10.48047/jocaaa.2023.31.4.24

BIOMETRIC AUTHENTICATION IN DIGITAL PAYMENT SYSTEMS: SECURITY ENHANCEMENTS AND PRIVACY CONCERNS

Ceres Dbritto
Independent Researcher, USA.
IEEE Senior Member, USA
Orcid Id: 0009-0001-7494-8799

Abstract

Biometric authentication is transforming the security landscape of digital payment systems, offering enhanced security and convenience through methods like fingerprint, facial, and voice recognition. The aforementioned innovations enable for faster and greater precise identity confirmation, reducing dependence on conventional login credentials or PINs, as well as mitigating scams risks. Nevertheless, the use of biometric details also increases essential worries about anonymity, data protection, and ethical difficulties. Stolen biometric data details, unlike login credentials, cannot be transformed, making it a possibly permanent threat. This paper investigates the function of biometric verification in online payments, as well as concentrating on both its protection benefits and the confidentiality challenges it poses. Through secondary analysis, the study Reviews current biometric technologies, legal frameworks like GDPR, and real-world implementation examples to highlight the balance between innovation and privacy. The paper concludes with a look at future trends, including decentralized systems and AI improvements, aiming to ensure safer and

10.48047/jocaaa.2023.31.4.24

more inclusive biometric applications in financial services.

Keywords: *Biometric authentication, fingerprint recognition, data protection, digital payments, financial technology, privacy, ethical concerns and security.*

Introduction

The evaluation of new digital payment systems has paved the way for transforming and stated how financial transactions are conducted with this changed approach, evaluated the need for methods of payments with secure and user-friendly authentication. Conventional security methods like passwords and PIN systems are getting endangered with identified theft and prone to breaches. As the response of digital evaluation, biometric authentication systems incorporate unique features of different biological traits such as facial recognition of face features, voice, finger prints and have gained constant popularity based on user-friendly features, convenience and reliability. Although these innovations improve security, they additionally raise important confidentiality and ethical concerns with regard to information storage, abuse, and monitoring. This investigation examines the dual effect of biometric verification in electronic money transfers, concentrating on both privacy improvements and the obstacles to private anonymity.

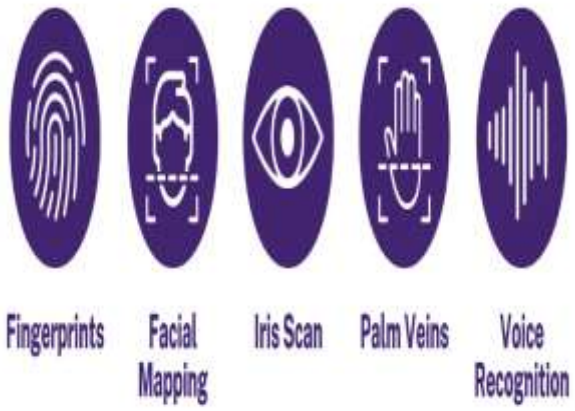


Figure 1: Different types of Biometric authentication

10.48047/jocaaa.2023.31.4.24

(Sourse:https://www.nmi.com/eu/blog/a-beginners-guide-to-biometric-authentication-for-payments/)

Method

This study used the qualitative research methodology, undertaking the process of secondary analysis in order to evaluate different roles of biometric authentication in the process of digital payment systems, considering the matters of privacy concerns and security improvements. In case of involving an approach this article has used the deductive approach, starting with the establishment of theories and frameworks based on data privacy, digital identity and cybersecurity[1]. This is being applied over the real-world application in the technological implementation. Interpretivism philosophy has been employed in order to identify the functional process of biometric technologies within social settings with different technical, legal and cultural contexts.

The secondary data analyzed by collecting information from different secondary sources that includes peer-reviewed journal articles, different government regulations like GDPR, and India's Personal Data Protection Bill, white papers, and existing case studies on biometric deployment in the process of using digital payment systems like Google Pay, Apple Pay, Phone-pay, and. Key topics including user permission, data protection, ethical factors and system flaws, are being collected and evaluated to offer understanding about the wider implications of biometric recognition. Both socio-ethical implications as well as technical aspects were identified and understood about the biometric systems by implementing this approach. By evaluating available knowledge under the perspective of theory, the study critically examines the balance between strengthening

10.48047/jocaaa.2023.31.4.24

the safety of data and maintaining individual confidentiality in financial environments.

