Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 41 No. 3 (2020)

Biometric Authentication for Secure Mobile Payments

[1]Arth Dave, [2]Pradeep Etikani,[3]Vijaya Venkata Sri Rama Bhaskar,[4]Krishnateja Shiva,[5]Ashok Choppadandi

[12345]Independent Researcher,USA.

Abstract

Mobile payments have evolved into a useful tool for everyday tasks. Mobile phone usage has increased dramatically due to the distinct benefits of mobile transactions over conventional means of payment. Concerns about the security of mobile apps and devices have grown as a result of the robust demand for mobile applications. Novel mobile gadgets are created to fulfil multiple purposes, such as preserving confidential data, gaining access to it, and transferring it via payment methods. In this study, we try to clarify the advantages and difficulties associated with using biometrics to secure mobile payments. The new payment mechanism known as mobile payment gives consumers accessibility, convenience, compatibility, and mobility. However, because payment via mobile device is wireless and electronic in nature, there is a tremendous deal of danger and uncertainty. As a result, in recent years, biometric authorization has become increasingly common in mobile payments. Though the technological prerequisites for safe mobile payments have been satisfied, there are currently no standards or uniform procedures for user authentication in payments through mobile devices. Mobile payment flow management for user authentication is still in its infancy. In order to facilitate secure transactions, avoid user information leakage, and lessen identity theft, this article suggests an anonymous authenticating and administration flow for mobile payments. The suggested management flow processes users' biometric data and personal information based on the smartphone authenticating carrier by integrating transaction key creation, decryption and encryption, and comparison.

Keywords**:** -Mobile Payments, User Authentication, Personal Information, Biometric Characteristics, Early Stage, Encryption and Decryption, Technology Requirements, Mobile Applications, Mobile Phones, Reachability.

I.Introduction

When two people use a mobile device to exchange money for products and services, this is known as a mobile payment. Another way to describe it is as the movement of funds between parties via information exchange. Mobile phones, PDAs, wirelessly laptops, [1, 2], and any other kind of device that may be linked to a mobile telecommunications network in order to process payments are examples of mobile devices [1]. The following obstacles must be removed in order for mobile payments to become generally used and recognized. Cross-border payments, the cost, rapidity, straightforwardness, universality, [2], in the privacy, security, and interoperable. Of all these issues, security is the most important [2, 3].

Three categories of authentication exist. The first method, [3], which is based on hidden knowledge, is utilizing a combination of a password and a PIN (Personal Identification Number). This method offers rapid and inexpensive authentication. The second strategy is the Subscriber Identification Modules (SIM) method, [3, 4], which is based on tokens. With this method, the SIM card is removed from the phone when the user decides not to use it. However, because it is inconvenient, it is not advised to remove the SIM [4, 5]. Payment mechanisms built using tokens and passwords are vulnerable to misuse because of their flaws (lost, copied, shared, distributed, and forgotten) [6, 7]. The use of biometric technology is the final strategy. This method relies on a person's distinctive trait for identification and verification, as personal traits are the basis for this process [7, 8]. Physiological and behavioural biometric techniques are the two main types of biometric approaches.

Over the past 20 years, a variety of methods of payment have been made possible by the emergence of technological trade, the expansion of the Internet, [8, 9], and the advancement of wireless technologies. Particularly, mobile payments are applicable worldwide due to the remarkable rise of mobile networks and devices. Wireless techniques allow users for processing payments over wireless networks with their handheld devices for online as well as offline micropayments, or Examples of these technologies are Near Field Communication (NFC), Bluetooth, QR Code, and Radio Frequency Identification (RFID) [9, 10]. At retail points of sale, mobile payment technology is replacing cash, [10], checks, credit cards, and credit or debit cards as the preferred method of payment. Mobile money transactions are widely accepted in emerging nations with limited formal banking system penetration. In 2018, the value of mobile payments globally reached $391.435 billion [10, 11]. The anticipated annual growth rate for the mobile payment transactions between 2018 and 2022 is 35.7%. In 2022, the total value of transactions made through mobile payments will be $1,328.244 million. Users benefit from mobility, reaching, connectivity, and comfort when they use mobile payments. It gives customers the freedom to pay whenever and from wherever, without being restricted by time or place. However, because mobile payments are wireless and electronic in the natural world, there is a lot of risk and unpredictability involved [11].

