Deep Learning Enabled Secure IoT Handover Authentication for Blockchain Networks

Mikail Mohammed Salim¹, Vimal Shanmuganathan², Vincenzo Loia³, and Jong Hyuk Park¹, *  

Abstract
Blockchain is an emerging key technology for safeguarding telecommunications networks against rogue base stations. Combining Internet of Things (IoT) devices with a decentralized network secures data transmission from machines to support cloud-based smart city applications. Critical applications such as Smart Healthcare deploy portable IoT devices such as blood pressure monitors, pacemakers, and electrocardiogram (ECG)-supported smartwatches to provide personalized services to users. Devices frequently move between different base stations to improve their coverage in hotspots and wireless link quality. Immutable ledgers in decentralized base stations ensure that data transmission from base stations to data centers is secure; still, it does not guarantee that the received data is from an authorized device. In the IoT layer, impersonation attacks involve a malicious user spoofing an honest user and transmitting manipulated data to the base station. Attackers impersonate legitimate machines during the handover authentication process when devices move from one base station to another. This paper proposes a fast, efficient handover authentication (HO-Auth) scheme using deep learning to authenticate devices and build a user profile-based system for immediate authorization. The channel state information (CSI) of a user’s movement pattern trains the model and detects malicious users spoofing as honest users. The simulation-based analysis shows an initial profile accuracy of 0.91 in identifying a malicious device. The detection accuracy increases to 0.94 as the profile is retrained based on the movement of the user. The scheme ensures that the blockchain decentralized networks receive data from valid devices, protecting cloud applications from corrupt data.

Keywords
Handover Authentication, Internet of Things, Deep Learning, IoT Security

1. Introduction
Blockchain is an important technology for securing telecom networks and providing seamless service to users. A 5G service guarantees continuous network connectivity to users. Private organizations such as Oracle, Microsoft, and SAP collaborate with other 5G telecommunications networks to build blockchain-based infrastructure. Swisscom in 2018 collaborated with Swisspost to construct a national...
private blockchain infrastructure using Hyperledger Fabric2, providing data security with secure transactions and immutable ledgers. Nonetheless, most of the implementation of blockchain technology in telecom networks is still in its infancy stage, with little or no real-life deployment on a substantial scale. In partnership with SAP and Camelot ITLab, Deutsche Telekom focuses on securing data from malicious users in case of device theft. A system-wide implementation to validate devices moving between different base stations has yet to be accomplished, however. Various service providers such as Reply, a consortium of specialized organizations, help telecom networks build a blockchain network to authenticate Internet of Things (IoT) devices with local networks [1]. Nonetheless, the adoption rate is still low due to the networks’ extensive customer base, requiring a multi-billion-dollar investment [2].

A less expensive alternative to the prevalent technology is necessary for telecom networks to authenticate devices with local base stations.

As a core technology aspect of 5G networks, HetNet provides high data rates to demanding real time-based cloud computing applications. The 5G networks meet data rate requirements by densifying the wireless network and deploying small cells or low-powered base stations proposed by the 3GPP committee. There are different types of base stations such as Femtocell, which is used primarily in the home and office environment along with Wi-Fi; as the smallest among all cells, they have a range of 10 meters. Pico cells cover small but busy areas such as train stations, airplanes, and shopping malls. Microcells have a range of several hundred meters, and they are used to provide coverage in more considerable distances. The 5G network environment’s densification resolves limited signal strength (SS) coverage in blind spots and increases data requirements in high-density areas. Data capacity growth is enabled by thousands of IoT devices supporting real-time cloud computing-based architecture for smart city applications and mobile communication, shifting focus from voice to data-based services [1–3]. The growth of wireless networks and the reduction in base stations’ costs have led to increased interest in both academe and industrial consumption.

