ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

ΣΥΓΧΡΟΝΕΣ ΜΕΘΟΔΟΙ ΕΛΕΓΧΟΥ ΤΑΥΤΟΤΗΤΑΣ: ΜΙΑ ΟΛΟΚΛΗΡΩΜΕΝΗ ΕΡΕΥΝΑ

Παπαθανασάκη Μαρία

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων
Κολομβάτσος Κωνσταντίνος

Συνεπιβλέπων
Μαγλαράς Λέανδρος

Λαμία, 2022

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

MODERN AUTHENTICATION METHODS: A COMPREHENSIVE SURVEY

Papathanasaki Maria

Master thesis

Supervisor
Kolomvatsos Konstantinos

Scientific Advisor
Maglaras Leandros

Lamia, 2022

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

Σύγχρονες Μέθοδοι Ελέγχου Ταυτότητας: Μια Ολοκληρωμένη Έρευνα

Παπαθανασάκη Μαρία

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων
Κολομβάτσος Κωνσταντίνος

Συνεπιβλέπων
Μαγλαράς Λέανδρος

Λαμία, 2022

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Η ΔΗΛΟΥΣΑ

Ημερομηνία

Υπογραφή

MODERN AUTHENTICATION METHODS:
A COMPREHENSIVE SURVEY

Παπαθανασάκη Μαρία

Τριμελής Επιτροπή:

Ονοματεπώνυμο: Κολομβάτσος Κωνσταντίνος

Ονοματεπώνυμο: Λουκόπουλος Αθανάσιος

Ονοματεπώνυμο: Τζιρίτας Νικόλαος

Επιστημονικός Σύμβουλος:

Μαγλαράς Λέανδρος

Index

1. Introduction – Brief history of authentication

Daily, we authenticate ourselves many times. Simply by displaying ownership of the key, we authenticate ourselves to the place we are entering each time we unlock the door with a key. When we use a bankcard to make a purchase, we authenticate ourselves by having the card and knowing the Personal Identification Number (SFA). The issue of authentication became more essential with the invention of the computer. It is up to cryptographers to devise appropriate procedures.

Impersonation of a user is among the most critical security hazards to any computer. The first defense mechanism against this attack is user authentication, which consists a critical constituent of any security system. On a computer system, authentication is the procedure of successfully validating the identity of a person or device [1]. The data that is used to confirm a user's identification can be classified into three classes: knowledge-based (e.g., passwords), those based on the possession factor (e.g., smart cards) and those that originate from the inheritance factor. Even though other factors are also suggested in the previous published work, such as the use of social networks and location-based verification, the factors that were mentioned above are the most widely known factors [9][10].

The concept of authentication was born much earlier than the first written proof of its existence. Since the creation of the human species there has been a need to identify members of the tribe mainly through the use of watchwords. This technique of authenticating people continued in the following centuries until the fall of the Roman Empire. Until then, watchwords had been created that included words, numeric codes, gestures, or a combination of the above.

Eighty-six years have passed since the creation of the first computer in 1936, the Z1, by Konrad Zuse, during which time the development of computers has been rapid. Twelve years later, in June 1948, the first electronic stored-program computer, the Small-Scale Experimental Machine (SSEM), was released. In the following years the use of computers, although in its early form, was limited exclusively for use by universities and researchers. Their large size and difficulty in use did not allow them to spread for widespread use. In the early 1960s, there were universities that made it possible for students to use a computer to perform complex calculations and conduct research. More specifically, MIT constructed time-sharing operating systems such as the Compatible Time-Sharing System (CTSS) to let several users share a single computer's resources. Users mainly used dumb terminals to communicate with these centralized computers at the time. Many users would sometimes share one of these terminals to transfer their tasks to

the mainframe, resulting to the problem of shared file systems. So, what was the best way for one person to keep his or her files hidden from other users? In 1961, Fernando Corbató, an MIT researcher and one of the founders of CTSS, resolved the issue by encrypting user data on this multi-user time-sharing system with passwords. Allan Scherr, an MIT Ph.D. researcher, discovered relatively soon a significant weakness that had the codes storing. Each server-based system that authenticates users using a password stores the passwords in a specific location. Scherr located this site and the file that contained the passwords of all the users, printed it and gained access to all the accounts.

More than 50 years ago, humanity used passwords to authenticate to computers for the first time, but they quickly revealed several issues that the industry needed to address in order to make them more secure. Regardless of the fact that encryption and authentication are distinct ideas, they use resemble technologies and work in tandem. Another important era for authentication was the 1970s, when Bell Labs researcher Robert Morris devised a method to safeguard the Unix operating system's master password file. It is definitely not a wise suggestion to save credentials in a clear .txt file, as we discovered from the CTSS password breach. Morris utilized a cryptographic technique known as a hash function to save passwords in such a way that computers had still the ability to check them without keeping the passwords themselves. This basic concept was adopted by the majority of other operating systems, and it continues to expand with supplementary safeguards. As hackers figured out how to "brute-force" hash algorithms, the industry has emerged improved hash functions and included extra randomization components, which are called salts, to make hashes more unique. In summary, Morris' creation of hash-based password storage methods in the 1970s significantly improved the security of authentication systems.

Other cryptographic approaches, in addition to hashes, 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 for the first time. While those discoveries 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 developed new ways to exploit passwords since more digital systems depended on them for protection. As a consequence, the industry is always seeking for new ways to safeguard authentication. 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 checked in? One-time passwords are the name for this concept (OTP). Some are time-based (TOTP), yet others (HOTP or event-based) base the next password (HASH) on the preceding one, and so on. Various researchers developed strategies to distinguish humans from computers in the late 1990s. These techniques were dubbed CAPTCHAs. CAPTCHAs cannot be used to authenticate humans, but they can be used to protect against some automated authentication assaults.

The time for MFA has come, which is still under development, and gained a lot of traction in the 2000s. Passwords were the most used form of digital authentication in the 2010s. They are, however, displaying their age and frailty. Passwords are a good authentication mechanism when used properly and in accordance with strict security guidelines. The issue is that most people do not follow the onerous 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. Multi-Factor Authentication (MFA) is able to help fix this problem, but to this day, authentication systems and alternatives were prohibitively expensive or difficult. That is where cellphones came in, paving the way for the authentication of the future. In the 2010s, the widespread availability of smartphones made biometrics and two-factor authentication technologies more accessible to the general public.

1. Why authentication is important

Mobile services that may now be accessible from anywhere on the earth have been influenced by the gradually increasing range of smart gadgets and the consequent connectivity loads. Authentication is the first enabler in such a linked society for keeping transmitted data secure [54].

Authentication is a procedure wherein a user recognizes his identity by providing x to the system, which the system then verifies by calculating F(x) and comparing it to the saved value y. Despite the fact that, from an information technological standpoint, a basic password in not any more the primary need for validating a user, his definition has remained mostly unchanged in the long run. Authentication, whether offline or online, is still an important protection against unwanted permission to the device or other critical application. Physical presence, such as the application of the wax seal [55], was used to validate transactions in the past. With the growth of our society, it has been established that validation relied just on dispatcher identification is not sufficient on a worldwide magnitude [56]. To authenticate the subject, only one factor was used firstly. On account of its lack of complexity and easiness to use, Single-Factor Authentication (SFA) was extensively applied by the society back then. For instance, using a password (or a PIN) to verify the user ID's ownership could be explored. This appears to be the most vulnerable stage of authentication [57,58].

The account can be immediately compromised if the password is shared. Furthermore, an unauthorized user can employ the dictionary attack, or social engineering techniques to acquire access. When using this method of authentication, the minimum password complexity requirement is usually taken into account [59].

Furthermore, due to a variety of security concerns, it was found that SFA is insufficient to offer effective security. Two-Factor Authentication (2FA) was recommended as an intuitive step forward, combining representative data (username/password combination) with a personal ownership factor, as a smartwatch [60]. To link an individual with existing credentials, three different types of factor groups are currently available [61]:

1. Ownership factor – a thing that the user has, such as cellphones.
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 behavior.

Subsequently, MFA was suggested as a way to supply a higher degree of security and make it easier to safeguard computer equipment and other vital services from unauthorized access by

combining at least three types of credentials. Multi Factor Authentication mostly relies on biometric or behavioral data. Users were needed to give confirmation of their identification, which was based on more than two independent variables, which strengthened security [62].

MFA is now expected to be used in areas with higher-than-normal safety standards. Sixty eight percent of European citizens are complaisant to use biometric authentication as a payment method, according to SC Media UK. Consider the daily practice of withdrawing cash from an Automated Teller Machine (ATM). To enter a personal account and withdraw money, the user must submit a physical token that represents the ownership factor, while the knowledge factor is represented by a PIN code. This system might easily be made more complex by adding an additional route, such as an OTP be entered once the user credentials have indeed been provided. [63].

Facial recognition technologies could be used in a more intriguing setting. Furthermore, according to a recent survey, thirty percent of businesses want to use the MFA solution in 2017, with fifty one percent reporting that they already use it and thirty eight percent claiming that they use it in "certain areas" of operations [64]. Multi-factor authentication, based on this information, appears to be a very feasible strategy for authentication development. Authentication among a person and the vehicle he owns, may be considered as a fascinating upcoming tendency. According to data [65], a vehicle is stolen every 45 seconds in the United States. The immobilizer key is still the current authentication technique for powering and using the car. The MFA has the ability to increase availability to most electronic gadgets, both in terms of security and user friendliness.

MFA implementations can be categorized into 3 classes according to their commercial relevance:

(i) commercial applications [66], including account login, e-commerce, Automated teller machine

(ii) governmental applications, like id card, government ID, passport, driver's license

(iii) forensic applications, including criminal cases, missing people.

The number of authentication options is rather large in general. Today, MFA is essential for:

- validating the user's identity and the electronic device's (or system's) identity
- ensuring that the infrastructure link is secure and

- verifying the linked IoT devices, such as smartphones, wearables, and many other digital tokens.

