Computer Systems Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2024.050846

REVIEW

Biometric Authentication System on Mobile Environment: A Review

Qasem Abu Al-Haija[1,*] and Sara Othman Al-Salameen[2]

[1]Department of Cybersecurity, Faculty of Computer & Information Technology, Jordan University of Science and Technology, P.O. Box 3030, Irbid, 22110, Jordan

[2]Department of Cybersecurity, King Hussein School of Computing Sciences, Prince Sumaya University for Technology, P.O. Box 1438, Amman, 11941, Jordan

*Corresponding Author: Qasem Abu Al-Haija. Email: qsabuhaija@just.edu.jo

Received: 20 February 2024 Accepted: 24 May 2024 Published: 17 July 2024

ABSTRACT

The paper discusses the importance of biometric verification systems in mobile environments and highlights the challenges and strategies used to overcome them in order to ensure the security of mobile devices. Emphasis is placed on evaluating the impact of illumination on the performance of biometric verification techniques and how to address this challenge using image processing techniques. The importance of accurate and reliable data collection to ensure the accuracy of verification processes is also discussed. The paper also highlights the importance of improving biometric verification techniques and directing research toward developing models aimed at reducing risks and ensuring the security of mobile devices. The paper provides a comprehensive overview of the important research conducted in this field between 2015 and 2023, with a focus on analyzing the technologies used, the challenges they face, and the strategies used to overcome them. The paper concludes by mentioning future trends and the need for continued research and development in the field of biometric verification on mobile devices to ensure improved security and reliability in the mobile environment.

KEYWORDS

Cyber security; mobile devices; physiological authentication; behavioral authentication; biometric security

1 Introduction

The technology sector experienced a sequence of advances in response to the times, starting with the landline phone being replaced by the mobile phone with buttons, which then underwent further development to become smartphones with advanced technical features. And the advantages that encourage individuals to utilize and incorporate them throughout their lives. Mobile device users experience the tremendous comfort that mobile devices offer. Yet, smartphones are created for an interconnected world with a basic security model that makes users not pay attention to how their information and data are kept, sent, or processed [1].

However, its broad use raises serious security issues. Because they have complete access to data (pictures, emails, contacts, location, etc.) for mobile tools and mobile applications. Because most applications use biometric authentication technologies as a point of security for mobile devices, this vulnerability in their security was an easy point in favor of viral attacks, malware, botnets, and security breaches of mobile devices targeting this group of people. Making it an objective problem, an inevitable starting point is a significant turning point for most large businesses.

This paper integrated behavioral biometrics, in particular (fingerprint and face print) authentication processes, to increase the level of security since the subject of our research is the mobile phone environment, which will help prove that the authenticated person is the authorized one to enter. This paper used to clarify concepts related to biometric authentication, where we focused in particular on the topic of the mobile phone user authentication approach, in addition to clarifying the types of attacks that the user may encounter and algorithms to reduce them, also to assessing risks through developing models of threats and assessing vulnerabilities. The work method of this study contributed to working on further clarification, analysis, and evaluation of all previous studies related to this topic.

The rest of this paper is organized as follows. Section 2 gives a background on the biometrics systems and the methods commonly used for mobile user authentication while focusing on their limitations. Next, we elaborate a literature review on the existing biometric authentication techniques in Section 3. Further, we draw a summary table of the reviewed research work and discuss them in the same section. Finally, we conclude this work and list our future directions in Section 4.

2 Background

In recent years, some authentication has been included as a security component due to the growing popularity of biometrics among smartphone users. This is a difficulty for smart device makers trying to integrate and evolve the security model with the mobile sector. This section will define authentication and its many variants, focusing on behavioral and physical biometric authentication and assault countermeasures.

2.1 Biometric System

Measurements about the human body are called "Biometrics," which also involves statistical analysis of a person's physical and behavioral traits. Biometrics are based on behavioral traits such as gestures, typing speed, keystroke, etc., or physiological traits such as face, fingerprint, and palm.

In different applications worldwide, including forensics, surveillance, border control, and attendance management, biometrics are widely employed in digital devices like phones for security, logical and physical control, etc. The majority of biometric authentication systems are used to identify and authenticate people based on the biometric information that has been gathered. Systems that use biometric authentication have significantly shortened the time it takes to identify and confirm an individual's one-of-a-kind, universal, and permanent. As a result, many outdated identification and access control methods have been replaced by biometric authentication systems or combined with them to ensure the highest security level [2]. Below, we will explain registering and verifying the user's Biometric Authentication [3].

a) Registration Phase: The user's biometric characteristic is used for identification at the registration step. The biometric characteristics are first captured. This data is transformed into a mathematical representation known as a biometric template, like the "Direct Matching Algorithm" for fingerprint or Convolutional Neural Networks (CNNs) for face recognition,

which, when required, is compared to the live version supplied by the user. After being processed by the phone, it is stored in a database where it is impossible to duplicate any one piece of biometric information described in Fig. 1, which shows the Sequence Diagram Registration Phase Design.

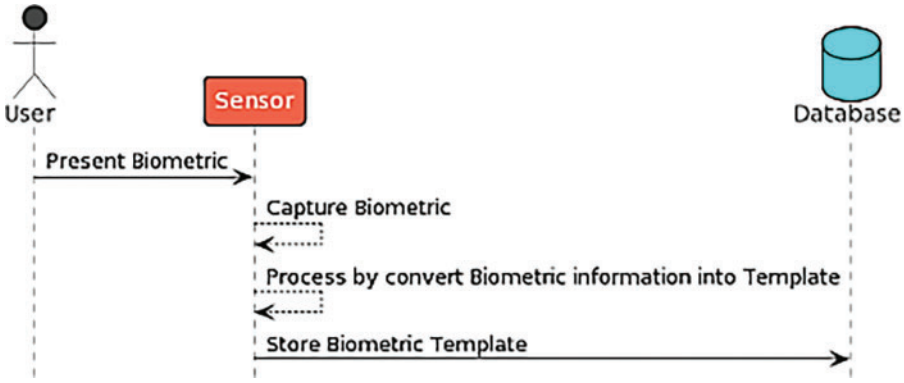

Figure 1: Sequence diagram registration phase design

b) Verification Phase: The verification process ensures that the individual has permission to use the access point. The procedure begins with entering a fingerprint or face print; at this point, a biometric scanner records and digitizes the user's features. The feature extractor then processes the digital data to create a compressed digital representation. The feature matching tool compares the resulting presentation with a single user template retrieved from the system database. If the results match, the sensor will retrieve the user template from the system database and then re-check between the data it extracted and the one retrieved, thus in the event of accuracy. If it matches, the user will be accepted and allowed to use the phone. Otherwise, it will not be allowed to access Fig. 2, which explains the design of the Sequence Diagram verification phase.