Figure 2: Advantages of Biometric authentication

(Source: https://www.relevantinsights.com/articles/secondary-research-advantages-limitations-and-sources/)

This methodological approach initiates in evaluating deeper-insight over the use and impact of biometric recognition over digital payment systems[2]. Technical evaluation in the field of finance provides utmost security that fosters an improved process of financial settings. Utilization of different secondary sources provides authentic and reliable information that strengthen the base of this evaluation. Thus this approach will initiate the research to be conducted with any chaotic situation and provides different effectiveness of the digital systems.

Discussion

In this digital world, the evaluation of Biometric authentication has brought a drastic change in the way people access payments. Thus it provides a time saving approach with better security and a faster user experience, but along with benefits it also generates concerns about privacy maintenance. This section of the article will explore the benefits, and disadvantages associated with digital payment systems.

10.48047/jocaaa.2023.31.4.24

Figure 3: Advantages of Biometric authentication

(Source: https://appinventiv.com/blog/biometrics-technology-in-digital-banking/)

1. Stronger Security through Unique Identification

One of the significant aspects of this digitalized payment system is biometric authentication that uses different body parts such as face features or fingerprints for the purpose of identification. Thus the body features are different to every individual that makes it harder for other individuals to duplicate and steal identity. This advanced digitalized system provides with more scopes of security. In conventional payment systems, buyers use credentials or PINs that can be overlooked, suspected, or exploited. Hackers may mislead victims into releasing them. However with biometrics, the fingerprint and face constitutes a possession that only the victim possesses [4]. Thus making digital payments less vulnerable and protecting users from theft. For example the applications like google-pay, apple pay and other digitalized modes of payments often used the facility of biometrics and face recognition, within the process of payment approval. This feature prevents trespass from misusing an individual's phone without his or her consent.

10.48047/jocaaa.2023.31.4.24

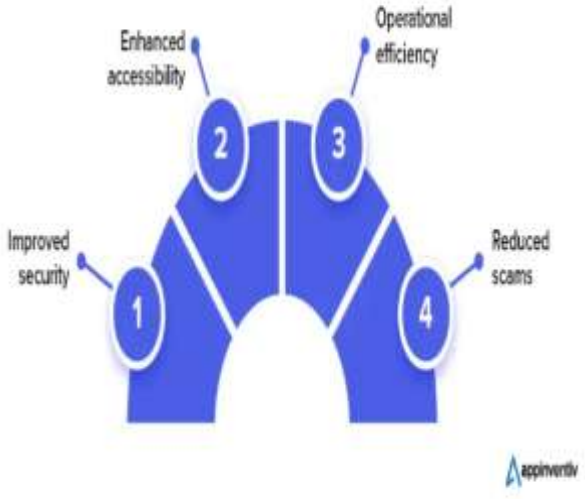
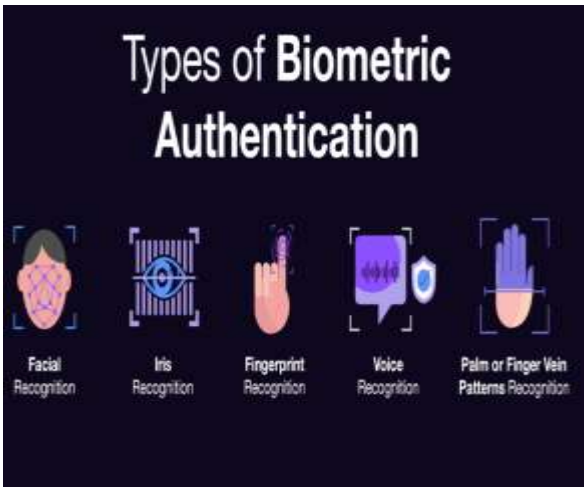


Figure 4: Advantages of Biometric authentication

(Source: https://appinventiv.com/blog/biometrics-technology-in-digital-banking/)

2. Convenience and Faster Transactions

Biometric authentication provides with more faster and user-friendly process of payments. Users are not required to recall their passwords or PINs each time they complete a purchase. Rather it includes the features like scanning, face or finger of an individual[3]. This initiates a cashless, user friendly payment process, which enables easy access of transactions within safe and secure environments[11]. This is beneficial, particularly with payments via mobile devices and contactless systems. One may accept the transaction within a few seconds, which enhances the client interaction. In congested contexts like convenience stores, public transport, or internet buying, this swiftness may reduce time as well as alleviate stress. This evaluation incorporated an effective transaction process with smoother and easier techniques that initiates in safer means of transaction and secure financial management.



