Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 8
August 2023

Blockchain-Based Multi-Factor Mobile DeviceAuthentication Technique in Mobile Cloud Computing

Mr. Vikram Patalbansi[1] , Dr. Jayshree Jain[2] , Dr. G. Prasnna Laxmi[3]
Research Scholar, Pacific University, Udaipur, India Professor, Pacific University Udaipur
1. Woman Scientist, DST-WISE Postdoctoral.

Abstract-Combining general cloud computing with mobile computing, MCC[1] requires the use of mobile electronics and peripherals, such as mobile smartphones, laptops, and other devices, toaccess resources from a remote cloud data center using cellular technology or wireless communication. Storage space, computing power, and battery life are just a few of the resource limitations that mobile devices in general come across. Therefore, we are unable to manipulate information from cloud data centers on mobile devices using basic mobile computing tools and programming. The process of mobile device authentication involves establishing the legitimacy of themobile network and cloud computing system to safeguard the user's sensitive data from control orders from unauthorized users or user equipment. Information in the form of radiosignals has been experiencing increased security difficulties due to the open nature of wireless networks or cellular networks utilized in mobile cloud computing systems. Mobile device authentication must be necessary to improve the security performance of the wireless system in MCC due to the open nature and susceptibility of wireless communication. In theproposed thesis, we make various identity and access management (IAM) suggestions to control which devices connect and are permitted to access business data from the cloud server via a wireless mobile network, or 5G mobile networks. A blockchain-based authentication system has been developed recently with the rise of blockchain technology to securely confirm user identification in online mode. With the use of blockchain technology, the complete information system network can maintain its data integrity; no external entity is required to centrally monitor the network. The level of security of authorized access to company data, information, and resources from the MCC cloud storage system will be increased by the multi-factor authentication system integrated with blockchain technology. In the proposed thesis, we also mentionseveral research projects on terminology for mobile device authentication utilizing the technology of blockchain.

Keywords: Mobile Cloud Computing, multi-factor authentication,wireless network, and blockchain security.

I.Introduction

The term "Mobile Cloud Computing," or MCC for short, refers to a new computing paradigm that combines aspects of cloud computing with mobile networks, each of which has a variety of components. The MCC grants access to cloud computing resources, including processing power, storage space and services, for any electronic mobile device. These resources are delivered using wireless communication networks, such as mobile or cellular networks, Wi-Fi[2] [1], andso on. Using Mobile Cloud Computing (MCC), all of theprocessing and storage is done over the cloud computing areainstead of the mobile device due to the mobile device's limitations in storage and processing
power, and informationis stored in multiple locations so that MCC is a reliablesystem and on-demand we can get access to any information regardless of location and hardware configuration of usermobileelectronic devices and thereforesharing
ofinformation between two or more entities via the wirelessconnection. [22].The purpose of this thesis paper is to represent a new theory of encrypting information as well as authenticating the user of a mobile device. Specifically, this study will focus on mobile devices authentication. Because of this, mobile devices need to be registered and authorizedbefore they can get any form of service from wirelessnetworks or cloud servers. Because of the limited resources and processing power that mobile devices have, so it is notadvisable to carry out complicated tasks on a

mobile device toauthenticate a user [8]. In MCC, if the mobile user and thecloud service provider are both registered with the mobile wireless network, then the mobile device and the cloud server will be authenticating to each other with a uniqueauthentication protocol.This will establish secure communication between mobile devices and cloud serversover secure channels at both ends to prevent any vulnerabilityand ensure the legitimacy of data access [11]. Despite this, security is a major issue in MCC, particularly when it comes to mobile authentication. The process of confirming theidentification of a user or an electronic device that is attempting to access information or resources from a cloud

[1] Mobile Cloud Computing

computing system is referred to as mobile device authentication [5]. The Mobile Device, as well as the user, must serve as an integral component of the Mobile Cloud Computing system's security mechanisms. If any unauthorized user or any mobile device is successful in entering the system due to the lack of a high-security algorithm and authentication technique, then it can access sensitive corporate information or any other decision-making information, then he can misuse this information, and finally, it will impact badly on our business process [10]. Because of these sorts of mobile devices are susceptible to distinct threats in an uncertain mode that are not experienced in static environments, additional levels of sophisticated security measures are required for mobile devices, particularly wireless devices. This is because mobile devices of this kind are more likely to be used in dynamic environments. Altering of information, denial of service (DoS) or denial of access, interruption of transactions, transmission delays, and signal volatility during communication are some of the dangers associated with mobile communication [4]. For instance, if a user logs in to access MCC services using their digital signature on their digital assistant (PDA) or laptop, the user will not be able to access the data, if a personal digital assistant (PDA) is misplaced or forgotten, a hacker may abuse the PDA or laptop to get unauthorized access to sensitive information or manipulate the authentication procedure, which may lead to the loss of sensitive information. Hackers or users not authorized to do so will install malware scripts, which will provide them access to user credentials. Therefore, authentication of mobile devices is one of the most important criteria in the MCC system's security to safeguard our data at any level of the system. [4] Mobile device authentication is the process of confirming the identity of mobile users to allow permission to access services from MCC system resources. The majority of MCC's authentication methods fall into one of three categories:

1. Knowledge-based authentication is a form of authenticationthat involves the use of mechanisms that require mobile users to enter something that only they know, such as a password, a personal identification number (PIN), or any security questions. This method is frequently utilized for authentication processes, even though it is susceptible to attacks such as phishing and brute-force attacks [4].

[2] Wireless Fidelity

2. Authentication that is primarily based on Biometric variables technique uses authentication methods that are primarily based on biometric variables such as fingerprint recognition, facial recognition, voice recognition, and iris recognition. When compared to knowledge-based authentication procedures, biometrically-based authentication techniques offer a higher level of protection. On the other hand, there are instances in which it is susceptible to spoofing attacks [4].
3. Context-aware authentication method verifies the user's identification by using information about the user's context, such as the time, the location, and their conduct at the current

technique [4]. During the authentication process for mobile devices used with MCC, some different parameters are required to be taken into consideration according to the approaches described above. As a result of our research and the numerous RA[3] evaluations that we combed through, we have compiled a summary of several of the characteristics that are helpful in mobile device authentication.

i. Behavioural Biometrics: The techniques of behavioral biometrics analyze the one-of-a-kind behavioral patterns of an individual user to authenticate his identification. These unique behavioral patterns include typing speed, swiping

patterns, and touch pressure. When using this technology, it is very difficult to spoof a mobile user's identity, and it gives an additional degree of protection when mobile device authentication is beingperformed [7].

ii. Risk-based authentication: Risk-based authentication makes use of data analytics to determine the level of risk connected with a login attempt. Using this strategy, the locationof the user, the device which user is using, and the behavioral patterns that the user exhibits can be used to determine the same type of fraudulent login attempt [20].

iii. Token-based authentication: This method requires the creation of a new token that is exclusive to each login attempt and is only valid for a single use. This token is transmitted to the user's mobile device, and, in addition to the user's login credentials, it is required to be typed into the MCC system to acquire access.

iv. Voice Recognition: The technology of voice recognition analyzes the distinctive vocal patterns of an individual to verify the user's identity on a mobile device. This method is simple to implement and adds an extra degree of protection because it is difficult to imitate the voice of any individual.

