Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

Payment Integration using Biometric and Virtual 3D Password

Prof. N.M. Mule
Department of Information Technology
Government College of Engineering,
Karad, Satara, India

Abhishek Bhosle
Department of Information Technology
Government College of Engineering,
Karad, Satara, India

Vivek Mote
Department of Information Technology
Government College of Engineering,
Karad, Satara, India

Pratiksha Jadhav
Department of Information Technology
Government College of Engineering,
Karad, Satara, India

Ankita Kulkarni
Department of Information Technology
Government College of Engineering,
Karad, Satara, India

Abstract - This research paper discusses the advantages and disadvantages of various payment methods including fingerprint, iris recognition, voice recognition, face recognition. While biometric authentication uses unique physiological and behavioral characteristics of the user, it raises privacy and ethical concerns, as biometric data is sensitive and can be compromised. To address these limitations, this paper proposes the integration of 3D password authentication with biometric authentication to provide a higher level of security. The proposed method involves first performing biometric authentication and then 3D password authentication. If both authentication methods are successful, encrypted payment details, including user information and payment information, are sent to the bank for verification. If the user information is accurate, the payment is processed; otherwise, the payment is rejected. This system provides a more secure, convenient, and streamlined authentication process. The advantages and disadvantages of the proposed system are highlighted in this paper, including improved security and privacy, but also ethical concerns regarding biometric data collection and storage along with a conclusion of the research study. Overall, the proposed method improves upon existing payment systems by providing a unique, memorable, and secure password for each user, while also addressing the limitations of biometric authentication.

Keywords: 3D password, Biometric Authentication, Payment, Integration, etc.

I. INTRODUCTION

Payment integration using biometric technology has gained significant attention in recent years as a more secure and convenient way to authenticate users for financial transactions. Biometric techniques such as fingerprint, face recognition, iris recognition, and voice recognition have been widely used for authentication purposes. However, each of these biometric techniques has its advantages and limitations [1]. Fingerprint recognition is the most commonly used biometric technique due to its low cost, easy deployment, and high accuracy. However, it can be easily hacked with fake fingerprints or lifted prints. Face recognition and iris recognition are also popular techniques, but they require high-quality images and may fail due to variations in lighting, pose, and facial expressions. Voice recognition is another biometric technique, but it can be fooled with pre-recorded voice samples[2].

To overcome these limitations, our research proposes the, integration of 3D password technology with biometric authentication. 3D password is a user-friendly and more secure authentication technique that involves creating a three-dimensional virtual environment where the user can set up a series of personalized gestures and movements as their password [3]. By combining biometric and 3D password authentication, we can provide a higher level of security and protection against fraudulent activities.

The objective is to assess the current state of research on the integration of biometric and 3D password technologies for payment authentication. This paper aims to examine the feasibility and effectiveness of combining various biometric

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

techniques with 3D password technology for payment authentication purposes, while also investigating the usability and user acceptance of such systems in real-world settings. Through a thorough analysis and synthesis of existing literature, this paper intends to provide valuable insights into the potential of biometric and 3D password technologies in creating a more secure and user-friendly payment integration system.

II. EXISTING BIOMETRIC TECHNIQUES

Among the biometric techniques, fingerprint has Unresolved challenges such as Efficient automated fingerprint classification, Fully automated latent fingerprint recognition, Detection of altered or fake fingerprints, efficient compression of fingerprint templates, and automated artificial fingerprint generation [4]. A study by [5], Iris recognition technology poses difficulties in miniaturizing the hardware for image acquisition. And it may have limited convenience, means it may struggle with recognizing individuals with black eyes and can be dependent on lighting conditions, impacting its convenience and ease of use [5]. The detailed comparison of various biometric techniques is shown in Table 1. Another study in palm authentication system [6] has the vocal tract biometric method that is non-invasive, requiring no physical contact or insertion of devices into the body. voice authentication has several advantages like minimal intrusiveness [7] means the process of collecting vocal tract data for identification purposes does not require invasive procedures, such as physical contact or insertion of devices into the body. It avoids discomfort or potential health risks associated with invasive biometric methods, contributing to its overall acceptability and usability in various identification scenarios.

