IntechOpen *Journals*

AI, Computer Science and Robotics Technology

RESEARCH PAPER

Modern Authentication Methods: A Comprehensive Survey

Maria Papathanasaki[1], Leandros Maglaras[2,*] and Nick Ayres[2]

1 University of Thessaly, Faculty of Sciencse, Lamia, Greece
2 Cyber Technology Institute, De Montfort University, Leicester, UK
*Corresponding author. E-mail: Leandros.maglaras@dmu.ac.uk

Abstract

This paper presents a comprehensive investigation of modern authentication schemes. We start with the importance of authentication methods and the different authentication processes. Then we present the authentication criteria used and we perform a comparison of authentication methods in terms of universality, uniqueness, collectability, performance, acceptability, and spoofing. Finally, we present multi-factor authentication challenges and security issues and present future directions.

Keywords: authentication, performance evaluation, MFA

Citation
Maria Papathanasaki, Leandros Maglaras and Nick Ayres (2022), Modern Authentication Methods: A Comprehensive Survey. *AI, Computer Science and Robotics Technology* 2022(0), 1–24.

DOI
https://doi.org/10.5772/acrt.08

Published
1 June 2022

1. Introduction

Since their development and introduction computing systems were shared devices that lacked any form of security or confidentiality in data created and stored. In the early 1960s the Massachusetts Institute of Technology (MIT) developed a time-sharing operating system known as the Compatible Time-Sharing System (CTSS). This system enabled multiple dumb terminals to concurrently share a single centralised computer's resources. This led to issues of a shared file systems with no inherent security. To establish a secure file system, in 1961, Fernando Corbató, an MIT Computation Center member and a founder of CTSS resolved this lack of security issue through the use of passwords to authenticate users to specific held data and files. However, Allan Scherr, an MIT researcher discovered that server-based systems stored passwords in a master password file in an easily accessible location thus enabling access to any password protected files. In the 1970s, Bell Labs researcher Robert Morris devised a method to safeguard the Unix operating system master password file. Morris utilised a cryptographic technique known as a "hash function" that rendered a password unreadable to the human eye but not to the computer system. This basic concept was soon adopted by the majority of other operating systems.

To gain access to data or a service, verification of a user's identity must first be established through authentication. Authentication is the process of successfully

validating the identity of a person or device [1]. When we use a bank card to make a purchase, we authenticate ourselves by having the card and knowing the Personal Identification Number (PIN). Authentication has become more essential since the widespread use of computers. User impersonation is a critical security hazard to any computer system and the first defence mechanism against this type of attack is user authentication. Data that is used to confirm a user's identification can be catagorised into three classes:

- Knowledge-based that include passwords and PINs
- Possession-based that include smart cards and tokens
- Inheritance-based such as biometrics that include fingerprints and retinal scanning

Over time as attackers figured out how to "brute-force" hash algorithms, the industry has improved hash functions and included extra randomisation components. For example, salting, to make a hashed password unique. Robert Morris' creation of hash-based password storage methods in the 1970s improved the security of authentication systems.

Other cryptographic approaches, besides hashing, are effective for authentication. Public-key or asymmetric cryptography is one such technology. In the early 1970s, asymmetric cryptography and public/private keys were found used. While those encryption techniques were not made public until the 1990s, public researchers discovered new techniques by themselves to exploit asymmetric key technology in the late 1970s, leading to the development of the widely used RSA asymmetric key algorithm. In the field of authentication, digital certificates and signatures have become crucial.

Researchers and cybercriminals have developed new ways to exploit passwords since more digital systems depended on them for protection. As a consequence, the industry is always seeking to incorporate new ways to safeguard the authentication process. One of the greatest drawbacks with a typical, permanent password system, is that if an attacker can assume, steal, or overhear somebody's credentials, they can replay them. To counteract this, what if a user's password was different each time he or she logged in? Researchers developed strategies to distinguish humans from computers in the late 1990s. These techniques known as Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA). A CAPTCHA cannot be used to authenticate a user, but they can be used to protect against some automated authentication assaults.

The time for Multi-factor Authentication (MFA) has come, which is still under development, but has gained a lot of traction in the 2000s. Passwords are the most used form of digital authentication. They are, however, displaying their age

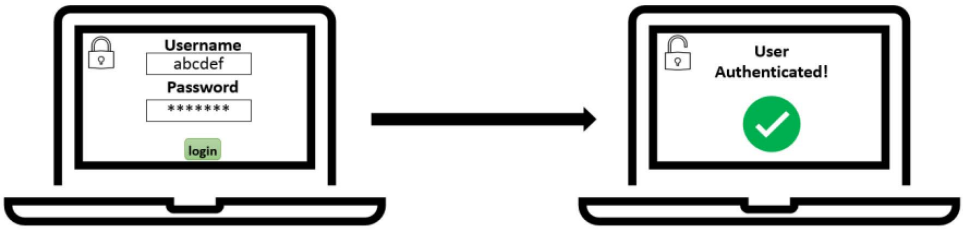

Figure 1. Single factor authentication.

and frailty. Passwords are a good authentication mechanism when used properly and under strict security guidelines. The issue is that most people do not follow the recommended practices, and many businesses that handle passwords do not follow them either. Countless password database leaks have occurred as a result of this password mismanagement over the last few decades, demonstrating that passwords alone are incapable of protecting our online identities. MFA can address and help fix this problem, but authentication systems and alternatives are often prohibitively expensive or difficult to implement. Modern cell phones are paving the way for the authentication of the future. In the 2010s, the widespread availability of smartphones has made biometrics and Two Factor Authentication (2FA) and MFA technologies more accessible to the general public.

2. *Factor authentication*

Authentication, whether offline or online, is an important protection against unwanted access to a device, service or data. Authentication is a procedure where the user confirms their identity by providing x to the system, which the system then verifies by calculating $F(x)$ and comparing it to a saved value y.

2.1. Single factor authentication (SFA)

The most widely used authentication technique is a username and password combination (See figure 1).

2.1.1. Advantages

Due to its simplicity and easiness to use, SFA was extensively utilised, for example, using a password (or a PIN) to verify the user identity. Passwords comprise a combination of letters, numbers, and special characters. The more complex the combination of the above, the stronger the password and consequently the harder it is for the attacker to detect it.

2.1.2. Disadvantages

The average person owns about twenty-five online accounts but only the half of the users have different passwords in each account. The reality is that a single user has a lot of passwords to remember. As a consequence, most people prioritise ease over safety. Numerous people choose easy passwords rather than secure ones. Extremely simple passwords, which may include the name of the user, date of birth etc. are vulnerable to phishing attacks. Passwords have numerous flaws and are, alone, no longer effective for protecting data accessed and transferred via internet. User account security can be compromised if the password is shared or discovered. An unauthorised user can employ brute force in the form of dictionary attacks, or social engineering techniques to acquire access. Hackers can simply use freely available tools which can be automated to guess a user's password by attempting all possible combinations until they find a match.