2.2 Methods of Mobile User Authentication

Mobile authentication uses authentication techniques to protect a mobile phone from being accessed by unauthorized persons. Existing authentication technologies, such as passwords, Personal Identification Numbers (PINs), Facial Patterns, and Unlock Patterns, rely on private information only authorized users should know. Research has recently presented many Biometric-Based Authentication technologies that can be categorized according to the types of biometrics detected by smartphone sensors based on user behavior. Therefore, these basic metrics depend on different factors used to verify the user's identity, and Fig. 3 illustrates the approach taken. For each factor in biometric authentication in the mobile environment [4].

According to the figure, we may categorize these techniques based on the biometric characteristics that smartphone sensors can detect. Physiological biometric authentication techniques employ users' physical traits, such as fingerprints or faces, to confirm their identity. In addition, methods of behavioral biometric authentication (such as keystroke dynamics and gate patterns) are based on how the user interacts with their mobile device. Also, we may categorize based on the time needed to gather user data and validate them; biometric authentication systems may be further classified into

two primary categories: One-Time Authentication calls for the user to carry out a particular action for a brief amount of time (such as entering a PIN).

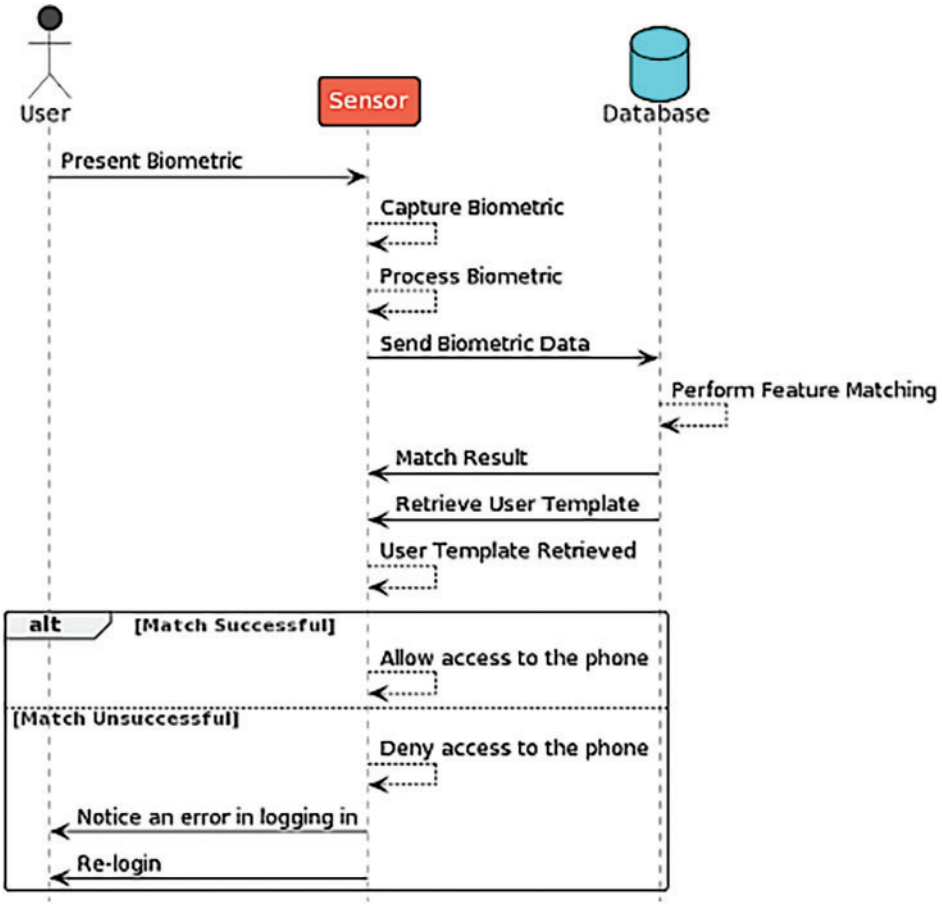

Figure 2: Sequence diagram of the verification phase

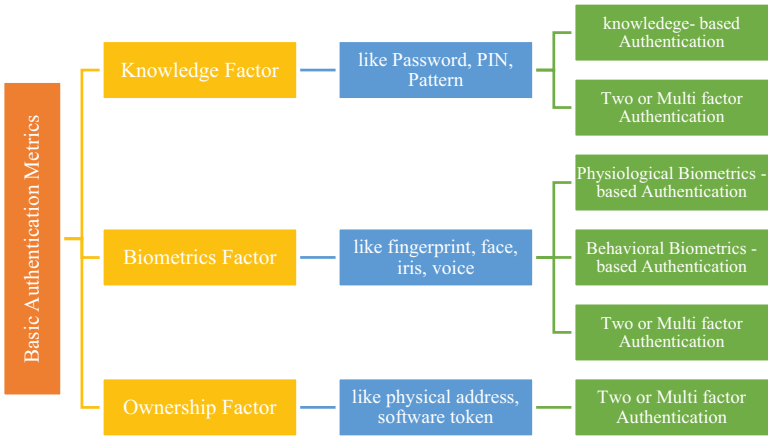

Figure 3: Methods for mobile user authentication

A One-Time Authentication mechanism must be as quick as feasible while achieving high accuracy to minimize user impact. In addition, continuous authentication may require collecting sensor data over an extended length of time. In reality, a continuous authentication technique carries out two jobs concurrently: The user's behavioral profile is (i) progressively formed by adding fresh observations from sensors and (ii) verified to ensure that the present observation fits the behavioral profile of the user created from earlier observations (such as gestures and gait) [4].

a) **Physiological:** Herein, we cover the most relevant physiological biometric authentication techniques. Some can be modified to run on mobile devices even though they were not specifically designed for smartphones. But first, physiological biometrics refers to analyzing a person's physical characteristics, such as a face, fingerprint, palm, or iris. Therefore, they are constant qualities—the body ages, but the lines of the prints do not change, nor do the face and its features. So, these physical characteristics can be used to identify, verify, or authenticate that person. Several authentication methods based on physiological biometrics on smartphones have already been deployed.

