symmetry

MDPI

Review

Authentication Securing Methods for Mobile Identity: Issues, Solutions and Challenges

Zuriati Ahmad Zukarnain [1,*], Amgad Muneer [2,3,*] and Mohd Khairulanuar Ab Aziz [1]

[1] Department of Communication Technology and Network, Faculty of Computer Science and Information Technology, University Putra Malaysia, Seri Kembangan 43400, Malaysia; gs61317@student.upm.edu.my
[2] Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Seri Iskandar 32160, Malaysia
[3] Centre for Research in Data Science (CERDAS), Universiti Teknologi PETRONAS, Seri Iskandar 32610, Malaysia
* Correspondence: zuriati@upm.edu.my (Z.A.Z.); muneeramgad@gmail.com (A.M.)

Abstract: Smartphone devices have become an essential part of our daily activities for performing various essential applications containing very confidential information. For this reason, the security of the device and the transactions is required to ensure that the transactions are performed legally. Most regular mobile users' authentication methods used are passwords and short messages. However, numerous security vulnerabilities are inherent in various authentication schemes. Fingerprint identification and face recognition technology sparked a massive wave of adoption a few years back. The international mobile equipment identity (IMEI) and identity-based public key cryptography (ID-based PKC) have also become widely used options. More complex methods have been introduced, such as the management flow that combines transaction key creation, encryption, and decryption in processing users' personal information and biometric features. There is also a combination of multiple user-based authentications, such as user's trip routes initialization with the coordinates of home and office to set template trajectories and stay points for authentication. Therefore, this research aimed to identify the issues with the available authentication methods and the best authentication solution while overcoming the challenges.

Keywords: mobile; mobile identity; authentication; mobile authentication; mobile security; authentication method; mobile payment

Citation: 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

Academic Editor: Alexander Shelupanov

Received: 13 March 2022
Accepted: 6 April 2022
Published: 14 April 2022

1. Introduction

An identity card (IC) is used for compulsory registration and identification for each citizen to be identified in such a way that they can claim citizenship. Without identification, one cannot carry out citizenship-related tasks or enjoy citizenship advantages [1]. In recent years, many organizations have introduced online transactions on a mobile platform. Smart parking meters, smart traffic management, smart public transit, healthcare, precision agriculture, building management, public monitoring, and smart petrol stations are some of the mobile phone applications that have improved business efficiency and user satisfaction [2]. In addition to the COVID pandemic, the global online commerce volume has expanded dramatically [3]. This is where the mobile identity is required; to authenticate and log in, users need reliable digital identities [4].

Mobile identity is often tied to the subscriber identity module (SIM) card, where it can represent the owner and be used for authenticating the SIM card, thus representing, and authenticating the owner virtually. Simply put, mobile identity utilizes a user's identity attributes tied to a mobile device for identity verification, authentication, and authorization [5]. However, mobile threats are continuously being updated with new features, shifted into new distribution channels and supported by investments in the development of detection avoidance techniques [6]. We believe that it is crucial to perform

a study on finding the best method of guarding the confidentiality of transactions, integrity of the information, and the availability of the services for mobile identity.

Additionally, because information security solutions impose more safety standards on identity authentication, professionals consider increased security during the design process of identity authentication, oblivious to the operation's simplicity [7]. With the fast growth of network edge devices, current cloud computing frameworks find it increasingly challenging to meet network bandwidth and real-time needs as they transmit large amounts of data to cloud data centers [8]. While the technological prerequisites for secure mobile payment have been satisfied, there are no standards or standardized regulations that exist. User authentication flow management is still in its infancy in mobile payment [9]. These are among the challenges we need to look at for establishing a trusted and solid mobile identity. This is a more critical issue than addressing accessibility alone, and security is a primary concern. The SIM card, which is encrypted and integrated into each mobile device, is undoubtedly the most secure method of storing identifying information [10].

Based on our survey of telecommunication companies, mobile authentication involves many parties that can be grouped into three entities: the operator, the aggregator, and the merchant. The operator is the mobile network service provider, the aggregator is the entity that connects between operators and merchants, and the merchant is the mobile application provider. All parties have their own secure authentication method. Making it more complex will enhance security but will delay the transaction speed. Moreover, if authentication is breached within one of the parties, it is hard to trace the source due to the involvement of different organizations. Additionally, synchronizing the mobile authentication method into one single platform will ease authentication security and threat management. Thus, the contributions of this study are threefold, summarized as follows.

- First, we have conducted a comprehensive review of the existing common mobile identity authentication issues based on recent research papers.
- Second, this study highlights the vulnerabilities of 4G and 5G authentication and the necessity for it to evolve consistently.
- Based on the extensive literature review conducted, we have proposed a solution on having a fourth entity as an authentication provider, known as mobile identity, that we think is the best approach to balance the requirement of security and the convenience of transactions.

The next section will discuss the common mobile authentication types found in the referred research papers and identify the issues. In Section 3, we will evaluate the proposed solution in terms of flows and functions and how it works. Some of the challenges will be addressed in Section 4, before we summarize this study in Section 5.

2. Mobile Authentication Method and Issues

Many research studies have produced solutions to address mobile online authentication issues, such as a mobile authentication system based on the Blowfish encryption algorithm [7], handover authentication protocols using ID-based PKC [8], a trajectory-based identity authentication method [9], the integration of cryptographic methods for anonymous biometric authentication [11], authentication using a public behavior dataset (i.e., keystrokes on touch screens) with different feature selections to improve the authentication accuracy [12], and using cipher policy attribute-based encryption bonded with the geographical location [13]. However, few have narrowed the issues down to the mobile identity authentication service, for example, the national electronic identities (eID) [4] and decentralized and self-sovereign identity (SSI) solutions [14]. This section will address the issues of standard authentication commonly used for mobile transactions.

2.1. Static Password Authentication

The static password is the earliest and most widely used means of authentication [2]. The system sets up two tuples of information for each legitimate user during registration: a commonly named username and password. User information provided during the

registration will be tied to the username. Each login will require the user to self-introduce by entering the username and authenticating it using a secret password. Figure 1 represents the idea of how registration is performed.

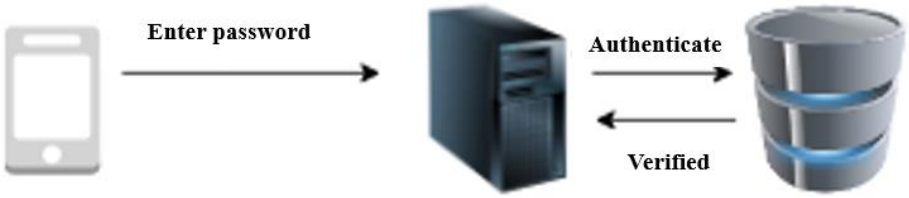

Figure 1. Static password authentication.

This type of authentication purely depends on the user to memorize. Commonly, users will select a word that they can easily remember, potentially exposed to attack. Cybercriminals have created many tools that can help in guessing passwords. On the other hand, a complex password may be forgotten, and the user will have to reset that. This will take away the convenience of the authentication.