Mobile devices could become misplaced or infected with viruses, and mobile networks are susceptible to hacker attacks. For instance, when users of mobile payments connect their electronic gadgets to unreliable Wi-Fi, their data for authentication may be captured [11]. Sensitive data kept on handheld gadgets may end up in the wrong hands in the event that they are lost or stolen. Therefore, among those who use mobile payment methods, security is a top issue. The goal of user authentication is to verify or refute an individual's claimed identity. One common technique used in electronic means of payment for user authentication and message security is cryptographic [11, 12]. Conventional methods of identification rely on either the user's possessions (such as tokens, electronics cards, passports, badges, or smartcards) or their knowledge (such as secret phrases, passwords, PINs, and user IDs). Passwords, [12], PINs, and keys, however, are guessable. SIM (Subscriber Identity Module) cards, [13], which are easily misplaced or stolen, are integrated in consumers' mobile handsets for mobile money transactions. For this reason, mobile financial needs are not satisfied by security safeguards based on traditional authenticating approaches. Therefore, biometric technologies are used for authenticating users in mobile payments [12, 13]. For instance, in 2013 fingerprint recognition was used by Android from Google Pay and Apple Pay to verify customer identity and process payments. In order to ensure user information security, Ali Pay started utilizing fingerprint recognition features in 2015 [16]. Standards and uniform demands are lacking, despite the fact that the technological needs for safe mobile payments have been fulfilled. Mobile payment workflow administration for user authentication is still in its infancy. To enable safe transactions, avoid user information leakage, and lessen identity theft, this article suggests an undetectable authenticating and oversight flow for mobile payments [16, 17].

Biometrics is a technique that allows persons to be uniquely identified or authenticated based on their distinct patterns in physical or behavioural characteristics. Biometric technology is gradually replacing more conventional forms of identification, such as passwords and PINs, as biometric scanners on cell phones and other devices become more commonplace and more services demand strong security and positive user experiences [17, 18]. The most apparent disadvantages of passwords are that they can be stolen, misused, or misunderstood. On the other hand, biometrics provide an alternative solution to the problem of identifying or authenticating a person based on biometric characteristics [18]. They cannot be misplaced or discarded, and unlike passwords, they are difficult to counterfeit. Certain biometric characteristics, such as a person's voice, face, iris, fingerprint recognition, fingertip vein, and furthermore, can be described [18].

The following four components make up a typical biometric system: the template a database, matched module, sensor module, and the extraction of features modules. More specifically, a biometric image is obtained by the sensor module [18, 19]. The feature extraction module takes the obtained biometric image and extracts a set of global or regional characteristics from it. Template data, or standardized feature visualizations, are kept in the template database. To determine whether there is a match or not, the matching module compares the query and templates data [19].

As seen in Figure 1, a typical biometric technique performs authentication in two stages: enrolment and verification. Consider the case of fingerprint identification [20]. When a user places their finger in front of a fingerprint reader during the enrolment process, [20, 21], the sensor module takes a picture of the fingerprint. In the process of verification, specific elements from the obtained fingerprint picture are taken out and modified or converted to provide template data that can be compared [21, 22]. The sensor module gathers a query's fingerprinting image at the verification phase. To get query data, the feature representations of the query fingerprint picture undergo the same procedure as in the enrolment step. After that, the query and template data are compared to ensure an appropriate result [22].