As a prime example of physiological biometrics, manufacturers have recently begun to include a specific digital fingerprint biosensor on high-end smartphones. However, mobile devices often need specialized sensors, such as the capacitive fingerprint scanner [5] and depth camera [6] on iPhones and the iris reader on Samsung smartphones, to acquire biometric features from users' body parts. The illustration in Fig. 4 describes the latest relevant physiological biometric authentication techniques that present in detail the technologies used in mobile devices.

b) **Behavioral Biometrics:** This partition outlines the most important behavioral biometric authentication techniques. As a result, behavioral biometric authentication is a technology that verifies an individual's identity using their behavior. It achieves this by continuously monitoring its physiological and behavioral characteristics and comparing these patterns with user data recorded on the device's database. It considers a few factors: Typing velocity, frequency of errors, and duration of key depressions. Fig. 5 shows the latest behavior biometric approaches that are used as biometric approaches in the mobile environment.

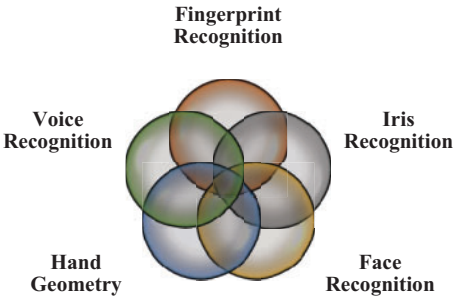

Figure 4: Physiological biometric authentication techniques

2.3 Limitations

In the context of the mobile environment, biometrics faces many technical and practical difficulties. In this section, we will highlight the main challenges of them outlined below:

1. Restrictions on specifications about hardware and the operation of the software [1]:

a) Device limitations: The range from the ability of the device to last for a certain period to the cost of fairly priced installation and maintenance. At the same time, it maintains the ability to collect samples with a low rate of errors and possible readings. External factors that may reduce its effectiveness and quality do not affect it.
b) Environmental Factors: When fingerprint biometrics systems are exposed to shriveled or wrinkled fingertips resulting from extended contact with water, degradation is seen.
c) Weak encryption technology: There is a chance that the phone system will develop security flaws if a weak encryption technology is used. To give each algorithm a certain level of security, the collected feature data is encrypted before being saved in the database using the proper technology. Thus, the key that is used has to be the key size that affects how quickly the algorithm processes the data during unbreakable encryption; the bigger the key, the slower the algorithmic data processing.
d) Database limitations: To guarantee system efficiency, the biometric database needs to be of a suitable size in which whenever several characteristics are obtained from a user for a sizable sample, the database size substantially rises, one that can hold the number of results that emerge from the registration stage for numerous samples, and that has quick encryption and decryption with minimal processing time for the system to function well.

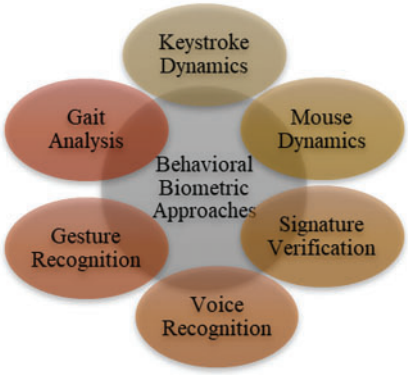

Figure 5: Behavior biometric approaches

2. Security threat [1]:

a) Sensor-level attacks, where false biometric samples are provided to gain access. This can apply to objects one handles or objects with artificial features.
b) Attacks through observation: The adversary may immediately obtain the user's knowledge-based secrets and enter identity secrets to pass authentication. They may also obtain the user's biometric data, which can forge the real user's biometrics to pass authentication.
c) The synthesis attack collects partial biometric data to create complete biometrics representing a real user about the authentication mechanism.
d) Side-channel attacks: Using the original systems' leakage of irrelevant identifying information to infer the user's identity. Although the many built-in sensors provide adaptable

and flexible interfaces to interact with users, a hacker may exploit them to obtain user-identifying information and circumvent the authentication mechanism.

2.4 Risk Assessment & Security Solution

Reducing the number of attacks to which this environment is exposed is done by enhancing the security of the biometric authentication system. Given the above, the following improvements can be made:

a) Security risk management: This assessment and analysis is part of the cyber security risk assessment process, as the assessment and risk assessment are often performed first, and then controls are chosen to deal with the identified risks to reduce them. At each point of failure, an "alert" will be sent from the incident log to indicate until an agent or event occurs or reaches a critical situation.
b) Anti-spoofing and direct attacks involve spoofing: It is possible to use one of the types of devices that detect pulses from real fingers to determine the vitality of the fingerprint so that it can distinguish between real and fake fingerprints based on the pores in terms of their number, to measure the patterns of sweat pores along the ridges to identify fake fingers, the illustration in Fig. 6 demonstrates how real fingerprints often have bigger ridge ends than phony fin- fingerprints. Consequently, a liveness detection test may be performed by counting the fingerprint's minute details [1].
c) Implementing a more secure algorithm: An elliptic curve encryption scheme that requires only 224–255 bits can be used to achieve security. A powerful algorithm created today may be easily hacked due to increased computer processing power. Choosing and updating the algorithm is essential.
d) To identify and create efficient hash codes that can differentiate between biometric data, fuzzy fingerprint identification based on hash codes can be used [7].
e) Smart cards as an alternative to the database: They use enough capacity to hold encrypted biometric data to reduce the risk of losing the entire database to hackers as sensitive material is divided.

Figure 6: The difference in ridge endings in genuine and fake fingerprint

3 Literature Review

The most significant research and advancements in biometric authentication will be discussed in this section.

- **Fingerprint matching:**

In [8], Alkahtani et al. discuss and exploit the system's flaws to develop a new technique for identifying malicious signature-based attacks that are antivirus programs against novel malware on the Android mobile environment, built using artificial intelligence, machine learning and deep learning algorithms that predict malware. Support vector machines (SVM), K-Nearest Neighbors (KNN), Linear Differentiation Analysis (LDA), Long-Term Memory (LTM), Long Short-Term Memory (LSTM), and Convolution Neural Network-Long Short-Term Memory (CNN-LSTM), so auto-encoder methods were used to build and construct a security system in their study. Several inferences were drawn from the findings gathered, chief among them being that using the CICAndMal2017 and Drebin datasets of Android malware applications, the suggested approach was assessed and looked at. Machine learning algorithms such as SVM, KNN, and LDA have shown to be good at detecting malware, with SVM being the most successful.

