IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 February 2023, accepted 23 February 2023, date of publication 27 February 2023, date of current version 3 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3249969

RESEARCH ARTICLE

Blockchain-Based Lightweight Multifactor Authentication for Cell-Free in Ultra-Dense 6G-Based (6-CMAS) Cellular Network

ADNAN SHAHID KHAN[1], (Senior Member, IEEE), MOHD IZZAT BIN YAHYA[1], KARTINAH BT ZEN[1], JOHARI BIN ABDULLAH[1], ROZEHA BINTI A. RASHID[2], (Member, IEEE), YASIR JAVED[3], (Member, IEEE), NAYEEM AHMAD KHAN[4], AND AHMED M. MOSTAFA[5,6]

[1]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia
[2]Communication Engineering Department, Faculty of Engineering, School of Electrical Engineering, Universiti Teknologi Malaysia, Johor Bahru 81310, Malaysia
[3]Department of Computer Science, Prince Sultan University, Riyadh 11586, Saudi Arabia
[4]Faculty of Computer Science and Information Technology, AlBaha University, AlBahah 65511, Saudi Arabia
[5]Computer and Systems Engineering Department, Faculty of Engineering, Helwan University, Cairo 11795, Egypt
[6]Information Technology Department, Faculty of Computer Science and Information Technology, AlBaha University, AlBahah 65511, Saudi Arabia

Corresponding author: Ahmed M. Mostafa (ahmed_youssef01@h-eng.helwan.edu.eg)

This work was supported in part by the Ministry of Higher Education (MOHE), Malaysia, Universiti Teknologi Malaysia (UTM) Collaborative Research, under Grant Q.J130000.2451.08G07; and in part by the Universiti Malaysia Sarawak (UNIMAS) under Grant GL/F08/CRGUTM/01/2019.

ABSTRACT Cell-Free mMIMO is a part of technology that will be integrated with future 6G ultra-dense cellular networks to ensure unlimited wireless connectivity and ubiquitous latency-sensitive services. Cell-Free gained researchers' interest as it offers ubiquitous communication with large bandwidth, high throughput, high data transmission, and greater signal gain. Cell-Free eliminates the idea of cell boundary in cellular communication that reduces frequent handover and inter-cell interference issues. However, the effectiveness of the current authentication protocol could become a serious issue due to the dynamic nature of Cell-Free in densely distributed, high number of users, high mobility, and frequent data exchange. Secondly, secure communication may be achieved in such a dynamic environment at the expense of high authentication overhead, high communication and computational costs. To address the above security challenges, we proposed a lightweight multifactor mutual authentication protocol for Cell-Free communication using ECC-based Deffie Hellman (ECDH). This scheme utilizes timestamping, one-way hash function, Blind-Fold Challenge scheme with public key infrastructure. The proposed cryptosystem integrates with blockchain technology using proof of staked (POS) as a consensus mechanism to ensure integrity, non-repudiation and traceability. The proposed scheme can enforce the mitigation of several major security attacks on communication links such as spoofing attacks, eavesdropping, user location privacy issues, replay attacks, denial of service attacks, and man-in-the-middle (MITM) attacks, which is one of the significant features of the scheme. Furthermore, this scheme contributes to reducing authentication, communication, and computational overheads with an average of 32.8%, 52.4% and 53.2% better performance respectively as compared baseline authentication protocols.

INDEX TERMS 6G, cell-free, authentication, lightweight multifactor, ECDH, MITM attack.

I. INTRODUCTION

Despite the implementation of 5G that still undergoing in this era, the attention and initial blueprint of the transition from 5G to 6G has become a voluminous discussion among researchers. The extensive network communication traffic in this era is a major factor for 6G technology to assist the demands and will be centered around users, mobile device, network operators and service providers [1] as a key enabler in 6G ecosystem.

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Masini.

6G performance requirements are at peak data rate of 1000Gbps with less than 100 microseconds air latency which is 50 times better data rate and one-tenth latency of 5G. Thus, to handle and support massive traffic growth in mobile network, 6G were expected to provide 1000 times higher throughput and sub-milliseconds service latency [2]. According to Cisco Visual Networking Index in 2021, there will be more than 11.6 billion Internet-of-Things Devices (IoDs) will be deployed in 6G-enabled IoT networks, which caused the IoT network to become more robust. Thus, with 6G, there will be higher transmission frequency, a large date rate, low latency, and high reliability for various novel applications such as AI-assisted and vehicular network intelligence communications [3]. 6G also has been anticipated as a remarkable revolution in aiding unlimited wireless connectivity and ubiquitous latency-sensitive services, such as augmented and virtual reality also healthcare and housing intelligent systems [4].

6G will be driven by many types of technology such as Artificial intelligence (AI), Terahertz communication, optical wireless technology, blockchain, UAV, big data analytic and Cell-free massive Multiple Input-Multiple Output (mMIMO) communication under its associated service requirement which is Ubiquitous mobile ultra-broadband (uMUB), Ultra-high-speed with low-latency communications (uHSLLC), Massive machine-type communication (mMTC) and Ultra-high data density (uHDD) [5]. Although with the innumerable applications, services, and reliability in 6G-enabled network technology, the security issues still cannot be overlooked [6]. Moreover, 6G provides massive network parameters especially in delivering high AI-empowered network capabilities which can be a big contributor to security and privacy issues such as malicious behavior, authentication issues, access control, encryption, and communication issues [6]. There is prior discussion and research on 6G with regard to security issues, specifically proposing multifactor authentication for 6G or utilizing blockchain technologies to assist in mitigating several communication attacks. We have conducted an extensive systematic literature review on security issues with regard to 6G addressing security mechanisms for cell-free environments [7], [8]. Besides our works, other researchers also contribute to addressing security concerns in 6G networks [9], [10], [11]. Hence, this research will focus on security issues on cell-free architecture for the ultra-dense environment, more specifically it will be dealing with mitigating communication attacks using multifactor authentication scheme assisted with blockchain technology. This research work is the extension of our previous works, where we proposed lightweight multifactor authentication scheme for cellular networks specifically 5G, and trust-based blockchain architecture for VANET, where we mitigate major communication attacks using blockchain technology [12], [13]. In this research work, we enhance our previous security schemes to address security issues in cell free 6G environment by integrating blockchain with lightweight multifactor authentication scheme [14]. Since cell-free mMIMO is one of 6G futuristic technology, where there will be no logical cellular boundaries, moreover one user equipment can be facilitated by two different access point at the same time. The detailed discussion on cell-free mMIMO is presented at the end of this section. In addition, for simplicity, we will use the term ''cell-free'' instead of cell-free mMIMO throughout this article.

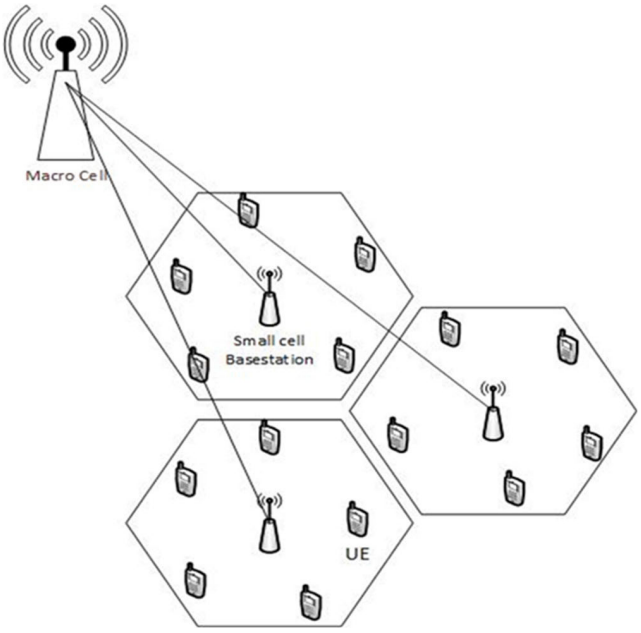

FIGURE 1. Small cell architecture.

Basic architecture for cell based cellular network is shown in Figure 1. A conventional cellular 5G small-cell communication architecture consists of non-cooperative base stations that can serve up to 100 users per cell with a smaller area and reduced power in signal transmission. The main difference of small cell with cell-free is that, instead of serving in user-centric manner such cell-free, small cell use a network-centric approach where each UE only served by one nearby AP with the largest RSSI value [15], [16].

Small cell provides higher communication capacity to the user. Moreover, it enables high data rates with greater bandwidth [17]. In addition, due to shorter distance between user with the AP, the rate of transmission power and path loss become lesser [18], [19]. However, there is a few challenges in deploying small cell system. Due to large number of users served by the AP, frequent handover [20] tends to occur when user moving from one cell boundary to another. This is also due to the coverage radius of a single cell is very small [21]. Hence, this problem leads to inter-cell interference [22], malicious behavior [23] and security issues which is pollution attack during packet encoding [24]. These issues by the end, brings the system to the packet integrity issues, data privacy [25] and possible data losses [26].

In cell-free network, user equipment (UE) is located within the coverage (i.e., area of influence) of distributed access

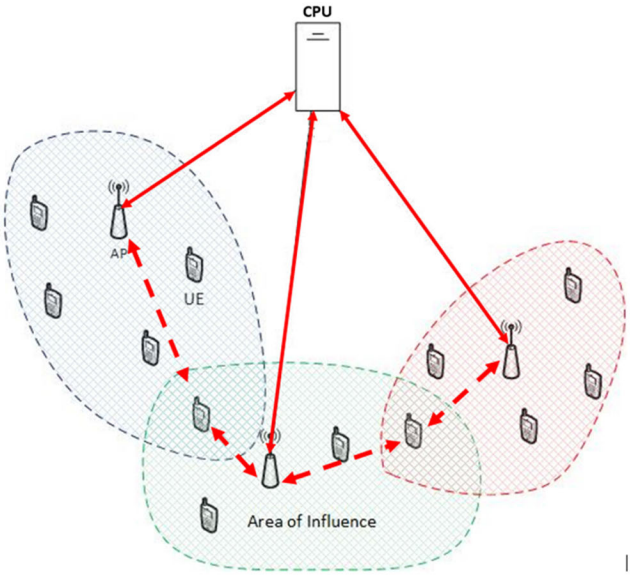

FIGURE 2. Basic cell-free mMIMO architecture.

point (AP) consist of multiple antennas. UE can be served by several APs at the same time to form a joint cluster which ''act'' as a communication cell in user-centric style, removes the idea of ''cells boundary'' in the network [17], [27]. The APs cooperate phase-coherently via backhaul network and serves all users at the same time-frequency resource [15]. There is a central processing unit (CPU) that connected with AP via backhaul network act as a coordination and computational assistance entity for APs as shown in Figure 2 [28].

Cell-free networks tends to improve 95% of user throughput compared to small cell communication [29]. Furthermore, it improves user coverage and mobility with minimal handover. Moreover, Cell-Free provides a larger bandwidth, increases throughput and higher data transmission rates [30], [31], [32], [33], [34]. However, we can see some drawback in this technology from technical point of view and in term of its security issues. The high-performance gain comes with greater challenges on maintaining the signal gain and active communication, which is not address well in current research. Due to the dense distributed network topology [35], Cell free mMIMO (Cell-Free mMIMO) is prone to security threats such as spoofing attack [36], [37], eavesdropping [38], user location privacy issues [39], man-in-the-middle (MITM) attack, and other common attack in wireless communication protocol where we are focusing on this research [40], [41]. This paper will contribute as follows.

1) Utilization of a lightweight cryptographic multi-factor authentication scheme that helps secure Cell-Free communication in an open insecure channel.
2) Utilization of ECC-based Diffie-Hellman secret sharing key agreement scheme for achieving confidentiality, integrity, and non-repudiation.
3) Mitigation towards several major security attacks.
4) Utilization of Blockchain to ensure the end-to-end security of the proposed scheme.
5) Reducing authentication, communication and computational overheads.

TABLE 1. Significance of proposed work.

