Ingénierie des Systèmes d'Information
Vol. 29, No. 6, December, 2024, pp. 2265-2273
Journal homepage: http://iieta.org/journals/isi

Blockchain-Driven Enhancement of SDN Security in IoT-Related Scenarios

Osman Diriye Hussein[1*], Husein Osman Abdullahi[2], Abdikarim Abi Hassan[1]

[1] Department of Telecommunication Engineering, Faculty of Engineering, SIMAD University, Mogadishu JH09010, Somalia
[2] Department of Computer Science, Faculty of Computing, SIMAD University, Mogadishu JH09010, Somalia

Corresponding Author Email: osman@simad.edu.so

https://doi.org/10.18280/isi.290616

Received: 19 December 2023
Revised: 6 August 2024
Accepted: 14 September 2024
Available online: 25 December 2024

Keywords:
Software Defined Networking (SDN), cloud computing infrastructure, network security, blockchain technology, IoT

ABSTRACT

The major way of contact in today's landscape of interconnected global commercial activities occurs via cloud-based networks that transcend national, geographic, and jurisdictional barriers. Software Defined Networking (SDN), a developing networking architecture meant to ease policy enforcement and dynamic network reconfiguration, enables this seamless integration. Even with all the obvious advantages brought in by SDN, the problem of larger attack surface size compared to traditional networking infrastructures cannot be considered minor, particularly within the context of safety-critical applications. This problem gets even more exacerbated if SDN has to handle networking features relevant to the IoT. In particular, such deployments are more vulnerable to certain types of attacks. Added to that is the increasing need for inter-cloud communications in IoT applications, creating a nightmare from the security point of view. Furthermore, the number of connected nodes significantly complicates the situation and creates an overwhelming barrier toward monitoring all entities to prevent system degradation and service disruption. The paper aims to provide a general overview of frequent security challenges concerning SDN and IoT cloud integration, going deeper into the basic design concepts of the newly established paradigm called Blockchain, which could be considered a critical security aspect in each SDN or IoT application. Given the peculiar features of the paper, it proposes a Blockchain implementation solution to help nullify and minimize the various security issues which come about due to the convergence of SDN and IoT.

1. INTRODUCTION

Most online interaction today is dominated by various commercial networks that are based on cloud computing frameworks. These will be those networks that cross national, regional, and jurisdictional boundaries, defined by specific interfaces which offer optimal flexibility, scalability, expandability, and security for all stakeholders involved with them [1]. This recent optimization in network architecture is enabled by what is called Software Defined Networking-SDN. SDN seeks to reform the existing architecture by overturning the current vertical integration that segregates the control logic of the core network from its underlying routing and switching elements. The goals of this research include the development of a logically centralized controller to be used in dynamic network reconfiguration and simplify policy enforcement easily [2]. In an SDN architecture, the networking components act as packet for-warders according to pre-set policies that are established or altered in another and subsequently sent to the network edges by another controller. This method allows the network operators to change network topologies on the fly, bringing in a new era of flexibility and responsiveness. The management is centralized via the controller, which eliminates the need to access and change every individual device distributed across the network. In this way, improvements in networks can be affected within minutes, as such among other changes that may be necessary, therefore resolving problems almost instantaneously. This SDN agility translates to network configuration disruption in almost real time for operators who oversee huge cloud computing installations running several thousand data centers around the world. Even so, with all these obvious advantages, there are some critical roadblocks preventing this new networking design from outclassing more traditional alternatives in every way [3]. Major points against SDN are that any successful attack will have a greater impact after the controller is compromised, and the attack surface is extended compared to regular networking systems. The interesting quandary with SDN is whether it's better to see topologies of networking evolve in a positive way, or to see the uncomfortable threat surface rise [4]. One can argue that due care in the protection of the latter preserves the advantages of the former, but as this position paper will explain, it becomes even more necessary when new and exciting verticals and applications, such as IoT, come up to reconsider and address the security challenge in a holistic and creative manner. The study's remaining sections are arranged as follows: Section III addresses the supplementary security concerns. The implementations of IoT bring along, while Section II discusses some main security issues related to SDN networking. Section IV gives one the extended use case with an explanation of basic concepts of the Blockchain technology and its application for network security enhancement. The last

section, Section V, covers future implementation and research efforts.

Recent development in SDN and IoT security has been forcing massive changes in areas related to network management and security. Research on emerging challenges and solutions regarding these two areas has received a considerable amount of attention in recent years. For instance, the implementation of some particular security protocols intended for SDN environments has increased resistance against different types of attack vectors [1]. In a similar spirit, considered state-of-the-art IoT security techniques, focusing on sophisticated encryption techniques and decentralized trust frameworks [2]. Even so, some gaps persist in the way in which a few of these problems—including dynamic threat detection and response—remain under-addressed.

For instance, Kreutz et al. [3] pointed out the lapses in the current SDN security frameworks, which are not efficient enough to handle complex attack scenarios. Building on the work of these mentioned studies, our research focuses on the challenge of real-time threat detection in the context of Internet of Things networks. We propose a novel solution for such problems by integrating the dynamic threat detection methodology proposed by Athanasopoulos et al. [4]. The outcome of this work contributes to the ongoing discussion of SDN and IoT security with a more secure real-time threat monitoring system. Our results are put into perspective with these recent works, underlining their applicability and possible influence on the area.

2. INTERACTION BETWEEN SDN AND IOT SECURITY

2.1 Integration and interaction between SDN and IoT

This section explaining the relationship between SDN and IoT in real-world installations to improve the paper's coherence. This section examines the interactions between various technologies and the potential effects of their security flaws on one another.

