ISSN 2278-9723
DOI:10.31838/ijccts/10.02.06

Research Article

User Authentication Mechanism for Access Control Management: A Comprehensive Study

SAJAAD AHMED LONE,A.H. MIR
Department of Electronics and Comm. Engineering,National Institute of Technology, Srinagar
Jammu and Kashmir, India
Email: sajaadlone@iust.ac.in,ahmir@rediffmail.com
Received: 05.01.22, Revised: 11.02.22, Accepted: 20.02.22

ABSTRACT
The threat of cyberattacks is growing in all sectors today, including banks, governments, healthcare institutions and other organizations due to the exponential increase in cloud, IOT and smart devices utilization in recent years. When it comes to protecting organizations' and clients' information and privacy in security risks, there is a strong desire to develop and use more secure authentication techniques. This paper presents an overview of authentication techniques built on the fundamental authentication metrics, i.e., knowledge, ownership, and biometrics, their advantages, limits, and open issues, and future possibilities for developing secure authentication techniques for securing critical and sensitive information.

Keywords:User Authentication, OTP, Multifactor, Knowledge, Token, Biometrics, Access Control Management

1. Introduction

One of the interesting facts in network and security is the major evolutions of new tools and technologies to mitigate security threats. There is also an exponential rise in attackers' policy to intrude and invoke various malicious activities over the secured network. Every year, news on security breaches persists where maximum attacks are targeted towards stealing the authentication rights of a legitimate user. Usually, the intruder seems to exhibit atypical behaviour over the internet. They track potential victims, surveil their online behaviour, understand their browsing patterns, and then create a hit list of similar types of victims. There are already software and various malicious codes that never seemed to be thwarted to date. Hence, the outcome of such malicious activities costs legitimate user sensitive and confidential transactional data, finally resulting in identity theft. Such intrusion activity has a collateral effect on multiple databases and web-server affecting millions of users online.

The security breaches over authentication and authorization policy were always on the rise to date, and therefore, it has attracted numerous researchers to find some sort of robust and fail-proof solution. Henceforth, in the advent of a massive volume of research work previously addressing such issues, interesting and uniquely, it was found that there exist a unique group of studies that focus on using multiple parameters to be considered at the time of authenticating a legitimate user.

A major concern in information security is determining whether or not the person seeking access to highly confidential, classified, or sensitive information is an authorized individual [1]. This can all be accomplished when the individual proves their identity through a verification process to access information. If they fail to do so, access will be refused. Authentication is the first move in the access control process and will continue to be the primary focus throughout this study.

2. User Authentication Mechanisms

The pervasive use of smart devices has increased the frequency of data breaches in today's world. Major financial institutions, health insurance companies, and state and federal government organizations have all been data breach victims, putting the private data of millions of people and consumers at risk.[2]–[8]. In tandem with the continual and rapid growth of data generated by the amalgamation of mobile, cloud technology, IOT, and persistent computing, additionally, the possibility of a breach in to one's data vaults can significantly increase. Many applications that deal with protecting confidential, classified, and sensitive information are increasingly reliant on strong authentication and authorization strategies among their users. To connect an individual with established credentials, three top ways of authentication are available today: something a user possesses. Keys, passports, and smart cards are examples of personal possessions. Knowledge: users having certain knowledge, such as passwords, PINs, and phrases, can use the service. Biometrics: the physiological or behavioural traits of a person that are unique and distinguish one individual from another, such as fingerprints, palm, iris, voice and so on.[2], [3], [9]–[15]. A discussion of the three

different categories will be provided in the following subsections, which will then be followed by outlines for some major authentication implementations in the following sections.

A. Knowledge-Based User Authentication

Unauthorized access to resources is still the most common problem, and authentication based on knowledge is still the most widely accepted solution to secure these resources. This is the simplest, easiest, and most common user authentication method, which involves users providing information like PINS, passwords, etc., or the reply to undisclosed questions that only users know. The graphical passwords are also a known branch of knowledge-based user authentication as well[12], [16]–[18]. Many factors, including the low cost, ease of implementation and extensibility, and widespread user familiarity, contribute to knowledge-based authentication being the most widely used authentication method today[2],[14], [19]–[22]. Knowledge-based authentication is based on the exact recall of confidential information. As a result, memorability is an important concern in this authentication mechanism, leading users to violate standard security rules by creating easy passwords to remember and, as a result, weak and low in entropy, writing them down, or reusing the very same passwords across multiple services pose a security threat. Studies have also shown that writing on onscreen keyboards is slower and more difficult than typing on physical keyboards; the widespread use of touchscreens has introduced an additional challenge for alphanumeric passwords. [23]–[25].

B. Token Based User Authentication

This form of authentication does not need the user to know something; instead is characterized by the physical possession that the user owns and carries at the time of authentication[26]. This can assume the shape of a secure storage device that contains login details, such as a credit card, smart card keys, or mobile phones, or it can be implanted in a portable object that can be carried easily, such as a key fob or USB flash drive. In this type of authentication, software-based objects are used in permission granting systems, where multipath authentication algorithms are used, and active devices that generate passcodes or time-synchronous challenge–responses are also included in this [27]. It is very difficult to duplicate and manipulate token devices of numerous types as they are generally temper-resistant. In case of tampering, special hardware disables the token or authentication attempts to exceed a certain threshold. If users choose to use token-based authentication, they must always keep track of additional hardware used solely for the authentication process. This additional equipment can be accused of stealing by a particularly intruder or even damaged or lost either by the end-user. The unfortunate reality is that scaling these forms of identification can be difficult, particularly for large organizations.

