LOAD BALANCED ATTACK DEFENSE SYSTEM WITH LIGHTWEIGHT AUTHENTICATION AND MODIFIED BLOCKCHAIN IN SDN FOR B5G

Ihsan H. Abdulqadder [1] and Israa T. Aziz [2]

[1] Department of Computer Science, University of Kirkuk, Kirkuk, Iraq
[2] Computer Center, University of Mosul, Mosul, Iraq

ABSTRACT

The involvement of unauthorized packets in Software Defined Networks (SDN) has raised the demand for security. These days, users can access the Internet of Things (IoT) wirelessly over long distances with the use of mobility, and handover. Due to changes in connectivity, the mobility feature is the main reason to permit unauthorized packets. This article uses handover authentication and a modified blockchain to overcome the security issue named LLModBloc. The 5G users are initially authenticated by the edge layer access points (APs) using a hash produced by the lightweight QUARK algorithm using identity and pseudo-ID. The likelihood determines the user's handover if there are too many users connecting to the same AP. A directed acyclic graph (DAC), Harris Hawks Optimization (HHO), and two-level packet based on hexa-features are used in this work. Based on packet characteristics, the capsule network initially divides packets into three categories: normal, suspect, and malicious. Suspicious packets are analyzed using user behavior features and a Q-learning algorithm. Many packets and behavior features were examined. The proposed LLModBlocare evaluated in several metrics such as packet loss, processing time, response time, bandwidth, and latency.The results demonstrate the effectiveness of the proposed system, showing that it outperforms other approaches in terms of network-specific parameters.

KEYWORDS

Packet classification, SDN, Blockchain, Handover authentication, Lightweight Hashing, 5G

1. INTRODUCTION

By employing 5G and beyond for ubiquitous connection, the expansion of wireless communication makes it possible to reach a vast number of consumers. Network management is necessary for diverse networks, which 5G supports [1,2]. Additionally, a crucial problem for effective network management has been resolved. In addition to supporting handover, these 5G capabilities enable access for a vast number of users. 5G is combined with Software Defined Network (SDN) to help respond to all of the incoming queries. [3,4]. As a result of the dynamic users, the received signal strength (RSS) varies and is farther away or moves closer from the access. The user with weak RSS must switch over from the existing link. Blockchain-based user privacy is one of the security needs that the 5G focuses on achieving. Because 5G users are unstable and have limited computing power, lightweight techniques are used for security. Security and latency reduction are guaranteed by this combination [5,6].

Mobile edge computing (MEC) and SDN are required to Build a robust 5G network communication [7,8]. Regarding network management flexibility, MFC, network function virtualization (NFV), and SDN are offered in the 5G and beyond network. The privacy needs in such a mix of network technologies are important. Blockchain technology, intrusion detection, factors-based authentication, and lightweight cryptography are the main security solutions [9,10].

Blockchain has emerged as a viable security option in recent years. Support for an increasing number of records is made possible by blockchain technology, which builds a chain of blocks. The purpose of this blockchain is to counteract fraudulent flows that come from 5G consumers. Additionally, the use of blockchain guarantees a decrease in the frequency of denial of service (DoS) and distributed denial of service (DDoS) assaults as well as unauthorized access [11,12]. Network performance will be destroyed by the attackers because of increased latency, resource shortages, and other factors. To identify anomalous network flows, the incoming packet_in messages are examined using the packet features.

When creating a secure system, a multi-controller SDN design is desirable since single controllers in SDN have the potential to fail [13, 14]. After being collected at edge devices, the incoming packets from 5G-IoT users are sent to the switch. Packet flows must be matched in the SDN core network by OpenFlow Switches. The packet_in will be sent straight to the controller for examination if it is a new flow. Multi-controller SDN is appropriate for large-scale network settings because if an attacker joins, there will be numerous mismatched flows, which means using a single controller will fail. SDN controllers handle flow analysis to identify both normal and abnormal flow.

This study designs a 5G-SDN with MEC that only permits 5G users after authentication. There is some unusual packet flow from genuine users even when the users are authenticated. According to a report, hacked users are the main way that DDoS attack packets get into networks. As a result, to distinguish between normal and aberrant packets, the arrived packet flow must be validated. This study discusses the use of an authentication handover and a modified blockchain structure to activate network security.

1.1. Motivation

Security in the network has become more important when 5G-SDN and MEC are combined. Blockchain technology is presented to meet the security requirements in this setting. Nevertheless, the earlier research was either concerned with user authentication or with user packet analysis. For large-scale network users, 5G-SDN must focus on both, though, to ensure security. The main difficult security issues include

- Secure authentication that uses cryptographic techniques to guarantee the privacy of the security credentials.
- AP will be connected by multiple users.
- The list of records grows linearly when utilizing classic blockchain technology.
- The packet flow properties analysis can also lead to the misclassification of a few additional malicious packets discovered during a single scan.

This led to the construction of 5G-SDN and beyond networks with MEC, blockchain, and several controllers for packet analysis, flow rule matching, and handover authentication. The suggested research project outlines a practical security solution for a 5G-SDN network environment in support of this goal.

1.2. Contribution

The following summarizes this study paper's main contributions:

- Toaddress the conventional problems with blockchain, we develop a 5G-SDN environment with customized blockchain technology as a separate layer.

- The QUARK algorithm, which transforms the user identity and pseudo-identity into hashes, provides lightweight authentication with credential privacy. The blockchain is used to confirm the user's finger vein biometric and physical unclonable function (PUF) to enhance authentication.
- A unique network component known as a load monitor keeps an eye on the load at APs and balances it while granting 5G users authentication access.
- The blockchain's built-in DAG, which can store more transactions and is hence appropriate for larger network environments, allows for quicker user validation.
- Harris Hawks optimization (HHO) is used to choose the best switch for flow rule matching at switches.

This document is organized as follows: Section 2 surveys current methodologies and their limitations while addressing identified security concerns in communication networks; Section 3 delineates proposed solutions to these significant security challenges; Section 4 offers an experimental evaluation of the network design through graphical representation; and Section 5 concludes with a discourse on future search directions arising from this study.

