Review of Biometrics-Based Authentication Techniques in Mobile Ecosystem

Fatimah Al-Jarba and Mohammed Al-Khathami,
fhaljarba@imamu.edu.sa maalkhathami@imamu.edu.sa
Information Systems Department, Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia

Abstract
Mobile devices have recently developed to be an integral part of humans' daily lives because they meet business and personal needs. It is challenging to design a feasible and effective user authentication method for mobile devices because security issues and data privacy threats have significantly increased. Biometric approaches are more effective than traditional authentication methods. Therefore, this paper aims to analyze the existing biometric user authentication methods on mobile platforms, particularly those that use face recognition, to demonstrate the methods' feasibility and challenges. Next, this paper evaluates the methods according to seven characteristics: universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention. Last, this paper suggests that solely using the method of biometric authentication is not enough to identify whether users are authentic based on biometric traits.

Key words:
Mobile phone; User authentication; Biometrics; Face recognition.

1. Introduction

Mobile devices have become more popular as a result of the rapid advancement of communication technologies and internet accessibility. The United States (US) is a leading country in regard to adopting smartphone technology. As per a recent release survey in 2019 [1], smartphone usage has significantly increased in recent times. In 2018, the total number of smartphones in use was nearly 274.1 million, and this is expected to reach 311.53 million by 2025, which is considered a large percentage (see Fig. 1). In addition, mobile banking has been classified as the most cost-effective and efficient platform for banking services [2]. Mobile banking is considered one of the fastest and cheapest ways to communicate and it now provides banking services to a vast number of customers [3]. In 2020, it was predicted that technology in the financial sector would be more advanced and grow at a rapid rate [4]. Various reports demonstrate that, at the end of 2013, US$115 billion was invested in implementing mobile banking technology [5]. In Spain, the transactional value of mobile payments per user is expected to grow from US$268.10 in 2017 to over US$850 in 2022 [6].

Manuscript received November 5, 2021
Manuscript revised November 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.11.43

However, the portability of mobile devices entails their susceptibility to being lost or stolen, which creates security challenges for users and merchants. Studies show that perceived credibility, include a degree to which an users believes mobile banking as trustworthy and secure are positively affected merchants and users accepting payment by mobile phones [7]. Perceived usefulness, perceived ease of use and perceived risk are factors that affect behavioral intention of consumer acceptance of mobile banking and the developers should pay attention of these factors [8]. It is well-known that a primary issue of these emerging technologies is that the security level fails to meet the requirements of the finance sector or card issuer [9]. A critical risk associated with mobile payments is that existing technologies fail to offer sufficient authentication of users and their mobile devices.

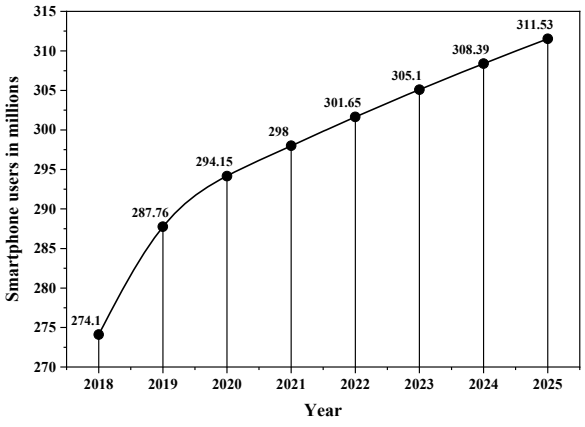

Fig. 1 Number of smartphones users in U.S from 2018 to 2025.

In recent years, the secure authentication scheme has gained prominence in light of controlling access to mobile devices. User authentication confirms users' authenticity by actively transferring between the user and their mobile device. There are three types of user authentications: knowledge-based authentication, possession-based authentication and physiology-based authentication (see Table 1) [10, 11, 12]. Knowledge-based authentication is simple to design and

use; therefore, it is currently the most widely used authentication method (through passwords and personal identification numbers). However, password authentication is vulnerable because passwords can be easy to crack through malware techniques or unsafe user behavior. That is, users are required to create passwords for various applications and thus they often use passwords that are easy to remember, which means that they can be easily compromised [13]. Biometric authentication is a security type that measures an individual's unique characteristic that cannot be duplicated. Therefore, this research used biometric authentication to avoid the limitations of the knowledge-based authentication approach [13, 14].

