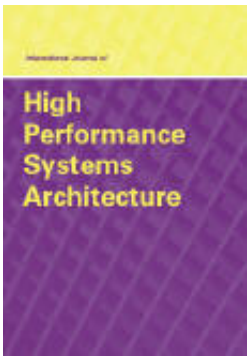


International Journal of High Performance Systems Architecture

ISSN online: 1751-6536 - ISSN print: 1751-6528
https://www.inderscience.com/ijhpsa

Countermeasure SDN-based IoT threats using blockchain multicontroller

K. Janani, S. Ramamoorthy

DOI: 10.1504/IJHPSA.2022.10054069

Article History:

Received:	01 November 2021
Last revised:	25 June 2022
Accepted:	29 July 2022
Published online:	06 April 2023

Countermeasure SDN-based IoT threats using blockchain multicontroller

K. Janani and S. Ramamoorthy*

Department of Computing Technologies,
SRM Institute of Science and Technology,
Kattankulathur – 603203, Tamil Nadu, India
Email: jk6005@srmist.edu.in
Email: ramamoos@srmist.edu.in
*Corresponding author

Abstract: The Internet of Things (IoT) is making significant progress in various fields; software-defined networks with multiple controllers have become popular because they make it easier to manage large networks. But they are open to several attacks, which makes controller topologies inconsistent. To solve this problem, we suggest a multi-controller blockchain for software-defined networking (SDN) network. This security architecture combines blockchain and multi-controller SDN and divides the network into several domains. We put forth a blockchain-based solution. This paper proposed a model blockchain-enabled SDN multi-controller architecture for IoT networks that uses a clustering algorithm and a new routing protocol that is both secure and energy-efficient. Experimental results indicate that the cluster-based routing protocol has a greater capacity, a shorter response time, and a lower overall power requirement than other protocols. It has been shown that our proposed architecture outperforms the classic blockchain.

Keywords: adaptive fading reputation; IoT attacks; blockchain; IoT; SDN multicontroller; security; power consumption; cluster based routing protocol.

Reference to this paper should be made as follows: Janani, K. and Ramamoorthy, S. (2023) 'Countermeasure SDN-based IoT threats using blockchain multicontroller', *Int. J. High Performance Systems Architecture*, Vol. 11, No. 3, pp.117–128.

Biographical notes: K. Janani is a Research Scholar in the Department of Computing Technology in SRM Institute of Science and Technology, Kattankulathur. She received her MTech degree in Computer Science and Engineering from SRM Institute of Science and Technology, Kattankulathur, Chennai, India. She has five years' experience in Healthcare Industry as Quality Lead and 2 Years' experience as Teaching Assistant in SRM Institute of Science and Technology, Kattankulathur Her research interest includes IoT, BlockChain and Deep Learning.

S. Ramamoorthy obtained his under graduate and Master degree from Anna University, Chennai. Presently, he is working as an Associate Professor in SRM Institute of Science and Technology, Kattankulathur, Chennai. He has 15 years of overall teaching experience and 10 Years of Research Experience in Computer Science and Engineering discipline. More than 50 research papers published in international journals with high impact factor which includes SCI, Scopus, Web of Science and so forth. Over 20 research papers are published in international conferences like IEEE, Springer conferences and so on. He received the Travel Grant from TNSCST to present a paper in international conference held in Malaysia. He has published more than 5 Indian Patents and acting as an Editorial board member and reviewer for many international research forums.

This paper is a revised and expanded version of a paper entitled 'A secure multicontroller SDN blockchain model for IoT infrastructure' presented at *Cyber Security, Privacy and Networking, Proceedings of ICSPN 2021*, India, Online, 17–19 September, 2021.

1 Introduction

According to a survey titled 'State of IoT Security', attacks on the Internet of Things (IoT) surged by 22% in the last quarter. According to the survey Mohamed et al. (2020), 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 decentralised, irreversible, transparent, autonomous, anonymity, and free software, has emerged as one of the modern approaches acknowledged by both research and industry in the last decade. Likewise, the 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.

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. Because the number of connected things to the internet is increasing these days, managing and controlling IoT has become a difficult task. Software-defined networking (SDN) steps in to provide the IoT network's adaptability and scalability without requiring existing implementations to change their design. Because the majority of smart gadgets are low-end, they are more vulnerable to attacks. As a result, a lightweight algorithm for cryptographic provision of a safe, and computing was necessary to create IoT-based communication services (Hang et al., 2021), the confidentiality, integrity, and availability (CIA) primary security purpose must be kept updated by the application. With the growing popularity of blockchain technology, an increasing study has focused on the use of blockchain in conjunction with SDN, allowing untrustworthy persons to connect with others in a suitable area without the need for a trusted third-party (Li, 2022).

As a general rule, we need to provide an architecture capable of balancing energy and usage of resources at the physical, network, and application layers for the IoT. This architecture will be implemented using software-defined interconnectivity and blockchain, which we are investigating. The network has been updated with a new architectural style that divides the control plane, also known as the 'brains', from the data plane (the 'brains'). An OpenFlow-based controller manages and configures specific network switches in accordance with a set of policies, monitoring, and fully programmable (Ramu et al., 2017), control of the network, interaction, and remote control can all be provided by the SDN controller, as can powerful approach, increased flexibility, and fully programmable. In addition, the SDN controller allows for the implementation of centralised and safe communications systems have advantages over decentralised ones in many respects (Shukla et al., 2021), including but not limited to: security; routing; power usage; throughput management; and the prevention of unauthorised access to network resources. There are millions of new IoT devices being sold every single day, and SDN promises to make managing them much simpler and more programmable. SDN and IoT can improve network performance. IoT system dynamic nature causes network configuration changes that can be controlled by the SDN controller. The IoT network lacks a central controller, but the SDN controller can offer one for communicating with IoT system. The security of SDNs is a major area of concern. The transfer of files on an SDN network can be protected by blockchain. Because it protects users' privacy and the availability of resources even when they are accessed by untrusted users, blockchain's security-by-design feature can be utilised throughout the SDN network.