Static passwords are easy to forget, lose, or leak [11]. They are simple to crack using tactics such as guessing, dictionary attacks, brute force cracking, theft, replay assaults, Trojan horse attacks, and other methods [7]. They are also too risky to use independently, especially for the purpose of mobile identity authentication.

2.2. Dynamic Password Authentication

The SMS verification code is one of the most commons dynamic password authentications. Like the static password, the system will require identification information from the user, paired with the server's generated PIN or token for access authentication [7].

Additionally, users need to register themselves and provide a username and mobile phone number as a primary key tied to their information, as shown in Figure 2. During the login, the user will need to enter the username, and once the server validates that their profile exists, an SMS of the generated password will be sent to the correlated mobile number. The mobile phone user will then use the generated password for authenticating their access. SMS authentication codes are sent in plain text. This presents some vulnerability that is constantly exposed to high-risk threats.

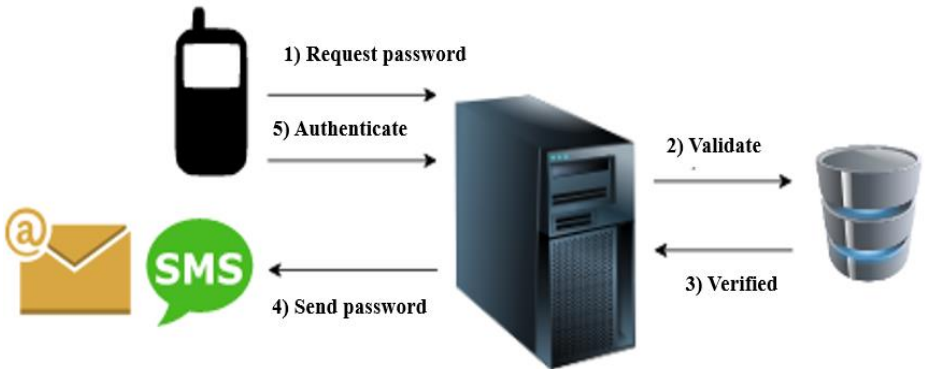

Figure 2. Dynamic password authentication.

2.3. Biometric Authentication

Each individual has unique biological traits, and because biometrics cannot be easily falsified over an extended period of time, they can be utilized as a trustworthy method of identity authentication [15]. The emergence of biometric modalities also sparked a realization that this issue warrants further exploration and discussion. However, there is no clear baseline concerning the criteria and specifications required for security testing, specifically for biometric products, systems, etc. that the national government uses in

adopting biometric technologies [14]. Therefore, some biometric authentication technologies have been accompanied by an optimization algorithm. Authors in [16] proposed a multimodal system based on an evolutionary algorithm for the security of the biometric system. However, some of the recent optimization algorithms can be adopted to overcome the challenge of the evolutionary algorithm used for the security of the biometric system, such as the algorithms suggested by [17] and [18].

Each legitimate user will capture their biometric information for this type of authentication. This is easier nowadays, because most smartphones are equipped with a built-in camera to capture face or iris, a voice recorder to capture voice, and a fingerprint reader to capture thumbprints. The biometric information will be preprocessed and bound with user information during registration. Each login will require the user to present their biometrics for authentication.

The risks of using biometrics are quite huge. Once breached, they are not available for recovery. The data are not renewable and hence, cannot be used once stolen. Some disadvantages of using biometric authentication are the high computational cost, required accuracy and usability during the unlocked state, plus hardware sensor devices that are not practical for frequent logins/authentications [12]. Another issue with biometric authentication is that it might slightly change over time. Table 1 lists the impact of having biometric changes [14].

Table 1. Impact of change on biometrics [14].

Usability	**Culture**		**Performance**
	Condition	**Impact**	
FINGERPRINT RECOGNITION			
Most comfortable and fastest	Sweating/Dry skin	Low	High
	Change of fingerprint structure	High	Low
FACIAL RECOGNITION			
Unpredictability of facial appearance (e.g.,: facial expressions)	Wearing Hijab	Medium	Medium
	Make up	Medium	Medium
	Wearing glasses	Low	High
IRIS/EYE RECOGNITION			
Cause of discomfort (e.g.,: proximity close to camera)	Wearing contact lenses	Low	High
	Eye blinks	Medium	Medium
Impact Low—affecting or altering the environment as little as possible Medium—affecting or changing the environment as much as possible High—unalterable			

2.4. Trip Trajectory Authentication

Different mobile phone users will have different personal trip trajectories and stay points. This type of authentication determines the validity of the present mobile device user based on his trajectory data [9]. The travel trajectory's system architecture is depicted in Figure 3, which includes the registration and authentication phases.

In the registration phase, a user registers his information, comprising his home and workplace coordinates and trip routes, in the template library, which is dynamically expanded to accommodate the user's trip regularities. While in the authentication phase, the data gathering module collects the user's daily travel trajectories using GPS-enabled mobile devices, calculating the similarity between the sample and template trajectories in order to determine likely stay point coordinates. The results of this calculation will be used to judge whether the user is valid or not.

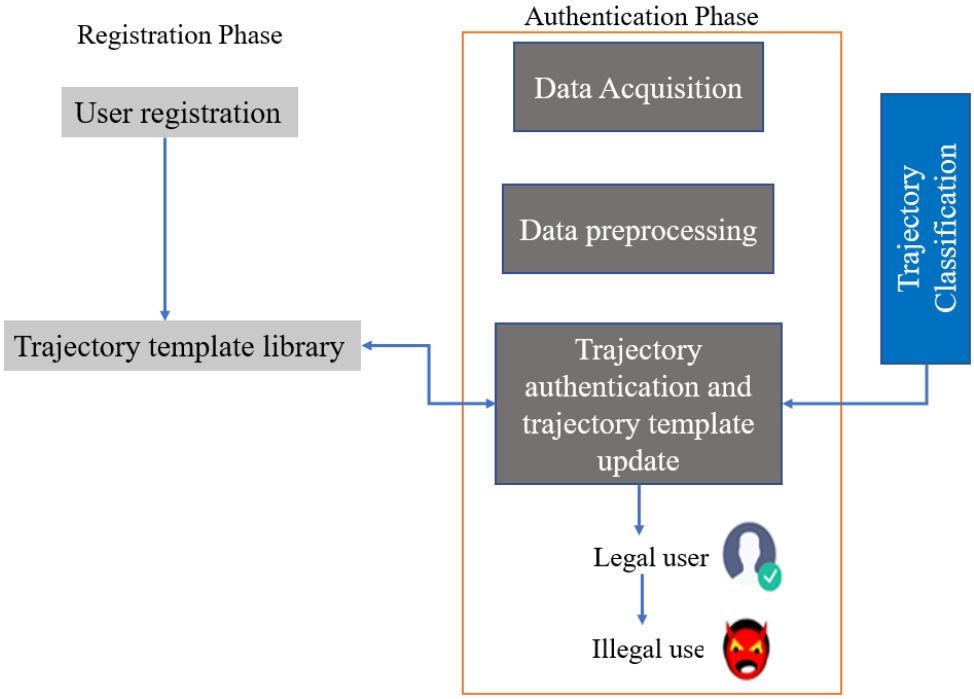

Figure 3. Architecture of system for trip trajectory authentication.

