SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Review on User Authentication on Mobile Devices

Usman Abdul Gimba[1], Noor Afiza Mohd Ariffin[2, *]

[1] Department of Cyber Security, Faculty of Computing, Federal University Dutse, Jigawa, Nigeria
[2] Department of Information security, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia

ARTICLE INFO

Article history:
Received 16 Augist 2023
Received in revised form 5 December 2023
Accepted 2 March 2024
Available online 4 June 2024

Keywords:
Knowledge-based authentication; Biometric-based authentication; Physiological biometric; Behavioral biometric; Single-factor authentication; Multifactor authentication

ABSTRACT

Mobile devices have made life easier and provide great convenience in the 21st century. They give users the freedom to gain access anytime, anywhere to numerous applications with the help of information and communication technology. Online shopping, social media, and banking transactions, to name a few, are all now at our fingertips. However, they also come at a cost, as black/grey hat hackers attempt to gain access to these devices. They tend to access sensitive information on these devices by unlocking them, and, moreover, some applications and mobile services are exposed to security threats. This paper reviews the current existing authentication methods on mobile devices, which are based on knowledge and biometrics and are used for authentication. The types of authentication factors, including Single Factor, Two-Factor, and Multifactor authentication, are also discussed, along with the associated threats. The paper points out that the most secure authentication factors, and multifactor authentication is the current trend in mobile authentication.

1. Introduction

Information and Communication Technology (ICT) plays a significant role in our everyday lives, encompassing the use and access to everyday gadgets, such as mobile/smart devices that facilitate communication and provide access to various modern-day features and applications. Mobile/Smart devices are utilized for accessing social media platforms (like Twitter, WhatsApp, Instagram, etc.), emails (such as Yahoo, Gmail, etc.), performing banking transactions (such as transfers, bill payments, etc.), and engaging in business enterprises (such as buying and selling).

The usage of these mobile devices is increasing rapidly daily, and due to the sensitive information, they hold, security is paramount by Olade *et al.*, [1]. As mentioned by some researchers [1-3], most authentication schemes strike a delicate balance between security and usability. User authentication is typically categorized into three factors: something the user knows (e.g., PINs), something the user has (e.g., tokens), and something the user is (e.g., facial recognition) as mentioned by several authors [4,5].

* *Corresponding author.*
E-mail address: noorafiza@upm.edu.my

https://doi.org/10.37934/araset.46.2.2636

Security in mobile devices has evolved over the years, transitioning from traditional methods that rely on something the user knows (PINs, Android patterns, etc.) to biometric methods based on something the user is (face, fingerprint, etc.). Despite advancements in authentication, traditional methods like passwords by Barkadehi *et al.*, [6] and PINs by Stragapede *et al.*, [7]remain widely popular.

However, despite the widespread use of traditional methods, biometric authentication offers enhanced security measures as mentioned by several authors [8-11]. Innovations in authentication have introduced single-factor authentication, two-factor authentication, and multifactor authentication. Single-factor authentication (SFA) relies solely on what the user knows mentioned by several authors [12-14], representing the traditional method of authentication. SFA has a single point of failure; once an unauthorized person gains knowledge of the user's credentials, they can access the device without further scrutiny. Security provisions, typically deployed on popular computing devices like smartphones, as seen with Apple and Samsung by Chen Wang *et al.*, [13], involve two-factor authentication (2FA), adding an extra layer of security. With 2FA, access to the device is restricted even if an individual possesses the device's security credentials (e.g., password), providing an additional layer of security. 2FA applies to a wide range of everyday scenarios and offers more comprehensive security than single-factor authentication, as it combines two distinct methods of identity verification.

This research focuses on various authentication methods for mobile devices, offering a comprehensive review of both traditional and biometric authentication methods by referencing previous literature. The paper assesses different authentication methods used in mobile devices, highlighting their advantages and disadvantages, potential vulnerabilities, and the significance of two-factor and multifactor authentication.

To the best of our knowledge, such a review has not been conducted previously. While there are reviews covering different authentication methods, they often focus solely on their advantages, disadvantages, and possible vulnerabilities. In contrast, this review also delves into two/multifactor authentication and provides recommendations for the best authentication methods.

The paper is organized as follows: Section II presents related works on user authentication; Section III discusses the types of authentication factors; and Section IV concludes the paper. Figure 1 shows general user authentication methods.