In the 5G era, many IoT devices are connected to the Internet request for frequent handover authentication among the different base stations [4]. Compared to existing LTE networks, the coverage area of microcells is expected to increase along with the number of active users. The distance between nodes is expected to decrease to 10m or more up to 25,000 users within a km [5–7]. The objective of cells’ growth is to allow a single node to serve each user [6, 8]. Several active base stations in 5G HetNet handle growing traffic, giving rise to new challenges in network management. Smart devices and portable IoT devices frequently move between different base stations, and current LTE networks are unable to handle large handover requests [9–11]. A new challenge introduced with 5G HetNet is quick authentication and authorization to connect devices between different base stations. Increased latency due to slow handover authentication allows an attacker to launch man-in-the-middle attacks that affect cloud computing-powered critical applications’ data security. An attacker impersonates a machine to receive confidential data and return false data to the smart application, affecting its users’ Quality of Service (QoS) and Quality of Experience (QoE). Base stations or small cell networks have low resources; as such, any delay in authentication results in the suspension of authentication of other devices [12–14]. Several rounds of authentication are required to complete a signaling message exchange between the user equipment (UE) and the base station.

Small base stations such as femtocells that operate along with Wi-Fi in the home and office environments are easily acquired. An attacker can efficiently launch man-in-the-middle and user impersonation attacks [15–17]. The efficiency of the authentication process is essential to handle frequent handover requests and reduce the strain on base station access points. Fast, secure authentication service is required to prevent attackers from spoofing the network to steal user data and from providing smart applications with false information and reducing optimized services offered by 5G systems.

The base station’s key agreement and authorization are required for a device to connect securely [18, 19]. 5G networks do not commonly exist in many countries. As such, there is a research gap in authenticating and authorizing devices quickly and efficiently, especially on low power base stations.
such as femtocells used in hospitals, business offices, and home environments. Inter-connection and authorization are required between different base stations of the 5G network. Moreover, network systems use an authentication server (AS) to authorize devices to roam between different base stations. These servers are vulnerable to cyberattacks and, as such, cannot be trusted for a seamless handover experience. When devices roam between base stations, they are authenticated and authorized using a single server. AS is vulnerable to cyberattacks, and implementing many of such servers results in high latency, which in turn affects device application performance. There is a need for a common authentication mechanism that efficiently operates for all base stations in a 5G network.

Channel state information (CSI) is used by devices to communicate with the base stations such as IoT machines, which serve as a transmitter, and to send data to the base station receiver [20–22]. CSI depends on the communication environment and the receiver’s hardware device; as such, it has its applications for security purposes. When a user moves across different geographical points, however, CSI changes, making differentiating between an attacker and a real user challenging. The data gathered from CSI supports building a model that analyzes the distance measurements, such as channel fading and frequency responses. A stationary device’s CSI data remains static due to lack of movement; for a device such as a smartphone that moves along with the user, however, the CSI data keeps changing.

Modern cloud computing-based applications benefit from the fast data rates of 5G networks for quick data transmission from IoT devices to improve system performance and real-time analysis. Nonetheless, weaknesses in the security protocol expose user devices to attackers during cyberattacks. The 5G AKA Protocol process explained in [23] has security vulnerabilities that allow an attacker to impersonate any user. The AKA protocol’s main objective is to establish a mutual connection between the UE and the SN. In conjunction with the HN, a session key or a anchor key called K_seaf, which is a secret key, is determined. The key during the AKA protocol is believed to come from an honest, uncompromised UE. The attacker determines the secrecy of the anchor key, K_seaf, and impersonates the UE due to a lack of containment policy [24–26]. The attack occurs when a user initiates the AKA protocol and completes it as a normal session. The attacker eavesdrops on public radio transmission and records the SUCI data. Using a legitimate USIM, the attacker disables and extracts the long-term key established during the AKA protocol. The attacker is now free to impersonate an authorized user and receive confidential data, consequently sending malicious data to the base station.

In this paper, a new handover authentication (HO-Auth) scheme is proposed using a deep learning-based recurrent neural network (RNN) algorithm. The scheme builds a user profile for existing blockchain-based decentralized networks requiring secure handover authentication. It addresses attackers spoofing real users to steal confidential data and transmit corrupted data to cloud computing-powered critical smart applications. CSI data is collected to build a user profile, which correlates with the device’s movement pattern. Environmental factors such as concrete walls affect the collected CSI data’s accuracy and negatively impact a unique device fingerprint’s profile building process. A static device fingerprint can be learned by an attacker and used negatively against the network. Note, however, that the HO-Auth scheme relies instead on understanding the user’s movement pattern, which an attacker cannot imitate despite the environmental impact on the CSI. A user’s movement pattern does not remain the same, so the profile differs each time. The user profile is retrained as the user shifts his/her position when approaching a different base station for handover authentication. The retention of user profile prevents an attacker from building a fake profile. In this paper,