10.48047/jocaaa.2023.31.4.24

Figure 5: Types of Biometric authentication

(Source: https://www.tokenring.com/learn/biometric-authentication)

3. Multimodal Biometrics for Extra Safety

Some systems in recent days use different multimodal biometrics that demonstrate the use of more than one or two biometric data at the same time. For example, both voice, and fingerprint are recognized at same time as the verification process. This implements another secure layer in security checks. By the incorporation of more than one process of verification, it makes the entire system harder for thieves or someone with stealing intention[12]. It will be provided with strict features to prevent easy access to someone's device or account. In the event that someone succeeds to imitate one biometric trait, they're unable to mimic both. This can be beneficial in high-security financial transactions, including substantial cash exchanges or confidential banking processes.

Figure 6: Multimodal Biometrics authentication

(Source: https://appinventiv.com/blog/biometrics-technology-in-digital-banking/)

10.48047/jocaaa.2023.31.4.24

4. Data Breaches and Storage Risks

Even though this technological integration has several benefits and seems to be effective and safe, it has several odds which make it imperfect. Some of the greatest risk factors are the preservation of data. Whenever biometric information is gathered, it's required to be kept saved in a certain location, whether that is the device being used or within an organization's databases[10]. In such a case if the database where the information of the users are stored is not a secure one then it will serve with a smoother access for the hackers, break it and steal all valuables kept inside[5]. A prime instance involves the Biostar 2 hack in 2019, whereby biometrics and recognition of face information for more than one million individuals were made public owing to inadequate safety precautions. This demonstrated how hazardous biometric data could be if not managed efficiently.

Passwords can be changed if required or in the case of users' unconsciousness but biometric recognition is not changeable in that way if the device is stolen [9]. Users may reset the password but cannot change the face pattern or finger print data stored in the stolen device$_6$. As the results make this breach to be more dangerous with log-lasting after effects.

Figure 7: Biometrics authentication

(Source:

https://blog.koorsen.com/biometrics-the-

10.48047/jocaaa.2023.31.4.24

convergence-of-digital-and-physical-identity-for-better-access-control)

5. Privacy and Consent Issues

The major concern in this technical approach lies within matters of privacy. There are many individuals who have not been aware or concern about the fact of data storage, like how their data are being stirred for repetitive usage. This is also a matter of concern as breaking security and theft of overall data could result in mass theft which could be extremely dangerous. In some circumstances, organizations acquire data without offering sufficient details to individuals or seeking for explicit authorization. This is considered an absence of informed authorization. Also, individuals are concerned that their personal information could potentially be utilized for other reasons, for example advertising or monitoring, without their permission. This worry of "function creep", may give rise to the circumstance where information can be utilized for purposes exceeding what was initially agreed upon which can decrease public confidence in biometric authentication systems[9]. In order to reduce the risk of such dangers the organizational bodies are required to be more transparent with their employee, and associated stakeholders in keeping their personal details. They should provide clear insight on how and why the biometric data is collected, storied, protected and mention the period of time.

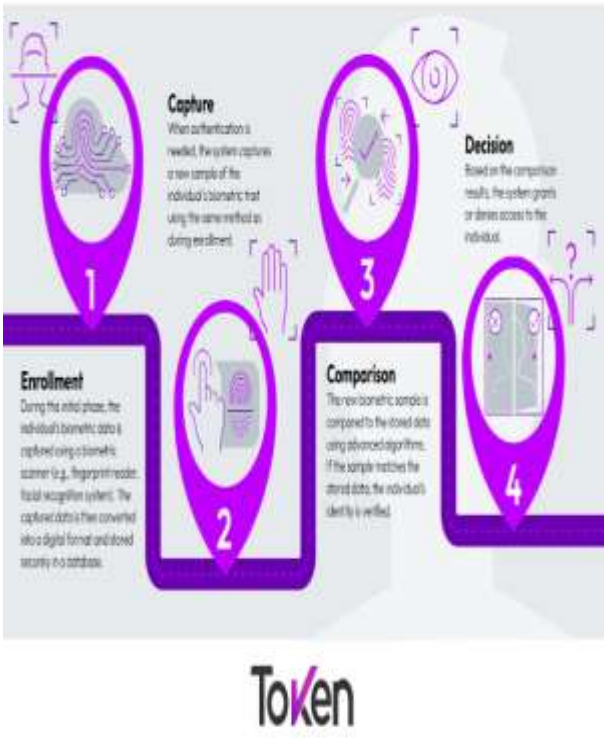


Figure 8: Biometrics authentication

10.48047/jocaaa.2023.31.4.24

(Source: https://www.tokenring.com/learn/biometric-authentication)