v. Multifactor authentication: The multifactor authentication combines two or more authentication parameters or factors, such as login credentials information like username and password, fingerprint or any other biometric impression of the human body, and mobile device hardware configuration data like IMSI (International Mobile Subscriber Module) or SIM[4] card and IMEI (International Mobile Equipment Identity), i.e., MAC [2] or physical address of the mobile devices, etc. In this scenario, attackers will not be able to acquire access to the system even if they gain access to any one of the criteria, as long as they do not also have information regarding the other elements. Because of each element, he is required to carry out a large number of activities that are both time-consuming and challenging from a technical standpoint [12].

vi. Certificate-based Authentication: This method verifies the genuineness of mobile devices by using a digital identity as a certificate. In this particular scenario, the reliable third party will issue a digital signature that will be kept in the chip-like digital circuit or virtual smart card. In this kind of additional hardware slot that is incorporated into mobile devices, some one-of-a-kind identification information is manufactured on a chip, and that one-of-a-kind information is used as one of the parameters for authentication. According to the findings of our Universal Integrated Cloud Circuit (UICC) to each mobile user as an individual identity purpose. [13].

vii. Authentication Application: The authentication application that was developed and provided by the service provider to its individual system users. Within our MCC system, the user interface (UI) of a mobile application that has been exclusively designed and is solely offered by CSP to provide proper platform to valid mobile users is how any mobile device user can access the service. There is not a single application program that is incapable of connecting to the MCCsystem. This variety of authentication applications was produced with the assistance of tools that are compatible with both the Android and iOS operating systems. The Android application is currently the most popular and easiest-to-operate option available on the market. We can create an authentication program for laptops and personal computers using languages such as Java, Python, Android and others. The authentication application that is commonly installed on mobile devices carries with it a set of parameters that are used when it was properly configured, guarantee the authenticity and safety of the authentication procedure. The authentication application gives you access to all of the following parameters:

4. moment. The level of security can readily be
5. increased by
6. combining this technique with any
7. other authentication

[3] Research Article

[4] Subscriber Identity Module

study, cloud service providers (CSP[5]s) give a User Identification: The authentication program will first take legitimate login credentials, which may include a username, password, email address, mobile number, or any other social security number, etc.

1. Password Strength: The AA[6] ought to enforce password strength standards such as minimum length, complexity, and expiration time to ensure that users have strong passwords that are not easily guessed.
2. Device Security: AA should be able to examine the security status of the mobile device, such as whether or not it has been jail broken or whether or not it has had any other form of malware covertly planted on it. Because of this, it is possible to prevent assaults of any kind that take advantage of vulnerabilities in the operating system of the device.
3. Session Management: AA is responsible for managing user sessions and ensuring that secure connections are made at the beginning of each session, as well as that sessions end without any issues after they have been completed. Attacks like session hijacking and man-in-the-middle attacks might be avoided as a result of this measure.
4. Audit logging: The AA should record all authentication events, including successful and unsuccessful attempts to log in. This will enable forensic investigations and increase the system's level of security.
5. Biometric impression sensors: AA's ability to take a human body biometric impression for use in the future authentication process. Therefore, AA needs to be compatible with the sensors that are found on mobile devices so that it may take input in the form of a biometric impression like a thumbprint, iris scan, facial recognition, or other similar methods.

[5] Cloud Service Provider

[6] Authentication Application

In brief we can say that authentication application that is installed on mobile devices has several different functions and settings, some of which are listed here. The particular characteristics, as well as how they are implemented, are subject to change based on the functionality and level of protection offered by the mobile device in question.

Blockchain Technology: The blockchain, which is a sort of distributed database, uses distributed ledger technology to avoid the falsification of data records brought about by arbitrary alteration. This technology is disseminated across the internet. A blockchain has a variety of advantages over traditional centralized systems, including advantages in the areas of efficiency, security, resilience, and transparency [1]. Blockchain network technology uses decentralized ledgers to record transactions. A blockchain system is simple to administer, and all of the transaction details are saved on the computers of every participant in the system. In comparison to centralized data management, the blockchain system features a more robust set of security protocols. The hazards of hacker incursions into the centralized control node of the centralized data management system, as well as the possibility of the system failing, are present in this type of system. Because all information is distributed uniformly throughout all of the participating nodes in the blockchain network, the system does not contain a single point of failure. Because it would require the attention or approval of every node in the blockchain system, modifying data or information is nearly impossible under this architecture. This is because data is replicated throughout all nodes of the blockchain system in an equal fashion. No node has the authority to alter data. If there is a need for any changes to be made to the data, then all of the nodes in the system will be notified about it, and the modified data will be saved in every node. Therefore, this form of transparency about data resources and utilization is implemented in the blockchain, and every node of the system has metadata about data usage recording [25].

Ii.. Related Works

Using smart mobile devices, users may now enjoy a greater degree of ease in their day-to-day activities. This makes it possible for users to take advantage of a variety of applications at any time and from any location, including mobile media, navigation, online banking, and mobile

shopping[4]. Individuals' private information, such as their name and credit card number, could be given to a third party in an unauthenticated manner if they use mobile devices, even though these gadgets allow individuals more flexibility and convenience. By unlocking the mobile device in an unauthorized manner, a potential adversary could gain access to the sensitive private information that is kept on the mobile device, exposing themselves to potential security vulnerabilities in mobile services and applications. For instance, an adversary could make use of the user's mobile device to carry out activities that are not permitted, such as conducting online transactions or putting malware on the user's mobile device. As a result, authentication on mobile devices plays an important

role in protecting the sensitive information that users store on mobile devices and preventing unauthorized access to mobile devices. The authors, Chen Wang et al. [4], classify the different mobile authentication methods into one of four groups, particularly based on the basic authentication metrics that are employed in existing mobile authentication methods. These metrics include knowledge, ownership, and biometrics.

1. Authentication based on the possessor's knowledge (such as using a password or a specific combination for a lock)
2. Authentication methods based on a person's physiological characteristics (such as scanning of the iris and fingerprints, for example)
3. Authentication based on behavioral biometrics (such as, for example, gait and hand gestures)
4. Authentication using combination of at least two or more above factors

Based on the aforementioned elements, any user can integrate all of the aforementioned authentication factors to determine the user's identity and carry out a multi-factor authentication scheme for the authentication purpose of smart mobile devices. The authors examine and contrast a variety of authentication methods for mobile devices according to the kind of identification information that is used during authentication. The identity information can be knowledge (such as a password or an unlock pattern), biometrics (such as fingerprints or retinas), or ownership (such as a software token or the mobile device itself). These three types of information correspond to the three most important questions that are asked during an identity check: what you know, what you have, and who you are.