A. Category	B. Achievements
Security	*Mitigation towards Replay attack, DoS attack, MITM attack, Rouge Relay Station & Impersonation attack*
Privacy	*Ensure CIA (Confidentiality, Integrity and Availability)*
Computational	*Provide better scheme with ample processing capabilities and operational cost*
Traffic	*Reduce authentication overhead*

The significance of this work also provided as follows.

II. MOTIVATION

As a part of emerging technology in 6G era, the security capability of Cell-Free communication is of concern especially to the end user. For researchers, the complexity of the communication is one of the major concerns and we are interested to evaluate how our proposed solution can be secure towards security attacks such spoofing attack, eavesdropping, user location privacy issues, replay attack, denial of service attack, man-in-the-middle (MITM) attack and other known attacks. Several researchers have been developing a security algorithm to cope with the objectives of lightweight, trusted, and secure algorithm. However, those proposed security algorithm might be not compatible for Cell-Free environment. This is due to the densely distributed nature, high mobility, frequent data exchanged and high number of UEs and APs that makes the Cell-Free environment ultra-dense. Cell-Free promises a high-speed data-rate, increase in throughput and greater signal gain beyond the conventional cellular communication capability; hence, a well-balanced lightweight and secure communication environment is needed.

The remainder of this paper is organized as follows. In Section III, related work is presented. Section IV illustrates our proposed system design, section V discussed blockchain management and integration of 6-CMAS, section VI demonstrates mathematical analysis, and Section VII presents a security analysis of our proposed scheme from different perspectives followed by section VI, which is the conclusion.

III. RELATED WORKS

Multifactor authentication mechanism to ensure confidentiality, integrity, and availability is not a new term. Several

researchers proposed multifactor authentication mechanisms for different networks. However, discussion on integrating multifactor authentication with blockchain specifically on 6G ultra-dense networks is limited. Our research domain for this article is more on multifactor authentication, blockchain, and 6G ultra-dense networks, so we use the Scopus index library to locate technically sound articles, which must have a clear proposed cryptographic mechanism with concrete analysis. Since, blockchain-based multifactor authentication is scarce, to build up with our theoretical framework, we utilize any other similar networks, like the Internet of Things, wireless access networks, medical or industrial internet of things, etc. In our related works, we discussed their methodology in terms of proposed solutions, and later we discussed their strength and weaknesses. We analyze the weaknesses found in existing research works to come up with our main problem statement.

Wazid et al. proposed a new remote user authentication key management scheme [42]. The authors discuss about a newly discovered potential MITM attacks in THz 6G Network. Hence, it is very important to highlight the security and privacy issues in ''6G-enabeled NIB for industrial applications'' that might be vulnerable to various types of attack such as replay attack, MITM attack impersonation attack, sensitive information leakage and smart industrial device stolen attack. In this scheme, a genuine user able to authenticate a smart industrial device and have access to a real-time data by using an established session key. The mutual authentication and key agreement are established among the user and smart industrial devices via content server. This scheme mentioned the importance to enhance security mechanism that can overcome various attacks such as replay attack, MITM attack, illegal session key computation and other common attack. It is proven that this scheme significantly reduces computational cost. However, in the evaluation part, the authors did not test the authentication cost. In the scenario of embedded or micro smart industrial device, the scheme seems complex and impractical. This is because, those tiny devices might not have ample computation capability to compute the proposed algorithm.

A Lightweight Group Authentication scheme was proposed by [43]. The authors stated that in conventional authentication methods, the client and server usually have a shared key before starting the communication process. A random value, which is selected and sent by the server to the client, is encrypted by the client with the key, and the encrypted value is sent back to the server. Finally, the server vali-dates the client by decrypting the response. During the process, there is one claimer and one prover. The prover can only authenticate one user at a time. Hence, this approach is not scalable for densely deployed IoT networks, where millions of nodes are expected to be operational [44]. This scheme proposed to overcome a problem in group authentication. This can be used in centralized or decentralized group authentication environment. The scheme offers group authentication for massive machine-type communication (mMTC) where each group can recover the same group key for further communication. In term of security issues, this scheme will prevent the intruder to perform MITM, impersonation and replay attack. However, this scheme does not support in high mobility mMTC environment where fast handoff and lightweight authentication are needed. Furthermore, the implementation of this authentication scheme may have issues in ultra-agile radio access architecture due to dynamic cell structure.

In [45], the author proposed a secure endogenous wireless access network architecture based on blockchain. The authors stated that the existing identity authentication technologies all adopt centralized method, and fast identity authentication cannot be achieved in a massive connection scenario. Current heterogeneous networks use different identity authentication technologies, and it is difficult to ensure continuous connectivity when terminals frequently handover between heterogeneous networks. Hence, this scheme combining blockchain and mobile edge computing to research the authentication mechanism in 6G WSN. A unified identity authentication framework is proposed that consist of terminal, blockchain and certificate management. The certificate management will issue and create certificate transactions. Blockchain network is used to store the certificate transactions and information while terminal can store certificate related information after applying certificate anonymously [46]. This scheme proven to have less time consumption and lower communication overhead. However, a public key-based certificate system is not suitable in an IoT-based network environment due to devices' limited resources. There are many computational and communication overheads in issuing, revoking, signing, and verifying certificates. The author also did not consider the threat issues where this scheme is prone to impersonation attack. The attacker will impersonate the legitimate nodes and extracted the value of certificate issuance transaction (the certificate uses for authentication between nodes in blockchain).

RESEAP, an ECC-Based Authentication and Key Agreement scheme were proposed by Vinoth et al. in [47] for IoT applications. This is a revised protocol where the author uses a Physically Unclonable Function (PUF) to provide IoT environment from various of security flaws. The authors stated the interconnected system of data flow in IoT raises many challenges. To be precise, the devices that are connected through IoT, can capture, and transfer many sensitive data that may easily com-promise privacy. Hence, there should be a mechanism to control the access to the captured and transferred data by any devices in an IoT system. The proposed scheme heuristically proves the security of the proposed protocol against different attacks and security analysis shows that it provides desired semantic security in the model. This scheme also proven to be secure against different attacks such as password guessing, traceability, impersonation, insider attack and desynchronization.

In [48], the author proposed a secure multifactor authenticated key agreement scheme for Industrial IoT (IIoT). This scheme proposed to support users' remote access to a sensing

device in IIoT. The collected data by IoT devices is usually transmitted via an open channel, where it is vulnerable to the attacks launched by the adversary. An unauthorized user may illegally access the sensing devices to obtain the real-time data which brings challenges to security and privacy in IIoT or even destroy the industrial production. Therefore, it necessitates establishing a secure authenticated key agreement protocol to overcome security and privacy problems in IIoT. The structure of this scheme shows an adaptation of secret-sharing technology to help construct a multifactor authentication for IIoT sensing device where the au-thors use hash function, XOR operation and symmetric cryptography, which is suit for resource constrained sensing device [49]. This scheme is proven to be immune against chosen-plaintext attack, Denial-of-Services (DoS), offline guessing attack, MITM at-tack and other various attacks. The experimental result also shows that the scheme effectively reduces communication and computational cost compared with previous schemes during the process of the authenticated key agreement. However, some flaws can be identified in this scheme such as; multiple credential computation is complex and time consuming considering IIoT devices are naturally limited with computation and communication capability [50]. From the evaluation also shows that the author does not consider the requirement of data availability.

In [51], the author proposed a secure decentralized spatial crowdsourcing scheme for 6G-enabled network in box. The author mentioned that it is hard to maintain system security which only relay on trust Spatial Crowdsourcing (SC) server. In 6G-NIB, workers need to submit their locations to the SC-server and without the SC server, attackers may get locations to obtain some sensitive information such as an individual health record. Furthermore, without the SC-server, spatial tasks and answers are shared in public, which discloses sensitive information in spatial tasks and answers. Hence, this scheme provides a decentralized platform for the control station and sensing nodes. This design allows sensing nodes to verify their own location. This scheme also protects the security of spatial tasks and answers. Control station shares location strategy parameters to negotiate a session key with a sensing node, and the sensing node apply the CCM authenticated encryption mechanism and the session key to encrypt the answer, which guarantees the security of the answer.

A lightweight mutual authentication and key agreement scheme proposed by [52]. In medical IoT, the patient medical data is highly confidential and supposed to be private. However, due to the openness and mobility of the wireless network, it is easy to be stolen or forged by an adversary, this will lead to extremely serious consequences and may even endanger the lives of patients. Hence, a lightweight and anonymous mutual authentication is proposed for WBAN. It only needs to perform hash function and XOR operation where forward secrecy can be guaranteed without using asymmetric encryption.

The analysis of this scheme indicates that this pro-posed solution reduces computational cost compared to the schemes that uses asymmetric encryption. However, form the algorithm we can see that the data ex-change between SN and AP is not secure. Moreover, the AP is not verified hence leads to rogue relay attack and possible MITM attack [53], [54].

In [55], the author proposed a two-factor authentication for IoT. An IoT devices need to have something like a biometric factor such as fingerprint which are unique for each device. Many IoT devices are installed in the area that easily accessible to adversaries [57]. Therefore, an adversary can easily capture these devices and subject them to physical and side-channel attacks. This may lead to stolen secret keys from the device's memory and launching a spoofing attack. In such attacks, the attacker impersonates as one of the legitimate IoT nodes and may gain access to crucial network resources from a remote location. Hence, it is crucial to keep an IoT device secure form location disclosure attack [57]. The proposed scheme provides a physical unclonable function (PUF) based scheme to assign a hardware fingerprint (bio-metric) to IoT devices. Based on security analysis, this scheme can protect IoT communication from spoofing attack and DoS attack.

There are other significant contributions published by Author [58], who proposes a blockchain-based authenticated group key agreement protocol by introducing a new entity called the device manager, which acts as an intermediary to ensure secure communication in IoT devices, and author [59] who proposes a secure and effective blockchain-enabled privacy-preserving authentication scheme by utilizing an elliptic curve cryptosystem to construct a pairing-free ring signature scheme, which greatly reduces the resources over-head and ensures unconditional anonymity and data batch integrity verification with simplified key management issues

In the above discussions, we found that most of the proposed mechanisms are complex with high computational, communication costs, and authentication over-head in a multihop ultra-dense environment. Besides that, most algorithms are prone to key security issues like password guessing attacks and privacy issues in terms of identity theft. Secondly, most of the schemes only address a few attacks like replay attacks, denial of service attacks, or man-in-the-middle attacks. However, to have an end-to-end security mechanism, it is mandatory to address the security issues of communication attacks, starting from spoofing, impersonation, password guessing, replay attack, denial of service attacks, and man-in-the-middle attacks. Thus, to address the above security concerns, there is a need for such a mechanism that must address those communication attacks with less computational, communication, and authentication overhead.

IV. PROPOSED SYSTEM DESIGN

A. CELL-FREE NETWORK MODEL

Figure 3 shows 6-CMAS cell free network model. The model is an upgraded version of Figure 2 of section I. A detailed discussion about the basic architecture of cell-free mMIMO

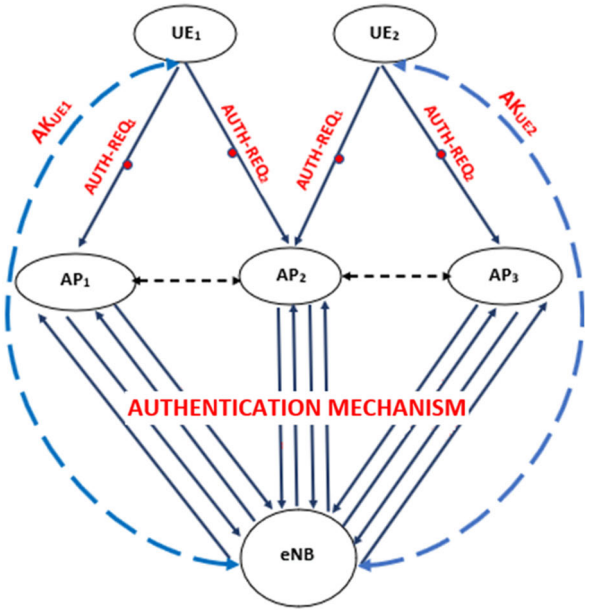

FIGURE 3. 6-CMAS cell-free network model.