2. LITERATURE REVIEW AND PROBLEM STATEMENT

An essential component of every large-scale network is load balancing. The purpose of load balancing is to control the network's response to an increase in users. Each layer, the data plane, and the edge were subject to load balancing. Incoming packets are transferred to the correct switch by the data plane layer, while user handover is managed by the edge layer. Due to the diverse data types received by this network from 5G users, load balancing at the edge layer is necessary [15]. By dividing the traffic into three categories—management, internal, and external—the traffic from user equipment was evenly distributed. To balance the load, user and packet handover was enabled. By generating a distinct tag for every user based on their identification, MAC address, and standard E.164 numbering, packet forwarding was introduced [16]. A load imbalance would undoubtedly result from the targeted DoS/DDoS attack submitting an excessive number of packets with a similar protocol. As a load-balancing monitoring system, a non-cooperative game was created [17]. In this work, the aggregate message authentication code (AMAC) technique was used. Mobile device authentication was carried out by confirming both individual and collective identities. A message authentication code (MAC) was created when the signature was confirmed. The eNB received from mobile users served as validation for this MAC. However, if the user's credentials are not unique, unauthorized individuals will be able to access the network. The controller of the switch analyzes the network traffic to determine whether any malicious packets are involved in the network. A hybrid is fuzzy with an artificial neural network (HF-ANN) and tree-based switch assignment (TBSA) was suggested [18]. The HF-ANN method uses the packet features to categorize the received packets. To counteract the flow table overloading assault, a switch assignment was done. The number of successfully transmitted packets, packet loss, and error rate are the packet features that were considered in HF-ANN. Attack packets were only identified at the control plane layer, which permits transmissions from both authorized and unauthorized users, significantly increasing the number of packets. A SeArch was built with an intelligent intrusion detection system (IDS) [19]. The main issue was that making accurate class predictions required a large number of training sets. The packets were then categorized using randomly chosen attributes, which may have overlooked certain important features and failed to accurately forecast dangerous packets. The packets were also classified using techniques like SVM, decision trees, and random forest (RF) [20]. The packets were classified as either regular or attack packets based on a set of 23 attributes. The created decision tree, which is difficult to analyze, was used for the RF-based categorization. For a large network, where a vast number of packets arrived every second, this was time-consuming.

The blockchain technology was introduced for network traffic analysis [21,22]. Along with blockchain, SDN covered security provisioning based on the Markov model. Reducing the involvement of malicious packets in the network also required network entity authentication. To protect privacy, the identities of the network devices were concealed through the use of Hidden Authentication (HiAuth), which also reduced the impact of DoS attacks [23]. The foundation of this HiAuth was lightweight processing, which was created using three steps: distribution correction mechanism, data mixing, and one-time pad generation. The data was encrypted using the ChaCha lightweight method. The identities were just concealed, though, and the packet features were not examined.

The main issues with security in a 5G-SDN context are discussed in this section. 5G-SDN handover is carried out based on 5G users' mobility, with an emphasis on authentication provisioning [24,25]. Implementing a capability-based privacy-protection mechanism (CPPHA) involves generating a MAC, which is a hash of capability, count value, temporary identity, and session key. After receiving a request, the base station (BS) verifies the count value before MAC. Handover authentication was achieved if the MAC and counter value were accurate. Next, a novel method for handover authentication that minimizes re-authentication was discussed. The user asks the blockchain center directly for the integrity key during authentication. After that, the controller received updated authentication data to verify the user. Following validation, the target access point and serving AP were notified of the user's access. Re-authentication with the following AP was lessened by detecting the user's moving path.

It was suggested to use a neural multi-fuzzy algorithm for packet validation and user authentication in blockchain [26]. Individual user signatures, identities, and elliptic curves were generated using the linear homomorphic signature (LHS) technique. Six key packet features were retrieved and evaluated simultaneously using fuzzy logic for classification. The flow table of a distributed lightweight DDoS threat analytics and response system (DTRAS) is used to confirm the received packet. [27]. A hybrid machine learning model (SVM and SOM) and an enhanced history-based IP filtering technique (eHIPF) were then covered [28]. The SVM classifies packets as normal, malicious, or suspicious. The SOM classifier then processes the suspicious packets. Other techniques have been presented in [29-32] to overcome the issue ofunauthorized packets.

The studies suggest that there is a lack of an integrated vision of security since most of the technologies emphasize either user-provisioned token login or pack analysis but not the two [18,23,24]. As advocated by extensive studies, the integration of SDN systems within blockchain frameworks poses difficulties such as an increase in record lists while increasing network complexity leads to a decrease in processing speed [21,24]. Most of the load balancing algorithms available today use either static or heuristic methods which are not suitable for the complexities and time requirements within 5G/6G structures [15,17]. Methods such as support vector machine (SVM), random forests and HF-ANN have been utilized to classify packets, but issues arise because of their failure to account for more complex relationships among packet features resulting in misclassification. [19,28]. The inability to efficiently deal with handover authentication is one of the main issues facing 5G networks, these problems are caused by the mobility of the user as well as differences in received signal strength (RSS). Some methodologies cite the delay and resource waste arising from the need for constant authentication as an issue, with many demanding of solutions to automatically resolve this problem [23,25]. High traffic volume puts pressure on single-controller SDN frameworks which limiting their functionality and collapses the entire system [14,27]. As a result, application areas such as self-driving cars, health care, and industrial automation require new forms of communication that would allow their unreliability and new conditions to be required, which this system has not reached [24,30].

The proposed research, which is based on the analysis of packet classification, blockchain, and handover authentication, resolves the stated issues.

3. LLMODBLOC IN 5G-SDN AND BEYOND

This section provides a detailed description of the proposed LLModBloc in 5G-SDN and beyond.

3.1. Model of the Network

The secure architecture that has been built in this research project supports users in 5G and beyond. The edge layer, blockchain layer, data plane layer, control plane layer, and application layer make up the built architecture. A collection of network entities that carry out their respective functions make up each layer. The Internet of Things users who send packets to the edge devices are the 5G users. Allow IoT users to send numerous packets to edge devices by having $I_k = \{i_1, i_2, i_3, \ldots\}$. Since they are primarily utilized to forward arriving packets to next-layer entities, edge devices often have little resources. To confirm that user credentials and flow rules match, a blockchain layer is created. For quicker validation, the updated blockchain structure is supported. Then, by choosing a switch that matches the flow rule, the issue of overload at switches is lessened. The control plane layer then analyzes the mismatched packet flow using a two-level packet validation based on hexa-features.

Figure 1 illustrates this multi-layered 5G-SDN secure architecture model. Together with the algorithms each one employs; the primary network entities are shown. This 5G-SDN architecture with a modified blockchain is meant to provide environmental security, according to the suggested approach. The anonymous attack packets on the network result in greater resource usage and longer response times. The proposed 5G-SDN architecture would certainly improve network performance by providing packet analytics to detect attack packets.

Users' queries are first sent to the edge layer, which is where 5G APs are installed and handle offloading, or user handover. After that, the packets are sent to the data plane, where the switches check that the flow rule is being followed. Blockchain provides functionality for these two security layers. After that, the packets are categorized by feature analysis.

3.2. Authentication Handover

A verified handover is performed by confirming the user's location, finger vein, PUF, identification, and pseudo-identity. A person's finger vein is one biometric that can be used to identify them. These security credentials are protected by lightweight hashing generation and a one-time pad to preserve privacy. The hash values are saved in the blockchain after users have registered with their security credentials. During the authentication procedure, AP looks up the credentials on the blockchain. The QUARK algorithm integrates sponge creation and core permutation to optimize resource usage.