The LSTM and CNN-LSTM models have also been put out to detect dangerous applications, with the LSTM model being more effective in improving Android security. Sensitive analysis using the metrics Mean Square Error (MSE), Root-Mean-Square Error (RMSE), and Pearson's correlation coefficient (R) using R^2 revealed discrepancies between target values and expected output during the validation step. The LSTM and CNN-LSTM algorithms produced fewer prediction errors in the Drebin dataset. However, the SVM approach performed better on the CICAndMal2017 dataset. The outcomes of the machine learning and deep learning validation phases were good, with the performance of the LSTM and SVM models being particularly strong. Also, to verify the success of their research, they contrasted the current study's findings with those of more recent studies. Both suggested classifiers produced accurate results. However, LSTM's accuracy of 99.40% showed that it could beat more recent models.

Samangouei et al., in their research [9], stated that users regularly save important information on their mobile devices, such as login credentials for their private accounts or bank account information, which has become an indispensable aspect of people's lives. Personal data can only sometimes be secured because over half of users do not use an authentication mechanism on their phones. They created a Deep Convolutional Neural Network (DCNN) architecture for persistent mobile device authentication. These computers must learn intermediate attributes rather than IDs to reduce network complexity and maximize their limited resources. They show how the DCNN architecture performs several tasks while being selective in discovering traits that surpass the most recent methods in terms of accuracy. The suggested design allows them to explore the embedding space for features derived from various face characteristics, such as lips and eyes, and to find new features. Furthermore, they discovered via thorough testing that for the active authentication job, the trait features extracted by our technique beat the method based on pre-submitted characteristics and the fundamental Local Binary Pattern (LBP) method. Finally, they evaluated battery usage patterns and prediction speed on a real mobile device to determine whether the suggested design was beneficial regarding speed and power consumption. Additional discrimination adds a section for improved authentication performance.

To enhance the fingerprint acquisition process, the researchers highlight Double Line Single Point (DLSP) assistive technology in their paper [10], which suggests a palmprint recognition system on mobile devices by using sophisticated methods for creating and matching PalmCodes, an assessment

of the benefits and efficacy of the developed algorithm is provided on the gathered database, enhancing the functionality of the palm print (lower portion of the hand) recognition system. The best practices for creating and matching PalmCodes were established based on the results of their analysis of multiple databases, with an emphasis on enhancing the system's efficacy, accuracy, and performance in light of significant obstacles like a variety of hand positions and movements, intricate backgrounds, varied lighting conditions, and constrained hardware resources. They show that their future system developments are also planned, including creating a novel DLSP preparation and using cutting-edge feature extraction and matching methods to improve performance.

- **Behavior adoption:**

Progonov et al. discussed in their research paper [11] that the vast majority of contemporary mobile phone solutions rely on a "device unlock" scenario, which involves verifying the data (authentication factors) supplied by the user to unlock the smartphone. These variables determine whether it uses a single "strong" authentication factor or numerous "weaker" ones. These methods call for extra user activities, including having the user type a password or take a fingerprint, which may need to be revised for fast authentication. The smartphone stays open and may be swiftly locked if acts other than the owner are recognized, according to their suggestion that the BehaviorID functionality is used in the new "device lock" scenario. This is done by employing built-in sensors to monitor user behavior following triggering events like emails and social media posts.

They evaluate behavioral patterns precisely and modify them to fit the new use scenario using an Advanced Adaptive Neural Network (A-RNN). The suggested BehaviorID approach enables trustworthy user authentication in various use circumstances by retaining minimal energy consumption. The performance evaluation of both contemporary solutions and suggested solutions in various usage settings demonstrated the efficiency of the behavior identifier in actual circumstances. In contrast to contemporary alternatives, BehaviorID also shows a low error level deviation in the long-term usage situation. As a result, the suggested BehaviorID approach is a strong contender for inclusion in mobile devices' next behavior-based user authentication systems.

In their study, Zhou et al. [12] detail how shoulder surfing is a critical component of the security vulnerabilities that password-based mobile user authentication is exposed to. The focus of recent studies has been on influencing the security behavior of mobile device users, which may be done by strengthening user passwords or developing safe password generation procedures, even though there is a substantial body of research on password security in this subject. Little is known about how an attacker can track the target user's password. The purpose of this study was to empirically investigate how attackers behaved while watching password-based mobile user authentication sessions across the course of three surveillance attempts.

Thanks to the study of server log data, they could recognize several shoulder surfer's behavioral patterns over several tries. Starting, the sensitivity of password guesses gets better, and they get longer with time. These results also align with the cognitive load theory, which holds that human working memory capacity is constrained. The number of elements that can be stored in short-term memory is believed to be four, which is a lot fewer than the length of the passwords that were used in their experiment. Repetition is one of the factors that most impact memory, according to studies based on it. Repetition has a noticeable impact on memory assessments. Based on the Levenshtein distance, there was, therefore, greater adjustment between the first and second efforts than between the final two attempts. The length of the guessed password also changed more between the first two attempts than between the final two. Simply put, it gathers data through a long-term study of the user and

analyzes the data gleaned from the system log. When the data were public, they showed several of the attackers' behavioral patterns, showing they strategically used shoulder surfing attacks.

The authors of [13] discussed their study on behavior-based authentication, a feature of smartphones that operates in the background and does not require the user to pay attention. However, based on earlier research on past behavior authentication, additional features still need to be added. For instance, gyroscope and accelerometer signals are irrelevant regarding touch screen biometrics. These motion-based sensors can only be used when there is continuous body movement. Because they get fixed values, several pressure-related properties are not relevant. Based on their practical knowledge, they say swipe movements are where the Random Forest (RF) classifier performs best.

The chosen feature set outperforms the current approaches regarding frequency modulation and accuracy. They created a system in real-time, putting it through several test swipes before deciding on it after several iterations. Only seven and ten motions were used in the experiments. No quack has been successfully verified with a threshold of 40. Their long-term goal is to include more touch motions like tap, double-tap, and pinch by developing generic and customized user interfaces and contrasting the outcomes. They stressed that the system now employs a two-class classifier, necessitating gathering data from both genuine and impersonated users. They indicated that this might be improved by employing a single-class classifier, in which case the fraudster's data would be unnecessary.