Algorithm 1.1 – Authentication Request Message UE-AP

Step 1: Get participant's IDs through neighbour discovery
Step 2: Get Public key of
$AP=K_{AP}$; $eNB=K_{eNB}$; $UE= K_{UE}$
Step 3: Get Private key of $UE=K^{UE}$
Step 4: Generate challenge using Blind fold challenge scheme for
$Ch_{UE\text{-}AP}$
Step 5: Solve the challenge for
$Ch_{UE\text{-}AP} = Ch_{UE\text{-}AP}'$
Step 6: Generate timestamps T_{SUE}
Step 7: Compute
$RSSi_{AP_1}, PID_{UE}, PID_{AP}, Ch_{UE\text{-}AP}, Ts_{UE} = M$
Hash of timestamps = $H(Ts_{UE})$
Step 8: Encrypt (UE-AP) //Encryption for AP
$[H(Ts_{UE})]^{KUE}$
$[M, H(Ts_{UE})]^{KUE}]_{KAP}$
Step 9: AUTH-REQ: *[Encrypt (UE-AP)]*
Step 10: Send AUTH-REQ to AP

FIGURE 4. Authentication request message.

architecture can be found in section I under the figure description. Hence, this model consists of several components which is user equipment (UE), access point (AP) and evolved node base station (eNB).

UE is located within the coverage of distributed AP consist of multiple antennas. UE can be served by several APs at the same time to form a joint cluster which ''act'' as a communication cell. The AP act as a relay device to eNB where it forwards and responds a message from both UE and eNB. eNB is a Base Station with strong coverage and ability to provide authentication and authorizations to devices in its area. Finally, the CPU is a server connected via backhaul network act as coordination and computational assistance to eNB. According to Figure 3, UE1 is connected to AP1 and AP2 while UE2 is connected to AP2 and AP3. Both UEs send their authentication request message to their respective nearby APs. Once respective APs received the authentication request from UEs, they initiate authentication procedures, not only for UE, but also for themselves from nearby eNB. Therefore, once eNB authenticates respective APs, APs with the assistance of eNB authenticate their respective UEs. The details of the authentication procedures is discussed in next subsection.

B. DEVELOPMENT OF 6-CMAS PROTOCOL

In the development of this protocol, user equipment (UE1 & UE2) is connected to eNB through access points (AP1, AP2 & AP3). Since in cell-free environment, one UE can be served by nearby more than one AP, thus for initial authentication process, UE must send first authentication message to nearby both APs. At this point, AP cannot authenticate UE on behalf of eNB, as during registration all the critical credentials are securely saved at eNB server. Once AP received authentication request message, it will generate its own authentication message to get authentication from eNB. Later, AP together with UEs authentication messages with its own authentication messages sent to eNB. eNB received both messages, verify the critical credentials and send the challenges only to corresponding APs, once participating APs are authenticated, eNB will generate the sequences of challenges to APs, so that APs can authenticate UEs on behalf of eNB. In depth, multifactor mutual authentication is elaborated in the shape of pseudo codes in Algorithm 1.1 to 1.8.

Figure 4 shows algorithm 1.1 i.e., Authentication Request message from UE to AP. Since, our proposed mechanism utilize public key infrastructure, it required public keys, which must be available online publicly. However, these public keys later assist the eNB to transform the identity of the devices into pseudo identity. Only eNB and authorize APs have the information of such transformation mechanism. At this point, UE also get its private key through PKI procedure (from certificate authority (CA)). During the message preparation phase, after receiving public and private keys, one-time password must be created as challenge using blindfold challenge scheme [12], [53]. Then timestamps are generated, and hash is computed for timestamps. Since entire message is encrypted using PKI, so secrecy is now not the issue, instead of hashing the entire message, we propose to hash only timestamp to reduce computational cost. To ensure the non-repudiation, only hashed value of timestamps is encrypted with the private key of UE. The whole message is then encrypted using the public key of AP. Later, the message is sent to AP to get authentication and services from eNB. The message is sent to AP with pseudo-ID, timestamp, challenge, and hash of the timestamp. The hash value is encrypted with private key of UE. Finally, the whole message encrypted using public key of AP.

Algorithm 1.2 – Authentication Request Message AP-eNB

Step 1: Get participant's IDs through neighbour discovery
Step 2: Get Public key of
$AP=K_{AP}$; $eNB=K_{eNB}$; $UE= K_{UE}$
Step 3: Get Private key of $AP=K^{AP}$
Step 4: Generate challenge using Blind fold challenge scheme for
$Ch_{AP\text{-}eNB}$
Step 5: Solve the challenge for
$Ch_{AP\text{-}eNB} = Ch_{AP\text{-}eNB}$ '
Step 6: Generate timestamps Ts_{AP}
Step 7: Compute
$RSSi_{AP_1}$,PID_{UE},PID_{AP}, PID_{eNB}, $Ch_{AP\text{-}eNB}$, Ts_{AP} = M
Hash of timestamps = $H(Ts_{AP})$
Step 8: Encrypt (AP-eNB) //Encryption for eNB
$[H\ (Ts_{AP})]^{KAP}$
$[M, [H\ (Ts_{AP})]^{KAP}]_{KeNB}$
Step 9: AUTH-REQ: [Encrypt (AP-eNB)]
Step 10: Send AUTH-REQ to eNB

FIGURE 5. Authentication request message.

In Figure 5, the request message received at AP is decrypted by AP using its public key. It also decrypts the hashed value of timestamps using the public key of UE. Later, AP matches the message received from UE with hash of message, if both are equal then the message is valid and fresh otherwise discards the message. The AP is now invoked, and it sends the authentication request message to eNB. AP utilized the same procedure as mentioned above for algorithm 1.1.

In Figure 6, eNB receives encrypted request message from AP. It decrypts this message using its private key. It also decrypts hashed value of timestamp using public key of AP, and then matches the actual timestamp with hash of the timestamp. If the match is equal then it considers the message as valid and fresh, otherwise the message will be discarded. As the message is sent from AP, eNB responds AP with new challenge to validate either AP is a legitimate device. eNB encrypts the message including pseudo-ID, challenge, timestamp and challenge solution with its private key and public key of AP and sends to AP. To develop the encrypted message, eNB used the same procedures of encryption as discussed in algorithm 1.1.

In Figure 7, AP receives response message from eNB to address the challenge given. AP first decrypts the message with private key, solves the challenge, decrypt the hashed value of timestamp using the public key of eNB, check the timestamp, and matches it with hashed value of timestamp. If timestamp is fresh, it considers the message is a valid and fresh message and there is no replay attack. AP generate the message using the same encryption procedures discussed in algorithm 1.1. AP sends the challenge response to eNB with

Algorithm 1.3 – Authentication Challenge Response Message at eNB

DECRYPTION:
Step 1: Get Public key of
$AP=K_{AP}$;$eNB=K_{eNB;}$ $UE= K_{UE}$
Step 2: Get Private key of $eNB =K^{eNB}$
Step 3: Get AUTH-REQ (AP- eNB):
[Encrypt (AP- eNB)] = $[M, [H\ (Ts_{AP})]^{KAP}]_{KeNB}$
Step 4: Compute using private key of $eNB\ (K_{eNB})$
$M, [H(Ts_{AP})]^{KAP}$
Step 5: Compute using public key of AP (P_{AP})
$M, H\ (Ts_{AP})$
Step 6: Compute $H(Ts_{AP})$ & Compare with Ts_{AP}
Proceed if Condition Satisfied (both same values) else discard message
Encryption
Step 7: Generate challenge using Blind fold challenge scheme for
$Ch_{eNB\text{-}AP}$
Step 8: Solve the Challenge for
$CH_{eNB\text{-}AP} = CH_{eNB\text{-}AP}'$
Step 9: Generate timestamps Ts_{eNB}
Step 10: Compute
PID_{eNB}, PID_{AP}, $Ch_{eNB\text{-}AP}$, $Ch'_{AP\text{-}eNB}$, $Ts_{eNB} = M$
Hash value of $Ts_{eNB}= H\ (Ts_{eNB})$
Step 11: Encrypt (eNB-AP)
$[H\ (Ts_{eNB})]^{KeNB}$
$[M, [H\ (Ts_{eNB})]^{KeNB}]_{KAP}$
Step 12: AUTH-CHALLENGE-REQ: [Encrypt (eNB-AP)]
Step 13: Send AUTH-CHALLENGE-REQ to AP

FIGURE 6. Authentication challenge-response message.

hash value of timestamp encrypted with its private key. Later, AP encrypt the whole message with the public key of eNB.

In Figure 8, the response message from AP is received at eNB. eNB decrypts whole message using its private key. Later eNB decrypts the timestamp message using public key of AP. Then eNB address the challenge solution and compare the hashed timestamp with the actual timestamp. If both messages are equal, then proceeds otherwise discards the message. After decryption, eNB generates authorization key to complete the mutual authentication with AP. The authorization key and timestamp are hashed and signed by its private key and send it to AP.

In Figure 9, AP decrypts message received from eNB using its private key, decrypt the hashed value and AK using public key of eNB, and utilize the authorization key and checks timestamp. Then compares the hash values, if messages are same, it considered the message is valid and there is no replay attack. Now AP is mutually authenticated with eNB, it proceeds with its authentication process with UE by addressing challenge given and responds with new challenge for UE to

Algorithm 1.4 – Authentication Challenge Response Message at AP

DECRYPTION:
Step 1: Get AUTH-CHALLENGE-REQ
[Encrypt (eNB-AP)] = $[M, [H(Ts_{eNB})]^{KeNB}]_{KAP}$
Step 2: Compute using private key of AP (K_{AP})
$M, [H(Ts_{eNB})]^{KeNB}$
Step 3: Compute using public key of eNB
$M, H(Ts_{eNB})$
Step 4: Compute $H(Ts_{eNB})$ & Compare with Ts_{eNB}
Proceed if Condition Satisfied (both same values) else discard message
Encryption
Step 5: Generate challenge using Blind fold challenge scheme for
$Ch_{AP\text{-}eNB}$
Step 6: Solve the Challenge for
$Ch_{AP\text{-}eNB} = Ch'_{AP\text{-}eNB}$
Step 7: Generate timestamps Ts_{AP}
Step 8: Compute
$PID_{AP}, PID_{eNB}, Ch'_{AP\text{-}eNB}, T_{S_{AP}} = X$
Hash value of $Ts_{AP} = H(Ts_{AP})$
Step 9: Encrypt (AP-eNB)
$[H(Ts_{AP})]^{KAP}$
$[M, [H(Ts_{AP})]^{KAP}]_{KeNB}$
Step 10: AUTH-CHALLENGE-RESP: [Encrypt (AP-eNB)]
Step 11: Send AUTH-CHALLENGE-RESP to eNB

FIGURE 7. Authentication challenge-response message.

Algorithm 1.5 – Authentication Response Message at eNB

Decryption:
Step 1: Get AUTH-CHALLENGE-RESP
[Encrypt (AP-eNB)] = $[M, [H(Ts_{AP})]^{KAP}]_{KeNB}$
Step 2: Compute using private key of eNB (K_{eNB})
$M, [H(Ts_{AP})]^{KAP}$
Step 3: Compute using public key of AP
$M, H(Ts_{AP})$
Step 4: Compute $H(Ts_{AP})$ & Compare with Ts_{AP}
Proceed if Condition Satisfied (both same values) else discard message
Encryption:
Step 5: Generate Authorization Key for AP
AK_{AP}
Step 6: Generate timestamps Ts_{eNB}
Step 7: Compute
$PID_{eNB}, PID_{AP}, AK_{AP}, T_{SeNB} = M$
Hash value of AK_{AP} and $Ts_{eNB} = H(AK_{AP}, Ts_{eNB})$
Step 8: Encrypt (eNB-AP)
$[H(AK_{AP}, Ts_{eNB})]^{KeNB}$
$[M, H(AK_{AP}, Ts_{eNB})]^{KeNB}]_{KAP}$
Step 9: AUTH-RES: [Encrypt (eNB-AP)]
Step 10: Send AUTH-RES (eNB- AP) to AP

FIGURE 8. Authentication response message.

address. To generate the encrypted message, AP utilized the same procedure as discussed in algorithm 1.1.