Blockchain is another sophisticated technology that can be combined with SDN-based IoT applications (Pourvahab et al., 2019). Blockchain is a developing decentralised 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 IoT, 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.

A distributed Blockchain-based SDN-IoT-enabled infrastructure for smart buildings is proposed in this paper (Islam et al., 2020). In this regard, smart buildings serve as a dependable domain for automatically controlling and managing temperature, security, lighting, and other building functions. Furthermore, SDN-based smart buildings include important factors such as goals, technique scope, target design (centralised network controller), networking devices, resources configuration (homogeneous and heterogeneous), etc. Security, energy efficiency, network monitoring, reliability, QoS, and delay reduction are some of the main goals. Wi-Fi, LiFi, Zigbee, and Bluetooth are the communication technologies for SDN-enabled smart buildings.

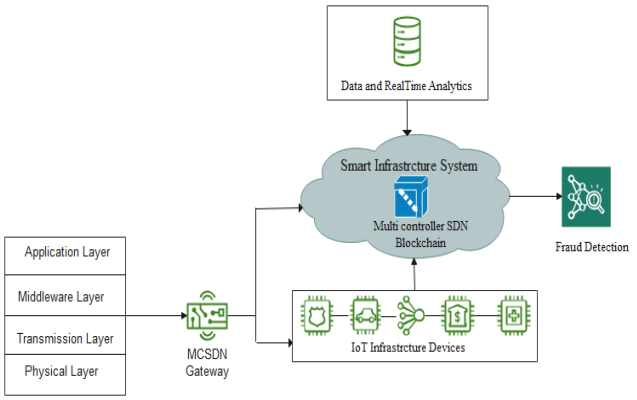
To address the IoT security dilemma, we provide infrastructure security that blends blockchain using a multi-controller software definition network (Rahman et al., 2020). The key notion of the design and architecture is to allocate a set of controllers from each domain, which employs a large number of control systems to provide error detection, 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.

- To secure inter-controller interaction, we present MCB-SDN (Multicontroller Block), 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 Figure 1.
- 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 rank 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 unfavourable experiences fade away. (3) This study contains an in-depth explanation of the infrastructure as well as its workings on the inside, including the operations that are responsible for the transfer of data between Smart sensors as well as energy and system performance procedures.
- Analysis methods, including Mininet software products, ONOS, and Multicontroller SDN-Chain are used to execute the suggested MCB-SDN design. MCB-SDN With a low detection delay Figure 6 (https://www.multichain.com/), it is possible to identify all inserted processes. According to the findings of the evaluation. Furthermore, the reputation approach provides for flexible detection time of rogue devices based on the network executive's needs.
- A new routing protocol that is adapted to the clustering technique is an absolute necessity if one wishes to Provide a safe and Power-efficient method for transmitting data between IoT devices within an SDN domain.
- We show the results of our both simulations and analytical evaluations of the architectures and its route optimisation protocol's performance and reliability. Finally, we summarise our findings and discuss our plans for the future.

The remaining parts of this work are structured as follows: Section 2: Related Work on SDN, Blockchain-based Multicontrollers, and Energy Consumption Detailed Methodology. Section 3: Traditional Multi-controller SDN Model and Attacks Discussion; Section 4: Multicontroller-SDN Security Attacks and Mitigation Using Blockchain Section 5: Detailed explanation of SDN-Blockchain-based energy consumption for IoT devices. Finally, the result analysis based on the proposed algorithms is well suited for computational overhead in IoT devices. Section 6: Results and discussions Section 7: Discussed future work and concluded the overall work of this paper.

Figure 1 IoT multicontroller SDN-blockchain based infrastructure (see online version for colours)



2 Related work

In this section, we will discuss related research analyses that have concentrated on the combining of IoT with Multi-SDN controller and blockchain.

Researchers have shown a significant amount of interest in the topic of SDN with IoT security (Bhayo et al., 2021) proposed a collaborative technique for detecting and mitigate attacks on SDN across multi-controller domains, as well as proposed a framework that detects conflicts in distributed environments. SDN controller environment (Zaman et al., 2020). Each controller produces a directed graph from the forwarding rules using the information in the graph. The various graphs are combined in order to generate a global network state, which enables the detection of any type of flow rule violation as well as loops in the forwarding process (Pourvahab et al., 2019). An SDN architecture that allows for failure of individual controllers to be tolerated was proposed. This architecture would replace the single controller with multiple independent controllers for a multidomain SDN network, they proposed a security architecture that was based on policies. The flow of packets is analysed so that an eventual unauthorised flow can be located and security policies can be dynamically updated.

Blockchain protects multi-controller SDN. first multi-controller SDN connectivity level, then blockchain-based layer. The SDN controller's management instructions are encrypted and saved in a blockchain smart contract. The smart contract checks the command's integrity.

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 (Chaganti et al., 2022). We were able to tackle the aforementioned concerns by distributing the SDN control plane across numerous devices while maintaining it logically centralised. Furthermore, blockchain assisted in resolving the common issues that arise when attempting to employ a multi-controller architecture, like Device-to-device state synchronisation Workload is distributed evenly among all processors. A database containing flow entries that cannot be changed. For vulnerability analysis and analysis, a record of neural impulses is kept.

Smart applications IoT blockchain technology was optimised. Their lightweight blockchain design eliminates overhead. Distributed consensus architecture sped up verification. The suggested design ignores IoT devices' similarity and power limits.

Blockchain-based DistBlockNet is an IoT architecture model that distributes and verifies Flow Rules Tables among IoT devices (Sharma et al., 2018). Using SDN principles, this design generates an IoT network plan that adheres to the principles of security and comprehensibility. Using blockchain to update the flow rules tables, it can automatically isolate threats. But it does not take into account how much power IoT devices use and how limited their resources are. In addition, security concerns could arise as a result of energy usage issues in the architectural style.