Buddhacharya et al. [14] highlighted in their research that as technology has advanced, the smartphone has become a trustworthy source for storing private data while also becoming a viable target for attackers. Typically, cell phones need all information conveniently accessible after the initial login. They propose in this paper that increasing the efficiency of implicit, continuous smartphone authentication by relying on the user's behavioral characteristics, which architecture to distinguish between legitimate smartphone owners and intruders relying on the sensors built into the smartphone such as the accelerometer, gyroscope, and Global Positioning System (GPS) as the sensors respond according to the user's behavior that is recorded by that smartphone and to test. They examined multiple machine learning algorithms for the rest of the filter model and discovered that the XGBoost model performed the best, with an accuracy of 98%. They selected the dominating features based on mutual information and trained a convolutional neural network individually for each to prepare the dataset for training the remainder filter model. On the remaining filtered data, the average accuracy was 95.79%. To see results that confirm that their model is more accurate with increasing data, as well as improved performance after integrating GPS data with the proposed prediction model, as it enables you to predict legitimate intruders and intruders in a few seconds, allowing it to be used for real-time applications, high accuracy rates, with the lowest error rate of 3.64%, surpassing conventional methods of data augmentation, feature extraction, and continuous authentication when combined with Generative Adversarial Networks (GAN) to achieve continuous authentication on smartphones [15].

Also, Reichinger et al. [16] discussed continuous mobile user authentication, a system embedded into mobile devices that continuously analyzes the user's biometric characteristics to see if the monitored inputs are consistent with and come from the previously authorized user. They suggest and develop a permanent user authentication system for the Android ecosystem. It executes experiments to gather data from various subjects while continually monitoring and recording touch, accelerometer, and timestamp data. The objective was to test continuous mobile user authentication using Hidden Markov Model (HMM) classifiers for Android smartphones. Their work reveals how aggregating many gestures improves speed but also poses issues for the system's overall security because the inputs

of individual gestures provide a random output for the prediction algorithm; despite achieving high-performance metrics, particularly when compared to other systems, more data must be collected to modified model and finally forecast these values.

In their article, Azimpourkivi et al. [17] suggested a new multimedia behavioral biometrics that uses data gathered when a user unlocks a smartphone to take a call. To apply biometrics to their behavior, we leverage swiping, arm movement to bring the phone closer to the ear, and voice recognition. They next utilized a real phone to implement the process. They performed controlled user research with 26 individuals in various circumstances to assess their suggested proto-type—a novel multimedia biometric system for smartphone user identification designed with simplicity in mind. The characteristics gathered during the slide-opening motion on the system are used on the smartphone. They, therefore, concentrated on using finger position, pressure, volume, and time displacement to create a model and classify upcoming slide motions.

They also demonstrated how combining single-modal and multimodal systems using slide, capture, and sound methods can significantly improve performance. They found that the Bayesian network classifier outperformed other classifiers in terms of computation time and error rates. The sliding approach fared better with a FAR of 22.28% and a False Rejection Rate (FRR) of 4.84%, yielding a Half Total Error Rate (HTER) of 13.56%. The performance of the capture technique was somewhat worse, with FAR and FRR of 26.69% and 6.19%, respectively, and an HTER of 16.44%; but, when they were combined, they produced a significantly better performance, with FAR of 11.01% and FRR of 4.12%, leading to an HTER of 7.57%. Due to our usage of a subpar open-source application programming interface, the voice-based model performed significantly worse. However, they demonstrated how slide capture and sound techniques might optimize the multimedia system.

In addition, Arteaga-Falconi et al. [18] reveal that biometric authentication in mobile phones based on lips is the process of validating an individual based on visual information obtained while speaking, researching whose potential for life can be captured using the device's front-facing camera, which does not require dedicated hardware. They noted that lip-based biometric verification was substantially slower than face, fingerprint, or iris biometric authentication. Their role in their paper is to propose the most recent approach for lip-based biometric authentication using a deep Siamese network trained on triple loss with real-world challenges so that the proposed system, LipAuth, is rigorously examined with real-world data and the challenges that can be expected in lip-based solutions deployed on mobile. The findings demonstrated for the first time how a lip-based authentication system operates outside of a closed-set protocol while testing a new open-set protocol on the XM2VTS dataset with equal error rates of 1.65%. New datasets, qFace and FAVLIPS, have been gathered to advance the field by allowing systematic assessment of the content and amount of data required for lip-based biometric verification and flagging problematic areas for future study. The FAVLIPS dataset is intended to imitate a simulation system that depicts the most difficult issues predicted in a publishing scenario and contains various problematic lighting conditions.

On the other hand, Jorquera Valero et al. [19] discussed systems for mobile persistent authentication concentrating on identifying people based on how they interact with mobile devices. The greater security of the system when users are permanently registered is one of the advantages provided by these systems. They also improve user experience by decreasing the usage of authentication credentials. Despite these systems' advantages, they are nonetheless susceptible to problems with authentication precision and their capacity to change the behaviors of new users. Continuous authentication solutions must address these issues while considering the crucial characteristics of mobile devices, including battery life, processing power, and reaction time. To overcome these prior difficulties, their design

and implementation of an intelligent and adaptable continuous authentication system from mobile devices is their primary contribution to this work. By taking into account statistical data from apps, sensors, and machine learning approaches based on anomaly detection, their suggested system enables real-time authentication of users. Numerous tests showed how accurately, adaptable, and resource-efficiently their approach worked. By creating and executing an online banking application as a proof of concept, which enables users to carry out various operations depending on their degree of authentication, its usefulness was finally proven. The results for the True Positive Rate (TPR) measurements of 50 users ranged from 48% to 98%. This discrepancy indicates that, depending on the behavior of the users, the proposed system recognizes the anomaly more or less accurately. They analyzed the results and realized that users interacting with the mobile device lying on a table had a lower TPR. In conclusion, the proposed solution can distinguish normal user behavior from 50 other abnormal users with satisfactory performance.

- **Heart rate monitoring:**

As for Buriro et al. [20], in their research paper, they explain Pixie, a camera-based two-factor authentication solution for mobile and wearable devices. The user needs to learn that the thing is a trinket. Pixie uses a supervised learning classifier to successfully handle differences between photographs of the same trinket shot under various settings and extracts strong new features from trinket image datasets. Using 40,000 native photos they took and gathered from public databases, Pixie generated 14.3 million authentication attempts with a false acceptance rate of less than 0.09%.

Wright et al. discussed in [21] and proposed a mobile biometric authentication technique based on an Electrocardiogram (ECG) since conventional mobile login methods, such as numeric or graphic passwords, are susceptible to passive assaults. This technique might obtain access by touching two ECG electrodes on a portable device. The algorithm was evaluated in a controlled laboratory experiment utilizing a cardiac monitor in a mobile phone case at various times and situations with ten people and with 73 records taken from the Physionet database. With 4 s of signal collection, the findings show that the algorithm has a false acceptance rate of 1.41% and a real acceptance rate of 81.82%. Their study and findings indicate that this is the first mobile phone verification method that uses ECG biometric signals, and this technology has a bright future. More advancements are needed to increase accuracy while keeping a quick validation acquisition time. Their long-term goal was to use machine learning techniques like SVM to enhance True Acceptance Rate (TAR) and False Acceptance Rate (FAR).

