Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 7, pp. 2007–2024
DOI : 10.47974/JDMSC-1840

Comprehensive analysis of continuous authentication for mobile devices

Aishani Dagar *
Modern School
Barakhamba Road
New Delhi
India

Karan Singh †
Tayyab Khan §
School of Computer & Systems Sciences
Jawaharlal Nehru University
New Delhi
India

Abstract

Continuous mobile authentication is an imperative aspect of ensuring the security and privacy of data in the contemporary mobile computing landscape. With the proliferation of mobile devices and the increasing dependency on mobile applications, traditional authentication methods are steadily becoming inadequate to protect sensitive information from unauthorized access. Continuous authentication techniques aim to provide ongoing and seamless verification of user identities, enhancing security while minimizing user inconvenience. This survey paper presents a comprehensive analysis of traditional authentication methods, highlighting key techniques, their integration in mobile systems, applications, and limitations. Then, we elaborate on the various techniques employed in continuous authentication. By examining the strengths and weaknesses of different approaches, this survey aims to provide researchers, practitioners, and developers with a

* *E-mail:* aishanidagar26@gmail.com (Corresponding Author)
† *E-mail:* tayyabkhan.cse2012@gmail.com
§ *E-mail:* karancs12@gmail.com

comprehensive understanding of continuous mobile authentication, enabling them to make informed decisions when implementing authentication mechanisms in mobile applications.

Subject Classification: *68P27.*

Keywords: *Continuous mobile authentication, Security, Data protection, Mobile devices, Seamless verification, Authentication mechanism, Survey.*

I. Introduction

Mobile devices have become an indispensable part of our daily lives, serving as a hub for communication, connectivity, and a wide range of activities. With their ever-growing capabilities, mobile phones have garnered immense popularity and have transformed into essential tools for telephony, social networking, multimedia entertainment, photography, online banking, navigation, health and fitness, productivity, education and business operations. As of 2022, the global number of smartphone users reached a staggering 6.4 billion individuals [1], showcasing the ubiquitous nature of these devices and their impact on society. As the locus of human lives, mobile devices harbor sensitive information which makes their data privacy, security and protection of paramount importance. The rising preponderance of mobile devices calls for the adoption of novel and secure authentication techniques to disable unauthorized access.

Authentication is the crucial process of verifying a user's identity. There are two major categories of authentications: traditional and biometric. A summary of these two categories are shown in Figure 1 [2]. Conventional mobile authentication methods have significant limitations in terms of security. They are susceptible to various attacks such as shoulder surfing and smudge attacks. Additionally, these methods only provide authentication at the entry point. Once an unauthorized individual gains access to the device, there are no fallback measures in place to safeguard the data. In December 2022, the number of global mobile cyber-attacks was approximately 2.2 million [3].

Conventional authentication techniques are insufficient to adequately safeguard the vast amount of sensitive data stored on users' devices. Therefore, it is advisable to implement continuous authentication, which falls under the umbrella of behavioral biometrics, as a more robust security measure. Continuous authentication for mobile users is adaptive and continuous authentication by multiple ways, such as unique finger gestures, facial recognition, touch gestures, behavioral attributes, etc of a mobile user. With minimal user intervention, no additional hardware and

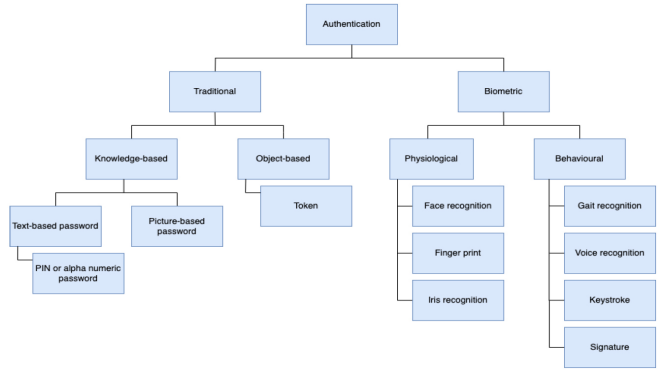

Figure 1

Classification of Authentication Techniques

high accuracy rates, continuous authentication methods promise data protection on mobile devices. Methods such as gait, power consumption, voice recognition, keystroke dynamics, behavioural profile etc. comes under continuous authentication.