Algorithm 1.6 – Authentication Challenge Response Message at AP

DECRYPTION:
Step 1: Get Public key of
$AP = K_{AP}; eNB = K_{eNB}; UE = K_{UE}$
Step 2: Get Private key of $AP = K_{AP}$
Step 3: Get AUTH-RES (eNB-AP):
[Encrypt (eNB-AP)] = $[M, H(AK_{AP}, Ts_{eNB})]^{KeNB}]_{KAP}$
Step 4: Compute using private key of AP
$M, [H(AK_{AP}, Ts_{eNB})]^{KeNB}$
Step 5: Compute using public key of eNB
$M, H(AK_{AP}, Ts_{eNB})$
Step 6: Compute $H(AK_{AP}, Ts_{AP})$ & Compare with AK_{AP} and Ts_{AP}
Proceed if Condition Satisfied (both same values) else discard message

Encryption
Step 7: Generate challenge using Blind fold challenge scheme for
$Ch_{AP\text{-}UE}$
Step 8: Solve the Challenge for
$Ch_{AP\text{-}UE} = Ch_{AP\text{-}UE}'$
Step 9: Generate timestamps Ts_{AP}
Step 10: Compute
$PID_{AP}, PID_{UE}, Ch_{AP\text{-}UE}, Ch'_{UE\text{-}AP}, Ts_{AP} = M$
Hash value of $Ts_{AP} = H(Ts_{AP})$
Encryption for UE:
Step 11: Encrypt (AP-UE)
$[H(Ts_{AP})]^{KAP}$
$[M, [H(Ts_{AP})]^{KAP}]_{KUE}$
Step 12: AUTH-CHALLENGE-RES: [Encrypt (AP-UE)]
Step 13: Send AUTH-CHALLENGE-RES to UE

FIGURE 9. Authentication challenge-response message.

In Figure 10, UE decrypts message received from AP using its private key, solves challenge and checks timestamp. Then compares this with hash of timestamp that is encrypted with private key of AP. UE decrypts the message using public key of AP. Then compares both messages, if messages are same, it considers message is valid and there is no replay attack. Then UE send respond message with the challenge solution given by AP to allow AP to generate authorization key for UE be able to receive services from both AP and eNB.

In Figure 11, the response message from UE is received at AP. AP decrypts whole message using its private key. Later AP decrypts the timestamp message using public key of UE. Then AP address the challenge solution and compare the hashed timestamp with the actual timestamp. If both messages are equal, then proceeds otherwise discards the message. After decryption AP generate authorization key to complete the mutual authentication with UE. The authorization key and timestamp are hashed and signed by its private

Algorithm 1.7 – Authentication Challenge Response Message at UE

DECRYPTION:
Step 1: Get AUTH-CHALLENGE-RES
Encrypt (AP-UE) = $[M, [H (Ts_{AP})]^{KAP}]_{KUE}$
Step 2: Compute using private key of UE
$M, [H (Ts_{AP})]^{KAP}$
Step 3: Compute using public key of AP
$M, H (Ts_{AP})$
Step 4: Compute $H(Ts_{AP})$ & Compare with Ts_{AP}
Proceed if Condition Satisfied (both same values) else discard message
Encryption
Step 5: Generate challenge using Blind fold challenge scheme for
$Ch_{UE\text{-}AP}$
Step 6: Solve the Challenge for
$Ch_{UE\text{-}AP} = Ch'_{UE\text{-}AP}$
Step 7: Generate timestamps Ts_{UE}
Step 9: Compute
$PID_{UE}, PID_{AP}, Ch'_{AP\text{-}UE}, T_{S_{UE}} = M$
Hash value of $Ts_{UE} = H(Ts_{UE})$
Step 10: Encrypt (UE-AP)
$[H (Ts_{UE})]^{KUE}$
$[M, [H (Ts_{UE})]^{KUE}]_{KAP}$
Step 11: AUTH-CHALLENGE-RES: [Encrypt (UE-AP)]
Step 12: Send AUTH-CHALLENGE-RES to AP

FIGURE 10. Authentication challenge-response message.

Algorithm 1.8 – Authentication Response Message at AP

Decryption:
Step 1: Get AUTH-CHALLENGE-RES
[Encrypt (AP-UE)] = $[M, [H (Ts_{UE})]^{KUE}]_{KAP}$
Step 2: Compute using private key of AP
$M, [H (Ts_{UE})]^{KUE}$
Step 3: Compute using public key of UE
$M, H (Ts_{UE})$
Step 4: Compute $H(Ts_{UE})$ & Compare with Ts_{UE}
Proceed if Condition Satisfied (both same values) else discard message
Encryption:
Step 5: Generate Authorization Key for UE
AK_{UE}
Step 7: Generate timestamps Ts_{AP}
Step 10: Compute
$AK_{UE}, Ts_{AP} = M$
Hash value of AK_{UE} and $Ts_{AP} = H (AK_{UE}, Ts_{AP})$
Step 11: Encrypt (AP-UE)
$[H (AK_{UE}, Ts_{AP})]^{KAP}$
$[M, H (AK_{UE}, Ts_{AP})]^{KAP}]_{KUE}$
Step 12: AUTH-RES: [Encrypt (AP-UE)]
Step 13: Send AUTH-RES (AP-UE) to UE

FIGURE 11. Authentication response message.

key and send it to UE. The detail algorithm is illustrated in Figure 12.

V. BLOCKCHAIN MANAGEMENT AND INTEGRATION WITH 6CMAS

Blockchain is a technology that comprised of an unlimited sequential chain of blocks. Blockchain has been defined as distributed digital ledgers that keep records and transaction as encrypted timestamp chains. It able to operate independently without intervention from other entities to ensure the credibility of transaction [51].

A. BLOCKCHAIN CHALLENGES AND ATTACKS

Blockchain technology provides a secure means of storing data. Trust in transactions is ensured as a result of cryptography, decentralization, and consensus regulations. A distributed ledger technology (DLT) typically consists of blocks that contain transactions. It is almost impossible to manipulate the blocks because they are linked in a series. All transactions within a block are confirmed and approved through consensus methods, which ensure their validity and accuracy. A distributed ledger technology (DLT) facilitates the simultaneous access, confirmation, and updating of records across multiple entities or locations on a network in a stable manner. Blockchain technology permits decentralization by establishing a distributed network of associates or members. Transaction records cannot be modified by one user and there is no single point of failure. In order for cryptocurrencies to function, blockchain technology is their fundamental technology. Businesses have increasingly used blockchain technology to create blockchain-based applications ranging from distributed databases to digital transactions to healthcare. Despite this, there are some important differences between blockchain technologies in terms of security.

According to Halborn, many popular cryptocurrency wallets were vulnerable to a critical vulnerability in MetaMask in June 2022. In spite of some in the blockchain space believing it was unhackable until recently, many attacks have demonstrated that blockchain technology cannot be hacked. Security breaches are becoming more common in smart contract platforms and blockchain applications. During 2016, $72 million worth of Bitcoin was stolen from Bitfinex, one of the largest crypto exchanges. If there is an analysis done for all these attacks, it was insider attacker who was able to share the keys with attacker or the access was given to non-validated user by insider. The attacks that can do successful on blockchain by an attacker are phishing attack, routing attack, Sybil attack and 51% attack [52] as shown in Figure 13. A phishing attack involves hacking into a user's credentials in order to obtain their credentials. Wallet key holders receive emails that appear to come from a legitimate source from a hacker. The emails are designed to trick the user into providing their private key or password for their account. Routing attacks are attacks on the blockchain network infrastructure. A blockchain can only function if extensive data

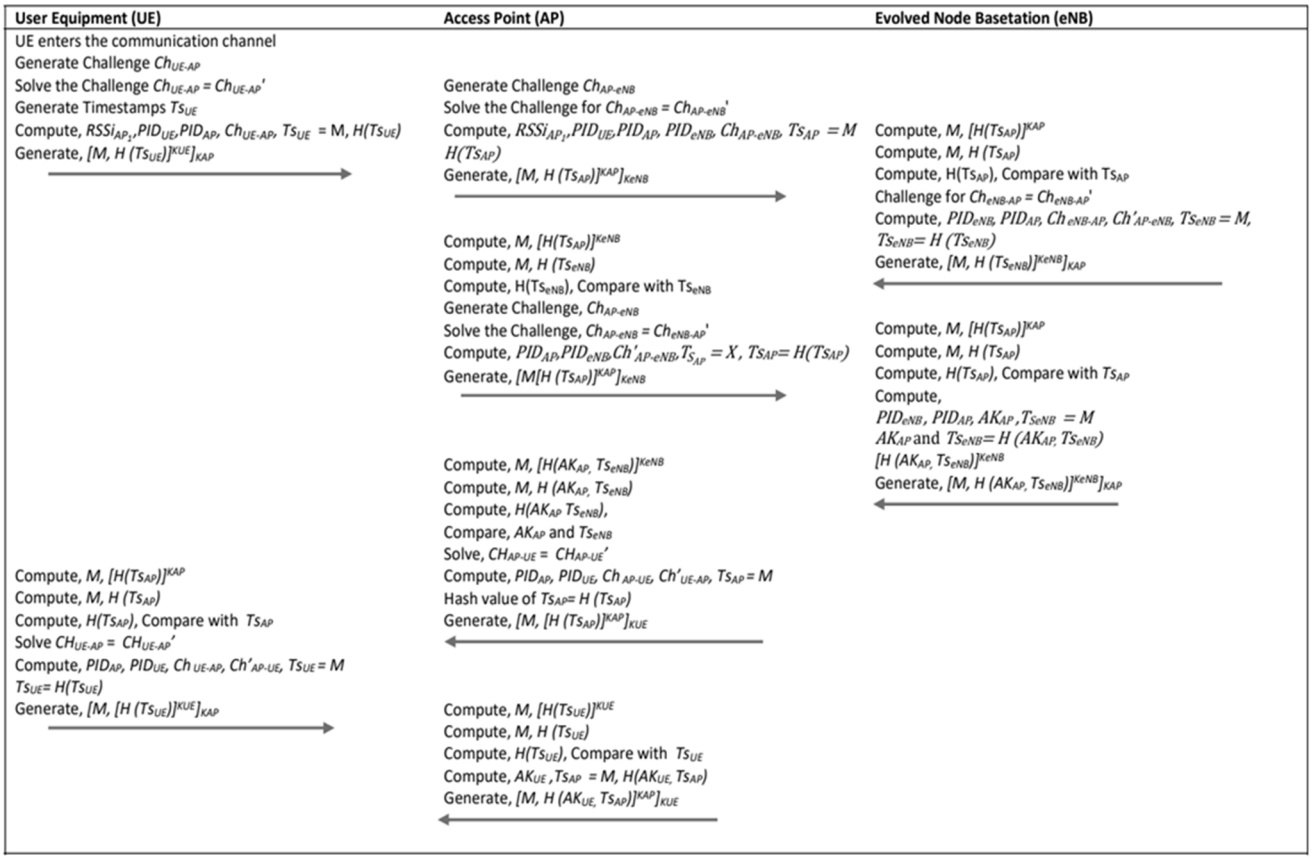

FIGURE 12. 6-CMAS scheme timing diagram.

transfers are conducted in real time. If an attacker is able to isolate segments of a network, the network can be divided into multiple segments. The aim of a Sybil attack is to gain outsized influence over a network by creating a large number of false accounts. The use of this method is not allowed for the purposes of breaking block-chain consensus, but other attacks can still be conducted using it. The goal of a 51% attack is to gain control over the system. It is possible for a miner or a group of miners to mobilize sufficient resources to gain more than 50% of the mining capacity of a blockchain network. Having more than 50% of the capability indicates that you have power over the ledger and are able to exploit it.