Table 1: Authentication Categories

Categories	*Type*	*Features*	*Example*
Knowledge-based authentication	What you know	Password forgotten or used by others	Password and ID
Possession-based authentication	What you have	Equipment copied or used by others	Watch and keys
Physiology-based authentication	What you are	Biometric features of each person that cannot be duplicated	Face and fingerprint

Recently, researchers [10, 15] surveyed regarding biometric authentication on mobile platforms; however, these studies did not provide a comprehensive survey nor solve limitations regarding using biometric authentication. Therefore, this research differs from previous studies by aiming to fill this gap. It completed a comprehensive review of user authentication methods in the mobile ecosystem (particularly those using facial recognition) and evaluated them according to the abovementioned seven characteristics. That is, this research surveyed current effective authentication systems of user identities in mobile ecosystems. This research reviewed articles regarding biometric authentication techniques and analyzed the findings, as well as determined potential user identity authentication threats that can affect mobile payments. Section 2 discusses the user authentication approach, Section 3 characterizes the development of the biometric user authentication, and Section 4 provides a comparative analysis and discussion. Last, Section 5 presents the conclusion.

2. Related Work

This section discusses user authentication approaches—a critical issue regarding information security and privacy protection in mobile device applications [16]. Various research presented a secure authentication protocol based on two-party computation for an internet environment. This protocol aims to solve issues regarding the requirement that there should be an honest third party in control after the authentication method secret reconstruction process. However, a prototype of this protocol has not been implemented in a real-world environment to assess and ensure its practical utility [17]. Previous research [18] presented the RiskCog system, which depends on available and privacy-insensitive motion sensors to detect users' daily device usage data. In addition, it requires no direct input from users nor users' motion state or device location; it is usable without internet access through performing offline user identity verification, whereas other systems require internet access to perform user authentication.

The authors [19] aimed to create a safe internet credit card transaction by proposing a Secure M-Commerce Scheme (SMCS). The SMCS was designed to protect online transactions from various attacks through organized cash flow of a trading system and its credit card entities. In addition, the SMCS uses data connection core to link the card-issuing bank and consumers before initiation of their wireless communication; however, it must ensure that it is secure and feasible by developing a complete SMCS simulation system and search for potential cooperative banks that would run the SMCS. Further, a transaction scheme that adopts an efficient certificateless signature (CLS) crypto module implemented on Android Pay would eliminate the need for heavy computation of bilinear pairings. Instead, this scheme evaluates the practicability of the proposed scheme by implementing the core security components of scheme on an IoT-based test bed. It must improve system performance and enhance the adopted security components [20].

However, passwords can be easily seized by either directly observing the user input their password or using malware techniques. Previous user authentication approaches noted that it could not be determined whether the user was authenticated or someone who had hacked the device (through either borrowing or stealing). To solve the above limitations, user authentication can conduct through users' possessions (e.g., keys), but this requires additional costly hardware. Thus, it is not widely used in smartphone authentication. Therefore, biometric-based user authentication can be used to solve these limitations because biometric features use physiological or behavioral features unique to the user [12].

3. Development of Biometric User Authentication

Biometric authentication is a security approach that authenticates a user's identity through one of their unique characteristics by storing the biometric data and completing a secure mobile payment. Biometric approaches are based on physiological or behavioral characteristics that are advantageous compared to traditional authentication methods, particularly in terms of accuracy, reliability, and suitability [21]

3.1 Behavioral Biometric Authentication

The behavioral biometric authentication approach uses a pattern of human actions. First, signature recognition is fast and simple and capable of acquiring either offline or online through individually extracting the ideal features of the signatures of various individuals. Second, voice recognition is easy to use and aims to identify the human voice by characterizing the voice; however, a limitation is that the voice may change over time [11]. Third, gait patterns discriminate and analyze the way an individual walks but is still under development [11, 12]. Last, the rapid growth of mobile platforms has established touch screen technology a popular input method. Touch dynamics is considered a behavioral biometric authentication that extracts the characteristics of the inputs received from a touchscreen, including multi-touch or the touch-movement [11, 12].

