Received: July 14, 2023. Revised: September 26, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Efficient Handover Authentication Mechanism Using Deep Learning in SDN-Based 5G HetNets

Shivanand V. Manjaragi[1,2]* **S. V. Saboji[1]**

[1]*Department of Computer Science and Engineering, Basaveshwar Engineering College, Bagalkote,*
Visvesvaraya Technological University, Belagavi-590018, Karnataka, India
[2]*Department of Computer Science and Engineering, Hirasugar Institute of Technology, Nidasoshi,*
Visvesvaraya Technological University, Belagavi-590018, Karnataka, India
* Corresponding author's Email: shiva.vm@gmail.com

Abstract: The fifth generation (5G) networks are a popular standard that carries effective skills to conquer the tests of next generation wireless networks. Also, the 5G systems can support high data traffic by rendering high throughput and low latency towards the massively connected nodes. Here, handover is highly significant for data processing, portability and real time data creation in mobile technologies. With the 5G entrance, the cellular network has become a completely heterogeneous network (HetNet). The Software Defined Network (SDN) concept is used in 5G HetNets for better mobility management. Most existing research works have concentrated on handover authentication, but those works are often prone to re-authentication issues and increased handover delay. Therefore, to overcome the re-authentication process and provide users with better services, a novel handover authentication mechanism using deep learning (DHan_Auth) is proposed. Initially, the 5G data attack and normal data are collected, and the malicious and non-malicious users are classified using the Convolution Stacked long short term memory network model (Conv_SLSTM). To improve handover process and resist network attacks, only the non-malicious user data are authenticated through the key generation and the 5G Handover-Authentication and Key Agreement (5G_AKA) protocol. The process of encryption and decryption are performed using Extended Elliptic curve cryptography (Ex_ECC). When simulating with the PYTHON platform, performance such as handover latency, accuracy and precision are analyzed. The handover latency of the proposed model is 11.8 seconds to 200 nodes, while the classification accuracy in categorizing the malicious and non-malicious users reaches 98.98%.

Keywords: 5G networks, Software defined network, Stacked LSTM, Handover authentication, Key agreement protocol, Elliptic curve cryptography.

1. Introduction

The 5G networks possess increased capacities and data rates recommended over applications, including mobile banking and the Internet of Things (IoT) [1]. The 5G cellular technology intends to realize the next generation network where the devices, machines and objects employ together [2, 3]. The emergence of sensor devices, data exchange, sharing, sensing and analysis of gathered data to render enhanced facilities are gaining high priorities towards daily life activities. As highly sensitive data are exchanged in several applications, privacy and security schemes are necessary for deployments [4]. One of the major focuses of 5G networks is the huge accessibility of several users with enhanced communication rates [5]. The concurrent association of diverse cell types with differing software configurations generates heterogeneous networks (HetNets) in 5G. The immense participation of users involves numerous diversity in 5G HetNet because of lower coverage and processing ability.

In 5G-HetNet, the user devices cannot directly link over outdated cellular base stations accountable for geographical cells [6, 7]. The providence of security services and network administration inside heterogeneous cells are challenging since the user equipment (UE) may often leave one cell for another.

5G requires taking into account the accept to suppress these consequences, 5G separates the standard cells over reduced geographical areas and possesses diverse small cells, including femtocell, picocell and microcell in 5G networks for network access support [8-9]. The issues of blind spot signal coverage and hotspot capacity improvement can be effectively solved through 5G HetNets, and thereby, the resource utilization and capacity enhancement of wireless mobile communication systems can be enhanced [10]. As intense user devices are connected towards the network, the 5G HetNet density will be highly maximized.

The placement density of diverse forms of fewer power nodes in the case of different wireless broadcast methods will reach 10 times greater than the coverage area [11]. The huge small cell exploitation and coexistence of numerous heterogeneous network nodes are subjected to adverse challenges in handover based security aspects and network administration [12, 13]. In the case of 5G HetNets, handover-based security is critical for real-time data generation, data handling in mobile technology, and data portability. The cellular network has turned into the whole HetNet because of integrated user networks with mobile devices with the entrance of 5G technology [14]. Recently, advanced technologies, including Software Defined Networks (SDN), have gained increasing importance in the growth of next-generation wireless networks [15]. The control plane is detached from the SDN data plane, while its control section meets the control needs in 5G with better management of network flexibility and programmability.

The SDN controller is recommended for the whole cell control in which the SDN switch deals with the behavior variations and data transmission in the network based on the controller commands [16-17]. The combination of SDN in 5G is highly valuable because increased scalability is needed in future mobile networks [18]. The SDN flexibility can render greater benefits towards 5G applications with respect to machine to machine (M2M), human to human (H2H) and quality of service (QoS) communications [19]. The use of a huge variety of user devices tends to complicate handover security, especially when the resource-constrained 5G users have less computing power. Hence, to maintain the handover security, trust between the users is highly necessary to perform an authentication process [20]. A fast and secure connection is required with the elimination of the re-authentication process among handover operators between the heterogeneous cells, possessing less delay.

1.1 Motivation

With the emergence of mobile communication and smart device technologies, the wireless communication network has been upgrading continuously. By establishing hardware and software technology and effectively minimizing the cost of micro base stations, the HetNets have attracted much attention in 5G applications. The existence of numerous heterogeneous network nodes creates a problem in network management and handover security. Because of these emerging drawbacks, excessive handoff latency has resulted in SDN-based 5G HetNets. The re-authentication process is required at handover operators and requires fewer delays due to the lack of proper authentication schemes. On the other hand, the nodes used in the SDN-based 5G HetNet are easy to reach and not particularly trustworthy.

Some of the major assistances of the proposed research work are given as follows.

- To introduce an effectual handover authentication mechanism using deep learning (DHan_Auth) to maintain uninterrupted communication while upholding security measures and upsetting unauthorized access.
- To prevent unauthenticated users from entering the network during the handover process. Upon successful completion of the handover authentication, the communication session smoothly transitions to the new access point, enabling the user to proceed with their tasks seamlessly.
- To develop a novel deep learning approach called convolution stacked LSTM network model (Conv_SLSTM) for categorizing the malicious and non-malicious users effectively. It enhances the classification accuracy and lessens the rates of error possibilities.
- To provide a better handover authentication process for generating keys using 5G Handover-Authentication and key agreement (5G_AKA) protocol and data exchange using extended elliptic curve cryptography (Ex_ECC) to provide strong security with relatively small key sizes.

The rest of the paper is organized into different sections, presented as follows. Section 2 signifies the recent current works commenced by numerous authors in handover authentication using diverse technologies. Section 3 describes the proposed methodology implemented through data classification, encryption, authentication and decryption for presentation assessment. Section 4 represents the results and discussion with the performance analysis of the proposed approach. Section 5 provides the conclusion of the proposed work pursued by feasible future scope and references.

2. Related works

The incorporation of SDN into the 5G cellular network was demonstrated by Monira et al. carried out [21] to enable better handover management and simplify the HetNets. To minimize handoff delay in HetNet's simplified form, pre-authentication and idle-time scanning were employed. Network access was secured through allowed network components through the authentication policy. Device-to-device communication was taken into account during the handover. During reactive handover between domains, 42% of the delay was optimized, and 50% of the lower communication overhead was analyzed. The latency can be greatly minimized with the mobility management approaches. Since the handover decision is based on inaccurate measurements, an effective handover solution cannot be achieved.

Salim *et al.* [22] presented an effective, rapid handover authentication (HO-Auth) system for device authentication using deep learning (DL). The major objective of this approach was to ensure that the blockchain decentralized networks obtain data from legal devices and prevent the cloud applications from corrupting data. For immediate authorization, a user profile based system was generated. The model was trained through the channel state information (CSI) over the movement pattern of users and identified the malicious users who are employed, to be honest. When the profile was retargeted based on user movement, the identification accuracy was maximized to 95%, but due to high network congestion, there was a high authentication delay.

An evolutionary approach that utilizes the fuzzy model was developed by Divakaran *et al.* [23] for handover regulation and key management to enhance authentication performance. Delays and complexities have been minimized when authenticating 5G networks based on nanocore technology. When the model is trained with significant attack data, the attacks can be mitigated, and validation is performed. Performances such as communication effort, spatial complexity and handover latencies were evaluated. Mobile health programs promote secure authentication of input messages and network users against numerous forms of attacks. As handover authentication involves verifying a user's identity with the requirement of exchanging cryptographic keys, high communication overhead has resulted in this study.

Yazdinejad *et al.* [24] proposed an effective authentication approach that adopted SDN and blockchain based approaches to eradicate the re-authentication problems. The authentication process was employed in recurrent handover among the heterogeneous cells. The presented method was effectively intended to promote minimized delay and is highly suitable for 5G networks. The users can be switched with less delay across heterogeneous cells utilizing the private and public keys rendered by the blockchain component with privacy protection. The main advantage of this research work was less authentication handover delay. Energy consumption tends to be high due to computationally intensive cryptographic operations such as encryption and decryption.