Additionally, using this type of authentication makes it hard to validate users who love to travel a lot. The frequent changes in user coordination and stay points will make it hard to authenticate.

2.5. Cryptography Authentication

Cryptography can be utilized to secure data during transmission, storage, and computation. Cryptography is a technique that utilizes a key and algorithm to convert plain text (readable text) to ciphertext (unreadable text) [13]. There are two types of cryptography used: symmetric and asymmetric. The same key is utilized in symmetric key cryptography to encrypt and decrypt. It consists of five elements: plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm. However, the asymmetric key cryptography uses different keys for encryption and decryption, referred as a public and private keys and known as public key infrastructure (PKI).

2.5.1. ID-Based PKC (Public Key Cryptography)

Traditional public-key cryptography (TPKC) was introduced based on PKI. Several protocols using the TPKC have been proposed, where each user will have a certificate to bind their identity and public key. Those certificates are produced by a trusted third party called the certificate authority (CA) [8]. However, the system has an overhead to be borne when the number of users increases.

To overcome the weaknesses in these TPKC protocols, identity-based public-key cryptography (ID-based PKC) has been proposed in the last several years. The participant's identity itself is taken as the public key so that no certificate is needed to bind its identity and public key [8]. Figure 4 shows the flow of ID-based PKC authentication.

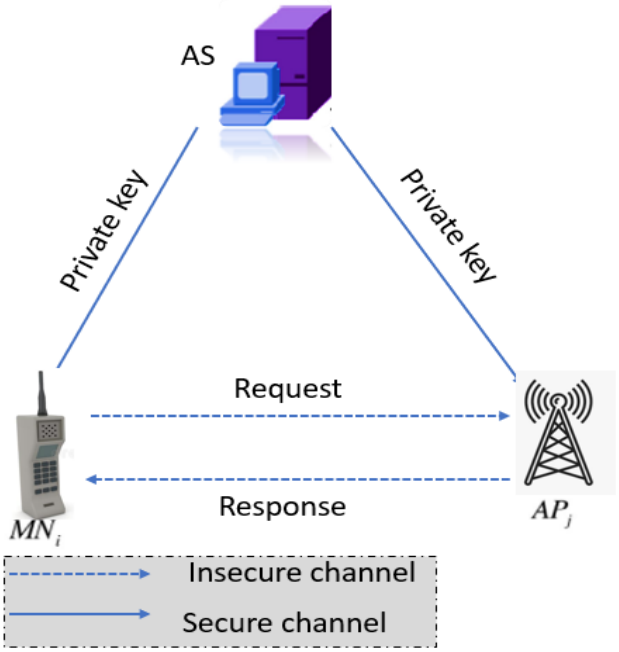

Figure 4. ID-based PKC authentication.

2.5.2. Geo-Encryption

Geo-encryption is an encryption method that uses the user's geographical location as the user's identity itself. It enables data encryption for a specific place that may be identified spatially and temporally. Without the position information received using an anti-spoof GPS device, it is impossible to decode the data with the particular availability spoofing module (SAASM). The GPS signal includes encrypted binary Y codes. SAASM receivers can track Y codes only when loaded with the correct decryption key [13]. This type of encryption is useful when there is a requirement for disabling decryption outside a specified geo-location.

2.6. Multi-Factor Authentication (MFA)

Instead of using a single authentication method, multi-factor authentication combines another layer of authentication. For example, using a static password with a dynamic password is tied. Users will be required to enter the password, send entering the password, and send the request to an authentication server. Once the password is verified, the authentication server will send a random generated PIN/password to the user's registered mobile number through SMS or to the user's registered email address. The user then needs to enter the generated password to complete the authentication. However, users will need to authenticate themselves twice or more using this MFA method [11].

For improvement, other combination methods are proposed for MFA, which reduce the authentication attempt by the user. For example, using bio-encryption combines the benefits of traditional cryptography with the security provided by biometrics [8]. Although this method is much more secure than the static–dynamic password combination, it requires higher-end devices. Table 2 shows some of the mobile authentication method and issues.

Table 2. Authentication comparison.

Authentication	Method	Issues	Risk Level	Study
Static password	User enters the username and authenticates using a secret password.	— Depends on user to memorize, is easy to forget, lose, or leak. — Exposed to guessing, dictionary attack, brute force cracking, stealing, replay attacks, Trojan horse attacks and others.	High	[2,7,11]
Dynamic password	Register username and mobile phone number as a primary key. The user's identification information is paired with the server's generated PIN or token.	— Code is sent in plain text. — Vulnerability is constantly exposed to high-risk threats.	High	[7]
Biometric	User captures their biometric information, then preprocess and bind it with user information. Each login will require the user to present their biometric data.	— Once breached, it is not available for recovery. The data are not renewable. — Requires high computational cost, accuracy, and usability during the unlocked state, plus hardware sensor devices that are not practical for frequent logins/authentications. — Biometrics slightly change over time.	Low	[12,14,15]
Trajectory	User registers coordinates of home and office and the trip routes as the initial template, dynamically extended trip regularities. Data acquisition uses mobile GPS to collect the daily trip trajectories, calculate the similarity between the sample and the template trajectories.	— Frequent changes in user coordinates and stay points for users that travel a lot. — Authentication failed due to frequent change of trajectory location for user that frequently travels.	Medium	[9]
Public Key Cryptography	Plain text (readable text) is converted to ciphertext (unreadable text) with the help of the key and algorithm. The user will have a certificate to bind their identity and public key.	— The system has an overhead to be borne when the number of users increases. — Cost increases and increasingly complex maintenance.	Low	[8]
ID-Based Public Key Cryptography	The participant's identity is taken as the public key to bind its identity and public key.	— The system has an overhead to be borne when the number of users increases. — Cost increases and increasingly complex maintenance.	Low	[8]
Geo-Encryption	User's geographical location as the identity of the user. Data to be encrypted for a specific location obtained using an anti-spoof GPS receiver that can be identified in terms of space and time.	Only applicable when there is a requirement for disabling decryption outside specified geo-location.	Low	[13]
Multi-factor	Combines authentication method used with another layer of authentication.	Users will need to authenticate themselves twice or more using this method.	Low	[11]

2.7. Securing Authentication for Mobile Networks

Authentication and key management are critical components of cellular network security because they establish mutual authentication between users and the network

and generate cryptographic keys for the protection of both signaling and user plane data. Each generation of cellular networks has specified at least one type of authentication [19]. For instance, the fourth-generation mobile network (4G) specified 4G EPS-AKA, but the fifth-generation mobile network (5G) specifies three authentication methods: 5G-AKA, EAP-AKA [20], and EAP-TLS (transport layer security) [20].