The absence of connectivity among the person's ID and the ID's of smart sensors in the device, is one of the most critical MFA challenges. Only the legal user, i.e., one whose identification has been verified beforehand, should be granted access permission. Simultaneously, the MFA procedure has to be as straightforward as possible, for instance:

1. To activate and administer services, users should initially register to the service supplier and authenticate themselves.
2. After gaining access to the service, the user must complete a SFA with a token signed beforehand by the service provider.
3. After being admissible by the system, the user authenticates by logging in with the same credentials as set up in the customer portal previously. Secondary authentication factors can be enabled by the managing platform for added security. The framework automatically checks the validity to the service platform once they have completed all of the tests.
4. Because secondary authentication relies in biological data based Multi Factor Authentication, the client will only be required to input a passcode if the MFA fails.

4. Single factor authentication

The most widely used authentication technique is passwords. Passwords are made up of 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. Extremely simple passwords, which may also include the username of the user, are vulnerable to phishing attacks.

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 prioritize ease over safety. Numerous people choose easy passwords rather than secure ones. Last but not least, passwords have numerous flaws and are not effective for protecting data that are transferred via internet. Hackers can simply guess a user's username and password by attempting all possible combinations until one matches.

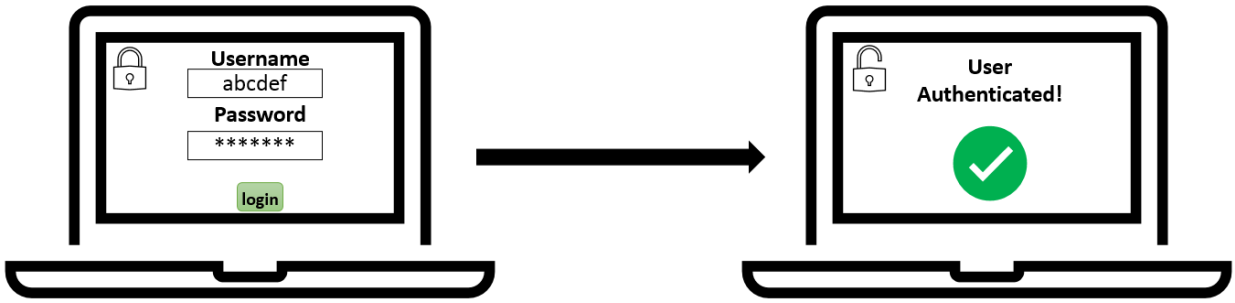

Figure 1: Single factor authentication.

5. Two-factor authentication

The authentication of two or more factors (two factor / multifactor authentication), is a method of further identification of the user, offering more security. The application of this method of identification requires an electronic device such as a mobile phone, tablet, or computer. This device will be sent an additional code, in addition to the classic one chosen by the user and will be asked to fill in it in a special form. Thus, if someone steals the user's classic password, he will need to fill in the additional code that will be sent to a device of the user, to which the interceptor does not have access. This ensures the security of the user's personal data.

We find authentication mainly in applications and services which require the user to register in order to access them. Upon entering later, he should enter the password he had chosen during registration, which may be some alphanumeric, fingerprint, facial recognition, or something else. This is the way in which it is certified that the user is the same, since only he has knowledge of the password, thus creating the first level of authentication, the one factor authentication.

Nowadays, however, it is necessary to have further levels of security, since attacks are becoming more and more targeted, with better organization and more serious consequences. Especially for accounts involving banks, or platforms containing the user's personal data, it is now imperative that there is more and deeper control over the identity of the person attempting to enter them.

So, we come to the point where in our everyday life in most applications, mandatory or not, the user is asked to secure his account in two or more ways. In the case of one factor authentication, as an "extra code" could be used:

- "Something the user has", such as a smart card,
- "Something the user is", such as his biometric features, or
- "Something that the user knows", like a code that he creates himself and only he knows.

Thus, after the completion of the first step of authentication, the second one follows, in which the user is usually asked to enter upon entry, One Time Password (OTP), which is sent to him through email, SMS, or other way of sending a message [7].

With these steps, 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 maximize security, and we come in this way to multifactor authentication (MFA).

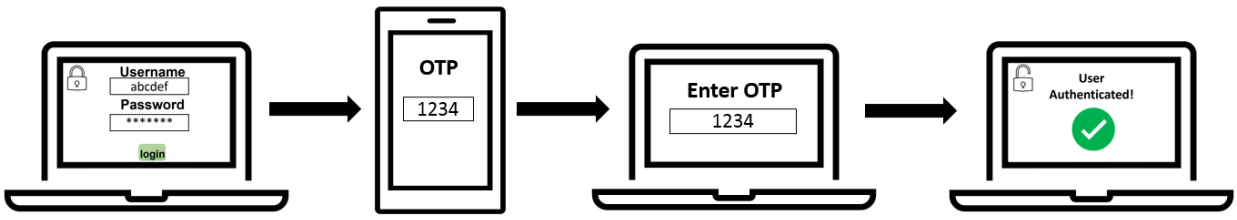

Figure 2: Two-factor authentication.

6. Multifactor authentication

Usually, the MFA finds greater use in banking systems, where the need to maximize security is particularly important, in which case three or more safeguards protect the data of the utmost importance. MFA is mainly based on unique biological characteristics of the user, such as fingerprint or iris reading, which is why to date these techniques are inviolable, but at the same time particularly accurate in their creation and maintenance [8]. Biometrics contribute in the MFA scheme and pairing the knowledge factor with biometric factors can significantly increase identity proofing, making it hard for a fraudster to overhear on a system while acting as if he is someone else. Though, using biological elements entails several drawbacks, mostly in terms of ease of use, which has an important impact on the MFA system's usefulness.

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. It should not, however, be used as an independent authentication procedure. However, using biometrics frequently necessitates the employment of a number of different sensing equipment.

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. Another issue is that biometrics use is based on a binary choice method.

From the perspective of authentication, this has been widely researched in conventional statistical decision theory during the last few decades. A slight disparity between the measured biometrics and the data that were recorded in earlier acquired instances, can be controlled in a number of ways. False accept rate (FAR) and false reject rate (FRR) are both extensively used approaches. Manipulation of decision criteria enables the authentication framework to be adjusted based on established costs, risks, and advantages. FAR and FRR are extremely important to the MFA operation because getting zero values these two metrics is nearly impossible. The assessment of many biological related features to identify an individual's identity can greatly improve the MFA system's operation.

The MFA approach allows a wide range of situations where security is paramount. Many of them are mentioned below: [9]:

1. Massive Open Online Courses (MOOCs), where it's tough to tell the difference among a registered user and a user that will take an exam or do homework. With the rise of MOOCs

at colleges, it's more essential than ever, to securely verify students' identities. Since the mixes 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.

2. Bank applications like electronic money transfer or online payments must be secured. MFA can be utilized to rapidly verify rightful users. The amount of 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.
3. 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.
4. MFA can be expanded more for use at various levels of Internet Computing. Here is a list of a few of them:
    a. Level of applicability (social media).
    b. User level (administrators, visitors).
    c. Document level (sensitive pdf's, sensitive images, videos).

6.1. The benefits of authenticating two or more factors

In general, authentication has only benefits to offer and especially when it is multilevel. We could say that in cases where we have devices for public use that require a code (e.g., security doors to companies), it is ideal to use biometric data as described earlier. In this way we bypass the two factor and multifactor authentication and ensure maximum security with one factor authentication, saving mainly time. Smart devices have now occupied a large part of our lives, and so with innovations in communication and computers, A-IoT (Advanced Internet of Things) has been created. Although the development of smart objects can enrich the daily lives of individuals, access without permission to such equipment is possibly perilous. Simultaneously, people want convenient interplay with these devices, since they use them daily, however, they must ensure the security of his data while they use it.

Security breach to A-IoT systems poses major security risks, and trustworthiness has emerged as an extremely pressing research challenge in protecting A-IoT solutions.

Authentication and user authentication are both part of the access control process. A-IoT devices can use advanced capabilities on-the-art society. Especially if the user who needs to be identified has portable devices, then these could act as providers of the identification code (e.g. OTP), or even could become the means to identify biometric data or find the location of the user. Wearable technology can offer their user's login information by connecting to the A-IoT system through short-range radio waves. This solution necessitates the adoption of effective security protocols so that the platform can authenticate the data gathered from the user's equipment. At the same time, consumers may rest certain that their personal information is kept private [10].

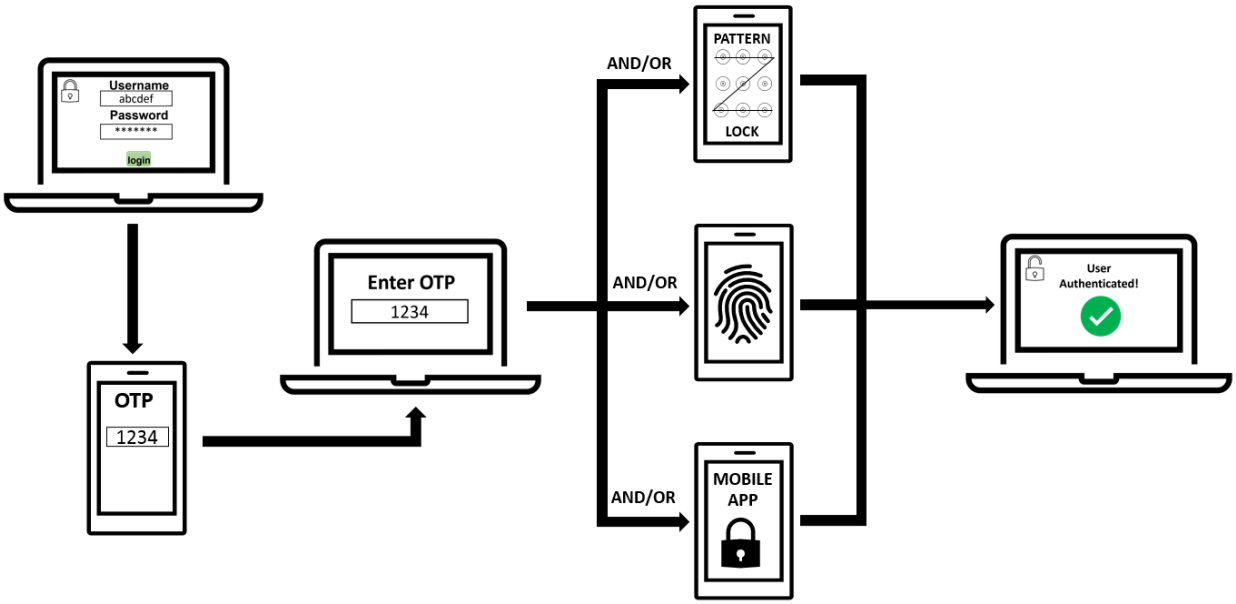

Figure 3: Multifactor authentication.