In IoT networks, Blockchain has proven to be a promising technology for mitigating erroneous data entry (Tselios et al., 2017). Utilised blockchain systems to protect IoT network localisation and ensure the accuracy of shared data. As a result, localisation errors are reduced with the solution.

Blockchain has also been shown to reduce fraudulent data insertion in IoT networks. Blockchain technology was used to secure IoT geolocation and information accuracy. The suggested approach detects erroneous data injection, reducing localisation errors.

3 Security attack model

As Figure 2 shown, SDN system with many and remote controllers is considered. The interface, control, and data layers make up the overall SDN Architecture framework. The application layer is made up of applications that tell the actuators about their specifications and desired system regulations. The controls layer is composed of N controllers that are spread over the network. Devices registered in N separate domains are found in the data layer. A master controller is used to control each zone, so each controller unit has multiple child or duplicate controllers. The master serves as an alternative controller for multiple domains in addition to the primary function. In a decentralised shared by multiple SDN, all controllers have same global network view. Any changes in every controller's status, including such new flow conditions or link failures, must be communicated immediately to other regulators. The network approaches may not have been executed correctly if the directors have an incorrect perspective, resulting in network configuration errors such as routing, packet loss rate, and firewalls leakage.

Figure 2 General multicontroller SDN system (see online version for colours)

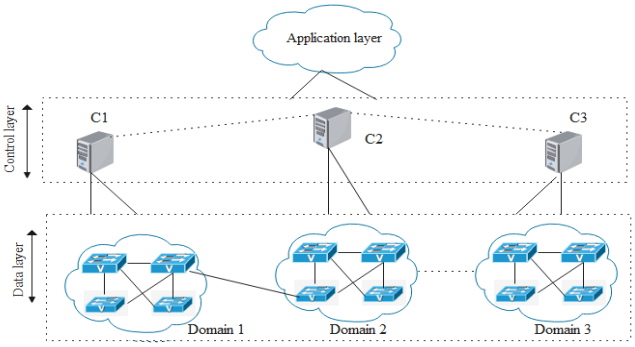


Figure 3 shows the dangers and assaults that could be launched against a multi-controller SDN network the network may be divided if interaction between controller C1 as well as the other controllers' breaks. In this situation, if the network topology in controller C1's area changes, some other controllers will be not be notified, and conversely.

As a result, the controllers may make routing choices based according to their own outdated picture of the system architecture, potentially resulting in unexpected outcomes.

Furthermore, an attacker intercepts controller transmission and insert false data. This MIM attack (Figure 3: arrow 1) can result in an erroneous network perspective, that can result in networking issues such routing information (Figure 3: arrow 2), Firewall vulnerabilities, bad and incorrect routing decisions, and overcrowding of vital links whenever the bulk of erroneous flow rules pass through same link, which all have an impact on system performance (Bhunia et al., 2017)

Furthermore, an attacker can fake controllers (Figure 3: arrow 3) and convey misleading info about just the architecture, the state of the links, and the addresses of every domain using this communication model. This inaccurate information could lead to congestion, device overloaded, and incorrect route discovery, among other issues. Another serious assault might be launched by taking advantage of specific APIs provided by the SDN controller. Developers using these APIs to create new control plane solutions. Therefore, if one application is hacked (Figure 3: arrow 4), the whole channel's safety is threatened. An assault can have drastic implications, such as changing a network's behaviour and stealing network activity, which can lead to large-scale spread DoS attacks.

4 Methodology

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 multi-controller SDN Figure 4. MC- SDN 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 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 North bound connections in information exchange.

Figure 3 Traditional SDN-MC system (see online version for colours)

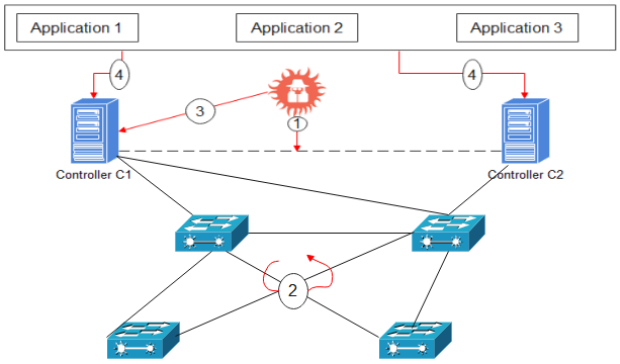
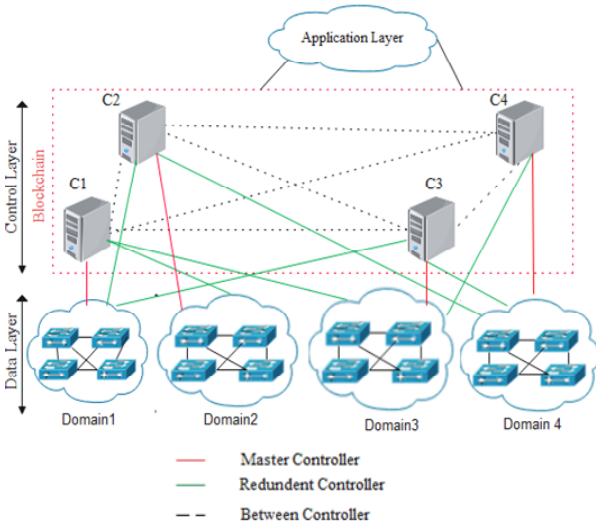


Figure 4 Proposed MCB-SDN system (see online version for colours)