- We analyzed the CSI movement pattern collected from multiple receivers to differentiate between the attacker and the honest user.
- An initial profile-based detection was designed to prevent attackers from launching impersonation attacks before a full user profile is created.
- The Ho-Auth scheme reduces false alarm rates by analyzing the count of authentication requests received from devices.
- A full profile using the long short-term memory (LSTM) algorithm prevents an attacker from imitating the honest user.
• The experimental analysis showed high accuracy in the initial profile building to detect malicious devices.
• Detection accuracy increases as multiple access points are used to build the user profile.

The rest of this paper is organized as follows: Section 2 discusses the existing research on the authentication of devices in 5G networks in detail; Section 3 presents the proposed HO-Auth scheme with its general overview, and the methodology is described in detail; Section 4 focuses on examining the HO-Auth scheme’s validity based on initial and retrained user profile building; finally, Section 5 presents the conclusion.

2. Related Works

In this section, we study in detail recent research in the field of HetNet-based HO-Auth schemes securing networks. Zhang et al. [27] addressed the security challenges of frequent handover mechanisms such as universality, anonymity, and reliable traceability and proposed Robust and Universal Seamless Handover (RUSH) authentication protocol in 5G HetNets. RUSH achieves several key characteristics of a secure mechanism such as perfect and master key forward secrecy, randomness, anonymity, key agreement, traceability, and universality. Mutual authentication using a key agreement method is achieved using the trapdoor collision property of a chameleon hash function and blockchain technology. Two random values and long-term secret keys between two participants based on the Elliptic-curve Diffie-Hellman key agreement provide perfect forward, master key forward, and known randomness secrecy. The authentication, authorization, and accounting (AAA) server detects any malicious device by computing a chameleon-based hash function from authentication messages and compares the hash function with the one recorded in the blockchain. Inter-domain authentication is similar to intra-domain authentication by benefitting from blockchain technology’s immutable consistent data management. Security proof and analysis of the RUSH protocol based on BAN logic and verification using the AVISPA tool show resistance to malicious attacks.

Frequent movement of users among different cells results in repeated authentication attempts by the base station and delay, affecting the 5G network’s QoS. Yazdinejad et al. [28] proposed a new approach to efficient authentication using blockchain and SDN technology by removing repeated re-authentication attempts in 5G HetNets. A blockchain center (BC) is present and is used to store and produce the encryption of parameters like device identification, certification, and unique data related to the device under a false name. Each new device in the network registers to join the cell and uses a pseudo name when moving from one base station to another, allowing it to alter any identifying information. Blockchain ledgers managed by mobile operators are used to store the details of mobile users. Once identified, malicious users are traced using the blockchain ledger and publicly announced to the mobile network, allowing their removal. SDN controllers oversee the system, form part of the blockchain's consensus mechanism, and validate all network transactions. An analysis of the approach showed reduced latency by removing multiple re-authentication attempts, making it suitable for 5G networks.

Cao et al. [29] presented a capability-based privacy protection (CPP) handover authentication mechanism for SDN-based 5G HetNets by integrating user capability and SDN. The CPP mechanism allows users on 5G networks to control the security information directly and enforce security goals directly on the base station; thus foregoing the need for complex communication protocols between devices and authentication server. The CPP architecture collects traffic flows, enabling the SDN controller to monitor and determine users’ location and movement routes on the 5G network for the selection of the relevant nodes and ensure seamless handover authentication. The architecture using SDN provides mutual authentication and key agreement between devices and base stations. The CPP satisfies essential security properties such as anonymity, traceability, unlinkability, and fewer handover costs compared to other existing models. The CPP’s security analysis is done using BAN logic and
Scyther, a verification tool that realizes reduced computation and communication costs compared to other recent research on 5G HO-Auth schemes.