2.2 Interaction in practical deployments

SDN and IoT in contemporary network architectures frequently coexist. SDN offers centralized management and control over network resources, whereas IoT comprises a large number of networked devices that produce and consume data. Improved scalability and more effective network management are possible outcomes of integrating SDN and IoT. But since flaws in one system can impact another, this integration also poses new security risks.

2.3 Impact of SDN security issues on IoT

Security issues SDN flaws, including issues with the data plane or SDN controller, can have an immediate effect on IoT implementations. For example, unapproved access to or alteration of IoT devices' data could result via a compromised SDN controller. For the IoT network as a whole to remain intact, SDN component security must be guaranteed.

2.4 Impact of IoT security issues on SDN

On the other hand, SDN operations may be affected by security vulnerabilities in IoT devices. For example, insecure Internet of Things (IoT) devices may launch assaults against the SDN infrastructure, such as Distributed Denial of Service (DDoS) assaults against the SDN controller or data plane. To protect the SDN environment, IoT security vulnerabilities must be addressed.

2.5 Bridging security measures

Security controls need to be incorporated into the SDN and IoT domains in order to handle these interactions. Putting in place thorough security protocols that address SDN and IoT components can aid in risk mitigation and improve network security as a whole. This entails putting in place strong access controls, guaranteeing secure communication connections, and routinely scanning for vulnerabilities.

3. SECURITY DILEMMAS IN SOFTWARE DEFINED NETWORKING (SDN) LANDSCAPE

Security concerns crop up as one of the key facets of assessment against the multi-dimensional backdrop of Software-Defined Networking. The concepts basically laying a premise for SDN stress the imperative need to have software in full control over network systems. This conceptual revolution consists of providing a single focal point for network intelligence residing in a separately identifiable entity termed as the controller. The controller is considered the most important building block within the architecture of SDN. This makes it play a key role in supervising and coordinating the network, hence fully implementing the software-defined paradigm. On the other hand, these design principles pose security challenges in the quest to maximize efficiency and flexibility; hence, careful evaluation is needed within a broader context of the SDN ecosystem. In order to strengthen the security posture of SDN environments, new solutions and strategic considerations are required due to the complex interplay between software-driven control and security concerns [5, 6]. SDN architecture's core principles highlight the necessity of complete software control over networks. The necessity of a single node—referred to as the controller—housing central network intelligence is emphasized by this rule. The key to navigating the intricate security conundrums that emerge in the dynamic, software-driven SDN environment is this centralized management mechanism. In addition to being in line with the fundamental tenets of SDN, the controller's centrality is essential in fortifying the network against possible security risks and offering a strong foundation for proactive security actions and reactions within the dynamic SDN ecosystem.

3.1 Application layer

The fundamental ideas of SDN architecture emphasize how important total software control over networks is. This rule highlights the need for a single node, called the controller, to house core network intelligence. This centralized management approach is crucial to negotiating the complex security puzzles that arise in the software-driven, dynamic SDN environment. The controller's centrality is crucial for protecting the network from potential security threats and providing a solid basis for proactive security actions and reactions within the dynamic SDN ecosystem, all while adhering to the core principles of SDNVectors (1) and (2), which represent the layers and their interactions inside the SDN framework, are used in Figure 1

to demonstrate these concepts. These vectors emphasize how crucial the controller is to overseeing network security and preserving the SDN ecosystem's general wellbeing. Vector 1 in this diagram identifies where the controller, again, is interacting with the data plane of the network to perform this configuration and management of network devices per the policies dictated by it. The communication between the controller and different applications or network services is depicted in Vector (2), which also shows how the controller adjusts to changing application needs and network conditions. To maximize network performance and guarantee that security regulations are implemented uniformly throughout the network, this dynamic interaction is necessary.

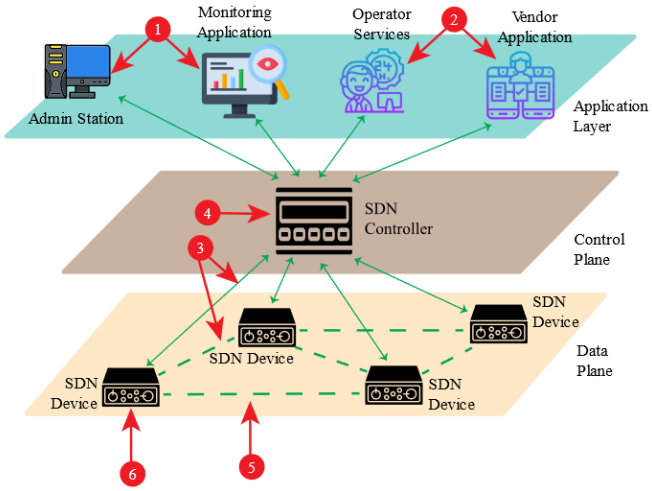


Figure 1. Possible exposed SD network connections

3.1.1 Control of unauthorized/unauthenticated availability

Attackers aim to compromise the critical operations of any networked SDN entity, including SDN administrative stations and poorly designed third-party apps installed in the top layer, and then manipulate the SDN controller for maximum network destruction. All SDN apps have the inherent privilege of connecting to the controller and having direct access to configuration methods and network resources, increasing the potential for brute force attacks [5], which were previously theoretically possible in traditional network systems. To mitigate emerging threats. This centralized control, while a significant advantage in terms of flexibility and scalability, introduces a single point of failure, making it crucial to design robust mechanisms for fault tolerance and security [6]. Recent advancements in software-defined networking (SDN) have emphasized the integration of machine learning algorithms to predict and prevent potential breaches before they occur. Any security weakness is regarded as potentially harmful since SDN networks can be rapidly updated from a single location [7]. Even though access control and application accountability provide significant security challenges, protocols requiring dual-factor authentication can be implemented to stop rogue nodes from independently launching attacks. Furthermore, once the attack has been stopped, several recovery techniques can be employed to return to a stable state

3.1.2 Incorrect net rule placing

Once compromised, the malicious or benign program may initiate to generate traffic, tamper with appropriate transmitting packets and signaling, which is or even attempt to enforce some flow rules fictitiously, targeting first its neighbors and then trying to reach the whole network of SDN. Besides, it is a difficult task to scan a program to ascertain if it is compromised in a safety way, especially third-party applications, which most of them are designed with other encapsulated applications running harmoniously as one application. A malicious program continually uses up the network resources without fail.