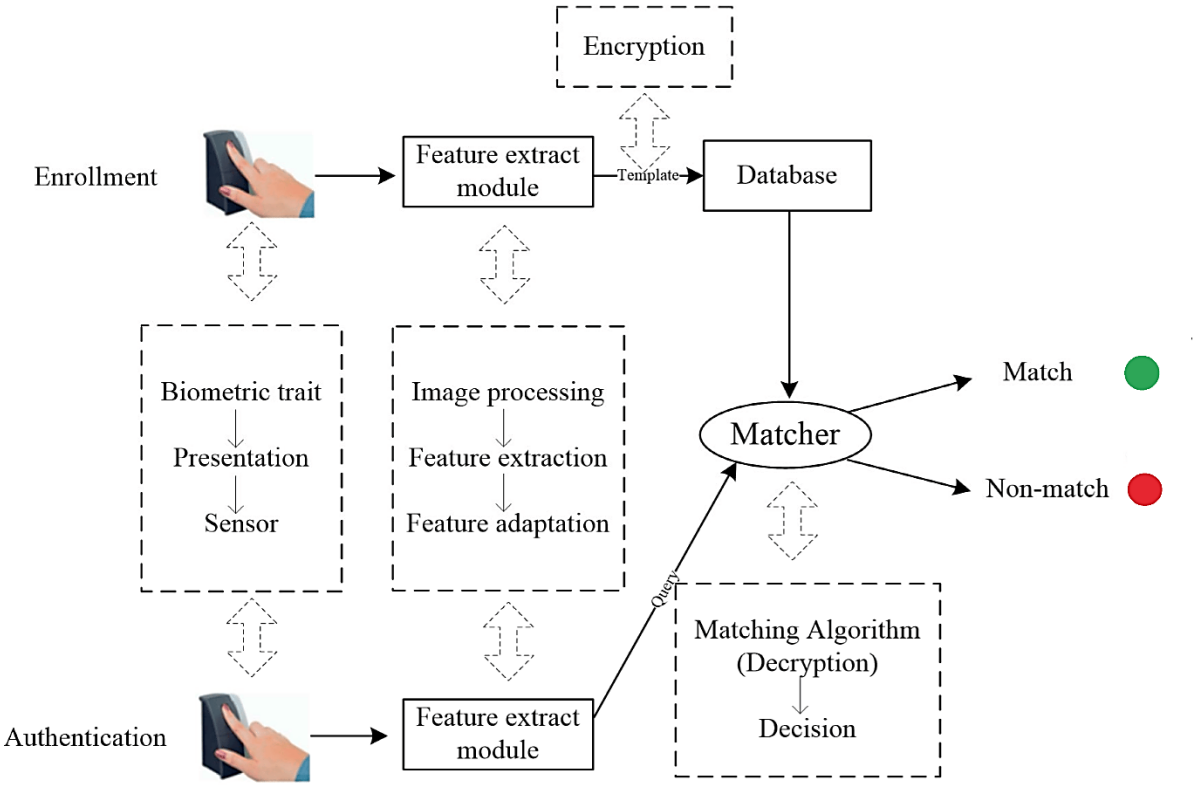

Fig. 1 A Visual Representation of the enrolment and verification phases of a biometric identification system. [22]

Access to the device is provided by knowledge Based on Authorization (KBA), which requires only one authentication step. Knowledge-based authenticating raises security concerns because of things like passwords methods that force online shoppers to make one click payment. Password-based authorization is not appropriate for every user and is very manipulable, with hackers able to get passwords through a variety of techniques [22]. For e-wallet the transactions, ownership-based authenticity has been proposed as a way to lessen the problems associated with knowledge-based verification [22, 23]. Previous research found that the limited application of ownership-based factor-based authenticating was ineffective in preventing fraud. There are issues with attacks from inside and token fabrication when using ownership-based authenticity [23]. Because of this security vulnerability, users' accounts can be exploited by fraudsters who give account holder' additional information to perform unlawful transactions. Preventing fraudulent transactions involving e-wallets is an important priority for the financial industry. Because of this, [23], it can be difficult to discern between authorized and fraudulent transactions when using the present authentication systems [22, 23].

To validate the user's identity, [23], a trustworthy multiple-factor authorization system is needed. A multifactor method for authentication was proposed and put into practice by a number of researchers to lessen this restriction [23, 24]. A small number of researchers concentrated on biometric methods that included face and fingerprint recognition among other authenticating components [24]. There is still a lack of authenticating

capabilities; some are not used because they are difficult to develop, while others have been framework-based solely not being used in practice. Developments are also required to the device identity-based authentication technique that uses (enter the full form of IMEI here) IMEI [24, 25]. Thus, to improve the security of e-wallet apps, gadget identity-based multiple-factor authentication capabilities must be added to the current authentication procedures [25].

II.Payment Flow Administration For Anonymous Biometric Authenticity

This section will cover three main components of biometrics authentication: the personal data of users, biometric traits, and mobile gadgets [26]. These elements are used to authenticate mobile payments. Only once these components are validated can entrusted credits be granted and fund transactions completed [27]. Biometric authorization typically captures a user's fingerprint, facial features, or iris. A biometric identity system for smartphone payments should be able to scan and map users' biometric traits, [27], register them in a database, and provide a template that can be compared to subsequent scans to confirm the user's identity. Consider authentication using fingerprints as a case study [27, 28]. First, the users' fingerprints are pre-processed. The minutiae of each user's fingerprint are then retrieved. Finally, fingerprinting template matching is carried out to determine the relationship between the processed fingerprint picture and one or more stored designs [29].

2.1 Anonymous Biometric the Authentication Process

Authentication for mobile payments, including anonymous authorization, has requirements. First, authentication servers are unable to discover anything about a user if the credential has been encrypted and transmitted with or without the identity [28, 29]. Second, authenticating servers can decode a credential using a secret key or private key produced specifically for confirming companies [29].