A. *Background*

Mobile phones have become an indispensable component of our lives. With advent in technology, mobile phones have developed increasingly secure authentication systems [18-20]. However, as the preponderance of mobile phones continues to rise, the authentication systems implemented have struggled to keep pace. In the digital era, where our phones store vital and sensitive information, it is crucial to execute robust data protection.

This paper aims to examine the functionality of various traditional mobile authentication methods and provide an in-depth analysis of continuous authentication systems. By comparing and contrasting these different methods based on specific criteria, we will evaluate their strengths and weaknesses. Additionally, we will explore the future prospects and potential advancements in the field of continuous authentication.

B. *Motivation*

The primary objective of this study is twofold. Firstly, we aim to provide an overview of traditional authentication techniques, examining their functionality and identifying their limitations. Secondly, we seek to

classify and analyze Behavioral Biometrics (BB) and Continuous Authentication (CA) in the context of mobile devices. Moreover, we conduct a comparative study to differentiate between various CA methods, outlining the advantages and disadvantages associated with each approach. Lastly, our discussions delve into the insights gained, the existing challenges, and the anticipated future trends in the field.

C. Contribution

The contribution of this paper can be summarized as follows:

- We address the inadequacy of traditional authentication methods in safeguarding sensitive information on mobile devices. The paper presents an overview of traditional authentication techniques, analyzes their functioning, and identifies their limitations.
- We explore the emergence of continuous authentication techniques that provide ongoing and seamless verification of user identities.
- We further classify and analyze the categories of Behavioral Biometrics (BB) and Continuous Authentication (CA) in mobile devices, comparing their advantages and disadvantages.
- The discussions cover lessons learned, current challenges, and future trends in mobile authentication.

II. Traditional Techniques

A. Text-based Passwords

Text-based passwords encompass various forms such as PINs, PUKs, and alphanumeric passwords. However, this authentication technique

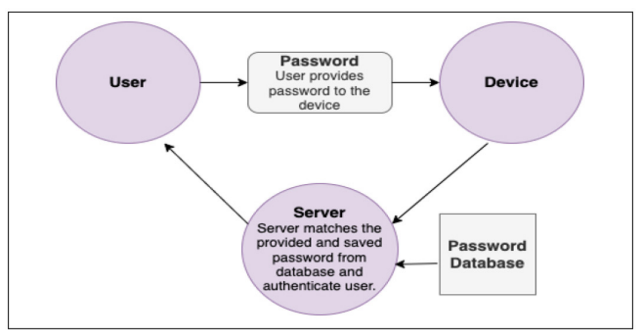

Figure 2

Text-based Passwords

faces several challenges, including the difficulty of remembering passwords, vulnerability to shoulder surfing attacks, the tendency to reuse passwords across various different accounts, the risk of writing passwords down to keep them in memory, the need for customer service when wrong PUK code is entered, weak passwords, the absence of password and no password usage altogether. Despite these issues, password authentication holds an advantage over other methods as it can be easily changed at any time (Figure 2).

B. *Picture-based Passwords*

Graphical passwords were introduced as a solution to the memorization challenge associated with alphanumeric passwords. The concept is based on the belief that users find it easier and more natural to authenticate using image recall. As a result, graphical passwords overcome the drawbacks of alphanumeric passwords. The benefits of graphical passwords include the provision of highly secure systems, user-friendly password options, resistance to dictionary attacks and brute force searches. However, there are also challenges associated with graphical passwords, such as the requirement for increased storage space, longer registration times for passwords, and vulnerability to shoulder-surfing attacks [6].

The Picture Password authentication mechanism comprises two main components: initial password enrollment and subsequent password verification. Graphical-based password schemes can be categorized into four primary types:

- Recognition-Based Systems: Users are challenged to identify images they had previously selected during the registration process. This method typically requires users to memorize a set of images and then identify them during login [7].
- Recall-Based Systems: Pure Recall-Based Systems: Users are required to reproduce passwords they created or selected during the registration stage from memory [7].
- Cued Recall-Based Systems: Users are provided with hints or cues to assist them in recalling their passwords [7].
- Hybrid Systems: These systems combine two or more schemes, such as a combination of recognition and recall-based methods or a blend of textual and graphical password schemes [8].