But leading disadvantages like Local acoustic of the environment [7], it introduce variability and impact the accuracy of the voice-based biometric system, leading to potential recognition errors or false identifications.

Table 1: Comparison of Various Biometric Techniques

Types of Biometric Techniques	Accuracy	Cost	Advantages	Disadvantages	References
Fingerprint	High	Medium	1. Cost-effective 2. Quick processing 3. Compact storage 4. Seamless integration	1. Securing the fingerprint recognition system and its template database is critical to prevent unauthorized access and privacy breaches. 2. Unresolved challenges. 3. false match and false non-match.	[4,7]
Face	Medium	Medium	1. Manual Monitoring is eliminated thus man power is saved. 2. Fast Processing	1. Slowness during image processing.	[8,9]
Iris	High	High	1. Contactless 2. Distinctiveness 3. Consistency	1. Challenging to miniaturize 2. Limited convenience	[5,6]
Palm	Medium	Low	1. The Phase Symmetry technique boasts flawless recognition accuracy of 100%, minimal CPU overhead, as well as rapid, straightforward, and efficient performance.	1. Inefficient for mass production.	[6]
Voice	High	Medium	1. Used effectively with telephones, enabling remote authentication 2. Minimal intrusiveness	**1.** Age and illness can impact the quality and characteristics of the voice **2.** Local acoustics can throw off the biometric system	[7]

III. LITERATURE SURVEY

The research [10], necessitates the development of 3D software, utilizing the Unity3D package to construct a 3D virtual environment. This environment employs leap motion technology to enable interaction between the user and their mobile device,

detecting movements made by the user's right hand. Each time

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

a cube is touched, its state changes and this is visually displayed. The order in which the cubes are touched is recorded and passed to an algorithm that generates a unique password. During the creation of the password, the position of the cubes in 3D space can be randomized and selected. However, drawback of this approach is that it exclusively employs cubes as 3D objects, with simple letter labels, which may limit the variety of objects and labels that can be used for password generation in the virtual environment.

The research paper [11] presents a novel approach called the Secured Biometric Payments model utilizing Tokenization. This approach allows for payments to be made using biometric methods while keeping the actual card number concealed, ensuring enhanced security. Instead, It provides a unique identification for each customer and links a payment card to each of their fingers. When making a payment at a merchant point of sale, users can use any of their enrolled payment fingers, and the payment will be processed using the linked payment card associated with the scanned finger. As a result, there is no need payment cards or invest in expensive mobile phones exclusively for the purpose of making convenient payments.

JuCheng Yang[1] proposed a secure multimodal biometric payment system that combines digital signature and biometric verification techniques. The system uses fingerprint and IR face features for authentication and has nine authentication models. Biometric images undergo feature extraction to produce templates stored in a database. The algorithm for fingerprint verification includes preprocessing, feature extraction, and core point determination. Blood perfusion data is used for face recognition through the skin heat transfer model. The algorithm for multimodal biometric fusion involves feature extraction, concatenation, feature reduction, and scoring. The study highlights security vulnerabilities and privacy protection. In Alsulaiman and El Saddik [3] introduced the concept of a 3-D password, which is an authentication scheme that incorporates multiple techniques within a virtual environment. This allows users to select the techniques they want to use for authentication. The authors discussed the guidelines for constructing the virtual environment, conducted security analysis, and presented experimental results. The 3-D password system offers a larger password space, making it more challenging for attackers to guess the password. The authors highlighted the significance of considering the difficulty for attackers to compromise a system in the security analysis, and suggested that a larger password space and lack of prior knowledge of user password selection can enhance security. The study revealed that most users tended to have only a limited number of unique textual passwords, with the majority having fewer than eight unique textual passwords. Additionally, the study indicated that most users found the 3-D password system acceptable and not a threat to personal privacy.

Bharti S. Yerne and Prof. Fazeel.I.Z.Qureshi [12] proposes an enhanced content-based shoulder surfing safe graphical password plan that uses colours for easy and efficient login. The strategy entails implementing a two-tier authentication system that incorporates a basic text-based shoulder surfing graphical password as the initial level, followed by the use of 3D pictures as the secondary level. The 3D password adds an extra layer of security to the user's login process. The authors review several existing shoulder surfing safe graphical password plans and their limitations. The proposed plan aims to be both secure and user-friendly. The paper provides a detailed description of the proposed plan's security and usability features and demonstrates its resistance to shoulder surfing and accidental login.It seems that you have provided an excerpt from a research paper or a technical report discussing different authentication schemes proposed in the literature to enhance the security of login systems against shoulder surfing and other types of attacks. The passage describes various techniques proposed by different researchers, including the use of colors, images, and 3D passwords, among others.