Anonymous biometric authorization requires the following elements: users' personal data (ID number, name, date of birth, gender, title, and photo), [29, 30], biometric characteristics (fingerprint, face, or iris), and mobile equipment authenticating carrier (SMS card). Anonymous biometric authentication requires the following three conditions [30].

1. **Hardware demands:**Users' mobile devices ought to include a video camera or a fingerprint CPU for capturing their fingerprint, face, or iris [30, 31]. Users' handheld gadgets must have enough memory and space to process the collected biometric data information.
2. **Biometric Authorization System:**Users' mobile devices and mobile payment systems should be equipped with biometric authentication systems [31, 32]. Users' mobile devices must be able to commence the collection of biometric data and prepare for real-time identity verification. Furthermore, users' smartphones and tablets should be allowed to produce and deliver the mobile payment key to the system [32]. The smartphone payment method must be able to compare users' biometric features templates, interpret transactions, and complete anonymous authentication.
3. **Networking: 2G, 3G, 4G, And 5G:**Wireless connections or Wi-Fi networks are required to provide connectivity between consumers' mobile devices & mobile payment systems. Biometric authentication requires a fast and stable network connection. Many cell phones now include built-in cameras thanks to advancements in mobile device technology. This function makes collecting faces much easy. In contrast, [32], just a few high-end cell phones include fingerprint scanners. As a result, it is easier to capture a face than a fingerprint. Face authentication is more convenient for mobile payments than fingerprint authentication. As mobile technologies advance, biometric authentication is projected to become more widely used in payments via mobile devices [32].

2.2 Anonymous Actually Biometric Identification and Mobile Payments

Management Flow Anonymous biometric authorization in payment devices attempts to conceal users' identities while still ensuring private conversations and secure transactions [33]. In execution, anonymous biometric identification can successfully prevent users' information from being disclosed during interactions while also protecting users' privacy in mobile payments. However, there are no standards or consistent requirements for

mobile payment authentication. Although the technical prerequisites for secured mobile payment methods have been addressed, management of flows in mobile payments is still in its early stages [34]. A widely acknowledged management of flows is not accessible with mobile payments [35, 36].

Figure 2 depicts how each component in mobile payment flow management functions independently. As a result, there are gaps in current mobile payment flow management. Take the use of fingerprint authentication in payments via mobile devices as an example [37]. If a user's signature is accepted, their fingerprints are pre-processed on their mobile devices before being transferred to an authentication service. Next, the server extracts minutiae from the users' fingerprints. Finally, fingerprint template matching is performed on the server to determine whether a processed fingerprint picture corresponds to any of the stored templates [38, 39]. A matching algorithm must be used to carry out the matching. If a match is identified, authentication is successful, & users can proceed to the next stage of their transaction in mobile payment [40].