C. Possession Based User Authentication

Traditional authentication systems based on knowledge and token authentication are widely accepted because of their ease of installation, user familiarity, and design simplicity. However, while being utilized in many modern applications, these systems for authentication don't meet stringent security performance requirements. Among the many viable alternatives to these authentications is authentication systems based on biometrics, which involves the identification and verification of a user's specific physiological or behavioral characteristics such as their face, , palm, iris, fingerprints, keystroke, voice, signature, and so on[28]–[35]. When using attributes for authentication, it is significantly more difficult to separate an individual from their characteristics than knowledge or token-based. As a result, biometric features cannot be misplaced or overlooked, and it is extremely difficult to recreate, share, and distribute them in any way. Additionally, the user to be authenticated must be present at the moment of authentication, which increases the system's reliability even further. According to information published by the International Biometrics Group, no single biometrics technology is appropriate for every application. [36].

In general, the following are the numerous types of biometrics that are routinely employed in today's automated authentication systems:

- Fingerprint: Since its inception, fingerprints have been used by governments and law enforcement agencies to identify individuals. They are recognized as a unique and reliable identification. After being put through rigorous testing, fingerprints have proven to offer the highest level of security, with no reports of attempts to deceive the device being made. Although some factors like dirt, cosmetics, and age can cause false positives and false negatives, the overall error rate has been shown to be 1 in 500 or less, making this feature far superior to other biometrics.
- Retinal or Iris Scan: Using a retinal or iris scan, a biometric can be used to identify an individual based on the arrangement of veins in their retina or the colour patterns in their iris. Iris scans have shown to be an excellent user verification method, but they are not without their flaws. For example, wearing spectacles and working in poor illumination can result in erroneous readings. Iris scans are generally not

difficult to deceive, but they have an acceptance rate of approximately 1-131,000, which is considered to be reasonable.

It has been demonstrated that retinal scanners are superior to iris scanners in that they can authenticate even blind users or users who lack pigment in their iris. Furthermore, retinal scans are extremely difficult to deceive, with a mistake rate of 1 in 1,000,000, which is exceptional compared to the error rates of all other biometric traits.

- Voice Recognition: It makes use of a voiceprint, which examines how a person utters a phrase or a word sequence that is unique to him, to do this. An attacker can capture the voice of the authenticated user and then utilize that recording to bypass the voice recognition system's protection.
- Facial Recognition: A person can be recognized by their distinctive facial characteristics. Although such authentication mechanisms can be deceived by using a mask at their original settings, this can be avoided by increasing threshold values to 96 percent. Furthermore, the individual's facial characteristics may change as they grow older. [37].
- The inexpensive cost of fingerprint technology, which costs under $100.00, is an additional advantage of using biometrics for authentication.in contrast, retina scans can cost anywhere from $2,000.00 to $2,500.00, putting the technology there at the high end of the cost spectrum. Although it delivers great reliability that cannot be breached in locations requiring special security, it is more expensive. [38]. On the contrary, selecting a particular biometric characteristic for any application is determined by the degree to which the following aspects are met.

i) Uniqueness or Distinctiveness: Biometric characteristics of every person should be unique

ii) Universality: Every person should have a biometric characteristic.

iii) Permanence: The biometric feature should be invariant over time.

iv) Collectability: the characteristic should be quantitatively measurable

A combination of all these attributes determines the effectiveness of any biometric application, there is no biometric that satisfies any attributes absolutely, nor one that has all to a completely acceptable level simultaneously, hence resulting in many comprises[10]. Although biometric systems, like other systems, provide significant usability advantages, they are vulnerable to various attacks. In contrast to the knowledge-based authentication systems, which can be readily reset, biometrics records traits such as blood vessel patterns, retinal patterns, cardiac rhythms, and so on. Even if the system is compromised, it is not easy to reset it. Furthermore, biometric-authentication systems are not very responsive to changes; even a slight change in facial expression and obstructions such as glasses, scarves, and hats might result in the denial of access to confidential information even to those who are authorized to do so.

3. Implementation Of Authentication Mechanism

Current physical and cyber security systems still rely on traditional authentication methods discussed above. For simplicity and user-friendliness, most authentication schemes are used separately, a single factor at a time since it has been found that a single factor based authentication is not credible that can provide sufficient protection due to a variety of security threats, most well-funded information systems have fallen victim to attacks[39]. Therefore, for strong authentication, more than one factor should be augmented together to assert the identity of a user requesting access to an application or service. The most well-known method of this sort of authentication is two-factor authentication (2FA), which combines your first authentication factor (normally something you know like your secret word) with a second factor of a unique kind, for example, something you have and something you are[40]–[42]. Having examined the distinctive authentication method classification in the last section, this section assesses the effective authentication implementation that falls into these classifications.

A. Multifactor Authentication

A multifactor authentication system is one of the most effective safeguards an organization can adopt to prevent an attacker from gaining access to essential and sensitive data. It is possible to choose authentication parameters more than single from among independent credentials categories to recognize authorized users in this form of authentication system.[43]. The authentication factors chosen for recognizing authorized users in multifactor authentication (MFA) should be independent of one another, with the ultimate goal being that gaining access to one factor does not point toward access to other factors, and the tradeoff of any one factor does not have an impact on the respectability or secrecy of another factor, among other things.