3.2 Physiological Biometric Authentication

The physiological biometric authentication approach involves the unique characteristics of the human body. First, facial recognition is a popular and broadly used method—it is a biometric technique that captures users' facial features from a digital image or video. Second, fingerprint recognition is the most widely used method [13]—it involves touching biometric scanners or capturing users' fingerprint through a camera and extracting features for authentication. Good quality samples depend on the extraction of reliable minutia points from the finger. Third, hand recognition is a biometric technique that is advised to be combined with other individual features to improve the overall security because human hands are not unique [11, 12]. Moreover, new hand recognition technology is based on scanning superficial vein patterns—the biometric system is expected to discriminate between different vein patterns accurately [12]. Last, eye recognition has not been officially implemented for biometric authentication for mobile phones. Iris identification involves a unique pattern based on eye and retina identification regards a thin tissue composed of neural cells behind the eye [11, 12]. Electrooculography signals involve an electrical recording of the eyeball and eyelid movements when blinking [12].

3.2.1 Face Recognition

In literature, numerous surveys regarding biometric user authentication focused on facial recognition authentication on mobile platforms. Wang et al. [22] provided a deep reinforcement learning approach with Convolutional Neuron Networks (CNN) for facial recognition. Wang et al. [22] attempted to solve challenges related to vague facial features during the facial recognition process to determine users' identity for mobile payment. This authentication scheme used a backpropagation algorithm to improve the accuracy of facial recognition using feed-forward network architecture for CNNs, which would enhance the recognition precision compared with existing CNN schemes. Conversely, Samangouei et al. [23] focused on how to extract facial attributes for continuous user authentication purposes. First, the facial attributes of mobile device users were extracted. Next, authentication is completed by comparing and recognizing the difference between the current attributes and the enrolled attributes of the original user. Accordingly, these two methods focus on Single-Factor Authentication (SFA) for recognizing a user's face in terms of vague facial features, but cannot avoid the issue of identity fraud if an impostor uses a picture of the user to gain access to the mobile device. Considering a large number of security threats that the world faces, SFA is no longer effective nor reliable for security purposes and is not considered a secure method for internet transactions or banking [24, 25].

Moreover, Crouse et al. [26] and Mahbub et al. [27] have proposed a continuous authentication method based on users' faces. The first study integrated data from the device's accelerometer, gyroscope, and magnetometer (Inertial Measurement Unit) to improve the performance and accuracy and correct camera sensor orientation and facial image. Therefore, it will enhance face matching performance and accuracy, significantly reduce the time that impostors have to access a device, as well as require a separate server for matching parts, which is considered a challenge. The second study detected partially cropped and occluded faces that were captured using a smartphone's front-facing camera for continuous authentication, which detected facial segments to find one most likely to contain a face. This increased accuracy and processing speed but did not perform detection overlapping facial segments accurately.

Despite being important to continuously verify the user's identity during all interactions rather than just at log in time, Fathy et al. [28] focused on solving the active authentication problem in smartphones. The results of face authentication were studied using videos recorded by the front camera as users performed a task under three different ambient conditions. These recordings were collected from three sessions to extract the variations that are usually present

with mobile devices, which will assist in continuously monitoring the user's identity after the initial access has been granted. Conversely, it is difficult to address the variations in illumination and context that are likely to be present because of the device's mobility. In addition, a user's three sessions are conducted on the same day, which indicates that the dataset would fail to detect variations in appearances such as hairstyle or shaving.