Dianqi Han et al. [10] provide a theory on mobile authentication using the approach of acoustic fingerprinting to identify a mobile device based on its internal microphone and speakers, which are unique in terms of their functionality due to an error in the manufacturing process. They are the basis for concluding the appropriateness of the existing acoustic fingerprinting system for mobile authentication in terms of accuracy, deployability, and security. The authors introduced the notion of a dynamic challenge-response mechanism to authenticate fingerprint input from a variety of sources to circumvent the difficulties presented by fingerprint emulation attacks. Acoustic non-linear patterns (ANP), which are hardware properties of mobile devices like speakers, microphones, or speaker-microphone pairs, can be used as acoustic fingerprints rather than the traditional method of using acoustic fingerprints. However, the most significant limitationof this theory is that there will be no one-time solution to the problem of mobile authentication if any of the features of mobile devices are damaged, lost, or replaced, or if there is any change in the configuration of the device. In the study manuscript that they wrote, Jamil Asim and his colleagues [12] introduced multifactor authentication approaches. According to the definition that has been standardized, multifactor authentication is a mechanism that was designed for security and employs several kinds of authentication from different

Multifactor authentication was developed for security purposes. Multifactor Authentication's (MFA) major goal is to develop layered defenses that make it extremely difficult for unauthorized individuals to get access to mobile devices, locations, networks, and databases. This is accomplished through the use of a variety of different authentication methods. However, while reviewing the material, we discovered that even if one of the barriers or layers is breached, an attacker, hacker, or any other unauthorized user still needs to break through one or more security

layers to entirely infiltrate the applications and system through software and hardware. The primary purpose of multifactor authentication, also known as MFA[7], is to strengthen the security of digital transactions. A. Mukherjee and colleagues [1] suggested the authentication theory for small devices that might be used in a smart home with the assistance of blockchain technology. They propose a secure authentication theory for people and devices by merging blockchain technology and public key cryptography. The process of generating a cryptographic key and storing it at each node of a blockchain network of nodes consumes additional time. Additionally, the storage of cryptographic information in each node presents challenges related to code redundancy. It will generate a token for each device, and the value of this token will be encrypted and stored at the node. If someone gains access to this token, they will have the ability to quickly enter the smart home system, hack it, and influence its operations. The authors, Umoren O. et al. [25], established safe authentication mechanisms with increased performance using the Neo Blockchain platform, with advancements in security and faster executions. An IoT and fog computing environment necessitates the implementation of a smart contract based on the Neo blockchain to address concerns regarding secure authentication as well as other restrictions. Edge devices, sensors, and any other devices with limited resources are taskedwithin a cloud computing environment with the responsibility of creating this kind of environment as well as collecting and transmitting data. The authentication of mobile devices is a difficult job because of the resource limits that they have. The authors, H. Ali et al. [11], offer a new protocol framework that protects IMSI[8] from bogus BS. These technologies establish the secret key identifier between the user equipment (UE) and the genuine base station (BS), which results in an increased level of security for the 5G mobile network. During transmission between the user equipment (UE) and the base station (BS) in a 5G cellular network, the authentication procedure in their technique makes use of the XOR operation to encode IMSI with a secret key. The mobile device is responsible for generating its keys and then performing an XOR operation between those keys and the IMSI code to encode the IMSI. This encoded IMSI is then publicly communicated as the UE's unique identification within an open wireless network. The phony BS and IMSI devices are successful in capturing the secret code, but they are unable to retrieve the original information. Using biometrics and secret parameters, th
independent sources and through varying
credentials to verifythe user's identity to
log in and conduct transactions.

[7] Multifactor Authenticator

[8] International Mobile Subscriber Identity module

authors, SungJin Yu et al. [24], suggested a safe and effective three-factor authentication protocol as a solution to the security flaws that are present in mobile devices to protect against a wide variety of different types of attacks. They make use of both informal and formal security analyses, such as the real-or- random (RoR) model and the Burrows-Abadi-Needhan (BAN) logic, to test the efficacy of the protocol. The authors compared the computation cost and security features of their proposed mechanism with those of an already existing scheme related to the authentication of devices. The authors found that their proposed authentication scheme, which is based on three factors and gives good performance while also having a low computation cost, satisfies the security requirements for roaming service. In this paper, the authors, Reichinger D. et al.,
[21] propose the theory of a continuous user authentication system for the Android-based mobile device ecosystem. This system continuously monitors and records touch, accelerometer, and timestamp data and runs experiments to gather data from a variety of parameters and functionalities. It is possible to accomplish this by integrating data from the location and accelerometers using gestures that contain at least 50 data points and then averaging the outcome of making predictions based on 25 consecutive gestures. They use several different body movements as inputs and then aggregate those gestures together to achieve the highest possible performance outcomes in terms of the system's overall security. Their newly designed

technology gives an in-depth look at a completely integrated system by first gathering the essential data and then using a model to anticipate the beneficial values that should be provided as input. However, if the user sustains injuries to any of their body parts as a result of an accident or if the sensors on their mobile device are not functioning correctly, then this method may no longer be applicable. The authors, L. Yi et al.,[16] said in this research that traditional authentication schemes are more susceptible to various attacks, such as shoulder surfing attacks, and biometric-based attacks in the biometric-based scheme, such as fingerprint recognition andface recognition, can be readily broken. To accomplish all of these different kinds of authentication schemes, a supplementary device support system is required, although it has some limitations. There are numerous authentication techniques, and every once in a while, those schemes either prioritize security over usability and ignore availability, or they prioritize usability over security and have insufficient levels of security. Therefore, to confirm the identity of the mobile device through the MCC system, we require a new form of authentication scheme. This scheme needs to be able to strike a balance between security and usability to safeguard the user's private credentials and the data stored on the mobile device. One-time authentication does not provide adequate protection against spying attacks, as demonstrated by the author's Dee. T. et al. [7]. The intelligent mobile device possesses different user identities and its own parameter fetching facilities for authentication, just like biometric-based authentication. The authors took into account the behavioral characteristics of the human user while the user was operating a mobile device. These behavioral characteristics included touch-screen swipe
interactions, touch-screen input pressure intensity, and other similar characteristics. The virtual keyboard that is available for mobile device interactions delivers a consistent biometric data stream as well as biometric profiles by making use of touch pressure, position, and timing. The convenience of transparent authentication can be maximized with the assistance of this continuous authentication technique that runs in the background. [27] The authors of this work, Zukarnian Z.A., use a variety of multifactor authentication methods, such as a unique impression of the user's fingerprint, identification of the user's present position obtained from a GPS[9] system, identification of the mobile device's MAC address and IMSI code, and assignment of a private key for cryptography. The authors, Nerini M. et al. [18], recommended using a PIN as a method of authentication by taking into account behavioral biometrics, such as the motions of a smartphone, about individual user usage of a smartphone. Using their proposed methodology, which is based on anomaly detection and is capable of recognizing whether the PIN is being inserted by the authenticated user of the smartphone or by an attacker, they canaccomplish this. Through the use of the device's built-in motion sensors, this approach keeps track of how the user moves the smartphone while entering the PIN. Using the machine learningmethod, your PIN will generate a score that is unique for each digit. After that, the scores of these individual PIN digits are merged to get the final decision score metrics. The authors improve the safety of the N-digit PIN authentication that is used on mobile devices by making use of behavioral biometrics. This improvement may be achieved simply by following thetechniques that have been provided. Based on this information, they conclude that they can determine whether the proper PIN was entered by the genuine users of the mobile device or by an attacker. In general, an authentication, authorization, and access control system will guarantee security for any kind of data that is collected and stored on a cloud server[25]. We ensure that our data stored on the cloud server is protected to a high degree by putting in place a dependable authentication system that can be used with mobile devices. When authorization and authentication are dependent on a third party that can be trusted,there is a greater risk of a variety of breaches and assaults. For this reason, a more sophisticated verification method is required for mobile devices to guarantee the safety of the data.