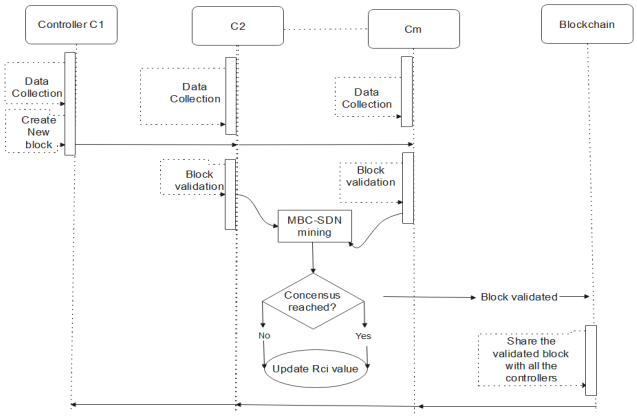


The network manager and network software's key concern are keeping the SDN controllers synced and shared significant network information to make the best routing informed choices. Microcontroller SDN, but on the other hand, might be vulnerable to a variety of vulnerabilities, involving false data insertion,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

The architecture's core concept is to assign a collection of actuators to each domain. Unlike, 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, blockchain with MCB-SDN, 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.

Figure 5 shown MCB-essential SDN's procedures and activities are explained in this flowchart. The controller unit is in charge of coordinating the traffic in its area, whereas the backup controllers observe the web address, receive the very same events, and make the very same changes as the master controller but have no influence it over. In the event that the controller unit fails, a redundant controller can take control of the zone, as previously stated. The manager has a spatial pattern that stores OpenFlow instructions as well as local data such topology, host list, and connection status. Many events, such as topological changes, link failures, and device failures, might cause this data to alter. In the event of a change, the controller unit gets the event, makes the necessary updates, and notifies other units. As a result, the controller unit creates a block comprising these modifications and delivers it to its duplicate controllers over the blockchain.

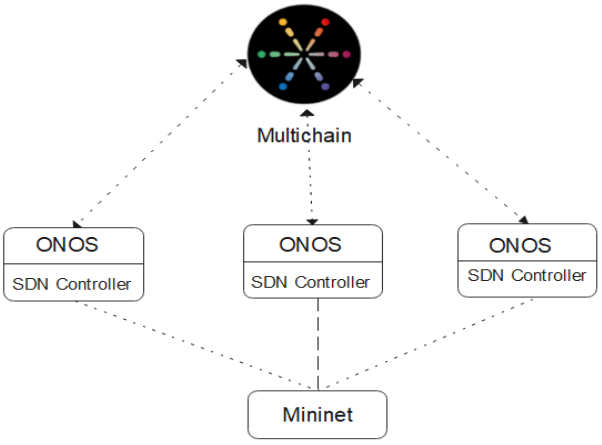
Figure 5 MBC-SDN sequence model (see online version for colours)



This block is validated by the latter, who have already received the same event as the master, using the appropriate consensus protocol: The consensus is attained when the number of duplicate controllers confirming the block surpasses a limit S. The block is regarded genuine in this situation and will be added to the chain. This provides all controls with a comprehensive knowledge of the overall

network. The gained a lot of traction and duplicate devices who verified this block would be graded badly inside this situation.

Figure 6 Implementation of MC-SDNBC architecture (see online version for colours)



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 Multi-SDN architecture. In the face of the many vulnerabilities mentioned in Section 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. That layer's control layer and east-west interaction. We evaluate our research in Yazdinejad et al. (2020) 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, $2 \le M < N$. 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 behaviour and contribute to the consensus of evaluating the master device's blocks of data.

4.1 Trusted MCB-SDN node

In MCB-SDN, the authorised 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.

4.2 Trust multi-controller(if R_i is less than 0.8)

The miners assess and take into account the data sent by the controller in this situation.

4.3 Uncertainty multi controller(if R_i = 0.8 and 0.4)

The evidence provided by the controller is analysed in this situation, however, the miners do not consider that.

Figure 7 Attack experiment

```
janani@ubuntu:~$ python3 thread.py 10 1 100
flow rules injection at : 25/03/2021 08:22:00
flow rules injection at : 25/03/2021 08:22:01
flow rules injection at : 25/03/2021 08:22:02
flow rules injection at : 25/03/2021 08:22:03
flow rules injection at : 25/03/2021 08:22:04
flow rules injection at : 25/03/2021 08:22:05
flow rules injection at : 25/03/2021 08:22:06
flow rules injection at : 25/03/2021 08:22:07
flow rules injection at : 25/03/2021 08:22:08
flow rules injection at : 25/03/2021 08:22:09
```

4.4 Reputation and consensus MCB-SDN mechanism

The controllers of this group are known as miners. They're 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 analysing the outcomes included in the faulty block to their personal information (Nair et al., 2016). 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 modelled as such an added step of defense for the SDN controller, so the overall system. This strategy is centered on the management of controller reputation. Every controller (C_i) must have a reputation (R_i) value, which is distributed through the chain by all miners. Reputation (R_i) is a number that ranges from 0 to 1 ($0 \le R_i \le 1$). Every controller in this system can be in one of three states, based on its reputation score R_i.

4.5 Attack multicontroller

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

4.6 The consensus C_i 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.

4.7 The amount of R_i is calculated in the following way

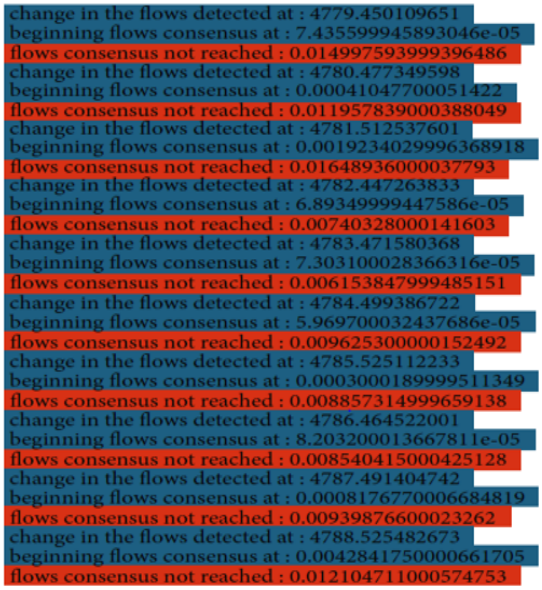
Throughout each time frame, we calculate the repute of regulator C_i ($R\ P_i$) (or observation interval). RPi is defined as $P_i/T\ P_i$, with P_i is a lot of quality participations made by manager C_i in blockchain activities and $T\ P_i$ seems to be the overall lots of successful participations made by control C_i (creation and validation of blocks).