Further, Du [29] attempted to improve the mobile payment identification scheme combined with the method of dynamic heteroscedasticity division and facial feature division, which were split into seven sections. The improved algorithm had superior performance and could be effectively implemented in android smartphones; however, the recognition rate was low in a real environment because environmental influences and the storage capacity restricted the recognition rate. Scheme-based cloud architecture is not used to reduce the computational cost of the mobile terminal and increase the recognition rate. Pal et al. [30] used cloud computing and identity-based encryption and biometric scheme to access data in the cloud to securely solve the problem of excessive data regarding store details and users. Pal et al. [30] aimed to secure user log in and safe banking transactions through privacy-preserving and biometric-based authentication algorithm and Rivest–Shamir–Adelman public-key encryption scheme on direct debit methods by scanning the product barcode using mobile applications. All experiments reflected the efficiency of the algorithm to ensure a safe procedure. The algorithm was secure in a semi-honest model because no third party could learn anything about the original message; however, an impostor could hack the user's account by taking a picture of the user to log in. It would not be detected whether this picture was taken by the authenticated user, which is considered a significant setback.

3.2.2 Fingerprint Recognition

Mathur et al. [31] used a two-stage protocol that aimed to enroll vertical and horizontal finger scanning through small rectangular area sensors to cover the largest area in few scans. The Accelerated-KAZE was proposed as a matching algorithm, which uses multiscale texture descriptors and Fourier Mellin Transform to determine whether sufficient overlap between consecutive fingerprint scans exists. This protocol is faster, efficient, and more accurate. However, this paper focuses on SFA because fingerprints could be fraudulent and it cannot obtain larger fingerprint images through the stitching of horizontal and vertical scans acquired during enrollment.

3.2.3 Multimodal Biometric System

Soviany et al. [32] studied two specific biometric traits for a biometric security model in mobile applications—fingerprint and iris. The study included two research stages for both biometrics: data acquisition using a mobile camera and data processing through the same feature extraction algorithm. Low complexity is present because the same feature extraction algorithm is used for both biometrics; however, there is no security analysis on the model and it requires further improvements and newly defined functional fusion rules to improve the recognition performance.

Islam and Islam [33] proposed a system for mobile security that uses one or more biometric signatures. The user will first provide a personal key and then a biometric signature. Authentication can be performed using one or more biometric signatures, which will be encrypted to enhance overall protection. To enhance the protection against any reasonable changes in signatures over time (e.g., small scratches affecting the fingerprint), additional signatures are added to the database on a temporary basis and discarded after a particular time or iteration. In addition, this system could be applied in various mobile platforms without requiring dedicated biometric scanners. Therefore, the primary aim of this paper was to identify method(s) to collect biometric signatures and simultaneously minimize variations. The second challenge was to research the biometric signature size and verification data that required comparison.

3.2.4 Combining Biometrics and Devices

Mobile devices are prone to be easily stolen or lost. Therefore, it is crucial to ensure protection against unauthorized access to a mobile or application data. Wong and Ho Kim [34] aimed to overcome this issue by using a practical user authentication solution for mobile payment systems and combining mobile devices and biometrics. This solution intended to divide users' private data (e.g., credit card information) and store it in mobile and wearable devices such as smartwatches. Therefore, it differs from the existing solutions that only use a biometrics-based mobile authentication. Importantly, this would assist in preventing leakage of the biometrics template and security attacks, particularly if a device is lost or stolen, as well as improving banking application security. However, it requires two separate devices, which is difficult and more expensive for the user. In addition, it is assumed that the likelihood of the owner to lose both devices simultaneously is relatively low in comparison to losing a single device, and it is expected that the user could erase the authentication information on the lost device.

Various studies focus on Near Field Communication (NFC) technology, which is short-range wireless technology (approximately 10 cm) that enables connecting and exchanging data with close by mobile devices [35]. Vishwakarma1 et al. [36] and Ahamad et al. [37] have studied NFC technology; in which to complete a payment,

the user would select the debit or credit card stored in their mobile and perform a thumb scan for authentication. Consequently, mobile information would be extracted, including International Mobile Equipment Identity or device identification. This process is an effective approach regarding speed and convenience and ensures complete security and confidentiality. Conversely, to successfully complete the transaction, the mobile device must be located near a point-of-sale terminal and a host card emulation device.