The sponge is produced through the processes of initiation, absorption, and squeezing. In initialization, a multiple of r, where r is the block length, is obtained by adding the identity and pseudo-identity by one bit. From the first block until the state $s = (s_0, \ldots., s_{b-1})$, r-bit blocks are then executed using the XOR technique. The formula for the$b$-bit is $b = r + c$, where c is the capacity. The final r bits are thus obtained as an outcome ofthe squeezing process. Similarly, initialization, state update, and output prediction are used to carry out the permutation r using the b bit as input. The internal state $(X^t, Y^t, L^t)$is used to initialize the states created in the sponge. The identity and pseudo-identity hash result is as follows:

$$s = (s_0, \dots, s_{b-1}) = (X_0^{4b}, X_1^{4b}, \dots, Y_{b/2-2}^{4b}, Y_{b/2-1}^{4b}) \quad (1)$$

The 5G-AP at the edge layer verifies the hashed identity and pseudo-identification. One-time pads (OTPs) are then generated using ChaCha stream cipher algorithm according to PUF, location, and finger vein. Once the vein in the finger has been transformed into binary data, a set of binary values is taken into consideration for authentication. The four-bit words a, b, c, and d are formed using these three security credentials. First, a quarter round of 32-bit integers is used to process the Chacha state as a 4x4 matrix.

The following is how the matrix is written:

$$X = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{pmatrix} \quad (2)$$

This matrix is represented as $\begin{pmatrix} co & co & co & co \\ k & k & k & k \\ k & k & k & k \\ bc & bc & n & n \end{pmatrix}$, the terms If n is the set of nonce values, k is the key, and bc is the block counter. The exclusive-or operator and the addition operator will be used to perform this quarter-round function 32 times. From these modified states, we get a 64-bit keystream. The 5G access point at the edge layer authenticates the generated one-time password within the blockchain. The load monitor will periodically evaluate the load at a specific AP if the user is authenticated. Using the connected users' load, connectivity, and channel strength, this load monitor calculates a likelihood value. The mathematical expression for the load at i^{th}AP is:

$$AP_i(L) = \sum_x^k I_k \quad (3)$$

The equation is utilized to determine each access pointsof individual load L, where k is the total number of Internet of Things users using that specific access point. The ratio of signal to noise (SNR), which shows if a signal is there in a channel, determines the channel's strength. $C_s = Blog_2(1 + SNR)$ is the formula used to calculate the channel strength C_s.

$$C_s = Blog_2(1 + SNR) \quad (4)$$

B represents the channel's bandwidth. These three are used to estimate a probability value, which is

$$P_L = (AP_i(L), C_u, C_s) \quad (5)$$

Depending on the threshold, a threshold value between 0 and 1 is assigned to the load and channel strength. We move the user from serving AP to targeting AP based on the likelihood value. If its load is high, it will connect to the target AP; otherwise, it will stay connected to the source AP. Since the status report will be updated to reflect the target AP as soon as the authentication is successful in servicing the AP, frequent authentication during handover is not necessary. Packets are routed to various switches based on the connected access point.

3.3. Switch Selection and Flow Rule Matching

The flow table that the switches utilize is compared with the user packets. Typically, when a large number of flows come, the switches will overflow. Both a physical switch and a virtual switch make up the data plane in this 5G-SDN system. However, the virtual switch will only be established when there isn't a single best switch to balance the flow of arriving packets. The HHO

method is used to choose the best switch, and a switch is chosen based on the estimated fitness value. Three important constraints—load degree, bandwidth, and flow entries—are used to calculate the fitness value. The mathematical formulation of the load balancing degree (LB_D) is as follows:

$$LB_D = \frac{\sum_j^m t_j}{m \times C_t} \quad (6)$$

This degree is derived from t_j, which shows how long it takes for flow j to process, m, which is the total number of flows in the switch, and C_t, which shows how long it takes for all m flows in the switch to finish. The available flow entries in a specific switch are then measured after accounting for the available bandwidth A_B. Every switch will have a predetermined number of flow entries; that is, the flow at switches can be permitted up to that limit; if it is exceeded, overflow happens. Each switch's fitness value is determined by these three criteria and is provided as follows:

$$(S_1, S_2, \dots, S_n) \rightarrow (f_1, f_2, \dots, f_n) \quad (7)$$

Exploration and exploitation are the two stages of processing the HHO algorithm. This algorithm is based on how hawks attack rabbits in order to capture them. The Hawks $X(t+1)$ position vector is constructed as follows during the exploring phase:

$$X(t+1) = \begin{cases} X_{rand}(t) - r_1 |X_{rand}(t) - 2r_2 X(t)| & q \geq 0.5 \\ \left(X_{rabbit}(t) - X_m(t)\right) - r_3\left(l_b + r_4(u_b - l_b)\right) & q < 0.5 \end{cases} \quad (8)$$

Assuming that $X(t)$ represents the hawks' position vector at time t, Equ. (8) is used to formulate the position vector for the following iteration, where Xr_1, r_2, r_3, r_4 are defined as random integers. These random numbers have values in the interval [0,1]. Let $X_{rand}(t)$ represent the hawks chosen at random from the total number of hawks$N$, u_b, and l_b. represents the upper and lower bounds, and X_m represents the average hawk position, which may be calculated analytically as

$$X_m(t) = \frac{1}{N}\sum_{j=1}^{N} X_i(t) \quad (9)$$

This rule is used to calculate the hawks' average location. After the prey energy E is predicted, the phase shifts from exploration to exploitation.

$$E = 2E_0\left(1 - \frac{t}{T_{Max}}\right) \quad (10)$$

T_{Max} is the maximum number of iterations, and $E_0$is the prey's energy at the beginning. In exploitation, either a soft or severe besiege is employed, depending on the energy value. Soft besiege is used when $|E| \geq 0.5$, while hard besiege is used for a position update if $|E| < 0.5$.
The expression for soft besiege $X(t+1)_S$ And hard besiege $X(t+1)_H$ is illustrated below,

$$X(t+1)_S = \Delta X(t) - E|JX_{rabbit}(t) - X(t)| \quad (11)$$
$$X(t+1)_H = X_{rabbit}(t) - E|\Delta X(t)| \quad (12)$$

In this case, $\Delta X(t) = X_{rabbit}(t) - X(t)$, where J is the rabbit's strength. The best switch selection process, which determines which switches receive the arrived flows, is described in the pseudo-code above. For privacy, the flows are hashed and saved in the altered blockchain. To confirm the flow rules, every switch is linked to the blockchain. The linear blockchain structure has been replaced with a DAG one. Vertices and edges make up this DAG, with the edges directed toward

the vertices. A cycle of blocks is not created in a modified blockchain; that is, although the blocks connect, they do not form the parent node as its edge. Assume that the built graph $G = (V, E)$ has V vertices and E edges [33].