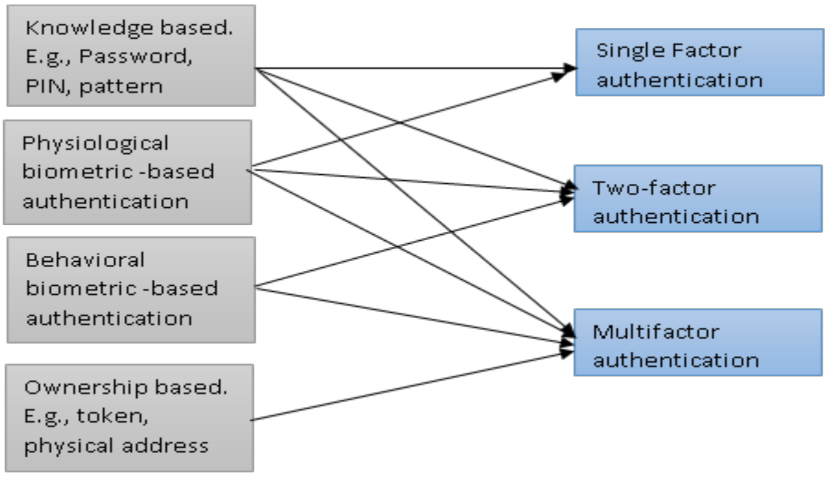
Knowledge based. E.g., Password, PIN, pattern
Physiological biometric -based authentication
Behavioral biometric -based authentication
Ownership based. E.g., token, physical address
Single Factor authentication
Two-factor authentication
Multifactor authentication

Fig. 1. General user authentication methods

2. Related Works

2.1 Knowledge-Based Authentication

Knowledge-based authentication, also referred to as the traditional authentication method by Thosar and Singh [15], is a type of user authentication method that relies on the knowledge possessed by the user. This method ideally assumes that the user's knowledge is kept secret and not shared with anyone except the authentication system. This enables the system to reject any other secret that the user or an attacker possesses, which does not match the one registered.

Knowledge-based authentication can be categorized into two categories as stated by Joshi [16]:

i. Recall-based: Recall-based techniques require the user to replicate something used during the registration stage.

ii. Recognition-based: Recognition-based techniques present an image for the user to identify and recognize the secret chosen during the registration stage.

2.1.1 Text-Based Scheme

2.1.1.1 Pins and password authentication

Text-based authentication schemes, as described by Morris and Thompson [17], have been in existence for a long time for authorizing system access. PINs, which stands for Personal Identification Numbers, consist of purely digits, while passwords can be pure text or a combination of numbers and text, sometimes even including symbols to enhance password strength. Text-based schemes remain widely used for user authentication and for protecting access to mobile devices. Prior to the advent of computers, this information was traditionally exchanged through either spoken passwords, memorized combinations, or physical locks by Zin *et al.,* [18].

According to a report by Shen *et al.,* [19], most mobile users choose text-based schemes for authentication, with 66% of users opting for PINs and passwords as their first choice. To enhance security, mobile users should memorize passwords longer than the minimum required length. However, mobile device users tend to use easily memorable PINs and passwords, such as their date of birth, making them weak and susceptible to attacks like dictionary attacks by Spaffordt [20], brute force attacks by Amico *et al.,* [21], and guessing attacks by Bonneau and Anderson [22].

2.1.1.2 Graphical authentication

Graphical authentication, sometimes referred to as graphic passwords, uses images or graphical patterns to verify users' identities. This type of authentication takes advantage of the human brain's ability to remember visual information, and it doesn't require the memorization of numbers or alphanumeric content. Studies have shown that people can recognize images more quickly than alphanumeric characters as mentioned by several authors [23-25] making graphical passwords a viable alternative to text-based methods.

Graphical authentication can be classified into two categories: recognition-based, which requires users to recognize graphical patterns, and recall-based, which requires users to replicate the same graphical pattern as mentioned by several authors [13,26]. However, graphical passwords are vulnerable to shoulder surfing attacks as mentioned by several authors [15,27].

2.1.1.2.1 Recognition-based graphic authentication

Blonder [28] introduced graphical passwords for the first time, determining if users can recognize the graphical content, they previously selected during the registration stage. According to Dhamija and Perrig [29] and Angeli *et al.,* [30], recognition-based passwords require users to select from a wide variety of graphical content during registration. During authentication, users are required to recognize the specific image they selected to prove their identity. Recognition-based passwords focus on translating information from graphical content into graphical passwords.

2.1.1.2.2 Recall-based graphic authentication

Recall-based techniques require users to replicate something they used during the registration stage, usually a drawn picture or pattern. Recall-based techniques can be further divided into two categories: pure recall-based and cued recall-based as stated by authors in two papers [31,32].

