block authentication. We can see that as the switching frequency grows the total runtime grows.

We also notice that as the switching frequency and hosts increase, so does the time it takes to reach a consensus. Despite this, the processing times measured are incredibly short. The proposed system's (Fig. 9) detecting time if a device acts deliberately under three different fading ratios = 0:4; 0:3; 0:8, and the combination fading component where 3 = 0:8, 2 = 0:6, and 1 = 0:3. We could see that the operator's repute declines slowly with a high constant fading rate, resulting in a long detection time (i.e., = 0:8), and rapidly with a that instead of fading factor, resulting in a short detection rate (i.e., = 0:3). We also see that based on the controller's reputation, the total fading factor uses various fading rates. If Ri 0:8 and the fading ratio is large (i.e., = 0:8), the fading component slowly diminishes. If Ri is 0:8, it declines at a faster rate, resulting in a shorter trace level.

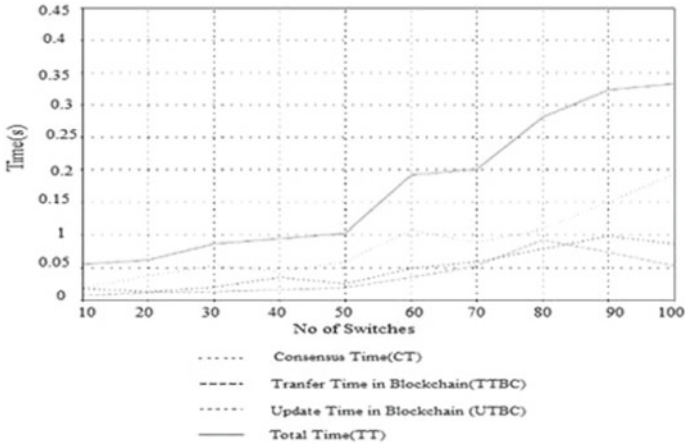

Fig. 7 Number of switches versus execution time

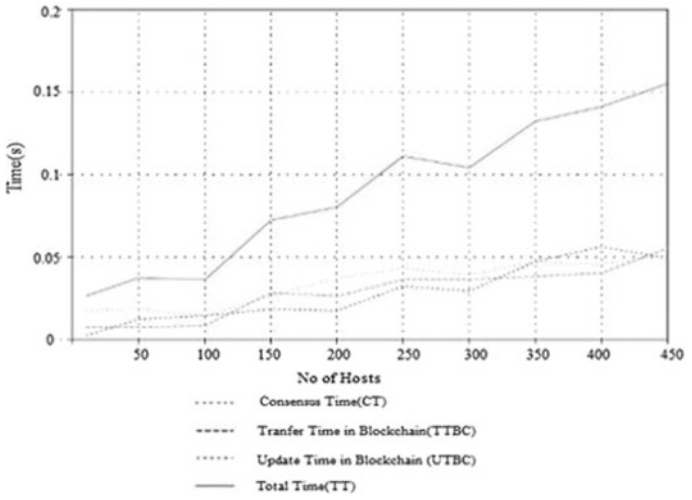

Fig. 8 No of hosts versus execution time

6 Conclusion and Future Work

For secure software-defined networks, MC-SDNBC is a blockchain-based multi-controller design. We cluster wireless networks into SDN domains in this design. Every SDN domain has one master controller and several backup devices. We were using a blockchain, in which the controller unit makes blocks of dynamic network updates, which are then validated by alternative supervisors. Each SDN domain has that there is single master regulator plus several redundant controllers in this system. We were using a blockchain, where the controller unit creates sets of dynamic

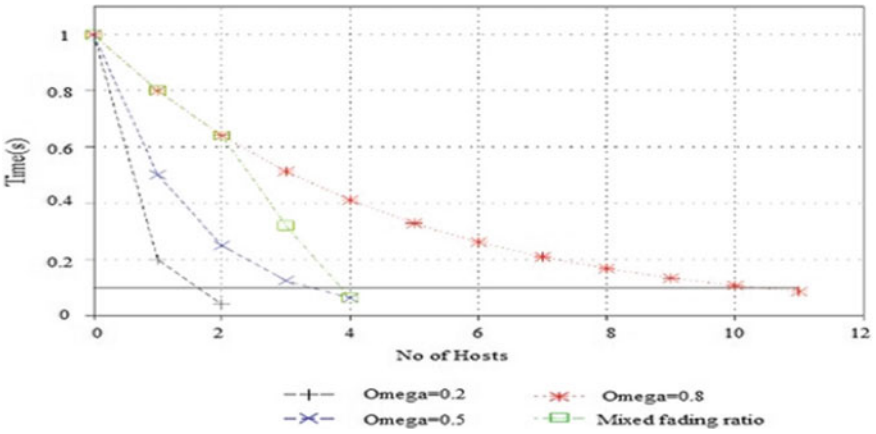

Fig. 9 Detection time of reputation mechanism

Table 2 No of switches versus execution time

Total no of switches	CT	TTBC	UTBC	TT
10	0.018	0.06	0.017	0.054
20	0.037	0.011	0.012	0.061
30	0.053	0.012	0.01	0.086
40	0.043	0.015	0.034	0.094
50	0.058	0.018	0.024	0.102
60	0.017	0.034	0.048	0.191
70	0.088	0.052	0.048	0.201
80	0.108	0.092	0.078	0.282
90	0.15	0.074	0.099	0.323
100	0.193	0.053	0.087	0.333