The leaf nodes in DAG are sequentially labeled, and each node is represented with a distinct identity. Leaf nodes may or may not be present in every node. The nodes must preserve both the hashed packet flow and the user hash values in addition to the identification. First, the parent transactions are identified following a request for flow verification or authentication. After that, the block's other transactions are verified. The new transaction is updated following verification. Security credential validation and flow rule verification are carried out. The packets are sent into the control plane for validation if the flow rule does not match. The appropriate application receives all of the matched flows. The SDN controllers verify the new flows from a certain user, and if the flow is unknown, a new flow rule is created and put into every switch. It is determined whether the new flows enter the data plane layer after deployment.

3.4. Based on Hexa-Features Two-Level Validation of Packets

To lessen single-point failure, the control plane layer is used with many controllers. To precisely forecast the packet's behavior, the SDN controllers in this layer carry out two validation stages. Using the capsule network (CapsNet), miss-matched packets are classified as normal, suspicious, and malicious at the first level. The suspicious packets are then solely examined using Q-learning in the second stage, which determines if the packet is malicious or legitimate. The IP and port numbers of the source and destination, protocol, packet size, service, flow time, and flag are the features considered for first-level analysis. The second level, on the other hand, uses jitter, bandwidth, time-to-live (TTL), retransmission count, packet arrival time, and authentication score.

One type of deep learning network, known as CapsNet, makes use of loss estimations, primary capsules, and capsules in higher layers. An input matrix is used to characterize the incoming flow, and the weight values of each packet feature are assigned to it. To feed into the next layer, the first one takes the weighted values of each packet feature and stores them. In order to establish if a flow is malicious, suspicious, or normal, we add up all of the input vectors and use a weighted total. Regular packets are processed by the application layer, whereas malicious ones are dropped. We take into account the following packet characteristics: Port number and IP address: Protocol: Message size: Duration of flow and flagging service:

A convolution layer, primary capsule layer, digicaps layer, and output layer are all included in the architecture of this capsule network. The convolution layer redefines the packet features by extracting the six characteristics from each flow. The principal capsule layer then receives it as input. The summation and multiplication operations are used with the digicaps layer. The output layer is then fully connected and operated according to softmax. Consequently, this layer classifies the packet as malicious, suspicious, or normal.

CapsNet, A set of examples with different packet properties is used to train CapsNet. Based on the training results, incoming miss-matched packets are analyzed to determine their sort. If there are just malicious and legitimate packets, the packet analysis is terminated. In the second stage, any suspicious packets are analyzed using the reinforcement learning algorithm and features of user behavior. The reinforcement learning algorithm is a clever method of decision-making that defines an action according to the present situation. Each suspicious packet's state is influenced by its jitter, bandwidth, retransmission count, TTL, authentication score, and packet arrival time. The activity of the particular user is reflected in these attributes. The totality of the features determines the user's present condition. The related user information is gathered once it has been

determined that the packet is suspicious. The behavior features examined in this work are *Scores for authentication* (A_s), *Packet arrival time* (A_p), *Jitter*(J_e) ,*TTL*(T_l), *Bandwidth*, and *Retransmission count*(R_c).

Prior to making a decision, reinforcement learning learns the environment. The temporal differences that the agent measures are used to estimate the Q-values. With n states S represented as $\{S_1, S_2, \ldots., S_n\}$ and m actions a represented as $\{a_1, a_2, \ldots., a_m\}$, a Q-table is produced. A packet's states are determined by its behavior characteristics. The calculations of reward$r$ will be based on the action for the relevant S. Each state is specified as $S = (A_s, A_p, T_l, R_c, J_e, B)$ and their activities are classified as either normal or malevolent based on their unique characteristics. Let S_tBe the state that needs to act right now. a_t with r_t as the reward. The agents learn the policy π in Q-learning from their surroundings, and the next state is defined as S_{t+1}. The Bellman equation is used to define the Q-function, which can be written as

$$Q^{\pi}(S_t, a_t) = E[r_{t+1} + \gamma r_{t+2} + \gamma^2 r_{t+3} \ldots | S_t, a_t |] \quad (13)$$

γ is the discount rate, then this Q-function is updated from the following as $Q^*(S, a)$,

$$Q^*(S, a) = Q(S, a) + \alpha[r(S, a) + \gamma max Q'(S', a') - Q(S, a)] (14)$$

The current state, action pair, and $\gamma max Q'(S', a')$ are represented as $Q(S, a)$. specifies the highest predicted reward that will be granted for the new action a' and the new state S'. The learning rate is denoted by α. Only when there are suspicious packets is the second level of packet analysis carried out. By analyzing the flows, the suggested SDN multi-controllers protect the network from malicious flows. In order to match the arrival of new flows in the data plane, a new rule is written and installed in switches upon identifying the malicious packets.

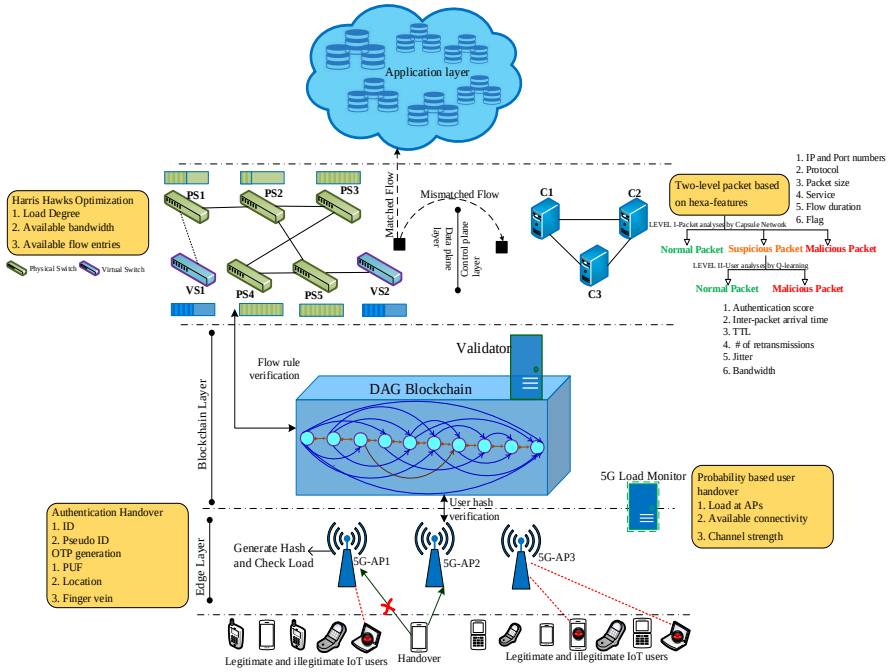

Figure 1. LLModBloc in 5G-SDN

4. SIMULATION ENVIRONMENT

This section examines the development of the designed 5G-SDN system paradigm. The system's performance is assessed based on the network design. This part emphasizes the significance of the suggested research and is divided into two categories: comparative analysis and simulation environment. The effectiveness of the suggested 5G-SDN architecture is supported by this simulation system component.