A multifactor authentication system is a layered strategy for securing sensitive services and applications in which the system requires the user to present a combination of the two or more factors to identify legitimate users. Multifactor authentication is typically accomplished by combining a conventional text-based username and password with another

factor such as a fingerprint. A prominent example of multifactor authentication is popularly used in bank ATMs for accomplishing banking transactions; customers in this authentication carry both their credit/debit card and pin when using ATM banking service, in which something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN) is used to identify the legitimate bank user. Customers must carry their credit/debit card and personal identification number when using ATM services. In this situation, if somebody snips or discovers a lost card, they will need to know or predict the customer's pin, which is a higher security measure than a password alone. Because multifactor authentication (MFA) requires impostors to progress beyond a single authentication device and instead use multiple, the advantages of MFA are numerous. When properly designed, such authentication systems will need to fizzle in various ways before their security is significantly compromised, which would take time. The unquestionable advantage of multifactor authentication is that it increases security by giving more layers of assurance to the authentication process. With the increase in the number of layers (factors), the more challenging it becomes for a potential attacker to gain access to the records, frameworks, and information. MFA can also aid organizations in achieving and maintaining consistency, which can help to reduce the possibility of legal liability. Whatever the case, multifactor authentication is anything but a magic trick; keep these difficulties in mind when creating a multifactor authentication system [25], [42], [44]–[48].

B. One Time Password (OTP)

Many scholars have analyzed various problems about authentication and security of highly privileged and private information. While studying various schemes adopted in the present and the past, the use of One-Time Passwords, also known as OTPs, appears to improve access management security in both private and public networks[49]–[52]. When attempting to complete a unit of transactions, the one-time password (OTP) is only acceptable for one access attempt. For those who are utilizing OTP, one of the most obvious benefits is that it offers fail-proof protection against replay attacks. This ensures that a specific password formed once can never be repeated a second time, rendering the password unusable if it falls into the hands of an intruder. Following this, OTP is being investigated to see if there is a more streamlined solution to improve user authentication that can be implemented[7]. Because of the many presentations of OTP practice and the architecture built by previous protocol designers and researchers, several different OTP schemes have been patented, but standardizing remains a difficult task. This part will go over several different OTP-based authentication systems.

a) HMAC-based One-Time Password (HOTP)

A one-time password (OTP) technique based on hash-based message authentication code (HMAC) is known as HOTP, and it is used to authenticate users by symmetrically creating one-time passwords, which are only needed once throughout the authentication process. Authenticator, and token both share a secret key (seed), as well as an authentication counter, in this kind of OTP-based authentication. Both parties use the default hash function SHA1 in conjunction with the secret key and the counter to compute the HOTP value. It is displayed on the token as a 160-bit value that has been reduced to 6 or 8 decimal digits after computing it. After that, the authenticator (Server) compares the OTP value delivered locally with the OTP value associated with the token to determine whether the token is authentic. Each party starts a new counter. The fact that HOTP is not subject to a time-based constraint makes it slightly easier to use; however, because of the large window of time during which HOTP is valid, it may be more susceptible to brute force attacks [53]–[55].

b) Time-Based One-Time Password (TOTP)

An OTP is generated by the Time-based One-Time Password (TOTP) algorithm using a secret key and the current time. An OTP can only be used once and is only valid for a specific period. In this case, the technique is a variant of the HMAC-based One Time password (HOTP), but it can be used only once. Where a proprietary authentication server is used, the token contains a precise timekeeping device that has been synced with the proprietary authentication server's timekeeping device (if applicable). When creating an OTP value, the authenticator server must consider both the secret key and the current time for the token to be validated by the server. A legitimate user can only be determined by comparing the token's generated OTP value to the authenticator's produced OTP value; if both values match, then both values indicate that the user is legit [49], [58]–[60]. The authenticator generates a one-time password (OTP) using the same algorithm as that of the token; if the values are equal, the user is valid [59In spite of the fact that TOTP is more secure than HOTP, a fundamental flaw in this authentication technique is that it is unable to identify users if somehow the token and authenticator are not synchronized; as a result, TOTP has a short lifespan after which OTP value changes. To generate the One-Time-Password, the Google 2-factor authenticator employs the TOTP technique. Because all TOTP systems rely on the user's phone's time to match the server's clock, the Google authenticator becomes out of sync because

this is not the case with this Google authenticator's time[49], [56]–[58].

c) Challenge-Response Based OTP Authentication

When using this type of authentication system, an entity (Server) issues a challenge or question, and a valid response is presented by another entity (token) to be authenticated, the user attempting to gain entry to a computer, network, or other services is identified and authenticated. For authentication to take place while using a challenge-response authentication scheme, a series of steps must be completed, during which the secret key must first be communicated between the token and server before authentication can take place. Following successful token authentication, the server sends an authentication challenge value to the token's client (the token). To generate the OTP, both the server and the client use the challenge value and the secret key. After calculating the OTP, the token needs to send it to the server, which then relates it to the OTP that was previously generated to ascertain whether or not the user is permitted. Since the value used by the server for the challenge is generated in a one-of-a-kind manner, this type of authentication is considered to be relatively safe. By utilizing the challenge response-based authentication method, it is possible to protect against a variety of attacks, including session reply attacks, reply attacks, and man in the middle attacks, to name a few. On the other hand, the challenge values are made public, and the system becomes highly susceptible to communication-based attacks[59]–[63].

d) S/Key Authentication

In addition to being known as the Lamport scheme, this authentication method generates one-time password (OTP) values by hash chaining from the secret key. A hash value is generated once a secret key is shared between the client and server. This hash value is then used as input by the second hash function in this process of OTP-based authentication between the client and server. This procedure is repeated by the algorithm an undetermined number of times. [64], [65]. if the one-way hash function is denoted by f, the secret key is denoted by S. If we apply f to the seed S for N times, we obtain a hash chain of length N.