In our scheme, the trustworthiness (in terms of integrity and traceability) of message passing between participant in Cell-Free communication achieved by placing the credential in a public blockchain to support traceability service architecture. This means we propose to integrate our proposed scheme in blockchain architecture as shown in Figure 14.

B. BLOCKCHAIN DESIGN FOR 6-CMAS

In our proposed blockchain integration structure, we consider the whole message with header and the payload. Blocks from blockchain reside inside the payload or under sub header [14]. Each block contains the critical credentials from the authentication messages. Blocks are sequentially connected to form a blockchain. Refer to blocks at UE_1, numberings at first

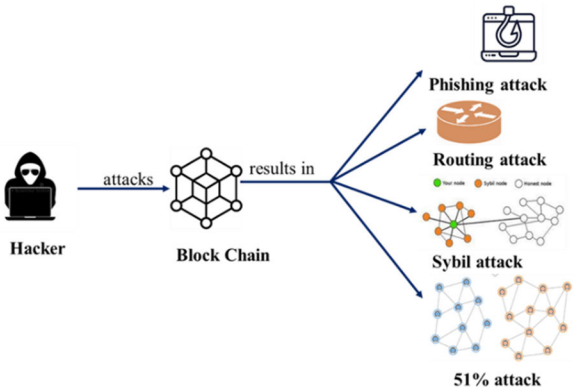

FIGURE 13. Possible attacks on blockchain by hacker.

rows denotes that the blocks belong to that particular message (to know the message number refer to figure 12). Since these messages are generated at UE_1, so hashed it follow the hashed sequences at UE_1. Same goes to blocks at AP_1, where have four different messages 2, 4, 6 and 8. These messages are generated at AP_1, so follow their own sequences. The same goes to AP_2 and eNB. Each device are responsible of managing their own sequences. Table 1 discussed the block generated and received by different devices their authentication procedure. During the blockchain management and integration with 6-CMAS, it is mandatory to have all the

TABLE 2. Resources held by participating devices in (%).

Devices	Block Generated/Received								Percentages
UE	$[1]^G$					$[6]^R[7]^V$		$[8]^R$	24%
AP	$[1]^R[2]^V$		$[3]^R[4]^V$		$[5]^R[6]^V$		$[7]^R[G]^V$		50%
eNB	$[1]^R[2]^V$	$[3]^G$		$[4]^R[5]^V$					36%

blocks synchronize within all the participating devices. For instance, If at UE_1, the blocks are generated and updated, the blocks must be updated at each shared points, which we called consensus management. The detailed discussion on consensus management can be seen in our next subsection, where we also proved that at any points none of the participating devices contains more than or equal to 50% of the blocks to avoid 51% attack.

C. CONSENSUS MANAGEMENT

Due to the decentralized nature of blockchain, the resources on its network are prone to some security attacks. In addition, our proposed scheme may include multiple participation of devices that may increase the chances of malicious device. Consensus mechanism is designed to manage a series of rules and procedures to be follow among participating devices in the communication so that they can agree on a particular state of the blockchain e.g., if there is a new block is added in a blockchain, who will add it in the blockchain will be defined by achieving consensus.

There is different consensus algorithm available such as Proof of Work (POW) and Proof of Stake (POS). In POW, all participants or nodes needs to spend some computing power to perform calculation before adding a new data/block in a blockchain. This will proof which node has more and better computing power and finally can decide who can enter the new block in the blockchain. On the other hands, POS reduces the computation and resource consumption, which relies on the ''stakes'' that will be put in before entering applying into the blockchain. This allows the participants to proof that it is not malicious and trustworthy. Hence, to decide who can enter the new block is by defining the one who have the highest stake. The resources on the blockchain network are often breached by utilizing certain techniques. For a successful attack, the attacker must control more than 50% of the whole network resources, which is termed a 51% attack. In order to deal with such attacks, it is mandatory to reduce the number of authentication credentials retained by any participating devices.

The block generated by the blockchain solely depends on a consensus mechanism to retain its consistency. Amongst popular consensus mechanisms, this article chooses proof of staked (POS) as the consensus mechanism of the traceability of the blockchain to analyze the possibility of minimizing 51% attack. The main concern here is to reduce computational operations, hold fewer resources (less than 51%), and verification of blocks. Compared with the proof of work (POW) mechanism used in the past research, POS reduces the resource consumption by mathematical operations to a certain extent and improves the performance accordingly. These features are inherent in our 6-CMAS authentication protocol, which is a lightweight authentication mechanism and assists in lightweight verifications.

TABLE 3. Mitigation strategies that 6-CMAS is going to address.

Attack Name	How 6-CMAS is going to mitigate the attack?
Phishing attack	Phishing attacks in blockchain is only possible when the user can be lured into sharing the personal information but 6-CMAS is based on purely principle that doesn't require sharing of private key. Encryption is done using the public key of receiver and even introduce multifactor authentication, thus it will require physical as well as digital presence of attacker with receiver that is not possible. Thus, phishing attack is not possible.
Routing attack	Routing attack require the breaking of network into smaller segments. Let's say if the attackers divide the network into smaller network. 6-CMAS approach uses verification through base station as well as require sharing of credentials thus the attack will be detected if the verification cannot occur or is done through fake BS as fake BS cannot generate the actual private key of BS or CH.
Sybil attack	Sybil attack is not possible as 6-CMAS is based on cellular communication. It requires a creation of account using BS that require personal credentials as well as biometric registration in context of 6-CMAS. Thus, sybil attack is not possible in 6-CMAS.
51% attack	51% attacks require creation of more than 51% of block nodes that is not possible in private cellular networks. Thus 51% attack is not possible if 6-CMAS is used in ceullular networks.

The detailed discussion on how the POS consensus mechanism works is as follows. Figure 15 depicted the overall scenario of ultra-dense cell-free networks, where we have multiple access points (APs) communicating with user equipment (UEs). For better elaboration, let's consider UE_4, which is communicating with three access points (AP_1, AP_2 & AP_4). Usually, to have proper POS consensus mechanism implementation, there are a few conditions that must be fulfilled simultaneously. For instance, firstly, there must be one validator, which should be the block creator. Secondly, the validator must own coins or tokens to receive transaction fees or rewards. Lastly, POS requires multiple validators to agree

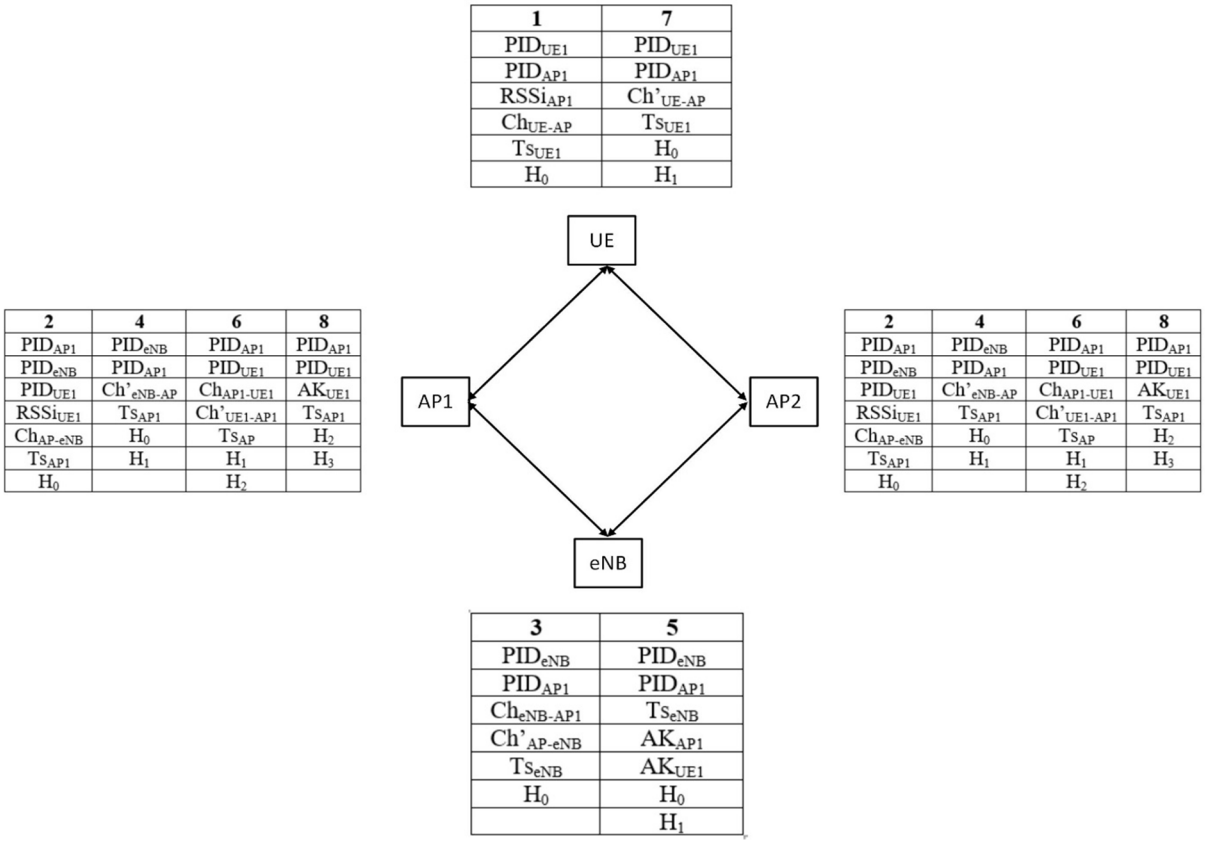

FIGURE 14. Proposed blockchain integration with 6-CMAS.

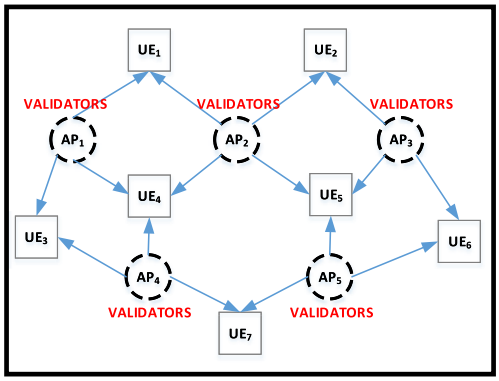

FIGURE 15. Ultra-dense cell-free scenario.

that transactions are authentic and accurate, if enough validators validate the transactions, it goes through successfully.

Based on these conditions, if we visualized ultra-dense cell-free network, UEs initially register themselves with nearby coordinating access points. Access points consequently maintain all the credentials for authenticating and validating those newly joined UEs. Multiple coordinating access points validate the transactions or authentication messages from each UE i.e. UE_4 validated by $AP_{1,2\&3}$. Thus, for ultra-dense cell-free networks, all these conditions are fulfilled. In this scenario, the participating access points are the validators, so will be given the rewards or must be paid. Usually, in such a scenario, the rewards or payments are based on policies to which all-commercial parties agreed before launching of the business.

Moreover, 6-CMAS doesn't allow all participating devices to hold more than 50% of the critical credentials, as shown in Table 2. The table illustrates that at UE, block 1 & 6 is generated while block 6 and 8 is received. Since generated blocks are not critical credentials on their own, so here the critical credentials are 6 and 8 which are received by other participating devices, thus UE is holding 24% of critical credentials. Since AP is considered a gateway between UE and eNB, it's holding 50% of total critical credentials. However, AP is prone to rouge relay station attacks, where any relay device can act as AP and can initiate authentication procedures and become part of the legitimate network. Our proposed 6-CMAS assist in mitigating such rogue relay station attack by reducing the chances of password guessing. Lastly, eNB holds 36% of total critical credentials.

D. COMPARISON OF SECURITY OF 6-CMAS WITH BLOCKCHAIN ATTACKS

As stated in Figure 13, there are still few possible attacks that occur on blockchain as it happened recently on recent blockchain exchanges. 6-CMAS is carefully designed to address the attacks that can occur on blockchain. It is already a limitation of blockchain related to 51% attack that is not

possible on current scheme when applied in cellular communication as cellular communication will form a private block chain but if its public blockchain the cost of creation of 51% will be extremely high but the attacks are still possible. Table 3 shows the attack names and how 6-CMAS handles the attacks.