C. *One-time Passwords*

OTP systems can be considered as a bridge between a static password authentication and a better authentication method. As OTP generates a password, the verification requires synchronisation between the token and the monitor (Figure 3). There are several categories of OTP, depending on counter synchronised, time synchronised, involving a secure channel, or with a shared list of passwords.

There are two primary OTP algorithms: HMAC-based One-time Password (HOTP) and Time-based One-time Password (TOTP). HOTP utilizes a Hash-based Message Authentication Code (HMAC) and operates as an event-based OTP, where each code is derived from a counter. In simpler terms, pressing a button generates a new password for logging in, and with each validation, the moving factor is incremented based on a counter.

Time-based One-time Password (TOTP) is an OTP that operates based on time. Similar to HOTP, TOTP uses a static seed, but the significant difference is that the moving factor in TOTP is based on time instead of a counter. The TOTP token contains an internal clock that synchronizes with the server's clock. New passwords are generated by utilizing the value of the current timestamp [9][10].

One-time passwords (OTPs) offer several advantages, including their resistance to cracking during replay attacks, avoidance of risks associated with traditional passwords, and enhanced security. However, there are also drawbacks to consider. These include the need for additional

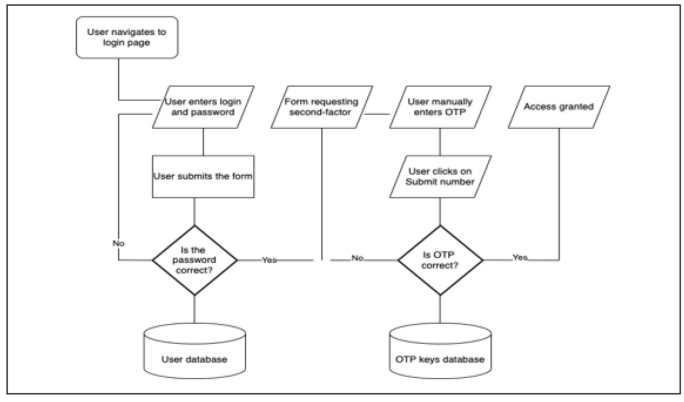

Figure 3

OTP-based Passwords

technology, the potential for security tokens to fail or break, and the potential complexity of the OTP generation process [11].

D. *Face Recognition*

Face recognition is a method of biometric identification that enables the identification, verification, and authentication of individuals by analysis of their unique facial biometric patterns and data (Figure 4).

Unlike other authentication methods that require memorization, face recognition offers the advantage of utilizing built-in sensors in smartphones, eliminating the need for additional equipment or requirements.

The development of a robust face recognition system involves three fundamental steps: face detection, feature extraction, and face recognition. Face detection is responsible for locating and identifying human faces within the captured images. Feature extraction extracts the relevant characteristics of the detected faces, generating feature vectors. Finally, in the face recognition step, the extracted features are compared with template face databases to determine the identity of the person [12].

However, this authentication model faces several challenges that affect its accuracy. These challenges include factors such as aging, occlusion (obstacles in the image, such as objects or parts of the face being covered),

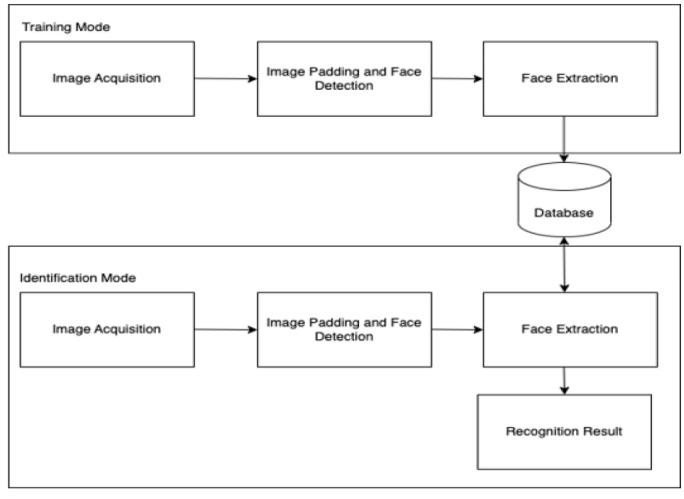

Figure 4

Face Recognition

variations in pose (different angles or orientations of the face), and variations in illumination (changes in lighting conditions) .