In the long term evolution network, an SDN based centralized solution was promoted by Emran *et al.* [25] for handover management. In this research work, the handovers are managed by an SDN controller that holds the whole network management track. The flow entrances were dictated to the open flow switches in the SDN network. The two UEs were associated with two evolved nodes; one UE has undergone handover from one evolved node to another. The data rate of the running application can be widely enhanced with reduced delay. The accuracy of handover evaluations was influenced by the high handover probability, and the handover facilities were not convincing because of the complex handover authentication process.

Zhang *et al.* [26] proposed a robust and universal seamless handover (RUSH) authentication protocol for 5G HetNets to address universality and anonymity issues. The anonymous mutual authentication with the key agreement was allowed for handovers through trapdoor collision stuff exploitation of chameleon hash functions and blockchain tamper-resistance. In the case of all different mobility conditions, universal handover authentication can be attained through RUSH. Authentication can be exemplified through network handover and consistency. Establishing secure authentication depends on the effective management of cryptographic keys. Particularly in environments with a large number of devices, key generation processes can require significant resources. Therefore, it was found that the authentication cost and transmission overhead are very high.

A 5G key organization and handover protocol was proposed by Nyangaresi *et al.* [27] to conquer

Table 1. Analysis of existing works with their limitations

Author name & Reference	**Techniques**	**Contributions**	**Results**	**Limitations**
Monira *et al.* [21]	Pre-authentication and idle time scanning.	To decrease the handover delay and communication overhead during device to device communication.	Handover time, Controller scanning time, Intra and Inter-domain handover.	Appropriate handover solutions cannot be achieved.
Salim *et al.* [22]	HO-Auth scheme	To confirm that the blockchain decentralized networks attain data from legal devices.	Accuracy and authentication requests by device.	Higher authentication delay.
Divakaran *et al.* [23]	Fuzzy evolutionary model	To enhance the authentication performance through handover and key management.	Communication overhead, Space complexity, Handover latency and Executed handover security.	Very high communication overhead.
Yazdinejad *et al.* [24]	Blockchain based authentication approach and SDN methods.	To eradicate the re-authentication problems among the heterogeneous cells.	Signaling overhead, Energy consumption, bandwidth, processing time and handover authentication delay.	High energy consumption.
Emran *et al.* [25]	SDN-based Centralized solution for handover management.	To improve network performance by reducing the delay and growing the data rate when running the application.	Analysis of delay time and data rate.	Degraded accuracy because of high handover probability.
Zhang *et al.* [26]	RUSH authentication protocol	To address anonymity issues through anonymous mutual authentication with a key agreement.	Transmission overhead, computational cost, storage cost and authentication cost.	Less performance over authentication cost and transmission overhead.
Nyangaresi *et al.* [27]	5G key management and handover protocol	To utilize diverse handover triggering parameters to overcome security issues.	Communication overheads, handover latency and space complexity.	Improper mobility management.
Ozhelvaci *et al.* [28]	EAP-TLS	To focus on a seamless and secure handover authentication mechanism.	Security analysis and validation.	Ineffective handover facilities.
Yang *et al.* [29]	Link signature based handover authentication mechanism	To extract the wireless channel characteristics between AP and the user.	Latency, overhead and simulation time.	High latency and simulation time.
Tong *et al.* [30]	MPTCP based handover mechanism	To contribute to network selection, location prediction and handover execution effectively.	Delay, Throughput, Loss rate, cost and handover time.	Increased time and loss rates.

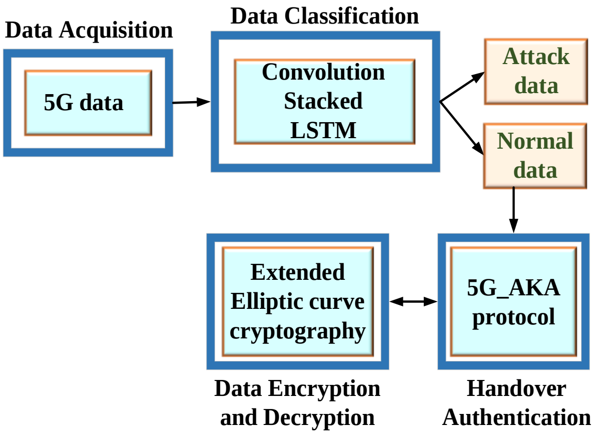

Figure. 1 Proposed architecture

certain performance and security issues. The protocol presented in this paper acts as a multi standards strategy that utilizes power density, path loss, call blocking likelihood, traffic intensity and velocity as delivery activating constraints. The performances like communication overheads, handover latencies, space complexity and the total number of executed handovers were analyzed. Given the significant resources, the protocols developed were not efficient in terms of energy parameters, and mobility was not managed effectively.

Ozhelvaci *et al.* [28] focused on seamless and secure handover authentication mechanisms for promoting rapid mutual authentication. A robust handover authentication protocol called extensible authentication protocols-transport layer security (EAP-TLS) was presented in this work. The protocol depends on the public key infrastructure and utilizes the user certificate, and communication happens between the authentication server and user equipment. The main drawback of this study was that the handover options were not convincing due to the complex interactions between users.

Yang *et al.* [29] introduced wireless link signatures decided through user location in the form of handover authentication data in 5G SDN based HetNets. As the protected context information (SCI), the wireless channel features between the serving access point (AP) and the user were extracted. The authentication performance associated with various attributes was analyzed to demonstrate the authentication strength. Through proper decision threshold settings and sub-ideal performance derivation, optimal performance can be obtained. The latency and overhead were analyzed and compared with existing handover authentication mechanisms. Due to complex authentication procedures, the simulation time and latency proved very high.

Tong *et al.* [30] proposed a mobility-aware seamless handover process dependent upon multipath transmission control protocol (MPTCP) in SDN based 5G enabled nanocore technologies. This work comprises three procedures: network selection, location prediction and handover execution. Initially, the user location was predicted using an echo state network. The target network was chosen utilizing the fuzzy analytic hierarchical process (FAHP) algorithm, and the seamless handover was realized using MPTCP based handover process. The major drawback of this research was increased time delays and loss rates due to insecure data transmission. Table 1 indicates the descriptions of existing methods with their equivalent drawbacks.

If large amounts of data have to be transferred, evaluating direct interactions takes more time. It is computationally complex as there may be huge operations to be done. Diverse networking attacks occur because of ineffective authentication in SDN based 5G HetNets. The signaling overhead becomes high with the increased energy consumption during communication. Most of the work uses machine learning (ML) approaches to effectively classify malicious and non-malicious data. Compared to machine learning, DL has a greater importance in improving classification accuracy due to high trainability. Hence, mutual authentication amongst 5G users and gNBs is mandatory to endure attacks. To overcome the existing problems, an effective handover authentication mechanism using DL is proposed to achieve better QoS.

3. Proposed methodology

On consideration of core technology aspects in 5G networks, higher data rates can be obtained through HetNet compared to real-time applications. The densification of the 5G network environment overcomes the signal asset coverage issues in blind spots and maximizes the data necessities in great density parts. But, in most of the existing research works, security attacks are found to be the major concern because of improper authentication. The major issue developed in SDN based 5G HetNet is rapid authentication for linking devices between diverse gNBs. The maximized potential due to slower handover authentication permits an attacker to present security attacks that influence the data security and QoS in heterogeneous cells. Fig. 1 demonstrates the schematic architecture of the proposed model.

Initially, the 5G data are collected, and the SDN based 5G HetNets are considered with the initialization of 5G users and gNB. To overcome the re-authentication process and to provide better

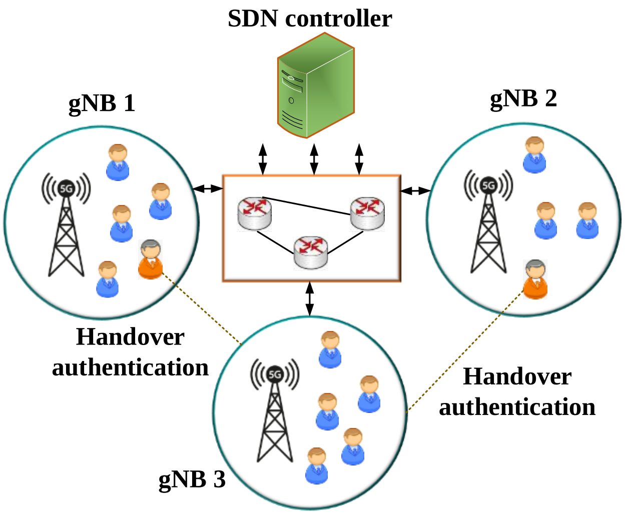

Figure. 2 Schematic workflow of the proposed model

services to the users, a novel DHan_Auth model is proposed. The initial step is classifying malicious and non-malicious data through a DL model called Conv_SLSTM. To enhance handover process and security against network attacks, only the non-malicious user data are authenticated through the key generation and 5G_AKA protocol. The data exchange process is carried through Ex_ECC, and the process of encryption and decryption can be undertaken. After the fruitful authentication, the BS guarantees related QoS to the users. The input data is initially fed into the convolutional layers of Conv_SLSTM, and the significant deep features can be extracted. The extracted features are fed over the pooling layer, and the unwanted features can be diminished. Then, the features are processed using the SLSTM model, and finally, the normal and attack are classified as effective using the fully connected layer.