VI. MATHEMATICAL ANALYSIS

In this section, mathematical analysis has been performed on 6-CMAS and other benchmark algorithms using Capkun Equation. For this purpose, we use our 6-CMAS cryptographic algorithm without the blockchain, as blockchain technology assist in security paradigms, for instance, integrity, traceability and trustworthiness (evaluation from trustworthiness perspectives will be our one of the future research works). Firstly, communication cost of proposed algorithm is calculated to evaluate whether proposed algorithm is lightweight as compared to other benchmark algorithms and it is found how much this scheme is improved over benchmarks algorithms in communication cost. Authentication overhead of the proposed algorithm is also computed to find the overhead of messages over the network.

A. COMMUNICATION COST

In our proposed algorithm, UE wants to communicate with AP and eNB. AP is Access Point which forwards authorization from eNB to UE. Several messages flow from UE to AP and eNB. To compute the total cost, this research considers all operations that contribute to secure communication. In the proposed algorithm 6-CMAS, there are five operations that are part of secure communication. The messages sent in 6-CMAS protocol consist of pseudo-ID, challenge, challenge solution, hash and timestamp that is denoted by SZ_{PID}, SZ_{Ch}, $SZ_{Ch'}$, SZ_H, and SZ_{Ts} respectively. Communication cost for each message is calculated as below. Initial message is sent from UE to AP that contains request from UE for communication with AP. The message sent includes pseudo-IDs, challenge, timestamp, and hash. Thus, the total size of message will be sum of pseudo-IDs, challenge, timestamp, and hash that is sum of $\{SZ_{PID}, SZ_{CH}, SZ_{TS}, SZ_{DH}\}$. Thus, the size of authentication message can be computed in Equation 1.

$$m_{C1} = \sum_{Au=1}^{k=1} \{Sz_{PID} + Sz_{Ch} + Sz_{TS} + Sz_H\} \quad (1)$$

Second message is sent from AP to eNB, after it invoked by the request message from UE. The communication cost for message 2 is shown in Equation 2.

$$m_{C2} = \sum_{Au=1}^{k=1} \{Sz_{PID} + Sz_{Ch} + Sz_{TS} + Sz_H\} \quad (2)$$

Third message is response message from eNB to AP to verify AP with new challenge. The communication cost for message 3 is shown in Equation 3.

$$m_{C3} = \sum_{Au=1}^{k=1} \{Sz_{PID} + Sz_{Ch} + Sz'_{Ch} + Sz_{TS} + Sz_H\} \quad (3)$$

Fourth message is sent from AP to eNB where AP addressed the challenge form eNB. The communication cost for message 4 is shown in Equation 4.

$$m_{C4} = \sum_{Au=1}^{k=1} \{Sz_{PID} + Sz_{Ch} + Sz'_{Ch} + Sz_{TS} + Sz_H\} \quad (4)$$

Message number five is a response message from eNB to AP where eNB sends authorization key AK for AP. The communication cost for message 5 is shown in Equation 5.

$$m_{C5} = \sum_{Au=1}^{k=1} \{Sz_{PID} + Sz_{AK} + Sz_{TS} + Sz_H\} \quad (5)$$

Message number six is response message from AP to UE where AP address challenge from UE. The communication cost for message number 6 is shown in Equation 6.

$$m_{C6} = \sum_{Au=1}^{k=1} \{Sz_{PID} + Sz_{Ch} + Sz'_{Ch} + Sz_{TS} + Sz_H\} \quad (6)$$

Message number seven is response message from CH to UE where UE address the challenge from AP. The communication cost for message number 7 is shown in Equation 7.

$$m_{C7} = \sum_{Au=1}^{k=1} \{Sz_{PID} + Sz_{Ch} + Sz'_{Ch} + Sz_{TS} + Sz_H\} \quad (7)$$

In message number eight, AP sends an authorization key AK to UE. The communication cost for message 8 is shown in Equation 8.

$$m_{C8} = \sum_{Au=1}^{k=1} \{Sz_{AK} + Sz_{TS} + Sz_H\} \quad (8)$$

After looking into above Equations 1 - 8 and for Message 1 to message 8, cumulative computation of communication cost has been calculated as follows.

$$AuthM_C = \alpha^* \sum_{Au=1}^{k=\beta} \left\{ \begin{matrix} Sz_{PID} + Sz_{Ch} + Sz'_{Ch} \\ + Sz_{TS} + Sz_H + Sz_{AK} \end{matrix} \right\} \quad (9)$$

Equation 9 shows message for one hop communication where α shows the number of individual messages and β represents the number of messages transmitted. As shown that 6-CMAS can handle multi hops communication as shown in Equation 10.

$$AuthM_C(h) = h\left(\alpha^* \sum_{Au=1}^{k=\beta} \left\{ \begin{matrix} Sz_{PID} + Sz_{Ch} + Sz'_{Ch} \\ + Sz_{TS} + Sz_H + Sz_{AK} \end{matrix} \right\}\right) \quad (10)$$

For more than one hops, the number of messages transmitted is multiple of number of hops. In multi-hop scenario, total

TABLE 4. Total communication cost.

Scheme	Number of Hops						
	2	3	4	5	6	7	8
Wazid	17664	26496	35328	44160	52992	61824	70656
Vinoth	23296	34944	46592	58240	69888	81536	93184
Xu	8192	16384	20480	24576	28672	32768	36,864
6-CMAS	8960	13440	17920	22400	26880	31360	35840

authentication cost is equal to number of hops multiplied by number of messages in single hop plus number of messages in forwarding request.

To calculate the total communication cost, we consider that all credentials is represented with value of 16-byte (128-bit length) to keep the symmetry of all benchmarks and our 6-CMAS scheme. Hence, by taking consideration of Equation 9 for single hop communication in 6-CMAS, the total communication cost for our scheme is 4480 bits. Also applied on total communication cost for Wazid's scheme, Vinoth's scheme and for Xu's scheme which are 8832, 11648, and 4096 bits respectively. Since Xu scheme utilizes symmetric cryptosystem, where every time the scheme needs to refresh the keys (scalability is one of the key concerns once we talk about symmetric key), this is the reason that there is not much different in total communication cost with Xu's schemes.

Correspondingly, the total communication cost of multi-hops scenario in respective scheme will be defined as $4480h$, $8832h$, $11648h$ and $4096h$ bits. Where h represents as number of hops. Overall, 6-CMAS performed better in communication cost compared to Wazid's, Vinoth's and Xu's scheme by 80.8%, 27.4% and 51.42% respectively. Table 4 and Figure 15 shows the total communication for multi-hops scenario.

B. COMPUTATIONAL COST

Another major contribution in this research is computational cost. In order to address the computational cost or we will consider several major operations such as hash function, bitwise XOR operation, encryption, decryption, generation, and validation process required to flourish the authentication environment. The total computation for each operation in proposed and benchmarks schemes will be counted and calculated. Table 5 shows the total computation for the operation mentioned above.

In our proposed 6-CMAS scheme, we adopt an asymmetric cryptography to complete the encryption and decryption process. By utilizing private key, K^n and public key, K_n of the participant in the network, we can ensure mitigation on MITM attack, impersonation attack and masquerading attack. Referring again to Figure 5 - 12, every hash value of

TABLE 5. Computational cost of all 6CMAS compared to its benchmark.

Scheme	Number of Computation						
	H()	XOR	Enc	Dec	Generation Process (Computes)	Validation Process (Check)	Total Computation
6-CMAS	10	None	8	8	72	6	104
Wazid	175	22	Use ECM		44	4	245
Vinoth	71	11	3	3	37	12	137
Xu	92	28	Froward Secrecy		44	12	176

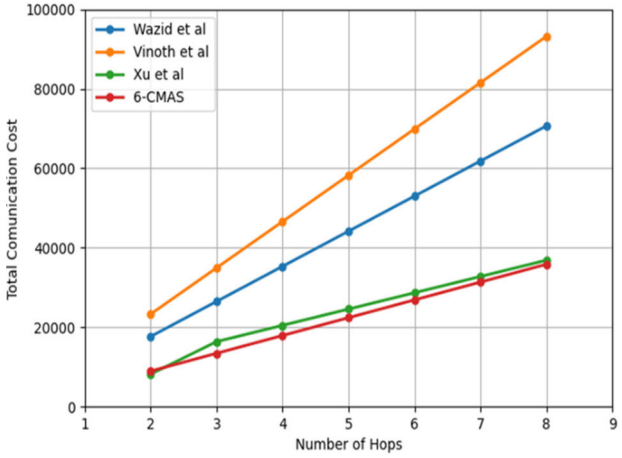

FIGURE 16. Total communication cost.

the timestamp in each message is encrypted (signed) by the private key of the sender. As the purpose of hashing is to keep the data from any modification, the encryption process also to ensure that the message is sent by the legitimate device or entity. Then, the whole message is also encrypted using public key of the receiver. The purpose of this process is to maintain the secrecy of the message, hence mitigating masquerading attack. Overall, our proposed scheme required 8 times computation of encryption process also 8 times of decryption process. Hence, 6-CMAS shows better performance compared to Wazid's, Vinoth's and Xu's scheme by 65.4%, 88.9% and 2.8% respectively as shown in figure 16.

C. AUTHENTICATION OVERHEAD

In authentication overhead we will evaluate the concerns of how many messages are created and sent before the actual communication transmission. The authentication overhead is required to ensure the actual part of authorization and communication is secure enough. While maintaining its security requirement, 6-CMAS is designed to have as minimum authentication overheads as possible with only eight messages created to achieve mutual authentication within the entities in single hop scenario.

TABLE 6. Total authentication overhead.

Scheme	Number of Messages/hops						
	2	3	4	5	6	7	8
6-CMAS	16	24	32	40	48	56	64
Wazid	24	36	48	60	72	84	96
Vinoth	22	33	44	55	66	77	88
Xu	12	24	36	48	60	72	84

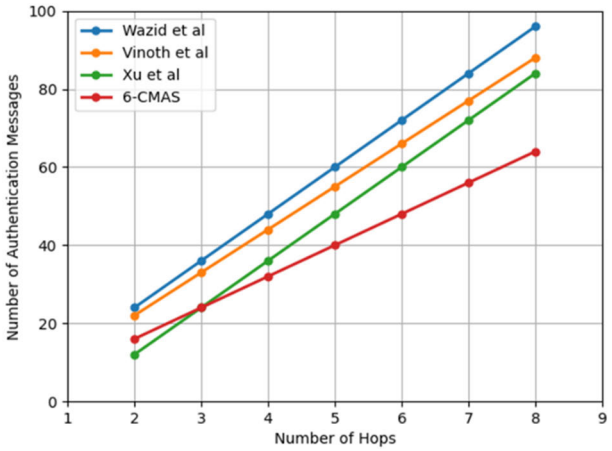

FIGURE 17. Total authentication overhead.

The total authentication overheads in multi hop scenario for our proposed and all benchmarks shown in Table 6 and Figure 16. The total authentication overhead of 6-CMAS for multi hop can be denote as $8(h)$. While for Wazid, total authentication overhead is $12(h)$, for Vinoth total authentication overhead is $11(h)$ and Xu total authentication overhead is $4(h)$, where h is number of hops. There is a small intersection with Xu and 6-CMAS scheme, as Xu scheme utilized symmetric cryptosystem, so as the number of hops increases, authentication overhead increases, this is due to the reason of sharing new symmetric key every time. 6-CMAS after 12 hops, the graphs can be stabilized. Overall, 6-CMAS performed better than Wazid's, Vinoth's and Xu's scheme by 40%, 31.5% and 27% respectively as shown in figure 17.

VII. SECURITY ANALYSIS

As mentioned, there are some potential security threats during each authentication message passing between UE, AP and eNB. Hence, a secure communications system should fulfil the following security requirements where the identification of communicating parties must be checked.