3.2 Sphere of authority

Strengthening the resistance of Considering the SDN control system versus possible threads as the key defense against such actions that might result in the attacker's full command over the main infrastructure of the network. Such examples include flawed or malicious software creating a security vulnerability by enabling the production of spurious traffic, loss of connectivity through the erasure of forwarding tables, controller reprogramming, reprogramming of the router or switch. Figure 1's vectors (3) and (4) show the most common control layer attacks.

3.2.1 DoS (Denial-of-Service) attacks involve

Given that control and data planes in this topology are designed to work independently of each other, the most critical type of threat involves DoS and DDoS on an SDN controller. The communication channel between these planes may be exploited by malicious attackers; hence, this design feature may easily be found vulnerable. Malicious flow traffic injected by an attacker could make a controller or other network entities unreachable to valid users. The network scanning application, which changes the response time of flows, as demonstrated by Shin and Gu [7], is a representative of this class of attack that discovers the underlying SDN nodes. Once the topology of the SDN network is determined, the attacker sends crafted flow demands across the Datapath to the controller. Thus, with an increase in the number of flows inside Datapath, more flow setup requests will be forwarded to the controller that can lead to an eventual service interruption to the controller. This kind of vulnerability can be exploited by DoS attacks by continuously sending IP packets with randomized headers to unblock the controller [8]. Another technique involves the transmission of signals to nodes in a network that are under-resourced, thereby highlighting the well-known weak point perspective that the strength of any given chain is only as strong as its weakest link. DDoS attacks targeting multiple controllers have been seen to trigger cascading failures; at the same time, it is suggested to implement multiple within the same network, independent SDN controllers [9, 10]. Consequently, employing an additional detection method becomes quite essential. In order to mitigate DDoS attacks, it suggests using several oligarchic trust models that rely on numerous trust-anchor verifying bodies. However, if new lightweight communication protocols with alternative orientations and scopes arise, or if the number of associated nodes surpasses a particular threshold, these approaches may become out of date.

3.2.2 Attacks against SDN controllers

That is one aspect of the specialized attack on the control layer in the SDN networking era. This was not possible in legacy networking, where no single central node could be compromised to act as a passage that might compromise all the nodes connected to it. Running third-party applications on the controller is the source of this vulnerability. The malicious

programs can then change the entire network as controllers provide only layers that allow the underlying infrastructure to receive configuration commands [11]. Replication strategies are countermeasures against these types of attacks because they can detect, stop, or isolate anomalous behavior. Such defenses include diverse infrastructures that can prevent single points of failure and procedures for restoring the system to a stable and dependable condition on a regular basis. But expanding the network to a big number of linked nodes could cause data or content loss, similar to DoS, especially when the controller needs a reboot quite frequently. Therefore, these types of deployments are unsuitable for industries or mission-critical applications that require constant gathering of data from a remote source.

3.3 The data layer

It achieves this by decoupling the data and control planes, whereby all forwarding devices, including routers, can act as basic packet handling elements remotely controllable through specialized interfaces. Such virtual reconfigurations of switches, routers, or access points are possible over a secure channel of communication flow-wise. The data plane can be programmed at fine granularity with remarkable freedom that is just restricted by the installed flow tables' capabilities. The data plane is more adaptable now that the control and data planes are separated, but there are still certain unique security challenges that need to be addressed within the otherwise dependable and straightforward data plane. Different vectors, as shown in Figure 1, engage the most common data plane attacks.

3.3.1 Flooding attacks and forged switch flow

For the deployment of flow rules on specific tables, the controller has to connect to the network switches via OpenFlow networks. Such deployment is done either reactively, whereby the installation of flow rules happens synchronously to the request by a host for initial packet handling, or proactively, prior to new hosts sending any ingress packets. In both approaches, switches store rules in finite, sometimes limited, numbers of flow tables. The key data plane security risk in the era of SDN is that switches are not intelligent enough and have not the decision-making capability to distinguish between malicious and valid flow rules. By making the switches simply basic forwarding nodes, they may get the chance to become the victim of forged flow rules [12]. Not only that, but even the buffer of the switch and all the spaces for storing rules could also be the target of the attacker. Since the data plane nodes do not have the capability to buffer unsolicited flows, saturation attacks are allowed. These attacks, much like the classical man-in-the-middle attack [13], involve a malicious intermediary node intercepting a valid communication channel and imposing its will within the network.

3.3.2 Issues with TLS and TCP

Due to the complexity in the configuration requirements the particular security of Transport Layer Security (TLS) [14], update has been implemented as an optional feature in the newer versions of OpenFlow [11]. The initial steps included creating separate certificates for the switches and controllers and then creating a certificate representing the site as a whole. These distinctive certificates were then distributed to all the nodes once they were signed by using the sitewide certificate. Because this tactic is the switches are now more vulnerable since they are no longer supported. On the other hand, the counter-argument against TLS in network security uses the proof that TCP protection is not guaranteed by its use. Because the plain-text TCP channel has no connectivity or authentication, the OpenFlow deployments are more vulnerable to man-in-the-middle attacks. In the present research work, basic security issues in SDN and IoT are elaborated separately. To enrich the discussion about SDN security problems, we will refer to certain attack scenarios, such as DDoS attacks against SDN controllers and MitM attacks against protocol vulnerabilities. These are going to be more extensive examples to support the present study and point out real-life relevance for the issues under discussion.