$$f(S), f(f(S)), \ldots, f^{N}(S) \qquad (1)$$

N hash values are stored on the client-side, and on the server-side, f (S), f (f (S))…. f^{N-1} (S) are deleted, and only one hash value is stored, which is f^{N} (S). When the client has been authenticated, the N-1 hash is sent to the server by the client. For each N-1 hash value received from the client, the server calculates the N^{th} hash value and matches it with the N^{th} hash value previously recorded to determine whether or not the user is legitimate. When the user m^{th} logs in, the server sends a challenge code (N-m), and the user creates an OTP due to the challenge code.

$$OTP = f^{N-m}(s) \qquad (2)$$

The server authenticates the user's OTP as

$$f(OTP) = f^{N-m+1}(S) \qquad (3)$$

After the (m-1)th login, the f N-m+1 (S) is already memorized in the server's database. If the above values for the client and the server are the same, the server retains the received hash value and deletes the previous (N-(m-1)th hash value from the client's cache. This technique is simple to develop, incorporates both challenge and hash chaining, and does not require very sophisticated hardware [50]. Attackers posing as hosts can compromise S/Key authentication by sending a brief challenge to the user, who then replies with the hash chain's initial values, allowing an attacker to compute more one-time passwords. A "little challenge" attack is used to describe this type of attack. As a result, the user's processing requirements increase throughout the computations for the chain's initial values, making the system unusable for devices with limited computing capabilities such as cell phones. Although the technique is impenetrable to eavesdropping and replay assaults, it is subject to server spoofing and offline dictionary attacks, among other things[63].

e) Short Message Service (SMS) Based One Time Passwords

Thanks to recent advances in smartphone technology, self-care services in healthcare, banking, and e-commerce have grown significantly, particularly in the banking and healthcare sectors. When it comes to implementing these services, the most difficult problem businesses must deal with is security in the authentication and authorization of legitimate users. Usernames and passwords, which are traditionally used for authentication purposes and are vulnerable to being breached by intruders, pose a serious risk of being compromised, as proved by the recent Yahoo data breach. These techniques can be targeted by various attacks, including password guessing attacks, shoulder surfing attacks, and brute force attacks, all of which can be effective[5], [16], [66]. To combat such attacks, an additional factor, known as an OTP, was established to make sure that only authorized users could gain access. The most basic concept of the one-time password is that every client account is tied to a mobile phone number in a scheme under the control of the account's proprietor.

So the only person who can receive an SMS One-Time Password (OTP) from the mobile phone number associated with the account is the person who created the account in the first place. In this

authentication technique, clients are required to input a one-time password after providing their login and secret phrase to accept the transaction; each OTP generated is used just once and then discarded. The most appropriate method of communicating one-time passwords created by the authenticator is via a short messaging service, which saves the need to create password lists in the process.[67]. When it comes to account verification, most banks and other corporations that provide online services such as Google Mail, Dropbox, and Google App Engine rely on SMS-based one-time passwords (OTP). When it comes to SMS-based OTP, it is deemed safe since every time the user is required to input newly generated passwords, the system is protected from brief exposure and is more resistant to reply attacks[52].

4. Open Issues And Challenges In User Authentication Mechanism

Having presented research into the different security systems available in access management and the findings of the study, it is possible to conclude that there are still flaws in the security solutions that are currently available. The challenges that have been identified range from security vulnerability to computational complexity to user adaptability and everything in between. To summarize, the progressive review process will result in the following open issues at the conclusion of the process:

1. In traditional user authentication mechanisms such as user names and passwords, memorability is a significant problem, resulting in users breaking basic security rules by creating passwords that are easy to remember and are therefore weak and low entropy, writing them down, or reusing the same passwords for different services. They become a security risk to online apps due to their bad and inaccurate password habits. Because of the widespread usage of touchscreen devices, alphanumeric passwords have faced additional difficulty, as studies have shown that typing on virtual keyboards is both slower and more difficult than typing on real keyboards[12].
2. Inability in protecting a wide range of threats [67], including touch-loggers/keyloggers, mimic attacks, liveness detection, and other similar attacks
3. Aside from being inconvenient for users, the extra equipment needed in some authentication systems[68]–[71] , such as smartcards, can also be expensive for service providers. This is because technical adaptations to such authentication systems are not possible. As a result, because of their lack of user-friendliness, those systems' technical adaptability is hindered.
4. GSM is used in a few authentication schemes for the distribution of authentication messages and one-time passwords (OTP), which is a severe security concern in and of itself [37], [72], [73].
5. Because of the use of a public key, fuzzy vault schemes, operations, and self-updating hash chains, contemporary access control mechanisms have been found to have a number of drawbacks, including increased processing time, reduced system speed, increased computational cost, and large amounts of data stored in memory. .
6. The ability to use the same token across multiple service providers is only offered by authentication systems [74]. The need to maintain a separate token for each service provider in the majority of authentication mechanisms causes the user to be inconvenienced once more.
7. The inability of some authentication systems[75] to provide service pool scalability for large numbers of users means that they can only be used for a limited number of applications.
8. As a result of the widespread use of insecure password generation techniques such as AES, SHA-1, MD5, and others in most authentication schemes [7], they are rendered vulnerable and unable to keep up with technological advancements.
9. Multi-channel communication in a few authenticating systems results in service charges being charged to the user, increasing the burden on the user[7][76].
10. In the current state of development, authentication schemes depend on a single biometric characteristic as the third authenticating factor or consider only biometrics while ignoring the first two authenticating factors, which may be susceptible to impersonation attacks. As a result, those authentication schemes have security flaws and cannot be used in applications requiring high levels of security, such as the financial system, airport information systems, and so on[47], [77]–[84].
11. When used for authentication, popular biometrics such as voice, iris scan, and facial characteristics encounter a number of difficulties. The speech authentication system can be compromised because an intruder can record the voice of the authenticated user and then use that recorded voice to break through the speech recognition system, which is the foundation of the proposed authentication mechanism. Furthermore, iris scanners require proper lighting to function properly, and they can produce false results if not used properly. [85].
12. The attack by a Man-in-the-Middle is another possible scenario that has not been considered in the previous studies. This attack scenario