- **Matching faces:**

Also, Wang et al. explained in [22] that the use of numerous smart devices has increased dramatically in recent years due to advancements in the mobile phone industry and intelligence. As a result, numerous studies have been done to apply user authentication through biometric behaviors. Only some of them, after all, take into account ongoing user authentication across several smart devices. Therefore, their research aimed to examine user authentication from a novel angle: persistent authentication on many devices, that is, ongoing user authentication both during initial user access to one device and after user transfer to other devices.

They differ from earlier research by suggesting a continuous user authentication technique that uses the recognition of behavioral biometrics on a variety of smart devices. The accelerometer and gyroscope sensors on both smartphones and tablets were considered in their study methodology. Additionally, they used a CNN and LSTM to create their better neural network model, which was

then fed input from multi-device behavioral biometric data. To improve the efficacy and efficiency of authentication on many devices, they created t*wo-dimensional* field pictures to understand better how they defined the fundamental characteristics of sensor signals between various devices. They then fed these images into their network for categorization. Results were determined by assessing how well the multi-device continuous user authentication system performed in various circumstances. The extensive experimental findings demonstrate its viability and efficiency. They attained an average accuracy of 99.8% and 99.2% for smartphones and tablets in roughly 2.3 s using the technique, suggesting that it authenticates users accurately and rapidly.

Abdul Wahid et al. [23] explained that, even in the pre-smartphone era, personal identification numbers and passcodes were the most popular authentication methods in smartphones, followed by the development of a new biometric authentication method for smartphones that gained widespread acceptance. In their article, they want to study variables influencing smartphone users' adoption of biometric authentication techniques by constructing a new model based on the Technology Adoption Model (TAM) and verifying data from a survey of 233 Indonesian smartphone owners. Structural Equation Modeling (SEM) is used to examine data that is available online. In terms of results, their study revealed that all nine hypotheses mentioned in the proposed model are supported, indicating that they significantly affect the behavioral intention to adopt biometric authentication methods among smartphone owners. Their findings indicate that most Indonesian smartphone users have a positive attitude toward biometric authentication standards, which is why they are willing to adopt them. Furthermore, the perceived advantage of the biometric identification technique on cell phones trumps the perceived simplicity of use.

In [24], Raghavendra et al. described a novel multimodal biometric data set (facial, speech, and eye contour) gathered using a smartphone in their paper. The new data set includes 150 respondents recorded in six sessions that simulated genuine phone-assisted authentication circumstances. One of the dataset's distinguishing aspects is that it is divided into four geographical regions. Furthermore, they presented a multimedia Presentation Attack (PA) or decoy data gathering with a low-cost Presentation Attack Instrument (PAI) such as print and electronic presentation attacks. New collection techniques and the diversity of data subjects allow for the construction of a new biometric algorithm. They disclosed that they assessed the performance of basic biometric verification and Presentation Attack Detection (PAD) on the newly gathered dataset; they presented an assessment of the performance of their core algorithms on both biometric verification PAD, so they gave an evaluation of the performance of their core algorithms on both biometric verification and presentation attack detection. The performance of the baseline algorithms provided using the experimental protocol's equal error rate (%). They presented the performance of their core PAD algorithms using Bonafide Presentation Classification Error Rate (BPCER), and Attack Presentation Classification Error Rate (APCER), and the BPCER while reducing APCER to 5% and 10% were by the recommendations provided in their study.

Moreover, to summarize the related state-of-the-art, Table 1 recaps the reviewed research work in this paper.

Based on previous studies that were referred to in the previous section, which are concerned with biometric authentication systems in the mobile phone environment, these researches showed common challenges in how to enhance security and ease of use in the biometric authentication environment, along with the extent to which the user accepts and trusts these systems, as it confirmed that the problem lies in dealing with all the differences and the need for specialized equipment to support them, it represents a strong competitor in applying biometric authentication techniques, which can

be concluded from the necessity of focusing on the user experience in raising the level of acceptance and confidence in biometric authentication, in addition to a clear fear of using it despite its ease, but in terms of trust in it. To fully rely on them, the user experience can be improved by providing more research on improving user interaction with these systems while enhancing security in the mobile environment.

Table 1: Related state of the art papers reviewed in this paper

Ref.	Year	Platform	Datasets	Mechanism	Remarks
[8]	2022	Android	CICA & Mal2 017 & Drebin	SVM, KNN, LDA, LSTM, and CNN-LSTM are used to build and construct a safety system. Algorithms for CNN-LSTM and autoencoders.	- Improved malware identification, real-time detection, and resolution of privacy issues.
[9]	2016	In the mobile environment, in general	Publicly available datasets MOBIO and AA01	By extracting exact facial characteristics on mobile devices using a multi-task DCNN architecture.	- It needed to be validated that the results were generalizable and relevant to a larger data collection because a small and limited sample was employed. - The concept could require further conditioning or training to handle the variety of faces and obstacles. - Due to mobile devices' processing speed and memory limitations, the suggested model will not be able to be implemented on them.
[10]	2018	In the mobile environment, in general	Create different databases for the study	- A palm fingerprint system was developed that relies on Double Line Single Point (DLSP) assistive technology to identify regions of interest (ROI) in fingerprint images and extract the required vital information. In addition, Gabor filters were used to create PalmCodes to improve matching between images.	- The challenges lie in recognition accuracy, versatility, cost of implementation, how to protect data, and compatibility with various mobile devices.
[11]	2022	In the mobile environment, in general	They apply to different datasets like Extrasensory, Sherlock datasets . . . etc.	A-RNN estimates and adjusts behavioral patterns accurately for a new usage scenario, achieved by monitoring user behavior.	- Enhanced security through monitoring user behavior and contextual constraints will pose challenges in applying it to all possible scenarios, so it can be a basic basis for developing more advanced and effective encounter systems in the future.
[12]	2021	In the mobile environment, in general	Information gathered by system log	It is based on experimental analysis of the attacker's behavior by studying server logs to find recurring patterns of the attacker's activity based on the Levenstein distance in changes between attempts to enter the system.	A larger sample size may benefit the generalizability of the findings and the ability of the study to identify trends in attacker behavior.
[13]	2021	Mobile and wearable devices	RF, J48, MLP, SMO, & Ink	RF and other machine learning techniques were used to classify the user's swiping gestures by swipe movements given a specific set of attributes that performed better than the current methods, and a real-time system was created that uses cloud computing to boost classification performance and work around smartphone performance issues user.	- Using swipe gestures as an authentication method simplifies the authentication procedure and makes it easier for the user. - Expanded system support for more touch gestures in multiple environment conditions.