4. IOT SECURITY CONSIDERATIONS

Over the last few years, the Internet of Things has sufficiently acquired momentum to emerge as a paradigm change. Its foundation is the idea of a ubiquitous network, which links various devices with the ability to gather, compile, and analyze data despite the nodes' dispersed physical locations. Effective end-to-end communication should be able to be detected and facilitated by the heterogeneous combination across a broad spectrum of technologies. The IoT concept's fundamental strength is unquestionably its profound influence on a variety of facets of daily life as well as the personal and professional decisions made by its potential users. IoE would significantly expand upon IoT [15].

Many businesses considered IoT as the cornerstone of their digital strategy since it has a substantial impact on a wide range of technical domains, including architecture, network design, core business strategy, and risk management [16]. As of right present, no comprehensive integrated solution or commercial IoT platform is available. IoT remains an emerging field, characterized by unclear distinctions between products and technologies [17].

Businesses seeking shortcuts are reluctant to invest since researchers are attempting to develop applications with unclear protocols. Devices, operating systems, and underlying platforms in the Internet of Things (IoT) face an intriguing new set of security dangers and concerns for which traditional security solutions might not be effective.

The possibility that hostile activity could use an IoT node to infiltrate the entire infrastructure is another issue with this increased attack surface for any systems linked to one. The subsequent sections go into more depth about these security flaws that were recently discovered.

4.1 Unattended devices with limited resources

Most IoT nodes are physically distributed throughout the lifetimes of their operation and are made for unmanned operation. Therefore, they are susceptible to physical attacks, which the cybersecurity countermeasures of today's cloud computing architecture are incapable of facing. With many of the nodes serving special purposes and their energy efficiency and processing capacity greatly bound, it is highly probable that most of them lack the necessary resources for adequate self-defense.

Whatever the foreseen lifetime of the device, security cannot be an afterthought. For this reason, there should be a dedicated mechanism that enables hardware interventions, or

an interface that is specifically designed for software updates. As highlighted in the study by Francillon et al. [18], a major challenge lies in ensuring the efficient protection of a large number of resource-limited nodes.

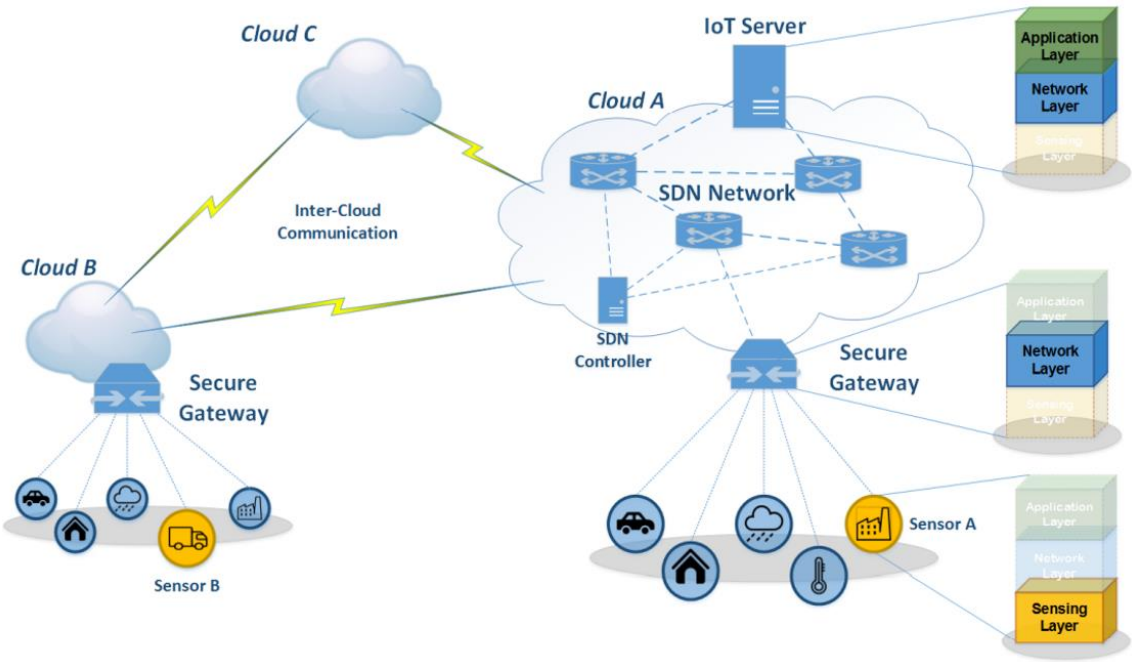


Figure 2. Blockchain-enabled secure IoT inter-cloud connectivity

4.2 Assessment of reliable security status

Large dispersed systems were specifically intended to be supported by the Internet of Things architecture. For instance, hundreds of deployed devices arranged into specific networked subsystems for tasks like data gathering, content aggregation, and monitoring could be found in a smart city. Any governing authority must therefore be able to consistently confirm if such a vast number of entities are operating as intended. Traditional cloud computing techniques, such as authentication protocols requiring nodes to employ cryptographic methods for trust verification through a remote authenticator [19], are anticipated to struggle with addressing both transparencies demands and operational efficiency simultaneously. Furthermore, a lot of devices with limited resources can find it difficult to handle the computationally demanding task of ciphertext creation. Even in the event that they do, the sheer quantity of these devices poses a significant administrative challenge in addition to unaffordable high expenses of the distributed network controller or cloud authority in charge of these tasks. Last but not least, when handling real-world problems, it is crucial to confirm that equipment installed years ago—possibly by different suppliers—has not been hacked in the past.