6. Legal and Regulatory Protection

Use of the Biometric data is implied with different laws in many countries to make a safer use of it and ensure a proper use with authentic process. For example, the General Data Protection Regulation (GDPR) in the country of the European Union undertook this issue of biometric data security as one of the most sensitive factors of protection of personal information. Adhering to the guideline of GDPR, organizations should get with a clear or transparent consent from an individual before collecting this data and must ensure security and confidentiality[7]. While in the country like India, where Aadhaar system includes biometric lock system like iris scans and fingerprints data, for keeping individuals identity and payment purposes

In India, the Aadhaar system uses biometric data (like fingerprints and iris scans) for identity and payment purposes. Although it has assisted countless individuals gain access to amenities, it has come under criticism regarding privacy issues. Several court decisions currently restrict whether Aadhaar data may be utilized, notably by private enterprises[8]. These stated examples are crucial to understand the incorporation of laws are important to ensure fair and safer use of the biometric data within any organizational settings.

10.48047/jocaaa.2023.31.4.24

Figure 9: Biometrics authentication challenges

(source:https://www.gsmarena.com/google_pay_finally_adds_biometric_authentication_for_money_transfers-news-39841.php)

Conclusion

Concluding on the digital advancement in the modern era of financial management it can be said that Biometric authentication has significantly enhanced the associated security and convenience on the digital payment systems with the provision of reliable, user-specific and fast verification. Nevertheless, it also creates significant security obstacles, which comprises the possibility of data violations, exploitation of sensitive data, and ethical considerations. Although legislation including GDPR offers substantial security, additional prerequisites to be undertaken to guarantee users permission, accountability, and appropriate data management. These biometric systems are required to be created with more security and confidential features to ensure users with trust and effectiveness. And also by assuring inclusion, equitable treatment, and consideration for individual liberties in an emerging digital financial environment ensures individual's trust and confidence towards the application of this system.

Future Perspectives

Better Privacy Protection:

10.48047/jocaaa.2023.31.4.24

With the implementation of advanced and new technologies ensure the biometric data to be safely stored. Biometric encryption ensures prevention and protection of face and fingerprint, even in the situation of theft, as this restricts third-party use.

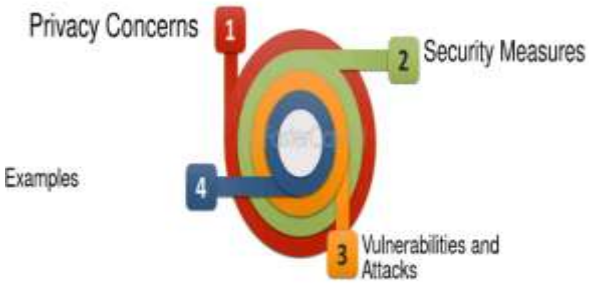


Figure 10: Biometrics data privacy and Security

(source: https://www.google.com/url?sa=i&url=https%3A%2F%2Ffastercapital.com%2Ftopics%2Fbest-practices-for-biometric-data-encryption.html&psig=AOvVaw0k5AaLG9GnUQOz4lx-jAbN&ust=1746874416975000&source=images&cd=vfe&opi=89978449&ved=2ahUKEwiB3P-5nJaNAxXQPlkFHfN7Kj4Q3YkBegQIABAd)

Decentralized Storage:

As a futuristic approach, biometric data of an individual may be the system to be stored on his or her own phone or within the platform of a secure block chain system, not within a common big main database. Thus these approaches will be initiated in reducing the occurrence of different big data leaks.

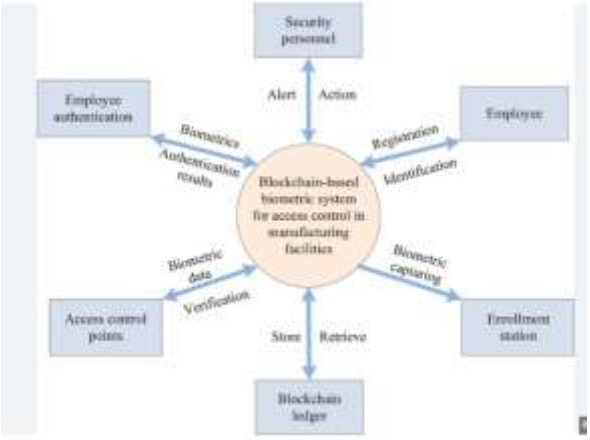


Figure 11: Decentralized Storage

(source:https://www.researchgate.net/figure/Context-diagram-for-blockchain-based-biometric-authentication-system-for-access-control_fig14_377894975?__cf_chl_rt_tk=c