Because 5G defines additional authentication techniques, wireless practitioners frequently inquire about the rationale for 5G's adoption of these new authentication methods and how they differ from 4G authentication [21]. The purpose of this section is to address those problems by performing a comparative analysis of 4G and 5G mobile authentication methods [22]. The analysis demonstrates that 5G authentication outperforms 4G authentication in several ways [23], including the use of a unified authentication framework that can support a more significant number of user cases, enhanced user equipment identity protection, enhanced home-network control, and increased key separation during key derivation. Additionally, this section highlights the vulnerabilities of 5G authentication and the necessity for it to evolve regularly. Prior generations' security and privacy challenges, notably in radio access networks (RANs), have been thoroughly explored. The following are only a few of the numerous concerns uncovered.

1. Due to the absence of network authentication in 2G, attacks such as network spoofing by faked base stations are possible. For example, a faked base station can advertise a different tracking area code with a stronger signal strength to entice user equipment (UE) away from its legitimate cellular network and register with the faked base station [24].
2. Inadequate secrecy in certain signaling messages, resulting in a violation of privacy. For example, unencrypted paging information can be employed to detect the presence of a specific user and even trace the person to a precise location [25].

To address these concerns, the 3rd Generation Partnership Project (3GPP) provides an Authentication and Key Agreement (AKA) protocol and associated procedures that support entity authentication, message integrity, and message secrecy, among other security aspects [26]. The 3GPP AKA protocol is a challenge-and-response authentication scheme based on the sharing of a symmetric key between a subscriber and a home network. Following mutual authentication between a subscriber and a home network, cryptographic keying materials are generated to safeguard further communication between the subscriber and a serving network, which includes both signaling messages and user plane data (e.g., over radio channels) [26].

Additionally, because the 5G network is IP-based, it will be vulnerable to all IP-specific vulnerabilities. Based on these findings, ensuring a high level of security and privacy will be one of the most crucial parts of deploying 5G networks successfully. Table 3 is presented a comparative analysis of security and privacy of 3G, 4G and 5G cellular networks.

Table 3. Comparative analysis of security and privacy of 3G, 4G and 5G cellular networks.

Study	3G	4G	5G	Privacy-Preserving	Authentication	Remark
[21]	0	√	√	√	√	Investigated authentication and privacy-protection methods for 4G and 5G wireless mobile networks.
[26]	X	√	X	X	0	Outlined the 3GPP standard's security structures and mechanisms.
[27]	X	X	√	X	X	Outlined the security and privacy issues that 5G networks face.
[28]	X	√	X	X	X	Long term evolution (LTE) jamming and spoofing mitigation strategies were investigated.
[29]	0	√	X	X	X	Proposed the cryptographic algorithms for LTE.

Remarks: √: indicates fully supported; X: indicates not supported; 0: indicates partially supported.

2.7.1. Schemes for Authentication in 4G and 5G Cellular Networks

We will compare authentication and privacy-preserving strategies for 4G and 5G cellular networks in terms of authentication and privacy models in this section. Figure 5 presents the classification of 4G and 5G cellular network authentication and privacy-preserving schemes.

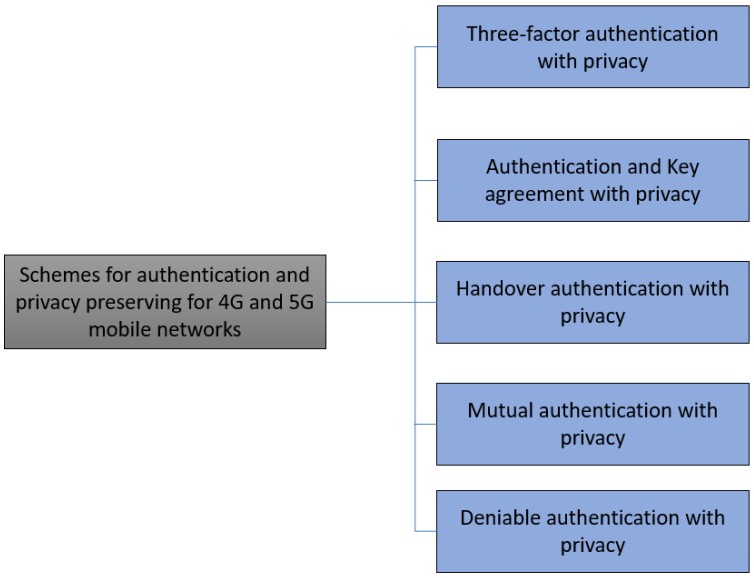

Figure 5. Classification of 4G and 5G cellular network authentication and privacy-preserving schemes.

1. Three-factor authentication with privacy

Three-factor authentication with privacy falls into three categories: protocols based on smart cards, passwords, and biometrics. To address the following research question of whether we can combine the three factors, according to [30], smart cards show what you have, passwords show what you know, and biometrics show who you are. To achieve good biometric privacy, the authors proposed a three-factor authentication approach. The server accepts only if each factor (password, smart card, and biometric data) passes authentication. Compared to the three-factor authentication techniques suggested in [30] and [31], the protocol presented in [30] uses less computation. According to authors in [32], biometric systems fall into three categories: traditional [33], wearable (e.g., smartphone), and hybrid [34]. Regarding wearable biometrics and implantable medical devices, we refer the reader to both recent surveys [33].

2. Authentication and key agreement with privacy

The AKA protocol is a symmetric cryptography-based challenge–response system. With RFC 3310, the Universal Mobile Telecommunications System (UMTS) has implemented the 3GPP's AKA protocol, also known as the 3G standard [35]. Authors in [36], therefore, suggested an enhanced authentication and key agreement methodology based on public key cryptography. The protocol is vulnerable to a variety of attacks, including replay, man-in-the-middle, and denial-of-service (DoS) attacks [37]. The following question is: Is it truly required for the AKA protocol to conceal communication content from an external adversary? Authors in [38] developed a hybrid method based on LTE-AKA modifications that employs both symmetric and asymmetric key encryption to identify and avoid both insider and outsider threats.

3. Handover authentication with privacy

Existing handover authentication systems for LTE wireless networks can be categorized into three types depending on their cryptographic primitives: (1) symmetrical key-based schemes, (2) public key-based schemes, and (3) hybrid techniques. There are two

kinds of base stations in LTE wireless networks: home eNodeB (HeNB) and eNodeB. (eNB). According to [39], the 3GPP project's proposed changeover mechanism from an eNB/HeNB to a new eNB/HeNB cannot provide backward security. The authors specifically presented a handover authentication technique for LTE network mobility scenarios. The technique in [39] is based on the concept of proxy signature and provides various security features, including perfect forward and backward secrecy. Additionally, the approach [39] is more efficient in terms of computational cost and communication overhead than [40] the handover scheme, although identity privacy is not considered.