4.8 Both good and negative memories are remembered at the same pace when the fixed fading factor is used. Let's 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 unfavourable 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. 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 have various drawbacks. To address this problem, we propose employing varying fading factors based on the controller's trustworthiness.

$$R_i = \begin{cases} \omega_3 R_i + (1-\omega_3)\, RT_i, \text{when } R_i \geq 0.8, \\ \omega_2 R_i + (1-\omega_2)\, RT_i, \text{when } 0.5 \leq R_i < 0.8, \\ \omega_1 R_i + (1-\omega_1)\, RT_i, \text{when } R_i < 0.5 \end{cases} \quad (1)$$

Figure 8 Threat detection experiment (see online version for colours)



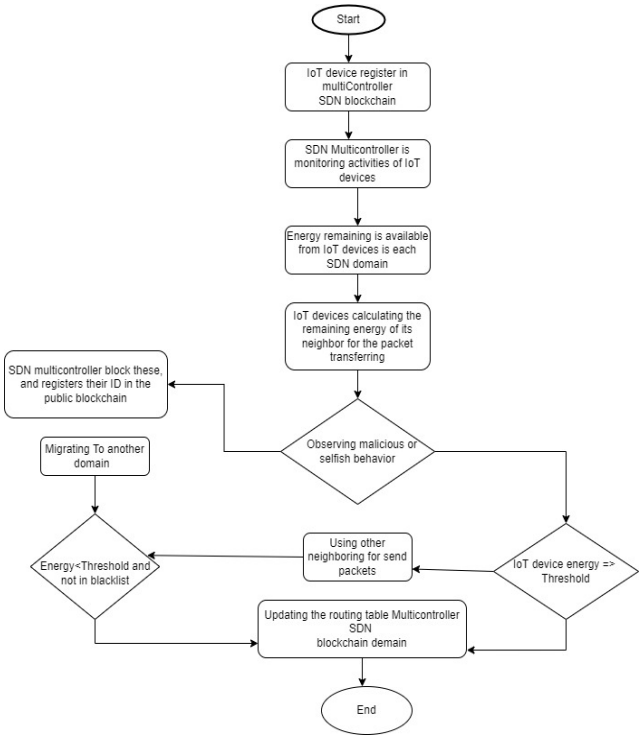
5 Proposed design for security and energy efficiency

New blocks on public blockchains are committed via a consensus technique known as POW. There are so many resources required for POW that blockchains in the IoT area have proven practically impossible because they require so much energy or computing power (Sundriyal et al., 2017) Compatibility among miners also adds time to the process, as it requires a consensus. Since the SDN controller and the verification technique with distributed trust are utilised to tackle the POW problem at public blockchains, we suggest a clustering results and a distributed consensus authentication system. Communication between cluster head is a process on both blockchain networks. When blocks are inserted without the POW, its overhead is removed (Rahman et al., 2021) Distributed identity is used for Multi SDN controller authentication to ensure block authenticity and minimise block verification overhead. The SDN controller generates a block's hash when it is formed. Because its data is dynamic, the controller must constantly recalculate the hash. Using the hash function of the block to create a chain is a safe method. In the proposed architecture for the IoT, we have the ability to share data, carry out transactions, and investigate features thanks to the utilisation of smart contracts. In addition, every single SDN domain has its own unique collection of heterogeneous systems, all of which have varied degrees of both security and the production of energy. This indicates that the

suggested design needs to incorporate an appropriate routing mechanism in order to take into account the energy efficiency and consumption of IoT devices within each SDN domain. This is necessary in order to ensure that the design is successful. IoT devices now have the capability to access network services thanks to the utilisation of the SDN Multi-Controller in each and every SDN domain.

IoT devices typically have a low power consumption and a limited capacity for computation, the proposed protocol can help reduce energy usage by preventing malevolent and selfish nodes from entering the SDN domain (Sundriyal et al., 2017). Depending on the SDN domain, power consumption has a significant impact on data transport. A flowchart summarising the security and energy efficiency measures is provided in Figure 9.

Figure 9 IoT security and energy efficient flowchart diagram



It is necessary for IoT devices to be registered in the SDN controller of the file. Each IoT device that is part of an Multi SDN domain will have its own unique set of public and private keys generated by the SDN Multi-controller. When it comes to IoT devices, the SDN controller keeps tabs on their energy usage and transactions. Energy sources and IoT device energy remaining data are provided in each SDN private blockchain domain. Every IoT device may compute its neighbour's remaining packet-transfer energy. IoT devices send packets based on energy usage (Wadhwa et al., 2022). If energy exceeds the threshold, it uses neighbouring nodes. Malevolent nodes' controller disables their power when they cross the threshold. They cannot join other clusters because their IDs are in the public blockchain (Xiong et al., 2021). A node registered in an SDN controller's blockchain network is approved in another Multi controller SDN domain.

SDN Multi-controllers can grant private keys to nodes that fall below the threshold and are not on the blacklist. As long as the SDN Multi-controller's public keys are in the block it can migrate between clusters of IoT devices. The proposed algorithm for increasing SDN domain security while minimising energy usage is presented in Algorithm 1 (Abbassi et al., 2022). The SDN controller improves the efficiency of IoT devices and allows them to perform a wide range of services. IoT devices can connect with two SDN domains using the controllers proposed. The controller creates a safe network using blockchain technology and peer-to-peer (P2P) communication. IP addresses, public and private keys, as well as energy, are all contained within our system. The enforcement of device limits and the management of network transactions are the responsibilities of SDN Multi-controllers.