III. Proposed System

Mobile consumers have shown a preference for utilizing internet services throughout the past year. These services include accessing social media, doing financial transactions, trading stocks

and currencies, and many more. All of these services can be accessed by sophisticated mobile devices from the data repositories that are stored on cloud servers through various forms of wireless communication media, such as a mobile communication network (cellular network). As a result of the open nature of radio or wireless signal propagation, wireless signals are susceptible to a wide variety of security

[9] Global Positioning System

vulnerabilities, and the valuable information that we send over these signals is in danger of being hacked or intercepted by a MITM[10] attacks. Therefore, we need to come up with some sort of security mechanism so that unauthorized users will not be able to access our information system. Therefore, the identity of the new user must be verified before they can be added to the MCC system, and only then can they be permitted to access MCC. The authentication of mobile devices is vital to the protection of mobile devices, wireless networks, and cloud service providers from unauthorized access. For this reason, mobile user data ownership and digital identity authentication are critical criteria for privacy and security for end users who want to keep their business information secret from the outside world. For mobile device authentication in our suggested system, we take into consideration the Multi-Factor Authentication (MFA) technique. When using the MFA technique, the user is required to provide two or more authenticating parameters, and only after our system has made the appropriate

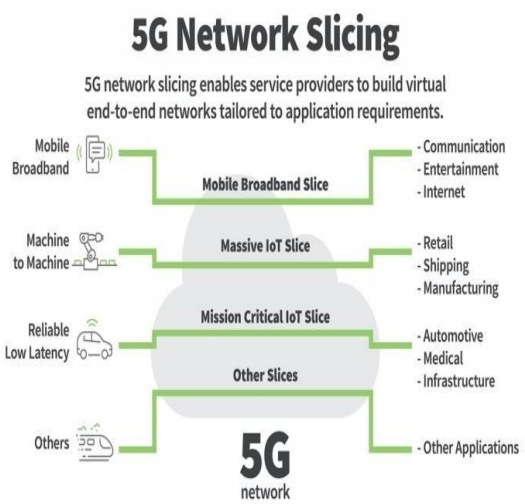

Fig.1 5G Network Service Network Architecture [source: https://www.stl.tech/blog/5g-network-architecture/]

computation will it permit the user to receive services from MCC. The purpose of proposed thesis paper is to present our proposal for an authentication system for mobile devices that makes use of multi-factor authentication (MFA) in conjunction with blockchain technology. Transactions involving cryptocurrencies can now be carried out using a cutting-edge and widely adopted decentralized network technology known as the blockchain. Within the framework of blockchain technology, it is possible to authenticate users' identities while also validating significant digital information. The authentication process that makes use of the technology of blockchain provides a safer means of determining whether or not the digital data that is kept in its chain of blocks is accurate and where it came from. In the real world, each node on the blockchain-powered network is capable of maintaining its data integrity. This is one of the many advantages of using blockchain technology. It is not necessary to utilize the services of a third party to carry out centralized monitoring of the network administration. In a nutshell, we can assert that there is no requirement for a centralized server to store and manage the information. Every node that is a part of the blockchain network stores the data in the form of blocks, and within each block, a transaction history of the information is saved along with a suitable date and a unique identity. In blockchain authentication, the personal information that is used to validate any other node's identity is saved as a hash value of the name and a unique identity number. This information can only be accessed by the blockchain itself. In the blockchain-based authentication system, network users are required to have a unique identity. This can be in the form of a unique MAC code, unique login credentials, a private key for cryptography, or any other identifying number based on biometrics.

The authentication system that is based on blockchain technology includes a few unique characteristics.

1. Safe and reliable authentication and identification ofintelligent mobile devices
2. The device that is using the blockchain system always stores cryptographic keys in the

flash memory of the device.

3. Mobile devices have security measures in place to prevent cyberattacks, spying attacks, MITM attacks, and replay attacks.

We are attempting to suggest that one potential future research direction for user authentication on smart mobile devices is the development of new authentication approaches that are based on integrated multi-dimensional authentication metrics, such as knowledge, biometric, and ownership-based input information by the embedded sensors in mobile devices and blockchain technology. All of these multiple authentication metrics are collected at one instance or one time, and this authentication approach decreases the user effort required throughout the entirety of the authentication process. This is what makes multi- factor user authentication practicable in practice. In particular, these integrated authentication metrics should be gathered at the same time. This gives many dimensional relationships that are difficult to fabricate by an attacker and considerably improves the security strength of the procedures for authenticating mobile devices. We are going to integrate knowledge-based and biometric-based variables that comprise the unique identity information of a user. This is the integration of different user characteristics into two distinct physical domains. Even if an attacker were to note down the user's input parameter values, it would be extremely difficult to fake such an integration of the information. User authentication on mobile devices is an important technology that prohibits unauthorized access to a mobile device or any other application in the MCC system to protect the sensitive information of the user.

[10] Man-in-the-Middle attacks

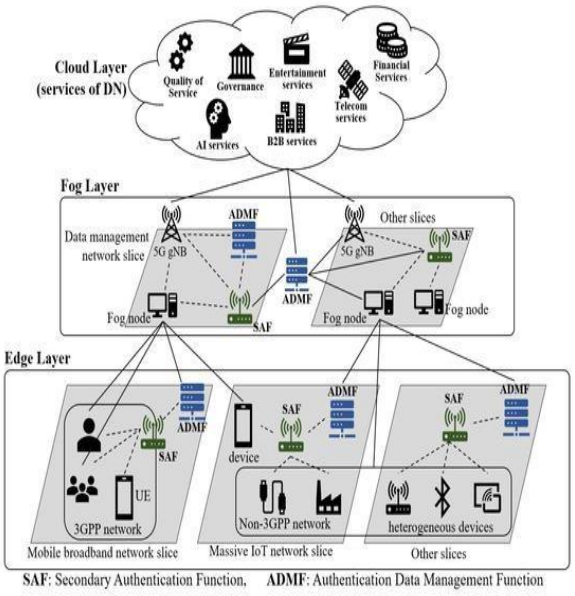

Fig.2 5G core Service-Based Architecture (SBA) [source: https://www.digi.com/blog/post/5g-network-architecture]

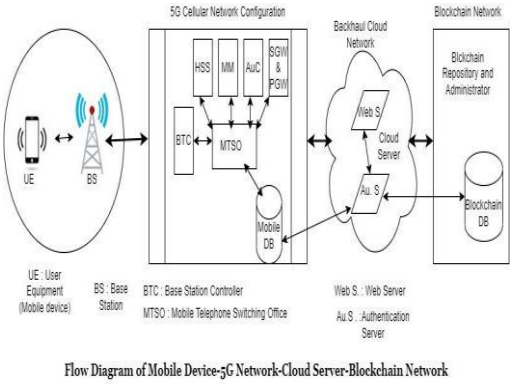

Fig. 3 Flow Diagram of Mobile Device Authentication using MobileNetwork and Cloud Server

Step 1: Mobile devices, also known as user equipment (UE), are required to be verified and registered with a cloud server in mobile cloud computing. This is done to prevent phishing attacks on user communication that takes place between a mobile device and a cloud server. We are aware that mobile devices have both an IMSI, which stands for "International Mobile Scriber Identity" (also known as a SIM card), and an IMEI, which stands for "International Mobile Equipment Identity" (also known as a MAC or physical address of mobile devices). Using today's cutting-edge technology, it is possible to clone or otherwise replicate an individual's one-of- a-kind

characteristics. An unauthorized person can attack cloud storage on behalf of the user who was originally authorized to do so by hacking the IMSI and IMEI codes. Every mobile user should be given a tamper-proof universal integrated circuit card (UICC), which is our recommendation for how these issues should be resolved. Cloud service providers might also take this step. The UICC[11] is functionally identical to a smart card, except that it allows for the implementation of one-of-a-kind kind of integrated circuits on its surface. Cloud providers alone decided on the architecture of this integrated circuit.