2.2. Two-factor authentication (2FA)

Due to a variety of security concerns, it was found that SFA could not offer effective security. 2FA increases security by combining representative data (username/password combination) with another form of identification such as a personal ownership factor which could include a secure token utilising a One Time Password (OTP) [2]. 2FA can be drawn from three different types of factor groups as shown in figure 2:

1. Ownership factor—a thing that the user has, such as cell phones
2. Knowledge factor—a thing that the user is aware of, such as a password
3. Biometric factor—a fact about the user biometrics or behaviour

Applying this method of identification requires an additional mechanism that may include an electronic device such as a mobile phone, tablet, or computer or physical component (See figure 3). After completing the first stage of authentication, the second mechanism follows where the user is asked to present a physical mechanism or an OTP sent through email, SMS, or other device [3].

2.2.1. Advantages

This method of utilising two or more factors is an improved mechanism for user identification offering improved security. The second authentication mechanism is in addition to the classic one chosen by the user. Thus, if someone steals a user's password, they will need access to the second authentication mechanism which the threat actor does not have access to therefor enhancing the security of the user's personal data. Through the availability of smart devices such as passcode generation tokens, Radio-frequency identification (RFID) cards, 2FA is easy to use improving usability as well as enhancing overall security.

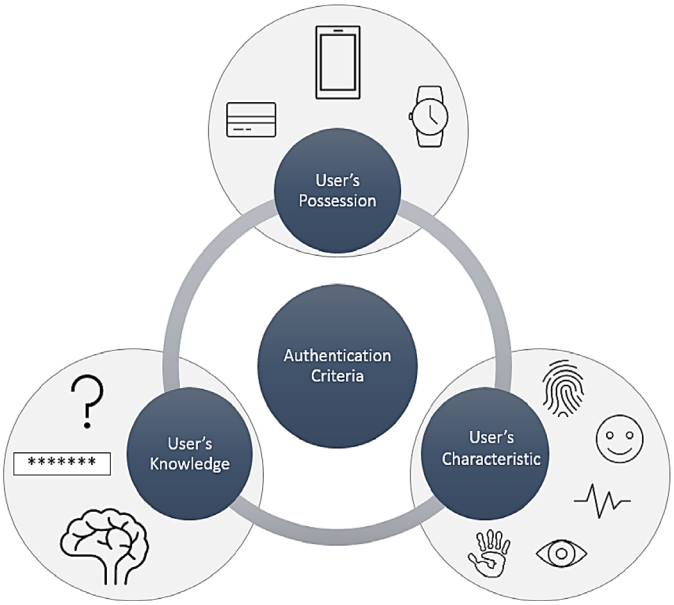

Figure 2. Authentication criteria.

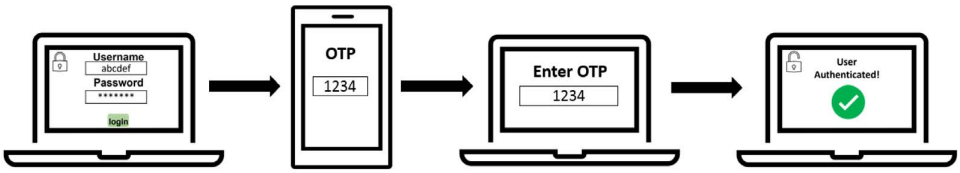

Figure 3. Two-factor authentication.

2.2.2. Disadvantages

More authentication mechanisms lead to a more complex authentication process. 2FA incurs additional hardware which adds to cost and often reducing usability. Another drawback is that without both authentication mechanisms even the authorised user cannot gain access. Also, connectivity to these smart devices is a challenge within an 2FA procedure. For example, the absence of connectivity of the smart device is one of the most critical MFA challenges.

2.3. Multi factor authentication (MFA)

Nowadays, it is necessary to have further levels of security since attacks are becoming more targeted and the consequences of unauthorised access are serious. This is especially prevalent for banking or personal data platforms. It is now imperative that there is more control over identity verification of the person attempting to access these systems. With these additional requirements, there is no doubt that the protection offered is considerably greater, but it is still not enough in some cases. This creates the need to create more levels of authentication that will

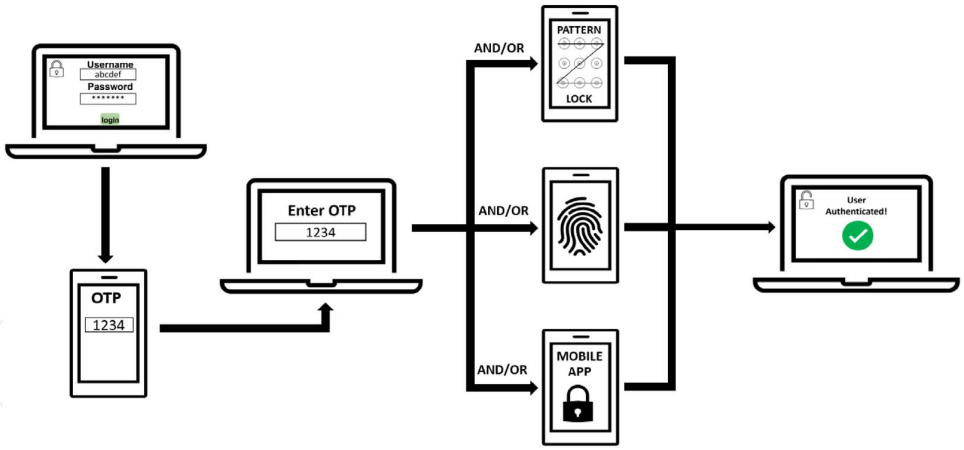

Figure 4. Multifactor authentication.

maximise security. To address this, MFA is becoming increasingly more common (See figure 4). MFA commonly includes unique biological characteristics of the user, such as fingerprint or iris scans as these are often highly accurate in their creation and use [4]. It is a way to offer an increased level of security to safeguard the security of computer equipment and other vital services from unauthorised access by combining at least three types of credentials [5].

Consider the daily practice of withdrawing cash from an Automated Teller Machine (ATM). To gain access to a personal account and withdraw money, the user must submit a physical token (bank card) that represents the ownership factor, while the knowledge factor is represented by a PIN. This system might easily be made more secure by adding an additional biometric mechanism.