- ***Convolutional layer:*** The conforming input data features are designated as the summary of the convolutional layer. The original data form is filtered in this layer, and a convolution operation is carried out. The deep data features can be extracted and fed over the pooling layer through this layer.
- ***Pooling layer:*** The pooling layer progressively minimizes the feature size to reduce the amount of parameters and computational complexity and to overcome the overfitting difficulties. The pooling layer encapsulates the features from the convolution layer and also controls the feature resolution to improve stability.
- ***SLSTM layer:*** The SLSTM layer is employed to learn the long-term addictions of data to overcome the vanishing gradient problems and improve the training process.
- ***Fully connected layer:*** In case of classification problems, the fully connected layer integrates the features for data classification.

3.1 System model

To mitigate the limitations in SDN based 5G HetNets, the proposed research work presents an Efficient Handover Authentication Mechanism Using the DL model. Fig. 2 demonstrates the system model of the proposed methodology.

The amount of users considered in the simulation of the projected experiment is 200, and 3 gNBs are deployed. An SDN controller is called the domain controller, which is responsible for the process coordination of the authoritative domain. It can trace any form of network equipment, like end devices and switches, within its domain. The open flow enabled SDN switch, also called a cell switch, is accountable for cell management. The switches manage the 5G geographical cell under the supervision of the SDN controller. It links diverse end users within the geographical coverage area. Table 2 signifies the notations used in the handover initialization and authentication phase.

3.2 Data acquisition

The proposed DHan_Auth model employs a 5G attack detection dataset as the input, comprising intercepted 5G network data. The dataset includes normal and attack data created in a simulated environment [31]. The data are gathered through an internet associated Linux machine running a 5G core network applied with open source free 5G core software. The Wireshark application captures all network traffic on the 5G core machine boundaries.

3.2.1. Normal data model description

The normal data is categorized into data collection with one user equipment simulation and data collected using two user equipment simulations.

3.2.2. Attack data model description

The malicious data includes ten attacks that come below three major groups: reconnaissance, denial of service (DOS) and network reconfiguration. The access and mobility management function looking for a unified data management (ALU) attack, get all network functions (GAF) attack, get user data (GUD) attack, automatic redirect with timer (ART) and

Table 2. Notations and its description

Notations	Description
q_{t-1}	Information quantity from the previous layer
W_{PF}	weight matrix amongst $P_t$andF_t
W_{qF}	weight matrix amongstq_{t-1}andF_t
B_F	The bias factor of forget gate
B_G	Bias factor of the input gate
$\hat{z}_t$	Intermediate cell input state
$E_{S(a,b)}$	Elliptic curve
PRK	Private key
PUK	Public key
SEK	Secret key
$SUCI$	Subscription Concealed identifier
AMF_1	Access and Mobility Management Function
$AUSF$	Authentication Server Function
$SEAF_{ID}$	Security Anchor Function
$ARPF$	Authentication Credential Repository and Processing Function
$v_{UE}, v_{AMF}, v_{ARPF}, w_{uE}, w_{N2}$	The private key of user equipment, AMF and ARPF
$W_{UE}, W_{N2}, V_{UE}, V_{AMF}, V_{ARPF}$	The secret key of user equipment, AMF, ARPF and AUSF
$R*/ER*$	Response/ Expected response at user equipment and AUSF
$HER*/EHER*$	Response/ Expected response at user equipment and AMF
$K_{AUSF}/K_{SEAF}/K_{AMF}$	Access key at ARPF, AUSF and AMF/User equipment
NGK	Next generation key identifier
K_{N1}^{UE}/K_{N2}^{UE}	Session key between the user equipment and $N1$ /$N2$
$AUTN$	Authentication token
$MG_{AMF}, MC_{UE}, MC_{N2}$	Message authentication code
$INFO_{UE}$,$INFO_{N2}$	Authentication information
PL_{ID}	Public Land Mobile Network
EXP_T	Expiration time of HOM_{UE}
$ID_{N2}, W_{N2}. MC_{N2}, INFO_{N2}$	Handover command

random data dump (RD) attack comes under reconnaissance attack. The fake access and mobility management function insert (FAI) attack, fake access and mobility management function delete (FAD) attack, random access and mobility management function insert (RAI) attack, random access and mobility management function delete (RD) attack come under the network reconfiguration attacks. The crash network repository function attack (CN) comes under the DOS attacks.

The entire dataset has been downloaded from https://github.com/IdahoLabResearch/5GAD. Using Wireshark software, the data present in the above link can be viewed. The data has been divided into 80% for training and 20% for testing, and the total number of records is 50,000. The obtained data are exported in a .csv file and are used in the proposed research work. The attribute details like time, source, destination, protocol, length, sequence numbers (Seq), acknowledgement numbers (Ack), window size (Win), length (Len), timestamp echo reply field (TSecr) and timestamp value field (TSval) are considered in this work.

3.3 Model training and data classification

Using the proposed classifier model, the malicious and non-malicious user data can be precisely classified. The framework of the proposed model has been provided clearly in the upcoming sub-section.

3.3.1. Framework of the proposed model

In the DHan_Auth model, only the normal data must be encrypted and authenticated for better services. The normal and attack data are initially classified using the Conv_SLSTM model to eradicate the attack data. Convolutional LSTM is a special form of recurrent neural network (RNN) that combines the attributes of convolutional layers and LSTM units. This fusion allows them to effectively process large datasets by reusing acquired features in different sections of the input. Unlike standard LSTMs, which deal with the vanishing gradient dilemma and delay the training of extended sequences within deep networks, convolutional LSTMs tend to mitigate this challenge to some extent. This is due to their convolutional architecture, which helps maintain gradient flow during backpropagation. The input data are fed as the input towards convolution layers for extracting some relevant features, the obtained features are served as the input to the stacked LSTM structure. The computational complexity can be greatly minimized through high

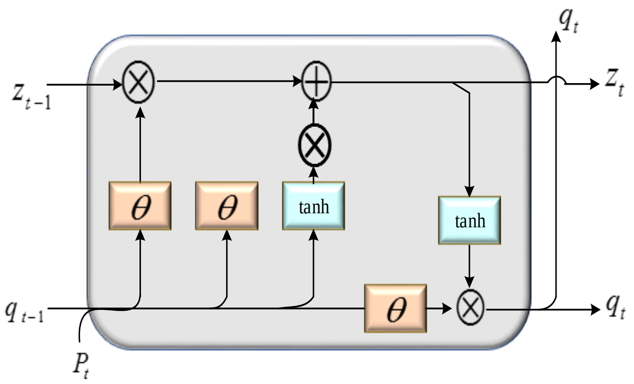

Figure. 3 LSTM architecture

parameter range settings like input bias, output bias and learning rate. In an LSTM cell, a memory cell is integrated that can obtain the information present in memory for a longer duration. As an advanced version of RNN, the vanishing gradient problem can be effectively minimized, and long term dependencies can be acquired in LSTM [32]. There are three gates included in the LSTM input gate, output gate, and forget gate. The neurons in LSTM includes three gates and memory cell. The fundamental design of LSTM is portrayed in Fig. 3.

In order to determine the information quantity from the previous layer q_{t-1}, which has to be forgotten depending on the current input, the forget gate is utilized. The mathematical formulation for the forget gate outcome is given as follows.

$$F_t = \theta\left(W_{PF}P_t + W_{qF}q_{t-1} + B_F\right) \tag{1}$$

From the above equation θdenotes the sigmoid activation function, W_{PF}represents the weight matrix amongst P_t and F_t . W_{qF} means the weight matrix amongstq_{t-1}andF_t. The trainer input at the time$t$ is indicated asP_t, the previous hidden layer outcome is denoted as q_{t-1}, and the forget gate bias factor is specified asB_F. The input gate is used for analyzing the network input amountP_t in the present cell state. The input gate can be expressed as follows.

$$G_t = \theta\left(W_{PG}P_t + W_{qG}q_{t-1} + B_G\right) \tag{2}$$

From the above equation, $B_G$represents the bias vector, W_{PG} represents the weight matrix between P_t and G_t, W_{qG} specifies the weight matrix betweenq_{t-1}andG_t. The output gate is employed for analyzing the information amount directed over the LSTM network from $z_t$cell state. The LSTM gates act as a fully connected network whose input signifies a vector and output signifies a real number. The output gate can be mathematically implied as follows.

$$H_t = \theta\left(W_{PH}P_t + W_{qH}q_{t-1} + B_H\right) \tag{3}$$

From the above equation, B_H signifies the bias vector, W_{PH} specifies the weight matrix between P_t and H_t , W_{PH} indicates the weight matrix betweenq_{t-1}andH_t. The outcomes of LSTM are cell output state z_t and layer output q_t that can be formulated in the below given equations.

$$z_t = F_t \otimes z_{t-1} + G_t \otimes \hat{z}_t \tag{4}$$

$$q_t = H_t \otimes tanh(z_t) \tag{5}$$

The intermediate cell input state is denoted as $\hat{z}_t$, that has been formulated as follows.

$$\hat{z}_t = tanh(W_{Pz}P_t + W_{qz}q_{t-1} + B_z) \tag{6}$$

From equation (6),B_z indicates the bias vector, W_{Pz}specifies the weight matrix amongst$P_t$and$\hat{z}_t$, and the weight matrix amongst$q_{t-1}$and $\hat{z}_t$is denoted as W_{qz} correspondingly. Even though LSTM possesses a robust approach, suitable information cannot be utilized from future data. Hence, a stacked LSTM network with two hidden LSTMs in opposite directions to a similar output has been utilized. The construction of the Conv_SLSTM approach is illustrated in Fig. 4.