[11] Universal Integrated Closed Circuit

Step 2: In the traditional method of conducting an encryption procedure, the devices used for sending and receiving data exchange the symmetric key, also known as the public key. The kreyvium then encrypts the data based on the sender's public key and sends both the encrypted data and the public encryption key to the receiver. At the other end, the data is decrypted with the assistance of a public key that was sent by the sender along with the cipher data. This allows the recipient to access the data. The most significant drawback of this strategy is that, as a result of eavesdropping, the third party or hacker was able to break into the encryption key all at once during the transmission session. As a result, they were able to decrypt all of the data. As a result of this, to solve these issues, we will need to make use of the Diffie-Hellman key exchange protocol to exchange secret keys between two different entities while using mobile cloud computing. The information exchanged between the sender and the receiver is considered public, which means that it is vulnerable to being hacked by anyone. However, the information cannot be decrypted because encryption and decryption are both performed using secret keys that are calculated with the assistance of the Diffie-Hellman Key Exchange protocol. To facilitate the trade of the secret key between users, we will employ asymmetric encryption, often known as the idea of public and private keys. During the process of registering mobile devices through a cellular network's registration center (RC), the RC will create key VIdents and VIdents that will be shared with mobile devices and cloud servers and stored in the memory of those entities. Everyone involved in mobile cloud computing is familiar with VIdent on a worldwide level.

Step 3: To generate the private key of the mobile devices (UE) randomly, we are going to utilize the cryptographic Secure Hash Algorithm 256 (SHA-256), which generates hash values that are difficult to anticipate based on the input. The SHA-256 hashing algorithm is available for free to the general public, and many high-level programming languages come equipped with pre-built libraries that can be used to implement it. The application of SHA-256 ensures that the sequence of random numbers generated is both accurate and unpredictable about the values that were entered. Now, to use cloud services offered by a particular provider, an authentication application must first be installed on mobile devices. These applications are offered by the respective cloud service providers. The initial step for mobile users is to log in with the authentication application by providing a username and password that are both legitimate. IMSI, IMEI (in the case of laptops and iPods, the MAC address according to IEEE standardization), and Universal Integrated Closed Circuit (UICC) are issued by the cloud service provider only to its customers, and their identities are unique worldwide. They are like hardware chips embedded into mobile extensible hardware slots that, using a biometric module or fingerprint scanner existing in mobile devices, take valid user finger impressions. All of these parameters, including user, pwd, IMSI, IMEI, UICC, and fp#, are assumed to be entered as seed values into the hash function to generate the required value as a seed value of the user of the mobile device during that session alone to input into SHA-256. We are required to produce brand-new seed values at the beginning of every session. $DInfo_{MU}$ may be calculated as follows:

$DInfo_{MU}$ = hash (user || pwd || IMSI || IMEI || fp# || UICC).

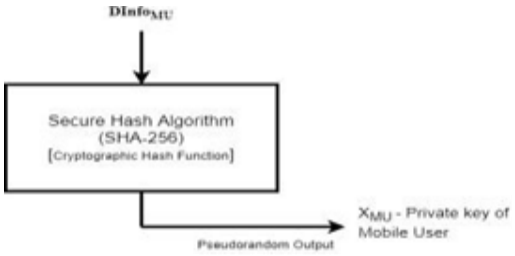

Fig. 4. Generation of Private key of Mobile User

Any pseudorandom number generator (PRNG) should have a seed value and a deterministic technique for producing a stream of pseudorandom functions (PRF) to produce the necessary private key for the user. These are the fundamental components. Secure Hash Algorithm-256 (SHA-256) and $DInfo_{MU}$ are the algorithms that we are making use of right now.

X_{MU} = SHA-256 ($DInfo_{MU}$)

Similarly, we can generate the private key for the Cloud Server (CS). Also, an authentication application is installed on a cloud server to take the username (userCS) and password (pwdCS) of a valid cloud server administrator, the MAC address of the cloud server (approved by IEEE registration authority and can be online cross-checked on IEEE supporting websites), the IP address of the cloud machine (IP) to get internet services that are factory programmed and act as a unique identity, and the port number (PORT) over which the application (web) server is running in the cloud server.

$DInfo_{CS}$ = hash (userCS || pwdCS || MAC || PORT || IP)

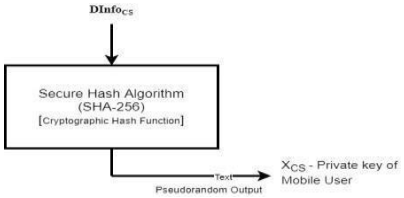

Fig. 5 Generation of Private Key of Cloud Server

X_{CS} = SHA-256($DInfo_{CS}$)

Both the values Y_{MU} and Y_{CS} are globally known to every entity in mobile cloud computing and are public keys of
mobile devices and cloud servers, respectively, and we will calculate them as follows:

Now consider a prime number 'q' and assume that 'α' such that it must be the primitive root of the q and α<q. Both the values 'α' and 'q are mutually decided by both end devices and are publicly known to all entities.

Hence, by using Diffie-Hellman key exchange formulas, we can derive the public keys of both mobile devices and cloud servers as follows:

1. $Y_{MU} = \alpha^{X}{}_{MU} \bmod q$……for Mobile DeviceAnd
2. $Y_{CS} = \alpha^{X}{}_{CS} \bmod q$……for Cloud Server.

Both the private keys X_{MU} and X_{CS} of mobile devices and cloud servers, respectively, are kept secret, and mobile devices and cloud servers share the public keys Y_{MU} and Y_{CS}. Then we have to calculate the secret key (SKM) when mobile devices are the senders of the packet using the Diffie-HellmanKey Exchange formula.

$SK_{MU} = (Y_{CS})^{XMU} \bmod q$ ….Secret key for packets on mobile devices during the sending of packets.

$SK_{CS} = (Y_{MU})^{XCS} \bmod q$ …. Secret key for packets at thecloud server during the sending of packets.

According to the Diffie-Hellman Key Exchange protocol or rules, the secret keys at both ends must be equal. This is a basic assumption in our proposed methodology. i.e.