4.3 Appropriate response to security breaches

The majority of incident response techniques used today rely on coercive procedures that force a reboot of a possibly compromised system in order to restore its software to a secure state, which affects all related subsystems simultaneously. IoT is expected to play a significant role in mission-critical systems, however these systems are unfortunately not well suited for such highly disruptive responses. Rebooting is simply not an option in applications where continuous operation is essential, like e-Health, smart cities, intelligent transportation systems, manufacturing facilities, and vehicle-to-vehicle (V2V) communications [20]. Passengers in a moving car are at risk when a vital sensor is activated, and stopping a big power generator is more harmful than keeping it running continuously and implementing the required preventative measures during planned maintenance intervals.

Addressing security challenges is required for major organizations to embrace IoT technologies on a widespread scale. Concentrating the technological gaps between existing cloud computing and the emerging IoT paradigm necessitates a new architecture that heavily relies on SDN to manage its complex networking infrastructure while bringing processing, management, and storage capabilities closer to end-user devices.

Figure 2 shows the architecture, which highlights the features of each subsystem as well as the intercloud connectivity required to connect multiple installations. Any cloud deployment with native IoT capability has three main components: the SDN Network, the IoT Application Server (also known as the IoT Server), which runs the primary IoT application, and the recently proposed Secure Gateway node [21]. The latter can link to sensors anywhere in the topological view as long as a communication connection is constantly active, providing for consistent and continuous data flow. As shown in Figure 2, the sensors, Secure Gateway, and IoT Server can manage all three layers—application, networking, and sensing. However, some levels are necessary for basic node and subsystem operation. Before being sent to SDN Network nodes, every sensor and IoT Server communication goes via the Secure Gateway.

Being the platform's initial line of defense and ensuring package validity, the Secure Gateway regulates incoming traffic. Message flows that pass through the Secure Gateway are handled as though they are benign. Following industry standards, the SDN Controller manages connectivity with nearby clouds. The idea of using a Secure Gateway to examine

packages targeted at sensors depends on this node's capacity to verify the legitimacy of incoming data. The majority of IoT security issues still exist, however this is where the recently developed Blockchain technology excels.

5. INFLUENCE OF BLOCKCHAIN TECHNOLOGY ON TRANSACTION

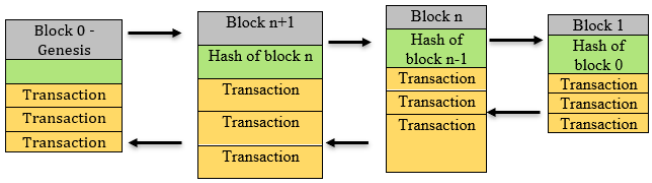


Figure 3. Blockchain transaction

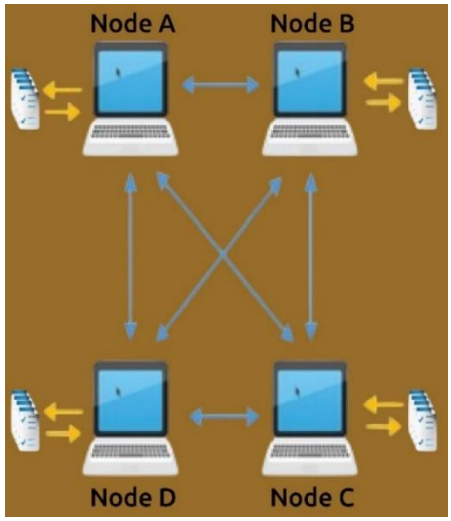
In recent times, blockchain technology has drawn attention from a variety of sectors, including businesses, public and private organizations, and industries, as a developing method for quick transaction verification. Beyond its current use, this disruptive technology has a wide range of potential applications across all domains that need to move away from a centrally authorized authority serving as a reliable go-between or, sporadically, a third-party confirmed trust anchor. The evolution has led to the deployment of a purely distributed authentication architecture, indicating a paradigm shift in the way trust and authentication are handled to established in a variety of applications. Blockchain is positioned as a flexible and significant solution with broad implications for a decentralized and secure future in a variety of fields due to its revolutionary power.

A chain of ledgers is a distributed, immutable, and decentralized data structure that is copied by network members. This data structure functions as a log, with items (or blocks) grouped into timestamped entries that can be uniquely identified by a cryptographic hash [22]. The hash is calculated using the block's text, or header, and a piece of the entire transaction record created by all connecting nodes with permitted system access.

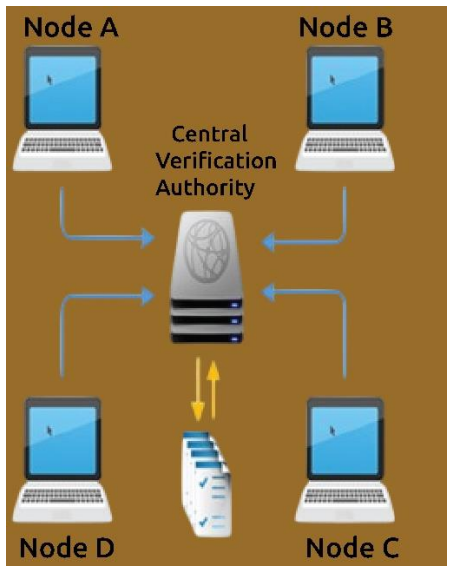
It also contains a reference to the hash of the previous blocks, as seen in Figure 3, forming the blockchain, a continuous chain. Every client with access to the blockchain network receives the first block in this chain, known as Genesis, which is a little different and serves as a "key" to the encrypted data stored on the blockchain. By using this procedure and explicitly asking nearby nodes for complementary blockchain snapshots, every node acquires the ability to comprehend the whole set of facts included in the overall data structure.