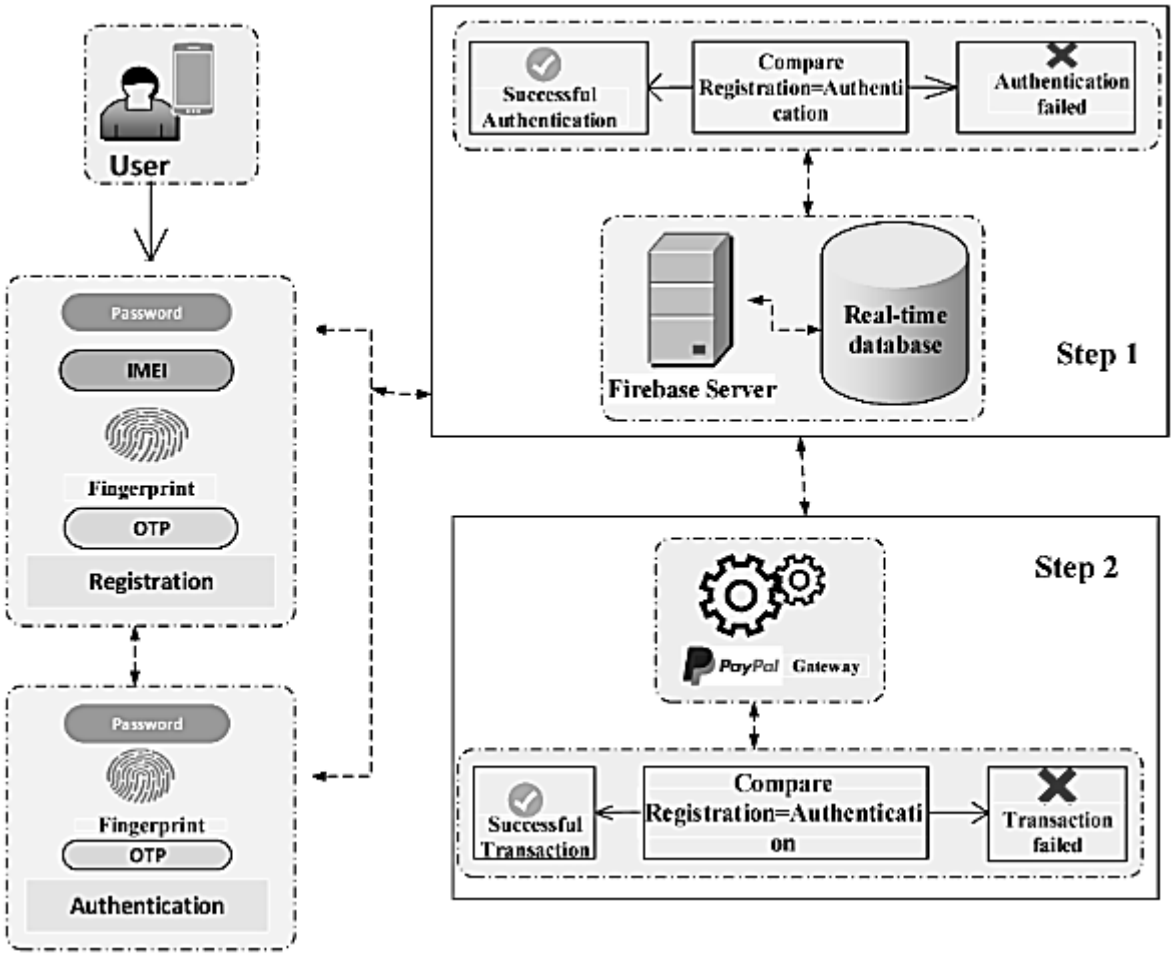

Fig. 2 Flow of obtaining the mobile payment key by biometric identity identification. [41]

III.Summary Of The Authentication Process In Mobile Payments

In the last two decades, the rise of electronic business, the expansion of the Internet, and the advancement of wireless technology have facilitated the creation of a variety of methods. Wireless techniques including Near Field Communication (NFC), [41, 42], Bluetooth connectivity, the Quick Response (QR) Code, and RFID (Radio Frequency Identification) allow users to make payments over wireless networks using their mobile phones or tablets for both online transactions and offline micropayments [43, 44]. Because of its electronic and electromagnetic nature, payments via cell phones are fraught with uncertainty and risk. As a result, mobile payment must include identity identification and privacy protection to improve access control [45, 46]. Biometric authorization can be more secure than authentication with a password. In particular, anonymous

biometric authorization may successfully prevent users from disclosing personal information during conversations [47, 48]. Biometric authentication has become popular in mobile payments in recent years [48, 50]. In 2013, for example, the success of Apple, Ali-pay, and WeChat Payment implemented fingerprint authentication for mobile payments. Later, Ali Pay and We Chat Payment implemented face authentication for mobile payments. Biometric authentication is projected to be used more widely in mobile payments.

IV.Conclusion

In this study, the multimodal biometric payments model is combined with the biometrics multi-server authentication model. This study was prepared from a broader perspective of payments and transactions, as well as security considerations. The suggested biometric payment methodology provides clients with a user-friendly transaction and payment experience. And the multi-server authentication paradigm allows the user to connect to different servers around the world for various features and accesses meeting the varied security measures such as resisting guessing attacks, resisting replay attacks, and resisting stolen - verifier attacks.

The suggested management flow includes public key and private keys generation after generation, transaction data encryption and decryption, trace management, and matching to process users' individual information and biometric information using a mobile equipment authenticating carrier. The supervision of cash flow promotes secure business interactions and settlement of payment in mobile payments by lowering internal identification alteration and decryption risks. Anonymous biometric authorization will become more common in mobile payments. Future research should test the management flow presented in this paper and integrate pseudo-face, fingerprints, and dynamic authentication of identity to improve the authentication process in mobile payments.

V.References

[1] Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. Cryptography 2018, 2, 1.