4. Mutual authentication with privacy

To establish mutual authentication while maintaining privacy, suggested security systems for 4G/5G networks must maintain location privacy, identity privacy, data integrity, and authenticity, as illustrated in Figure 6. Authors in [41], on the other hand, introduced the IDM3G protocol for ensuring mutual authentication and identity privacy in 3G. The IDM3G protocol is divided into two phases: (1) authentication of the UMTS Subscriber Identity Module (USIM) by the provision of a personal identification number, and (2) mutual authentication between the USIM and the mobile operator. The IDM3G protocol is more efficient than both protocols in terms of the quantity of messages exchanged along the path [42], but location privacy is not addressed. In a similar vein to the IDM3G protocol, authors in [43] introduced the BIO3G protocol for safe and privacy-preserving biometric authentication in 3G mobile contexts. In comparison to the IDM3G protocol, the BIO3G protocol cannot withstand DoS attacks and does not consider location or identity privacy [41].

Figure 6. Mutual authentication with privacy techniques classified.

5. Deniable authentication with privacy

Deniable authentication differs from standard authentication in that a third party cannot be persuaded by the receiver [44]. Authors in [45] suggested a non-interactive authentication methodology to accomplish deniable authentication. The protocol in [45] is based on the shared session secret and the ElGamal signature scheme, and it not only considers the security issues proposed by [46], such as forgery, impersonation, deniability, and completeness, but it can also maintain security when the session secret has already been compromised. As a result, in cellular networks, the employment of message authentication codes (MACs) between two parties can provide deniable authentication. Authors in [47] defined an experimental protocol for the Internet community named EAP-PSK under RFC 4764, which provides less scalability and security. RFC 3748 [48] and RFC 2284 specify the Extensible Authentication Protocol (EAP), which is widely used in wireless networks.

2.7.2. Authentication and Privacy-Preserving Techniques Employ Countermeasures

Some important countermeasures employed by the authentication and privacy-preserving techniques for 4G and 5G cellular networks are described in this subsection. These defenses fall into three categories: cryptographic techniques, human factors, and intrusion detection techniques.

First, a physical unclonable function (PUF) is a gadget that takes advantage of intrinsic randomness produced during production to provide a unique 'fingerprint' or trust anchor for a physical entity [49]. These devices have a number of potential uses, ranging from anti-counterfeiting, identity, authentication, and key generation to advanced protocols such as oblivious transfer, key exchange, key renovation, and virtual proof of reality. Another possibility is to use PUFs, which are clone-proof, cost-effective, and resistant to a variety of physical attacks. A PUF takes advantage of the inherent random variations created by manufacturing processes to generate secret keys on the fly [49].

Second, physical-layer authentication (PLA), which is based on the dynamic nature of physical layer properties, is gaining traction as a viable method for increasing wireless security [50]. PLA has recently attracted considerable academic interest due to its information-theory security and simplicity. However, numerous academics have concentrated on PLA and its potential for increasing wireless security [51].

3. Results

Although many studies exist, the research gaps in multi-factor authentication remain open for different combinations. To fill this literature gap, we will further discuss the proposed combination of MFA authentication methods for mobile identity. Depending on the user's mobile phone capability, there are two proposed combination options: mobile phone SIM number with biometric fingerprint or SIM number with geo-location information. Both fingerprint and geo-location will be used as the encryption key to secure the transaction data.

In this study, we propose the use of biometric authentication, specifically fingerprint authentication, due to its unique criteria, which between each person. However, not every device can capture biometrics due to its own limitations. Considering the multitype of mobile devices with a probability of not having a biometric recognition module, we take into count the geo-location identification, as we know that every mobile device will have its own built-in GPS module.

The strong side of geo-location authentication is that most impersonation attempts are made outside the user's area, and some are even made outside the user's country. At present, limiting the geo-location transaction source is performed on the IP level. However, there are some scenarios where the restriction brings trouble to the legitimate user. For example, some countries have used geo-location to restrict the use of the internet due to internal reasons such as riots. During this time, the internet connection for the whole country was shut down. This led to some civilians trying to reach the internet using a VPN service provider, and their IPs changed to external IPs, which ended up being blocked by the system. Due to this, GPS geo-location sounds a bit promising to counter the issue. Now, back to the proposed authentication. Referring to Figure 7, the authentication system design should require a SIM number representing the user's identity, International Mobile Equipment Identity (IMEI), first and second fingerprints and initial geo-location during registration, and the user's information to create an account. Considering the biometric impacts shown in Table 1, a second fingerprint is needed as a backup authentication key upon authentication failure.

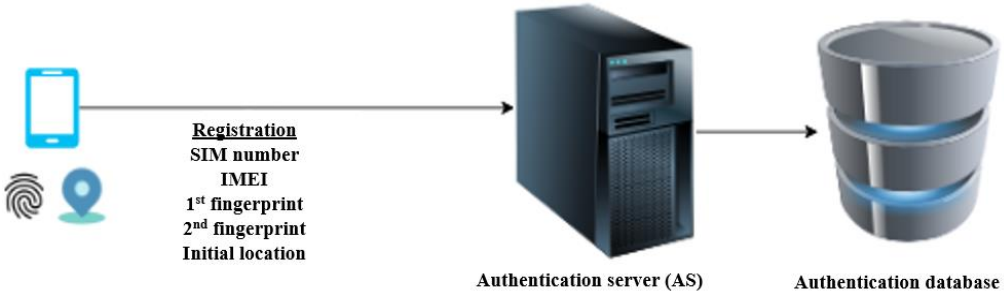

Figure 7. Mobile identity registration.

Once an account is created, the user can perform the transaction on any platforms that are connected to the authentication server (AS). Whenever the user initiates a transaction that requires authentication, the system will first identify if the user's mobile device can capture the fingerprint or not. If the fingerprint capture module is present on the phone, then the SIM number and fingerprint will be used for authentication. However, if not, the combination of SIM number and geo-location will be used instead. Figure 8 shows the flow for the authentication.

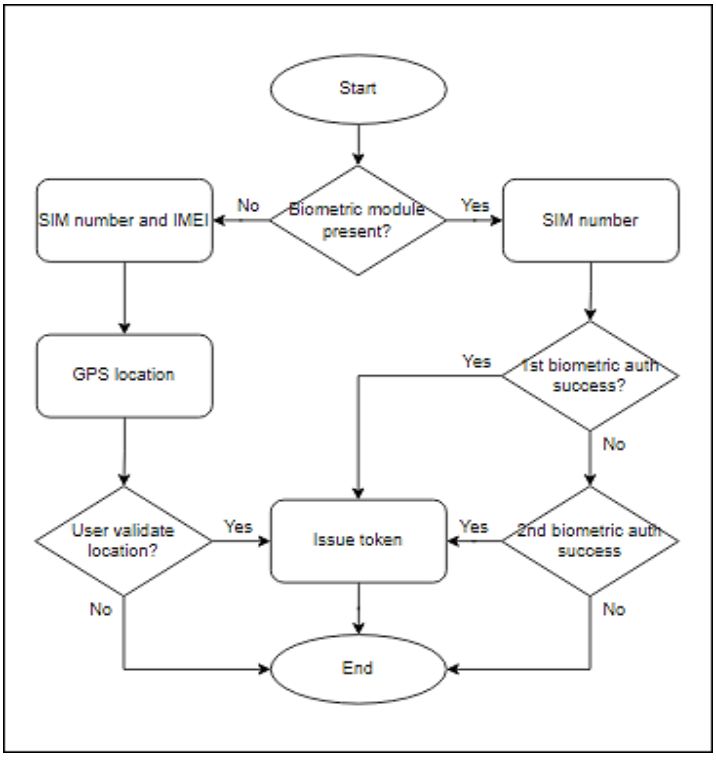

Figure 8. Biometric-geo mobile identity authentication.