4.1. Simulation Setup

The ns3.26 version of the network simulator utility implements the suggested 5G-SDN network. Network modules and technologies can be incorporated into network simulators. The Ubuntu 14.04 LTS operating system comes with this ns3.26 installed. A dual-core processor, 2GB of RAM, and 32-bit support are utilized to help the operating system. SDN controllers $\{ct_1, ct_2, ct_3\}$ OpenFlow switches $\{sw_1, sw_2, \dots, sw_8\}$ and 5G IoT users $\{i_1, i_2, i_3, \dots, i_{50}\}$make up the system. This arrangement of the network's entities serves as the foundation for the network's construction. OpenFlow switches, 5G specs, and SDN configuration modules for the SDN controller are all included.The suggested system is stacked and processed using packet analysis, flow rule verification, and authentication handover by this simulation scenario. Python code is used to run the algorithms after they have been built in the C++ programming language. To maintain network environment security, each layer is run according to the appropriate processing techniques. First, the OTP generation and lightweight QUARK algorithm are integrated into the edge layer that is connected to the blockchain for authentication. Next, a threshold probability is assigned to the 5G AP in order to balance the load at the edge layer.

Second, after being assigned to a switch chosen by the HHO algorithm, the flow rules are validated in the blockchain. After assessing the switch's capability, this method receives the incoming packet. In order to precisely forecast the malicious packet that has entered the network, the packets are next examined using two distinct six features on two different approaches in the third step. While the malicious packet will be dropped by the network entities within the network itself, all matched flows will be sent to the appropriate service in accordance with the request. While the IoT users are either authentic or fraudulent, the basic network components—AP, validator, switches, and controllers—are regarded as trustworthy in this work. Not every authorized user submits with a typical packet; some infected users create malicious packets that utilize more resources and certainly impair network performance.

4.2. Comparative Analysis

The comparative analysis is performed to evaluate the efficacy of the proposed 5G-SDN compared to previous research. to evaluate this proposed system's higher performance.

4.2.1. Bandwidth Consumption

The performance of bandwidth consumption in response to an increase in authentication requests is shown in Figure 2.Comparative results show that the suggested LLModBloc uses less bandwidth since it uses a modified blockchain structure that uses DAG in block generation.

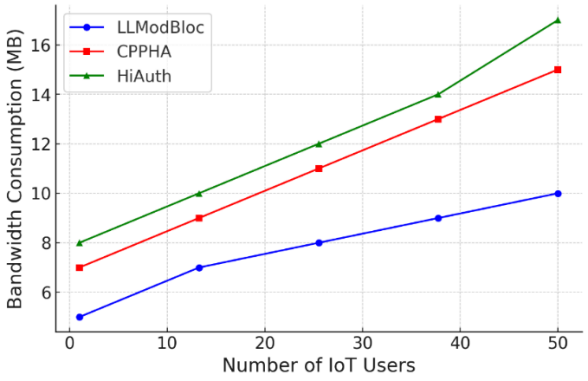

Figure 2. Comparison of bandwidth consumption

4.2.2. Authentication Time

The time required to confirm a user's identity by examining their credentials is known as the authentication time. Figure 3 displays the results of comparing the authentication time to the arrival of requests. Although the suggested LLModBloc uses computationally constrained lightweight techniques, it also protects the security credential's secrecy. The main factor reducing the authentication time compared to the current works is the adoption of a lightweight method. Due to its flexibility, blockchain authentication speeds up authentication for larger packet requests. In LLModBloc, the average estimated time for authentication is 1 s, while in CPPHA and authentication handover, it is 1.7 s and 2.3 s, respectively. The processing time will be minimal even if the packet size is raised.

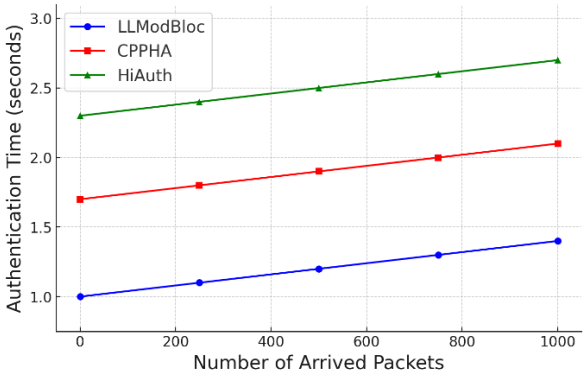

Figure 3. Comparison of authentication time

4.2.3. Delay and Response Time

One crucial performance indicator that gauges the time needed to process data is delay. Figure 4 compares the delays for proposed and current works. By using a load-balanced edge layer, switch selection, a modified blockchain, and lightweight algorithm-based authentication, the suggested LLModBloc reduces latency. Figure 5 illustrates the results of minimizing delay, which also significantly lowers response time. This is the time needed to handle a request that has arrived. The response time will be longer if there is a greater delay in packet processing.

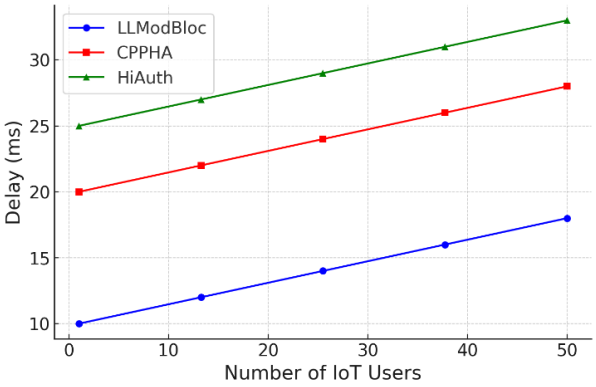

Figure 4. Comparison of delay

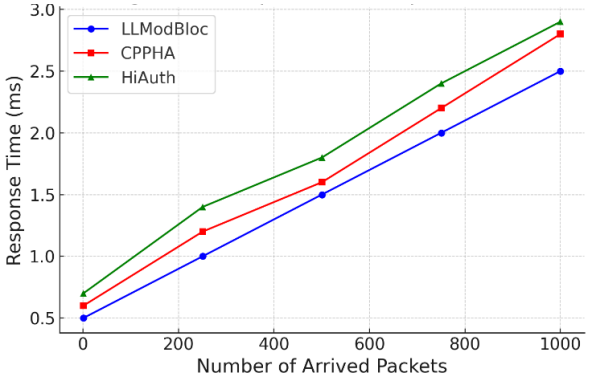

Figure 5. Comparison of response time

4.2.4. Packet Loss

In a network, packet loss is a critical parameter,Figure 6 shows the results of evaluating packet loss performance to expand the number of IoT users.