7. State-of-the-art and potential multifactor authentication sources

Currently, authentication systems make use of a large number of sensors to enable a user's identity. This chapter describes the MFA-suitable factors connected with commercially accessible sensors, as well as related issues. We also share further details on the ones which might be implemented in the close future.

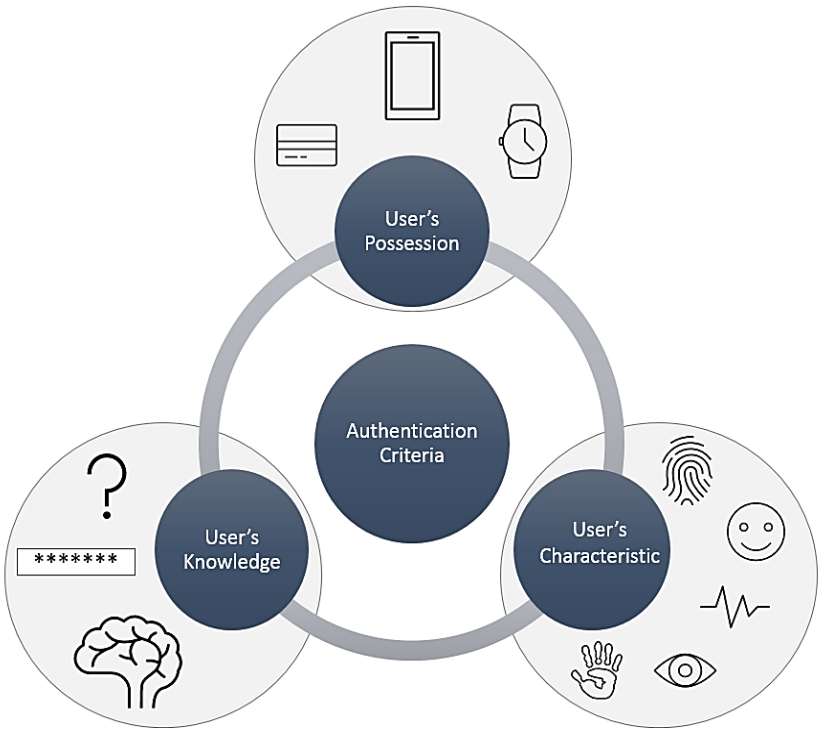

Figure 4: Authentication criteria.

7.1. Authentication Techniques

According to Velásquez, Caro and Rodríguez [11], there are about fifteen different authentication techniques that are either used individually (one factor authentication) or in combination (two factor/multifactor) authentication. Depending on the criteria mentioned before, we group together and report below these techniques:

CRITERION	TECHNIQUE
User's Possession	Smart Card
	One Time Password
	Cell Phone
	Smartwatch
CRITERION	**TECHNIQUE**
User's Knowledge	Codes in text format
	Cognitive Password
	PIN
	Questions
CRITERION	**TECHNIQUE**
User's Characteristic	Fingerprints
	Brainwaves/Heartbeats
	Hand Geometry
	Typing Biometrics
	Hand Movements
	Other

Table 1: Authentication techniques.

Studying the above table, we observe that the techniques concerning the biometric characteristics of the user are numerically more, but also more secure. However, the cost is prohibitive in most cases and that is why they are chosen only in very special and rare cases. In the case of combining two or more techniques, it is good to select one of each group-criterion and combine it with a technique from a different group [11].

It is worth noting that in many cases the user's location information is also considered. This kind of authentication procedure uses the person's location to identify them. This criterion usually uses Global Positioning System (GPS) systems, the user's IP address, or even a hive tower identifier. The system will verify the user's location whether they are allowed to connect from that place if they have the necessary credentials. This sort of authentication has the ability trace the time and location of the user's login. For instance, if someone was logged in someplace in the

globe but then appeared to be logged in somewhere else a few minutes later, maybe one of them is a fraudster, and the account should be frozen to prevent suspicious behavior [9].

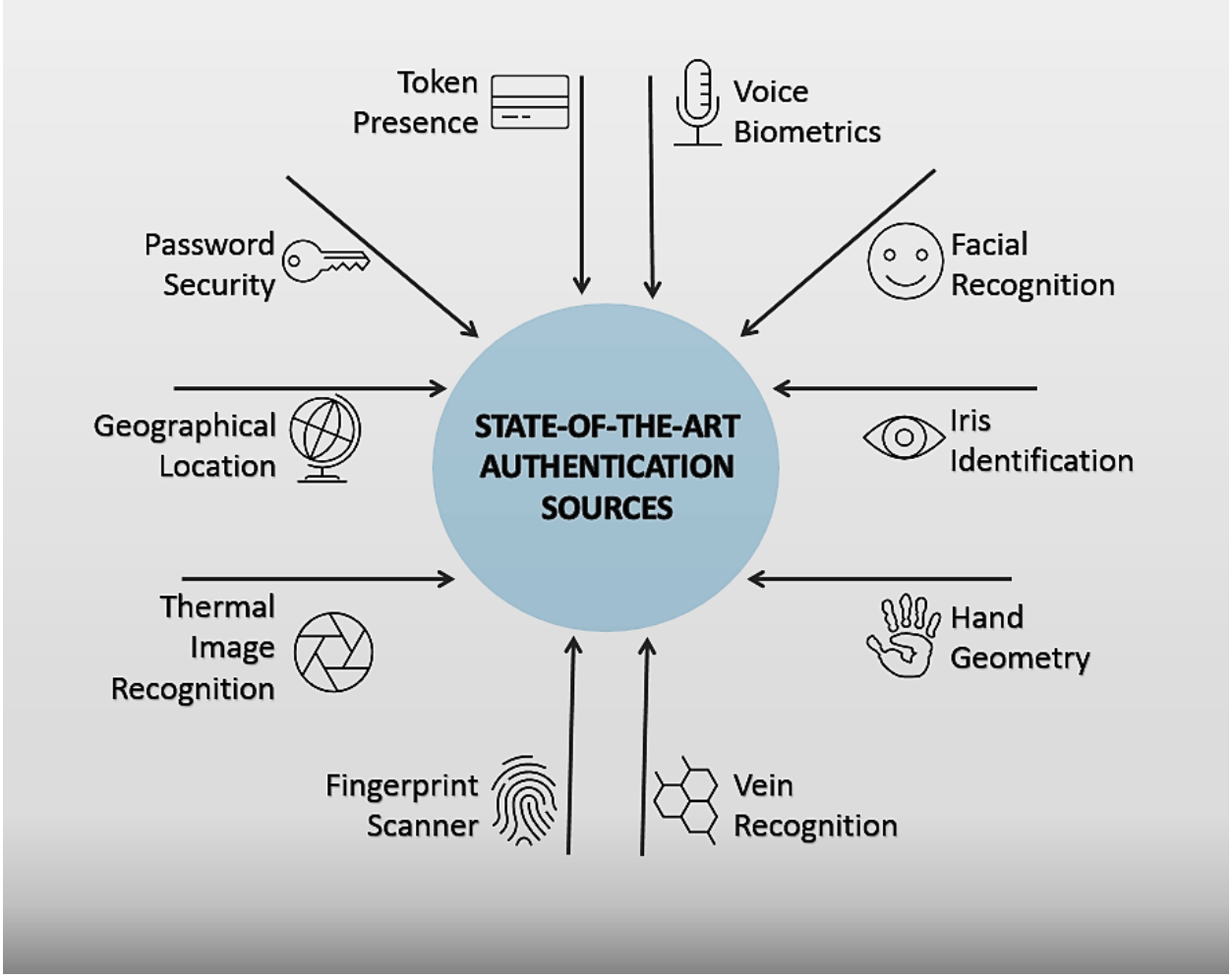

Figure 5: State-of-the-art authentication sources.

One of the most common uses of MFA nowadays is for identification and authentication while accessing sensitive data. We also mention the factors that are already available for MFA use without the need for extra specialist equipment.

Password Security

Requesting a PIN code, password, or other form of authentication is the traditional method [16]. A knowledge aspect is generally represented by the secret pass. To authenticate the user, all that is required is an input device. PIN codes are accepted globally due to their extensive adoption by ATMs and the advent of mobile phones. A-IOT (Advanced Internet of Things) systems can

intelligently make use of a password, although they have now been significantly replaced by voice, face, or fingerprint recognition.

Token Presence

The password might be augmented with a tangible token, to prove ownership [17]. A user may produce a smartcard, phone, wearable device, or other device, all of which are more difficult to delegate [18]. The system ought to be supplied with a cellular platform that allows a two-way connection with the token in this circumstance [19]. The most well-known software token, on the other hand, is the one-time program generated password. The problem of unregulated duplication is the fundamental disadvantage of the above.

Biometrics of the voice

The majority of contemporary smart electronic gadgets have a microphone, allowing people to use their voice [20]. Concurrently, upcoming technological improvements might allow special agencies both to detect speakers and recreate their voice, including pitch, tone, and other features, which would solve a key flaw in utilizing voice as a significant verification approach. A microphone is commonly included in all A-IoT devices to enable for voice recognition.

Devices are now able of discerning innumerable of different voices once they hear a short sentence, according to recent reports. However, unlike facial recognition, these methods are more sensitive to spoofing assaults. The following is a description of the attack:

Eve intercepts Alice's digital voice signal or analog and rams within it its message on the sensor that authenticates in actual time. A-IoT systems are anticipated to possess adequate computational capacity to identify the related intrusions in a timely way if a sentence is predicated on the recorded articulation of syllables and tones.

Facial Recognition

Face recognition with integrated camcorders was first developed for sightseeing assessment, which appeared to be subject to small attacks, such as showing a photograph that was not the genuine one. In relation to three-dimensional recognition, these techniques have advanced dramatically during the last twenty years. 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. If the user is asked to move his head in such a way that the subsequent pattern is not known ahead of time, the user's safety can be improved even further. Looking at the problem from a different perspective, a drone is able to allegedly fly encircling the user to create

a three-dimensional model of his full body. 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 computer with a snapshot. The following stage was to facilitate 3D facial recognition, that necessitated the user moving their head in a precise manner during the authentication process. This technology eventually developed to the point where it could identify the user's actual expressions. To allow facial recognition, the system must have at least one output device as well as a camera [21].