The user will need to provide the fingerprint upon authentication for a device that supports fingerprints. The fingerprint will be sent with the SIM number to the AS for verification. Once authorized, the AS will issue an encrypted token used to validate the transaction. The online application server will use the token and cross-check with AS for verification. However, if the fingerprint authentication fails, the user may use the second fingerprint to replace the failed one.

On mobile devices that do not support biometric recognition, the user will need to validate their geo-location. Once validated, the SIM number, device IMEI and the validated location will be sent to AS for verification. AS will cross-check if the provided information of mobile number and IMEI are identical with the record, and the provided location is matched with the GPS location or registered location or within a nearby radius. If either

SIM number and IMEI, or SIM number and geo-location, are correct, the user then will be authorized and receive the token. The authentication flow for these combinations is expressed in Figure 9.

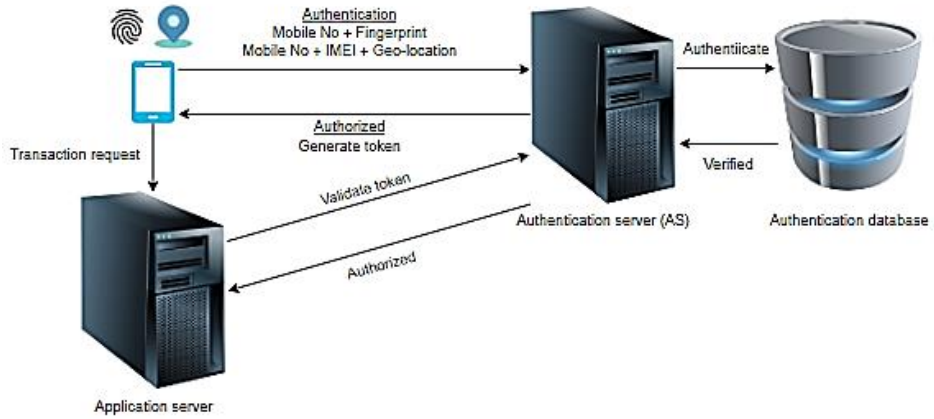

Figure 9. Identity validation and token issuance.

A more systematic and theoretical analysis is required for making this authentication method clearer and more realistic. The system will start by executing a biometric module check on the device. As an example for the Android operating system, the Java class android.hardware.biometrics.BiometricManager can be used to check the availability of biometric devices [52]:

```
public class BiometricManager
extends Object
java.lang.Object
android.hardware.biometrics.BiometricManager
```

Or in IOS using [53]:

```
var biometryType: LABiometryType {get}
```

These code lines are samples for common smartphone types used nowadays. Other types will have their own code functions for serving the same purpose. As a result, once it has confirmed whether a biometric reader exists, the authentication system can now proceed with the subsequent flow, which is to check the SIM number for a mobile device with fingerprint recognition or the SIM number with IMEI extraction for devices that are not supported.

3.1. Mobile Device with Fingerprint Recognition

In the devices with fingerprint modules, the authentication system will require specific privileges and entitlement before extracting the SIM details. These can be obtained during the registration of the user identity account on AS. These code libraries can be used to check on the fingerprint recognition device on the mobile devices subjected to certain conditions on Android [54]:

```
public String getSubscriberId ()
```

and

```
CFStringRef CTSIMSupportCopyMobileSubscriberIden-
tity(CFAllocatorRef allocator);
```

in IOS.

The following steps of the authentication system are to obtain the fingerprint [55]. An asymmetric encryption method is used where the user scans the fingerprint, and it will be used as an encryption key for the transaction details and to receive a token from AS. It is then sent to the application server for verification. The application server will check the validity of the token with the SIM number and proceed to complete the transaction once AS has verified the user identity.

3.2. Mobile Device without Fingerprint Recognition

Like the earlier condition in the previous section, the devices without fingerprint modules also require specific privileges but use different code libraries for extracting the SIM number and IMEI depending on the mobile device type. Once the SIM number and IMEI are successfully recorded, then geo-location will be obtained using the mobile device's GPS receiver.

The captured GPS location will be compared to the initial location defined in the AS, and if identical or within an accepted radius, the token will be issued. However, if the location is outside the accepted range, the user will be required to verify the GPS location manually from a registered device. Once verified, the transaction details and received token from AS will be encrypted using the initially defined geo-location before moving to the application server. The application server will check the validity of the token with the SIM number and IMEI, then proceed to complete the transaction once AS has verified the user identity.

The difference in geo-location captured by GPS will be recorded and analyzed by AS from time to time. The new location will also be whitelisted, allowing for future authentication within acceptable frequency and occurrence. This will reduce the number of user interventions required for authentication.

4. Challenges

Many challenges and open issues need to be addressed in securing mobile identity authentication. It is essential because mobile identity represents us in the virtual world of transactions. This will probably be the only identity recognition that we will use in all daily activities. Any discrepancy in security will cause severe damage to many parties. We have highlighted the challenges and open issues related to mobile identity in the subsection below.

4.1. Different Policies and Regulations

Different policies and regulations related to mobile identity are in use in different countries. Due to the differences, there is no global standard, and it is hard to standardize the mobile identity authentication requirements. There are also different organizations developing different mobile identity infrastructures. Hence, the coverage or a mobile identity system is hard to expand beyond boundaries due to this limitation.

This issue can only be addressed if there is a mobile identity base system capable of integrating multiple mobile identity providers into a single platform. Alternatively, it can be a single software with multiple customizable modules, which can be configured with different required settings such as the Systems Applications and Products (SAP).

4.2. High-End Devices

The authentication method that was presented in this study requires a high-end device that supports biometric recognition. However, there are still many low-end devices in widespread use. Even if all the devices support the GPS authentication method, it may expose them to location spoofing.

The minimum requirement for this authentication method is that mobile devices with GPS support the anti-spoofing module, such as the selective availability spoofing module (SAASM). On the other hand, we believe that all devices supporting biometric recognition and anti-spoof geo-location modules will come sooner.

4.3. Changes in User's Information

The mobile identity is tied to the SIM number. We frequently hear that people keep changing their SIM number, also having multiple SIM cards and shared SIMs. This is quite troublesome in maintaining the integrity of the identity, especially when recycling mobile numbers is also widespread and still growing. The challenge is to make information change convenient at the consumer end. The harder it becomes, the lesser public involvement in registering for mobile identity. This limits the expansion potential of the mobile identity system.

To overcome this issue, the user identity cannot be tied to a mobile number or known as a Mobile Station International Subscriber Directory Number (MSISDN). It may be identified using the MSISDN account number, which is only known by the customer and the service provider. The account number may act as the physical identity card number and will be permanently assigned to the user. So, the mobile identity system, instead of using an MSISDN number, should register the user using the user's service provider account number. In this case, changing or having multiple SIMs should not be an issue.