2.3.1. Advantages

Biometrics contribute in MFA through combining knowledge and ownership factors with biometric factors to increase identity proofing, making it hard for a threat actor to deceive a system through impersonation. The assessment of many biological related features to identify an individual's identity can greatly improve the MFA system's operation. The fingerprint scanner has become the most often incorporated biometric interface in terms of user experience. This is mostly due to smartphone manufacturers' extensive adoption. The usage of pre-integrated ones lowers the cost of the authentication system and makes it easier for end users to use it. One of the most significant elements to consider in modern authentication systems is the trade-off among usability and security. The MFA approach allows a wide range of situations where security is paramount. Several are detailed below [6]:

- Massive Open Online Courses (MOOCs), where it's difficult to distinguish between a registered user and a user that will take an exam or do homework.

With the rise of MOOCs at colleges, it is now essential than ever, to securely verify students' identities. Since the mix of authentication factors vary and may be created even based on the complexity of the job, MFA is a suitable solution for confirming student IDs because of its consistency and scalability.

- Bank applications like electronic money transfer or online payments must be secured. MFA can be utilised to rapidly verify authorised users. Money transferred can be a determining factor, so that identity changes are necessary to successfully identify users, correspondingly less strict factors authentication may be selected for lower amounts of money.
- Safe accessibility to all sorts of electronic health records can be readily linked with the MFA. This medical information is highly sensitive and private, and it must be protected. By identifying the user's device, media, and surroundings, the MFA can determine an identity test technique, resulting in more secure authentication.

2.3.2. Disadvantages

Using biological elements entails several drawbacks, mostly in terms of ease of use, which has an important impact on the MFA system's usefulness. From the perspective of biometric authentication, a disparity between the measured biometric presentation and the data recorded at the initial biometric registration can be problematic especially with inexpensive and inaccurate equipment. False Accept Rates (FAR) and False Reject Rates (FRR) are issues concerning biometric authentication. FAR and FRR are extremely important to the MFA operation as achieving complete accuracy within these two metrics is near impossible.

3. Authentication techniques

According to Velásquez, Caro and Rodríguez [7], there are about fifteen authentication techniques used either individually in single factor authentication or in combination (2FA) authentication (See table 1). Depending on the criteria mentioned before, we group together and report below these techniques:

Studying the above table, we observe there are more different biometric characteristic techniques when compared to knowledge and possession criteria. Biometric is based on the individual and thus their characteristics are individual to the user offering a highly personalised and secure authentication mechanism. However, the cost of biometric presentation is usually expensive and that is why they are included only in special and rare cases. In the case of combining two or more techniques in MFA, it is considered a good practice to select from each group-criterion and combine them into a highly secure authentication process [7].

It is worth noting that in many cases the actual user's location information is also considered when attempting authentication. This authentication procedure uses a

Table 1. Authentication techniques.

Criterion	Technique
Users Possession	Smart Card Cell Phone Password Secure Token
Users Knowledge	Cognitive Password PIN Personal Questions
Users Characteristic	Fingerprints Retina Facial Features Hand Geometry

person's location to aid in identification. This criterion usually uses Global Positioning System (GPS) systems, the user's IP address, or even a hive tower identifier. The system uses the user's geographical location and determines if a login attempt can progress. For instance, if a successful login attempt was made in one geographical location and another attempt is made at a completely different location a few minutes later, the attempt can be denied and the account frozen to prevent suspicious behaviour [6].

One of the most common uses of MFA nowadays is for identification and authentication while accessing sensitive data. In figure 5 the state-of-the-art authentication sources are presented. Those sources are also analysed in the following subsections.

3.1. Password security

Requesting a PIN code, password, or other form of authentication is the traditional method of authentication [8]. The knowledge aspect is represented by a secret (known only to the user) word, phrase or number sequence. To authenticate the user, all that is required is an input device. PIN codes are generally accepted globally due to their extensive adoption by ATMs and the widespread use of mobile phones.

3.2. Tokens

An authentication can be augmented with a tangible token, to prove ownership [9]. A user may produce a smartcard, smartphone, wearable smart or other device, all of which are more difficult to delegate [10]. The system works with a cellular platform that allows a two-way connection with the token [11]. The most well-known software token, is the one-time program (OTP) generated password/passcode.

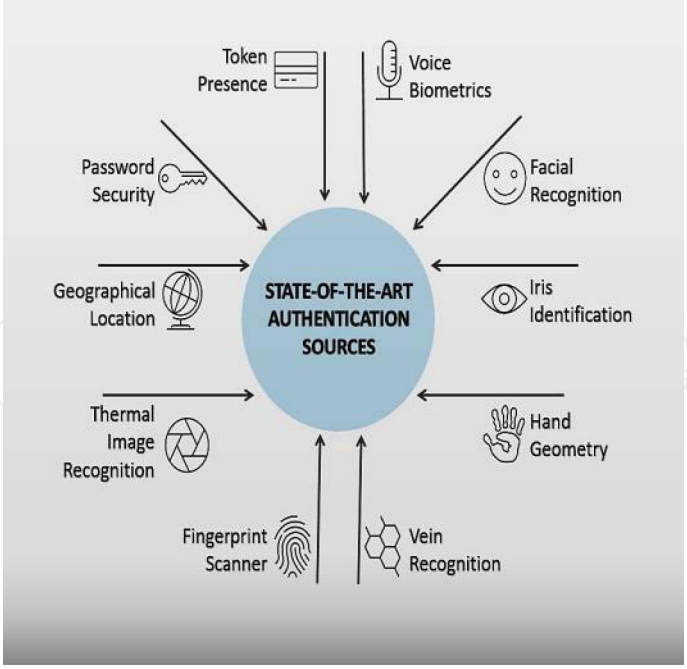

Figure 5. State-of-the-art authentication sources.

The problem of unregulated duplication is the fundamental disadvantage of this system.

3.3. Voice biometrics

The majority of contemporary smart electronic gadgets have a microphone, allowing people to use voice in the authentication process [12]. Voice impersonation can recreate a voice, including pitch, tone to potentially fool this type of system. However, upcoming technological improvements can detect features in the voice pattern which increase the detection of false positives and solve a key flaw in utilising voice as a significant verification mechanism. According to recent reports devices can now discern innumerable different voices once they hear a short sentence, according to recent reports. However, unlike facial recognition, these methods are more sensitive to spoofing assaults.

3.4. Facial recognition

Facial recognition is done by measuring the distance between the person's eyes, the breadth of the nose, the distance of the cheekbones and other unique features of the user. Facial recognition could be viewed as a stage in the future. The system was initially relied on landmark picture analysis, that was reasonably easy to duplicate by just presenting the system with a photograph. Three-dimensional facial recognition techniques have advanced dramatically during the last twenty years.