Methodology based on the eyes

Iris recognition is a sort of biometric identifier that takes a picture of the iris. This method analyzes data from that picture and develops patterns from it. Then he attempts to find a match in the stored data. The technique involves identifying the boundaries of the iris and detecting the position of the pupil. Also, the shape, contour and boundaries of the iris are checked, then the information merges to assemble a summary of characteristics for the iris. Retrieving the image requires a camera of very high resolution. The modern cameras that are marketed and are available for iris recognition, make use of infrared light to illuminate the iris, which however does not harm the eye in any case. Iris identification algorithms have been around for over 20 years. 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 intriguing technique. In this procedure, a fine membrane consisting of neural cells in the rear part of the eye is caught and analyzed. Each person's retina is sole due to the complicated configuration of the small blood vessels that carry blood to the retina. The two most major barriers in those technologies are the necessity for a great resolution camera and a rigorous mathematical strategy to interpret the image [22].

Retinal recognition is a sort of visual recognition in which the back of the eye is highlighted. The computer is able to obtain an accurate picture of the blood vessels since the blood vessels absorb photons differentially than the encircling tissue. When compared to iris recognition, scanning the retina takes a lot more work. Simultaneously, even the tiniest movement in the identification system necessitates even more advanced cameras than those used for iris recognition, significantly raising the cost. The following are the benefits and drawbacks of retina recognition:

Advantages:

- Fewer apparent false positives
- Almost zero false negative rates
- Verifying the user's identity is fast and reliable

Disadvantages:

- Reliability can be compromised by certain eye conditions
- The scanning process might be regarded uncomfortable
- It is not really regarded a user-friendly authentication technique
- It is the mechanism with the greatest cost in terms of equipment

In high-security contexts, retina scanning is regarded the most efficient and resilient way for authenticating users.

Geometry of the Hand

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 at present [23]. This procedure is identical to that used to determine heart rate. Hand geometry authentication can be used in lockers or interactive kiosks.

Recognition of Veins

Advances in fingerprint scanners now allow for the collection of a vein image of the finger. Palm print recognition is utilized in complex systems to capture and record the shape and movement of the complete hand [25,26]. Vein biometrics are still sensitive to spoofing attacks at this stage of elaboration [27].

Fingerprint Scanner

The bulk of smartphone/personal computer makers are now pushing fingerprint scanners as the most basic authentication mechanism. This approach is simple to use, but it's also simple to make, since our fingerprints can be collected from practically whatever we touch. This method has a lot of integration potential [28], but it's not suggested for usage as a stand-alone authentication mechanism. Instead of more secure vein recognition, most smartphone manufacturers include an extra camera to get the fingerprint.

Thermal Image Recognition

Thermal sensors, like vein recognition, are utilized to rebuild a unique thermal image of a person’s body blood flow in close proximity [29]. Many issues with this authentication method can develop as a result of the user's state of mind: sickness or emotion can have a substantial impact on the perceived figures [30].

Geographical Location

The use of the device's and user's physical positions to determine if admission to the service can be ceded is a unique situation of location-based authentication [31]. Due to the transmission characteristics of GPS signals, they can be rapidly blocked or regarded incorrect; hence, it is suggested to use more than two position providers, such as GPS and wireless network cell ID. From the standpoint of location capturing, a smartphone might be utilized to assist MFA.

MFA Integration's Future Prospects

The idea of tight MFA integration is being promoted by greater suspension of biometric services in a wide range of widely available consumer devices, in addition to accelerated adoption across numerous industries. Scientists are currently working to incorporate various sensors into MFA systems.

7.2. Behavior Detection

By examining the typing cadence of military telegraph operators, behavior identification was utilized to track military movements in the past. Since motor-programmed ability causes the motion to be planned before it is performed, modern authentication gestures can range from easy to difficult to imitate ones [31]. A current example of this type of identification is pressing the smartphone screen [32,33]. To capture and evaluate the unique characteristics of user activity, an A-IoT system can use multiple input interfaces: standard request response time, typing rate, or macro/micro-scale mobility, but it largely depends on the A-IoT device. In the case of wearables, the user behavior is retrieved by accelerometer fingerprints. As far as the drones are concerned, the user behavior characteristics include the control functions. Last but not least, smart vehicles offer a grate range of these characteristics, such as the pressure that the driver exerts on the brakes, or the placement of his hands on the steering wheel.

Because each person's typing pattern is unique, this strategy might be simply integrated with any text-input authentication mechanisms [34,35,36]. The user must reproduce a previously learnt movement while holding or wearing the sensor device if the MFA system is specifically created for programmed gesture analysis. The implementation of accelerometer fingerprinting for wearables that are extensively utilized, is a natural step of authentication [38,39]. For example, by continuously monitoring accelerometer data, each smartphone owner may be authenticated based on their stride pattern, which is nearly unachievable to spoof by someone else. For in-vehicle authentication, the integral plan was designed to observe driver features, that might be assessed through two points of view:

i. vehicle-specific behavior: speedometer, brake pressure sensor, and others.
ii. human factors: like the music they play, the calls they make, etc. Another key stumbling barrier is the alcohol sensor. When the level of alcohol in the cabin exceeds the legal limit, the engine start function may be disabled.

- **Beam-Forming Techniques**

Radio-frequency identification (RFID) and near-field communication (NFC) systems have gained significant acceptance and acceptance in the telecommunications industry [40]. Using wireless Multiple-Input Multiple-Output (MIMO) technology to track down the source of the signal could be a major discovery in authenticating the token on the human body, according to recent advances in physical-layer security.

- **Occupant Classification Systems (OCS)**

OCS technologies have been implemented into numerous vehicular systems in consumer cars. A sensor system can recognize that is presently in a seat, based on factors like as weight or posture and automatically alter the car to specific demands.

- **Recognizing electrocardiographic (ECG) data**

ECG data from someone's smart gadget might be collected and analogized 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.

- **Recognition of electroencephalographic (EEG) data**

That approach relies on the examination of brain function. It enables the collection of a one-of-a-kind specimen of a person's brain activity pattern. Medical probes underneath the cranium or wet-gel electrodes strewn across the scalp are used. EEG data acquisition could previously only be done in clinical settings. Simple EEG collection is now possible using commercially accessible devices the size of a headset [50].

- **DNA Recognition**

Human cell lines are an important research resource that are commonly employed in reverse genetics or as in vitro models of human disorders. Additionally, it is a source of one-of-a-kind DNA fingerprinting data. Despite the fact that the process is time-consuming and costly, it might be used to pre-authorize the user to the highly secure facility, among other things.

The following parameters are used to evaluate the factors/sensors:

- *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 lives.
- *Spoofing* refers to how difficult it is to collect and spoof a sample.

However, while implementing the MFA for end users, several other difficulties must be solved. We'll go over those issues in more detail in the next section, as well as formalize our proposals for improving integration ease.

Factor	Universality	Uniqueness	Collectability	Performance	Acceptability	Spoofing
Password	U	Low	High	High	High	High
Token	U	Medium	High	High	High	High
Voice	Medium	Low	High	Low	High	High
Facial	High	Low	Medium	Low	High	Medium
Ocular-based	High	High	Medium	Medium	Low	High
Fingerprint	Medium	High	Medium	High	Medium	High
Hand geometry	Medium	Medium	Medium	Medium	Medium	Medium
Location	U	Low	Medium	High	Medium	High
Vein	Medium	Medium	Medium	Medium	Medium	Medium
Thermal image	High	High	Low	Medium	High	High
Behavior	High	High	Low	Low	Low	Low
Beam-forming	U	Medium	Low	Low	Low	High
OCS	U	Low	Low	Low	Low	Medium
ECG	Low	High	Low	Medium	Medium	Low
EEG	Low	High	Low	Medium	Low	Low
DNA	High	High	Low	High	Low	Low

Table 2: MFA factors comparison: High, Medium, Low, U—unavailable

8. Multifactor authentication operation challenges

While integrating the MFA for end users, numerous other difficulties must be addressed. For both developers and managers, integrating new solutions has always been a huge difficulty. First and foremost, user acceptability is a vital component of strong identity and multi-factor authentication uptake. It is necessary to take a cautious and thorough approach while implementing and deploying MFA solutions, with the majority of issues arising from possibilities and possible rewards [51].

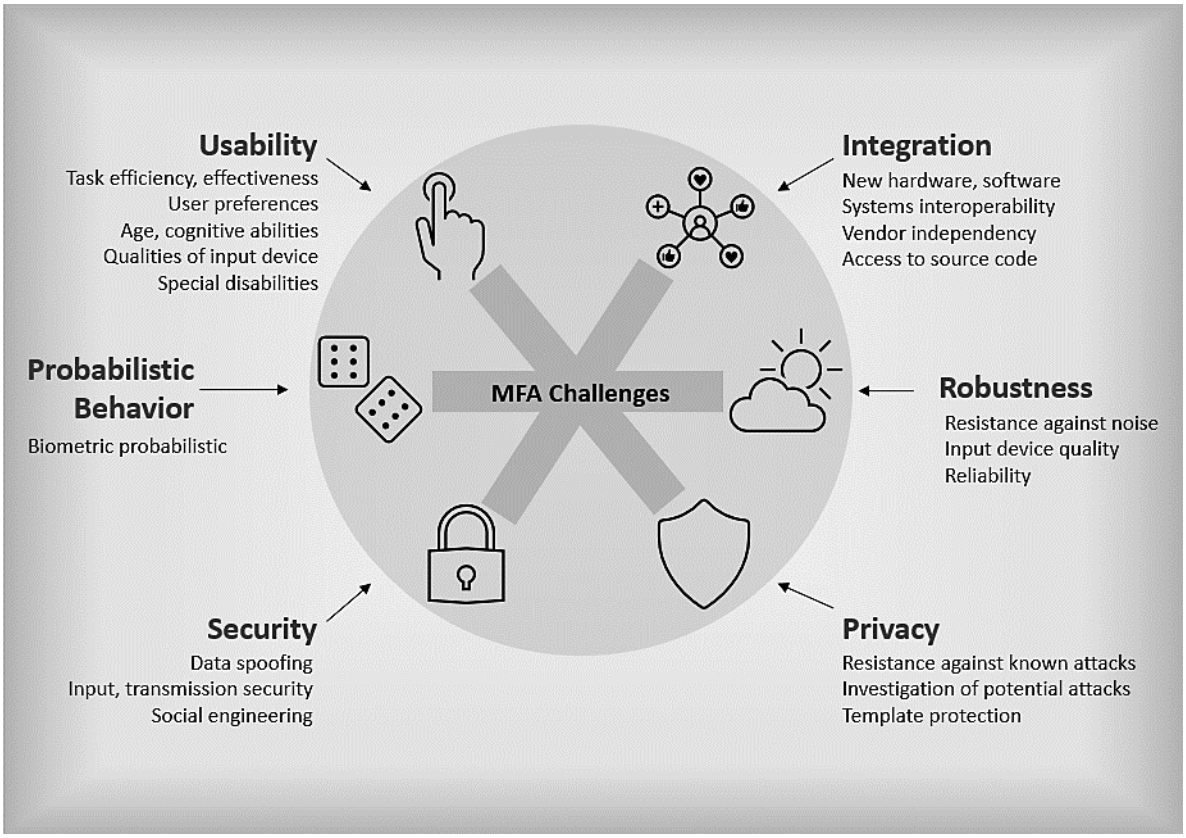

Figure 6: Main operational challenges of MFA.