The information from both directions can be integrated using stacked LSTM. The forward LSTM directs the input from left to right, the hidden state $\vec{q}_t$ on based on P_t and $\vec{q}_t - 1$ can be estimated. The backward LSTM directs the input from left to right, the hidden state $\overleftarrow{q}_t$dependent upon $P_t$and$\overleftarrow{q}_t - 1$can be estimated. The concluding hidden state of the stacked LSTM approach that integrates the forward and backward directional vector at a time t can be expressed as follows.

$$q_t = [\vec{q}_t, \overleftarrow{q}_t] \tag{7}$$

The forward LSTM in the stacked LSTM network model is indicated as$\vec{q}_t$, and the backward LSTM is specified as$\overleftarrow{q}_t$.

3.4 Handover authentication

The public and private keys are initially generated using the RSA [33] model, and the non-malicious

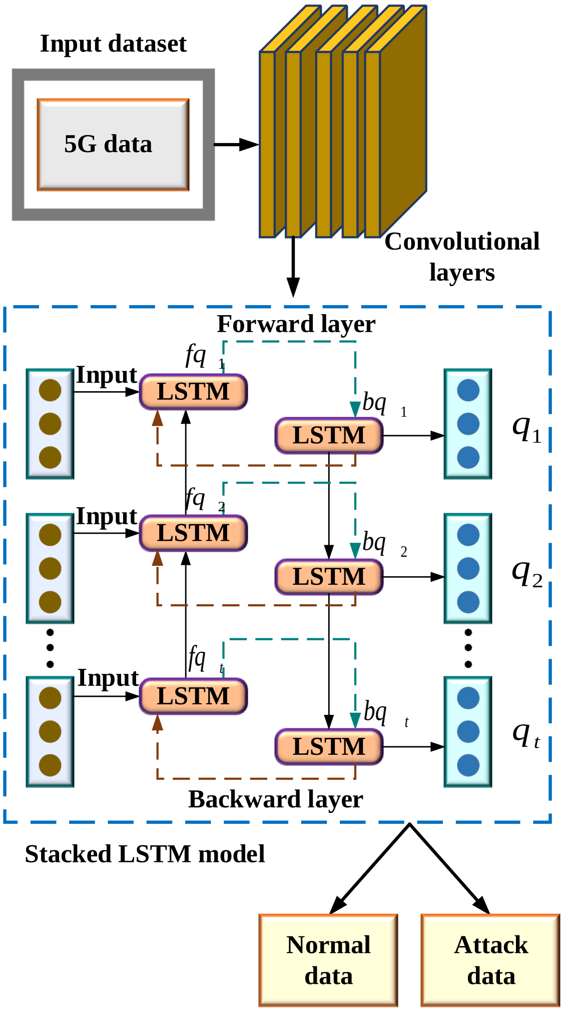

Figure. 4 Conv_SLSTM model architecture

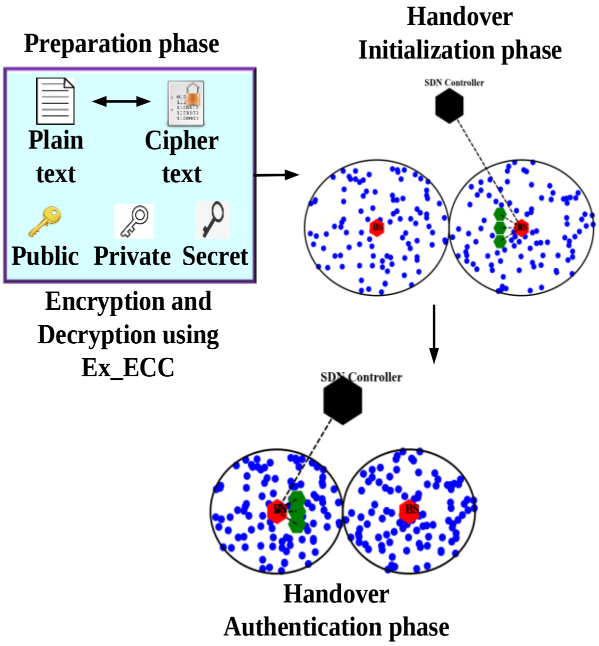
Preparation phase
Plain text
Cipher text
Public
Private
Secret
Encryption and Decryption using Ex_ECC
Handover Initialization phase
SDN Controller
BS
Handover Authentication phase

Figure. 5 Handover authentication process

data are authenticated using the 5G_AKA protocol. The 5G_AKA protocol includes strong security measures that effectively protect user identities and sensitive data throughout the handover process. By guaranteeing that sensitive information remains secret during authentication, the protocol maintains user privacy. Using the 5G_AKA protocol for handover authentication optimizes fast authentication procedures and limits service interruptions during transitions. Additionally, the protocol optimizes the allocation of resources during handoff and confirms that critical resources are available at the intended base station. This optimization increases network performance and reduces congestion. The data exchange process is carried through Ex_ECC, where encryption and decryption can be undertaken. To overcome the re-authentication issues and security susceptibilities, the 5G_AKA protocol is employed. The presented protocol comprises three phases that are given as follows.

- Preparation phase
- Handover Initialization phase
- Handover authentication phase

The meaning of Ex_ECC and security conventions are implied during the preparation phase. The user equipment is verified at Access and Mobility Management, and the node$N1$transfers the handover message towards the user equipment for effective communication during the initial authentication phase. When the user equipment arrives at the coverage area of a node$N2$from the node $N1$, the user equipment and the node $N2$performs the handover authentication process. Fig. 5 illustrates the processes involved in handover authentication.

3.4.1. Preparation phase

The ECC [34] acts as a public key encryption approach that depends upon the elliptic curve theory. The Ex_ECC denotes a curve based approach that possesses an appropriate base point evaluated from the functions of prime numbers. Since the ECC approach is more difficult to implement, the probability of implementation errors increases, reducing the algorithm’s security. To improve the security of the algorithm, Ex_ECC is utilized in the proposed work to produce the secret keys. In contrast to cryptographic algorithms such as RSA, Ex_ECC ensures robust security even with relatively short key lengths. This quality is particularly beneficial for resource-limited devices where storage and processing capabilities are of utmost importance. Ex_ECC requires fewer computing resources,

Received: July 14, 2023. Revised: September 26, 2023.

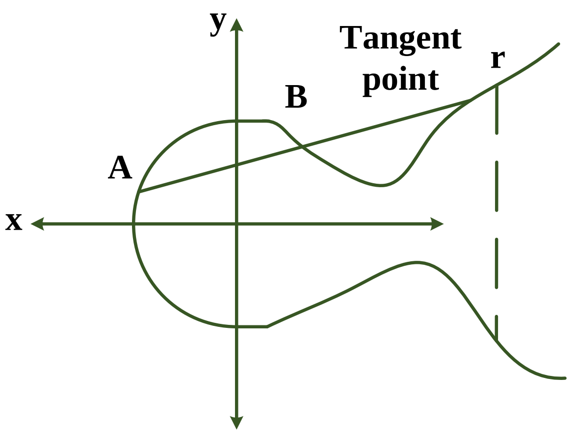

Figure. 6 Elliptic curve sample

including processing power and memory, compared to traditional methods such as RSA. The keys are generally more compact than those used by other cryptographic techniques, resulting in higher memory usage and more efficient transmission time. This aspect is particularly important in scenarios with limited storage capacity. Ex_ECC can be adapted to both resource-constrained environments and high-performance environments. The generated secret is integrated with the encryption formula and is subtracted during decryption. The intricacy of the two phases is augmented in this way, and if the encryption-decryption intricacy is elevated, original data detection tends to be complex. This process can automatically enhance data security. The elliptic curve sample is illustrated as follows in Fig. 6.

The mathematical illustration of Ex_ECC is deliberated using the below equation as follows.

$$q^2 = p^3 + ap + b \tag{8}$$

From the above equation, a and b denotes the elliptic curve integers. Assume$E_{S(a,b)}$as an elliptic curve, the elliptic point can be mathematically expressed as follows.

$$B = zA \tag{9}$$

From the above equation, B and A indicates in curve $A \in E_{S(a,b)}$ and$z < r$. Evaluation of$B$and$A$is simple, but the evaluation of $z$tends to be difficult and $z$indicates the trapdoor or one-way function. The elliptic curve$E_{S(a,b)}$is signified with parameters$a$,b the prime or integer value is indicated as Swhich represents2^k.