This technology eventually developed to the point where it could identify the user's actual expressions.

3.5. Eye recognition

One method of eye recognition is a biometric identifier that takes a picture of the iris. Iris identification algorithms have been around for over 20 years. This method analyses data from that picture and develops individual patterns from it. The technique involves identifying the boundaries, shape and contour of the iris and detecting the position of the pupil. These factors are combined to assemble a summary of characteristics for each individual iris. On presentation, retrieving the correct image from the database requires a very high-resolution camera [13]. Modern cameras used for iris recognition use infrared (IR) to illuminate the iris. While examining the human eye's color pattern, the client does not need to be near the capturing device to use this method. Retinal analysis is another eye recognition technique. In this procedure, the blood vessels in the rear part of the eye is captured and analysed. In a high-security context, retina scanning is regarded as one of the most efficient and resilient way for authenticating users, however, this comes with the high cost of equipment.

3.6. Hand geometry

The shape, form, and measurements of the palm are monitored and measured by the biometric hand recognition system. Differentiated, widths, and thicknesses of fingers and joints can be found in different areas of the hand. Different aspects of the epidermis of the hands, such as folds and lines, are also taken into account when calculating the geometry of the hands. The user places his palm on the reading area and positions his hand so that it is perfectly tangent throughout. The scanning device then records the geometry of the hands and extracts the attributes. These characteristics are contrasted with the user's stored record in the database. Authentication takes a few seconds to verify the person. Biometric hand-based depends mainly on the hand and the geometry of the fingers and therefore, this or the biometric technique can also work even with not clean hands. The image was captured using a flat open surfaced scanner, which eliminated the need for the person's hand to be placed in one position. Some systems today use standard cameras that do not demand close contact with the capturing surface. That method is not extremely resistant to environmental changes. Photoplethysmography (PPG) is a technique used by some suppliers to assess if a wearable device (such as wristwatches) is on the user's wrist or not [14]. This procedure is identical to that used to determine heart rate. Hand geometry authentication can be used in lockers or interactive kiosks.

3.7. Fingerprint scanner

Today a large number of mobile smart devices incorporate fingerprint scanning as a basic authentication mechanism. This technique is simple to use but can be potentially exploited through the collection of fingerprints from practically anything we touch. This authentication method has a lot of integration potential [15], but it's not suggested for usage as a stand-alone authentication mechanism.

3.8. Thermal image recognition

Thermal sensors are used to build a unique thermal image of an individual's blood vessel structure in the face [16]. This is particularly useful in situations where low light levels may be an issue. However, performance at presentation can be affected as a result of the user's state of wellbeing which may alter the individual's characteristics [17].

3.9. Geographical location

Using the device and user's physical location is used to determine if authentication or access to a particular service is granted [18]. Certain geographical location can be added to an allow or block list regardless of an individual's level of access. Attempted access from geographical locations can be combined with time stamps to determine if the user attempting authentication can actually be in both locations within a given timeframe.

3.10. Beam-forming techniques

RFID and near-field communication (NFC) systems have gained significant acceptance with users especially through the use of mobile phone technologies [19]. The issue with ownership factor authentication techniques is the lack of guarantee that the user presenting is the user that should be authenticated. These types of authentication mechanisms when used with other authentication types can and are being used to make cashless payments.

3.11. Occupant classification systems (OCS)

OCS technologies have been implemented into numerous vehicular systems in consumer cars. Sensors within the system can recognise various characteristics of the individual sitting in a particular seat for instance. Factors based on weight or posture for example can detect the user or type of user and automatically alter the vehicle characteristics to meet specific demands.

3.12. Electrocardiographic (ECG) data

ECG data captured from a worn smart gadget can be collected and analysed to a previously saved pattern. ECG signals appear like a possible biometric way that is difficult (if not impossible) to imitate, which is a major benefit of using this component for authentication. The only solution is to use a personal recording that already exists.

3.13. Electroencephalographic (EEG) data

This relies on the examination of brain function. It enables the collection of individual brain activity patterns. To collect data medical probes underneath the cranium or wet-gel electrodes strewn across the scalp were used. EEG data acquisition could previously be done only within clinical settings. However, simple EEG collection is now possible using commercially accessible devices built within a headset [20].

3.14. Deoxyribonucleic acid (DNA) recognition

This organic chemical within the body contains unique genetic information. It is as individual as fingerprints and highly accurate in determining user identity. The process to gather and analyse is time-consuming and costly, it can however, be used to pre-authorise a user to a highly secure facility or extremely sensitive top-secret information or data.

3.15. MFA factors comparison

The following parameters are used to evaluate individual authentication types (See table 2):

- **Universality** indicates that the feature is present in each individual
- **Uniqueness** denotes the ability of the factor to distinguish one individual from another
- **Collectability** denotes the ease with which data may be collected to process
- **Performance** denotes the precision, efficiency, and robustness that can be achieved
- **Acceptability** refers to how well people accept technology in their everyday live.
- **Spoofing** refers to how difficult it is to collect and spoof a sample

4. Multifactor authentication operation challenges

While integrating MFA for end users, numerous other difficulties must also be addressed (see figure 6). For both developers and implementers, integrating new

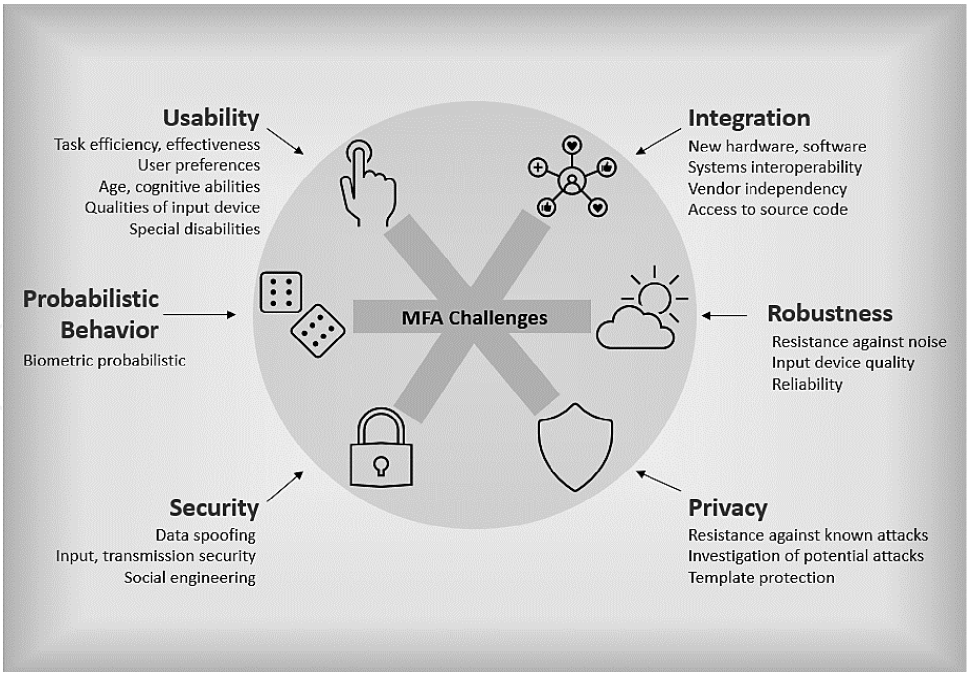

Figure 6. Principle Operational Challenges of MFA.