- Usability

The main usability issues that arise during the authentication procedure can be classified into three categories [52]:

- Task efficiency - time for both registering to the system and for the authentication process.
- Task effectiveness - the number of times the user tries to access the system.
- User preference - if the user favors one authentication method over another.

Researchers have already begun investigating more particular effects on authentication procedures based on a number of human characteristics, in addition to the approaches discussed above. Interestingly, the authors of [53] found that gender has no effect on the results in the identical situation. Belk et al. [54] published a study comparing the task completion efficiency and effectiveness of traditional and realistic passwords. The findings revealed that using visual passwords takes longer for the majority of the participants than using text passwords. However, cognitive differences across users, such as whether they are Verbal or Imager [52], have a major impact on job completion. Text-based tasks are completed faster by Verbals than by Imagers, and vice versa. In the same two settings, Ma et al. looked at the effect of handicap (Down syndrome). Textual passwords are used more frequently than graphical passwords, according to new research. Moreover, the authentication device's features play an important part in that procedure. When compared to traditional personal computers, using a smartphone or other device without keyboard to create a password has been demonstrated to be less usable.

- Integration

Despite the fact that all usability problems are solved throughout the creation stage, integration raises additional challenges from either a technological or a human perspective.

Hardware-based MFA solutions 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 the MFA system, biometrics autonomy has to be thoroughly investigated. Biometric data resulting from sensors apart from those which were originally installed should be handled by the framework. Multi-biometrics, or the utilization 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 anytime soon. It is also very important to mention that most existing MFA solutions are not always 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.

- Security and privacy

Any MFA scheme must have sensors, storage systems, processors, and networking channels. At various levels, they are all subjected to a variety of attacks, ranging from replay efforts to adversarial attacks. Consequently, security is an important tool for allowing and preserving privacy. Therefore, we'll begin by targeting the input device directly. The society is exposed to the main MFA security risks, which are listed beneath, by permitting just the authorized controller access and processing sensitive personal data. Data spoofing is the first big threat, which the MFA system would effectively allow. Because biometrics are employed in so many MFA schemes, the intruder has a natural opportunity to investigate the sensor's technology as well as the sensor, showing the greatest spoofing materials. 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 utilize a timestamp [56,62,63]. Nevertheless, a biometric spoofing attempt is rather easy to carry out.

While biometrics may enhance the efficiency of the MFA system, they simultaneously raise the frequency of vulnerabilities that an intruder might use. There's also a danger that sensitive data will be taken throughout the transfer among the sensor and the processing/storage unit. Theft may happen as a consequence of a not secure connection from the input device to the database using retrieval and pairing blocks, and an attack is possible. To combat this type of threat, the essential data encryption criteria must be met. Capturing the secret data sample is another way to attack the MFA mechanism.

If zero-knowledge solutions are not used for knowledge factors, the system will be immediately compromised. The capture of a biometric sample, that cannot be modified or changed gradually, is of particular importance. As a result, protecting biometric data during the capture, transmission, storage, and processing phases necessitates a greater level of security.

The theft of data storage poses the following threat. Databases are typically stored in a single location, resulting in a single point of failure. Simultaneously, a few of the database's distant systems are often not allowed access to the stored personal details. To protect data against fraud, in addition to adopting irrevocable encryption, a greater level of isolation is needed [57]. Attacks based on location are a potential. It's possible that the GPS signal is blocked, or that misleading information is transmitted to the recipient, leading it to estimate an inaccurate place

or time (spoofing). Cellular and WLAN-based location services can also benefit from similar strategies.

Last but not least, the MFA system, like any other information technology infrastructure, should have a high "throughput," which assesses a system's abilities to fulfil its users' needs in relation to the number of input requests per unit of time. In the unlikely case that the biometrics are deemed appropriate in all dimensions, if the system can just make one biometrics-based match hourly and one hundred samples per hour are required, it is not viable. For the server side, the recommendation is to use appropriate processing gear.

A penetration testing panel should be able to examine the MFA security framework's potential flaws. Today, developers frequently perform external audits to assess risks and take action based on that assessment for more cautious planning. As a result, the MFA system should be evaluated in order to provide a safer environment.

- Robustness to operating environment

Despite when the security breaches are entirely handled, biometric technologies, particularly fingerprinting, have consistently failed to meet the "robustness" requirement since their inception. This was primarily owing to the operational trials taking place in a lab rather than in the field. Voice recognition, for example, was mainly reliable in a silent environment but did not succeed to authenticate a user in metropolitan settings.

Early facial recognition algorithms, for example, failed to work in the absence of suitable lighting, a good camera, and other factors. The requirement for constant supervision of the investigated subject was the flip side of the coin. Even now, there are either hints on where to look/place fingers or visual aids accessible in security checks. Failure to Enroll (FTE) and Failure to Acquire (FTA) rates are often used to assess a deficiency of experience between computer and human contact [58]. They are both affected by the users' actions in addition to the added external noise.

Because a large portion of MFA is heavily reliant on biometry, it might be characterized as intrinsically probabilistic. The field of pattern matching, which depends on approximation, is at the heart of biometric authentication. Because differences between users can be essential due to a variety of reasons and uncertainties, in every MFA system, accurate matching is crucial. The picture taken in a fingerprint scan would differ each time it was examined due to presenting angle, force, moisture, or sensor difference, even if it was taken of the same individual.

FAR and FRR are two significant error rates to consider when evaluating a biometric identification system's outcome. The fraction of frauds who are wrongly authorized to use the system as real users is referred to as FAR. The number of faulty matches to the total amount of impostor match attempts is what it's called. The number of real users who have been denied access to the system is calculated as the ratio of erroneous eliminations to the overall amount of real match tries. In addition to the previously described measures, literature advocates using the Crossover Error Rate (CER) [59]. The likelihood of the system existing in a state where FAR equals FRR is specified by this parameter. The lower this number, the better the system's performance. "Higher FAR is preferable in systems where safety is not a top priority, but higher FRR is desired in high-security applications," according to. Equal Error Rate (EER) [84] refers to the place where FAR and FRR are equivalent. Based on the foregoing, it can be stated that a system based entirely on biometrics is unlikely to be deemed a preferable MFA framework.

It is feasible to examine and appraise the overall MFA system by studying the aforementioned problems. Depending on the accessibility of a wide range of sensors in contemporary cars, we offer a strategy to facilitate MFA for vehicular integration in the following sections.

9. Web Authentication Methods

Some of the most well-known Web Authentication Methods, are the following [61]:

1. Basic Authentication

When making a request, Hypertext Transfer Protocol (HTTP) authentication, requires the client to give a username and password. Because it doesn't involve cookies, sessions, or anything else, this is the easiest way to impose access restriction. To make use of this, the client must provide the Authorization header with each request. The login and password are not encrypted, but they are built in this manner.

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

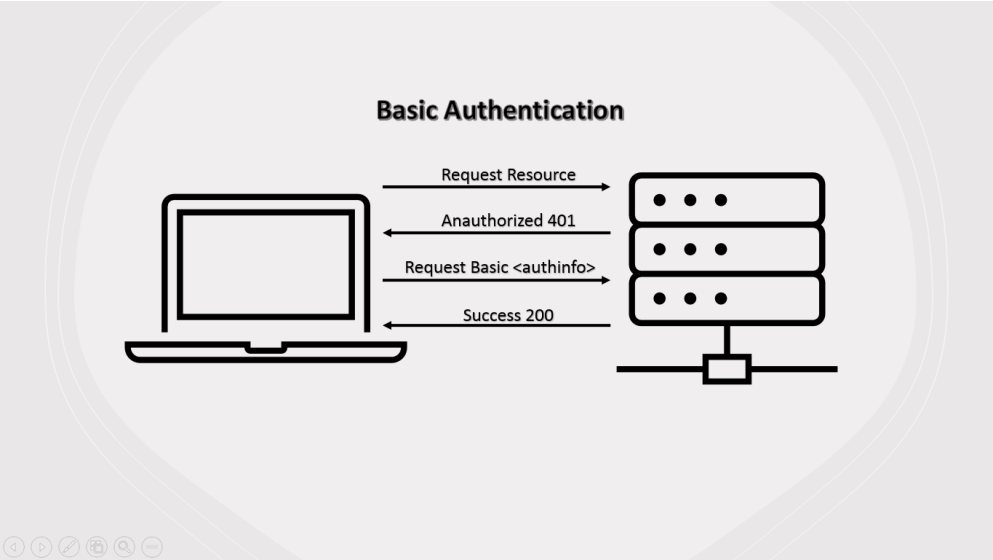

Figure 7: Basic authentication.

Advantages

- Simple to use and implement
- APIs are faster since they do not require complicated encryption or decryption.

Disadvantages

- Basic Authentication in a non-SSL (HTTPS) network is a major security flaw. Base64 is simple to decode.