Algorithm 1 Energy consumption based security model

Parameter
M: object // M is the SDN Multi-controller
I: object // I is a IoT Systems
IoT Sensors
P: Power Consumption
Private Key1, Public key 2
IoT sensors group (Group of IoT devices, IP Address list)
Public and Private Blockchain
Energy limit
IoT System (IP address, List of group address)
Function: Monitoring by Multi-controller SDN blockchain coordinator
Function: Calculating Power & Attacks in IoT (Spam, Group of address list)
Swap to IoT system
Routing
START
A→ this
Message → collect ()
IoT System Rejester
Group of Authentication = Public Blockchain.
Monitor= Controlling by multiSDN blocklist
Activity = Calculating Power and Attacks IoT
If (IP =Normal or Attacks) then
IP= Spam.addressgroup Position
Else if (Power_IP >th) Position
Else
IP=Swap IoT System
If (I. Rejaster (public key1, private key 2, Message))
Private_ Blockchain traditional (address: message)
Stop

6 Results and discussions

Section 4 performed the Figure 5 shows the blockchain-based secure multicontroller infrastructure. Section 5 Simulate proposed architecture's throughput, performance,

and power efficiency. We compare simulation and analysis results.

6.1 The performance calculations are used to assess BMC-performance SDN's in this category:

a *Execution time*: It denotes by $Time_{Total}$ 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.

$$Time_{Total} = T_{Consensus} + T_{Sent} + T_{Update} \quad (2)$$

b *Detection rate* (*DR*)*:* This is the number of threats multiplied by the number of attacks.

c *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 (Boukria et al., 2019) as portrayed inflows are identified as malicious in Figures 7 and 8 and notified to the admin by creating a record to the logs giving information of the identified anomaly Table 1 shows the prediction accuracy vs. the number of injected threats. As seen in Tables 2 and 3 and Figure 10 and, MC-SDNBC provides a detection rate of 100%, meaning that all injected threats were effectively recognised in the system. The duplicate devices have seen the same internet also as a control system, The fake flow supplied also by masters be 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 Figure 10 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 R_i 0 : 8 and the fading ratio is large (i.e., = 0 : 8), the fading component slowly diminishes. If R_i is 0 : 8, it declines at a faster rate, resulting in a shorter trace level.

6.2 Power consumption and security performance analysis

We describe the architecture's implementation, testing environment, and performance, Power Consumption and throughput,. We implemented the SDN Multicontroller domain using the mininet wireless network simulator and the open daylight Multi-controller. The pyethereum simulated program within the Ethereum platform has been used to build the ledger components (Rajesh et al., 2018).

Table 1 No. of attacks vs. 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

Table 2 No. of switches vs. executions 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

Table 3 No of hosts vs. execution time

Total No. of switches	*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

Figure 10(a) Number of switches vs. execution time (see online version for colours)

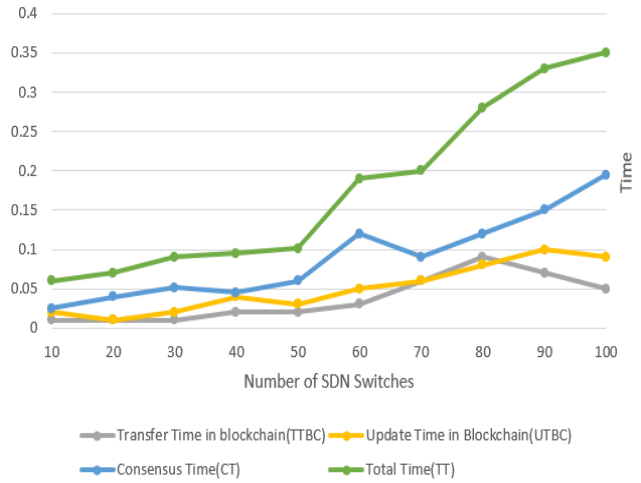


Figure 10(b) No. of hosts vs. execution time (see online version for colours)

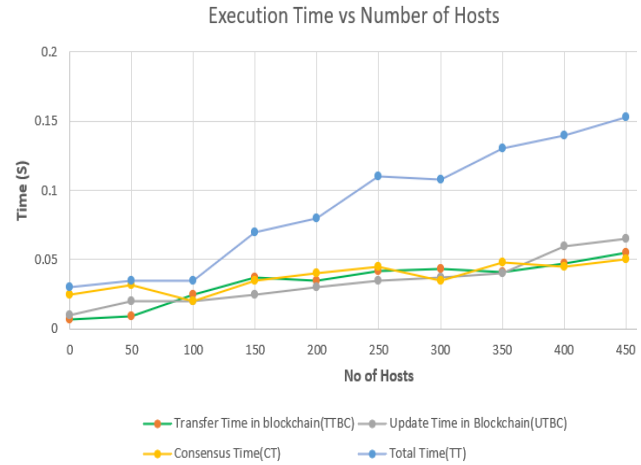
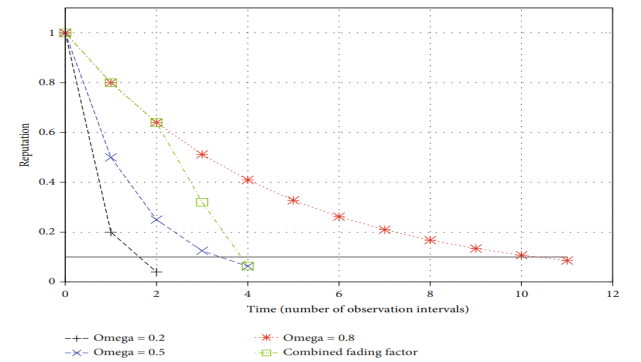