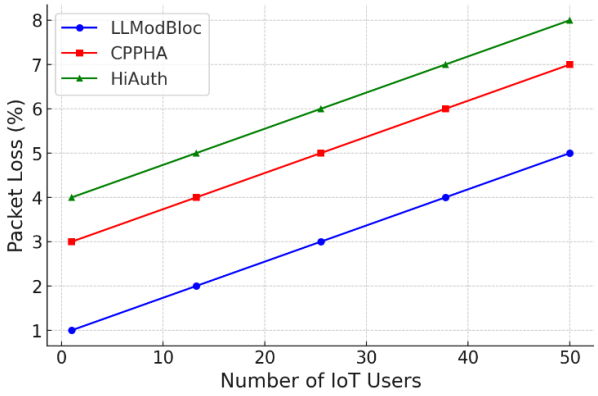

Figure 6. Comparison of packet loss

4.2.5. Detection Accuracy

The precision with which malicious packets are identified as they enter the network is known as detection accuracy. This work's primary goal is to identify malicious or regular packets in order

to maintain network security.Figure 7 shows the attack prediction which determines the detection accuracy.

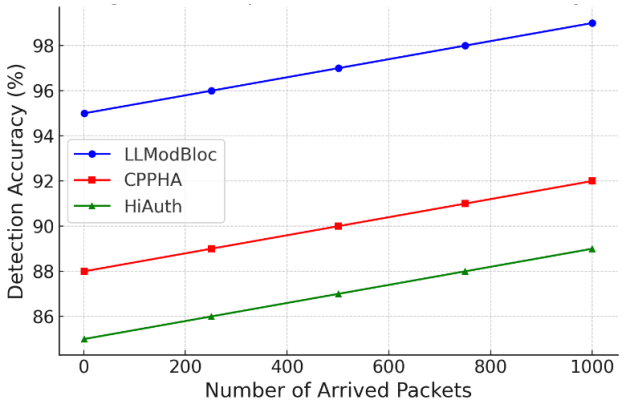

Figure 7. Comparison of detection accuracy

4.3. Comparison of LLModBloc with Related Literature

4.3.1. Key Features and Enhancements

The LLModBloc architecture introduces several advanced features that differentiate it from the existing methods in the literature as given in Table 1.

Table 1 Feature differences between LLModBloc and Literature

No	Feature	LLModBloc (Proposed)	Literature	Advantages
1	Authentication	QUARK algorithm for lightweight hashing, finger vein biometrics, and one-time pad (OTP) generation	Hidden Authentication (HiAuth) with ChaCha encryption, CPPHA with lightweight cryptography[23, 25]	LLModBloc combines lightweight techniques with physical biometrics, enhancing both efficiency and privacy.
2	Load Balancing	Load monitor using likelihood calculations with HHO for optimal switch selection	Non-cooperative game theory and virtualized packet forwarding[15, 17]	LLModBloc integrates user load, channel strength, and connectivity for real-time optimization.
3	Blockchain	Modified DAG-based blockchain for faster processing and scalability	Traditional linear blockchain[21, 24]	LLModBloc reduces transaction time and enhances scalability in large networks.
4	Packet Analysis	Two-level validation using CapsNet and Q-learning for hexa-feature analysis	SVM, Random Forest, and SOM for packet classification[19, 28]	LLModBloc achieves higher detection accuracy with reduced misclassification.

4.3.2. Comparative Metrics

To quantify the differences, LLModBloc is compared with contemporary methods across several performance metrics as given in Table 2.

Table 2 Metrics Comparison

No	Feature	LLModBloc (Proposed)	CPPHA [24]	HiAuth [23]
1	Authentication Time	~1 second	~1.7 seconds	~2.3 seconds
2	Detection Accuracy	98%	90%	92%
3	BandwidthConsumption	Low (due to DAG-based blockchain)	Medium	High
4	Packet Loss	Minimal	Moderate	High

4.3.3. Innovation and Performance Outcomes

The innovation and performance outcomes of the proposed work are listed below as:

- Authentication Mechanism: LLModBloc interprets HiAuth and CPPHA as substandard as it is able to combine lightweight cryptographic techniques customized integrated with physical unclonable function (PUF) and finger vein biometrics without incurring an additional computational cost.
- Blockchain Scalability: LLModBloc is able to eliminate the issues of conventional blockchain and nips in the bud the decentralization of a single ledger while at the same time increasing the throughput significantly, this beats the linear blockchains of HiAuth and CPPHA
- Advanced Machine Learning: For packet classification CapsNet in a multi-class configuration along with Q-learning for reinforcement-based validation resolves the classification problems experienced with HF-ANN and SVM methods.

In Figures (2-7) LLModBloc has outperformed other approaches on the specific parameters like authentication time, bandwidth utilization, detection performance and latency. These enhancements indicate LLModBloc is fit for purpose for future proof 5G/6G specifications. The LLModBloc's Main Finding are the following:

- Acute management of the existing gaps demonstrated by the solutions.
- Added value for the area of network security.
- Relevant in practice
- Improving the current creation in the area.
- Balancing security and performance.

Hence, the LLModBloc is not simply an incremental step towards the improvement rather it is a new dimension in accomplishing the security requirements of SDN 5G.

4.4. Novelty of the Proposed LLModBloc

The LLModBloc is introducing new ways of doing things which makes it unique in the context of 5G/SDN network security as compared to all the other methods and solutions available today. What is new and innovative is the formation of new technologies into more advanced systems and incorporation of new frameworks that have some of the aforementioned systems adjusted to the requirements that are posed in multiservice networks. The key novelties are given in Table 3.

Table 3 Key Novelties of Proposed LLModBloc

No		Novel Approach	Significance	Comparison
1	DAG-Based Blockchain for Scalability and Speed	Unlike traditional linear blockchain architectures, LLModBloc employs a **Directed Acyclic Graph (DAG)-based blockchain** to handle transaction records	Reduces transaction validation time and improves scalability by allowing parallel processing of blocks. Addresses the growing record size challenge in 5G networks, ensuring fast and reliable operations.	Traditional blockchain systems fail to scale effectively, leading to higher latency and resource consumption, whereas DAG offers superior performance under high transaction loads.
2	Advanced Authentication Mechanism	A unique combination of **lightweight QUARK hashing**, **biometric verification (finger vein)**, and **Physical Unclonable Function (PUF)** enhances authentication security and efficiency.	The use of biometric and PUF ensures **unclonable and highly secure authentication credentials**. Lightweight cryptographic operations minimize computational overhead, suitable for resource-constrained IoT devices.	Unlike traditional methods that rely solely on cryptographic keys, LLModBloc integrates physical attributes, ensuring stronger protection against impersonation attacks.
3	Capsule Network (CapsNet) for Multi-Class Packet Classification	The use of **Capsule Networks (CapsNet)** for packet analysis introduces a hierarchical learning model that captures spatial and relational features between packet attributes.	Accurately classifies packets into normal, suspicious, and malicious categories. Reduces misclassification rates seen in traditional classifiers like SVM and Random Forest.	CapsNet offers enhanced accuracy and robustness compared to flat feature-based methods, making it suitable for complex 5G network traffic patterns.
4	Reinforcement Learning for Adaptive Packet Analysis	The integration of **Q-learning** enables dynamic decision-making for suspicious packet validation, considering behavioral attributes like jitter, retransmission counts, and bandwidth.	Provides an adaptive mechanism to distinguish between legitimate and malicious packets based on real-time network conditions. Learns from historical data to continuously improve detection accuracy.	Static rule-based systems fail to adapt to evolving attack patterns, whereas Q-learning ensures resilience against sophisticated attacks.
5	Dynamic Load Balancing with Harris Hawks Optimization (HHO)	The use of **Harris Hawks Optimization (HHO)** for switch selection and load balancing is a novel metaheuristic approach in SDN-enabled 5G networks.	Optimizes the distribution of user requests across switches based on load, bandwidth, and flow entry availability. Prevents bottlenecks and ensures smooth network operations, even under high traffic conditions.	Traditional heuristic-based methods are unable to adapt dynamically, whereas HHO ensures optimal resource utilization in real time.
6	Comprehensive Two-Level Packet Validation	A two-level packet validation mechanism using **CapsNet** and **Q-learning** ensures multi-layered security.	Captures both high-level packet features (IP, protocol, port) and behavioral attributes (jitter, TTL, authentication score). Mitigates single-point	Most existing systems validate packets based on a single feature set, leading to higher false positive/negative rates. LLModBloc's