E. *Fingerprint*

Fingerprint authentication involves scanning a user's fingerprint using a mobile device's fingerprint sensor to verify their identity (Figure 5). This process analyzes various characteristics of the fingerprint, such as pressure, the three-dimensional shape of the finger, ridges, valleys, and other features through different sensors like optical, capacitive and ultrasonic sensors [13]. The information is then processed by the device's pattern analysis/matching software, which compares it to the list of registered fingerprints on file. A successful match means that an identity has been verified, thereby granting access. Attacking applications that use biometric-based authentication poses a lower risk compared to those relying on password-based authentication. However, this method faces several challenges in accurately extracting fingerprint information. Genetic factors, injuries to the fingers, and the natural aging process can affect the human fingerprint. Additionally, fingerprint readers are unable to distinguish between a live finger and a severed one [2].

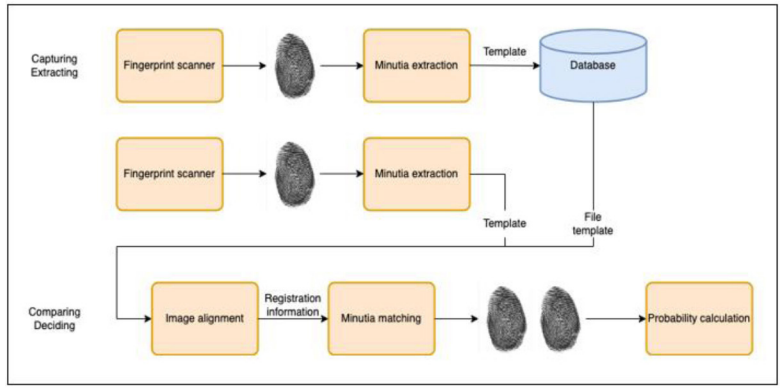

Figure 5

Fingerprint

F. Iris recognition

Iris recognition is a method of mobile authentication that relies on scanning a person's iris. This process involves using a specialized digital camera that captures a clear and high-contrast image of the iris using visible and near-infrared light. The camera focuses on the eye, identifying

the center of the pupil, the pupil's edge, the iris's edge, as well as the eyelids and eyelashes. This information is then processed by Iris Recognition software, which analyzes the unique iris pattern and converts it into an iris template[14] (Figure 6).

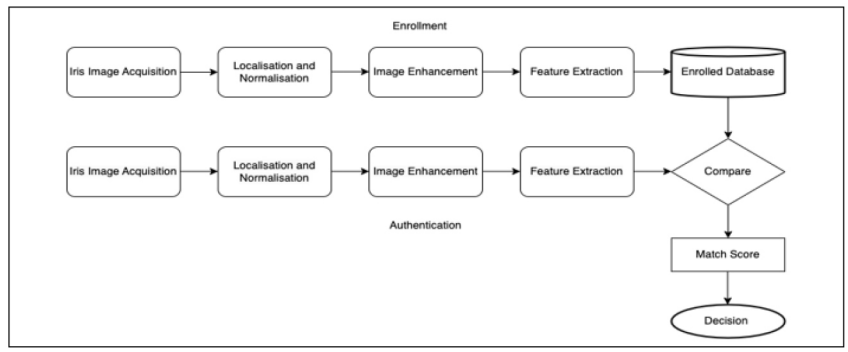

Figure 6

Iris Recognition

III. Continuous Authentication

A. *Gait dynamics-based continuous authentication systems*

Continuous authentication systems that are based on gait dynamics use individuals' walking patterns to identify them. The required gait data is captured by embedded accelerometer and gyroscope in mobile devices (Figure 7). Classifiers distinguish between different users using unique

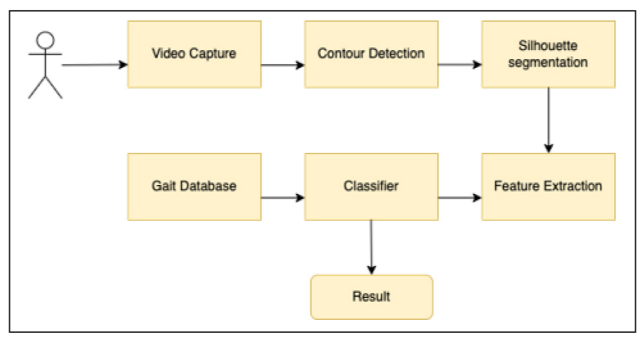

Figure 7

Gait-based Authentication

characteristics extracted from raw data. Over the past few years, diverse methodologies have come to light for gait-based authentication on mobile devices, depending on the types of features extracted from raw data and the authentication methods employed.