Wencheng Yang, Jiankun Hu and Jucheng Yang[2] discusses the potential benefits and challenges associated with using biometric authentication for securing mobile payments. Biometric authentication is considered a more trustworthy method of authentication compared to traditional methods such as passwords or tokens, but there are several challenges associated with it. The security of biometric templates, recognition accuracy, social acceptability, and system integration are identified as key challenges. To address these challenges, biometric template protection, biometric cryptosystems, multimodal biometric systems, and co-existence of password-based and biometric-based authentication are proposed as potential solutions. Stable feature sets or multimodal biometrics are recommended to enhance recognition accuracy. Overall, the article highlights the potential of biometric authentication for securing mobile payments and proposes solutions to address the associated challenges.

An Enhanced ID Authentication written by Praveen Kumar Singh and Bineet Kumar Gupta[13] explores the integration of biometric technology with smartcards to enhance identity authentication and verification. The paper discusses the advantages of using biometrics with smartcards and highlights different biometric techniques for identity authentication. It also addresses the key considerations that influence the use of biometrics in smartcards, such as privacy concerns and processing times for sample comparisons. Additionally, the paper presents limitations of DNA technology for authentication and suggests its use as a secondary source of authentication. The article concludes by proposing future scopes for improving biometric technologies and emphasizing the importance of adequate security measures to safeguard biometric data and balance security concerns with privacy considerations. The paper also highlights security and privacy concerns associated with the use of biometric technology, including the risk of data misuse, fraudulent access to central databases, and different types of biometric vulnerabilities. Finally, the article discusses techniques for biometric template matching and storage, as well as the use of multi-model biometric systems to enhance accuracy.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