Cao et al. [30] proposed an authentication and re-authentication protocol for massive machine-type communications in 5G HetNets. A grouping method and an Aggregate MAC collect multiple handover authentication requests and concurrently authenticate devices as they move from one base station to another. Grouped authentication requests prevent the base station from receiving a flood of messages that result in network congestion. A key agreement-based exchange session between the machines and the network provides secure transmission and data confidentiality. False identities of devices are created for each device in each authentication and re-authentication event, ensuring device anonymity. The protocol resists attacks such as man-in-the-middle, redirection, impersonation, and replay attacks. The protocol is simulated using BAN logic, and SPAN and AVISPA demonstrate the scheme’s resistance to malicious attacks. An analysis of the protocol compared to other models showed less bandwidth consumption during authentication as the number of devices increased. The protocol authenticates multiple devices in batch, whereas other models authenticate devices one by one.

Recent research focused on blockchain and cryptographic methods that, though secure, incur higher communication costs during multiple exchanges between dedicated authentication servers and devices for key agreement. Consensus algorithms include Proof of Work, which requires high computing power to mine blocks. The proposed HO-Auth scheme differs from other models since it relies on CSI data, which are easily collected from devices. CSI is researched extensively for secure authentication but creates a unique and static device fingerprint for each device. CSI fingerprinting using signal propagation is unreliable in areas where there are concrete walls in buildings or other environments with thick structural layouts. Nonetheless, CSI-based patterns are unique for each device primarily when based on a user’s specific movement around the base station. An attacker cannot imitate the movement patterns of a user unless they are standing right next to each other. Each device’s user profile is recorded and compared with another device imitating and sharing the same Device ID and MAC address.

The HO-Auth scheme addresses the security vulnerability in 5G-supported critical cloud computing-based sensitive and critical smart applications such as Healthcare where any malicious behavior may affect human well-being. The attack scenario begins when a user moves to a different base station and an attacker attempts to impersonate the user. The base station registers the attacker as the legitimate user and denies access to the honest user, preventing the latter from joining the network. The attacker transmits malicious data to the system and affects data confidentiality when communicating as an honest user with other devices.

We assume a smart building environment where there are different femtocells and users move from one access point to another. Access points act as base stations and provide service to a group of devices. We use CSI to build user profiles and avoid the cryptographic-based key agreement methods used in various recent research due to the overhead costs in both infrastructure and key management. CSI is available freely from Wi-Fi-based access points, ensuring an accessible collection of data for a lightweight, secure handover authentication solution. User profiles are shared across the decentralized base stations to prevent impersonation attacks throughout the system. A full profile (F_prof) illustrates the user’s movement pattern from the current base station to the second base station where authentication is required. Higher accuracy for a complete user profile is essential to prevent an attacker from gaining unwanted access.

The key area of consideration for the proposed scheme’s analysis is accuracy during two stages: the initial profile building and when a full user profile is built. The initial profile demonstrates the scheme’s ability to detect an impersonator during the initial phase of building the user profile. An attacker attempts to authenticate with the base station by impersonating an honest user. A full profile further decreases an attacker’s attempt to authenticate with the base station successfully. There is a need to produce a similar SS-based profile, and the count of SS is used to conduct a full profile.
3. Proposed Approach

3.1 Technological Aspects

The proposed HO-Auth scheme presents a new method for device authorization for existing decentralized telecom networks. We assume that a private blockchain network service provider manages each base station using a unique ID. This paper focuses on protecting the network from stealing users’ data and transmitting corrupt data to the pre-existing blockchain-based network. As shown in Fig. 1, HO-Auth implements a deep learning RNN-based LSTM algorithm to monitor all devices within different base stations part of the network. A user profile is generated by relying on the user movement pattern. Not depending on an accurate CSI-based fingerprint but focusing on the movement pattern allows the scheme to be unaffected by environmental factors such as thick walls, which hinder true CSI readings. Each device sends its SS data to the User Profile Builder. The process flow of the scheme is shown in Fig. 2. The pattern-based fingerprinting of all machines allows accurate detection of the positioning of the UE.

![Proposed HO-Auth scheme diagram](image-url)
The CSI of all UEs is monitored, which includes the SS indicators of base stations. The SS indicates a UE’s proximity with another base station and with the current base station. The weaker the SS is, the inefficient the network performance in terms of bandwidth. The stronger the signal, the closer the device is to the base station, offering more reliable network bandwidth service. Connected machines within a microcell such as picocell and femtocell generate SS recorded in dB units. Handover request is received when a UE moves closer to another base station, and there is a fading effect with the currently connected base station.