By granting a non-intrusive authentication method for mobile devices with accelerometers, gait recognition offers a significant advantage. As a result, this technology facilitates seamless and continuous verification of user identity without the need for user intervention [15].

The overall process of gait recognition typically involves five steps that are highlighted in the figure: video capture silhouette segmentation, contour detection, feature extraction and classification [2].

On the other hand, gait-based approaches do not showcase a high accuracy level in user authentication. Gait based authentication systems encounter several challenges namely requirement for numerous data sources, optimal sensors placement, lack of authentication in stagnant user, and concerns regarding reliability. First and foremost, acquiring sensory data related to gait necessitates the collection of both visual information and motion data using multiple sensors. Furthermore, device placement can greatly alter sensory readings. When the user is not moving, alternative authentication tasks are requires for CA. Lastly, the state if the user during enrolment might not align later on due to the dependency of gait-based traits on the user's physical condition [16].

B. *Voice Recognition*

Voice-related characteristics encompass both physiological aspects and behavioral traits, enabling the analysis of speech across a wide range of features (Figure 8). A distinctive combination of the anatomical feature of one's vocal tract, mouth, larynx and nose and influence of life experiences

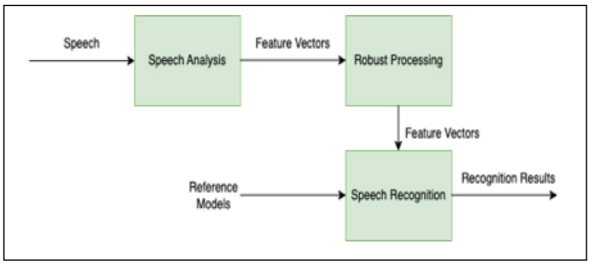

Figure 8

Voice Recognition

that mould one's manners, rhythm, accent, vibration of their speech form an individual person's voice.

A speaker can be authenticated through two ways: text-dependent approach and text independent approach. In the former approach, users voice a pre-defined phrase for verification and identification. Although this method is straightforward and highly accurate, it disables transparent, continuous authentication and does not rely on a secret-based mechanism. The latter approach grants higher flexibility, particularly for transparent authentication, but low accuracy attributable to the dynamic alterations in the feature space of voice input, which encompass factors such as user condition and environmental conditions. Under this approach, users are identified by voice regardless of spoken words.

User identification through voice features adheres to the standard process, commencing with data collection and preprocessing, progressing to feature extraction and selection, and concluding with modeling and pattern recognition. The accuracy of this approach is majorly affected by feature quality, evaluated on feature distinctiveness and ability to withstand potential noice sources introduced by factors such as user condition and environmental variables.

Initial voice recognition applications were numerous, namely access control, personalization, and forensic and criminal investigations. However, the scope of applications has expanded to include online banking, where customers can conduct transactions through voice communication as the voice recognition system ensures transparent and continuous authentication of the customer.

The advantages of employing voice recognition for biometric authentication systems is the prevalence of microphones in mobile devices and the inherent naturalness associated with both speaking and being recognized by one's voice.

The shortcomings of this authentication model are background noise, voice variations due to user physical and emotional state, adverbial attacks, system overhead in terms of both power and computation and low usability due to variable accuracy rates [16].

Furthermore, speaking continuously is often unnatural in most applications. Therefore, for the purpose of continuous recognition, the optimal approach is to combine voice with other traits. It is also advisable to utilize it in applications where frequent speech is anticipated to avoid compelling users to speak unnecessarily [2].

C. *Keystroke Dynamics*

Keystroke dynamics involves recognizing an individual based on their typing rhythm (Figure 9). The process of keystroke dynamics includes extracting various features such as duration, latency, pressure, and location. Duration refers to the time span between pressing and releasing a key. Latency represents the time between releasing one key and pressing the next key. Pressure indicates the force applied to a key, while location refers to the specific finger position or area on the screen. Additional metrics, such as error rate (frequency of using backspaces or deletion options), can also be employed. It is possible to utilize other metrics as well in keystroke dynamics analysis.