To fully appreciate blockchain's benefits and its role in the Internet of Things ecosystem, one must first grasp the key differences between distributed and centralized ledgers. In the centralized ledger architecture shown in Figure 4 transactions must be settled by a Central Verification Authority, which also needs several intermediaries to ensure transaction integrity.

The ledger can be edited by anybody who has access to it, and transaction data is vulnerable to assaults because a single security flaw might jeopardize the system's integrity. On the other hand, transactions can settle instantly utilizing the distributed ledger technology, eliminating the need for middlemen to verify their legality. Every transaction occurs in real time and is transparent to all parties involved, and once recorded in the blockchain, each block is time and data stamped to ensure immutability. This research emphasizes the synergy between blockchain technology and machine learning-based intrusion detection systems. This integration is designed to fortify IoT botnets and cloud networks against sophisticated security threats, demonstrating significant potential in enhancing IoT ecosystem security [23].



(1) Centralized ledger



(2) Distributed ledger

Figure 4. Varieties of ledgers

Using blockchain as the main distributed repository in the system, authorized nodes can immediately trace and verify specific quantities or the total number of sources as data from IoT devices is recorded onto the structure. By definition, the intrinsic resilience of an encrypted distributed database derives from the absence of a single point of failure. Blockchains, upon creation, cannot be tampered with or corrupted. Theoretically proven methods help to continuously verify and calibrate the legitimacy of the blockchain by indicating any attempted alterations. This study proposes a new, highly secured, self-powered IoT platform for smart agriculture. It will effectively address the issues of power consumption and security, so the platform can be one of the viable solutions for sustainable agricultural IoT applications [24]. This functionality means efforts at data tampering would be prevented because rogue nodes would need to decode any

information from the blockchain, you must first obtain the Genesis block. This is a highly uncommon process.

Having said that, Figure 2 now makes more sense to embed a blockchain-based security layer in the architecture. In a cloud setup, all sensors and networked nodes can access the Genesis block, which streamlines the authentication process for the Secure Gateway by generating immutable blocks and updating the existing blockchain. By just looking at the most recent blocks of it, a message can easily be determined as benevolent, part of the related blockchain.

A copy of the required Genesis block will provide access to a neighboring cloud implementation; thus, it improves inter-cloud communication. Due to this transparency, the IoT server in Cloud A can access data from Cloud B's sensor B, as blockchain establishes trustless networks outlined in the study (Figure 2).

The research studies the Sybil attack detection in Vehicular Ad Hoc Networks (VANETs) by the use of machine learning. The proposed scheme enhances security levels by efficiently identifying malicious nodes, thus enabling reliable communication in vehicular networks [25].

6. TECHNICAL IMPLEMENTATIONS

This study has improved network security and management by implementing a number of cutting-edge ideas and techniques into our strategy. Utilizing blockchain technology, which offers a decentralized and impenetrable record for network transactions and configurations, is one of the fundamental components of our implementation.

6.1 Blockchain technology in network configurations

Network settings' authenticity and integrity are guaranteed by the use of blockchain technology. Every modification to the network configuration in our suggested approach is documented on a blockchain ledger. The following steps are involved in this process:

- **Transaction Recording:** Every time a configuration modification is suggested, the blockchain records it as a transaction. The type of configuration modification, the timestamp, and the identity of the entity making the change are among the details included in this transaction.
- **Consensus Mechanism:** To make sure the transaction is legitimate, it passes through a consensus procedure. In our system, the transactions are validated by trusted entities through a Proof of Authority (PoA) consensus method.
- **Immutable Ledger:** A transaction is added to the blockchain as a new block as soon as it is verified. This guarantees an unchangeable and impenetrable configuration history, offering a clear documentation of all modifications.

6.2 Integration with SDN management software

It utilizes the following strategy to incorporate blockchain technology with the current SDN management software:

- **API Integration:** It creates an API that links the blockchain network and the SDN management software. Through the use of this API, the SDN controller can communicate with the blockchain by submitting new transactions and retrieving configuration records.
- **Smart Contracts:** On the blockchain, smart contracts are used to automate specific network management tasks. For example, a smart contract may be set up to automatically enforce network access regulations in response to configuration changes that are tracked on the blockchain.
- **Data Synchronization:** To ensure that both the blockchain network and the SDN controller are using the most recent configuration data, they are synchronized. Data integrity is ensured and discrepancies are handled by implementing data synchronization mechanisms.

6.3 Practical example

Imagine a situation where firewall rules need to be updated by a network administrator. In our implementation,

A. The SDN controller receives the suggested modification. B. The modification is entered onto the blockchain as a transaction by the SDN controller. C. The blockchain network verifies the transaction before adding it to the ledger. D. Based on the verified transaction; a smart contract automatically modifies the firewall rules in the SDN management software. Consumers get a better understanding of how SDN management software and blockchain technology interact in real-world scenarios by going over these technical implementations in depth. This method automates network management activities, improves network security, and offers a clear record of configuration changes.

This paper suggests applying blockchain technology to improve security in SDN and IoT. Blockchain ensures tamper-proof and transparent records of all changes by storing network configurations on a decentralized ledger, hence securing SDN. Through decentralized processes, it offers safe data exchanges and authentication for the Internet of Things. The implementation entails leveraging smart contracts to enforce policies and integrating blockchain with SDN controllers via APIs. Blockchain guarantees data integrity and transparency, which enhances security. However, it may also present issues with scalability and processing speed, which must be resolved to maximize performance in practical implementations.