(Continued)

Table 1 (continued)

Ref.	Year	Platform	Datasets	Mechanism	Remarks
[14]	2022	In the mobile environment, in general	Real data preprocessed	- A continuous authentication system based on Conditional Generative Adversarial Networks (CWGAN) uses smartphone sensors to allow users to interact with the phone. The Conditional Adversarial Generative Network (CAGANet) collects, processes, and augments accelerometer, gyroscope, and magnetometer data, then uses a designed CNN for feature extraction and principal component analysis (PCA) to identify distinct features. - Then, the system uses One-Class Support Vector Machines (OC-SVM) classifiers, Local Outlier Factor (LOF), Isolation Forest (IF), and Elliptic Envelope (EE) classifiers to perform user authentication and provide experience feedback.	The difficulty lies in preparing the data and implementation challenges on specific devices.
[16]	2021	Android	They collected random data from Android users and captured it using a tool to get the event	- By grouping multiple gestures to improve performance when evaluating the restriction of the gesture length used in the classification.	- Accuracy allows us to see a change in the real detection rates (False Positive), which impacts authentication's effectiveness. - Continuous authentication means that mobile devices are continuously and thoroughly protected and that authentication is not restricted to a single instance but occurs during use.
[17]	2017	Mobile and wearable devices	Collected from public datasets	Imaging and camera technology are used in the research as a tool for the authentication process. The camera is the first verification factor, and a password or lock pattern might be used as a second.	- The quality of the image captured by the camera can affect its accuracy and reliability and may increase the rate of false detection or rejection. - An authentication system may experience attacks for the unauthorized reproduction of images or fraud using image manipulation techniques.
[18]	2015	In the mobile environment, in general	Physionet database that they collected from mobile users	Their method was evaluated using a mobile environment-specific sensor, and the Physionet database by technique employs a hierarchal structure that cuts the time required to acquire ECG data for authentication to 4 s.	- The high degree of safety is due to its being a special resource for biometric verification, which has power. - The limitation that may be encountered in dealing with psychological disorders and handling this sort of data requires specialized equipment.
[19]	2018	In the mobile environment, in general	Information gleaned from sensors and applications	- The system creates a model of user behavior using data from sensors and mobile applications. The system uses semi-authorized Machine Learning algorithms to identify anomalies and carry out the authentication procedure by adjusting itself automatically as user behavior changes.	- The ability to adapt to changes in user behavior; however, it needs improvement in the machine learning algorithms used. - Expanding the data set to include other dimensions and variables, such as frequency and temporal information, strengthens the model and makes it more flexible and resilient.

(Continued)

Table 1 (continued)

Ref.	Year	Platform	Datasets	Mechanism	Remarks
[20]	2016	In the mobile environment, in general	Not mentioned	- They create a template specific to each user using data gathered from features such as finger locations, pressure, volume, and time during the dragging motion for using the users' prior swipe motions as a guide; this model is utilized to categorize subsequent swipe movements. - Systems' outputs are then integrated to produce a multimodal model, and single-modal systems are integrated to enhance performance.	- The multimedia recording system's performance has nearly doubled. The pull validation approach produced low false FAR and FRR, leading to a low HTER, making it the best method. To provide more precise and useful findings, further research must be done to determine how context & environment affect the effectiveness of this biometric technology.
[21]	2020	In the mobile environment, in general	XM2VTS, qFace and FAVLIPS	- Implementing Lip-Based Biometric Authentication (LBBA) on mobile devices and emphasizing LipAuth as the best solution, which impacts illumination and difficulties with the length and content of sign-up and authentication logins, were investigated. Dealing with lighting effects is essential for creating LBBA systems that can be used on mobile devices.	- Lightning effects can be fixed using image processing techniques to increase the technology's performance. - Finding a decent balance between having enough data to authenticate someone's identity and offering a quick and simple user experience takes time and effort.
[22]	2023	Smart devices	Collected user behavior data on various devices	- They used machine learning techniques for continuous authentication to evaluate the data to explore models and classifications for each user by employing the RF method, continuously validating the user's identification, and evaluating the performance using independent experimental data.	- Generalizing results to different situations can be a challenge, and differences in device capability affect identification accuracy.
[23]	2022	In the mobile environment, in general	Utilizing surveys to get information from Indonesian consumers	The SEM method analysis for acceptance of biometric authentication methods by using the R programming language, R Studio software, and the Lavaan library.	Accuracy is likely to be affected by online surveys, and sample size limitations being a small sample may make it difficult to generalize more widely.
[24]	2020	In the mobile environment, in general	Biometric data captured from mobile phones	- A smartphone-in-the-wild Peripheral Neuroimaging (SWAN) project with a dataset provided to present or spoof multi-modal biometric verification attacks. Key biometric validation algorithms and performance evaluation methodologies were fine-tuned to identify presenting attacks, and intercontinental and regional variation in individual biomarkers was emphasized.	- Novel data collected is quality, but the sample size needs to be bigger & it could not accurately reflect population variety, impacting how broadly the conclusions can be applied.

Future research directions based on the results extracted from the previous section can be summarized as developing an intelligent authentication system that seeks to monitor users' behavior and how they adapt to using smart sensors based on statistics extracted from their use of phone applications. Advanced encryption algorithms, such as the Elliptic Curve, can be used to protect biometric and behavioral data stored in the system's databases. With the continuous development in the phone environment, more research and studies can be conducted related to the mechanism of user adaptation to these systems for further improvements in biometric enhancement techniques. These

guidelines and results extracted from previous studies can help improve confidence and enhance its use by users.

4 Conclusions and Future Directions

With the rapid increase in smartphone users, there have been aspirations to protect this system. The increase in technologies and ideas on the issue of the security of cellular devices has formed a fertile environment for much research related to the security of mobile devices. Therefore, we explain in this research the concept of a biometric authentication system in its behavioral and physiological forms and the definition of each, in addition to the most important issues that may be faced in developing telephone systems and how to reduce them. This paper is intended for anyone who wants to learn or take a comprehensive picture of biometric authentication.

In the future, we will work on how to develop one of the existing algorithms, such as the neural network algorithm for behavior analysis, to give hypothetical alerts in case an unauthorized person hacks into the phone. Proactive behavior reduces the false alarm rate and increases the network's intelligence in determining whether a person is authorized.