To illustrate a handover scenario, we take the example of a valid user operating in a femtocell base first base station in an office environment. The user proceeds to leave the office building and moves outdoors. A request to connect to the macrocell base station is received based on the diminishing SS of the femtocell base station and the more reliable SS of the macrocell base station. To authenticate the device, CSI is analyzed, including both the signal strength from the sender base station (femtocell) and receiver base station (macrocell). Authentication is approved as no duplicate signals are attempting to disguise themselves as the genuine UE.

An intruder attempts to spoof the base station by authenticating with the base station, receiving the user’s confidential data, and returning malicious packets affecting the network performance, such as Denial of Service (DoS) attacks. Our attack model assumes that the intruder is equipped with a portable wireless receiver with omni-directional antennas. An intruder easily spoofs the device’s IP address and alters the MAC address to impersonate the honest UE. Therefore, the two parameters, IP and MAC addresses, are unreliable in detecting spoofing attacks. Using CSI, the attacker’s portable device and the valid user emit their SS to the central base station. It is unlikely that the SS’s match unless both UE and the attacker’s device are in proximity. Suppose the intruder manages to be in proximity to the user. In such case, the scheme follows a two-step process using the RNN algorithm to identify and deny authentication requests from malicious devices.

In the first step of our authentication scheme, we collect the device’s CSI data and build the initial user profile. The profile is retrained as the user is not stationary when moving to authenticate toward...
another base station. The final user profile built is a collection of movement patterns of the user based on the SS. Fig. 2 shows the process flow of the proposed HO-Auth scheme, and Algorithm 1 presents the HO-Auth scheme’s detailed detection method. A user profile ensures that an accurate profile is built even if the wireless network’s security is compromised. The user profile uses the SS of each machine, which is an element of CSI dependent on the device’s location and is unique and separate for each device. An intruder needs to be near the legitimate device continuously to spoof the network and move in exactly the same pattern as the honest user. Since our proposed scheme is for portable IoT devices, we form a user profile based on the equipment’s moving pattern from one location to another. A base station records the CSI data of the device and submits data for building the user profile. The RNN algorithm learns the historical pattern of the user profile using the received data. Accurate profile building from the data collected from the valid device is possible by recording the CSI from different location points. Various access points or base stations are different picocells or femtocells in the environment near the user. These act as sensors, and they are tuned to the same channel. The UE, which is close to the access point, allows the base station to record and report the user’s CSI for accurate device profile building. The temporal correlation of a device at different points of a room or outside a building varies due to spatial diversity; note, however, that they are not as different from each other as an intruder present at another location recording different CSI data. Once the RNN algorithm learns a user profile, any recorded change in temporal data results in a new profile built. The temporal correlation of the user profile of a user at Point A is less diverse at Point B than an intruder moving from Point C to Point D.

When moving between different base stations, repeated user profile generation results in slower authentication and poor network performance. Critical cloud-based smart healthcare applications require seamless data transmission flow to assist a user during a medical emergency. Our scheme works under the assumption that the decentralized private blockchain network maintains the user profile once generated by the User Profile Builder. Our example scenario, wherein a user is present in a smart building, moves from one base station to another requesting authentication. Wireless Internet service providers use a common service provider with multiple different base stations or access points. With a common service provider operating using blockchain technology, the decentralized base station records the first user profile generated. All adjacent base stations now have access to the user profile. A user with IoT healthcare devices moving within a building is not required to rebuild a new user profile; thus, authentication is performed without delay. Upon leaving the building, the User Profile Builder will construct a new user profile and share it with its adjacent base stations, thereby preventing future network delays.

3.2 Methodological Flow of the HO-Auth Scheme

As shown in Algorithm 1, an initial profile \( I_{prof} \) of the user is first built, which stores the first SS collected. We assume the possibility that an attacker may try to impersonate the device before the final device profile is created. When an attacker (UE2) attempts to authenticate with the base station where the user is part of, the network checks to verify the authenticity of UE2. Firstly, it compares the Device ID, which we assume in our scheme is unique to each device and MAC address to determine if UE2 is a unique device or attempting to impersonate. If both Device ID and MAC address match with UE1, the profile-based comparison initializes based on two conditions, comparison of \( I_{prof} \) of both UE1 and UE2 and the authentication attempts made by both devices. The base station collects the SS of UE2 and compares with \( I_{prof} \) of UE1. It is highly improbable for an attacker to share the same \( I_{prof} \) as an honest user. Since this is a comparison using \( I_{prof} \) which contains a single SS captured from both devices, it is possible an attacker is aware of the SS of UE1 and spoofs the information to the base station.