Table 2. MFA factors comparison.

Factor	Universality	Uniqueness	Collectability	Performance	Acceptability	Spoofing
Password	Unavailable	Low	High	High	High	Low
Token	Unavailable	Medium	High	High	High	Low
Voice	High	Medium	Medium	Low	High	Medium
Facial	High	Medium	Medium	Low	High	Medium
Eye	High	High	Medium	Medium	Low	High
Hand geometry	High	Medium	Medium	Medium	Medium	Medium
Fingerprint	High	High	Medium	High	Medium	High
Thermal image	High	High	Low	Medium	High	High
Location	Unavailable	Low	High	High	Medium	Medium
Beam-forming	Unavailable	Medium	Low	Low	Low	High
OCS	High	Low	High	Low	Low	Medium
ECG	High	High	Low	Medium	Medium	Medium
EEG	High	High	Low	Medium	Low	High
DNA	High	High	Low	High	Low	High

solutions always comes with difficulty. First and foremost, user acceptability is a vital component of strong identity and MFA uptake. It is necessary to take a cautious and thorough approach when implementing and deploying MFA solutions [21].

4.1. Usability

The primary usability issues that arise during the authentication procedure can be classified into three categories [22]:

- **Task Efficiency** time for both system registration and the authentication process
- **Task Effectiveness** the number of times the user tries to access the system
- **User Preference** if the user favours one authentication method over another

Usability is the fact of something being easy to use, or the degree to which it is easy to use and is a way we can measure and understand how easy it is for people to use a system. Generally, the intended users do not design these systems and therefore they don't know and don't care how it works. However, sometimes people are able to immediately use a system regardless of their previous interaction with it due to mental models. A usable system utilizes mental models that often come from life experience to help understand how users perceive a system thus improving overall usability. Interestingly, the authors of [23] found that gender does not affect usability. Belk *et al.* [24] published a study comparing the task completion efficiency and effectiveness of traditional and realistic passwords. Their findings revealed that using visual passwords takes longer for the majority of participants than using text-based passwords. However, cognitive differences across users, such as whether they classified as verbal or visual thinkers [22]. Text-based tasks are completed faster by verbal thinkers, and vice versa with regard to image-based tasks.

4.2. Integration

Although all usability problems are solved during the creation stage, integration raises additional challenges from either a technological or a human perspective. Hardware-based MFA are still the bulk of consumer MFA solutions. Convergence, at the other end of the spectrum, is more complicated. Linking together physical and IT security teams, blending disparate system components and updating physical access methods are all issues. When designing an MFA system, biometrics autonomy must be thoroughly investigated. Multi-biometrics, or the utilisation of many components at the same time, should also be examined.

Another important interoperability issue is vendor reliance. Enterprise solutions are frequently created as isolated, stand-alone systems with a minimal amount of adaptability. Integration of newly developed sensors would necessitate sophisticated and costly modifications, which are unlikely to be considered soon. It is also important to mention that most existing MFA solutions are often not open source. This highlights the question of the trustworthiness and dependability of third-party service providers. When selecting an MFA framework, the level of transparency given by the hardware and the software suppliers ought to be considered.

4.3. Security and privacy

Any MFA scheme must incorporate sensors, computing and storage systems and networking channels. At various levels, they are all subjected to a variety of attacks, ranging from replay to adversarial. Consequently, security is an important for preserving privacy. Therefore, we'll begin by targeting the input device directly. Data spoofing is a big threat. Biometrics are employed in many different MFA mechanisms which are commercially available and any potential intruder has opportunities to investigate sensor technology, overall system configuration including both hardware and software. The major purpose of system and hardware architects is to provide a secure environment or to anticipate spoofing opportunities. Consider the possibility of collecting actual or digital patterns and replicating them inside the MFA system. To protect against electronic replay assaults, it has traditionally been necessary to utilise timestamps [5, 25, 26]. Nevertheless, a biometric spoofing attempt is rather easy to carry out, however, how successful an attempt is determined by the quality of the system often replicated in the cost of that particular system.

While biometrics may enhance the efficiency of the MFA system, they simultaneously raise the frequency of vulnerabilities that an intruder might use. The capture of a biometric sample, is of particular importance to an attacker and therefore protecting biometric data during the capture, transmission, storage, and processing phases necessitates a greater level of security. There is also a danger that sensitive data could be intercepted between presentation at the sensor and the processing/storage unit. Theft may happen as a consequence of an insecure connection between the input device and the database using retrieval and pairing blocks. To combat this type of threat data encryption is essential. MFA authentication results are stored within databases which are typically stored in a single location, resulting in a potential single point of failure within the MFA system. To protect data against fraud, in addition to adopting high levels of encryption, a greater level of isolation is also needed [27]. Cellular and WLAN-based location services spoofing attacks are made possible through blocking a GPS signal or transmitting misleading information to the recipient, leading the system to estimate an inaccurate place or time.

4.4. Robustness to operating environment

Biometric technologies particularly fingerprinting, have often failed to meet the "robustness" requirement since their widespread introduction. Voice recognition, for example, is principally reliable in a silent environment but increased failure rates can occur with an increase in ambient noise levels near to voice presentation. Early facial recognition systems have failed to work consistently in the absence of suitable lighting or suitable camera hardware. The requirement for constant supervision of

the investigated subject was the flip side of the coin. Failure to Enrol (FTE) and Failure to Acquire (FTA) rates are often used to assess a deficiency of experience between computer and human contact [28].

Because a large portion of MFA is heavily reliant on biometrics, it could be characterised as intrinsically probabilistic. The field of pattern matching, which depends on approximation, is at the heart of biometric authentication. The differences between users is essential for every MFA system and accurate matching every time is crucial. The scan of a fingerprint will differ each time to some degree due to presenting angle, force applied, moisture levels in the skin, or sensor accuracy, even when taken from the same individual.