7. BLOCKCHAIN TECHNOLOGY FOR SDN AND IOT SECURITY

An overview of how blockchain technology might improve SDN and IoT ecosystem security is given in this section. We will now go into more detail on particular implementation strategies and technical specifics to provide a more thorough understanding:

Integration with SDN Controllers: SDN controllers and blockchain can operate together to protect network configuration integrity. In order to facilitate communication between the SDN controller and the blockchain network, APIs are used. For instance, a suggested configuration change is documented on the blockchain as a transaction. After that, this transaction is verified by a consensus method to make sure that only approved modifications are performed before it is implemented.

Smart Contracts for Policy Enforcement: The blockchain's smart contracts have the ability to automate policy enforcement. A smart contract might be designed to, among other things, automatically update access control lists or firewall rules in response to verified transactions. This guarantees that security measures are applied consistently

throughout the network and lowers the possibility of human error.

Blockchain in IoT Security: Blockchain can be used in Internet of Things contexts to govern access control and secure data exchanges. A blockchain ledger may record every data packet or device interaction, producing a verifiable audit trail. Only authorized devices can access the network thanks to decentralized authentication techniques. Installing thin blockchain nodes on Internet of Things (IoT) devices or interacting with the blockchain through intermediary gateways are two methods of integration.

Technical Challenges and Solutions: Scalability and processing speed are two of the issues that come with implementing blockchain technology. We advise utilizing scalable blockchain systems or Layer 2 solutions like state channels to handle scalability. Transaction throughput can be increased while preserving security by optimizing consensus procedures, such as Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT).

It has shed light on how blockchain technology might be used to improve security in SDN and IoT systems by outlining these particular implementation options and technical issues.

8. CONCLUSION AND FUTURE DIRECTIONS

The main conclusions of our study on leveraging blockchain technology to improve SDN and IoT security are succinctly outlined in the conclusion. We will now provide particular planning and feasibility assessments for potential future research directions to better enrich this section.

8.1 Future research directions

Integration and Optimization: Optimizing the integration of blockchain technology with SDN and IoT systems should be the main focus of future research. In order to overcome the performance and scalability difficulties found in our study, this involves investigating sophisticated consensus methods and scalable blockchain topologies.

8.2 Case studies and pilot projects

Insights into the real-world obstacles and efficacy of blockchain-based security solutions can be gained by putting pilot projects and case studies into practice. These investigations can aid in improving implementation tactics and validating our suggested models.

8.3 Interoperability and standards

It is essential to create standards and interoperability frameworks for blockchain integration with various SDN and IoT platforms. In order to guarantee smooth integration and interoperability, research in this field should concentrate on developing standard protocols and interfaces.

8.4 Feasibility analysis

8.4.1 Technical feasibility

Evaluating today's state of blockchain technology, their compatibility with current SDN and IoT systems, and determining required modifications or enhancements are all part of the technical feasibility analysis of integrating blockchain solutions.

8.4.2 Cost-benefit analysis

Finding the financial feasibility of implementing blockchain technology can be aided by performing a cost-benefit analysis. The expenses of blockchain infrastructure, possible cost savings from enhanced security, and the total return on investment should all be considered in this analysis.

8.4.3 Regulatory and ethical considerations

Future studies ought to focus on the moral and legal implications of blockchain implementation. The effective implementation of blockchain technology will depend on resolving ethical issues and ensuring adherence to data protection laws.

The important security concerns surrounding the Internet of Things (IoT) and Software Defined Networking (SDN) integration in cloud-based systems are the main topic of this essay. Cloud network integration has become a mainstay of global business, but innovative security solutions are needed due to the hazards posed by SDN, especially when it comes to applications that are vital to safety. This study explores the fundamental ideas behind Blockchain technology design and recommends using it as a vital security element in SDN and Internet of Things applications. The security challenges of the SDN ecosystem are explored in detail, exposing the wider attack surface and possible threats at multiple levels, including the data, control, and application layers.

The intricate relationship between security concerns and software-driven control emphasizes how crucial it is to find tactical ways to strengthen SDN systems. The Internet of Things brings with it new security considerations due to the proliferation of resource-constrained devices and the challenge of maintaining the security of devices that were deployed years ago. The study emphasizes the need for an efficient response to security breaches in IoT applications given the impracticality of conventional incident response strategies, such as system reboots, in mission-critical situations. A Based on blockchain technology reliability layer is included in the recommended design, which is depicted in Figure 2, to improve the security of Internet of Things deployments in cloud-based environments. The recently developed method addresses the security flaws that have been raised by utilizing the immutability, decentralization, and cryptographic verification of Blockchain technology.

Secure communication between numerous cloud deployments is made possible by Blockchain's trustless network features, while the Secure Gateway verifies the legitimacy of sensor-oriented packages. Examined is the effect of Blockchain technology on transaction verification, with a focus on its possible applications in various industries. The article outlines a blockchain's characteristics, highlighting its use as an immutable, decentralized data system. By incorporating Blockchain technology into the suggested design, the security issues related to distributed systems are resolved by giving authorized nodes a reliable means of monitoring and validating data produced by Internet of Things devices.

The adoption of Blockchain technology is suggested in the study as a revolutionary means of resolving security concerns in the intersection of SDN and IoT. The proposed architecture adopts a proactive stance that aligns with the evolving network of interconnected technologies, establishing the foundation for safe and effective cloud-based software. It is suggested that future study and implementation efforts expand upon and deepen the aforementioned concepts.