5. Conclusions

In this paper, we attempted to present the combination of multi-factor authentication that requires less user intervention. Due to security concerns, we introduced the asymmetric encryption protocol where the user's input itself is used as the encryption key. The PKI concept was used but without the requirement to engage certificate authority (CA), thus involving less cost.

As mentioned earlier in this study, due to the uniqueness of fingerprints to identify the user and the accuracy of using GPS for location identification, fingerprint authentication and geo-location identification can be used to correctly authenticate the user, as these methods are unique and affordable to implement. We can see from all advertisements that mobile phones nowadays do have hardware support for both types of authentications. Having a dedicated server for authentication of mobile user identities will ease transaction validation and reduce the possible threats. The way mobile identity works is somewhat similar to a computer's single sign on (SSO) scheme, where the number of attempts by users to validate themselves is reduced because all authentications are performed through the server.

However, the challenges and limitations of different policies and regulations, high-end device requirements, and the changeability of user information need to be addressed to make this authentication method more convenient, secure, and reliable for representing the user in the virtual world. Mobile identity is for more than simply providing access. Security is also an important consideration.

Author Contributions: Conceptualization, A.M. and M.K.A.A.; methodology, M.K.A.A. and Z.A.Z.; validation, M.K.A.A., Z.A.Z. and A.M.; formal analysis, A.M., Z.A.Z.; investigation, Z.A.Z., A.M.; writing—original draft preparation, M.K.A.A. and A.M.; writing—review and editing, Z.A.Z.; visualization, M.K.A.A. and Z.A.Z.; supervision, Z.A.Z.; project administration, A.M.; funding acquisition, Z.A.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We are grateful to the editor and three anonymous reviewers for their valuable suggestions and comments, which significantly improved the quality of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Khan, A.R. National Identity Card: Opportunities and Threats. *J. Asian Res.* **2018**, *2*, 77. [CrossRef]
2. Alavalapati, G.R.; Devanapalli, S.; Kolloju, P.; Ji, S.; Vanga, O. Provably secure pseudo-identity-based device authentication for smart cities environment. *Sustain. Cities Soc.* **2018**, *41*, 878–885.
3. Habib, S.; Hamadneh, N.N. Impact of Perceived Risk on Consumers Technology Acceptance in Online Grocery Adoption amid COVID-19 Pandemic. *Sustainability* **2021**, *13*, 10221. [CrossRef]
4. Pöhn, D.; Grabatin, M.; Hommel, W. eID and Self-Sovereign Identity Usage: An Overview. *Electronics* **2021**, *10*, 2811. [CrossRef]
5. SLA Digital. What Is Mobile Identity? *Mobile Identity.* Available online: https://sla-digital.com/blog/what-is-mobile-identity/ (accessed on 17 January 2022).
6. Alazab, M.; Alazab, M.; Shalaginov, A.; Mesleh, A.; Awajan, A. Intelligent mobile malware detection using permission requests and API calls. *Futur. Gener. Comput. Syst.* **2020**, *107*, 509–521. [CrossRef]
7. Yu, Y.; He, J.; Zhu, N.; Cai, F.; Pathan, M.S. A new method for identity authentication using mobile terminals. *Proc. Comput. Sci.* **2018**, *131*, 771–778. [CrossRef]
8. He, D.; Zeadally, S.; Wu, L.; Wang, H. Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography. *Comput. Netw.* **2017**, *128*, 154–163. [CrossRef]
9. Zhigang, G.; Zhichao, C.; Wenjie, D.; Jianhui, Z.; Huijuan, L. Identity authentication based on trajectory characteristics of mobile devices. *J. Syst. Architect.* **2021**, *112*, 101857.
10. GSMA. Mobile Identity—Unlocking the Potential of the Digital Economy. *GSM Association.* October 2019. Available online: https://www.gsma.com/identity/wp-content/uploads/2014/10/GSMA-SIA-paper_FINALNov-2014.pdf (accessed on 14 January 2022).
11. Feng, W.; Ge, B.S.; Yong, C.; Xianrong, Z.; Hong, W.; Sun, M.; Li, H. Identity Authentication Se-curity Management in Mobile Payment Systems. *J. Glob. Inf. Manag.* **2020**, *28*, 1.
12. El-Soud, M.W.A.; Gaber, T.; AlFayez, F.; Eltoukhy, M.M. Implicit authentication method for smartphone users based on rank aggregation and random forest. *Alex. Eng. J.* **2020**, *60*, 273–283. [CrossRef]
13. Salim, A.; Tripathi, S.; Tiwari, R.K. Applying Geo-Encryption and Attribute Based Encryption to Implement Secure Access Control in the Cloud. *Int. J. Comput. Netw. Commun.* **2019**, *11*, 121–135. [CrossRef]
14. Nor, Z.Z.; Nur, I.R.; Ahmad, D.J.; Farhan, A.M.; Mohdm, M.M.A. Biometric Acceptance in Malaysia Voyage. *e-Security* **2021**, *50*, 2–46.
15. Huaibei, L. Biometric identification of identity authentication technology. *Straits Sci.* **2012**, *10*, 41–43.
16. Muthukumar, A.; Kasthuri, C.; Kannan, S. Multimodal biometric authentication using particle swarm optimization algorithm with fingerprint and iris. *ICTACT J. Image Video Proc.* **2012**, *2*, 369–374.
17. Dong, J.; Zhang, G.; Luo, B.; Yang, Q.; Guo, D.; Rong, H.; Zhu, M.; Zhou, K. A distributed adaptive optimization spiking neural P system for approximately solving combinatorial optimization problems. *Inf. Sci.* **2022**, *596*, 2050054. [CrossRef]
18. Ju, X.; Rosenberger, J.M.; Chen, V.C.P.; Liu, F. Global optimization on non-convex two-way interaction truncated linear multivariate adaptive regression splines using mixed integer quadratic programming. *Inf. Sci.* **2022**, *597*, 38–52. [CrossRef]
19. Alraih, S.; Shayea, I.; Behjati, M.; Nordin, R.; Abdullah, N.F.; Abu-Samah, A.; Nandi, D. Revolution or Evolution? Technical Requirements and Considerations towards 6G Mobile Communications. *Sensors* **2022**, *22*, 762. [CrossRef]
20. Jang, U.; Lim, H.; Kim, H. Privacy-Enhancing Security Protocol in LTE Initial Attack. *Symmetry* **2014**, *6*, 1011–1025. [CrossRef]
21. Ferrag, M.A.; Maglaras, L.; Argyriou, A.; Kosmanos, D.; Janicke, H. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *J. Netw. Comput. Appl.* **2018**, *101*, 55–82. [CrossRef]
22. Behrad, S.; Bertin, E.; Crespi, N. A survey on authentication and access control for mobile networks: From 4G to 5G. *Ann. Telecommun.* **2019**, *74*, 593–603. [CrossRef]
23. Behrad, S.; Bertin, E.; Crespi, N. February. Securing authentication for mobile networks, a survey on 4G issues and 5G answers. In Proceedings of the 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 19–22 February 2018; pp. 1–8.
24. Li, Z.; Wang, W.; Wilson, C.; Chen, J.; Qian, C.; Jung, T.; Zhang, L.; Liu, K.; Li, X.; Liu, Y. *March. FBS-Radar: Un-Covering Fake Base Stations at Scale in the Wild*; NDSS: San Diego, CA, USA, 2017.
25. Shaik, A.; Borgaonkar, R.; Asokan, N.; Niemi, V.; Seifert, J.-P.; Capkun, S. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. *arXiv* **2016**, arXiv:1510.07563. [CrossRef]
26. Cao, J.; Ma, M.; Li, H.; Zhang, Y.; Luo, Z. A Survey on Security Aspects for LTE and LTE-A Networks. *IEEE Commun. Surv. Tutorials* **2013**, *16*, 283–302. [CrossRef]
27. Panwar, N.; Sharma, S.; Singh, A.K. A survey on 5G: The next generation of mobile communication. *Phys. Commun.* **2016**, *18*, 64–84. [CrossRef]
28. Lichtman, M.; Jover, R.P.; Labib, M.; Rao, R.; Marojevic, V.; Reed, J.H. LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation. *IEEE Commun. Mag.* **2016**, *54*, 54–61. [CrossRef]
29. Bikos, A.; Sklavos, N. LTE/SAE Security Issues on 4G Wireless Networks. *IEEE Secur. Priv.* **2012**, *11*, 55–62. [CrossRef]
30. Lee, J.; Ryu, S.; Yoo, K. Fingerprint-based remote user authentication scheme using smart cards. *Electron. Lett.* **2002**, *38*, 554–555. [CrossRef]