Three forms of keys are generated using Ex_ECC in which the public key is generated for encryption, the private key is generated for data decryption, and the secret key from the private-public key is generated at last. Consider the base point$B_x$on the curve and select a random number between 0 to$L - 1$ for generating a private key PRK. The public keyPUK can be generated using the below given equation.

$$PUK = PRK * B_x \tag{10}$$

Consider the below mentioned equation,

$$PUK = \prod(PRK, B_x) \tag{11}$$

From the above equations,PUKdenotes the public key,PRKrepresents the private key and indicate the point on an elliptic curve. The secret key can be created through the summation of PRK , PUK and$B_x$that can be expressed as follows.

$$SEK = \sum(PUK, PRK, B_x) \tag{12}$$

From the above equation, SEK indicates the secret key. After the generation of keys, the data can be encrypted, and the encrypted information comprises two cipher texts. The mathematical expression of two ciphertexts can be mathematically indicated as follows.

$$CIP_1 = (1SEK * B_x) + SEK \tag{13}$$

$$CIP_2 = M + (1SEK * PUK) + SEK \tag{14}$$

From the above equation, CIP_1andCIP_2indicates ciphertext 1 and ciphertext 2. The random number is indicated as$1SEK$that ranges between 0 and$L - 1$. The original information is denoted as$M$. The inverse of the encryption process is decryption, and the secret key created during the decryption phase is subtracted from the general equation given as follows.

$$M = ((CIP_2 - PRK) * CIP_1) - SEK \tag{15}$$

3.4.2. Handover initialization phase

During this stage, the user equipment is authentic at AUSF, ARPF and AMF through the execution of the projected protocol. After the fruitful user equipment verification, the exchanges secret session key towards$N1$, and it directs the message to a user for the upcoming handover procedure.

The steps involved in the handover initialization phase are described as follows.

Step 1: In this phase, the user equipment chooses the random number $v_{UE} \in C_q^*$ and produces $V_{UE} = v_{UE}.PRIME$. To initialize the full authentication

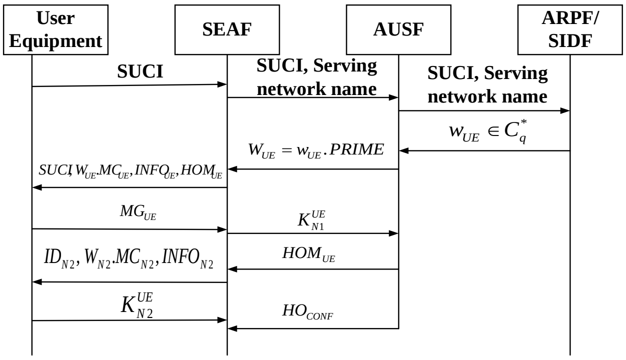

Figure 7: Handover authentication process

process with AMF_1 , $AUSF$ and $ARPF$, the user equipment transfers $MG_{UE}, SUCI, V_{UE}$ and V_{AMF} towards AMF_1 . The Subscription Permanent Identifier (SUPI) undergoes the same role as that of International Mobile Subscriber Identity (IMSI) in the 5G_AKA protocol, SUPI can never be transmitted. The Subscription Concealed identifier (SUCI) obtains the process and only$ARPF$ decrypts SUCI using the Subscriber Identity De-concealing Function (SIDF).

Step 2: The AMF_1 then verifies the message$MG_{UE}$and selects the random number$v_{AMF} \in C_q^*$, in which the secret key can be generated as$V_{AMF} = v_{AMF}.PRIME$. Then theAMF_1transfers the particulars $MG_{AMF}, SUCI, V_{AMF}, V_{UE}, V_{ARPF}, SEAF_{ID}$ towards$ARPF$.

Step 3:$ARPF$verifies the message, and the user equipment is authenticated. $ARPF$ verifies$SEAF_{ID}$obtained from$AMF_1$and matches with the users$SEAF_{ID}$. If it is matched, authentication is provided. The $ARPF$ selects $v_{ARPF} \in C_q^*$ and generates a secret key$V_{ARPF} = v_{ARPF}.PRIME$. Also, $CIP, INK, ER *, AUTN_{ARPF}, K_{AUSF}$ can be computed. The particulars are then transferred from $ARPF$ to$AUSF$.

Step 4: $AUSF$ receives the message from $ARPF$ and accumulates the $ER *$. It then evaluates $HER *, AUTN_{AUSF}, K_{SEAF}$ and transfers$AUTN_{AUSF}, V_{AUSF}$ to theAMF_1.

Step 5: The AMF_1 then transfers the particulars $HER *, V_{AUSF}, V_{ARPF}, NGK$ to the user equipment, and it computes $HER *, ER *, K_{AUSF}, K_{SEAF}, K_{AMF}$. Both are compared, and if it matches, $ARPF$ and$AUSF$ are authenticated. Also, the user equipment transfers $R *$toAMF_1.

Step 6: AMF_1 evaluates $HER *$ and compares with $EHER *$. If it matches, then successful authentication is considered and$K_{AMF}$is computed. Then AMF_1 transfers $R *$ to $AUSF$, then$SUCIandK_{N1}^{UE}$ transfers to$N1$.

Step 7:$AUSF$receives$R *$and compares with$ER *$. For a valid comparison, the user is authenticated to$AUSF$. Additionally,$N1$evaluates the handover message HOM_{UE} and transmits it to the user equipment for future handover. Finally, the user equipment computesK_{N1}^{UE} and makesHOM_{UE}highly secure.

3.4.3. Handover authentication phase

When the user equipment arrives into the coverage area of the node$N2$, mutual authentication and key agreement procedure is commenced between $N2$ and user equipment. The interaction diagram for the handover authentication process is described in Fig. 7.

The steps involved in the handover authentication phase are labelled as follows.

Step 1: When the user equipment enters the node's coverage area$N2$, the user equipment chooses a random number$w_{UE} \in C_q^*$ and evaluates$W_{UE} = w_{UE}.PRIME$. Now, MC_{UE} is computed and $SUCI, W_{UE}.MC_{UE}, INFO_{UE}, HOM_{UE}$ is transferred over$N2$.

Step 2: Once the message is received from user equipment, $N2$ evaluates K_{N1}^{UE} from HOM_{UE} . The validity of $HOM_{UE}$is checked depending on theEXP_T. For successful verification, $N2$believes that$MC_{UE}$is transmitted.

Step 3: In AMF handover, the node$N2$connects with AMF_1 that comprises of$PL_{ID}, EC, PC.AMF_1$Receives the appeal message and sends the handover acknowledgement to$N2$.

Step 4: The node$N2$chooses a random number $w_{N2} \in C_q^*$ and evaluates $W_{N2} = w_{N2}.PRIME$. The secure secret key is computed as K_{N2}^{UE} and created $MC_{N2}$for the user equipment. Then, the handover command $ID_{N2}, W_{N2}.MC_{N2}, INFO_{N2}$ is transmitted to the user equipment.

Step 5: The user equipment evaluatesK_{N2}^{UE} and verifies withMC_{N2} . If it matches, the handover confirmation messageHO_{CONF} is send to$N2$for the acknowledgement session key. After obtaining theMC_{N2},$N2$ confirms the handover completion with the user equipment.

The handover authentication delay can be reduced by overcoming the reauthentication issues using the 5G_AKA protocol. When the user enters from one location to another, the coverage area deviation can be overcome, and the user can authenticate the data efficiently. With the proposed DL model, only non-malicious users are authenticated so that the attack data cannot be

Table 3. Device configuration details

Sl. No	Parameters	Configuration
1	System type	64-bit operating system
2	Installed RAM	8.00 GB
3	Device name	SSM107
4	Processor	Intel(R) Core(TM) i5-3470 CPU @ 3.20 GHz

Table 4. Performance metrics and its description

Performance Metrics	Description	Mathematical formulation
Accuracy	The summation of true positive and negative to the overall summation of true and false metrics is termed accuracy.	$A = \frac{W+X}{W+X+Y+Z}$ W -True positive, Z -False negative, X -True negative, Y -False positive.
F1 score	The combination of precision and recall to a single value is an F1 score.	$F1S = 2\frac{PPV \times TPR}{PPV + TPR}$ TPR -True positive rate PPV - Positive predictive value
Precision	The section of substantial information from the assembled data advances the precision performance. It is also referred to as PPV.	$P = \frac{W}{W+Y}$
Recall	The classification results are highly sensitive if the data produces positive cases.	$R = \frac{W}{W+Z}$
RMSE	RMSE designates the standard deviation of classification errors.	$RMSE = \sqrt{\frac{\sum_{p=1}^{M}(x_p - y_p)^2}{M}}$ x -Predicted value, y -Actual value M -Overall data

injected during communication. By confining malicious users to the network, multiple data attacks can be avoided, thereby reducing delivery delay. Implementing the proposed model allows effective 5G handover authentication to be achieved with higher success rates. Through this research, effective QoS can be rendered towards the users. The outcomes obtained during the simulation process are described clearly in the following division.

4. Results and discussion

The result section labels the simulation and investigational inspection to evaluate the outcomes of the projected model in comparison with numerous existing methods. The depiction of simulations, performance evaluation and comparison are designated in the succeeding sections. The presentations of the proposed work are analyzed under the PYTHON simulation platform. The hyperparameters considered in the classification model are activation function as ReLU, initial learning rate as 0.001, batch size as 128, epoch size as 25 and number of iterations as 25. Table 3 specifies the device formation details of the proposed work.

4.1 Performance evaluation measures

To analyze the superiority of the presented approach, performance measures like precision, recall, accuracy and F1 score, root mean square error (RMSE), number of successful handovers and latency are examined. Diverse metrics are evaluated to effectively compare the proposed and existing approaches. Table 4 indicates the description of performance metrics considered with its mathematical description.