			failures often seen in control plane systems.	layered approach significantly reduces such errors.
7	Integration of Layers for Holistic Security	LLModBloc combines **edge layer**, **data plane**, **control plane**, and **blockchain layer** into a unified framework.	Ensures seamless interaction between layers for authentication, load balancing, and packet analysis. Provides end-to-end security from user authentication at the edge to flow validation at the control plane.	Unlike fragmented solutions that address specific aspects of network security, LLModBloc provides a fully integrated approach for 5G/6G networks.

4.5. Limitations of the Proposed LLModBloc System

While the LLModBloc system significantly enhances the security of 5G/SDN networks, it is important to consider its limitations and potential for improvement. Addressing those issues not only enriches the research but also makes foundations for future works. The limitations are:

- Computational overhead in advanced techniques
- Dependency on biometric data
- Energy consumption in multi-layered processing
- Initial deployment costs

5. CONCLUSION

The proposed LLModBloc presents a transformative solution for addressing critical security and efficiency challenges in SDN-enabled 5G and beyond networks. By integrating advanced features such as DAG-based blockchain, lightweight authentication mechanisms, and CapsNet-Q-learning-based packet classification, LLModBloc demonstrates higher performance in reducing bandwidth consumption, minimizing latency, enhancing detection accuracy, and ensuring robust scalability. The experimental results highlight the system's ability to:First, significantly reduce authentication time through the use of lightweight QUARK hashing and optimized blockchain structures. Second, minimize delay and packet loss with real-time load balancing and Harris Hawks Optimization (HHO)-based switch selection. Third, enhance detection accuracy by combining deep learning and reinforcement learning for packet analysis. Forth, improve scalability by addressing blockchain limitations with a DAG-based structure.

Compared to existing methods, LLModBloc achieves higher efficiency and security, making it a practical choice for real-world applications such as IoT ecosystems, industrial automation, and critical infrastructure protection. Its ability to handle massive user connections, adapt to dynamic network conditions, and ensure low-latency communication positions it as a foundational architecture for 6G and future networks.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGEMENTS

The authors would like to express their warm gratitude to both University of Kirkuk and University of Mosulfor their support and contributions to this research.

REFERENCES

[1] Stefan Schwarz, Blanca Ramos Elbal, Erich Zöchmann, Ljiljana MArijanovic, Stefan Pratschnere, "Dependable wireless connectivity: insights and methods for 5G and beyond", Springer, pp 449 – 455, 2018.

[2] Xinsheng Ji, Kaizhi Huang, Liang Jin, Hongbo Tang, Caixia Liu, Zhou Zhong, Wei You, Xiaoming Xu, Hua Zhao, Jiangxing Wu, Ming Yi, "Overview of 5G security technology", Science China Information Sciences, Springer, 2018.

[3] Muhammad Nauman Irshad, Liping Du, Imran Ali Khoso, Talha Bin Javed, Muhammad Muzamil Aslam, "A Hybrid Solution of SDN Architecture for 5G Mobile Communication to Improve Data Rate Transmission", 28th Wireless and Optical Communications Conference (WOCC), 2019.

[4] Lu Ma, Xiangming Wen, Luhan Wang, Zhaoming Lu, Raymond Knopp, "An SDN/NFV based framework for management and deployment of service based 5G core network", China Communications, Vol. 15, No. 10, pp. 86 – 98, 2018.

[5] Zainab Zaidi, VasillisFriderikos, Zarrar Yousaf, Simon Fletcher, Mischa Dohler, Hamid Aghvami, "Will SDN Be Part of 5G?", IEEE Communications Surveys & Tutorials, Vol. 20, No. 4, pp. 3220 - 3258, 2018.

[6] SanhapitPhatratipakorn, PongsatomSedtheetom, "Design of SDN concept for 5G Access Network", 19th International Symposium on Communications and Technologies (ISCIT), 2019.

[7] Bego Blanco, Jose Oscar Fajardo, loannisGiannoulakis, EnmanouliKafetzakis, Shuping Peng, Jordi JordiPérez-Romero, Irena Trajkovska, Pouria S. Khodashenas, Leonardo Goratti, Michele Paloino, Evangelos Sfakianakis, Fidel Liberal, George Xilouris, "Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN", Computer Standrads& Interfaces, Elsevier, Vol. 54, No. 4, pp. 216 – 228, 2017.

[8] Rabia Khan, Pradeep Kumar, Dushantha Nalin K. Jayakody, Madhusanka Liyanage, "A survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions", IEEE Communications Surveys & Tutorials, Vol. 22, No. 1, pp. 196 – 248, 2019.

[9] Hui Yang, Yongshen Liang, Jiaqi Yuan, Qiuyan Yao, Ao Yu, Jie Zhang, "Distributed Blockchain-based Trusted Multi-domain Collaboration for Mobile Edge Computing in 5G and beyond", IEEE Transactions on Industrial Informatics, 2020.

[10] Pal VArga, Jozsef Peto, Attila Franko, Davi Balla, David Haja, Ferenc Janky, Gabor Soos, Daniel Ficzere, MarkoszMaliosz, Laszlo Toka, "5G support for Industrial IoT Applications-Challenges, Solutions, and Research gaps", Sensors, MDPI, 2020.

[11] Zhedan Shao, Xiaorong Zhu, Alexander M.M. Chikuvanyanga, Hongbo Zhu, "Blockchain-Based SDN Security Guaranteeing Algorithm and Analysis Model", International Conference on Wireless and Satellite Systems, Wireless and Satellite Systems, pp. 348 – 362, 2019.