- Sending passwords across all HTTP requests, creates a pool of requests from which attackers might choose passwords. Once they've cracked one, the system is vulnerable to assault.

2. Digest Based Authentication

It's a more advanced variant of Basic authentication. It addresses the security flaws in basic authentication over an HTTP network. Instead of dealing with Base64 encoded texts, the server now gives a digest that the client can use to encrypt the login details. We are no longer concerned about a Base64 encoded string being globally known in digest base authentication.

1. Request a resource from a server that does not require authentication. The header is set by the server providing digest information.
2. Get the user's 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.

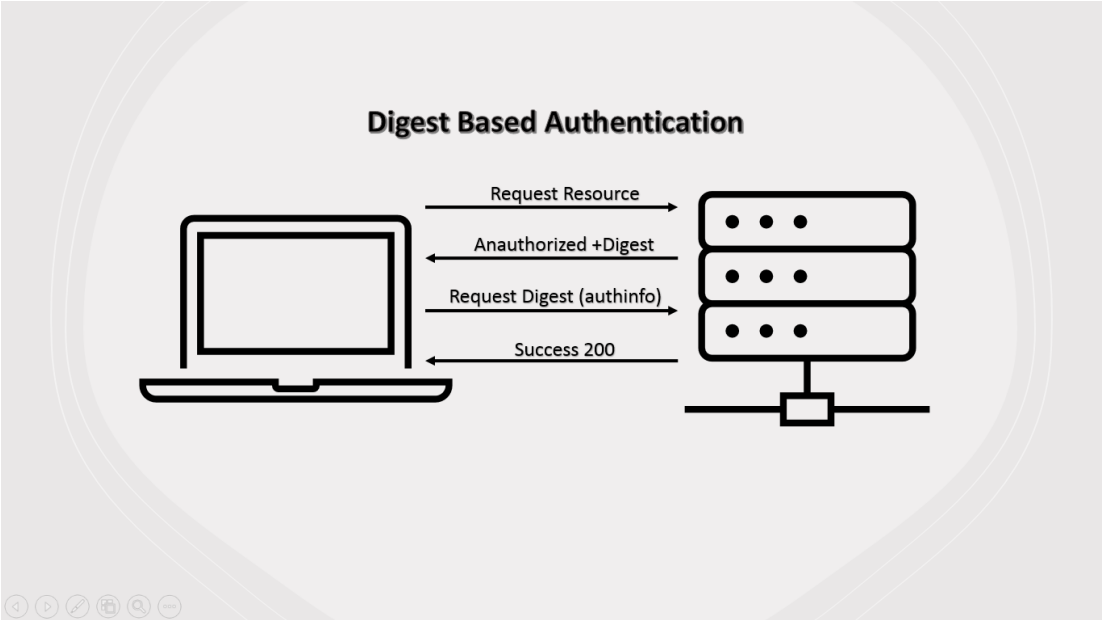

Figure 8: Digest based authentication.

Advantages

- Avoids phishing
- Prevents credentials from being sent in plain text.

Disadvantages

- Man-in-the-middle attacks are still possible with the digest approach.
- To obtain a resource, the client must make two calls: one to obtain digest data and another to login.

3. Cookie/Session Based Authentication

Cookie/session-based authentication is the most used method of authentication in online apps. 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 an HTTP request. The browser saves it in a cookie jar, and the cookie is delivered in the Cookie HTTP header with every request to the same origin. There are a few fundamental guidelines to consider when using cookies for authentication reasons. 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. What is the mechanism behind it?

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.

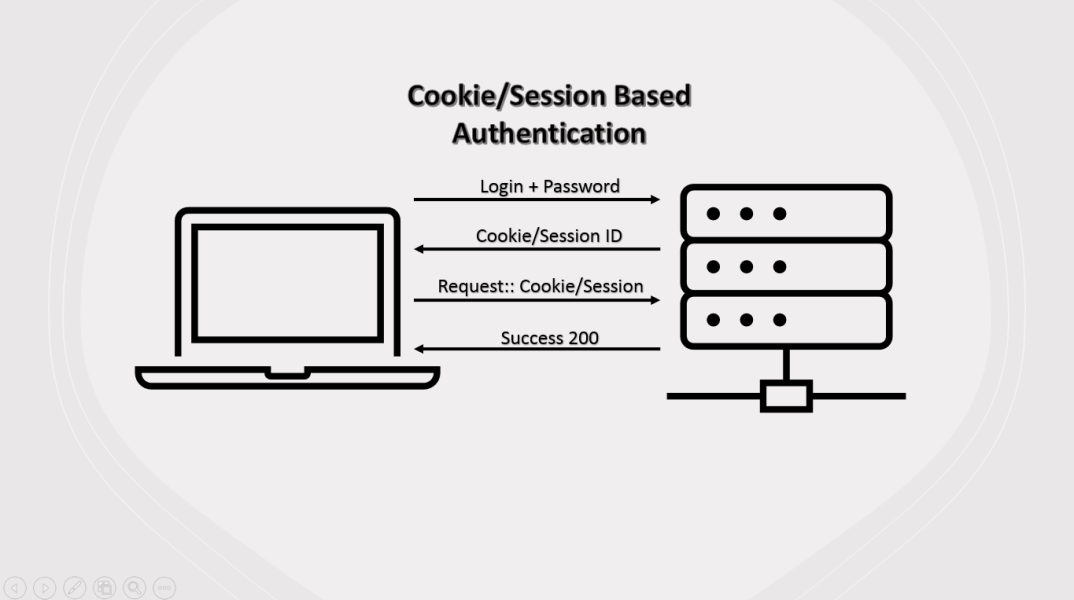

Figure 9: Cookie/Session based authentication.

Advantages

- The password is no longer set in every request, reducing the attack window.
- In a stateless system, it allows state maintenance. Cookies keep track of whether the user is signed in or not.
- A cookie's validity can be revoked.

Disadvantages

- Only a single domain system should use cookie-based authentication. User needs to deal with CSRF if he prefers a web and mobile app, or even a separate client server.
- Because the cookie is read by other applications, it is exposed to XSS and CSRF attacks.
- The session information must be stored in a database, which raises the scale issue.

4. JSON Web Token Based Authentication

Stateless authentication is a type of token-based authentication. We use a server-generated token for authentication instead of transmitting credentials. Token-based authentication includes Oauth and JWT.

JWT

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.

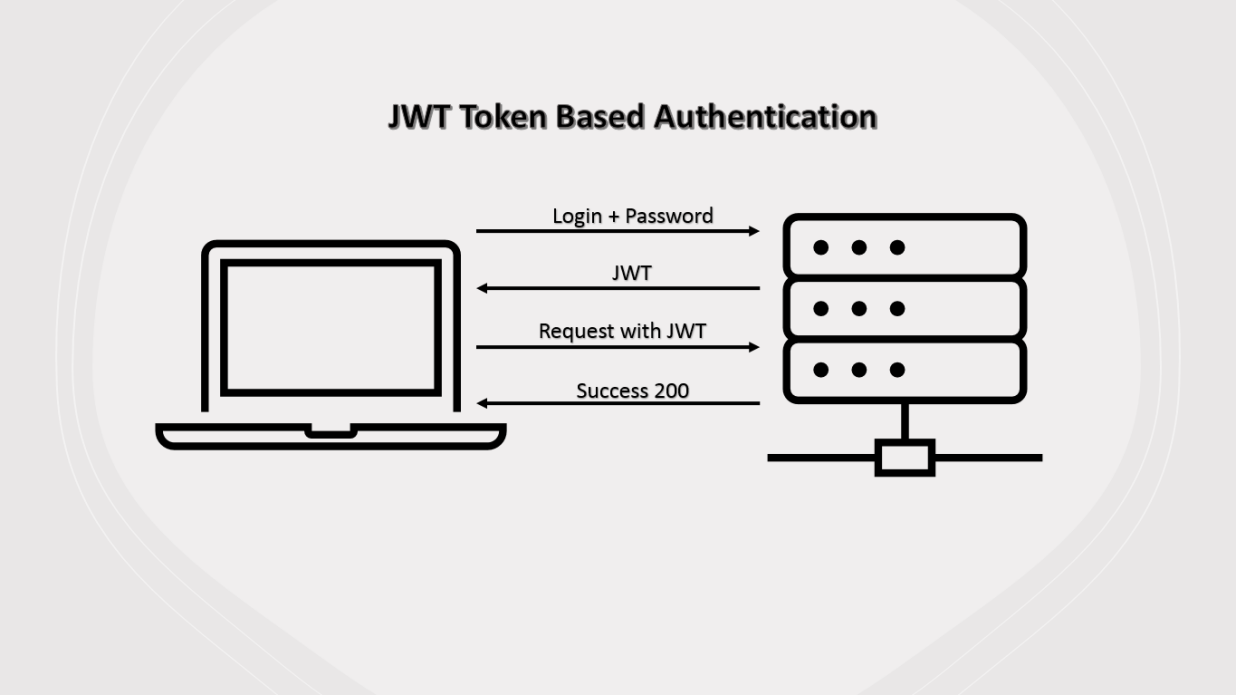

Figure 10: JWT Token based authentication.

Advantages

- The overhead of session information is no longer carried by the server.
- There will be no more CSRF. When using token-based authentication, you're dealing with a number of APIs that are used by various clients.
- On a microservices architecture, it works nicely.

Disadvantages

- A user's access cannot be revoked.
- The consumer of the token is responsible for the token's safety.

5. SSO/Oauth Based Authentication

SSO

Users only get to login to their account once to have access to all of their applications with Single Sign On (SSO) systems (e.g., Personal Computers). Another well-known example is Google, where one can log in to Gmail and have access to all his the GDrive apps.

1. Assume someone 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.
2. If he is not logged in, it shows the user a login screen to verify ID.

OAuth2

Token-based authorization is a more complex variant of Oauth2. We frequently use Facebook, Google, or Twitter to log into an app. These are some OAuth2 samples. It has two pairs of credentials for authentication, client credentials and user tokens, unlike other authentication techniques.