SK_{MU} = SK_{CS} (using the Diffie-Hellman Formula)

Step 4: In this methodology, we will discuss the authentication of mobile devices to the MCC system using blockchain technology. The MCC system includes a database configured to store blockchain records for authenticating mobile devices to access a public wireless network. Each blockchain is associated with mobile devices. The blockchain mining processor can check a blockchain record from a mobile device that is stored in the flash memory of UICC, compare it with blockchain records stored in the database of CSP, and then grant access to the mobile device to the MCC system. A new block of new authenticating records can be appended to a blockchain to produce a new blockchain for authenticating the access of the mobile device to the public wireless network at a future time. The current blockchain records are stored on mobile devices and can be accessed for authentication purposes via wireless networks and cloud services. Generally, SIM unique numbers are used to authenticate mobile devices using a challenge-

response mechanism. These SIM keys are known to the mobile device and cellular network provider, and they are stored in HSS[12] for future use. Whenever a mobile device attaches to the wireless network, the mobility management system retrieves the SIM card key from HSS and sends it to the AuC[13] for validation and authentication. If the SIM key values of both

[12] Home Subscriber Server
[13] Authentication Cente

the mobile device and the cellular network database are the same, then authentication is successful. All these processing steps, timestamps, and location information are stored in one block whenever a mobile device wants to connect with the MCC system, and in the form of a chain, this block is appended at the end of the chain and stored in the mobile database. One blockchain is dedicated to only one mobile device so that we can retrieve transaction details for future reference. In other words, we can dictate this procedure as the Blockchain Mining Processor generates a method instruction for receiving a blockchain record from a mobile device and compares the blockchain record to a blockchain associated with the mobile device in a database. Again, this method grants access to the mobile device to our public 5G cellular network when the same blockchain records are similar to those related to the mobile device stored in the mobile network database. The blockchain mining processor also appends a new block to a current blockchain to produce a newblockchain associated with the same mobile device, and then this new blockchain is useful in authenticating mobile devicesto access service from a public 5G wireless network at a future time. With the help of SIM card-based information authentication, the SIM manufacturer and the cellular network provider or network carrier have access to the pre-shared key. Hence, the use of blockchain to authenticate mobile devices eliminates the vulnerability associated with shared keys. Afterall this updating of the blockchain's records done in previous steps, the new blockchain is stored in the mobile device's UICC flash memory as well as the Mobile Network Database. The instructions used in mobile devices for processing are in a non-transitory computer-readable format; transfer these instructions to 5G network. A mobile network mobility management procedure takes the form of radio or wireless signals communication. Hence, proper encoding and decodingof signals must be done as part of the physical layer of the network protocol at both ends. So that both ends update their blockchain records for further authentication purposes in the future. The mobile devices we are using in MCC to get cloud services are smart electronic communication devices that have a cellular transceiver antenna for communicating with 5G or any other wireless network like Wi-Fi, WI-MAX, or any other wireless local area network. 5G cellular networks have multiple BS, and all of these BS are connected and controlled by the cellular network's controller, which enables carrying many signal types, such as real-time circuits switched to IP-based packet-waving traffic and analog voice signals.

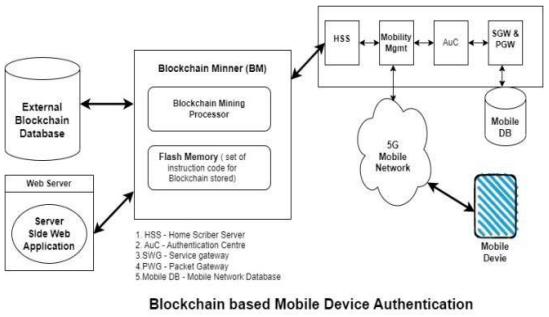

Fig. 6. Blockchain-based Mobile Device Authentication

The Blockchain Miner (BM) communicates with the Mobility Management of the 5G mobile network through HSS. The main role of BM is to handle controlling blockchain processing and storing blockchain records in the External Blockchain Database (EBD). The main purpose of the BM is to authenticate mobile devices whenever a request is coming from the mobile user using blockchain records stored in EBD[14] and comparing them with blockchain records coming from the mobile device into the AuC of the mobile network, and after successful comparison of the blockchain records, grant access to the services provided by the cloud server and internet or radio wireless services by the 5G cellular network. All the credentials of mobile devices and cloud servers

are stored in the Mobile DB as hashes and blocks during the authentication process. With the help of the authentication application, mobile users entered login credentials (username and password), and with the help of SHA-256, all these username, password, IMSI, IMEI, fingerprint impression, and UICC values are inputted into SHA-256 and sent to the MM[15] of the cellular network.

Algorithmic Steps to Authenticate the Mobile User's Device

1. The User Equipment (UE) comprises an in-built processor, a non-transitory computer-readable storage medium for storing programming instructions code for execution by the processor, various input sensors to take fingerprints or any biometric impression, extra hardware embedded slots to insert UICC provided by the CSP, and various mobile app software, including authentication applications developed and provided by the CSP to its verified cloud users, etc. We know that every mobile device on a cellular network has a unique IMSI and IMEI code globally.

2. 5G [2] Mobile networks typically include various security features to prevent unauthorized third parties from accessing or manipulating data. Like an LTE[16] [3] or 4G mobile network, a 5G network also has the security features of authentication, non-access stratum (NAS) security, and access stratum (AS) security. The authentication feature ensures that a user is an authorized subscriber to the MCC, which enables mobile networks to get cloud service, and during access to the mobile network service, NAS and AS security ensure the control of user data communication in an insecure way. First, UE must be verified by the mobile network. Hence, mobile users send IMSI and IMEI codes to the BTC[17] via BS in encrypted form using the public key provided by their home mobile network. Suppose that the public key of UE is VIdent.

$IMSI^* = Enc_{VIdent}(IMSI) IMEI^* = Enc_{VIdent}(IMEI)$

These two values, IMSI* and IMEI*, are transferred to the MTSO[18] via BTS, and the MTSO transfers them to Mobility

[14] External Blockchain Database
[15] Mobility Management [16] Long Term Evaluation [17] Base Station Controller
[18] Mobile Telecommunication Switching Office

Management, where AuC performs validation and verification of UE based on IMSI* and IMEI* by comparing them with values stored in the Mobile Database, where all authorized user identities are stored. If the comparison is successful, then UE [5] is authorized to get service. Here, the first step of UE authentication is successful.

1. In the previous section, we drew the secret key for the mobile device SK_{MU}, and with the help of this secret key, we encrypted the IMSI, IMEI, user name and password, and UICC value using the secret key of UE is SK_{MU}.
2. First of all, whenever users try to get cloud server service, they have to log in to the authentication application provided by the CSP [1]. The mobile user enters login credentials (username and password), and by processing instructions, they get encrypted as follows:

$userName = Enc_{SKMU}(username)$ $pwd = Enc_{SKMU}(password)$

3. The rest of the value of UE means IMSI, IMEI, and UICCcodes are also encrypted as follows:

$IMSI^{\#} = Enc_{SKMU}(IMSI)$ $IMEI^{\#} = Enc_{SKMU}(IMEI)$ $UICC^{\#} = Enc_{SKMU}(UICC)$

All these values, including userName, pwd, $IMSI^{\#,}$ IMEI#, and UICC#, are transferred to the cloud server of the MCC.