In pure recall-based techniques, users are required to recall the secret graphic content without any provided clues.

In cued recall-based techniques, users are provided with clues to help them recall the secret graphic content, making this technique easier than the pure recall-based approach.

2.2 Biometrics-Based Authentication Technique

Biometric-based authentication relies on unique information that every user is born with, verifying users based on "Who You Are." In contrast to knowledge-based authentication, which relies on "What You Know," this information is unique and cannot be obtained through theft or guesswork. Once someone gains access to the knowledge (text or graphics), they can easily bypass security measures.

According to Jain *et al.,* [33], a biometric system functions as a pattern recognition system that acquires biometric data, extracts a feature set from this data, and compares it to the template set in an individual's database. The goal of developing biometric authentication is to enhance security and safety in the digital world. Biometric techniques are categorized into two main types: behavioral biometrics and physiological biometrics.

2.2.1 Physiological biometric-based technique

Physiological biometrics consist of physical human body characteristics that are typically unique, including fingerprints, hand geometry, retina, face, or vital signs by Bours [34]. As described by Bhattacharyya *et al.,* [35], physiological biometrics encompasses physical attributes such as facial features, fingerprints, and hand characteristics. In this section, we will review the existing approaches to physiological biometric-based authentication.

2.2.1.1 Fingerprint

Fingerprint-based authentication uses a user's fingerprints to verify their identity, offering very high accuracy in identification by Radha [36]. It is the most popular form of biometric authentication. A fingerprint is the pattern of ridges and valleys on a user's fingertip, used for identity-related information in authentication. Each person has a unique fingerprint, even identical twins have different fingerprints. Mobile devices, such as the iPhone by Cherapau *et al.,* [37] and Samsung by

Chen Wang *et al.,* [13], have utilized capacitive fingerprint scanners for authentication over the years. These scanners consist of capacitive proximity sensor matrices, where a single ridge of a finger has a larger width than the spaces between them. The sensor captures and processes the fingerprint into a digital image for authentication when the finger is pressed on the scanner.

However, these capacitive proximity sensors may not perform well in rainy or dirty environments, as sweat, dust, and oil could easily alter the capacitance on the fingertip. Furthermore, due to factors such as aging, genetics, environment, or occupation, a fraction of the population may not be suitable for fingerprint-based identification.

2.2.1.2 Palmprint

Palmprints, like fingerprints, are unique to individuals and can be used for authentication. Mobile devices with built-in cameras can capture palm images and extract palm-print features for user authentication by Han *et al.,* [38]. Palmprints provide reliable recognition, even with low-resolution scanners and cameras. Line features, such as wrinkles, principal lines, and epidermal ridges, are unique among individuals and can be used for authentication. However, palmprints involve high computational costs and require a large scanner to capture the entire palm, which is why they are not commonly used for mobile device authentication.

2.2.1.3 Hand geometry

Hand geometry biometrics involve measuring the unique geometric dimensions of the hand and fingers by Ross and Jain [39]. The dimensions of the hand and fingers are measured and compared for authentication by Malatji *et al.,* [40]. Hand geometry authentication requires less computational time compared to fingerprint and palmprint methods. A camera is used to capture the hand, and the silhouette of the hand is extracted, along with some geometrical properties, which are then stored by Rani and Saurabh [41]. However, injuries, jewellery, and age may affect the results, so the hand must be in the same state as during the registration stage for successful authentication.

2.2.1.4 Face

Facial recognition systems use digital images extracted from users' facial characteristics for authentication. Modern mobile devices, such as Samsung and iPhone, have adopted facial recognition for authentication. Facial recognition techniques extract facial biometric features, including the position, size, and shape of eyes, nose, cheekbones, and jaw as mentioned by some authors [42,43]. While some facial recognition methods, as described by Galterio *et al.,* [11], focus on distinctive facial features such as nose and eye locations, mouth edges, cheekbones, and upper outlines of eye sockets. Facial recognition does not require physical contact, allows for easy template storage, has a fast identification process, and involves fewer complex statistics. For user authentication, facial characteristics are extracted and compared to templates. Access is granted if the characteristics match, and denied if they do not.

2.2.1.5 Iris

Iris recognition is another type of physiological biometric authentication that identifies users based on their unique iris patterns. The iris is complex, with patterns that are distinct and have a unique texture compared to fingerprints and faces. The uniqueness of the iris means that even identical twins have different iris patterns, and the iris is protected by eyelids, corneas, and humor by Kadëna and Ruiz [44]. Iris patterns are captured using infrared technology and then compared to authenticate the user. Iris recognition authentication extracts the user's eye information from images or videos to obtain the iris's texture pattern, which is unique, stable, and observable from a distance as stated by some authors [45-47]. To capture the iris pattern, infrared technology narrows the camera's focus to the iris pattern information, which is then stored and processed in the phone using an infrared diode by Daugman [48].