Keystroke dynamics-based methods have several advantages, namely high authentication accuracy, high power efficiency, hardware independence, implicit processing and resistance to shoulder surfing attacks.

However, implementing a keystroke dynamics-based approach can be challenging for several reasons, namely variations in user behaviour, vulnerability of extracted metrics to noise and behavioural changes. Additional challenges may arise in relation to typing with different languages and potential variations in a user's typing behavior across languages [16].

D. *Signature Recognition*

In this authentication technique, the system analyses how a user signs on the touch-screen of a mobile by extracting some features, namely time, speed, acceleration, pressure, and direction [2] (Figure 10).

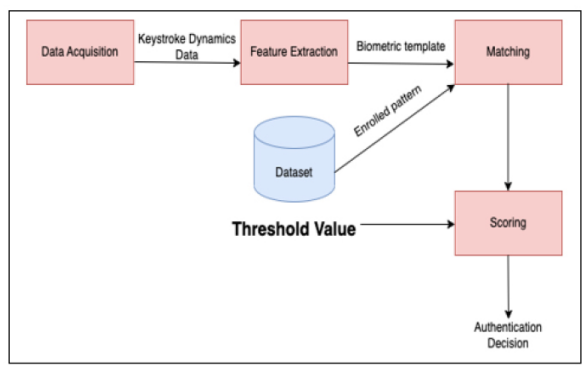

Figure 9

Keystroke Dynamics

Various devices are utilized for capturing and verifying mobile-biometric signatures, with the gyroscope and accelerometer being the two crucial components in mobile devices [17].

The accelerometer in mobile devices is responsible for determining the phone's orientation. On the other hand, the gyroscope is utilized to estimate the angular rotational velocity. These devices enable measurements of pen-tilt angles, hand movements, tablet direction, and other related aspects. Electronic pens used for signing purposes are also employed to extract various signature features, including position coordinates, velocity, pen pressure, and pen angles. This process involves the use of laser diodes, resonance frequency, magnetoelastic sensors, strain gauges, and similar technologies [17].

Since handwritten signature is an established means of individual authentication and is socially accepted; therefore, combining these two into one system would produce a foolproof and efficient biometric authentication system on the go [17]. There are five modules to a standard signature verification system: pre-processing, feature extraction, enrollment, similarity computation and score normalization. Firstly, signal obtained from the touch signature or pen movement on screen are digitised. In pre-processing, any missing parts of the signature are reconstructed. During feature extraction, a feature vector is generated from each acquired signal, consisting of signature duration or average speed. These features are either enrolled as templates or utilized by a statistical model that represents the generated signatures. The similarity computation module compares the claimed identity with the enrolled templates by calculating a similarity score. To grant access to the claimed user, score normalization is applied to standardize the similarity scores within a predefined range and compare the resulting score with a

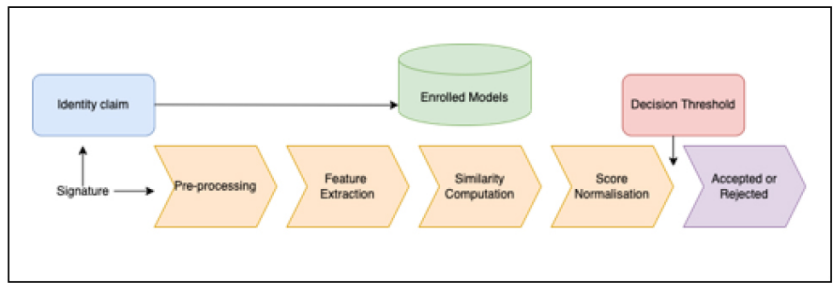

Figure 10

Signature Recognition

predetermined threshold value. Score normalization is valuable when multiple algorithms are employed in a system.

An advantage of this technique is that it has a high user's acceptance. As smartphones do not require any additional hardware.

However, signatures seem different on smart phones, signature pads or pen-based tablets. Also an individual's signature can vary due to different style over time or in case of injury, or many other causes [2].