[2] Fan, K.; Li, H.; Jiang, W.; Xiao, C.; Yang, Y. U2F based secure mutual authentication protocol for mobile payment. In Proceedings of the ACM Turing 50th Celebration Conference—China, Shanghai, China, 12–14 May 2017.

[3] Shaju, S.; Panchami, V. BISC authentication algorithm: An efficient new authentication algorithm using three factor authentication for mobile banking. In Proceedings of the 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, 19 November 2016; pp. 1–5.

[4] Okpara, O.S.; Bekaroo, G. Cam-Wallet: Fingerprint-based authentication in M-wallets using embedded cameras. In Proceedings of the 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Milan, Italy, 6–9 June 2017.

[5] Khattri, V.; Singh, D.K. Implementation of an Additional Factor for Secure Authentication in Online Transactions. J. Organ. Comput. Electron. Commer. 2019, 29, 258–273.

[6] Prabhakar, S.; Pankanti, S.; Jain, A.K. Biometric recognition: Security and privacy concerns. IEEE Secur. Priv. 2003, 1, 33–42.

[7] Awad, A.I.; Hassanien, A.E. Impact of Some Biometric Modalities on Forensic Science. In Computational Intelligence in Digital Forensics: Forensic Investigation and Applications; Springer: Berlin, Germany, 2014; pp. 47–62.

[8] Zheng, G.; Shankaran, R.; Orgun, M.A.; Qiao, L.; Saleem, K. Ideas and challenges for securing wireless implantable medical devices: A review. IEEE Sens. J. 2016, 17, 562–576.

[9] Zheng, G.; Fang, G.; Shankaran, R.; Orgun, M.A.; Zhou, J.; Qiao, L.; Saleem, K. Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks. IEEE J. Biomed. Health Inf. 2017, 21, 655–663.

[10] Zheng, G.; Fang, G.; Shankaran, R.; Orgun, M.A. Encryption for implantable medical devices using modified one-time pads. IEEE Access 2015, 3, 825–836.

[11] Awad, A.I.; Hassanien, A.E.; Zawbaa, H.M. A Cattle Identification Approach Using Live Captured Muzzle Print Images. In Advances in Security of Information and Communication Networks; Springer: Berlin, Germany, 2013; pp. 143–152.