A. DATA CONFIDENTIALITY

To verify data confidentiality of 6-CMAS algorithm, we need to ensure and check whether the data sent can be read by anyone other than receiving party. For this, we can refer to Figure 3 until Figure 10, all messages are encrypted with the public keys of receiving entity. As Figure 3, the message is encrypted with K_{AP} while in Figure 4 the whole message is encrypted with K_{eNB}. Also applied to Figure 5, 6, 7, 8, 9 and 10 where those messages are encrypted using K_{AP}, K_{eNB}, K_{AP}, K_{UE}, K_{AP}, and K_{UE} respectively. Thus, this shows that the message is fully confidential and can only be decrypted using the private key of the receiving devices. For key agreement and exchange, we use an ECC based deffie-helmen secret key sharing, so the chances of password guessing and exposure of secret is negligible.

B. DATA INTEGRITY

To verify the data and message integrity of 6-CMAS algorithm, our proposed algorithm provides integrity checks at two-fold, firstly message integrity check and second data (credential) integrity check. For integrity, it is mandatory to verify whether the data is modified during transmission. To achieve message integrity, we take some part of the message, like in our proposed method, we take only timestamps (to avoid high computational cost), thus, the timestamps of each message must be hashed. In addition, the actual timestamp also needs to be sent to the receiver along with the hashed timestamp. Whenever the message is received, the receiving party need to ensure that the message have not been modified by matching the hash value sent with the value of the hash received, if the hash value is different, then we have a modification issue in the message. Secondly, by using a blockchain where each block is hashed, data integrity of each credential is ensured. Thus, in our scheme, the messages sent are fully secure against any integrity lost as any modification will be detected. This is also applied in Figure 7 and Figure 10 where the authorization key also needs to be hashed along with the timestamp.

C. NON-REPUDIATION

To ensure the reliability of information transmitted, any parties that communicating with each other must agree at some point that either one of them is an originator of a particular message. At these states, the sender should not deny that one had not sent a message. Hence, to achieve non-repudiation requirement, digital signature is utilized. In 6-CMAS protocol, the hash value of timestamp is digitally signed with the sender's private key which is only known by the sender. Consequently, the sender cannot deny that the message is sent by one. Hence, non-repudiation is achieved.

D. USER PRIVACY

To verify the privacy of 6-CMAS algorithm, there is a need to ensure whether the real identity of the user can be revealed or not. In cell-free communication, knowing the real identities of all users can cause various privacy issues as well as real security threats such as identity reveal attack and location visibility attack. Thus, the real identities must be kept private by assigning pseudo identity of the participant. Secondly, participating device cannot know who is communicating to whom. These identities are only known to eNB since eNB is the one who needs to manage the authorization of APs and UEs.

E. TRACEABILITY

To verify the traceability of 6-CMAS algorithm, we need to verify whether the sender can deny that he was the sender of the message. For this, all hashed timestamp is encrypted with the private key of the sender as shown in Figure 3 and applied to the other figures. In addition, the returning hash is signed by the receiving party to make sure the reception and message generator. Secondly, referring to Figure 13, each message is blocked sequentially as shown in the first row of each block. For instance, blocks at UE_1, these blocks are based on messages 1 & 7 from our main algorithm at figure 12. Consequently, blocks at each device (UE, AP & eNB) are also sequentially placed. Moreover, hash value of previous block is also carried forward, thus such mechanism can ensure the legitimate original source of the messages. Subsequently, this method also can mitigate man-in-the-middle attack.

F. MUTUAL AUTHENTICATION

To ensure that impersonation attack cannot be performed, all users are registered with the network and their public key also gets registered at registration authority. In 6-CMAS, all communicating parties must be registered with eNB and authenticate each other securely. The CPU stores all registration records of validated devices and is shared with eNB. Thus, the validation trust and authorization keys are already established. Impersonation attack cannot be made on 6-CMAS algorithm as the private key is only known to the registered device

VIII. CONCLUSION

Cell-Free mMIMO is a part of the technology that will be integrated into future ultra-dense wireless networks. This cell-free approach has proven to be of interest to researchers because of its high bandwidth, high throughput, large amount of data transmission, and greater signal amplification capabilities. A key benefit of the Cell-Free authentication protocol is that it provides data security, location privacy, authentication, and authorization to User Equipment (UE) and Access Points (AP). Since the cell-free network is densely distributed, with a large number of users, high mobility, and frequent data exchange, the efficacy of the present authentication protocols could become a serious challenge. This article proposed a lightweight ECC-Diffie Hellman (ECDH) based multifactor authentication communication protocol to ensure secure communication in Cell-Free 6G cellular network. Moreover, timestamping function, a one-way hash function, and the Blindfold Challenge mechanism are employed to facilitate the multifactor mutual authentication. The proposed scheme provides security measures against typical medium access control layer communication attacks like impersonation attacks, denial of service attacks, replay attacks, and man-in-the-middle attacks. Compared with the existing research works, extensive mathematical and security analysis shows that the proposed scheme outperforms in terms of authentication overhead, communication costs, and computational costs. As part of the further research work of this article, we will integrate 6-CAMS with deep-learning techniques to enhance the current intrusion detection system to mitigate distributed denial of service attacks. In addition, we will also explore how 6-CMAS can ensure secure communication in multihop environment.

REFERENCES

[1] J. R. Bhat and S. A. Alqahtani, "6G ecosystem: Current status and future perspective," *IEEE Access*, vol. 9, pp. 43134–43167, 2021, doi: 10.1109/ACCESS.2021.3054833.

[2] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "IoT-based big data secure management in the fog over a 6G wireless network," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5164–5171, Apr. 2021, doi: 10.1109/JIOT.2020.3033131.

[3] W. Lu, P. Si, G. Huang, H. Han, L. Qian, N. Zhao, and Y. Gong, "SWIPT cooperative spectrum sharing for 6G-enabled cognitive IoT network," *IEEE Internet Things J.*, vol. 8, no. 20, pp. 15070–15080, Oct. 2021, doi: 10.1109/JIOT.2020.3026730.

[4] Y. Fu, Y. Hong, T. Q. S. Quek, H. Wang, and Z. Shi, "Scheduling policies for quantum key distribution enabled communication networks," *IEEE Wireless Commun. Lett.*, vol. 9, no. 12, pp. 2126–2129, Dec. 2020, doi: 10.1109/LWC.2020.3014633.

[5] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6G: A comprehensive survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 334–366, 2021.

[6] A. S. Khan, Y. Javed, J. Abdullah, J. M. Nazim, and N. Khan, "Security issues in 5G device to device communication," *Int. J. Comput. Sci. Netw. Secur.*, vol. 17, no. 5, p. 366, 2017.

[7] R. M. Saqib, A. S. Khan, Y. Javed, S. Ahmad, K. Nisar, I. A. Abbasi, M. R. Haque, and A. A. Julaihi, "Analysis and intellectual structure of the multi-factor authentication in information security," *Intell. Automat. Soft Comput.*, vol. 32, no. 3, pp. 1633–1647, 2022, doi: 10.32604/IASC.2022.021786.

[8] J. Asim, A. S. Khan, R. M. Saqib, J. Abdullah, Z. Ahmad, S. Honey, S. Afzal, M. S. Alqahtani, and M. Abbas, "Blockchain-based multifactor authentication for future 6G cellular networks: A systematic review," *Appl. Sci.*, vol. 12, no. 7, p. 3551, Mar. 2022, doi: 10.3390/app12073551.

[9] A. S. Khan, M. A. Sattar, K. Nisar, A. A. A. Ibrahim, N. B. Annuar, J. B. Abdullah, and S. Karim Memon, "A survey on 6G enabled light weight authentication protocol for UAVs, security, open research issues and future directions," *Appl. Sci.*, vol. 13, no. 1, p. 277, Dec. 2022, doi: 10.3390/app13010277.

[10] S. A. A. Hakeem, H. H. Hussein, and H. Kim, "Security requirements and challenges of 6G technologies and applications," *Sensors*, vol. 22, no. 5, p. 1969, Mar. 2022, doi: 10.3390/s22051969.

[11] K. Shahzad, A. O. Aseeri, and M. A. Shah, "A blockchain-based authentication solution for 6G communication security in tactile networks," *Electronics*, vol. 11, no. 9, p. 1374, Apr. 2022, doi: 10.3390/electronics11091374.

[12] A. I. Salameh and M. El Tarhuni, "From 5G to 6G—Challenges, technologies, and applications," *Future Internet*, vol. 14, no. 4, p. 117, Apr. 2022, doi: 10.3390/fi14040117.

[13] A. S. Khan, Y. Javed, R. M. Saqib, Z. Ahmad, J. Abdullah, K. Zen, I. A. Abbasi, and N. A. Khan, "Lightweight multifactor authentication scheme for NextGen cellular networks," *IEEE Access*, vol. 10, pp. 31273–31288, 2022, doi: 10.1109/ACCESS.2022.3159686.

[14] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi, and J. Abdullah, "Secure trust-based blockchain architecture to prevent attacks in VANET," *Sensors*, vol. 19, no. 22, p. 4954, Nov. 2019.

[15] S. U. Jan, I. A. Abbasi, F. Algarni, and A. S. Khan, "Corrections to 'a verifiably secure ECC based authentication scheme for securing IoD using FANET,'" *IEEE Access*, vol. 10, 2022, Art. no. 105496, doi: 10.1109/ACCESS.2022.3210727.

[16] G. Chopra, S. Jain, and R. K. Jha, "Possible security attack modeling in ultradense networks using high-speed handover management," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2178–2192, Mar. 2018.

[17] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, "Correction to 'cell-free massive MIMO versus small cells,'" *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 3623–3624, May 2020.

[18] W. H. Bailey, B. R. T. Cotts, and P. J. Dopart, "Wireless 5G radiofrequency technology—An overview of small cell exposures, standards and science," *IEEE Access*, vol. 8, pp. 140792–140797, 2020.

[19] H. Jiang, L. Song, Y. Ren, J. Zhang, and L. Hanzo, "A comprehensive survey of 6g wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1733–1762, 3rd Quart., 2021.

[20] W.-S. Liao, M. G. Kibria, G. P. Villardi, O. Zhao, K. Ishizu, and F. Kojima, "Coordinated multi-point downlink transmission for dense small cell networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 431–441, Jan. 2019.

[21] T. C. Mai, H. Q. Ngo, and T. Q. Duong, "Cell-free massive MIMO systems with multi-antenna users," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Anaheim, CA, USA, Nov. 2018, pp. 828–832, doi: 10.1109/GlobalSIP.2018.8646330.

[22] X. Ge, J. Ye, Y. Yang, and Q. Li, "User mobility evaluation for 5G small cell networks based on individual mobility model," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 528–541, Mar. 2016.

[23] S. Samarakoon, M. Bennis, W. Saad, and M. Latva-Aho, "Dynamic clustering and on/off strategies for wireless small cell networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2164–2178, Mar. 2016.

[24] V. Adat, I. Politis, C. Tselios, and S. Kotsopoulos, "Blockchain enhanced SECRET small cells for the 5G environment," in *Proc. IEEE 24th Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, Sep. 2019, pp. 1–6.

[25] R. Parsamehr, A. Esfahani, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, and J.-F. Martinez-Ortega, "A novel intrusion detection and prevention scheme for network coding-enabled mobile small cells," *IEEE Trans. Computat. Social Syst.*, vol. 6, no. 6, pp. 1467–1477, Dec. 2019.

[26] M. Ree, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, and I. Otung, "Key management for beyond 5G mobile small cells: A survey," *IEEE Access*, vol. 7, pp. 59200–59236, 2019.

[27] M. Z. Chowdhury, S. Ahmed, and Y. M. I. N. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Netw.*, vol. 1, pp. 957–975, 2020.

[28] E. Björnson and L. Sanguinetti, "Scalable cell-free massive MIMO systems," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4247–4261, Jul. 2020.

[29] G. Interdonato, E. Björnson, H. Q. Ngo, P. Frenger, and E. G. Larsson, "Ubiquitous cell-free massive MIMO communications," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–13, Dec. 2019.