False Acceptance Rate (FAR) and False Rejection Rate (FRR) are two significant error rates to consider when evaluating a biometric identification system's effectiveness. FAR is referred to as the percentage of identification occurrences where an unauthorised person is incorrectly accepted. FRR is concerned with the percentage of occurrences in which an authorised person is incorrectly rejected. In addition to FAR and FRR the Crossover Error Rate (CER) [29] is the likelihood of the system existing in a state where FAR and FRR are equal. In general, the lower the CER number the better the system's performance. A higher FAR can be tolerated in systems where safety is not a top priority, but a higher FRR is desired in high-security applications.

5. *Web authentication methods*

5.1. Basic authentication

When making a request Hypertext Transfer Protocol (HTTP) authentication requires the client to pass a username and associated password. This mechanism does not involve cookies or sessions this is the easiest way to impose restrictions on access. To make use of this, the client must provide an authorisation header with each request. Generally, the user ID and password are not encrypted. This method is simple to use and implement and the API's are faster since they require no complex encryption or decryption (See figure 7).

1. Get the username and password from user
2. Encode it using Base64 algorithm
3. Set it in the authorisation header and send it along each HTTP Request

5.2. Digest based authentication

This is a more advanced variant of Basic authentication and addresses the security flaws in basic authentication over an HTTP network such as credentials being sent in

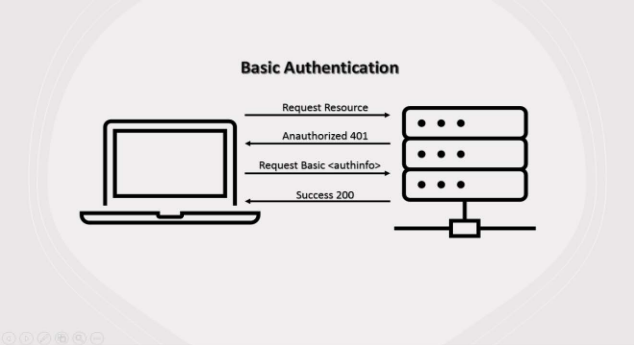

Figure 7. Basic authentication.

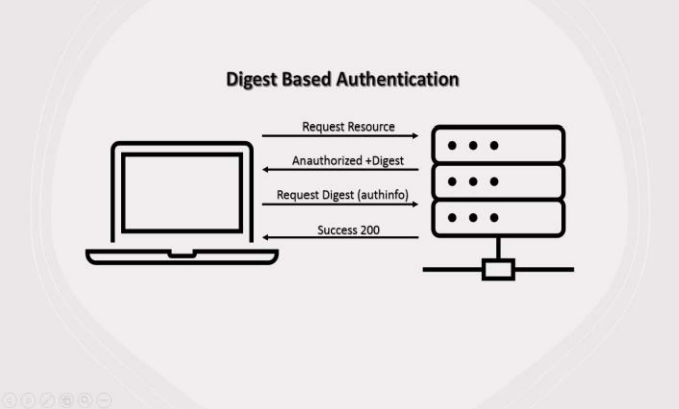

Figure 8. Digest based authentication.

plain text. Instead of dealing with Base64 encoded texts, the server now gives a digest that the client can use to encrypt the login credentials (See figure 8). We are no longer concerned about a Base64 encoded string being globally known in digest base authentication.

1. Request a resource from a server, the header is set by the server providing digest information
2. Get the username and password
3. Hash the login and password and transmit it to the server with the digest
4. The server decodes the string using the digest and gives the user access to it

5.3. Cookie/session based authentication

Cookie/session-based authentication is the most common used method of authentication in online applications (See figure 9). Although a cookie and a session are not equivalent, a cookie or a session is used by either the client or the server to identify itself as a logged in user. A Set-Cookie header can be sent by a server in response to a HTTP request. The browser saves it in a cookie jar, and the cookie is

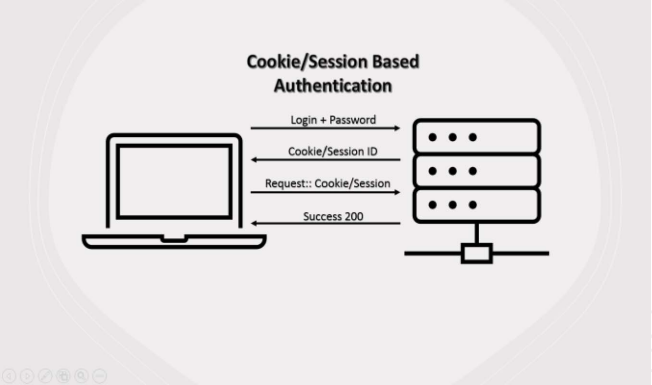

Figure 9. Cookie/Session based authentication.

delivered in the Cookie HTTP header with every request to the same origin. The advantage of this is the password is no longer set in every request, thus reducing the attack window. In a stateless system, it allows state maintenance. Cookies keep track of whether the user is signed in or not and a cookie's validity can be revoked as and when required. There are a few fundamental guidelines to consider when using cookies for authentication reasons. Because the cookie is read by other applications, it is exposed to Cross Site Scripting (XSS) and Cross Site Request Forgery (CSRF) attacks. HTTP-Only cookies should be used at all times. When setting cookies, always utilize the HTTP-Only flag to reduce the risk of XSS attacks. They won't appear in document cookies this way. A server can identify if a cookie has been modified by the client using signed cookies.

1. Get the user's username and password.
2. Set the parameters in the request form and submit it to the server.
3. The user's ID is verified by the server using the provided username and password.
4. Create a cookie and save it in the response after successful validation.
5. This cookie/session is then used by the client to make subsequent requests.

5.4. JavaScript object notation (JSON) web token based authentication

Stateless authentication is a type of token-based authentication. A server-generated token is used for authentication instead of transmitting credentials. Token-based authentication includes open authorisation (OAuth) and JSON Web Token (See figure 10).

1. Credentials are entered by the user
2. The server verifies the token and issues it as a singed token
3. Allows future requests by using the token

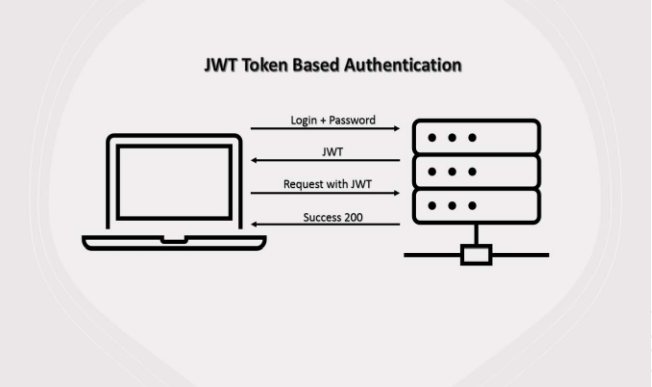

Figure 10. JWT Token based authentication.