2.3 Behavioral Biometrics

Behavioral biometrics authentication relies on human behavior on their mobile devices, such as keystroke dynamics. Unlike physiological biometrics, which are based on human body parts' characteristics, behavioral biometrics are based on dynamic behavioral patterns inherent in human motions, such as touch screen tapping behavior and gait patterns by Rub *et al.*, [49]. Behavioral biometrics characteristics are less sensitive in terms of privacy compared to physiological biometrics, are difficult to disclose to adversaries, and are challenging to replicate by Cong Wang *et al.,* [50]. Additionally, they are suitable for continuous user verification because they exhibit repetitive attributes.

2.3.1 Voice recognition

Voice recognition is a type of behavioral biometric authentication that uses the user's voice sound produced by the vocal cords for user authentication. Tones of vocal timbre, cadence, and pitch are captured and compared by Malatji *et al.,* [51]. Voice/speech recognition is user-friendly as it eliminates the need for memorizing passwords and identity cards. The extraction of a user's unique voice features mainly relies on Mel-Frequency Cepstral Coefficients (MFCCs) and wavelet-based features for authentication. Voice authentication can be categorized into two types: text-dependent and text-independent. In text-dependent authentication, the user is required to speak the designated text, and it's the most widely used method in voice recognition systems as mentioned by some authors [52,53]. In text-independent authentication, it is more flexible, accepting free utterances from speakers. The idea is to identify unique vocal tract shapes, unlike text-dependent authentication that requires the reading of specific text by Variani *et al.,* [54].

2.3.2 Gait recognition

Gait recognition is a type of behavioral biometric that allows for the automatic verification of a person's identity based on the way they walk. It is a continuous authentication scheme aimed at authenticating the mobile device user as long as they carry their mobile device. Gait biometrics are divided into three categories: Machine Vision Based, Floor Sensor Based, and Wearable Sensor Based gait recognition by Derawi *et al.,* [55]. With accelerometers in mobile devices, gait recognition using accelerometers to provide unobtrusive authentication on mobile devices is possible. This makes gait recognition visible for continuous verification of a user's identity without requiring user intervention.

2.3.3 Keystroke dynamics

Due to the uniqueness of a user's typing process, the term "keystroke dynamics" has emerged by Moskovitch *et al.,* [56]. Keystroke dynamics is a technique that analyses keystrokes to distinguish between unauthorized and authorized users. It is one of the oldest methods for user validation, based on the way users' type. This technique is unique to each individual, involving their typing habits, and can be used for user verification. Typing motion can be classified into static and dynamic typing. In static typing, a user is required to type a specific text, while in dynamic typing, the user types randomly, without a specific string provided by Chen Wang *et al.,* [13]. Some of the advantages of keystroke dynamics include the absence of additional equipment, additional authentication factors, and the possibility of user access control by Vyazigin *et al.,* [57].

3. Authentication Factors

3.1 Single Factor Authentication

Single factor authentication (SFA) has been used for decades by many authentication applications. SFA is an authentication process that verifies users based on the credentials presented by the user using a single attribute. SFA is a method for securing access to systems, such as applications and networks, identifying the user requesting access based on a single set of credentials by Noor Afiza [14].

PINs and passwords are the most common examples of single-factor authentication mechanisms widely used worldwide. These two serve as a passkey for users to gain access to the required system. Single Factor Authentication is the most common and widely used method in our daily lives, such as the use of passwords in Automatic Teller Machines (ATMs), mobile devices, and computers for logins, preventing unauthorized users from accessing a system. Biometric authentication, such as fingerprint recognition and facial recognition, is also considered a form of verification method for identifying individuals' identities. Using one of these biometrics for authentication is also categorized as SFA. However, SFA is vulnerable to various attacks, including shoulder surfing, brute force attacks, guessing attacks, impersonation attacks, and social engineering attacks by Ali *et al.,* [58].

3.2 Two-Factor Authentication (2FA)

2FA employs a multi-layered identification process, where individuals seeking access are required to confirm their identity using two attributes, such as something they are and something they have/know as mentioned by several authors [58,59]. This enhances the security of user authentication, making it more challenging for an unauthorized user to gain access to the device.