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

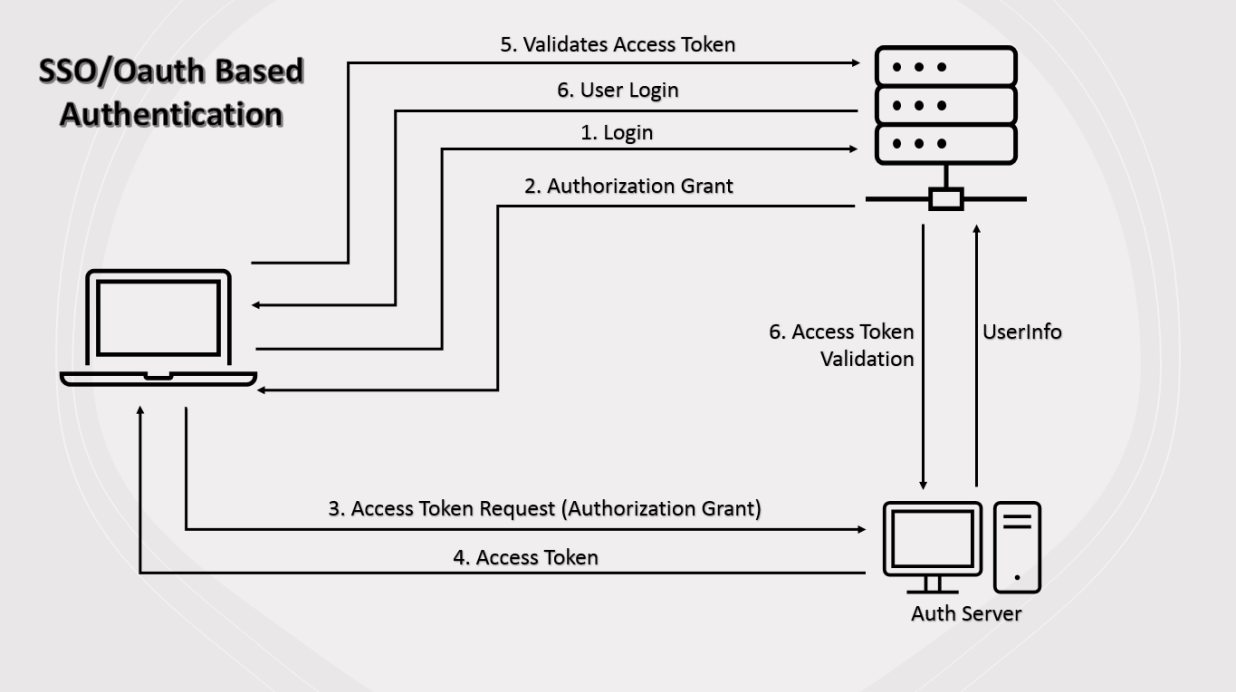

Figure 11: SSO/Oauth based authentication.

SSO vs Oauth

This seems similar to oauth, however the main distinction is that oauth only gives particular access to an app, whereas SSO permits full access to all data.

Advantages

- Let us talk about the user experience. Only one set of passwords must be remembered by the user.
- Because the password is held by a single provider that is responsible for its security.

Disadvantages

- When an authenticator goes down, all of the apps that rely on it are rendered inaccessible.
- Any vulnerability in the authentication mechanism will provide users access to a large number of apps and data.

10. Authentication: Security risks

Despite the effectiveness of sending SMS, SIM exchange is undoubtedly the number one security threat against communications, threatening the OTP mission for authentication. A SIM exchange attack "tricks" the mobile operator, usually by phone, and the customer's account is informed with information from the scammer's SIM card, convincing the provider that it is the same. its lost and access must be regained as quickly as possible to a new phone and a new SIM card. These attacks are extremely simple to occur. So long as an attacker manages to steal the victim's account, the rest of the attack is pretty easy. The attacker can perform bank transfers and other actions, in a more lawful way, as long as he receives the OTP code on his device pretending to be the victim [14]. Two-factor authentication with OTP is widely used for online transactions.

However, as mentioned above, it faces security problems which according to [15] Sharma and Nene are addressed by quantum computations. Their work suggests the use of quantum computing to generate QOTP and biometric user data for user authentication, as well as the usage of two-factor authentication. The study outlines three use cases relied on the operation, measurement, and transmission of qubits that define diverse user capabilities connected to the quantum environment. The threat model is used to conduct separate security analyses for each of the three use cases. The task fixes security vulnerabilities that QOTP addresses in the OTP application's present approaches. Using biometric data, the suggested model assures user authentication rather than device authentication.

11. Future of authentication

- Multi-factor One of the most secure ways to authenticate is using multi-factor digital authentication. It includes a great variety of topics in cyberspace, like online payments, communications, etc.

- The security needs for a famous person with millions of fans, differ from those for a small-follower profile, so while utilizing SMS as a 2FA for a few social media accounts is sufficient, it is preferable to use various methods for celebrities or politicians' accounts. Regardless of the method initially chosen, using a second type of identification has to be the first option. We are at a time when there are often invasions, so despite the huge number of combinations of names and codes, it is now quite easy and cheap for the attackers to violate them.
- Online banking is extensively used around the globe. The advantages of Internet banking services are characterized by a user-friendly environment, fast transfers and processing transactions in real time. Such services also remove existing time and location restrictions. Internet banking, on the other hand, has some disadvantages. Phishing, incursion, malware attacks, and other illegal activity can all affect bank accounts. To secure clients' credentials from hackers and other cybercriminals, most banks utilize two-factor authentication/multifactor authentication. Hackers, on the other hand, are spreading them around the internet and are continuously trying to come up with new ways to intercept vital banking data. Before allowing access to online banking systems, more banks utilize a trustworthy form of verification. As previously indicated, many banks utilize biometric technologies to authenticate their customers' identities, and these procedures may result in slower financial transactions and increased preventive maintenance expenditures.
- To enhance security in banking transactions, additional authentication elements (e.g., biometrics) could be incorporated into the existing scheme in future studies. More extended research could also include a thorough cost-benefit analysis of the various techniques available, such as smartcards, 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 [8].
- 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.

12. Conclusions and future directions

Authentication is more important than ever before. In the digital age, most people will depend 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 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 scheme and can considerably enhance identity protection by combining the knowledge 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.

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. We studied the progression of authentication from single-factor to two-factor to multi-factor systems in this study. We concentrated on the MFA methods that make up the state-of-the-art ones, as well as future probable aspects, difficulties, and hopeful solutions.

Enhanced authentication is clearly required. Instead of supporting two-factor authentication 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. Because there is such a pressing need to make authentication safer and easier, several 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 utilizing many other security-enhancing support techniques is the new frontier.

13. Abbreviations Index

14. Bibliography

1. W. Jensen, "Authenticating users on handheld devices," Proceedings of the Canadian Information Technology Security Symposium, 2003.
2. R. Madhusudhan and R. C. Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards: a review," J. Netw. Comput. Appl., 2012.
3. L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proc. IEEE, 2003.
4. C. Rathgeb and A. Uhl, "Two-factor authentication or how to potentially counterfeit experimental results in biometric systems, Image Analysis and Recognition," Springer, 2010.
5. S. K. Hafizul and G. P. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography," Math. Comput. Modell, 2013.
6. K. Das, P. Sharma, S. Chatterjee and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," J. Netw. Comput. Appl., 2012.
7. H. Shteingart, A. N. Gordon and J. Gazit, "TWO - FACTOR AUTHENTICATION," MICROSOFT TECHNOLOGY LICENSING, LLC, Redmond,WA (US), 2016.
8. C.-H. Tsai and P.-C. Su, "The application of multi-server authentication scheme in internet banking transaction environments," Springer-Verlag GmbH, Germany, 2020.
9. D. Dasgupta, A. Roy and A. Nag, Advances n User Authentication, 1 ed., USA: Springer International Publishing, 2017.
10. A. Ometov, V. Petrov, S. Bezzateev, Y. Koucheryavy and M. Gerla, "Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications," IEEE, 2019.
11. I. Velásquez, A. Caro and A. Rodríguez, "Authentication schemes and methods: A systematic literature review," Information and Software Technology, Chillán, Chile, 2018.
12. S. Ibrokhimov, K. L. Hui, A. A. Al-Absi, H. J. Lee and M. Sain, "Multi-Factor Authentication in Cyber Physical System: A State of Art Survey," 21st International Conference on Advanced Communication Technology (ICACT), Korea (South), 2019.
13. K. Mohsin, L. Han and M. Hammoudeh, "Two Factor Vs Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments," ICFNDS '17: Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 2017.
14. R. P. Jover, "Security Analysis of SMS as a Second Factor of Authentication: The challenges of multifactor authentication based on SMS, including cellular security deficiencies, SS7 exploits, and SIM swapping," 2020.
15. M. K. Sharma and M. J. Nene, "Two-factor authentication using biometric based quantum operations," Pune, India, 2019.

16. A. L. Kun, T. Royer and A. Leone, "Using tap sequences to authenticate drivers," *Proceedings of the 5th International Conference on Automotive User Interfaces and Interactive Vehicular Applications - AutomotiveUI '13,* pp. 228-231, 2013.
17. S. H. Khan, M. Ali Akbar, F. Shahzad, M. Farooq and Z. Khan, "Secure biometric template generation for multi-factor authentication," *Pattern Recognition,* vol. 48, no. 2, pp. 458-472, 2 2015.
18. Busold, C.; Taha, A.; Wachsmann, C.; Dmitrienko, A.; Seudié, H.; Sobhani, M.; Sadeghi, A.R. 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; ACM: New York, NY, USA, 2013; pp. 233–242.
19. P. Urien and S. Piramuthu, "Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks," *Decision Support Systems,* vol. 59, pp. 28-36, 3 2014.
20. F. Thullier, B. Bouchard and B.-A. Menelas, "A Text-Independent Speaker Authentication System for Mobile Devices," *Cryptography,* vol. 1, no. 3, p. 16, 9 2017.
21. W. Wójtowicz and M. R. Ogiela, "Biometric watermarks based on face recognition methods for authentication of digital images," *Security and Communication Networks,* vol. 8, no. 9, pp. 1672-1687, 6 2015.
22. Bowyer W. Kevin and Burge Mark J., Handbook of Iris Recognition, K. W. Bowyer and M. J. Burge, Eds., London: Springer London, 2016.
23. D. Phan, L. Y. Siong, P. N. Pathirana and A. Seneviratne, "Smartwatch: Performance evaluation for long-term heart rate monitoring," *2015, International Symposium on Bioelectronics and Bioinformatics (ISBB),* pp. 144-147, 10 2015.
24. Z. Zhang, "Photoplethysmography-Based Heart Rate Monitoring in Physical Activities via Joint Sparse Spectrum Reconstruction," *IEEE Transactions on Biomedical Engineering,* vol. 62, no. 8, pp. 1902-1910, 8 2015.
25. W. Kang and Q. Wu, "Contactless Palm Vein Recognition Using a Mutual Foreground-Based Local Binary Pattern," *IEEE Transactions on Information Forensics and Security,* vol. 9, no. 11, pp. 1974-1985, 11 2014.
26. M. Piekarczyk and M. R. Ogiela, "Touch-Less Personal Verification Using Palm and Fingers Movements Tracking," pp. 603-609, 2017.
27. P. Tome and S. Marcel, "On the vulnerability of palm vein recognition to spoofing attacks," *Proceedings of 2015 International Conference on Biometrics, ICB 2015,* 2015.
28. A. De Luca and J. Lindqvist, "Is secure and usable smartphone authentication asking too much?," *Computer,* vol. 48, no. 5, pp. 64-68, 5 2015.