4.2 Performance analysis and comparison

The presentation of the proposed model is examined and associated with other prevailing techniques for accuracy, precision, recall, F1 score, RMSE, number of successful handovers and latency. The proposed model is associated with certain prevailing methods to show the model's superiority. The comparison is made in the case of classification and handover authentication outcomes. The performance outcomes like accuracy, precision, recall and F1 score are demonstrated in Table 5.

From the above table, it can be analyzed that the projected DL model obtained better presentation outcomes associated with the prevailing ML based approaches. The performance of the proposed model is examined in comparison with the existing methods like logistic regression (LR), support vector machine (SVM), random forest (RF), naive Bayes (NB) and extreme gradient boosting (XGBoost). The existing methods like RF, NB, LR, SVM and XGBoost are implemented based on the proposed workflow and

Table 5. Performance assessment analysis

Techniques	Accuracy	Precision	Recall	F1 Score
RF	81.34	82.96	81.6	80.6
NB	86.24	84.65	85.69	86.21
LR	87.47	84.96	86.21	85.55
SVM	88.4	88.69	87.45	87.96
XGBoost	89.35	87.59	88.65	86.96
Proposed	**98.9832**	**97.3256**	**98.4356**	**98.7789**

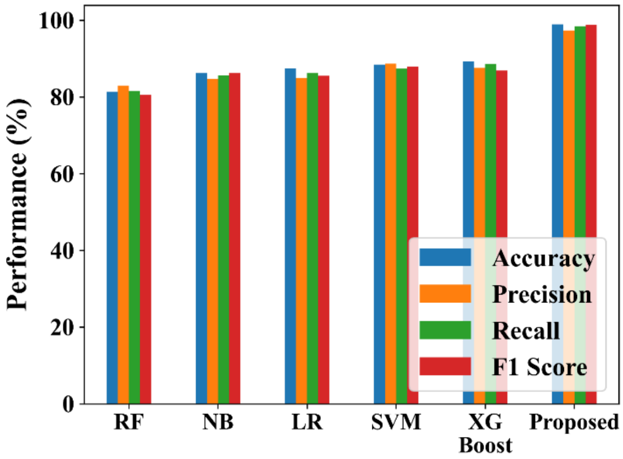

Figure. 8 Classification outcomes

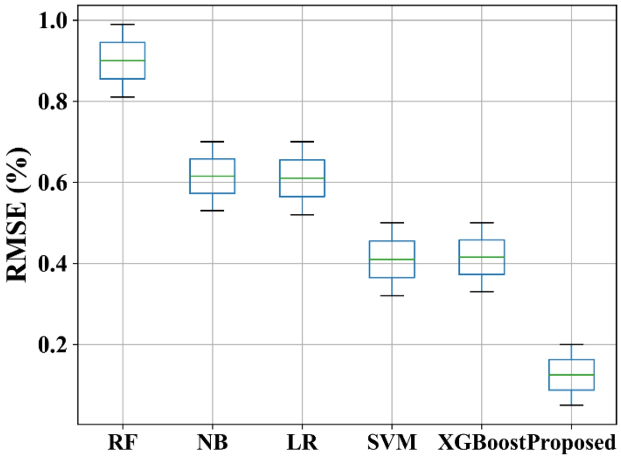

Figure. 9 RMSE performance

compared with the performances of the proposed model. Fig. 8 depicts the general performance attained by the proposed and prevailing models.

A clear examination can be made from the above graphical representation that the accuracy of the projected DHan_Auth approach in attack and normal data classification performs better than the existing models. Based on 5G data, the accuracy of the proposed method is attained as 98.98%, precision as 97.32%, recall as 98.43% and F1 score as 98.77%. A better accuracy rate can be obtained by the DHan_Auth model by focusing on the effective features. Improved training ability and only slight errors are perceived by handling effective features by the classification model. The existing models like RF, NB, LR, SVM and XGBoost have accomplished less performance than the proposed model because of certain drawbacks like huge consideration of features, high testing time and less feature learning capability. Fig. 9 indicates the RMSE performance attained by the proposed and existing techniques.

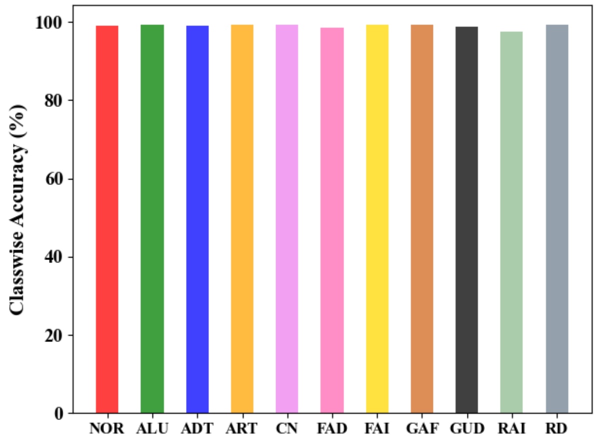

Figure. 10 Classwise accuracy performance

The RMSE value has to be comparatively less for an enhanced classification model. The RMSE presentation of the proposed DHan_Auth model and existing approaches are analyzed. From the above graphical representation, the proposed RMSE is 0.05 respectively. Compared to the RMSE value of the proposed model, existing models like RF have attained 0.81, NB as 0.53, LR as 0.52, SVM as 0.5 and XGBoost as 0.33, which are comparatively high. Because of utilizing incapable features, the existing models are highly prone to increased error rates. Fig. 10 illustrates the classwise accuracy performance of attack and normal data.

The normal class data and ten attack classes, ALU, ADT, ART, CN, FAD, FAI, GAF, GUD, RAI and RD, are effectively classified using the proposed classifier model. The overall accuracy is obtained to be 98.98%, whereas the normal data has attained 98.91% of accuracy. The ALU attack data has attained 99.35%, ADT at 98.95%, ART at 99.31%, CN at 99.31%, FAD at 98.45%, FAI at 99.22%, GAF at 99.32%, GUD at 98.78%, RAI as 97.58% and RD as 99.31% respectively. Fig. 11 illustrates the handover latency performance in the case of some users.

The handover authentication latency can be evaluated by estimating the time taken during the setup of the handover execution. The time taken to obtain handoff authentication by the non-malicious

Received: July 14, 2023. Revised: September 26, 2023.

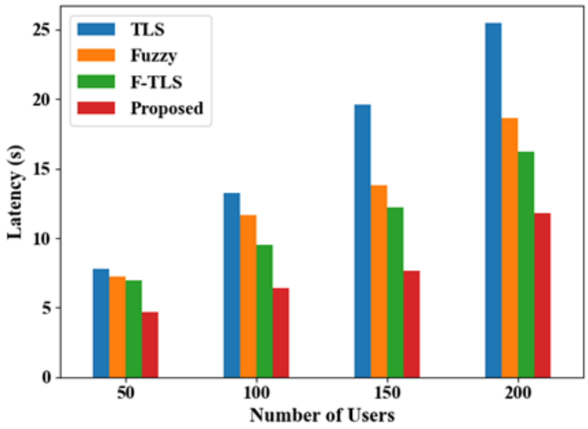

Figure. 11 Handover authentication latency

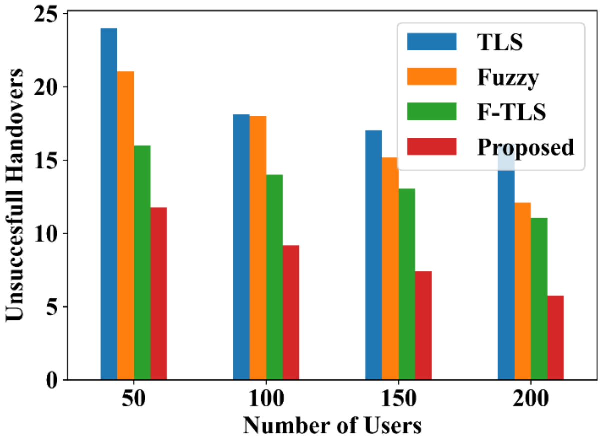

Figure. 12 Number of unsuccessful handover authentication

user node that moved from one location to another is called handoff authentication latency. The existing methodologies [23], like transport layer security (TLS), fuzzy algorithm and huzzy-TLS (F-TLS), are associated with the proposed approach. The handover delay indicates the overall delay experienced by the user during the handover authentication procedure in switching from one location to another. Fig. 12 describes the number of unsuccessful handover outcomes.

The unsuccessful handovers indicate the number of nodes that fail to get proper handover authentication during location migration. The handover delay and the number of unsuccessful handovers are analyzed by varying the number of users from 50-200. The proposed handover latency is 11.8 seconds for 200 users, which is comparatively lower than the existing models. The number of unsuccessful handovers in the proposed model is 5.76 for 200 users, significantly lower than the existing models. Fig. 13 describes the handover delay to some users.