4. Comparative Analysis and Discussion

Cybersecurity has always been a challenge for multiple domains but particularly in the mobile ecosystem because it is an integral part of daily life. Cyberattacks are quickly spreading and are becoming an enormous threat to cybersecurity—at least one million new viruses and malware are released each day [38]. Mobile payment (also referred to as m-payment) has become one of the most important application domains in the mobile ecosystem. A key problem associated with m-payment is that existing technologies fail to offer effective authentication of users and their mobile devices. Biometric authentication for m-payment is generally considered quicker, convenient, and a more secure channel to identify and authenticate users for online payment. However, the portability of mobile devices entails their susceptibility to being lost or stolen, which creates security challenges for users and merchants. Therefore, potential user identity authentication threats affect mobile payment.

Biometrics can securely authenticate the user because, although possible, it is not easy to steal or fabricate biometric properties. Biometrics could be hacked or imitated because attackers could duplicate a fingerprint; therefore, biometrics cannot be considered completely reliable [12]. A biometric system includes a sensor that records and reads biometric information and the fingerprint sensor is used each time the mobile device is unlocked. Therefore, there is a threat that any impurity could damage the brittle sensor, or fingerprint injuries (e.g., superficial burns or abrasions) could result in sensors not recognizing the fingerprint. In addition, a hacker could retrieve a user's fingerprint from a physical item (e.g., a cup of coffee that the user might have used) and copy the fingerprint to hack the user's devices or accounts, or an attacker could photograph the user and use the image to hack the user's accounts.

Once biometric information is compromised, an attacker would always have access to the user's account because unlike passwords, biometric traits cannot be changed. For this reason, a reliable and trustworthy method must be used to verify that the owner of these biometric traits is the user himself and not an impostor. This paper evaluates biometric factors based on seven characteristics: universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention [39] (see Table 2).

Table 2: Biometric Factor Characteristics

Characteristics	***Description***
Universality	Distinguish the common characteristics of people
Uniqueness	Uniqueness among individuals—no two persons are expected to have the same characteristic
Permanence	Stable and change over time
Collectability	Easy to acquire and collect
Performance	Stable under varied environmental circumstances
Acceptability	Acceptable by the system's users
Circumvention	Resist tricks and deception

Table 3 demonstrates an empirical evaluation of various biometric technologies based on three sources: literature, online sources, and personal experiences. Specifically, through evaluating data from the literature [11, 40], gathering relevant information from websites [41, 42], then, based on the collected information from literature and online sources, we discuss and find a result that is based on one's own experience.

Table 3: Empirical Evaluation

Reference	***Biometric Type***	***Universality***	***Uniqueness***	***Permanence***	***Collectability***	***Performance***	***Acceptability***	***Circumventio***
[22], [23], [26], [28], [27], [29], [30]	Face recognition	High	Low	Medium	High	Low	High	Low
[31], [33], [34], [37], [36]	Fingerprint recognition	Medium	High	Medium	Medium	High	High	Low
[32]	Fingerprint and iris recognition	Medium/high	High	High/medium	Medium/low	High	Low	High

Conclusion

This article surveyed user authentication techniques on mobile phones and specifically examined the physiological

biometrics that are based on a user's physical characteristics. By reviewing several related studies, it was found that solely using biometrics authentication is not enough to ensure that the owner of the biometric traits is the user and not a hacker. Future research aims to identify a new algorithm for user authentication in mobile devices that could solve the abovementioned limitation.

References

[1] "Number of smartphone users in the United States from 2018 to 2025," *Statista*. https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/ (accessed Aug. 23, 2021).

[2] A. Shankar, C. Jebarajakirthy, and M. Ashaduzzaman, "How do electronic word of mouth practices contribute to mobile banking adoption?," *J. Retail. Consum. Serv.*, vol. 52, p. 101920, 2020.