REFERENCES

[1] Tsagkaropoulos, M., Politis, I., Tselios, C., Dagiuklas, T., Kotsopoulos, S. (2011). Service continuity over intertechnology RATs. In 2011 IEEE 16th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Kyoto, Japan, pp. 117-121. https://doi.org/10.1109/CAMAD.2011.5941098

[2] Kreutz, D., Ramos, F.M., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S. (2014). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1): 14-76. https://doi.org/10.1109/JPROC.2014.2371999

[3] Kreutz, D., Ramos, F.M., Verissimo, P. (2013). Towards secure and dependable software-defined networks. In Proceedings of the second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, United States, pp. 55-60. https://doi.org/10.1145/2491185.2491199

[4] Athanasopoulos, D., Politis, I., Lykourgiotis, A., Tselios, C., Dagiuklas, T. (2016). End-to-end quality aware optimization for multimedia clouds. In 2016 International Conference on Telecommunications and Multimedia (TEMU), Heraklion, Greece, pp. 1-5. https://doi.org/10.1109/TEMU.2016.7551931

[5] Tselios, C., Birkos, K., Galiotos, P., Kotsopoulos, S., Dagiuklas, T. (2012). Malicious threats and novel security extensions in P2PSIP. In 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, Lugano, Switzerland, pp. 746-751. https://doi.org/10.1109/PerComW.2012.6197612

[6] Scott-Hayward, S., Natarajan, S., Sezer, S. (2015). A survey of security in software defined networks. IEEE Communications Surveys & Tutorials, 18(1): 623-654. https://doi.org/10.1109/COMST.2015.2453114

[7] Shin, S., Gu, G. (2013). Attacking software-defined networks: A first feasibility study. In Proceedings of the second ACM SIGCOMM workshop on Hot Topics in Software Defined Networking, United States, pp. 165-166. https://doi.org/10.1145/2491185.2491220

[8] Fonseca, P., Bennesby, R., Mota, E., Passito, A. (2012). A replication component for resilient OpenFlow-based networking. In 2012 IEEE Network Operations and Management Symposium, Maui, HI, USA, pp. 933-939. https://doi.org/10.1109/NOMS.2012.6212011

[9] Yao, G., Bi, J., Guo, L. (2013). On the cascading failures of multi-controllers in software defined networks. In 2013 21st IEEE International Conference on Network Protocols (ICNP), Goettingen, Germany, pp. 1-2. https://doi.org/10.1109/ICNP.2013.6733624

[10] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Turner, J. (2008). OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Computer Communication Review, 38(2): 69-74. https://doi.org/10.1145/1355734.1355746

[11] Ahmad, I., Namal, S., Ylianttila, M., Gurtov, A. (2015). Security in software defined networks: A survey. IEEE Communications Surveys & Tutorials, 17(4): 2317-2346. https://doi.org/10.1109/COMST.2015.2474118

[12] Callegati, F., Cerroni, W., Ramilli, M. (2009). Man-in-the-middle attack to the HTTPS protocol. IEEE Security & Privacy, 7(1): 78-81. https://doi.org/10.1109/MSP.2009.12

[13] Dierks, T., Rescorla, E. (2008). The transport layer security (TLS) protocol version 1.2 (No. rfc5246). https://www.rfc-editor.org/rfc/rfc5246.

[14] Liyanage, M., Gurtov, A. (2012). Secured VPN models for LTE backhaul networks. In 2012 IEEE Vehicular Technology Conference (VTC Fall), Quebec City, QC, Canada, pp. 1-5. https://doi.org/10.1109/VTCFall.2012.6399037

[15] Atzori, L., Iera, A., Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[16] Gartner Inc. (2018). Gartner Identifies the Top 10 IoT Technologies for 2017 and 2018. http://www.gartner.com/newsroom/id/3221818.

[17] Chiang, M., Zhang, T. (2016). Fog and IoT: An overview of research opportunities. IEEE Internet of Things Journal, 3(6): 854-864. https://doi.org/10.1109/JIOT.2016.2584538

[18] Francillon, A., Nguyen, Q., Rasmussen, K.B., Tsudik, G. (2014). A minimalist approach to remote attestation. In 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, Germany, pp. 1-6. https://doi.org/10.7873/DATE.2014.257

[19] Christidis, K., Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4: 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

[20] Tselios, C., Tsolis, G. (2016). On QoE-awareness through virtualized probes in 5G networks. In 2016 IEEE 21st International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), Toronto, ON, Canada, pp. 159-164. https://doi.org/10.1109/CAMAD.2016.7790351

[21] Hussein, O.D., Osman, H. (2024). IoT-based air quality management in Somalia. International Journal of Electronics and Communication Engineering, 11(3): 77-86. https://doi.org/10.14445/23488549/IJECE-V11I3P108

[22] Muhudin, A., Mondal, J., Dash, S., Hussein, O.D., Osoble, A.M. (2024). Advanced privacy-preserving rdh scheme for encrypting sensitive images: A two-level LSB embedding strategy. International Journal of Electronics and Communication Engineering, 11(4): 34-40. https://doi.org/10.14445/23488549/IJECE-V11I4P104

[23] Siddamsetti, S., Srivenkatesh, M. (2022). Implementation of blockchain with machine learning intrusion detection system for defending IoT botnet and cloud networks. Ingénierie des Systèmes d'Information, 27(6): 1029-1038. https://doi.org/10.18280/isi.270620

[24] Mohammad, M.T., Mahmood, H.A., Ali, Q.I. (2023). A self-powered IoT platform with security mechanisms for smart agriculture. Ingénierie des Systèmes d'Information, 28(6): 1525-1532. https://doi.org/10.18280/isi.280609

[25] Kakulla, S., Malladi, S. (2022). Sybil attack detection in VANET using machine learning approach. Ingénierie des Systèmes d'Information, 27(4): 605-611. https://doi.org/10.18280/isi.270410