29. A. M. Guzman, M. Goryawala, J. Wang, A. Barreto, J. Andrian, N. Rishe and M. Adjouadi, "Thermal imaging as a biometrics approach to facial signature authentication," *IEEE Journal of Biomedical and Health Informatics,* vol. 17, no. 1, 2013.
30. S. Hu, J. Choi, A. L. Chan and W. R. Schwartz, "Thermal-to-visible face recognition using partial least squares," *Journal of the Optical Society of America A,* vol. 32, no. 3, 2015.
31. S. P. Banerjee and D. Woodard, "Biometric Authentication and Identification Using Keystroke Dynamics: A Survey," *Journal of Pattern Recognition Research,* vol. 7, no. 1, 2012.
32. B. Shrestha, M. Mohamed, S. Tamrakar and N. Saxena, "Theft-resilient mobile wallets: Transparently authenticating NFC users with tapping gesture biometrics," *ACM International Conference Proceeding Series,* Vols. 5-9-December-2016, 2016.
33. H. Gascon, S. Uellenbeck, C. Wolf and K. Rieck, "Continuous authentication on mobile devices by analysis of typing motion behavior," *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI),* Vols. P-228, 2014.
34. D. Buschek, A. De Luca and F. Alt, "Improving accuracy, applicability and usability of keystroke biometrics on mobile touchscreen devices," *Conference on Human Factors in Computing Systems - Proceedings,* Vols. 2015-April, 2015.
35. W. Meng, D. S. Wong, S. Furnell and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Communications Surveys and Tutorials,* vol. 17, no. 3, 2015.
36. A. Buriro, B. Crispo, F. D. Frari and K. Wrona, "Touchstroke: Smartphone user authentication based on touch-typing biometrics," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* vol. 9281, 2015.
37. U. Burgbacher and K. Hinrichs, "An implicit author verification system for text messages based on gesture typing biometrics," *Conference on Human Factors in Computing Systems - Proceedings,* 2014.
38. T. Van Goethem, W. Scheepers, D. Preuveneers and W. Joosen, "Accelerometer-based device fingerprinting for multi-factor mobile authentication," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* vol. 9639, 2016.
39. C. Figueira, R. Matias and H. Gamboa, "Body location independent Activity monitoring," *BIOSIGNALS 2016 - 9th International Conference on Bio-Inspired Systems and Signal Processing, Proceedings; Part of 9th International Joint Conference on Biomedical Engineering Systems and Technologies, BIOSTEC 2016,* 2016.

40. D. He and S. Zeadally, "Authentication protocol for an ambient assisted living system," *IEEE Communications Magazine,* vol. 53, no. 1, 2015.
41. A. Bruun, K. Jensen and D. Kristensen, "Usability of single-and multi-factor authentication methods on tabletops: A comparative study," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* vol. 8742, 2014.
42. N. Harini and T. R. Padmanabhan, "2CAuth: A new two factor authentication scheme using QR-code," *International Journal of Engineering and Technology,* vol. 5, no. 2, 2013.
43. Neha and K. Chatterjee, "Authentication techniques for e-commerce applications: A review," *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016,* 2017.
44. N. A. Nor, G. N. Samy, R. Ahmad, R. Ibrahim and N. Maarop, "The proposed public key infrastructure authentication framework (PKIAF) for Malaysian government agencies," *Advanced Science Letters,* vol. 21, no. 10, 2015.
45. K. Han, S. Divya Potluri and K. G. Shin, "On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks," *2013 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS 2013,* 2013.
46. E. De Cristofaro, H. Du, J. Freudiger and G. Norcie, "A Comparative Usability Study of Two-Factor Authentication," 2014.
47. A. T. B. Jin, D. N. C. Ling and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition,* vol. 37, no. 11, 2004.
48. F. Schroff, D. Kalenichenko and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition,* Vols. 07-12-June-2015, 2015.
49. Feng, T.; Liu, Z.; Kwon, K.A.; Shi, W.; Carbunar, B.; Jiang, Y.; Nguyen, N. Continuous mobile authentication using touchscreen gestures. In Proceedings of the Technologies for Homeland Security (HST) Conference, Waltham, MA, USA, 13–15 November 2012; pp. 451–456.
50. Siswoyo, A.; Arief, Z.; Sulistijono, I.A. Application of Artificial Neural Networks in Modeling Direction Wheelchairs Using Neurosky Mindset Mobile (EEG) Device. EMITTER Int. J. Eng. Technol. 2017, 5, 170–191.
51. L. Kraus, J. N. Antons, F. Kaiser and S. Möller, "User Experience in Authentication Research: A Survey," 2016.
52. C. Katsini, M. Belk, C. Fidas, N. Avouris and G. Samaras, "Security and usability in knowledge-based user authentication: A review," *ACM International Conference Proceeding Series,* 2016.

53. F. A. Harby, R. Qahwaji and M. Kamala, "End-users' acceptance of biometrics authentication to secure E-commerce within the context of saudi culture: Applying the utaut model," *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications,* Vols. 3-3, 2013.
54. M. Belk, C. Fidas, P. Germanakos and G. Samaras, "The interplay between humans, technology and user authentication: A cognitive processing perspective," *Computers in Human Behavior,* vol. 76, 2017.
55. W. Melicher, D. Kurilova, S. M. Segreti, P. Kalvani, R. Shay, B. Ur, L. Bauer, N. Christin, L. F. Cranor and M. L. Mazurek, "Usability and security of text passwords on mobile devices," *Conference on Human Factors in Computing Systems - Proceedings,* 2016.
56. He, D.; Zeadally, S. Authentication protocol for an ambient assisted living system. IEEE Commun. Mag. 2015, 53, 71–77.
57. M. Gomez-Barrero, C. Rathgeb, J. Galbally, C. Busch and J. Fierrez, "Unlinkable and irreversible biometric template protection based on bloom filters," *Information Sciences,* Vols. 370-371, 2016.
58. K. B. Raja, R. Raghavendra, M. Stokkenes and C. Busch, "Multi-modal authentication system for smartphones using face, iris and periocular," *Proceedings of 2015 International Conference on Biometrics, ICB 2015,* 2015.
59. 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, 14–15 August 2012; pp. 54–57.
60. Kholmatov, A.; Yanikoglu, B. Identity authentication using improved online signature verification method. Pattern Recognit. Lett. 2005, 26, 2400–2408.
61. RANI, CH Jhansi; MUNNISA, SK Shammi. A survey on web authentication methods for web applications. *Int. J. Comput. Sci. Inf. Technol*, 2016, 7.4: 1678-1680.
62. M. Azrour, J. Mabrouki, A. Guezzaz and Y. Farhaoui, "New enhanced authentication protocol for Internet of Things," in *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 1-9, March 2021, doi: 10.26599/BDMA.2020.9020010.
63. F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban and R. C. Bansal, "A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network," in *IEEE Access*, vol. 9, pp. 31309-31321, 2021, doi: 10.1109/ACCESS.2021.3060046.
64. Anand, A., Singh, A.K. Watermarking techniques for medical data authentication: a survey. *Multimed Tools Appl* **80,** 30165–30197 (2021). https://doi.org/10.1007/s11042-020-08801-0
65. Christian Esposito, Massimo Ficco, Brij Bhooshan Gupta, Blockchain-based authentication and authorization for smart city applications, Information Processing & Management, Volume 58, Issue 2, 2021, 102468,ISSN 0306-4573, https://doi.org/10.1016/j.ipm.2020.102468.

66. Casey, M., Manulis, M., Newton, C.J., Savage, R., & Treharne, H. (2020). "An Interoperable Architecture for Usable Password-Less Authentication". ETAA@ESORICS.

Appendix

Base64 Algorithm in Java

```
class Base64Encode {
    private final static String base64chars = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
    public static String encode(String s) {
    // the result/encoded string, the padding string, and the pad count
    String r = "", p = "";
    int c = s.length() % 3;

    // add a right zero pad to make this string a multiple of 3 characters
    if (c > 0) {
        for (; c < 3; c++) {
        p += "=";
        s += "\0";
        }
    }

    // increment over the length of the string, three characters at a time
    for (c = 0; c < s.length(); c += 3) {

        // we add newlines after every 76 output characters, according to
        // the MIME specs
        if (c > 0 && (c / 3 * 4) % 76 == 0)
        r += "\r\n";

        // these three 8-bit (ASCII) characters become one 24-bit number
        int n = (s.charAt(c) << 16) + (s.charAt(c + 1) << 8)
            + (s.charAt(c + 2));

        // this 24-bit number gets separated into four 6-bit numbers
        int n1 = (n >> 18) & 63, n2 = (n >> 12) & 63, n3 = (n >> 6) & 63, n4 = n & 63;

        // those four 6-bit numbers are used as indices into the base64
        // character list
        r += "" + base64chars.charAt(n1) + base64chars.charAt(n2)
            + base64chars.charAt(n3) + base64chars.charAt(n4);
    }
    return r.substring(0, r.length() - p.length()) + p;
    }
}
```