In the second step of the I_prof authentication phase, we analyze the number of Authentication Requests \( A_{req} \) received from both spoofing and valid devices. The RNN algorithm differentiates the
Deep Learning Enabled Secure IoT Handover Authentication for Blockchain Networks

A legitimate device from the intruder using a secondary parameter, i.e., the number of $A_{req}$ packets received from UE1 and UE2. A DoS attack is identified when the intruder sends multiple authentication requests to obstruct the base station’s performance. To ensure quick handover authentication and authorization, however, RNN initially detects and differentiates between the intruder and the UE based on the received distances between the two devices using the differences of SS in $I_{prof}$ of both UE1 and UE2. If abnormal behavior is detected in the form of multiple authentication requests, UE2 is refused authentication, and its sent packets are dropped. The 5G guarantees communication for all its connected devices, but an attacker impersonating another user is denied authorized access to the base station. The attacker’s device resumes service on the previously connected base station. The second authentication parameter ensures that, when multiple devices attempt to authenticate the same time and share a similar user profile, the count of authentication requests received from both machines identifies which device is spoofing the network.

**Algorithm 1. Profile-based authentication**

1: **Input**: device signal strength (ss), Authentication requests ($A_{req}$)
2: **Output**: Initial profile ($I_{prof}$), Full profile ($F_{prof}$).
3. UE1 (ss) {capture signal strength} → $I_{prof}$
4. Receive Authentication request from UE2
   - Compare Device ID and MAC address of both devices (UE1, UE2)
   - Record $A_{req}$ of UE1 and UE2
   if { UE1 (Device ID, MAC address) != UE2 (Device- ID, MAC address)
       Compare UE1 $I_{prof}$ (ss) with UE2 (ss) & UE1 ($A_{req}$) with UE2 ($A_{req}$)
       if { UE1 $I_{prof}$ (ss) != UE2 (ss) & UE1 ($A_{req}$) < UE2 ($A_{req}$)
           #drop UE2 packet and deny access
       } else register UE2 and capture ss to build ($I_{prof}$,$F_{prof}$)
   }
5. UE1 (ss₁, ss₂, ss₃...ssₙ) → $F_{prof}$
6. Receive authentication request from UE3
   - Compare Device ID and MAC address of both devices (UE1, UE3)
   if
     { UE1 (Device ID, MAC address) != UE3 (Device- ID, MAC address)
       Compare UE1 $I_{prof}$ (ss) with UE3 (ss)
       if { UE1 $I_{prof}$ (ss) != UE3 (ss) & UE1 (ss₁, ss₂, ss₃...ssₙ) !=
         UE2 (ss₁, ss₂, ss₃...ssₙ)
           #drop UE2 packet and deny access
       } else register UE2 and capture ss to build ($I_{prof}$,$F_{prof}$)
   }
7: **END**

The HO-Ath scheme implements the RNN-based deep learning algorithm supported by the fog computing layer’s resource to learn and build each device’s user profile in the network. Under normal conditions, a user’s device profile is created and authorized to join the base station. Nonetheless, the intruder and the legitimate user may both be present during the initial profile building. The CSI data collected from both devices result in an inaccurate training of the RNN algorithm’s profile. A combination of the collected data allows an intruder to authenticate its equipment ahead of the legitimate machine. Our proposed scheme assumes that the legitimate device is the first device to request authentication and handover from one base station to another. The intruder activates and
attempts to mirror the honest user’s communication by sending authentication requests using a shared Device ID. Due to network delay problems commonly found in wireless networks, the first request sent by UE1 may not be successful. The device may not receive the return packets due to interference in the network. The intruder takes advantage of this scenario by pretending to be an honest user and sends a second authentication request using the same Device ID. The increase in distance from the threshold shows that the second request does not match with the first request. Distance is measured in dB, where a large increase in distance between two users using CSI shows that the two users are not the same, and there is a strong profile mismatch. Our proposed HO-Auth scheme discards the second authentication request during the initial profile building by dropping all received packets. The valid user’s second attempt to authenticate may contain different CSI data, which is a mismatch itself from the previously built profile. Implementing a threshold value enables the HO-Auth scheme to measure an acceptable difference in distance of the valid user’s location position.