10.48047/jocaaa.2023.31.4.24

ajFFIeq5j5BF.VKIXw8qQEkZkWkwcQDPptYnKIkCYQ-1746788231-1.0.1.1-WD9843a3EeCUJBfh0WR8lx.W17Xqcb7z7Wc2pMDLALg)

(source: https://www.leewayhertz.com/generative-ai-in-finance-and-banking/)

Smarter and Fairer AI:

By reading biometric data with accuracy and effectively, the implemented AI will be enhanced. It should therefore be programmed to prevent bias, so it performs similarly well for individuals of all age groups, complexion tones, as well as physical capabilities. These advantages will ensure individual's use of these protective payment systems safeguarded with utmost security.

Figure 12: AI implementation

More Inclusive Systems:

Developers are required to build such a design which can be accessible and easier to use to everyone including individuals with physical disabilities or any special physical traits.

Stronger Laws and Rules:

Government initiatives in enhancing existing systems will likely provide better means of laws in order to protect and evaluate the process of data collection and use of biometric data within the organizational boundaries. Rules are required to be strict and rigid with conscious, tactful laws. These new upgrades within existing laws will help prevent misuse of data and increase public trust over the data security system.

Balance of Security and Privacy creates More Awareness:

10.48047/jocaaa.2023.31.4.24

In future this system will ensure safety in the process of online payments, by adhering to laws and respecting user's freedom and privacy. Users will be more cautious about the intricate process and will show interest in learning more about their data rights, and companies will take initiatives in transparent explanation over the use of biometric information.

Reference List

Journals

Salimi, S., Mawlana, M. and Hammad, A., 2018. Performance analysis of simulation-based optimization of construction projects using high performance computing. Automation in Construction, 87, pp.158-172.

Kuraku, C., Gollangi, H.K. and Sunkara, J.R., 2020. Biometric Authentication In Digital Payments: Utilizing AI And Big Data For Real-Time Security And Efficiency. Chandrababu Kuraku,. et. al.(2020). Biometric Authentication In Digital Payments: Utilizing AI And Big Data For Real-Time Security And Efficiency Educational Administration: Theory and Practice, 26(4), pp.954-964.

Rui, Z. and Yan, Z., 2018. A survey on biometric authentication: Toward secure and privacy-preserving identification. IEEE access, 7, pp.5994-6009.

Patra, G.K., Rajaram, S.K. and Boddapati, V.N., 2019. Ai And Big Data In Digital Payments: A Comprehensive Model For Secure Biometric Authentication. Educational Administration: Theory and Practice.

Hassan, M.A., Shukur, Z., Hasan, M.K. and Al-Khaleefa, A.S., 2020. A review on electronic payments security. Symmetry, 12(8), p.1344.

Solat, S., 2017. Security of electronic payment systems: A comprehensive survey. arXiv preprint arXiv:1701.04556.

10.48047/jocaaa.2023.31.4.24

Iqbal, S., Irfan, M., Ahsan, K., Hussain, M.A., Awais, M., Shiraz, M., Hamdi, M. and Alghamdi, A., 2020. A novel mobile wallet model for elderly using fingerprint as authentication factor. IEEE Access, 8, pp.177405-177423.

Normalini, M.K. and Ramayah, T., 2017. Trust in internet banking in Malaysia and the moderating influence of perceived effectiveness of biometrics technology on perceived privacy and security. Journal of Management Sciences, 4(1), pp.3-26.

Porubsky, J., 2020. Biometric Authentication in M-Payments: Analysing and improving end-users' acceptability.

Nasution, M.I.P., Nurbaiti, N., Nurlaila, N., Rahma, T.I.F. and Kamilah, K., 2020, September. Face recognition login authentication for digital payment solution at COVID-19 pandemic. In 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE) (pp. 48-51). IEEE.

Liu, C., Hu, X., Zhang, Q., Wei, J. and Liu, W., 2019. An efficient biometric identification in cloud computing with enhanced privacy security. IEEE Access, 7, pp.105363-105375.

Hamidi, H., 2019. An approach to develop the smart health using Internet of Things and authentication based on biometric technology. Future generation computer systems, 91, pp.434-449.