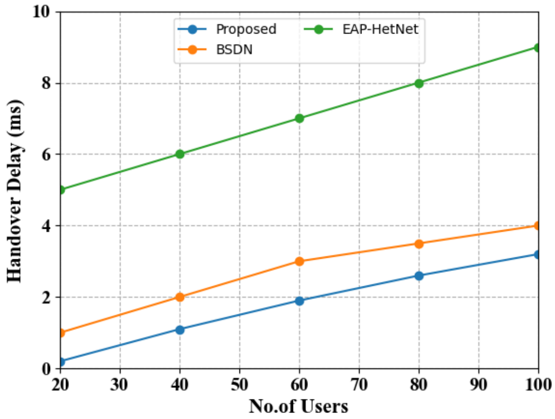

Figure. 13 Handover delay analysis [35]

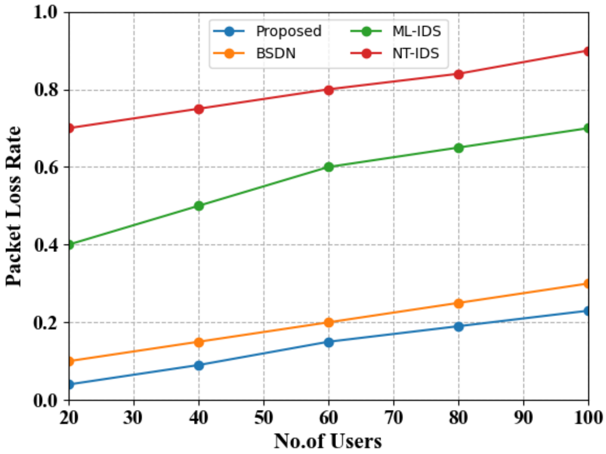

Figure. 14 Packet loss rate performance [35]

The comparison of handover delay between different users is analyzed. Here, the proposed model is compared with the existing techniques such as EAP-HetNet and Blockchain-based SDN (BSDN). The analysis shows that the proposed approach resulted in a lower handover delay than existing solutions. The proposed approach utilized a better handover algorithm that could quickly identify the target base station for the handover operation, resulting in a reduction in latency. Fig. 14 shows the packet loss rate of proposed and existing models with respect to the number of users.

The comparison between the proposed solution and existing methods is presented in terms of packet loss rate. The packet loss rate is determined by calculating the ratio of undelivered packets to the total number of packets sent. The results show that the proposed method outperforms alternatives such as BSDN, multi layered intrusion detection (ML-IDS) and network intrusion detection (NT-IDS) and has lower packet loss rates. In particular, the proposed approach uses an effective security model to ensure enhanced security measures by considering only the non-attack data. Fig. 15 shows the delay of

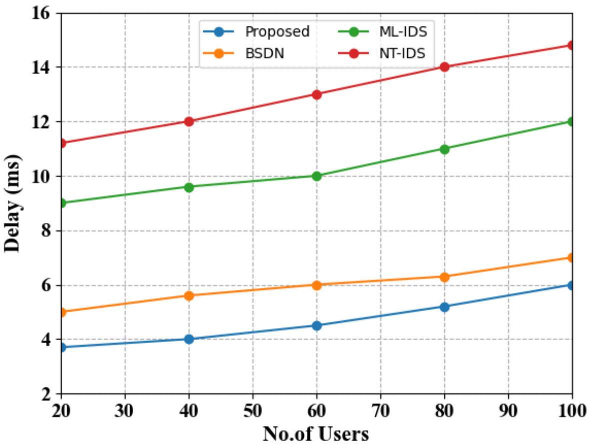

Figure. 15 Delay performance [35]

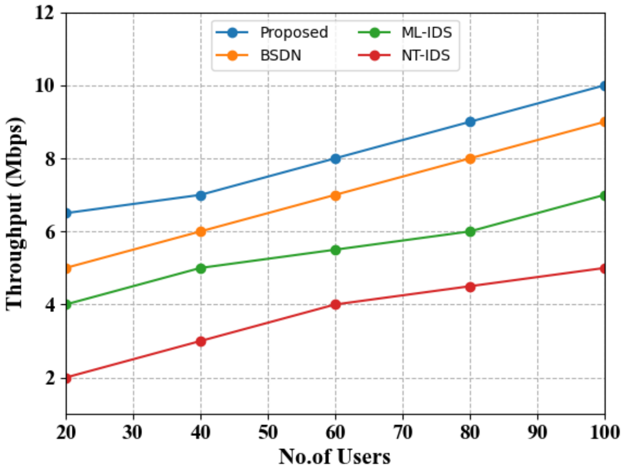

Figure. 16 Throughput performance [35]

proposed and existing models with respect to the number of users.

The delay indicates the additional time for the transmission of packets from the data plane to the control plane. The results show that the proposed model outperforms its counterparts by having a lower delay than the existing models. This is attributed to the early removal of malicious users, thereby reducing the authentication delay. Consequently, the proposed approach quickly identifies malicious users and minimizes the time required for detection. When the number of users is 100, the network delay is 6 ms. The throughput performance of the proposed and existing models is described in Fig. 16.

The volume of data transmitted from the sender to the receiver on considering certain duration of transmission signifies the throughput. The throughput achieved by the proposed method and existing alternatives across multiple users are analyzed. The comparison highlights the superior throughput achieved by the proposed scheme in contrast to existing solutions. This success is attributed to the adoption of an effective

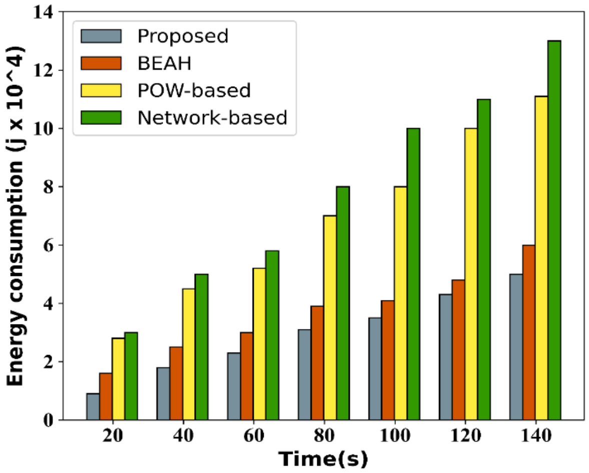

Figure. 17 Energy consumption analysis [24]

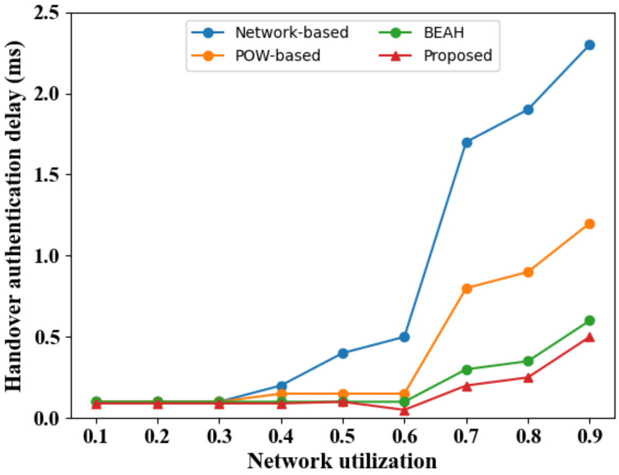

Figure. 18 Handover authentication delay [24]

authentication of non-malicious user data within the proposed approach, enhancing network security. As a result, this security enhancement contributes to elevated data delivery ratios and overall throughput. The throughput of 10 Mbps is attained by the proposed model that is comparatively higher. The energy consumption with respect to varied time is analyzed in Fig. 17.

The findings from this analysis on energy consumption are observed in the simulation. The existing models in terms of POW-based, network-based and blockchain-enabled authentication handover (BEAH) are analyzed. The presented results show that more energy is spent within the network-based model and the Proof-of-Work (POW)-based approach than the proposed method. Considering the existing models, BEAH only consumed less energy, but the proposed model is far superior to the existing models. Fig. 18 shows the comparison of handoff authentication delay versus network utilization.

The comparison of authentication delay between the proposed and the other three methods based on the utilization rate in the 5G network is analyzed. The network efficiency is determined by the ratio of the total data volume to the processing rates of handover authentication and SDN controllers. The productivity rate of the network is defined by various load conditions within the network. During periods of low network load, authentication delay issues do not occur with either the proposed or other methods. However, as the number of users increases and inter-cell mobility accompanied by data transfer operations occurs, the network load increases more in the other two methods compared to the proposed model. Consequently, the proposed model maintains an authentication delay of less than 0.5 ms, making it well suited for 5G networks. With the proposed model, the disadvantages analyzed in the survey section could be overcome through the improved effectiveness of the proposed model.

5. Conclusion

In this research paper, the DHan_Auth approach is proposed for better handover management and key management in SDN based 5G HetNets. The issues of handover delay and re-authentication are highly concentrated to promote an effective handover authentication process. The 5G data were collected initially, and to enhance the data security, the classification of attack data and normal data is performed using DL based Conv_SLSTM model. Considering the network attack resistance and better handover process, only the normal data are authenticated by key generation using the 5G_AKA protocol. The data exchange process is carried out via Ex_ECC while the process of encryption and decryption is performed. The performances are analyzed by evaluating the data using the PYTHON simulation platform. The performances like handover latency, accuracy, precision, recall, RMSE and F1 score are analyzed. Also, the proposed DHan_Auth approach is associated with the prevailing model to prove its superiority. The classification accuracy of the DHan_Auth approach is obtained as 98.98%, precision as 97.32%, recall as 98.43% and F1 score as 98.77%. The handover latency of the proposed model is found to be 11.8s on consideration of 200 nodes. In the future, the proposed work can be protracted by considering different handover issues. Also, effective methodologies will be applied, considering more performance evaluation parameters.