In 2FA, both parameters for authentication must succeed for access to be granted. If one of the parameters fails, access to the device is denied. This makes it more difficult for attackers to gain unauthorized access, as they do not know which of the three authentication characteristics are used. However, attacks like eavesdropping, Man-In-The-Middle, forgery/Trojan horse attacks, and phishing attacks are possible in 2FA by Ali *et al.,* [58].

3.3 Multi-Factor Authentication (MFA)

MFA also employs a multi-layered identification process. Unlike 2FA, which requires only two parameters for authentication, MFA combines two or more parameters for authentication. The three factors used for authenticating users are something they are, something they have, and something they know as mentioned by several authors [58,60]. Traditional multi-factor methods require users to provide two or more different types of authentication parameters, such as PINs and fingerprints, often involving additional costs and user effort by Chen Wang *et al.,* [13].

MFA has been proven to be more secure, especially when the authentication factors are physically separated from the device. The use of biometrics enhances identity verification and has a profound impact on system security. Attacks on MFA are minimal because attackers would need knowledge of two or three authentication factors to gain access to the device.

4. Conclusion

Mobile devices have become an integral part of our daily lives, and with the advent of ICT, most tasks can now be conveniently performed on these devices. This makes the security of mobile devices paramount. Mobile device authentication is a technology used to prevent unauthorized access to the device and protect the sensitive information stored by the genuine user. This paper provides a review of authentication approaches for mobile devices, including knowledge-based, biometric-based, and ownership-based methods.

We have reviewed knowledge-based authentication (text-based and graphical-based), discussed their brief history, and recognized their high usability, despite their vulnerability to different attacks such as shoulder surfing and guess password attacks. Biometric authentication is classified into two categories: physiological and behavioral authentication, both of which offer high security compared to knowledge-based methods but may have lower usability. Physiological biometrics rely on physical aspects of a person, such as the face and fingerprint, which are permanent features that cannot be forgotten or changed. Behavioral biometrics are based on how individuals behave, including aspects like gait and finger gestures, which can change over time and may suffer from low-fidelity sensor readings.

The types of authentication factors include Single factor, Two-Factor, and Multifactor. Single Factor Authentication (SFA) requires only one authentication approach, either knowledge-based or biometric-based. SFA has a single point of failure and is vulnerable to attacks. Two-Factor Authentication (2FA) requires two authentication approaches, typically something you know and something you have/are, and both must be fulfilled to gain access to the device. Multifactor Authentication (MFA) requires at least two or more approaches, which is a combination of knowledge-based and biometric-based methods. MFA is the most secure authentication approach with minimal vulnerability to attacks.

In the future, we plan to conduct an in-depth systematic review of user authentication on mobile devices, with a focus on newly developed authentication approaches and threats to mobile device authentication. Our goal is to integrate multifactor authentication approaches that can protect against various attacks using the available sensors on mobile devices without significantly increasing the cost of the devices.

Acknowledgement

This research was funded by Petroleum Technology Development Fund (PTDF), under Ministry of Petroleum Resources, Nigeria.

References

[1] Olade, Ilesanmi, Hai-ning Liang, and Charles Fleming. "A review of multimodal facial biometric authentication methods in mobile devices and their application in head mounted displays." *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)* (2018): 1997-2004. https://doi.org/10.1109/SmartWorld.2018.00334

[2] Tari, Furkan, A. Ant Ozok, and Stephen H. Holden. "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords." In *Proceedings of the second symposium on Usable privacy and security*, pp. 56-66. 2006. https://doi.org/10.1145/1143120.1143128

[3] Melicher, William, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. "Usability and security of text passwords on mobile devices." In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 527-539. 2016. https://doi.org/10.1145/2858036.2858384

[4] Skračić, K., P. Pale, and B. Jeren. "Knowledge based authentication requirements." In *2013 36th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1116-1120. IEEE, 2013.

[5] Dostálek, Libor. "Multi-factor authentication modeling." In *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)*, pp. 443-446. IEEE, 2019. https://doi.org/10.1109/ACITT.2019.8780068

[6] Barkadehi, Mohammadreza Hazhirpasand, Mehrbaksh Nilashi, Othman Ibrahim, Ali Zakeri Fardi, and Sarminah Samad. "Authentication systems: A literature review and classification." *Telematics and Informatics* 35, no. 5 (2018): 1491-1511. https://doi.org/10.1016/j.tele.2018.03.018

[7] Stragapede, Giuseppe, Ruben Vera-Rodriguez, Ruben Tolosana, Aythami Morales, Alejandro Acien, and Gaël Le Lan. "Mobile behavioral biometrics for passive authentication." *Pattern Recognition Letters* 157 (2022): 35-41. https://doi.org/10.1016/j.patrec.2022.03.014