1. In the previous section, we drew the secret key for the mobile device SK_{MU}, and with the help of this secret key, we encrypted the IMSI, IMEI, user name and password, and UICC value using the secret key of UE SK_{MU}.
2. First of all, whenever users try to get cloud server service, they have to log in to the authentication application provided by the CSP. Mobile The user enters login credentials (username and password), and by processing instructions, they get encrypted as follows:

$userName = Enc_{SKMU}(username)$ pwd = EncSKMU (password)

3. The rest of the value of UE means IMSI, IMEI, and UICCcodes are also encrypted as follows:

$IMSI^{\#} = Enc_{SKMU}(IMSI)$ $IMEI^{\#} = Enc_{SKMU}(IMEI)$ $UICC^{\#} = Enc_{SKMU}(UICC)$

All these values, including userName, pwd, $IMSI^{\#,}$ IMEI#, and UICC#, are transferred to the cloud server of the mobile devices via wireless network and explanation are in followingsteps

1. CSP via the 5G wireless communication network, and the UE, 5G network, and cloud server logical connections are synchronized to each other and mapped to the web component of the cloud server. All those encrypted values sent by the UE are fetched by the web component of the cloud server.
2. We know that the secret key of the mobile device for encryption and decryption is SK_{MU} and the secret key of the cloud server for encryption and decryption is SKCS, both of which are equal according to the Diffie-Hellman key exchange formula. We already proved this terminology in the previous section of the paper. In short, we can say that without sharing cryptography keys, UE and Cloud Server both know their key values, which mean both keys are equal,
and there is no need to transfer or exchange keys over any public communication network. So there is no possibility of hacking these keys by a third party. We follow the extra- layered authentication mechanism for UE provided by CSP.
3. All the received values (username, password, $IMSI^{\#,}$ $IMEI^{\#,}$ and UICC#) are decrypted by the web component ofthe cloud server using its secret key SK_{CS}.
Username = $Decrpt_{SKCS}$(username) Password = $Decrpt_{SKCS}$(pwd) IMSI = $Decrpt_{SKCS}(IMSI^{\#})$ IMEI = DecrptSKCS ($IMEI^{\#}$) UICC = $Decrpt_{SKCS}(UICCI^{\#})$
4. Then the authentication application (or set of instructions and programs installed in flash memory or permanent memory of the cloud server) takes the username and passwordand UICC values as input and validates and verifies their values by comparing them with values retrieved from the blockchain database. If values are equal, then one step of authentication is successful; otherwise, the UE request to join CSP and get the cloud service is rejected.
5. Then the blockchain miner gives some unique and challenging mathematical problems that would take a considerable amount of computational power to solve on the UE (or any other mobile device looking for cloud services). This mathematical problem is sent to the UE with the help of the web component of the web server.
6. If UE successfully solves this mathematical puzzle and its solution is sent to the blockchain miner with the help of the web server and authentication server, after cross-checking UE's solution, BM starts the procedure to add a new node to the blockchain network.
7. Then the authentication server or application applies the SHA256 hashing algorithm to the combination of username, password, IMEI, IMSI, and UICC values and generates the hashed values
8. In the BM flash memory, some blockchain solidity code starts execution, and based on the combined hash value, one block is generated with all details like the timestamp, its origin node, and the history of the transaction and stored in the External Blockchain Database for future reference.
9. This block is also transferred to UE, and UE stores these block-hashed values in the UICC permanent memory with proper encryption and the secret key of the UE.
10. The blockchain miner is implemented as a standalone server along with a cloud server, and the cloud server works as middleware, or sometimes BM, having connections with other network servers worldwide.
11. The BM has an initial block, or genesis block, in the blockchain repository database for future UE purposes.

Whenever new UE or next time same UE starts logging in to the cloud server, the same above 11 steps are repeated, and the next block is generated and appended to the end of the initial blockchain. In the same way, chains of blocks are generated, and every user of the blockchain will be notified
about the UE login and getting the service from the cloud server in a fully transparent way.

In our proposed theory, UE authentication blocks are never deleted and constitute permanent records of all authentication requests and services provided to the UE or mobile device's user. The authentication application installed in the UE mobile terminal can access all cloud services and interact with cloud servers to send and receive data or information. With the help of our proposed theory, UE performed multi-factor authentication with the help of advanced blockchain technology, and all its transaction details, along with all its authentication records, were permanently stored in a blockchain database for future logging purposes.

Next time, if UE sends the block that stores the

initial steps ofauthentication in the mobile device's UICC by encrypting it with the secret key SK_{MU}, the web server decrypts these encrypted block values using the cloud server's secret key SK_{CS}. And compare it with the block stored in the Extended Blockchain database; if the comparison is successful, UE is authenticated, and the next blockchain is created based on the new kind of service request and timestamp.

Conclusion And Future ResearchTrends

In the proposed thesis paper, we put forward a mobile device authentication system with different multi-factor authentication (MFA) methods to get services from mobile cloud computing. We try to do studies on MCC information storage and communication security. The first task should be to ensure that we have allowed authenticated users in our system to get service. Before that, we will have to validate and verify the UE.The components of MFA used in our system are authentication application software for mobile devices, UICC values that are provided by the CSP, IMEI and IMSI codes provided by the cellular network provider with unique values worldwide, and fingerprint factors that are unique and cannot be duplicated anyway. In our UE authentication theory, we are using the hardware configuration of mobile devices, the 5G mobile (cellular) network's various components, the cloud server, which consists of two sub-server authentication application servers and a web application server, and the blockchain network and its various storage resources. Due to security concerns, we generate the security key by using the Diffie- Hellman key exchange formula for encryption and decryption of values of various factors used in the authentication of mobile devices over the MCC system and blockchain network system. As mentioned earlier in our previous section of the research paper, due to the uniqueness of fingerprints in identifying the UE's user, fingerprint authentication can be used correctly to authenticate the user, as these methods are unique and affordable to implement. The CSP provider has to provide a dedicated server for information exchange and cryptography, the web server (WS), and for authentication of mobile user identities, the authentication server (AS), which will ease transaction validation and reduce possible hacking threats. Due to the use of blockchain network technology, authentication, storage, and information retention are transparent to allstakeholders in the MCC system.

This subsection highlights the future research trends and challenges in MFA using blockchain technology based on literature reviews we have done previously. It is noted that there are various research gaps in the integration of multi-factor authentication analysis into blockchain-based applications. There is a lack of research into the application of how blockchain integration can lead to multifactor authentication in the 5G mobile network technologies or its forthcoming 6G mobile network. Therefore, one of the main future research trends in MFA is to deliver good strategies to reduce time efficiency issues and increase the effectiveness and trust of mobile network and cloud network users. Whenever we integrate our MFA theory with a blockchain-based network, it requires more complex and immense computational power and resources, which leads to future research challenges to improve the blockchain-based system's computations and complexity issues for integration with an MFA-based secure authentication system.