Figure 10(c) Detection time of reputation mechanism (see online version for colours)

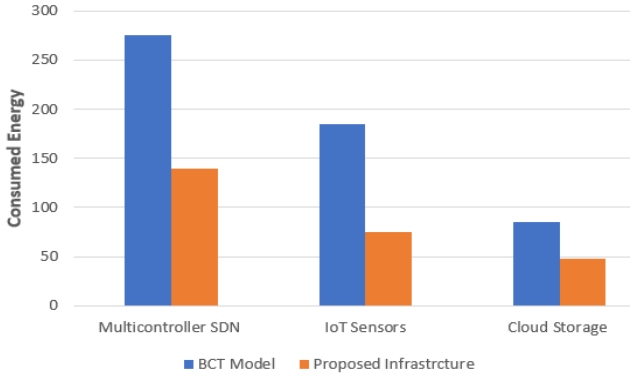


SDN domains can be created in a VM with distinct IP addresses and Mininet WIFI. Open Daylight was joined to this SDN topology via a remote connection. There are eight clusters in the simulation tool, and each cluster has a head connected to an IoT system. For each cluster, there are 15 Node IoTs that can be relocated to other clusters if there is an interconnection latency or a reduced power. The greatest speed of IoT nodes that we can mimic is 10 m/s. The cloud architecture of the open daylight controller was utilised so that blockchains, data, and block retrievals can be stored. Simulate another scenario compared the proposed architecture's overhead (Figures 11 and 12). We have been using Blockchain Fundamental's hashing and POW. Blockchain traditional (BCT) ignores IoT device and cluster limitations. POW costs IoT devices energy and time. Our open daylight controller architecture uses the routing protocol described in the previous chapter 5 to minimise IoT devices' energy usage. A total of 3000 transactions were generated during the simulation's 300 s of running time, resulting in an average of 10 simulations. Throughput, time overhead, power consumption, packet header overload, response time and were some of the measures considered in this study. Listed in Table 4 are the simulation parameters employed.

Table 4 Simulation IoT infrastrcture parameters

Parameter	*Values*
Simulator	mininet/Ethereum
No. of MultiSDN blockchain	8
No. of IoT sensors	100
No. of MultiSDN domain	8
Simulation time	300 s
Traffic type	Constant Rate
Mac protocol	802.11
Environment setup	1250 × 1250 m
Energy value	10–20 j
Antenna type	Omni Antenna
Size of packet	512 Byte

Figure 11 Power saving of the BCT model with proposed infrastructure (see online version for colours)



Using the simulation results as a guide, the suggested routing protocol will be evaluated. It is listed in Table 4 the simulation parameters that were used in the experiment. Comparisons of throughput and end-to-end delays are shown in Figure 13. According to our results, we have achieved 97% accuracy in terms of throughput, Power, end-to-end delay. As a consequence of this, our analytical model is validated by the outcomes.

Figure 12 Time overhead BCT model with proposed infrastructure (see online version for colours)

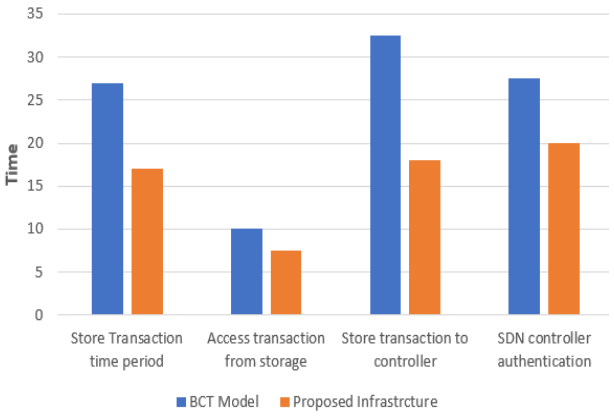
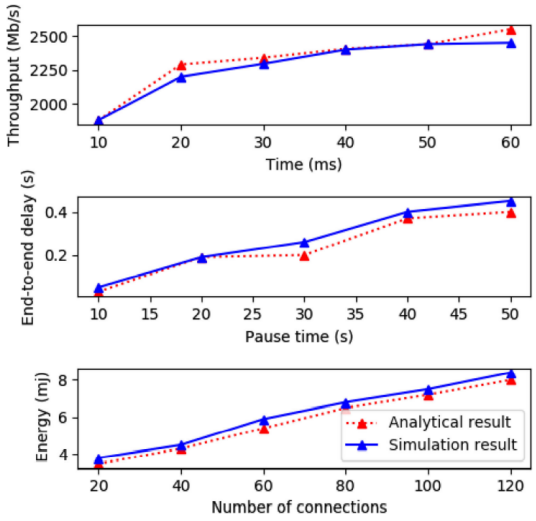


Figure 13 Analytical evaluation and simulation results (see online version for colours)



7 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 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 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. Since MC-SDNBC only focuses at east-west linkages, it reduced energy usage and increased IoT device communication security by using a routing protocol developed for IoT devices in the multi-controller SDN blockchain. Using IoT routing protocol, this was accomplished. In addition, excluding POW from the combination helped us achieve this impact. Our architecture outperforms BCT in bandwidth, efficiency, and energy grid. While also giving a better routing protocol.we aim to address the remainder of the security layers of SDN architecture in future work, particularly the southbound interface.

References

Abbassi, Y. and Benlahmer, H. (2022) 'BCSDN-IoT: towards an IoT security architecture based on SDN and blockchain', *International Journal of Electrical and Computer Engineering Systems*, Vol. 13, No. 2, pp.155–163.

Al-Sakran, H., Alharbi, Y. and Serguievskaia, I. (2019) 'Framework architecture for securing IoT using blockchain, smart contract and software defined network technologies', *2019 2nd International Conference on New Trends in Computing Sciences* (*ICTCS*), October, IEEE, pp.1–6.