involves using an unauthorized proxy server between both the authentication server and the communication channel to deceive the authentication server. Following the generation of an authentication token, the token travels through unsafe routes, revealing critical information to the attacker upon receipt of a service request from the attacker. And once the information has been stolen, the attacker will be able to configure the entire authentication system with relative ease, granting the attacker access to resources on an ongoing basis. Such attack scenarios have not been considered in previous works, and as a result, they remain an open question.

13. The security of SMS-based one-time passwords is highly reliant on the privacy provided by the cellular network. Serval attacks against GSM and 3G networks have been reported, demonstrating that the confidentiality and anonymity of SMS messages cannot be guaranteed. SMS privacy can also be compromised by injecting malware into mobile phones, intercepting and forwarding OTP SMS to attackers, making the phone vulnerable to man-in-the-middle attacks. An attack against SMS-based OTP known as the SIM Swap attack is a social engineering attack in which a SIM card replacement for the victims' mobile numbers is obtained. The SIM card is then linked to the victims' mobile phone numbers; as a result, the attacker receives all OTP SMS messages sent by the victims while initiating online transactions.[72], [86]
14. According to the study's findings, a larger proportion of the OTP computation procedures is dependent on time synchronization numerical calculations to generate one-time passwords. Because the arbitrariness inherent in these OTP frameworks breaks down after a period of time, passwords become predictably long and complex.[1], [64].

5. Conclusion

When it comes to safeguarding an information system, authentication is critical. As a result of the enormous number of authentication techniques available, it can be difficult to choose the most appropriate deployment strategy. This study has evaluated previous authentication strategies based on three core parameters: knowledge, possession, and biometrics. The significant pros and cons of the various security systems have been specifically identified and described in greater detail. All of the authentication techniques examined were determined to be deficient in some way or another. The requirement for a security system capable of thwarting current attacks and providing ongoing assistance without being constrained by technological advancement continues to exist. At the same time, user ergonomics should not be overlooked and should be given the same consideration as other design aspects. Furthermore, when building such systems, it is necessary to consider critical questions and difficulties to spur additional study in the field.

References

1. S. A. Lone and A. H. Mir, “A novel OTP based tripartite authentication scheme,” Int. J. Pervasive Comput. Commun., 2021, doi: 10.1108/IJPCC-04-2021-0097.
2. A. Sharma, V. Ojha, R. C. Belwal, and G. Agarwal, “Password based authentication: Philosophical survey,” in Proceedings - 2010 IEEE International Conference on Intelligent Computing and Intelligent Systems, ICIS 2010, 2010, vol. 3, pp. 619–622, doi: 10.1109/ICICISYS.2010.5658405.
3. R. Spolaor, Q. Q. Li, M. Monaro, M. Conti, L. Gamberini, and G. Sartori, “Biometric authentication methods on smartphones: A survey,” PsychNology J., vol. 14, no. 2–3, pp. 87–98, 2016.
4. T. Mehraj, M. A. Sheheryar, S. A. Lone, and A. H. Mir, “A critical insight into the identity authentication systems on smartphones,” in Indonesian Journal of Electrical Engineering and Computer Science, vol. 13, no. 3, 2019, pp. 982–989.
5. S. Komanduri et al., “Of passwords and people: Measuring the effect of password-composition policies,” ACM Int. Conf. Proceeding Ser., vol. 91, no. 12, pp. 2595–2604, 2019, doi: 10.1145/3359789.3359828.
6. N. A. Lal, S. Prasad, and M. Farik, “A Review Of Authentication Methods,” vol. 5, no. 11, pp. 246–249, 2016.
7. U. D. Deore and V. Waghmare, “Cyber security automation for controlling distributed data,” 2016 Int. Conf. Inf. Commun. Embed. Syst. ICICES 2016, no. Icices, pp. 12–15, 2016, doi: 10.1109/ICICES.2016.7518881.
8. S. Zulkarnain et al., “A Review on Authentication Methods,” Aust. J. Basic Appl. Sci., vol. 7, no. 5, pp. 95–107, 2013.
9. D. Kunda and M. Chishimba, “A Survey of Android Mobile Phone Authentication Schemes,” Mob. Networks Appl. 2018, pp. 1–9, 2018, doi: 10.1007/S11036-018-1099-7.
10. S. P. A. K. Jain, r. Bolle, Biometrics: Personal Identification in Networked Security. 1999.
11. P. Dwivedi and G. Thomas, “CHALLENGES AND BEST PRACTICES IN KBA SCHEME,” 2009.
12. R. Dhamija and A. Perrig, “Déjà Vu: A user study using images for authentication,” Proc. 9th USENIX Secur. Symp., no. 102590, 2000.