Conflicts of Interest

Authors have no conflict of interest to declare.

Author Contributions

Data collection & references are prepared by Shivanand Manjaraji & Saboji; Literature survey done by Saboji; Implementation part done by Shivanand Manjaraji; Manuscript prepared by Shivanand Manjaraji; Proof read & technical check done by Saboji.

References

[1] X. Yan and M. Ma, “A lightweight and secure handover authentication scheme for 5G network using neighbour base stations”, *Journal of Network and Computer Applications*, Vol. 193, p. 103204, 2021.

[2] Z. Chen, S. Chen, H. Xu, and B. Hu, “A security authentication scheme of 5G ultra-dense network based on block chain”, *IEEE Access*, Vol. 6, pp. 55372-55379, 2018.

[3] T. Ma, F. Hu, and M. Ma, “Fast and efficient physical layer authentication for 5G HetNet handover”, In: *Proc. of 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), IEEE*, pp. 1-3, 2017.

[4] Z. Ren, X. Li, Q. Jiang, Q. Cheng, and J. Ma, “Fast and Universal Inter-Slice Handover Authentication with Privacy Protection in 5G Network”, *Security and Communication Networks*, Vol. 2021, pp. 1-19, 2021.

[5] D. Sangeetha, S. Selvi, and A. Keerthana, “A Trust-Based Handover Authentication in an SDN 5G Heterogeneous Network”, *Computer Networks and Inventive Communication Technologies, Singapore*, pp. 841-852, 2022.

[6] M. Hojjati, A. Shafieinejad, and H. Yanikomeroglu, “A Blockchain-Based Authentication and Key Agreement (AKA) Protocol for 5G Networks”, *IEEE Access*, Vol. 8, pp. 216461-216476, 2020.

[7] H. Yang, Y. Liang, J. Yuan, Q. Yao, A. Yu, and J. Zhang, “Distributed blockchain-based trusted multidomain collaboration for mobile edge computing in 5G and beyond”, *IEEE Transactions on Industrial Informatics*, Vol. 16, No. 11, pp. 7094-7104, 2020.

[8] P. Krishnan, K. Jain, P. G. Jose, K. Achuthan, and R. Buyya, “SDN enabled QoE and security framework for multimedia applications in 5G networks”, *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, Vol. 17, No. 2, pp. 1-29, 2021.

[9] A. Kumar and H. Om, “Handover Authentication Scheme for Device-to-Device Outband Communication in 5G-WLAN Next Generation Heterogeneous Networks”, *Arabian*

Journal for Science & Engineering (Springer Science & Business Media BV), Vol. 43, No. 12, 2021.

[10] K. A. Alezabi, F. Hashim, S. J. Hashim, B. M. Ali, and A. Jamalipour, "Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2020, pp. 1-34, 2020.

[11] J. Cao, M. Ma, Y. Fu, H. Li, and Y. Zhang, "CPPHA: Capability-based privacy-protection handover authentication mechanism for SDN-based 5G HetNets", *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 3, pp. 1182-1195, 2019.

[12] X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer", *In: Proc. of 2016 IEEE International Conference on Communications (ICC)*, pp. 1-6, 2016.

[13] X. Duan, "Software-defined Networking Enabled Resource Management and Security Provisioning in 5G Heterogeneous Networks", *PhD diss., The University of Western Ontario (Canada)*, 2017.

[14] M. J. Alam and M. Ma, "Dc and comp authentication in lte-advanced 5g hetnet", In: *Proc. of GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1-6, 2017.

[15] H. B. Valiveti and P. T. Rao, "EHSD: an exemplary handover scheme during D2D communication based on decentralization of SDN", *Wireless Personal Communications*, Vol. 94, pp. 2393-2416, 2017.

[16] A. Ozhelvaci and M. Ma, "A Robust Vertical Handover Authentication for SDN based 5G HetNets", https://readpaper.com/paper/4283518583

[17] M. S. Abdelhady, W. Anis, A. A. Elhafez, H. Eldemerdash, and A. Abdelaziz, "Novel Framework for Secure Handover Authentication Protocol for 5G Mobile Network", *International Journal of Innovative Technology and Exploring Engineering*, Vol. 9, No. 4, PP. 2334-2339, 2020.

[18] C. Lai, Y. Ma, R. Lu, Y. Zhang, and D. Zheng, "A novel authentication scheme supporting multiple user access for 5G and beyond", *IEEE Transactions on Dependable and Secure Computing*, 2022.

[19] V. O. Nyangaresi, A. J. Rodrigues, and S. O. Abeka, "Machine learning protocol for secure 5G handovers", *International Journal of Wireless Information Networks*, Vol. 29, No. 1, pp. 14-35, 2022.

[20] T. A. Lone, A. Rashid, S. Gupta, S. K. Gupta, D. S. Rao, M. Najim, A. Srivastava, A. Kumar, L. S. Umrao, and A. Singhal, "Securing communication by attribute-based authentication in HetNet used for medical applications", *Eurasip Journal on Wireless Communications and Networking*, Vol. 2020, pp. 1-21, 2020.

[21] S. Monira, U. Kabir, M. Jahan, and U. Paul, "An Efficient Handover Mechanism for SDN-Based 5G HetNets", *Dhaka University Journal of Applied Science and Engineering*, Vol. 6, No. 2, pp. 49-58, 2021.

[22] M. M. Salim, V. Shanmuganathan, V. Loia, and J. H. Park. "Deep learning enabled secure IoT handover authentication for blockchain networks", *Hum. Cent. Comput. Inf. Sci*, Vol. 11, p. 21, 2021.

[23] J. S. Divakaran, S. K. Prashanth, G. B. Mohammad, D. Shitharth, S. N. Mohanty, C. Arvind, K. Srihari, R. Y. Abdullah, and V. P. Sundramurthy, "Improved handover authentication in fifth-generation communication networks using fuzzy evolutionary optimization with nanocore elements in mobile healthcare applications", *Journal of Healthcare Engineering*, Vol. 2022, 2022.

[24] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks", *IEEE Transactions on Network Science and Engineering*, Vol. 8, No. 2, pp. 1120-1132, 2019.

[25] M. Emran, V. Thayananthan, M. Umair, I. Kotuliak, M. S. Qureshi, and M. B. Qureshi, "The Handover and Performance Analysis of LTE Network with Traditional and SDN Approaches", *Wireless Communications and Mobile Computing*, Vol. 2022, 2022.

[26] Y. Zhang, R. H. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5G HetNets", *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 2, pp. 858-874, 2019.

[27] V. O. Nyangaresi, A. J. Rodrigues, and S. O. Abeka, "Neuro-fuzzy based handover authentication protocol for ultra-dense 5G networks", In: *Proc. of 2020 2nd Global Power, Energy and Communication Conference (GPECOM)*, pp. 339-344, 2020.

[28] A. Ozhelvaci, and M. Ma, "Secure and efficient vertical handover authentication for 5G HetNets", In: *Proc. of 2018 IEEE International*

Conference on Information Communication and Signal Processing (ICICSP), pp. 27-32, 2018.

[29] J. Yang, X. Ji, K. Huang, Y. Chen, X. Xu, and M. Yi, "Unified and fast handover authentication based on link signatures in 5G SDN-based HetNet", *IET Communications*, Vol. 13, No. 2, pp. 144-152, 2019.

[30] H. Tong, T. Wang, Y. Zhu, X. Liu, S. Wang, and C. Yin, "Mobility-aware seamless handover with MPTCP in software-defined HetNets", *IEEE Transactions on Network and Service Management*, Vol. 18, No. 1, pp. 498-510, 2021.

[31] C. Coldwell, D. Conger, E. Goodell, B. Jacobson, B. Petersen, D. Spencer, M. Anderson, and M. Sgambati, "Machine Learning 5G Attack Detection in Programmable Logic", In: *Proc. of 2022 IEEE Globecom Workshops (GC Wkshps)*, pp. 1365-1370, 2022.

[32] R. R. Drumond, B. A. D. Marques, C. N. Vasconcelos, and E. Clua, "An LSTM recurrent network for motion classification from sparse data", In: *Proc. of the 13th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*, Vol. 1, pp. 215-22, 2018.

[33] R. Minni, K. Sultania, S. Mishra, and D. R. Vincent, "An algorithm to enhance security in RSA", In: *Proc. of 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), IEEE*, pp. 1-4, 2013.

[34] H. Liang, G. Zhang, W. Hou, P. Huang, B. Liu, and S. Li, "A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography", *Applied Sciences*, Vol. 11, No. 12, p. 5691, 2021.

[35] A. F. Khan and P. Nanda, "Hybrid blockchain-based Authentication Handover and Flow Rule Validation for Secure Software Defined 5G HetNets", In: *Proc. of 2022 International Wireless Communications and Mobile Computing (IWCMC), IEEE*, pp. 223-230, 2022.