Bhayo, J., Jafaq, R., Ahmed, A., Hameed, S. and Shah, S.A. (2021) 'A time-efficient approach towards DDoS attack detection in IoT network using SDN', *IEEE Internet of Things Journal*, Vol. 9, No. 5, pp.3612–3630.

Bhunia, S.S. and Gurusamy, M. (2017) 'Dynamic attack detection and mitigation in IoT using SDN', *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, November, IEEE, pp.1–6.

Boukria, S., Guerroumi, M. and Romdhani, I. (2019) 'BCFR: blockchain-based controller against false flow rule injection in SDN', *2019 IEEE Symposium on Computers and Communications (ISCC)*, June, IEEE, pp.1034–1039.

Chaganti, R., Bhushan, B. and Ravi, V. (2022) *The Role of Blockchain in* DDoS *Attacks Mitigation: Techniques, Open Challenges And Future Directions*, ArXiv Preprint ArXiv: 2202.03617.

Hang, F., Xie, L., Guo, W., Lv, Y., Ou, W. and Shanthini, A. (2021) 'Pervasive hybrid two-stage fusion model of intelligent wireless network security threat perception', *International Journal of High Performance Systems Architecture*, Vol. 10, Nos. 3–4 pp.128–139.

Islam, M.J., Rahman, A., Kabir, S., Karim, M.R., Acharjee, U.K., Nasir, M.K., … and Mosavi, A. (2020) *Blockchain-SDN based Energy Optimized and Distributed Secure Architecture for IoTs in Smart Cities*.

Li, W., Wang, Y., Meng, W., Li, J. and Su, C. (2022) 'BlockCSDN: towards blockchain-based collaborative intrusion detection in software defined networking', *IEICE Transactions on Information and Systems*, Vol. 105, No. 2, pp.272–279.

Litoussi, M., Kannouf, N., El Makkaoui, K., Ezzati, A. and Fartitchou, M. (2020) 'IoT security: challenges and countermeasures', *Procedia Computer Science*, Vol. 177, pp.503–508.

Nair, J.M. and Pradeep, C. (2016) 'Intelligent selective modular redundancy for online fault detection of adders in International, FPGA', *Journal of High Performance Systems Architecture*, Vol. 6, No. 4, pp.213–221.

Pourvahab, M. and Ekbatanifard, G. (2019) 'An efficient forensics architecture in software-defined networking-IoT using blockchain technology', *IEEE Access*, Vol. 7, pp.99573–99588.

Rahman, A., Islam, M.J., Montieri, A., Nasir, M.K., Reza, M.M., Band, S.S., … and Mosavi, A. (2021) 'Smartblock-sdn: an optimized blockchain-sdn framework for resource management in IoT', *IEEE Access*, Vol. 9, pp.28361–28376.

Rahman, A., Islam, M.J., Rahman, Z., Reza, M.M., Anwar, A., Mahmud, M.P., … and Noor, R.M. (2020) 'Distb-condo: distributed blockchain-based IoT-SDN model for smart condominium', *IEEE Access*, Vol. 8, pp.209594–209609.

Rajesh, G., Krishna, C.V., Selvaraj, B.C., Karthik, S.R. and Sangaiah, A.K. (2018) 'Energy optimized cryptography for low power devices in internet of things', *International Journal of High Performance Systems Architecture*, Vol. 8, No. 3, pp.139–145.

Ramu, G., Mishra, Z., Singh, P. and Acharya, B. (2020) 'Performance optimised architectures of piccolo block cipher for low resource IoT applications', *International Journal of High Performance Systems Architecture*, Vol. 9, No. 1, pp.49–57.

Sarica, A.K. and Angin, P. (2020) 'Explainable security in SDN-based IoT networks', *Sensors*, Vol. 20, No. 24, p.7326.

Sharma, P.K., Singh, S., Jeong, Y.S. and Park, J.H. (2017) 'Distblocknet: A distributed blockchains-based secure SDN architecture for IoT networks', *IEEE Communications Magazine*, Vol. 55, No. 9, pp.78–85.

Shukla, N., Gandhi, C. and Choudhury, T. (2021) 'Leveraging blockchain and SDN for efficient and secure IoT network', *Blockchain Applications in IoT Ecosystem*, Springer, Cham, pp.151–166.

Sundriyal, V. and Sosonkina, M. (2017) 'Runtime power-aware energy-saving scheme for parallel applications', *International Journal of High Performance Systems Architecture*, Vol. 7, No. 3, pp.129–139.

Tselios, C., Politis, I. and Kotsopoulos, S. (2017) 'Enhancing SDN security for IoT-related deployments through blockchain', *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks* (*NFV-SDN*), November, IEEE, pp.303–308.

Wadhwa, S., Rani, S., Verma, S., Shafi, J. and Wozniak, M. (2022) 'Energy efficient consensus approach of blockchain for IoT networks with edge computing', *Sensors*, Vol. 22, No. 10, p.3733.

Xiong, A., Tian, H., He, W., Zhang, J., Meng, H., Guo, S., … and Kadoch, M. (2021) 'A distributed security SDN cluster architecture for smart grid based on blockchain technology', *Security and Communication Networks*, pp.1–9.

Yazdinejad, A., Parizi, R.M., Dehghantanha, A., Zhang, Q. and Choo, K.K.R. (2020) 'An energy-efficient SDN controller architecture for IoT networks with blockchain-based security', *IEEE Transactions on Services Computing*, Vol. 13, No. 4, pp.625–638.

Zaman, S., Kaiser, M.S., Khan, R.T. and Mahmud, M. (2020) 'Towards SDN and blockchain based IoT countermeasures: a survey', *2020 2nd International Conference on Sustainable Technologies for Industry 4*.0 (*STI*), December, IEEE.

Website

https://www.multichain.com/