13. J. N. Oruh, “Three-Factor Authentication for Automated Teller Machine System,” no. December 2014, 2021.
14. A. Of and A. Thesis, “Password based authentication,” 2009.
15. Y. W. Chow, W. Susilo, M. H. Au, and A. M. Barmawi, “A visual one-time password authentication scheme using mobile devices,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8958, pp. 243–257, 2015, doi: 10.1007/978-3-319-21966-0_18.
16. F. Towhidi, A. A. Manaf, S. M. Daud, and A. H. Lashkari, “The Knowledge Based Authentication Attacks,” World Congr. Comput. Sci., 2011, [Online]. Available: http://www.lidi.info.unlp.edu.ar/WorldComp2011-Mirror/SAM8123.pdf.
17. M. Zviran and Z. Erlich, “Identification and Authentication: Technology and Implementation Issues,” Commun. Assoc. Inf. Syst., vol. 17, no. January, 2006, doi: 10.17705/1cais.01704.
18. U. Uludag and A. K. Jain, “Attacks on biometric systems: a case study in fingerprints,” Secur. Steganography, Watermarking Multimed. Contents VI, vol. 5306, p. 622, 2004, doi: 10.1117/12.530907.
19. T. Turn, “Still relying on knowledge-based authentication? Let ’ s review the primary problems with KBA : what do you suggest,” 2020. https://medium.com/turn-technologies/still-relying-on-knowledge-based-authentication-12dfa376ff26 (accessed Mar. 25, 2021).
20. J. Subils, “Scholar Commons Authentication Usability Methodology,” no. October, 2019.
21. A. Nayak and R. Bansode, “Analysis of Knowledge Based Authentication System Using Persuasive Cued Click Points,” Procedia - Procedia Comput. Sci., vol. 79, pp. 553–560, 2016, doi: 10.1016/j.procs.2016.03.070.
22. A. Tasneem, H. Tauseef, S. Farhan, and M. A. Fahiem, “Measuring the Efficiency and Usability of Session Password based Authentication Systems,” pp. 31–45, 2014.
23. J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity,” J. Comput. Syst. Sci., vol. 80, no. 5, pp. 973–993, 2014, doi: 10.1016/j.jcss.2014.02.005.
24. R. Kainda, I. Flechais, and A. W. Roscoe, “Security and usability: Analysis and evaluation,” in ARES 2010 - 5th International Conference on Availability, Reliability, and Security, 2010, no. May, pp. 275–282, doi: 10.1109/ARES.2010.77.
25. B. Maclej, E. F. Imed, and M. Kurkowski, “Multifactor Authentication Protocol in a Mobile Environment,” IEEE Access, vol. 7, pp. 157185–157199, 2019, doi: 10.1109/ACCESS.2019.2948922.
26. S. Gupta, A. Buriro, and B. Crispo, “Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access,” Mob. Inf. Syst., vol. 2018, 2018, doi: 10.1155/2018/2649598.
27. C. Huber, J. Kubovy, M. Jäger, and J. Küng, “A secure token-based communication for authentication and authorization servers,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10018 LNCS, no. November, pp. 237–250, 2016, doi: 10.1007/978-3-319-48057-2_17.
28. L. N. Evangelin and A. L. Fred, “Biometric authentication of physical characteristics recognition using artificial neural network with PSO algorithm,” Int. J. Comput. Appl. Technol., vol. 56, no. 3, pp. 219–229, 2017, doi: 10.1504/IJCAT.2017.088196.
29. A. L. Fantana, S. Ramachandran, C. H. Schunck, and M. Talamo, “Movement based biometric authentication with smartphones,” Proc. - Int. Carnahan Conf. Secur. Technol., vol. 2015-Janua, pp. 235–239, 2016, doi: 10.1109/CCST.2015.7389688.
30. G. Lovisotto, R. Malik, I. Sluganovic, M. Roeschlin, P. Trueman, and I. Martinovic, “Mobile Biometrics in Financial Services: A Five Factor Framework,” 2017, [Online]. Available: https://www.cs.ox.ac.uk/files/9113/Mobile Biometrics in Financial Services.pdf.
31. C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides, “Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption,” 2015, doi: 10.14722/usec.2015.23003.
32. B. Abazi, B. Qeliaja, and E. Hajrizi, “Application of biometric models of authentication in mobile equipment,” IFAC-PapersOnLine, vol. 52, no. 25, pp. 543–546, 2019, doi: 10.1016/j.ifacol.2019.12.602.
33. R. Amin, T. Gaber, G. Eltaweel, and A. E. Hassanien, “Biometric and traditional mobile authentication techniques: Overviews and open issues,” in Intelligent Systems Reference Library, Intelligen., vol. 70, Springer, 2015, pp. 423–446.
34. L. M. Mayron, “Biometric Authentication on Mobile Devices,” IEEE Secur. Priv., vol. 13, no. 3, pp. 70–73, 2015, doi: 10.1109/MSP.2015.67.
35. A. K. Jain, A. Ross, and S. Pankanti, “Biometrics: A tool for information security,” IEEE Trans. Inf. Forensics Secur., vol. 1, no. 2, pp. 125–143, 2006, doi: 10.1109/TIFS.2006.873653.
36. “Biometrics - Home.” https://biometricstoday.weebly.com/ (accessed Oct. 25, 2020).
37. T. Mehraj, B. Rasool, B. Ul, A. Baba, and P. A., “Contemplation of Effective Security Measures in Access Management from Adoptability Perspective,” Int. J. Adv. Comput. Sci. Appl.,