As user UE1 moves in the environment connected to the base station, a series of SS (ss1, ss2, ss3 ..., ssn) are collected to build \( F_{prof} \). As shown in Algorithm 1, a legitimate device (UE1) and an attacking device (UE3) are finally compared using the full profile \( (F_{prof}) \) of both users. Initially, both Device ID and MAC addresses are compared; if they are found to be the same, \( F_{prof} \) is analyzed. A collection of SS’s captured from UE1 forms the \( F_{prof} \) created as the device moves in the environment. Attacker UE3 is required to have the same number of SS’s as in UE1’s \( F_{prof} \). An incomplete \( F_{prof} \) submitted by UE3’s previous base station is denied authorization to join the new cell. If UE3 attempts to inject a custom-made \( F_{prof} \) for its device, it is difficult to assume the count of SS in UE1’s \( F_{prof} \). The number of SS’s in any device is random and difficult for an attacker to detect. In the event the SS counts match in the \( F_{prof} \) of both UE1 and UE2, the HO-Auth scheme compares both profiles and determines the UE3 as an illegitimate device, so it is refused authentication to join the base station. All future attempts by UE3 are denied, and request packets are dropped.

Different devices have unique spatial characteristics such as location, so their CSI data is different. A single device can only be at a single physical location. If two devices claim to be the same device during authentication, their physical location-based SS identifies which device is an intruder. The RNN algorithm analyzes the separate device profiles and compares them with the same historical movement pattern as the previously learned device profile. Under an attack scenario wherein the wireless network itself is compromised and the attacker has control of the CSI data of the legitimate users, authentication of multiple malicious devices will be attempted. Multiple authentication requests are sent to authorize devices on other base stations. Using various devices, the attacker launches DoS attacks to disable the base station and affect network security and performance. The RNN algorithm analyzes the received authentication requests and compares them with the legitimate device. The request packets of the intruder device are dropped, and its user profile data are discarded. Valid devices are authenticated, and their profile data is used to retrain the algorithm further. User profiles created for each device are shared with other base stations via the network. Each base station has access to the network to request user profiles when an unknown device requests connection. If a new device connects, a profile is created, continuously updated, and shared with the network.

4. Analysis of HO-Auth Scheme

Our experimental setup tested our proposed scheme in two environments: the lab and two different university corridor floors. We assume in our design that a pre-existing blockchain-based set of base stations share the \( F_{prof} \) with each other, we assumed that, in the simulation setup, the lab and the corridor on the same floor each have access points that are not adjacent. The lab emulates a work environment, and the user’s movement across the corridor behaves as the point when the user attempts to switch from one base station to another. The activity recorded on the corridor a floor above is an
intruder’s attempt to impersonate a valid user. We used the Nexmon Channel State Extractor (Nexmon) tool to extract CSI data from two Google Nexus 5 devices. One device belongs to an honest user, and the other belongs to the intruder. We selected the 20 MHz bandwidth channel, with two Netgear AC1200 Routers serving as Access Points (AP) to record CSI data. One AP is placed in the lab, and the second in the corridor. The user traverses the lab and toward the corridor to connect with the second AP. We used these two APs as two base stations in our simulation. Using smartphones allows proper tracking and detection of mobile users moving from one point to a different position. A total of 522 packets were sent from both devices, representing the attempts at authentication by a valid user and an intruder with the base station.

The proposed HO-Auth scheme uses the LSTM-based RNN algorithm to identify attackers using the CSI data obtained based on SS. The RNN algorithm suffers from the vanishing gradient problem; therefore, in place of RNN, we used a modified RNN called LSTM algorithm. The advantage of LSTM over unmodified RNN lies in its capability to manage long-term temporal dependencies and the existence of cell state. Each cell consists of a memory cell in each RNN unit, which preserves the previous sequential input data’s data along with unit values. Using three gates—the input, forget, and output gate—the LSTM model captures long-term dependencies by filtering information through a sigmoid activation in each gate [15]. The LSTM model is used in the scheme to build a device profile using the captured CSI data, which has strong dependency on the device’s physical location. The device profile is initially built on the user’s fixed location and rebuilt as the user moves from the lab to the corridor. The movement patterns are recorded, with the profile stored along with its associated device ID, and a sequential correlation with CSI data is analyzed between the established user profile and a new device sharing a similar device ID. Device authentication is denied when the intruder device exhibits less association with the user profile and sends multiple authentication requests compared to the honest device. The CSI data captured in the lab and the corridor include 10 training points and ten testing points. Data captured from each location point via the access points in both the lab and the hallway are used to build a user profile.