31. Fan, C.-I.; Lin, Y.-H. Provably Secure Remote Truly Three-Factor Authentication Scheme with Privacy Protection on Biometrics. *IEEE Trans. Inf. Forens. Secur.* **2009**, *4*, 933–945. [CrossRef]
32. Blasco, J.; Chen, T.; Tapiador, J.; Peris, P. A Survey of Wearable Biometric Recognition Systems. *ACM Comput. Surv.* **2016**, *49*, 1–35. [CrossRef]
33. Rathgeb, C.; Uhl, A. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. Inf. Secur.* **2011**, *2011*, 3. [CrossRef]
34. Camara, C.; Peris-Lopez, P.; Tapiador, J.E. Human Identification Using Compressed ECG Signals. *J. Med. Syst.* **2015**, *39*, 1–10. [CrossRef]
35. Pedrycz, W.; Vasilakos, A.; Karnouskos, S. Guest Editorial—Special issue on computational intelligence in telecommunications networks and internet services—Part II. *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.* **2003**, *33*, 429–431. [CrossRef]
36. Deng, Y.; Fu, H.; Xie, X.; Zhou, J.; Zhang, Y.; Shi, J. A novel 3GPP SAE authentication and key agreement protocol. In Proceedings of the 2009 IEEE International Conference on Network Infrastructure and Digital Content, Beijing, China, 6–8 November 2009; pp. 557–561.
37. Ali, R.F.; Muneer, A.; Dominic, P.D.D.; Taib, S.M.; Ghaleb, E.A. August. Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review. In Proceedings of the International Conference on Advances in Cyber Security, Penang, Malaysia, 24–25 August 2021; pp. 128–154. [CrossRef]
38. Hamandi, K.; Abdo, J.B.; Elhajj, I.H.; Kayssi, A.; Chehab, A. A privacy-enhanced computationally-efficient and comprehensive LTE-AKA. *Comput. Commun.* **2017**, *98*, 20–30. [CrossRef]
39. Cao, J.; Ma, M.; Li, H. Unified handover authentication between heterogeneous access systems in LTE networks. In Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 5308–5313. [CrossRef]
40. Bohák, A.; Buttyán, L.; Dóra, L. An authentication scheme for fast handover between WiFi access points. In Proceedings of the 3rd International Conference on Wireless Internet, Austin, TX, USA, 22–24 October 2007. [CrossRef]
41. Dimitriadis, C.K.; Polemi, D. An identity management protocol for Internet applications over 3G mobile networks. *Comput. Secur.* **2006**, *25*, 45–51. [CrossRef]
42. Kormann, D.P.; Rubin, A.D. Risks of the Passport single signon protocol. *Comput. Netw.* **2000**, *33*, 51–58. [CrossRef]
43. Dimitriadis, C.K.; Shaikh, S.A. A Biometric Authentication Protocol for 3G Mobile Systems: Modelled and Validated Using CSP and Rank Functions. *Int. J. Netw. Secur.* **2007**, *5*, 99–111.
44. Di Raimondo, M.; Gennaro, R. New Approaches for Deniable Authentication. *J. Cryptol.* **2009**, *22*, 572–615. [CrossRef]
45. Lee, W.-B.; Wu, C.-C.; Tsaur, W.-J. A novel deniable authentication protocol using generalized ElGamal signature scheme. *Inf. Sci.* **2007**, *177*, 1376–1381. [CrossRef]
46. Shao, Z. Efficient deniable authentication protocol based on generalized ElGamal signature scheme. *Comput. Stand. Interfaces* **2004**, *26*, 449–454. [CrossRef]
47. Bersani, F.; Tschofenig, H. *The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method*; IETF: Marina del Rey, CA, USA, 2007. [CrossRef]
48. Aboba, B.; Blunk, L.; Vollbrecht, J.; Carlson, J.; Levkowetz, H. *Extensible Authentication Protocol (EAP)*; IETF: Marina del Rey, CA, USA, 2004. [CrossRef]
49. Gao, Y.; Al-Sarawi, S.F.; Abbott, D. Physical unclonable functions. *Nat. Electron.* **2020**, *3*, 81–91. [CrossRef]
50. Wang, X.; Hao, P.; Hanzo, L. Physical-layer authentication for wireless security enhancement: Current challenges and future developments. *IEEE Commun. Mag.* **2016**, *54*, 152–158. [CrossRef]
51. Xie, N.; Li, Z.; Tan, H. A Survey of Physical-Layer Authentication in Wireless Communications. *IEEE Commun. Surv. Tutor.* **2020**, *23*, 282–310. [CrossRef]
52. Developers. BiometricManager. Available online: https://developer.android.com/reference/android/hardware/biometrics/BiometricManager (accessed on 14 January 2022).
53. Developers. biometryType. Available online: https://developer.apple.com/documentation/localauthentication/lacontext/2867583-biometrytype (accessed on 24 January 2022).
54. Developers. TelephonyManager. Available online: https://developer.android.com/reference/android/telephony/TelephonyManager.html#getSubscriberId%28%29 (accessed on 27 January 2022).
55. Murray, D. Ios-Reversed-Headers. Available online: https://github.com/davidmurray/ios-reversed-headers/blob/master/CoreTelephony/CTSIMSupport.h (accessed on 27 January 2022).