vol. 6, no. 8, pp. 188–200, 2015, doi: 10.14569/ijacsa.2015.060826.
38. OS Timeline, “Mobile operating system - Wikipedia,” 2020. https://en.wikipedia.org/wiki/Mobile_operating_system (accessed Oct. 25, 2020).
39. N. Gunson, D. Marshall, H. Morton, and M. Jack, “User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking,” Comput. Secur., 2011, doi: 10.1016/j.cose.2010.12.001.
40. C. Gilsenan, “SMS: The most popular and least secure 2FA method,” 2018. https://www.allthingsauth.com/2018/02/27/sms-the-most-popular-and-least-secure-2fa-method/.
41. C. Z. Acemyan, P. Kortum, J. Xiong, and D. S. Wallach, “2FA might be secure, but it’s not usable: A summative usability assessment of Google’s two-factor authentication (2FA) methods,” in Proceedings of the Human Factors and Ergonomics Society, 2018, vol. 2, pp. 1141–1145, doi: 10.1177/1541931218621262.
42. A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multifactor authentication: A survey,” Cryptography, vol. 2, no. 1, pp. 1–31, 2018, doi: 10.3390/cryptography2010001.
43. Z. Ba and K. Ren, “Addressing Smartphone-Based Multi-factor Authentication via Hardware-Rooted Technologies,” 2017, doi: 10.1109/ICDCS.2017.88.
44. S. Sanyal, A. Tiwari, and S. Sanyal, “A multifactor secure authentication system for wireless payment,” in Advanced Information and Knowledge Processing, vol. 53, 2010, pp. 341–369.
45. B. A. Oke, O. M. Olaniyi, A. A. Aboaba, and O. T. Arulogun, “Multifactor authentication technique for a secure electronic voting system,” Electron. Gov., vol. 17, no. 3, pp. 312–338, 2021, doi: 10.1504/EG.2021.115999.
46. K. Abhishek, S. Roshan, P. Kumar, and R. Ranjan, “A comprehensive study on multifactor authentication schemes,” in Advances in Intelligent Systems and Computing, 2013, vol. 177 AISC, no. VOL. 2, pp. 561–568, doi: 10.1007/978-3-642-31552-7_57.
47. J. de Zheng, “A framework for token and biometrics based authentication in computer systems,” J. Comput., vol. 6, no. 6, pp. 1206–1212, 2011, doi: 10.4304/jcp.6.6.1206-1212.
48. A. Ometov and S. Bezzateev, “Multi-factor Authentication : A Survey and Challenges in V2X Applications,” pp. 129–136, 2017.
49. M. A. Hassan, Z. Shukur, and M. K. Hasan, “An Improved Time-Based One Time Password Authentication Framework for Electronic Payments,” Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 11, pp. 359–366, 2020, doi: 10.14569/IJACSA.2020.0111146.
50. S. A. Lone and A. H. Mir, “A stable and secure one-time-password generation mechanism using fingerprint features,” Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 9, pp. 2431–2438, 2019, doi: 10.35940/ijitee.i8919.078919.
51. L. Gong, J. Pan, B. Liu, and S. Zhao, “A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords,” J. Comput. Syst. Sci., vol. 79, no. 1, pp. 122–130, 2013, doi: 10.1016/j.jcss.2012.06.002.
52. Y. Huang, Z. Huang, H. Zhao, and X. Lai, “A new One-time Password Method,” IERI Procedia, vol. 4, pp. 32–37, 2013, doi: 10.1016/j.ieri.2013.11.006.
53. A. J. T. karimov Madjit Malikovich, Khudoykulov Zarif Turakuovich, “A Method of Efficent OTP Generation Using Pseudorandom Number Generators,” in 2019 International Conference on Information Science and Communications Technologies (ICISCT), 2019, pp. 6–9.
54. H. Frank, N. David, B. Mihir, and R. Ohad, “HOTP: An HMAC-Based One-Time Password Algorithm,” tools.ietf.org. https://tools.ietf.org/html/rfc4226#section-5.3.
55. A. Beikverdi and I. K. T. Tan, “IMPROVED LOOK-AHEAD RE-SYNCHRONIZATION WINDOW FOR HMAC-BASED ONE-TIME PASSWORD,” in IET International Conference on Wireless Communications and Applications (ICWCA 2012), 2012, pp. 1–5.
56. K.-H. K. Woo-Suk Park,Dong-Yeop Jwang, “A TOTP-Based Two Factor Authentication Scheme for Hperledger Fabric Blockchain,” 2018 Tenth Int. Conf. Ubiquitous Futur. Networks, no. 1075, pp. 817–819, 1997.
57. J. Rydell, M. Pei, and S. Machani, “TOTP: Time-Based One-Time Password Algorithm,” 2011. [Online]. Available: https://www.scinapse.io/papers/2254700249.
58. D. M’Raihi, S. Machani, M. Pei, and J. Rydell, “TOTP: Time-Based One-Time Password Algorithm.” 2011, doi: 10.17487/rfc6238.
59. “Challenge–response authentication - Wikipedia.” https://en.wikipedia.org/wiki/Challenge–response_authentication.
60. V. Hayashi and W. Ruggiero, “Non-invasive challenge response authentication for voice transactions with smart home behavior,” Sensors (Switzerland), vol. 20, no. 22, pp. 1–31, 2020, doi: 10.3390/s20226563.
61. A. De Keyser, Y. Bart, X. Gu, S. Q. Liu, S. G. Robinson, and P. K. Kannan, “Opportunities and challenges of using biometrics for business: Developing a research agenda,” J. Bus. Res., vol. 136, pp. 52–62, 2021.