[8] Gupta, Sandeep, Rajesh Kumar, Mouna Kacimi, and Bruno Crispo. "IDeAuth: A novel behavioral biometric-based implicit deauthentication scheme for smartphones." *Pattern Recognition Letters* 157 (2022): 8-15. https://doi.org/10.1016/j.patrec.2022.03.011

[9] Dargan, Shaveta, and Munish Kumar. "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities." *Expert Systems with Applications* 143 (2020): 113114. https://doi.org/10.1016/j.eswa.2019.113114

[10] Abazi, Blerton, Besnik Qehaja, and Edmond Hajrizi. "Application of biometric models of authentication in mobile equipment." *IFAC-PapersOnLine* 52, no. 25 (2019): 543-546. https://doi.org/10.1016/j.ifacol.2019.12.602

[11] Galterio, Mary Grace, Simi Angelic Shavit, and Thaier Hayajneh. "A review of facial biometrics security for smart devices." *Computers* 7, no. 3 (2018): 37. https://doi.org/10.3390/computers7030037

[12] Mohamed, Tamara S. "Security of Multifactor Authentication Model to Improve Authentication Systems." *Inf. Knowl. Manag. J* 4 (2014): 81-86.

[13] Wang, Chen, Yan Wang, Yingying Chen, Hongbo Liu, and Jian Liu. "User authentication on mobile devices: Approaches, threats and trends." *Computer Networks* 170 (2020): 107118. https://doi.org/10.1016/j.comnet.2020.107118

[14] Ariffin, Noor Afiza Mohd. "A multi-factor authentication scheme using attack recognition and key generator technique." Doctoral thesis. 2017.

[15] Thosar, Devidas S., and Manmohan Singh. "A Review on Advanced Graphical Authentication to Resist Shoulder Surfing Attack." In *2018 International Conference on Advanced Computation and Telecommunication (ICACAT)*, pp. 1-3. IEEE, 2018. https://doi.org/10.1109/ICACAT.2018.8933699

[16] Joshi, Ashish, Sonu Kumar, and R. H. Goudar. "A more multifactor secure authentication scheme based on graphical authentication." In *2012 International Conference on Advances in Computing and Communications*, pp. 186-189. IEEE, 2012. https://doi.org/10.1109/ICACC.2012.43

[17] Morris, Robert, and Ken Thompson. "Password security: A case history." *Communications of the ACM* 22, no. 11 (1979): 594-597. https://doi.org/10.1145/359168.359172

[18] Zin, Muhamad Zulfikri Md, Raihana Md Saidi, Faridah Sappar, and Mohamad Asrol Arshad. "Multi-factor Authentication to Authorizing Access to an Application: A Conceptual Framework." (2019).

[19] Teh, Pin Shen, Ning Zhang, Syh-Yuan Tan, Qi Shi, Wee How Khoh, and Raheel Nawaz. "Strengthen user authentication on mobile devices by using user's touch dynamics pattern." *Journal of Ambient Intelligence and Humanized Computing* 11 (2020): 4019-4039. https://doi.org/10.1007/s12652-019-01654-y

[20] Spafford, Eugene H. "Opus: Preventing weak password choices." *Computers & Security* 11, no. 3 (1992): 273-278. https://doi.org/10.1016/0167-4048(92)90207-8

[21] Dell'Amico, Matteo, Pietro Michiardi, and Yves Roudier. "Password strength: An empirical analysis." In *2010 Proceedings IEEE INFOCOM*, pp. 1-9. IEEE, 2010.

[22] Bonneau, Joseph, Sören Preibusch, and Ross Anderson. "A birthday present every eleven wallets? the security of customer-chosen banking pins." In *Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers 16*, pp. 25-40. Springer Berlin Heidelberg, 2012. https://doi.org/10.1007/978-3-642-32946-3_3

[23] Tabrez, Shums. "A multi-phase authentication system for data protection with the assistance of graphical password and fingerprint authentication system against shoulder surfing attacks." *Advances in Computational Sciences and Technology* 10, no. 10 (2017): 3015-3031. https://doi.org/10.1109/ICCONS.2017.8250568

[24] Van Balen, Nicolas Jorge. "Enhancing usability and security through alternative authentication methods." (2017).