Acknowledgement: The authors acknowledge and value the fruitful collaboration between the Jordan University of Science and Technology (JUST) and the Princess Sumaya University for Technology (PSUT).

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm their contribution to the paper as follows: study conception and design: Qasem Abu Al-Haija;data collection: Sara Othman Al-Salameen; analysis and interpretation of results: Qasem Abu Al-Haija and Sara Othman Al-Salameen; draft manuscript preparation: Qasem Abu Al-Haija and Sara Othman Al-Salameen; Supervision : Qasem Abu Al-Haija. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] N. Bhartiya, N. Jangid, and S. Jannu, "Biometric authentication systems: Security concerns and solutions," in *2018 3rd Int. Conf. Converg. Technol. (I2CT)*, Pune, India, 2018, pp. 1–6. doi: 10.1109/I2CT.2018.8529435.

[2] A. Mansour, M. Sadik, and E. Sabir, "Multi-factor authentication based on multimodal biometrics (MFAMB) for cloud computing," in *2015 IEEE/ACS 12th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Marrakech, Morocco, 2015, pp. 1–4.

[3] M. Olaniyi, A. Omotosho, E. Oluwatosin, M. Adegoke, and T. Akinmukomi, "Students exeat monitoring system using fingerprint biometric authentication and mobile short message service," arXiv preprint arXiv: 1506.03237, 2015.

[4] R. Spolaor, Q. Li, M. Monaro, M. Conti, L. Gamberini and G. Sartori, "Biometric authentication methods on smartphones: A survey," *PsychNology J.*, vol. 14, no. 2, pp. 87–98, 2016.

[5] M. Li *et al.*, "When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals," in *CCS '16: Proc. 2016 ACM SIGSAC Conf. Comput. Comm. Secur.*, New York, USA, 2016, pp. 1068–1079. doi: 10.1145/2976749.2978397.

[6] A. Bud, "Facing the future: The impact of Apple FaceID," *Biom. Technol. Today*, vol. 2018, no. 1, pp. 5–7, 2018. doi: 10.1016/S0969-4765(18)30010-9.
[7] T. F. Wu, L. Leng, and M. K. Khan, "A multi-spectral palmprint fuzzy commitment based on deep hashing code with discriminative bit selection," *Artif. Intell. Rev.*, vol. 56, no. 7, pp. 6169–6186, 2023. doi: 10.1007/s10462-022-10334-x.
[8] H. Alkahtani and T. H. H. Aldhyani, "Artificial intelligence algorithms for malware detection in android-operated mobile devices," *Sensors*, vol. 22, no. 6, pp. 1–26, 2022. doi: 10.3390/s22062268.
[9] P. Samangouei and R. Chellappa, "Convolutional neural networks for attribute-based active authentication on mobile devices," in *2016 IEEE 8th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS)*, Niagara Falls, NY, USA, 2016, pp. 1–8. doi: 10.1109/BTAS.2016.7791163.
[10] L. Leng, F. Gao, Q. Chen, and C. Kim, "Palmprint recognition system on mobile devices with double-line-single-point assistance," *Pers. Ubiquitous Comput.*, vol. 22, no. 1, pp. 93–104, 2018. doi: 10.1007/s00779-017-1105-2.
[11] D. Progonov, V. Cherniakova, P. Kolesnichenko, and A. Oliynyk, "Behavior-based user authentication on mobile devices in various usage contexts," *EURASIP J. Inf. Secur.*, vol. 2022, no. 1, pp. 1–11, 2022. doi: 10.1186/s13635-022-00132-x.
[12] L. Zhou and K. Wang, "Understanding attacking behaviors toward password-based mobile user authentication," in *Who Are You?! Adventures Authentication Workshop*, 2021.
[13] B. A. Ali *et al.*, "Smartphone security using swipe behavior-based authentication," *Intell. Autom. Soft Comput.*, vol. 29, no. 2, pp. 571–585, 2021. doi: 10.32604/iasc.2021.015913.
[14] S. M. Buddhacharya and N. Awale, "CNN-based continous authentication of smartphone using mobile sensors," *Int. J. Innov. Res. Adv. Eng.*, vol. 9, no. 8, pp. 361–369, 2022. doi: 10.26562/ijirae.2022.v0908.37.
[15] Y. Li, J. Luo, S. Deng, and G. Zhou, "CNN-based continuous authentication on smartphones with conditional wasserstein generative adversarial network," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5447–5460, 2021. doi: 10.1109/JIOT.2021.3108822.
[16] D. Reisinger, E. Sonnleitner, and M. Kurz, "Continuous mobile user authentication using combined biometric traits," *Appl. Sci.*, vol. 11, no. 24, pp. 1–24, 2021.
[17] M. Azimpourkivi, U. Topkara, and B. Carbunar, "Camera based two factor authentication through mobile and wearable devices," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 1, no. 3, pp. 1–37, 2017. doi: 10.1145/3131904.
[18] J. S. Arteaga-Falconi, H. Al Osman, and A. El Saddik, "ECG authentication for mobile devices," *IEEE Trans. Instrum. Meas.*, vol. 65, no. 3, pp. 591–600, 2015. doi: 10.1109/TIM.2015.2503863.
[19] J. M. Jorquera Valero *et al.*, "Improving the security and QoE in mobile devices through an intelligent and adaptive continuous authentication system," *Sensors*, vol. 18, no. 11, pp. 1–20, 2018.
[20] A. Buriro, B. Crispo, F. Del Frari, J. Klardie, and K. Wrona, "ITSME: Multi-modal and unobtrusive behavioral user authentication for smartphones," in *Technology and Practice of Passwords*. Springer International Publishing, 2016.
[21] C. Wright and D. W. Stewart, "Understanding visual lip-based biometric authentication for mobile devices," *EURASIP J. Inf. Secur.*, vol. 2020, no. 1, pp. 1–16, 2020. doi: 10.1186/s13635-020-0102-6.
[22] Y. Wang, X. Zhang, and H. Hu, "Continuous user authentication on multiple smart devices," *Information*, vol. 14, no. 5, pp. 1–19, 2023. doi: 10.3390/info14050274.
[23] L. O. Abdul Wahid and A. R. Pratama, "Factors influencing smartphone owners' acceptance of biometric authentication methods," *ILKOM Jurnal Ilmiah*, vol. 14, no. 2, pp. 91–98, 2022. doi: 10.33096/ilkom.v14i2.1114.91-98.
[24] R. Raghavendra *et al.*, "Smartphone multi-modal biometric authentication: Database and evaluation," arXiv preprint arXiv:1912.02487, 2020.