62. J. Y. Son, S. Noh, J. G. Choi, and H. Yoon, “A practical challenge-response authentication mechanism for a Programmable Logic Controller control system with one-time password in nuclear power plants,” Nucl. Eng. Technol., vol. 51, no. 7, pp. 1791–1798, 2019, doi: 10.1016/j.net.2019.05.012.
63. M. H. Eldefrawy, M. K. Khan, and K. Alghathbar, “One-time password system with infinite nested hash chains,” Commun. Comput. Inf. Sci., vol. 122 CCIS, pp. 161–170, 2010, doi: 10.1007/978-3-642-17610-4_18.
64. H. Choi and H. Kwon, “A Secure OTP Algorithm Using a Smartphone Application,” 2015.
65. B. N. Haller, “The S/Key One-Time Password System,” 1995. [Online]. Available: https://tools.ietf.org/html/rfc1760.
66. W. C. Kuo and Y. C. Lee, “Attack and improvement on the one-time password authentication protocol against theft attacks,” Proc. Sixth Int. Conf. Mach. Learn. Cybern. ICMLC 2007, vol. 4, no. August, pp. 1918–1922, 2007, doi: 10.1109/ICMLC.2007.4370461.
67. S. Babkin and A. Epishkina, “Authenticati o n Pr o t o c o ls Based o n O ne-Time Passw o rds,” pp. 1794–1798, 2019.
68. P. Sealy, “Get smart: why biometric cards will reshape the payments industry,” Biometric Technol. Today, vol. 2018, no. 8, pp. 5–8, 2018.
69. W. Bin Hsieh and J. S. Leu, “Design of a time and location based One-Time Password authentication scheme,” in IWCMC 2011 - 7th International Wireless Communications and Mobile Computing Conference, 2011, pp. 201–206, doi: 10.1109/IWCMC.2011.5982418.
70. S. J. Aboud, “Secure Password Authentication System Uisng Smart Card,” Int. J. Emerg. Trends Technol. Comput. Sci., vol. 3, no. January, pp. 75–79, 2014.
71. S. J. Wang and J. F. Chang, “Smart card based secure password authentication scheme,” Comput. Secur., vol. 15, no. 3, pp. 231–237, 1996, doi: 10.1016/0167-4048(96)00005-3.
72. S. Paper, P. Stewin, and J. Seifert, “SMS-Based One-Time Passwords : Attacks and Defense,” pp. 150–151, 2013.
73. N. A. Albahbooh and P. Bours, “A mobile phone device as a biometrics authentication method for an ATM terminal,” in Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 2015, pp. 2017–2024, doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.299.
74. M. Alzomai, A. J.-2010 F. I. Conference, and undefined 2010, “The mobile phone as a multi OTP device using trusted computing,” ieeexplore.ieee.org, pp. 1–3, 2010, doi: 10.1109/NSS.2010.39.
75. M. T. Maqsood and P. Shinde, “A Survey on One Time Password,” Int. J. Sci. Res., vol. 5, no. 3, pp. 142–145, 2016.
76. M. Alzomai, “The mobile phone as a multi OTP,” in 2010 Fourth International Conference on Network and System Security, 2010, no. September, pp. 75–82, doi: 10.1109/NSS.2010.39.
77. S. S. Mudholkar, “Biometrics Authentication Technique for Intrusion Detection Systems Using Fingerprint Recognition,” Int. J. Comput. Sci. Eng. Inf. Technol., vol. 2, no. 1, pp. 57–65, 2012, doi: 10.5121/IJCSEIT.2012.2106.
78. B. Ammour, L. Boubchir, T. Bouden, and M. Ramdani, “Face–Iris Multimodal Biometric Identification System,” Electron. 2020, Vol. 9, Page 85, vol. 9, no. 1, p. 85, 2020, doi: 10.3390/ELECTRONICS9010085.
79. Q. Tao and R. Veldhuis, “Biometric authentication system on mobile personal devices,” IEEE Trans. Instrum. Meas., vol. 59, no. 4, pp. 763–773, 2010, doi: 10.1109/TIM.2009.2037873.
80. S. Wang and J. Liu, “Biometrics on mobile phone,” Recent Appl. Biometrics, 2011, doi: 10.5772/17151.
81. P. Bond, “Biometric Authentication in MOOCs,” 2013, [Online]. Available: http://www.science.uva.nl/onderwijs/thesis/centraal/files/f2129185321.pdf.
82. A. El-Sisi, “Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filter,” Int. Arab J. Inf. Technol., vol. 8, no. 4, 2011.
83. E. Rahmawati et al., “Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone,” Proc. IES-ETA 2017 - Int. Electron. Symp. Eng. Technol. Appl., vol. 2017-Decem, pp. 234–238, 2017, doi: 10.1109/ELECSYM.2017.8240409.
84. D. Pawade, A. Sakhapara, A. Badgujar, D. Adepu, and M. Andrade, “Secure Online Voting System Using Biometric and Blockchain,” Adv. Intell. Syst. Comput., vol. 1042, pp. 93–110, 2020, doi: 10.1007/978-981-32-9949-8_7.
85. H. Ma, S. Yan, X. Bai, Y. Z.-P. O. F. 2013, and undefined 2013, “The research and design of identity authentication based on speech feature,” ieeexplore.ieee.org, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6553858/.
86. C. Yoo, B. T. Kang, and H. K. Kim, “Case study of the vulnerability of OTP implemented in internet banking systems of South Korea,” Multimed. Tools Appl., vol. 74, no. 10, pp. 3289–3303, 2015, doi: 10.1007/s11042-014-1888-3.