A microservices architecture is an advantage of JSON Web Token based authentication as the overhead of session information is no longer carried by the server. CSRF is minimised when using token-based authentication, you're dealing with several APIs used by various clients. However, a user's access cannot be revoked and the token consumer is responsible for the token's safety.

5.5. Single sign on (SSO)/OAuth based authentication

SSO authentication, users are only required to login to their account once to gain access to all of their applications, for example the initial login to a personal computer. Another well-known example is Google, where one can log in to Gmail and have access to all of their Google Drive applications. For example, a user is attempting to use Google Forms, if the current user is already logged in with the information, Google will send a request to the forms, which in turn calls an authentication service to make sure that the user is logged in. If they are not logged in, it shows the user a login screen to verify ID (See figure 11).

OAuth2 authentication is token based and a more complex variant of Oauth. Examples of OAuth2 authentication include Facebook, Google, or Twitter. This method has two pairs of credentials for authentication: client credentials and user tokens.

1. A user submits a request for authentication to a third-party service, such as Google or Facebook
2. If the Google server identified that the user has a Google account, it replies with an access grant
3. The requesting application makes advantage of the authorisation grant to gain access to certain data
4. The program generates an access token after receiving authorisation
5. The client uses the access token to gain access to a resource

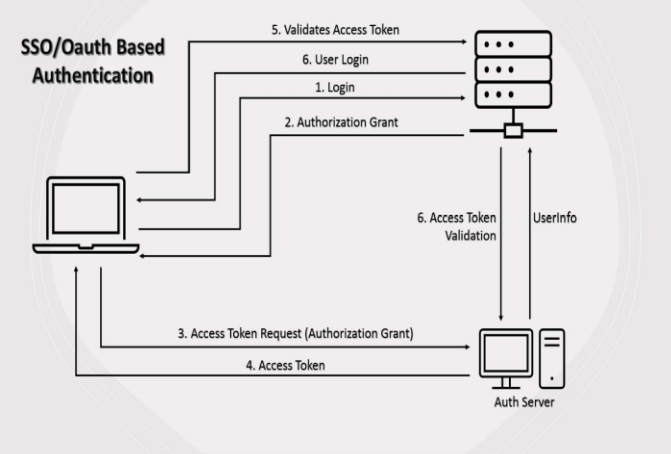

Figure 11. SSO/OAuth based authentication.

5.5.1. SSO vs OAuth

The two are similar in operation, however, the main distinction is that OAuth only gives specific access to an application, whereas SSO permits full access to all data. Advantages of SSO are focused on user experience, only one set of passwords must be remembered by the user. The password is held by a single provider that is responsible for its security. Unfortunately, if an authenticator goes offline, all of the applications that rely on it are rendered inaccessible. Any vulnerability in the authentication mechanism might provide users access to many applications and data.

6. Conclusions and future directions

Authentication is more important than ever before and user authentication is a significant factor of a secure system. Even after the development of advanced authentication mechanisms, such as biometrics, the use of simple passwords is still the most widely accepted means of authenticating user authentication. MFA is one of the most secure ways to authenticate when compared to SFA and 2FA. It incorporates multiple factors of which several are chosen.

Online banking is considered generally preferred by both provider and customer. The provider can reduce overall costs and overheads required in bricks and mortar premises and staff. For the customer it is access to services from anywhere at any time. The advantages of Internet banking services are characterised by a user-friendly environment, fast transfers and processing transactions in real time. Such services also remove existing time and location restrictions. Internet banking has some disadvantages, for example, phishing, incursion, malware attacks and other illegal activity can all affect bank accounts. Before allowing access to online banking systems, more banks utilise a trustworthy form of verification. To secure

clients' credentials from unauthorised access and cybercriminal associated activity, most banks utilise at least 2FA or MFA. Mal-actors are continuously trying to come up with new ways to intercept banking data. Banks are looking at at biometric authentication technologies to prove customers' identities, however, these procedures may result in slower financial transactions and increased preventive maintenance expenditures. More extended research could also include a thorough cost-benefit analysis of the various techniques available, such as smart cards, a dynamic password, and Biometric data. The conclusions of such studies may have an impact on the banking industry's deployment of related technologies, in order to create the appropriate combination of security factors.

In the digital age, most people will depend more on biometrics to supplement traditional passwords in terms of system security and authorisation. Despite the fact that privacy, security, usability, and accuracy concerns remain, when it comes to gaining access to sensitive information, MFA arises as a strategy that gives contemporary consumers the safety and reliability they demand. The lack of interrelation among the user profile and the smart sensors inside the biometric electronic device/system is now one of the most significant MFA issues. In terms of security, this connection must be created so that access rights are granted only to the genuine operator, i.e., someone whose identity has been verified in advance. Simultaneously, the MFA procedure should be as simple as possible. Biometrics play an important role in the MFA mechanism and can considerably enhance identity protection by combining the knowledge and possession factor with multimodal biometric elements, making it harder for a hacker to spy on a system while posing as someone else. From the standpoint of user experience, the fingerprint scanner is already the most commonly integrated biometric interface. This is mainly due to smartphone producers' extensive embrace of the technology.

Novel MFA methods that combine techniques from several sectors could also be applied to the Banking or Health sector. The importance of those methods is to not change the business processes too much, be efficient and also easily applicable to several systems and platforms. A novel method entitled 2FHA (two factor honeytoken authentication mechanism) was recently proposed that combines honeytokens and 2FA in order to offer increased level of security without compromising user friendliness and efficiency [30, 31].

Biometrics are undoubtedly one of the most important levels in enabling the evolution of MFA. This functionality is frequently viewed as an additional part, rather than a replacement for, traditional authentication mechanisms such as passwords and PINs. Mixing more than two authentication systems when authenticating a user is expected to improve security. The predicted evolution of MFA is concentrated on mixed biometric systems that give a much-enhanced user experience and MFA system bandwidth, that would be advantageous for a range of

implementations. All three sorts of factors, namely knowledge, biometrics, and ownership, will be intelligently coupled in such systems. This work has studied the progression of authentication from SFA to 2FA to MFA. We concentrate on the MFA methods as these make up the state-of-the-art mechanisms. Enhanced authentication is clearly required. Instead of supporting 2FA based on text messages and OTPs, more focus should be put on password-less alternatives based on public key cryptography, which provide significantly greater security and assurance. Because there is such a pressing need to make authentication safer and easier, companies are working hard to develop innovative solutions. While it's too early to determine which solution will eventually replace the current system, it's certain that things will grow to be far more secure and user-friendly than the password-based strategy we've been using for the past half-century. The future of authentication isn't in the techniques themselves: the industry still uses passwords and is not planning to eliminate it at all costs if they are given the option. Rather, the future lies in a pragmatic approach to dynamically managing identities and authentication processes at the company level, because the password is still useful. Understanding this and utilising many other security-enhancing support techniques is the new frontier.