[12] K. Xi, J. Hu, and F. Han, "An alignment free fingerprint fuzzy extractor using near-equivalent Dual Layer Structure Check (NeDLSC) algorithm," in 6th IEEE Conference on Industrial Electronics and Applications (ICIEA), 2011, pp. 1040-1045.
[13] W. Yang, K. Xi, and C. Li, "A cancellable and fuzzy fingerprint scheme for mobile computing security," in AIP Conference Proceedings, 2012, p. 1494.
[14] Y. Wang, J. Hu, and D. Phillips, "A fingerprint orientation model based on 2d fourier expansion (fomfe) and its application to singular-point detection and fingerprint indexing," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 29, 2007, pp. 573-585.
[15] Y. Wang and J. Hu, "Global ridge orientation modeling for partial fingerprint identification," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 33, 2011, pp. 72-87.
[16] P. Zhang, J. Hu, C. Li, M. Bennamoun, and V. Bhagavatula, "A pitfall in fingerprint bio-cryptographic key generation," Computers & Security, vol. 30, 2011, pp. 311-319. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, 2004, pp. 4-20.
[17] Du, X., Wang, H., Du, Y., Xu, L. D., Chaudhry, S., Bi, Z., & Li, J. et al. (2017). An industrial information integration approach to in-orbit spacecraft. Enterprise Information Systems, 11 (1), 86–104.
[18] Ferraiolo, D., & Kuhn, R. (1992). Role-Based Access Control. 15th NIST-NCSC National Computer Security Conference, 554-563.
[19] GeekPark. (2014). Pay for the New Future-Six Major Change You Can't Miss. Business Next.
[20] Guo, J., & Bouwman, H. (2016). An ecosystem view on third party mobile payment providers: A case study of Alipay wallet. Info, 18(5), 56–78.
[21] Hahn, I., & Kodó, K. (2017). Acceptance of Online and Mobile Payment: A Cross-Country Analysis of Germany, Hungary, and Sweden. Academic Press.
[22] Han, F., Hu, J., Yu, X., Feng, Y., & Zhou, J. (2006, January). A novel hybrid crypto-biometric authentication scheme for ATM based banking applications. In International Conference on Biometrics (pp. 675-681). Springer.
[23] Linnartz J. P. and Tuylus, P. (2003), New shielding functions to enhance privacy and prevent misuse of biometric templates, Proc. AVBPA 2003, Fourth International Conference on Audioand Video-Based Biometric Person Authentication, pp. 393-402, Guildford, UK.
[24] Putte, T and Keuning, J. (2000), Biometrical fingerprint recognition: don't get your fingers burned, Retrieved November 20, 2005 from
[25] Ratha, N. K., Connell, J. H. and Bolle, R. M. (2001), An analysis of minuntiae matching strength, Proc. AVBPA 2001, Third International Conference on Audio – and Video-Based Biometric Person Authentication, pp. 223-228.
[26] Ross, A., Shah, J. and Jain, A. K. (2005), towards reconstructing fingerprints form minutiae points, Proc. SPIE, Biometric Technology for Human Identification II, Vol. 5779, pp. 68-80, (Orlando, FL).
[27] Schneier, B. (1999), Inside Risk: The uses and abuses of biometrics, Comm. ACM, vol. 42, no. 8, p. 136. Shoniregun, C.A., (2003), Are existing Internet security measures guaranteed to protect user identity in the financial services industry? Int. J. Services Technology and Management, vol. 4, no. 2, pp.194-216.
[28] Aydos, M., Yanik, T., & Koc, C. K. (2001). High-speed implementation of an ECC-based wireless authentication protocol on an ARM microprocessor. IEE Proceedings. Communications, 148(5), 273–279.
[29] Benenson, Z., Dewald, A., & Freiling, F. C. (2009). Presence, Intervention, Insertion: Unifying Attack and Failure Models in Wireless Sensor Networks (Vol. 356). Technical report, University of Mannheim.
[30] Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., & Elliott, S. J. (2007). Privacy preserving multi-factor authentication with biometrics. Journal of Computer Security, 15(5), 529–560.
[31] Bi, Z., Liu, Y., Krider,J., Buckland,J., Whiteman, A., Beachy, D., & Smith,J. (2018). Real-time force monitoring of smart grippers for Internet of Things (IoT) applications. Journal of Industrial Information Integration, 11, 19–28.
[32] Carton, F., Hedman, J., Damsgaard, J., Tan, K. T., & McCarthy, J. (2012). Framework for mobile payments integration. Electronic Journal of Information Systems Evaluation, 15(1), 14–25.
[33] Fernando L. Podio: "Personal Authentication through Biometric technologies".