E. *Fusion*

Multimodal authentication systems have gained immense popularity because they leverage numerous biometrics and thus, offer accurate results in comparision to unimodal systems that depend on a single biometric modality. These systems provide enhanced security and offer flexibility in authentication. Implementing multimodal authentication may involve combining data from multiple sources, extracting features from different modalities, and employing various algorithms and models. Utilizing multimodal authentication on smartphones is feasible as modern devices are equipped with diverse sensors capable of capturing multiple biometrics. However, there are drawbacks to consider including the quality of input data from different sources, as poor data quality can lead to decreased performance. Additionally, utilizing multiple data sources requires reading from various sensors, which can be computationally demanding and energy-intensive. Multimodal-based approaches can result in longer training times, larger model sizes, increased memory usage, and longer inference times [16].

IV. Comparision

As discussed earlier, each technique has its own advantages and drawbacks. While no technique is considered optimal, it can still meet the user's needs to a certain extent. There are notable differences between traditional and biometric authentication methods. Traditional techniques are active, whereas biometric authentication is passive. Moreover, biometric data is inherently linked to its owner, unlike traditional credentials which can be forgotten, shared, lent, or stolen. Biometrics provide a reliable and natural means of identification as the user must be physically present during authentication and cannot deny access to the system. In contrast, with traditional techniques, users can deny login by sharing passwords. Lastly, biometric data is generally unique to each

Comparision Chart											
Characteristics		Traditional Authentication		Physiological Biometrics Authentication			Continuous Authentication				
		Password	OTP Token	Face Recognition	Fingerprint	Iris Recognition	Gait-based	Voice-based	Keystroke Dynamics	Signature-based	Multimodal
Usability	Cost-effective	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No
	Optimal accuracy level	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
	Low power and energy consumption	Yes	Yes	Yes	Yes	No	No	No	No	No	No
	Requirement for additional hardware/software	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
	Requirement for additional storage	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Security	Continuous authentication	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
	Vulnerability to shoulder-surfing attacks	Yes	No	No	No	No	No	No	No	No	No
	Vulnerability to dictionary and brute-force attacks	Yes	Yes	No	No	No	No	No	No	No	
	Vulnerability to impersonation attack	No	No	Yes	Yes	No	No	No	No	No	No
Variations	Variation with age	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
	Variation with occlusion	No	No	Yes	No	Yes	No	No	No	No	Yes
	Variation with injury	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Variation with physcial factors (eg.,pose,lighting,distance)	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Variation with background noise and behavioural changes	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Convinience	Ease of use	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Ease of remembrance	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Optimal registration time	Yes	No	Yes	Yes	No	No	No	No	No	No

Figure 11

Comparison Chart

individual. However, it is important to note that biometric data can be noisy, requiring accurate measurements, which presents significant challenges for biometric authentication as a developing field [2]. Figure 11 compares and contrasts each of the discussed techniques.

V. Conclusion and Future Scope

In conclusion, this survey paper has examined various aspects of continuous mobile authentication. We have explored different techniques, such as gait recognition, voice recognition, keystroke dynamics, and multimodal authentication, discussing their advantages, challenges, and applications. It is evident that continuous mobile authentication offers benefits in terms of unobtrusive and seamless user verification, enhancing security and user experience.

However, there are still areas that require further exploration and research. One such area is the integration of multiple biometric modalities for robust and accurate authentication. Additionally, the impact of changing user conditions, environmental factors, and different languages on the performance of continuous authentication systems warrants further investigation.

Furthermore, the cost-effectiveness of continuous authentication methods, as well as the management of privacy concerns and data security, are important considerations for future developments in this field.

However, there are still areas that require further exploration and research. One such area is the integration of multiple biometric modalities for robust and accurate authentication. Additionally, the impact of changing user.

In terms of future scope, advancements in machine learning, artificial intelligence, and sensor technologies hold promise for improving the accuracy and reliability of continuous mobile authentication systems. Exploring novel approaches and algorithms, as well as addressing usability and acceptance issues among users, will contribute to the widespread adoption of these systems.

Overall, continuous mobile authentication presents a promising direction for enhancing security and user convenience in mobile devices. Continued research and innovation in this field will pave the way for more sophisticated and effective authentication solutions in the future.