changes that are subsequently verified by redundant control systems. The controller, block producers, and voters are all rated using a repute approach, during each voting activity. To monitor and adjust the time consumption of rogue operators, the reputation system combines constant and dynamic combined fading reputation algorithms. ONOS, multi-blockchain, and Mininet software platforms have all been used to construct and test the proposed security IoT architecture. In a short period, the evaluation findings showed that flow rule injections were detected 100% of the time. Furthermore, dynamic fading factor adjustment was facilitated by the obtained with the proposed reputation system to reach the required detection time. Because MC-SDNBC only looks at the integrity of east–west interconnections, we aim to address the remainder of the security layers of SDN architecture in future work, particularly the southbound interfaces.

Table 3 No of hosts versus execution time

Total no of hosts	CT	TTBC	UTBC	TT
10	0.018	0.008	0.003	0.027
50	0.019	0.008	0.013	0.038
100	0.015	0.009	0.015	0.035
150	0.027	0.029	0.019	0.073
200	0.038	0.027	0.018	0.09
250	0.044	0.037	0.033	0.111
300	0.039	0.036	0.029	0.104
350	0.047	0.038	0.047	0.132
400	0.046	0.05	0.056	0.141
450	0.051	0.055	0.049	0.155

References

1. Liu M, Song T (2019) Deep cognitive perspective: resource allocation for NOMA-based heterogeneous IoT with imperfect SIC. IEEE Internet Things J 6(2)
2. Rahman A, Islam J (2020) Block-SDoTCloud: enhancing security of cloud storage through blockchain-based SDN in IoT network
3. Medhane DV, Sangaiah AK (2020) Blockchain-enabled distributed security framework for next generation IoT: an edge-cloud and software defined network integrated approach. IEEE Internet Things J
4. Sarica AK, Angin P (2020) Explainable security in SDN-based IoT networks
5. Krishnamohan T, Janarthanan K (2020) BlockFlow: a decentralized SDN controller using blockchain. Int J Sci Res Publ 10(3)
6. Lv Z, Hu B (2020) Infrastructure monitoring and operation for smart cities based on IoT system. IEEE Trans Ind Inform 16(3)
7. Mohanty SP, Choppali U (2016) Everything you wanted to know about smart cities. IEEE Consum Electron Mag
8. Yazdinejad A, Parizi RM (2020) An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Trans Serv Comput
9. Wani A, Revathi S (2021) SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL). https://doi.org/10.1049/cit2.12003.
10. Bhayo J, Hameed S (2020) An efficient counter-based DDoS attack detection framework leveraging software defined IoT (SD-IoT)
11. Lounis K, Zulkernine M (2020) Attacks and defenses in short-range wireless technologies for IoT
12. Frustaci M, Pace P (2018) Evaluating critical security issues of the IoT world: present and future challenges. IEEE Internet Things J 5(4)
13. Hu T, Guo Z (2018) Multi-controller based software-defined networking: a survey. IEEE
14. SDN controller. https://github.com/dariobanfi/multipath-sdn-controller
15. Mininet. https://github.com/mininet/mininet
16. Hu T, Guo Z (2018) Multi-controller based software-defined networking: a survey
17. Rajabi N, Qaddour J (2019) SDIoBoT: a software-defined internet of blockchains of things model. https://doi.org/10.5923/j.ijit.20190801.03
18. Karmakar KK, Varadharajan V (2020) SDN enabled secure IoT architecture. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2020.3043740

19. Li W, Meng W (2020) Towards blockchain-based software-defined networking: security challenges and solutions. IEICE Trans Inf Syst E103–D(2)
20. Thorat P, Dubey NK (2021) SDN-based predictive alarm manager for security attacks detection at the IoT gateways. In: 2021 IEEE 18th annual consumer communications & networking conference (CCNC)
21. Blial O, Mamoun MB (2016) An overview on SDN architectures with multiple controllers. https://doi.org/10.1155/2016/9396525
22. Ramya G, Manoharan R (2021) Enhanced optimal placements of multi-controllers in SDN. https://doi.org/10.1007/s12652-020-02554-2
23. https://thenewstack.io/multiple-sdn-controllers/
24. https://github.com/knetsolutions/learn-sdn-with-ryu/blob/master/overview.md
25. https://sdnwiselab.github.io/