[25] Fatehah, M. D., Mohd Zalisham Jali, M. K. Wafa, and Nor Badrul Anuar. "Educating users to generate secure graphical password secrets: An initial study." In *2013 IEEE 5th Conference on Engineering Education (ICEED)*, pp. 26-31. IEEE, 2013. https://doi.org/10.1109/ICEED.2013.6908297

[26] Golar, Priti C., and Brijesh Khandelwal. "Study of Usability Parameter for Graphical Based Authentication System." In *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, pp. 23-26. IEEE, 2020. https://doi.org/10.1109/SMART50582.2020.9337116

[27] Aravindh, B., VD Ambeth Kumar, G. Harish, and V. Siddartth. "A novel graphical authentication system for secure banking systems." In *2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, pp. 177-183. IEEE, 2017. https://doi.org/10.1109/ICSTM.2017.8089147

[28] G. E. Blonder, “Graphics Password.pdf.” 1996.

[29] Dhamija, Rachna, and Adrian Perrig. "Deja {Vu--A} User Study: Using Images for Authentication." In *9th USENIX Security Symposium (USENIX Security 00)*. 2000.

[30] De Angeli, Antonella, Mike Coutts, Lynne Coventry, Graham I. Johnson, David Cameron, and Martin H. Fischer. "VIP: a visual approach to user authentication." In *Proceedings of the working conference on advanced visual interfaces*, pp. 316-323. 2002. https://doi.org/10.1145/1556262.1556312

[31] Gokhale, Mrs Aakansha S., and Vijaya S. Waghmare. "The shoulder surfing resistant graphical password authentication technique." *Procedia Computer Science* 79 (2016): 490-498. https://doi.org/10.1016/j.procs.2016.03.063

[32] ALSaleem, Bandar Omar, and Abdullah I. Alshoshan. "Multi-factor authentication to systems login." In *2021 National Computing Colleges Conference (NCCC)*, pp. 1-4. IEEE, 2021. https://doi.org/10.1109/NCCC49330.2021.9428806

[33] Jain, Anil K., Arun Ross, and Salil Prabhakar. "An introduction to biometric recognition." *IEEE Transactions on circuits and systems for video technology* 14, no. 1 (2004): 4-20. https://doi.org/10.1109/TCSVT.2003.818349

[34] Bours, Patrick. "Continuous keystroke dynamics: A different perspective towards biometric evaluation." *Information Security Technical Report* 17, no. 1-2 (2012): 36-43. https://doi.org/10.1016/j.istr.2012.02.001

[35] Bhattacharyya, Debnath, Rahul Ranjan, Farkhod Alisherov, and Minkyu Choi. "Biometric authentication: A review." *International Journal of u-and e-Service, Science and Technology* 2, no. 3 (2009): 13-28.

[36] Radha, N., and A. Kavitha. "Rank level fusion using fingerprint and iris biometrics." *Indian Journal of Computer Science and Engineering* 2, no. 6 (2012): 917-923.

[37] Cherapau, Ivan, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. "On the Impact of Touch {ID} on {iPhone} Passcodes." In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 257-276. 2015.

[38] Han, Chin-Chuan, Hsu-Liang Cheng, Chih-Lung Lin, and Kuo-Chin Fan. "Personal authentication using palm-print features." *Pattern recognition* 36, no. 2 (2003): 371-381. https://doi.org/10.1016/S0031-3203(02)00037-7

[39] Ross, Arun, and Anil Jain. "Information fusion in biometrics." *Pattern recognition letters* 24, no. 13 (2003): 2115-2125. https://doi.org/10.1016/S0167-8655(03)00079-5

[40] Malatji, Wiliiam Ratjeana, Rene van Eck, and Tranos Zuva. "Acceptance of biometric authentication security technology on mobile devices." In *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, pp. 1-5. IEEE, 2020. https://doi.org/10.1007/978-981-33-4909-4_11

[41] Rani, Garima, and Anshuman Saurabh. "An overview of biometric techniques." *Journal of Emerging Technologies and Innovative Research* 1 (2014).

[42] Liu, Tao, Jian-Xun Mi, Ying Liu, and Chao Li. "Robust face recognition via sparse boosting representation." *Neurocomputing* 214 (2016): 944-957. https://doi.org/10.1016/j.neucom.2016.06.071

[43] Li, Hanxi, Peng Wang, and Chunhua Shen. "Robust face recognition via accurate face alignment and sparse representation." In *2010 International Conference on Digital Image Computing: Techniques and Applications*, pp. 262-269. IEEE, 2010. https://doi.org/10.1109/DICTA.2010.54

[44] Kadëna, Esmeralda, and Lourdes Ruiz. "Adoption of biometrics in mobile devices." *FIKUSZ'17 Proceedings* (2017): 124.