[30] S. Buzzi, C. D'Andrea, A. Zappone, and C. D'Elia, "User-centric 5G cellular networks: Resource allocation and comparison with the cell-free massive MIMO approach," *IEEE Trans. Wireless Commun.*, vol. 19, no. 2, pp. 1250–1264, Feb. 2020.

[31] X. Zhang, J. Wang, and H. V. Poor, "Statistical delay and error-rate bounded QoS provisioning over mmWave cell-free M-MIMO and FBC-HARQ-IR based 6G wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1661–1677, Aug. 2020.

[32] J. Beysens, Q. Wang, A. Galisteo, D. Giustiniano, and S. Pollin, "A cell-free networking system with visible light," *IEEE/ACM Trans. Netw.*, vol. 28, no. 2, pp. 461–476, Apr. 2020.

[33] S. Elhoushy and W. Hamouda, "Towards high data rates in dynamic environments using hybrid cell-free massive MIMO/small-cell system," *IEEE Wireless Commun. Lett.*, vol. 10, no. 2, pp. 201–205, Feb. 2021.

[34] S. Kim and B. Shim, "Energy-efficient millimeter-wave cell-free systems under limited feedback," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4067–4082, Jun. 2021.

[35] R. Abozariba, M. K. Naeem, M. Patwary, M. Seyedebrahimi, and P. Bull, "NOMA-based resource allocation and mobility enhancement framework for IoT in next generation cellular networks," *IEEE Access*, vol. 7, pp. 29158–29172, 2019.

[36] X. Zhang, D. Guo, K. An, and B. Zhang, "Secure communications over cell-free massive MIMO networks with hardware impairments," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1909–1920, Jun. 2020.

[37] X. Zhang, D. Guo, K. An, Z. Ding, and B. Zhang, "Secrecy analysis and active pilot spoofing attack detection for multigroup multicasting cell-free massive MIMO systems," *IEEE Access*, vol. 7, pp. 57332–57340, 2019.

[38] Y. Mao, Y. He, Y. Zhang, J. Hua, and S. Zhong, "Secure TDD MIMO networks against training sequence based eavesdropping attack," *IEEE Trans. Mobile Comput.*, vol. 19, no. 12, pp. 2916–2932, Dec. 2020.

[39] J. Xu, X. Wang, P. Zhu, and X. You, "Privacy-preserving channel estimation in cell-free hybrid massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, pp. 3815–3830, Jun. 2021.

[40] M. Wazid, A. K. Das, N. Kumar, V. Odelu, A. G. Reddy, K. Park, and Y. Park, "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 14966–14980, 2017.

[41] M. Wazid, A. K. Das, N. Kumar, and M. Alazab, "Designing authenticated key management scheme in 6G-enabled network in a box deployed for industrial applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7174–7184, Oct. 2021.

[42] Y. Aydin, G. K. Kurt, E. Ozdemir, and H. Yanikomeroglu, "A flexible and lightweight group authentication scheme," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10277–10287, Oct. 2020, doi: 10.1109/JIOT.2020.3004300.

[43] M. Chen, C. Tan, X. Zhu, and X. Zhang, "A blockchain-based authentication and service provision scheme for Internet of Things," in *Proc. IEEE Globecom Workshops (GC Wkshps*, Taiwan, Dec. 2020, pp. 1–6, doi: 10.1109/GCWkshps50303.2020.9367565.

[44] A. S. Khan, J. Abdullah, K. Zen, and S. Tarmizi, "Secure and scalable group rekeying for mobile multihop relay network," *Adv. Sci. Lett.*, vol. 23, no. 6, pp. 5242–5245, 2017.

[45] K. Y. Chan, J. Abdullah, and A. Shahid, "A framework for traceable and transparent supply chain management for agri-food sector in Malaysia using blockchain technology," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 11, pp. 1–8, 2019, doi: 10.14569/IJACSA.2019.0101120.

[46] M. Safkhani, N. Bagheri, S. Kumari, H. Tavakoli, S. Kumar, and J. Chen, "RESEAP: An ECC-based authentication and key agreement scheme for IoT applications," *IEEE Access*, vol. 8, pp. 200851–200862, 2020, doi: 10.1109/ACCESS.2020.3034447.

[47] R. Vinoth, L. J. Deborah, P. Vijayakumar, and N. Kumar, "Secure multifactor authenticated key agreement scheme for industrial IoT," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3801–3811, Mar. 2021, doi: 10.1109/JIOT.2020.3024703.

[48] S. O. Maikol, A. S. Khan, Y. Javed, A. L. A. Bunsu, C. Petrus, H. George, and S. Jau, "A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities," *Int. J. Integr. Eng.*, vol. 13, no. 2, pp. 127–135, 2021.

[49] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, and J. Bastos, "A lightweight authentication mechanism for M2M communications in industrial IoT environment," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 288–296, Feb. 2019.

[50] J. Zhang, Z. Wang, D. Wang, X. Zhang, B. B. Gupta, X. Liu, and J. Ma, "A secure decentralized spatial crowdsourcing scheme for 6G-enabled network in box," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6160–6170, Sep. 2022, doi: 10.1109/TII.2021.3081416.

[51] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, "A lightweight mutual authentication and key agreement scheme for medical Internet of Things," *IEEE Access*, vol. 7, pp. 53922–53931, 2019, doi: 10.1109/ACCESS.2019.2912870.

[52] R. Jang, J. Kang, A. Mohaisen, and D. Nyang, "Catch me if you can: Rogue access point detection using intentional channel interference," *IEEE Trans. Mobile Comput.*, vol. 19, no. 5, pp. 1056–1071, May 2020.

[53] S. Vanjale and P. B. Mane, "A novel approach for elimination of rogue access point in wireless network," in *Proc. Annu. IEEE India Conf. (INDICON)*, Pune, India, Dec. 2014, pp. 1–4, doi: 10.1109/INDICON.2014.7030418.

[54] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-factor authentication for IoT with location information," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3335–3351, Apr. 2019.

[55] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, Jan. 2021, Art. no. e4150.

[56] S. Aggarwal, N. Kumar, and S. Tanwar, "Blockchain-envisioned UAV communication using 6G networks: Open issues, use cases, and future directions," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5416–5441, Apr. 2021, doi: 10.1109/JIOT.2020.3020819.

[57] P. Zhu, J. Hu, X. Li, and Q. Zhu, "Using blockchain technology to enhance the traceability of original achievements," *IEEE Trans. Eng. Manag.*, early access, Apr. 15, 2022, doi: 10.1109/TEM.2021.3066090.

[58] A. S. Khan, Y. Javed, J. Abdullah, and K. Zen, "Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS)," *J. Ambient Intell. Hum. Comput.*, vol. 1, pp. 1–18, Mar. 2021, doi: 10.1007/S12652-021-02968-6.

[59] C.-M. Chen, X. Deng, W. Gan, J. Chen, and S. K. H. Islam, "A secure blockchain-based group key agreement protocol for IoT," *J. Supercomput.*, vol. 77, pp. 9046–9068, Feb. 2021.
[60] Q. Mei, H. Xiong, Y.-C. Chen, and C.-M. Chen, "Blockchain-enabled privacy-preserving authentication mechanism for transportation CPS with cloud-edge computing," *IEEE Trans. Eng. Manag.*, early access, Apr. 14, 2022, doi: 10.1109/TEM.2022.3159311.

ADNAN SHAHID KHAN (Senior Member, IEEE) received the B.Sc. degree (Hons.) in computer science from the University of the Punjab, Lahore, Pakistan, in 2005, and the master's, Ph.D., and Postdoctoral degrees in networks and information security from the Universiti Teknologi Malaysia, Johor Bahru, Malaysia, in 2008, 2012, and 2013, respectively. He is currently an Associate Professor with the Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak (UNIMAS). His research interests include cybersecurity in wireless communication, cloud computing, the Internet of Things, software-defined networking, cryptography, networks, and information security.

MOHD IZZAT BIN YAHYA received the bachelor's degree (Hons.) in computer science (network computing) from the Universiti Malaysia Sarawak (UNIMAS), Sarawak, in 2020, where he is currently pursuing the master's degree in wireless network technologies. He is also an Information Technology Officer with the Ministry of Education, Malaysia, where he is working on project in enterprise architecture. His research interests include wireless communication, cloud computing, the Internet of Things, cryptography, wireless networks, and information security.

KARTINAH BT ZEN received the Ph.D. degree in sensor network from Edith Cowan University (ECU), Australia. She is currently an Associate Professor with the Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak (UNIMAS). She is also a Research Fellow with the Centre of Excellence for Rural Informatics, where she is working on project in wireless sensor network. Her research interests include wireless sensor networks data transmission and sensor-related network technology and application.

JOHARI BIN ABDULLAH received the bachelor's degree in computer science (networking) from the Universiti Putra Malaysia, the master's degree in IT from the Queensland University of Technology, Brisbane, Australia, and the Ph.D. degree in computing science from Newcastle University, U.K. He is currently an Associate Professor with the Faculty of Computer Science and IT, UNIMAS, Sarawak. His research interests include ICT is wide and ranging from trusted systems, blockchain technology, web system design and development, system architecture, problem-solving using tools, such as TRIZ, ICT education for children and youth through computational thinking, scratch, computer science unplugged, and open-source system and software.

ROZEHA BINTI A. RASHID (Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Michigan, Ann Arbor, USA, and the M.E.E. and Ph.D. degrees in telecommunication engineering from the Universiti Teknologi Malaysia (UTM). She is currently an Associate Professor of the Communication Engineering Program with the School of Electrical Engineering, UTM, and also the Head of the Telecommunication Software and System (TeSS) Research Group. She is involved in many IoT based industry projects. To date, she has led more than 20 projects as the principal investigator and about 40 projects as a co-investigator under various types of grants, that including national, industry, community, and university grants. She more than 140 publications mostly in the area of telecommunication engineering. Her current research interests include wireless communications, sensor networks, cognitive radio, and the Internet of Things (IoT).

YASIR JAVED (Member, IEEE) received the Ph.D. degree from UNIMAS, Sarawak, in 2020. He is a skilled senior programmer/a developer with more than 15 years of experience in programming, software development, project management, and analytics. He is also a Research Engineer with the COINS Research Group. He has an Analyst Programmer with the Prince Megren Data Center, Center of Excellence and Research and Initiative center, Prince Sultan University, where he is currently an Active Member of RIOTU Group. He has successfully completed various international and national research funding projects. His research interests include programming, robotics, drones, vehicular platoons, secure software development, mobile apps security, signal processing, the IoT analytics, intelligent applications, statistics, data analytics, forensics analysis, big data, and predictive computing.

NAYEEM AHMAD KHAN received the Ph.D. degree in computer science from University Malaysia Sarawak, in 2018. He is currently an Assistant Professor with the Faculty of Computer Science and Information Technology, AlBaha University, AlBahah, Saudi Arabia. He is also an expert on attacks on critical infrastructures and has led many research projects. His research has been published in several high impact international journals. He has presented his research findings at many international conferences. He has several patents to his name. He has won many awards, fellowships, grants, and appreciations for his work. He has written a remarkable book on malicious JavaScript attack detection using machine learning. His research interests include cybersecurity, cyber intelligence and analysis, unmanned aerial vehicles, deep learning, and the Internet of Things. He has been the chair and the co-chair of many conferences and technical sessions. He has been a reviewer of many high impact journals.

AHMED M. MOSTAFA received the B.Sc. and M.Sc. degrees in electronics, communications, and computer engineering and the Ph.D. degree in computer engineering from Helwan University, Egypt, in 2001, 2007, and 2012, respectively. He is currently an Assistant Professor with the Department of Computer and Systems Engineering, Faculty of Engineering, Helwan University. He joined several other universities in Egypt, including Misr International University (MIU) and October 6 University. He is also an Assistant Professor with Albaha University, Saudi Arabia. His research interests include cloud computing, multi-core systems, real-time systems, real-time processing/scheduling, network-on-chip, distributed systems, and the Internet of Things.