Conflict of Interest

The authors declare no conflicts of interest.

References

1 Jensen W. Authenticating users on handheld devices. In: *Proceedings of the Canadian Information Technology Security Symposium*. 2003.

2 Jhansi Rani CH, Shammi Munnisa SK. A survey on web authentication methods for web applications. *Int J Comput Sci Inf Technol*. 2016;7(4):1678–1680.

3 Shteingart H, Gordon AN, Gazit J. Two-factor authentication. In: *Microsoft technology licensing*. Redmond, WA (US): LLC; 2016.

4 Tsai C-H, Su P-C. *The application of multi-server authentication scheme in internet banking transaction environments*. Germany: Springer-Verlag GmbH; 2020.

5 Azrour M, Mabrouki J, Guezzaz A, Farhaoui Y. New enhanced authentication protocol for internet of things. *Big Data Min Anal*. 2021 March;**4**(1):1–9. doi: 10.26599/BDMA.2020.9020010.

6 Dasgupta D, Roy A, Nag A. *Advances n user authentication*. 1st ed. USA: Springer International Publishing; 2017.

7 Velásquez I, Caro A, Rodríguez A. Authentication schemes and methods: A systematic literature review. In: *Information and software technology*. Chile: Chillán; 2018.

8 Kun AL, Royer T, Leone A. Using tap sequences to authenticate drivers. In: *Proceedings of the 5th International Conference on Automotive User Interfaces and Interactive Vehicular Applications – AutomotiveUI '13*. 2013. p. 228–231.

9 Khan SH, Ali Akbar M, Shahzad F, Farooq M, Khan Z. Secure biometric template generation for multi-factor authentication. *Pattern Recognit*. 2015;**48**(2):458–472.

10 Busold C, Taha A, Wachsmann C, Dmitrienko A, Seudié H, Sobhani M, Sadeghi AR. Smart keys for cyber-cars: Secure smartphone-based NFC-enabled car immobilizer. In: *Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 18–20 February 2013*. New York: ACM; 2013. p. 233–242.

11 Urien P, Piramuthu S. Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks. *Decis Support Syst*. 2014;**59**(3):28–36.

12 Thullier F, Bouchard B, Menelas B-A. A text-independent speaker authentication system for mobile devices. *Cryptography*. 2017;**1**(3):16.

13 Kevin BW, Burge MJ. In: Bowyer KW, Burge MJ, editors. *Handbook of iris recognition*. London: Springer London; 2016.

14 Phan D, Siong LY, Pathirana PN, Seneviratne A. Smartwatch: Performance evaluation for long-term heart rate monitoring. In: *International Symposium on Bioelectronics and Bioinformatics (ISBB)*. 2015. p. 144–147. 10, 2015.

15 De Luca A, Lindqvist J. Is secure and usable smartphone authentication asking too much? *Computer*. 2015;**48**(5):64–68.

16 Guzman AM, Goryawala M, Wang J, Barreto A, Andrian J, Rishe N, Adjouadi M. Thermal imaging as a biometrics approach to facial signature authentication. *IEEE J Biomed Health Inform*. 2013;**17**(1):214–222.

17 Hu S, Choi J, Chan AL, Schwartz WR. Thermal-to-visible face recognition using partial least squares. *J Opt Soc Am A*. 2015;**32**(3):431–442.

18 Banerjee SP, Woodard D. Biometric authentication and identification using keystroke dynamics: a survey. *J Pattern Recognit Res*. 2012;**7**(1):116–139.

19 He D, Zeadally S. Authentication protocol for an ambient assisted living system. *IEEE Commun Mag*. 2015;**53**(1):71–77.

20 Siswoyo A, Arief Z, Sulistijono IA. Application of artificial neural networks in modeling direction wheelchairs using neurosky mindset mobile (EEG) device. *EMITTER Int J Eng Technol*. 2017;**5**: 170–191.

21 Kraus L, Antons JN, Kaiser F, Möller S. User experience in authentication research: a survey, 2016.

22 Katsini C, Belk M, Fidas C, Avouris N, Samaras G. Security and usability in knowledge-based user authentication: A review. *ACM Int Conf Proc Ser*. 2016;1–6.

23 Harby FA, Qahwaji R, Kamala M. End-users' acceptance of biometrics authentication to secure E-commerce within the context of saudi culture: Applying the utaut model. In: *IT policy and ethics: concepts, methodologies, tools, and applications*. vol. 3-3, 2013. p. 225–246.

24 Belk M, Fidas C, Germanakos P, Samaras G. The interplay between humans, technology and user authentication: A cognitive processing perspective. *Comput Hum Behav*. 2017;**76**: 184–200.

25 He D, Zeadally S. Authentication protocol for an ambient assisted living system. *IEEE Commun Mag*. 2015;**53**: 71–77.

26 Azam F, Yadav SK, Priyadarshi N, Padmanaban S, Bansal RC. A comprehensive review of authentication schemes in vehicular ad-hoc network. In: *IEEE Access*. vol. 9, 2021. p. 31309–31321. doi: 10.1109/ACCESS.2021.3060046.

27 Gomez-Barrero M, Rathgeb C, Galbally J, Busch C, Fierrez J. Unlinkable and irreversible biometric template protection based on bloom filters. *Inf Sci*. 2016;**370–371**: 18–32.

28 Raja KB, Raghavendra R, Stokkenes M, Busch C. Multi-modal authentication system for smartphones using face, iris and periocular. In: *Proceedings of 2015 International Conference on Biometrics, ICB 2015*. 2015.

29 Sanmorino A, Yazid S. A survey for handwritten signature verification. In: *Proceedings of the 2nd International Conference on Uncertainty Reasoning and Knowledge Engineering (URKE), Jalarta, Indonesia*. 2012 August. p. 54–57.

30 Papaspirou V, Maglaras L, Ferrag MA, Kantzavelou I, Janicke H, Douligeris C. A novel two-factor honeytoken authentication mechanism. In: *2021 International Conference on Computer Communications and Networks (ICCCN)*. Piscataway, NJ: IEEE; 2021 July. p. 1–7.

31 Papaspirou V, Papathanasaki M, Maglaras L, Kantzavelou I, Douligeris C, Ferrag MA, Janicke H. 2021. Cybersecurity revisited: honeytokens meet google authenticator. arXiv preprint: https://arxiv.org/abs/2112.08431.