References

[1] Arnab Mukherjee, Mamatha Balachandra, Chetana Pujari c, Soham Tiwari, Abhay Nayar, Srinivasa Rao Payyavula, "Unified smart home resource access along with authentication using Blockchain technology", International Conference On Advances In Information, Computing, And Trends In Data Engineering (ICAICDE-2020,https://doi.org/10.1016/j.gltp.2021.01.005

[2] Asim, J.; Khan, A.S.; Saqib, R.M.; Abdullah, J.; Ahmad, Z.; Honey, S.; Afzal, S.; Alqahtani, M.S.; Abbas, M. Blockchain-based Multifactor Authentication for Future 6G Cellular Networks: A Systematic Review. Appl. Sci. 2022, 12, 3551. https:// doi.org/10.3390/app12073551

[3] Chang, Z.; Wang, L.; Li, B.; Liu, W. MetaEar: Imperceptible Acoustic Side Channel

Continuous Authentication Based on ERTF. Electronics 2022, 11, 3401. https:// doi.org/10.3390/electronics11203401

[4] Chen Wang, Yan Wang, Yingying Chen, Hongbo Liu, Jian Liu," User Authentication on Mobile Devices: Approaches, Threats and Trends ",2020 published by Elsevier,https://www.elsevier.com/open-access/userlicense/1.0/, and Version of Record: https://www.sciencedirect.com/science/article/pii/S1389128618312799

[5] Chow, M.C.; Ma, M. A Secure Blockchain-Based Authentication and Key Agreement Scheme for 3GPP 5G Networks. Sensors 2022, 22, 4525. https:// doi.org/10.3390/s22124525

[6] Cong Shi, Jian Liu, Hongbo Liu, and Yingying Chen. 2017. Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-enabled IoT. In Proceedings of Mobihoc '17, Chennai, India, July 2017, 10 pages. DOI: 10.1145/3084041.3084061

[7] Dee, T.; Richardson, I.; Tyagi, A. Continuous Nonintrusive Mobile Device Soft Keyboard Biometric Authentication. Cryptography 2022, 6, 14. https://doi.org/10.3390/ cryptography6020014

[8] Deebak, B.D.; Hwang, S.O. Federated Learning-Based Lightweight Two-Factor Authentication Framework with Privacy Preservation for Mobile Sink in the Social IoMT. Electronics 2023, 12, 1250. https://doi.org/10.3390/ electronics12051250

[9] de-Marcos, L.; Martínez-Herráiz, J.-J.; Junquera-Sánchez, J.; Cilleruelo, C.; Pages-Arévalo, C. Comparing Machine Learning Classifiers for Continuous Authentication on Mobile Devices by Keystroke Dynamics. Electronics 2021, 10, 1622. https://doi.org/10.3390/ electronics10141622

[10] Dianqi Han, Student Member, IEEE, Ang Li, Tao Li, Lili Zhang, Yan Zhang, Jiawei Li, Student Member, IEEE, Rui Zhang, Member, IEEE, Yanchao Zhang, Fellow, IEEE, "(In)secure Acoustic Mobile Authentication", DOI 10.1109/TMC.2021.3053282, IEEE Transactions on Mobile Computing

[11] HAMZA ALI , SHAHEER KHALID , SADIQ IQBAL , JEHAD

[12] M.HAMAMREH," Protecting IMSI from Fake Base Stations Exploitation and Spoofers Impersonation in 5G and Beyond Cellular Networks",Digital Object Identifier 10.46470/03d8ffbd.4f956b48, RS Open Journal on Innovative Coomunication Technologies, Volume 3 , 2022

[13] Jamil Asim, Adnan Shahid Khan, Rashid Md. Saqib et.al, "Blockchain-based Multifactor Authentication for Future 6G Cellular Networks: A Systematic Review", Appl. Sci. 2022,12, 3551, https://doi.org/10.3390/appl2073551 for the Internet of Drones. Drones 2022, 6, 264. https://doi.org/ 10.3390/drones6100264

[14] Jithu G. P., Ahmad Salehi S., Carsten Rudolph, "Athentication and Access Control in 5G Device-to-Device Communication "

[15] Kim, S.; Mun, H.-J.; Hong, S. Multi-Factor Authentication with Randomly Selected Authentication Methods with DID on a Random Terminal. Appl. Sci. 2022, 12, 2301. https://doi.org/10.3390/ app12052301

[16] Li, Y.; Yun, X.; Fang, L.; Ge, C. An Efficient Login Authentication System against Multiple Attacks in Mobile Devices. Symmetry 2021, 13, 125. https://doi.org/doi:10.3390/ sym13010125

[17] Mostafa Yavari, Masoumeh Safkhani, Saru Kumari, Sachin Kumar, and Chien- Ming Chen, "An Improved Blockchain-Based Authentication Protocol for IoT Network Management ", Hindawi, Security, and Communication Networks, Volume 2020, Article ID 8836214, 16 pages,https://doi.org/10.1155/2020/8836214

[18] Nerini, M.; Favarelli, E.; Chiani, M. Augmented PIN Authentication through Behavioral Biometrics. Sensors 2022, 22, 4857. https://doi.org/10.3390/s22134857

[19] Rajasekaran, A.S.; Maria, A.; Rajagopal, M.; Lorincz, J. Blockchain Enabled Anonymous Privacy-Preserving Authentication Scheme for Internet of Health Things. Sensors 2023, 23, 240. https:// doi.org/10.3390/s23010240

[20] Rana, M.; Mahmood, K.; Saleem, M.A.; Al-Turjman, F.; Kolhar, M.S.; Altrjman, C. Towards a Provably Secure Authentication Protocol for Fog-Driven IoT-Based Systems.

Appl. Sci. 2023, 13, 1424. https://doi.org/10.3390/ app13031424

[21] Reichinger, D.; Sonnleitner, E.; Kurz, M. Continuous Mobile User Authentication Using Combined Biometric Traits. Appl. Sci. 2021, 11, 11756. https://doi.org/ 10.3390/app112411756

[22] Saurabh Dey, Srinivas Sampalli and Qiang Ye, "MDA: message digest-based authentication for mobile cloud computing", Journal of Cloud Computing: Advances, Systems and Applications (2016) 5:18 DOI 10.1186/s13677-016-0068-6

[23] Seonghyeon Gong, Abir EL Azzaoui and Jeonghun Cha and Jong Hyuk Park, "Secure Secondary Authentication Framework for Efficient Mutual Authentication on a 5G Data Network", Appl. Sci. 2020, 10, 727; doi:10.3390/app10020727, www.mdpi.com/journal/applsci

[24] SungJin Yu, JoonYoung Lee, Yohan Park, YoungHo Park, SangWoo Lee, and Bo Heung Chung," A Secure and Efficient Three-Factor AuthenticationProtocol in Global Mobility Networks", Appl. Sci. 2020, 10, 3565; doi:10.3390/app1010

[25] Umoren, O.; Singh, R.; Awan, S.; Pervez, Z.; Dahal, K. Blockchain-Based Secure Authentication with Improved Performance for Fog Computing. Sensors 2022, 22, 8969. https:// doi.org/10.3390/s22228969

[26] Yavari M, Saf Khan M, K Saru, K Sachin, C Chien-Ming Chen, "An improved Blockchain-based Authentication Protocol for IoT Network management", Hindawai, Security Communication Network, Vol 2020, Article Id 8836214, https://doi.org/10.1155/2020/8836214

[27] Zukarnain, Z.A.; Muneer, A.; Ab Aziz, M.K. Authentication Securing Methods for Mobile Identity: Issues, Solutions, and Challenges. Symmetry 2022, 14, 821. https://doi.org/10.3390/sym14040821