References

[1] Laricchia, F., Number of smartphone users by leading countries in 2022. Statista (2023). https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

[2] Amin, R., Gaber, T., ElTaweel, G., Hassanien, A.E., Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues. In: Hassanien, A., Kim, TH., Kacprzyk, J., Awad, A. (eds) Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations. Intelligent Systems Reference Library, vol 70. Springer, Berlin, Heidelberg (2014). https://doi.org/10.1007/978-3-662-43616-5_16.

[3] Ceci, L., Number of mobile cyber attacks against users worldwide from January 2020 to December 2022. Statista (2023). https://www.statista.com/statistics/1305965/mobile-users-cyber-attacks/.

[4] Ambimat Electronics. SMS-based OTP Authentication and Its Disadvantages. Ambimat Electronics (2021, June 1). https://ambimat.com/sms-based-otp-authentication-and-its-disadvantages/.

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

[6] Er. Aman Kumar, E. N. B., A Graphical Password Based Authentication Based System For Mobile Devices. *International Journal of Com-*

puter Science and Mobile Computing, 3(4), 744–754 (2014). https://www.ijcsmc.com/docs/papers/April2014/V3I4201499a50.pdf.

[7] Bandakkanavar, R., Graphical Password Authentication. KrazyTech (2017, August 19). https://krazytech.com/technical-papers/graphical-password-authentication.

[8] Towseef Akram Vakeel Ahmad Israrul Haq Monisa Nazir. Graphical Password Authentication. *International Journal of Computer Science and Mobile Computing*, 6(6), 394–400 (6, June 2017).

[9] What's the Difference Between OTP, TOTP and HOTP? (n.d.). Onelogin Logo. https://www.onelogin.com/learn/otp-totp-hotp#:~:text=There%20are%20two%20types%20of%20OTP%3A%20HOTP%20and%20TOTP.

[10] Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartzmann. A Review on Authentication Methods. *Australian Journal of Basic and Applied Sciences*, 7 (5), pp. 95-107 (2013). hal-00912435.

[11] One-time password (OTP) – more security online. (2020, January 10). IONOS. https://www.ionos.com/digitalguide/server/security/what-is-a-one-time-password-otp/.

[12] HUSEYNOV, Emin, SEIGNEUR, Jean-Marc. WifiOTP: Pervasive Two-Factor Authentication Using Wi-Fi SSID Broadcasts. In: ITU / IEEE. Kaleidoscope International Conference. 2015.

[13] Goodner, S., What Are Finger Scanners and How Do They Work? Lifewire (2021, August 29). https://www.lifewire.com/understanding-finger-scanners-4150464.

[14] What is Iris Recognition and how does it work? NEC (2022, June 15). https://www.nec.co.nz/market-leadership/publications-media/what-is-iris-recognition-and-how-does-it-work/.

[15] M. O. Derawi, C. Nickel, P. Bours and C. Busch, "Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition," 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Darmstadt, Germany, pp. 306-311 (2010), doi: 10.1109/IIHMSP.2010.83.

[16] Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D., Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey (2020). ArXiv. /abs/2001.08578.

[17] Zareen, F.J. and Jabin, S., Authentic mobile-biometric signature verification system. IET Biom., 5: 13-19 (2016). https://doi.org/10.1049/iet-bmt.2015.0017.

[18] Shankar, V., & Singh, K., An improved user authentication scheme on smartphone using dominating attribute of touch data. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(8), 1549-1561 (2019).

[19] Shekhawat, K., & Bhatt, D. P., A novel approach for user authentication using keystroke dynamics. *Journal of Discrete Mathematical Sciences and Cryptography,* 25(7), 2015-2027 (2022).

[20] Ara, A., Sharma, A., & Yadav, D., An efficient privacy-preserving user authentication scheme using image processing and blockchain technologies. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(4), 1137-1155 (2022).

[21] Dinker, A. G., Sharma, V., Mansi, & Singh, N., Multilevel authentication scheme for security critical networks. *Journal of Information and Optimization Sciences*, 39(1), 357-367 (2018).

[22] Joshi, A., & Mohapatra, A. K., A novel lightweight authentication protocol for body area networks based on elliptic-curve cryptography. *Journal of Information and Optimization Sciences*, 41(7), 1645-1672 (2020).

[23] Kumar, A., Singh, K., & Khan, T., L-RTAM: Logarithm based reliable trust assessment model for WBSNs. *Journal of Discrete Mathematical Sciences and Cryptography*, 24(6), 1701-1716 (2021).

Received September 2023