We analyzed the scheme’s performance during the initial profile buildup of a user from a fixed position using the collected CSI data. We took the average distance threshold to authenticate the user of 17dB. The device was moved to different positions in the lab and the corridor to measure the authentication accuracy. As shown in Fig. 3(a), the proposed scheme’s user profile’s initial building achieved a 0.91 accuracy rate for an average distance threshold of 17dB in detecting spoofing attackers. As the distance increased, the scheme maintained a detection rate between 0.90 and 0.91. In Fig. 3(b),

![Fig. 3. (a) Initial profile build accuracy and (b) authentication requests by device.](image)
we observed that both device clusters sent repeat authentication requests. The intruder's device sent a burst of 426 packets to get authorized as a legitimate user and join the network. We also observed that, as both valid user and intruder came closer together, the number of authentication requests further differentiated the valid user from the intruder and allowed our scheme to reduce false alarms further. A burst of authentication requests also demonstrated an intruder's attempt to cause a DoS at the base station. The LSTM algorithm accurately differentiated the valid user from the intruder even though the two devices came closer. Both machines demonstrated an increase in device authentication requests, with the intruder sending a significantly higher number of requests than the legitimate device.

In Fig. 4, we saw that the Ho-Auth scheme’s accuracy increased as we introduced two access points to capture SS from the UE. A single AP achieved the highest accuracy of 0.95 at the 6th position after recording the UE from the previous five different positions. The dual AP built the $F_{prof}$ more quickly after three positional points and provided the highest accuracy at 0.95 to detect intruders at the 4th position. This is because a single AP requires recording a higher number of SS from a different whatto build a user profile. In our scheme, we require a minimum of five varying positions to create $F_{prof}$ because the UE may not necessarily remain in the AP’s signal range as users are mobile and Wi-Fi-based indoor APs have a lower frequency range compared to picocell-based base stations.

5. Conclusion

Fast and reliable handover authentication is required for efficient cloud computing-based smart healthcare applications supported by IoT devices. Spoofing attacks cause loss of confidential user data and transmission of malicious data to smart applications, preventing healthcare applications from providing optimum services. This study proposed a fast, reliable handover scheme using a deep learning-based LSTM algorithm. The scheme does not build a unique static fingerprint using CSI, recording instead the user’s movement pattern to design a user profile. Profiles of authenticated users are created using CSI obtained from devices. User profile-based fingerprinting allows the identification of attackers spoofing honest users. A distance-based threshold shows a lack of temporal correlation between the intruder and the legitimate device. An increase in authentication requests increases the accuracy of detecting intruders and lowers the possibility of false positives. Upon successfully identifying authorized users, a user device profile is trained again for increased user authorization accuracy in the future. An analysis of the proposed scheme yielded an accuracy rate of 0.91 in the initial profile build and 0.95 after retraining the user profile using dual access points. The Ho-Auth scheme is built for decentralized blockchain-based base stations, allowing the sharing of a generated
Final User Profile and preventing multiple handovers and authentication delay.

**Author’s Contributions**

Conceptualization, MMS. Funding acquisition, JHP, VL. Investigation and methodology, MMS. Project administration, JHP, VS. Resources, VL, JHP. Supervision, JHP. Writing of the original draft, MMS. Writing of the review and editing, MMS. Software, VS, VL. Validation, MMS, VL, VS, JHP. Formaly Analysis, MMS, JHP. Data Curation, MMS. Visualization, MMS. All the authors have proofread the final version.

**Funding**

This study was supported by the Advanced Research Project funded by SeoulTech (Seoul National University of Science and Technology).

**Competing Interests**

The authors declare that they have no competing interests.

**References**


[12] G. Chopra, S. Jain, and P. K. Jha, “Possible security attack modeling in ultradense networks using high-