[45] Fahmi, PN Ali, Elyor Kodirov, Deok-Jai Choi, Guee-Sang Lee, A. Mohd Fikri Azli, and Shohel Sayeed. "Implicit authentication based on ear shape biometrics using smartphone camera during a call." In *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 2272-2276. IEEE, 2012. https://doi.org/10.1109/ICSMC.2012.6378079

[46] Kumar, Ajay, and Arun Passi. "Comparison and combination of iris matchers for reliable personal authentication." *Pattern recognition* 43, no. 3 (2010): 1016-1026. https://doi.org/10.1016/j.patcog.2009.08.016

[47] Lim, Shinyoung, Kwanyong Lee, Okhwan Byeon, and Taiyun Kim. "Efficient iris recognition through improvement of feature vector and classifier." *ETRI journal* 23, no. 2 (2001): 61-70. https://doi.org/10.4218/etrij.01.0101.0203

[48] Daugman, John. "How iris recognition works." In *The essential guide to image processing*, pp. 715-739. Academic Press, 2009. https://doi.org/10.1016/B978-0-12-374457-9.00025-1

[49] Rüb, Matthias, Jan Herbst, Christoph Lipps, and Hans Dieter Schotten. "No One Acts like You: AI based Behavioral Biometric Identification." In *2022 3rd International Conference on Next Generation Computing Applications (NextComp)*, pp. 1-7. IEEE, 2022. https://doi.org/10.1109/NextComp55567.2022.9932247

[50] Wang, Cong, Yanru Xiao, Xing Gao, Li Li, and Jun Wang. "A framework for behavioral biometric authentication using deep metric learning on mobile devices." *IEEE Transactions on Mobile Computing* 22, no. 1 (2021): 19-36. https://doi.org/10.1109/TMC.2021.3072608

[51] Malatji, Wiliiam Ratjeana, Rene van Eck, and Tranos Zuva. "Acceptance of biometric authentication security technology on mobile devices." In *2020 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, pp. 1-5. IEEE, 2020. https://doi.org/10.1007/978-981-33-4909-4_11

[52] H. Gish *et al.*, "Cambridge, MA 02238," pp. 379–382, 1985.

[53] Reynolds, Douglas A., and Richard C. Rose. "Robust text-independent speaker identification using Gaussian mixture speaker models." *IEEE transactions on speech and audio processing* 3, no. 1 (1995): 72-83. https://doi.org/10.1109/89.365379

[54] Variani, Ehsan, Xin Lei, Erik McDermott, Ignacio Lopez Moreno, and Javier Gonzalez-Dominguez. "Deep neural networks for small footprint text-dependent speaker verification." In *2014 IEEE international conference on acoustics, speech and signal processing (ICASSP)*, pp. 4052-4056. IEEE, 2014. https://doi.org/10.1109/ICASSP.2014.6854363

[55] Derawi, Mohammad Omar, Claudia Nickel, Patrick Bours, and Christoph Busch. "Unobtrusive user-authentication on mobile phones using biometric gait recognition." In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 306-311. IEEE, 2010. https://doi.org/10.1109/IIHMSP.2010.83

[56] Moskovitch, Robert, Clint Feher, Arik Messerman, Niklas Kirschnick, Tarik Mustafic, Ahmet Camtepe, Bernhard Lohlein et al. "Identity theft, computers and behavioral biometrics." In *2009 IEEE International Conference on Intelligence and Security Informatics*, pp. 155-160. IEEE, 2009. https://doi.org/10.1109/ISI.2009.5137288

[57] Vyazigin, Andrey A., Nadezhda Y. Tupikina, and Eugene V. Sypin. "Software tool for determining of the keystroke dynamics parameters of personal computer user." In *2019 20th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM)*, pp. 166-171. IEEE, 2019. https://doi.org/10.1109/EDM.2019.8823502

[58] Ali, Guma, Mussa Ally Dida, and Anael Elikana Sam. "Two-factor authentication scheme for mobile money: A review of threat models and countermeasures." *Future Internet* 12, no. 10 (2020): 160. https://doi.org/10.3390/fi12100160

[59] Pahlevi, Rizka Reza, Vera Suryani, Hilal Hudan Nuha, and Rahmat Yasirandi. "Secure two-factor authentication for iot device." In *2022 10th International Conference on Information and Communication Technology (ICoICT)*, pp. 407-412. IEEE, 2022. https://doi.org/10.1109/ICoICT55009.2022.9914866

[60] Bartłomiejczyk, Maciej, and Mirosław Kurkowski. "Multifactor authentication protocol in a mobile environment." *IEEE Access* 7 (2019): 157185-157199. https://doi.org/10.1109/ACCESS.2019.2948922