[12] Upul Jayasinghe, Gyu Myoung Lee, Áine MacDermott, Woo Seop Rhee, "TrustChain: A Privacy Preserving Blockchain with Edge Computing", Wireless Communication and Mobile Computing, Hindawi, 2019.

[13] Hani Alquhayz, Nasser Alalwan, Ahmed Ibrahim Alzahrani, Ali H.Al-Bayatti, Mhd Saeed Sharif, "Policy-Based Security Management System for 5G Heterogeneous Networks", Recent Advances in Security and Privacy Issues for Internet of Things Applications, Wireless Communications and Mobile Computing, 2019.

[14] Othmane Blial, Mouad Ben Mamoun, Redouane Benaini, "An Overview on SDN Architectures with Multiple Controllers", Journal of Computer Networks and Communications, Hindawi, 2016.

[15] Sikandar Ejaz, Zeshan Iqbal, Peer Azmat Shah, Bilal Haider Bukhari, Armughan Ali, Farhan Aadil, "Traffic Load Balancing Using Software Defined Networking (SDN) controller as Virtualized Network Function", IEEE Access, Vol. 7, pp. 46646 – 46658, 2019.

[16] Fouad Ali Yaseen, Hamed S. Al-Raweshidy, "Smart Virtualization Packets Forwarding During Handover for Beyond 5G Networks", IEEE Access, Vol 7, pp. 65766 – 65780, 2019.

[17] Guowei Wu, Jinlei Wang, Mohammad S. Obaidat, Lin Yao, Kuei-Fang Hsiao, "Dynamic switch migration with noncooperative game towards control plane scalability in SDN", International Journal of Communication systems, Vol. 32, No. 7, 2019.

[18] Ihsan Abdulqadder, Deqing Zou, Israa Aziz, Bin Yuan, Weiqi Dai, "Deployment of Robust Security Scheme In SDN Based 5G Network Over NFV Enabled Cloud Environment", IEEE Transactions on Emerging Topics in Computing, 2018.

[19] Tri Gia Nguyen, Trung V. Phan, Binh T. Nguyen, Chakchai So-In, Zubair Ahmed Baig, Surasak, Sanguanpong, "SeArch: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks", IEEE Access, Vol 7, pp. 107678 – 807694, 2019.

[20] Reneilson Santos, Danilo Souza, Walter Santo, Admilson Ribeiro, Edward Moreno, "Machine learning algorithms to detect DDoS attacks in SDN", Concurrency and Computation Practice and Experience, Wiley Online Library, 2019.

[21] Liuwei Huo, Dingde Jiang, Sheng Qi, Lei Miao, "A Blockchain-Based Security Traffic Measurement Approach to Software Defined Networking", Mobile Networks and Application, Springer, 2020.

[22] Faizullah, Safiullah & Khan, M & Alzahrani, Ali & Khan, Imdadullah, "Permissioned Blockchain-Based Security for SDN in IoT Cloud Networks", Interfernce Conference on Advances in the Emerging Computing Technologies (AECT), 2020.

[23] Osamah Ibrahiem Abdullaziz, Li-Chun Wang, Yu-Jia Chen, "HiAuth: Hidden Authentication for Protecting Software Defined Networks", IEEE Transactions on Network and Service Management, vol 16, No 2, pp. 618 – 631, 2019.

[24] Jin Cao, Maode Ma, Yulong Fu, Hui Li, Yinghui Zhang, "CPPHA: Capability-based Privacy-Protection Handover Authentication Mechanism for SDN-based 5G HetNets", IEEE Transactions on Dependable and Secure Computing, 2019.

[25] Abbas Yazdinejad, Reza M. Parizi, Ali Dehghantanha, Kim-Kwang Raymond Choo, "Blockchain-enabled Authentication Handover with Efficient Privacy Protection In SDN-based 5G Networks", IEEE Transactions on Network Science and Engineering, 2019.

[26] Mehran Pourvahab, Gholamhossein Ekbatanifard, "An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology", IEEE Access, vol 7, pp. 99573 – 99588, 2019.

[27] Prabhakar Krishnan, Subhasri Duttagupta, Krinshnashree Achuthan, "SDNFV Based Threat Monitoring and Security Framework for Multi-Access Edge Computing Infrastructure", Mobile Networks and Applications, Springer, pp. 1896 – 1923, 2019.

[28] Trng V. Phan, Minho Park, "Efficient Distributed Denial-of-Service Attack Defense in SDN-Based Cloud", IEEE Access, Vol 7, pp. 18701 – 18714.

[29] Songma, Surasit, WatcharakornNetharn, and SiriluckLorpunmanee. "Extending Network Intrusion Detection with Enhanced Particle Swarm Optimization Techniques." International Journal of Computer Networks & Communications (IJCNC) Vol.16, No.4, July 2024.

[30] I. H. Abdulqadder, I. T. Aziz, and D. Zou, "DT-Block: Adaptive vertical federated reinforcement learning scheme for secure and efficient communication in 6G," Comput. Netw., vol. 254, p. 110841, 2024.

[31] Karimy, Aziz Ullah, and P. Chandrasekhar Reddy. "Enhancing Iot Security: Anovel Approach With Federated Learning and Differential Privacy Integration."International Journal of Computer Networks & Communications (IJCNC) Vol.16, No.4, July 2024.

[32] I. O. Lopes, D. Zou, I. H. Abdulqadder, S. Akbar, Z. Li, F. Ruambo, and W. Pereira, "Network intrusion detection based on the temporal convolutional model," Comput. Secur., vol. 135, p. 103465, 2023.

[33] Xu Wang, Guohua Gan, Ling-Yun Wu, "Framework and algorithms for identifying honest blocks in blockchain", PLOS ONE, 2020.

AUTHORS

Ihsan H. Abdulqadder received a BSc. Degree in Electrical Engineering from Baghdad University, Baghdad, Iraq in 2004, M.Sc. Degree in Computer Science — Computers, Information, and Network Security from DePaul University, Chicago, USA, in 2010, Ph.D. in Cyberspace Security from Huazhong University of Science and Technology, Wuhan, Hubei, China in 2018. And a Postdoc at the University of Electronic Science and Technology of China from 2019 to 2021, has worked in many positions such as on network switching subsystems, project manager, consultant, core network engineer, trainer, and as a faculty member in a computer science department. He is currently a lecturer at the Department of Computer Science, University of Kirkuk, His research interests include security in SDN, NFV, and cloud computing in 5G/B5G and 6G core Networks.

Israa T. Aziz received her B.Tech. Degree in Computer Engineering from Mosul Technical College, Mosul, Iraq in 2007. She received her M.Tech Degree in Computer Engineering from Sam Higginbottom University of Agriculture, Technology and Sciences, Allahabad, India in 2014. She received her Ph.D. degree in Computer Engineering from Huazhong University of Science and Technology, Wuhan, China in 2020. Currently, she is a Lecturer with the University of Mosul, Mosul, Iraq. She has several national and international publications in her credit. Her research interests include computer security and smart grids security.