[3] C. B. Chakiso, "Factors affecting Attitudes towards Adoption of Mobile Banking: Users and Non-Users Perspectives," *EMAJ Emerg. Mark. J.*, vol. 9, no. 1, pp. 54–62, 2019.

[4] C. Z. Maulana, Y. Suryana, D. Kartini, and E. Febrian, "Influencing Factors on the Actual Usage of Mobile Phone Banking in the Shari'ah Banks: A Survey in Palembang City, Indonesia," *Glob. Rev. Islam. Econ. Bus.*, vol. 7, no. 1, pp. 001–019, 2019.

[5] A. W. Siyal, D. Donghong, W. A. Umrani, S. Siyal, and S. Bhand, "Predicting mobile banking acceptance and loyalty in Chinese bank customers," *SAGE Open*, vol. 9, no. 2, p. 2158244019844084, 2019.

[6] "Digital Market Outlook: mobile payment transaction value Spain 2022," *Statista*. https://www.statista.com/statistics/745931/mobile-payment-transaction-value-in-spain/ (accessed Feb. 23, 2020).

[7] B. N. Vuong, V. T. Hieu, and N. T. T. Trang, "An empirical analysis of mobile banking adoption in Vietnam," *Gest. E Soc.*, vol. 14, no. 37, pp. 3365–3393, 2020.

[8] A. Massie, J. S. Lapian, and M. V. Tielung, FACTORS INFLUENCING CONSUMER ACCEPTANCE OF MOBILE BANKING AT SAM RATULANGI UNIVERSITY STUDENTS," *J. EMBA J. Ris. Ekon. Manaj. Bisnis Dan Akunt.*, vol. 7, no. 4, 2019.

[9] S. Raju, "Customer Perception Towards Mobile Banking Services In Warangal Urban District of Telangana State–An Empirical Study," *Our Herit.*, vol. 68, no. 1, pp. 7822–7832, 2020.

[10] I. Olade, H. Liang, and C. Fleming, "A Review of Multimodal Facial Biometric Authentication Methods in Mobile Devices and Their Application in Head Mounted Displays," in *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, 2018, pp. 1997–2004.

[11] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Commun. Surv. Tutor.*, vol. 17, no. 3, pp. 1268–1293, 2014.

[12] R. Jiang, S. Al-Maadeed, A. Bouridane, D. Crookes, and A. Beghdadi, *Biometric Security and Privacy*. Springer, 2017.

[13] P. Temdee and R. Prasad, *Context-aware communication and computing: Applications for smart environment*. Springer, 2018.

[14] V. Matyas and Z. Riha, "Toward reliable user authentication through biometrics," *IEEE Secur. Priv.*, vol. 1, no. 3, pp. 45–49, May 2003, doi: 10.1109/MSECP.2003.1203221.

[15] J. Khan, H. Abbas, and J. Al-Muhtadi, "Survey on mobile user's data privacy threats and defense mechanisms," *Procedia Comput. Sci.*, vol. 56, pp. 376–383, 2015.

[16] L. Xie, H. Xian, X. Tang, W. Guo, F. Hang, and N. Fang, "G-Key: An Authentication Technique for Mobile Devices Based on Gravity Sensors," in *2019 IEEE International Conference on Power Data Science (ICPDS)*, 2019, pp. 126–129.

[17] L. Wu, J. Wang, K.-K. R. Choo, and D. He, "Secure key agreement and key protection for mobile device user authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 2, pp. 319–330, 2018.

[18] T. Zhu *et al.*, "RiskCog: Unobtrusive real-time user authentication on mobile devices in the wild," *IEEE Trans. Mob. Comput.*, 2019.

[19] T. Dahlberg, N. Mallat, J. Ondrus, and A. Zmijewska, "Electronic Commerce Research and Applications," *Retrieved Novemb.*, vol. 6, p. 2011, 2007.

[20] K.-H. Yeh, "A secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments," *IEEE Syst. J.*, vol. 12, no. 2, pp. 2027–2038, 2018.

[21] S. Parusheva, "A comparative study on the application of biometric technologies for authentication in online banking," *Egypt. Comput. Sci. J.*, vol. 39, no. 4, pp. 116–127, 2015.