[34] Anil K. Jain, Arun Ross and Salil Prabhakar: "An Introduction to biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and VideoBased Biometrics, Vol. 14, No. 1, January 2004.
[35] Innoviti Simplifying Communications "Online Biometric Authenticated Payment Systems. 2008
[36] Vibha Kaw Raina and U.S Pandey "Biometric and ID based user authentication mechanism using smart cards for multi-server environment" Proceedings of National Conference on Communications INDIA Com 2011.
[37] Adler, A. (2004), Images can be regenerated from quantized biometric match score data, Proc. Canadian Conf. Electrical Computer Eng., pp. 469-472, (Niagara Falls, Canada).
[38] J. C. Liou and S. Bhashyam, A feasible and cost effective two-factor authentication for online transactions, in Proc. 2nd Int. Software Engineering and Data Mining Conf., Chengdu, China, 2010, pp. 47–51.
[39] S. Nseir, N. Hirzallah, and M. Aqel, A secure mobile payment system using QR code, in Proc. 5th Int. Computer Science and Information Technology Conf., Amman, Jordan, 2013, pp. 111–114.
[40] Z. Sahnoune, E. A¨ımeur, G. E. Haddad, and R. Sokoudjou, Watch your mobile payment: An empirical study of privacy disclosure, in Proc. 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 2015, pp. 934–941.
[41] M. Shao, J. Fan, and Y. Li, An empirical study on consumer acceptance of mobile payment based on the perceived risk and trust, in Proc. 2014 Int. Cyber-Enabled Distributed Computing and Knowledge Discovery Conf., Shanghai, China, 2014, pp. 312–317.
[42] H. Jiang, Study on mobile e-commerce security payment system, in Proc. 2008 Int. Electronic Commerce and Security Symposium, Guangzhou, China, 2008, pp. 754– 757.
[43] Benli, E.; Engin, I.; Giousouf, C.; Ulak, M.A.; Bahtiyar, S. BioWallet: A Biometric Digital Wallet. In Proceedings of the Twelfth International Conference on Systems (Icons 2017), Venice, Italy, 23–27 April 2017; pp. 38–41.
[44] Alibabaee, A.; Broumandnia, A. Biometric Authentication of Fingerprint for Banking Users, Using Stream Cipher Algorithm. J. Adv. Comput. Res. 2018, 9, 1–17.
[45] Houngbo, P.J.; Hounsou, J.T.; Damiani, E.; Asal, R.; Cimato, S.; Frati, F.; Yeun, C.Y. Embedding a Digital Wallet to Pay-with-aSelfie, from Functional Requirements to Prototype; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; Volume 206, ISBN 978-3-319-67836-8.
[46] Vengatesan, K.; Kumar, A.; Parthibhan, M. Advanced Access Control Mechanism for Cloud Based E-Wallet; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; Volume 31, ISBN 978-3-030-24642-6. [Google Scholar]
[47] Tirtea, R. Algorithms, Key Sizes and Parameters Report; European Union Agency for Cybersecurity (ENISA): Athens, Greece, 2013; pp. 1–5.
[48] Sönmez, F.; Abbas, M.K. Development Of A Client/Server Cryptography-Based Secure Messaging System using RSA Al-gorithm. J. Manag. Eng. Inf. Technol. 2017, 4, 6.
[49] Nwoye, C.J. Design and Development of an E-Commerce Security using RSA Cryptosystem. Int. J. Innov. Res. Inf. Secur. 2015, 2, 2349–7017.
[50] Aina, F.; Yousef, S.; Osanaiye, O. Design and Implementation of Challenge Response Protocol for Enhanced e-Commerce Security; Springer International Publishing: Berlin/Heidelberg, Germany, 2018; Volume 3, ISBN 9783030026837.
[51] Ashok : "Choppadandi, A., Kaur, J.,Chenchala, P. K., Nakra, V., & Pandian, P. K. K. G. (2020). Automating ERP Applications for Taxation Compliance using Machine Learning at SAP Labs. International Journal of Computer Science and Mobile Computing, 9(12), 103-112. https://doi.org/10.47760/ijcsmc.2020.v09i12.014
[52] Chenchala, P. K., Choppadandi, A., Kaur, J., Nakra, V., & Pandian, P. K. G. (2020). Predictive Maintenance and Resource Optimization in Inventory Identification Tool Using ML. International Journal of Open Publication and Exploration, 8(2), 43-50. https://ijope.com/index.php/home/article/view/127
[53] Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). AI Applications in Smart Cities: Experiences from Deploying ML Algorithms for Urban Planning and Resource Optimization. Tuijin Jishu/Journal of Propulsion Technology, 40(4), 50-56.

[54] Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service. International Journal
[55] of Transcontinental Discoveries, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98
[56] Choppadandi, A., Kaur, J., Chenchala, P. K., Kanungo, S., & Pandian, P. K. K. G. (2019). AI-Driven Customer Relationship Management in PK Salon Management System. International Journal of Open Publication and Exploration, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128
[57] Ashok Choppadandi et al, International Journal of Computer Science and Mobile Computing, Vol.9 Issue.12, December- 2020, pg. 103-112. (Google scholar indexed)
[58] Choppadandi, A., Kaur, J., Chenchala, P. K., Nakra, V., & Pandian, P. K. K. G. (2020). qhttps://doi.org/10.47760/ijcsmc.2020.v09i12.014
[59] Chenchala, P. K., Choppadandi, A., Kaur, J., Nakra, V., & Pandian, P. K. G. (2020). Predictive Maintenance and Resource Optimization in Inventory Identification Tool Using ML. International Journal of Open Publication and Exploration, 8(2), 43-50. https://ijope.com/index.php/home/article/view/127
[60] Shah, D., Dhanik, A., Cygan, K., Olsen, O., Olson, W., & Salzler, R. (2020). Proteogenomics and de novo sequencing based approach for neoantigen discovery from the immunopeptidomes of patient CRC liver metastases using Mass Spectrometry. The Journal of Immunology, 204(1_Supplement), 217.16-217.16.
[61] Shah, D., Salzler, R., Chen, L., Olsen, O., & Olson, W. (2019). High-Throughput Discovery of Tumor-Specific HLA-Presented Peptides with Post-Translational Modifications. MSACL 2019 US.
[62] Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76
[63] Fadnavis, N. S., Patil, G. B., Padyana, U. K., Rai, H. P., & Ogeti, P. (2020). Machine learning applications in climate modeling and weather forecasting. NeuroQuantology, 18(6), 135-145. https://doi.org/10.48047/nq.2020.18.6.NQ20194