[22] P. Wang, W.-H. Lin, K.-M. Chao, and C.-C. Lo, "A face-recognition approach using deep reinforcement learning approach for user authentication," in *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*, 2017, pp. 183–188.

[23] P. Samangouei, V. M. Patel, and R. Chellappa, "Attribute-based continuous user authentication on mobile devices," in *2015 IEEE 7th international*

conference on biometrics theory, applications and systems (BTAS), 2015, pp. 1–8.

[24] S. Acharya, A. Polawar, and P. Pawar, "Two factor authentication using smartphone generated one time password," *IOSR J. Comput. Eng. IOSR-JCE*, vol. 11, no. 2, pp. 85–90, 2013.

[25] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, p. 1, 2018.

[26] D. Crouse, H. Han, D. Chandra, B. Barbello, and A. K. Jain, "Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data," in *2015 International Conference on Biometrics (ICB)*, 2015, pp. 135–142.

[27] U. Mahbub, V. M. Patel, D. Chandra, B. Barbello, and R. Chellappa, "Partial face detection for continuous authentication," in *2016 IEEE International Conference on Image Processing (ICIP)*, 2016, pp. 2991–2995.

[28] M. E. Fathy, V. M. Patel, and R. Chellappa, "Face-based active authentication on mobile devices," in *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2015, pp. 1687–1691.

[29] M. Du, "Mobile payment recognition technology based on face detection algorithm," *Concurr. Comput. Pract. Exp.*, vol. 30, no. 22, p. e4655, 2018, doi: 10.1002/cpe.4655.

[30] D. Pal, P. Khethavath, T. Chen, and Y. Zhang, "Mobile payments in global markets using biometrics and cloud," *Int. J. Commun. Syst.*, vol. 30, no. 14, p. e3293, 2017.

[31] S. Mathur, A. Vjay, J. Shah, S. Das, and A. Malla, Methodology for partial fingerprint enrollment and authentication on mobile devices," in *2016 International Conference on Biometrics (ICB)*, 2016, pp. 1–8.

[32] S. Soviany, S. Puscoci, V. Sandulescu, and C. Soviany, "A biometric security model for mobile applications," *Int. J. Commun.*, vol. 3, 2018.

[33] M. F. Islam and M. N. Islam, "A biometrics-based secure architecture for mobile computing," in *2012 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2012, pp. 1–5.

[34] K.-S. Wong and M. H. Kim, "An enhanced user authentication solution for mobile payment systems using wearables," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4639–4649, 2016.

[35] O. Kerem, V. Coskun, B. Ozdenizci, and M. N. Aydin, "A role-based service level NFC ecosystem model," *Wirel. Pers. Commun.*, vol. 68, no. 3, pp. 811–841, 2013.

[36] P. Vishwakarma, A. K. Tripathy, and S. Vemuru, "A hybrid security framework for Near Field Communication driven mobile payment model," vol. 14, no. 12, p. 12, 2016.

[37] S. S. Ahamad, I. Al-Shourbaji, and S. Al-Janabi, "A secure NFC mobile payment protocol based on biometrics with formal verification," *Int. J. Internet Technol. Secur. Trans.*, vol. 6, no. 2, pp. 103–132, 2016.

[38] V. H. and J. Pagliery, "Nearly 1 million new malware threats released every day," *CNNMoney*, Apr. 14, 2015. https://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html (accessed Apr. 21, 2020).

[39] J. Andress, *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress, 2014.

[40] M. Sujithra and G. Padmavathi, "Next generation biometric security system: *an approach for mobile device security*," in *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology - CCSEIT '12*, Coimbatore UNK, India, 2012, pp. 377–381, doi: 10.1145/2393216.2393280.

[41] "Biometrics in 2020 (A helpful illustrated overview)." https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (accessed Jun. 23, 2020).

[42] "biometrics / Authentication technologies." http://biometrics.pbworks.com/w/page/14811351/Authentication%20technologies#FacialRecognition (accessed Jun. 23, 2020).