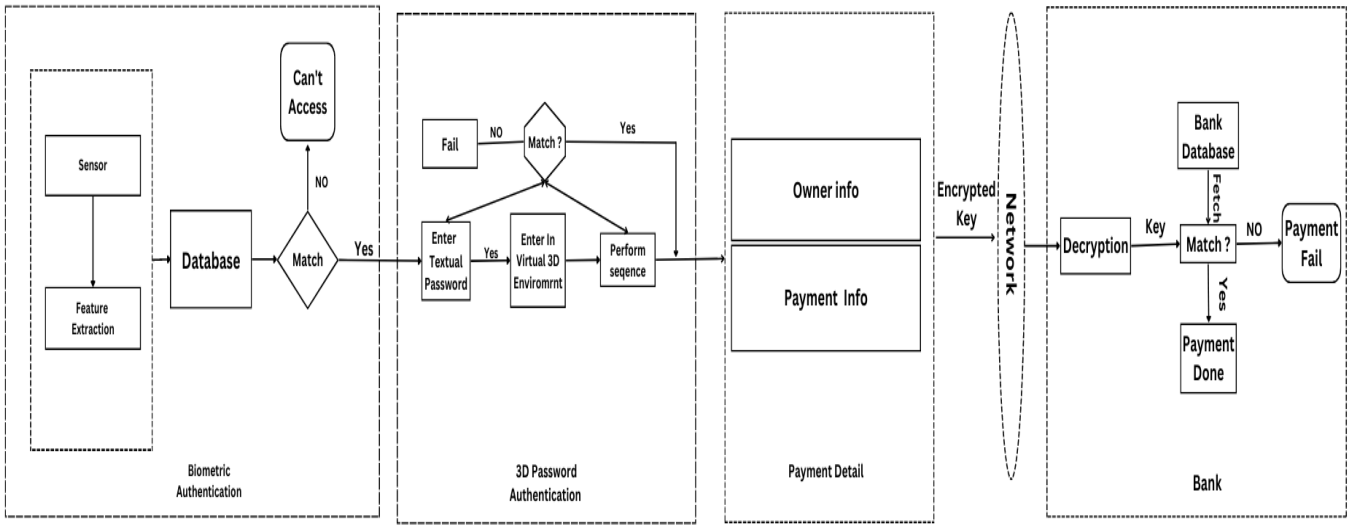

Fig 1: Architecture for payment integration using Biometric and 3d password

In [14], introduces a new way of entering PINs called 3DPIN, which utilizes a 3D display on an LG Optimus 3D smartphone. The method shows a stereoscopic image of a random challenge that only the rightful user can see from a specific point called the "3D spot." Glasses-free 3D displays commonly found in smartphones and handheld gaming consoles are particularly well-suited for this approach. The program was written in Java on Android 2.3.3. An initial test was conducted with twenty participants to assess the method's performance. The median authentication time was 12.7 seconds, and the error rate was 10.0%. To further examine the method's performance, a second test was performed with a focus group of 10 volunteers who showed that as users got accustomed to the method, the time required for authentication sessions gradually decreased. The error rate also decreased with time.

IV. PROPOSED METHODOLOGY

In today's digital age, securing online transactions is more critical than ever. The current standard of username and password authentication has its limitations, making it vulnerable to hacking and phishing attacks. As a result, there is a need for a more secure and reliable authentication method.This research proposes a novel approach to authenticate users for online transactions. The proposed methodology involves a multi-factor authentication system that combines biometric data, gesture sequences, and 3D environment. Architecture for payment integration using Biometric and 3d password [Fig 1].

A. Collecting biometric data

When it comes to collecting biometric data, it's important to ensure that the user's privacy is respected and their data is secured. Here are some points to consider when collecting biometric data for authentication purposes:

- *Informed consent:* Before collecting biometric data, it's important to obtain the user's informed consent. This means providing clear and concise information about how the data will be collected, stored, and used.
- *Collection methods:* There are several ways to collect biometric data, including through fingerprint scanners, facial recognition cameras, or even voice recognition technology. The collection method used will depend on the type of being collected and the device being used for authentication.
- *Security:* The security of biometric data is of utmost importance due to its high sensitivity, necessitating robust measures for storage. This entails utilizing encryption and other security protocols to prevent unauthorized access. Additionally, the security of the device employed for data collection and storage should be carefully considered.
- *Accuracy:* Biometric information is not infallible and may be influenced by different factors, such as illumination, facial follicles, or physical trauma. It is crucial to verify that the gathered data is precise and suitable for authentication objectives.
- *Data protection:* Biometric data should be treated as personal and sensitive data and protected accordingly this means adhering to data protection laws and regulations, and ensuring that the data is not shared or sold without the user's explicit consent

B. Storing biometric data

Here are some key points to consider when storing biometric data:

- Data format: Biometric data can be stored in various formats, such as templates, images, or feature vectors. The choice of format depends on the type of biometric data being collected and the algorithms used for authentication.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

- Sensor accuracy: The accuracy of the biometric sensor used to collect the data can affect the quality of the data stored in
- the database. Therefore, it's important to use high-quality sensors that can capture accurate and reliable biometric data.
- Encryption and security: Biometric data is sensitive information and should be encrypted and stored securely to prevent unauthorized access. It's important to implement strong security measures, such as encryption, hashing, and access controls, to protect the data from cyber threats.
- Database design: The design of the database used to store biometric data should take into account the size of the data, the search algorithms used for matching, and the performance requirements of the system. It's important to choose a database design that can efficiently store and retrieve large amounts of data while maintaining high accuracy and reliability.

  False Acceptance Rate (FAR) and False Rejection Rate (FRR) of a biometric authentication system:

  FAR = (False Accepts / Total Authentication Attempts) x 100% [15]

  FRR = (False Rejects / Total Authentication Attempts) x 100% [15]

  In these formulas, the False Accepts are the number of instances where the system incorrectly accepts an impostor as a valid user, while the False Rejects are the number of instances where the system incorrectly rejects a valid user as an impostor.

  The FAR and FRR are usually reported as percentages, with lower values indicating higher accuracy of the system. It's important to note that there is often a trade-off between the FAR and FRR, and finding the right balance between the two is a key challenge in designing an effective biometric authentication system [15]

C. Authenticate user data

After collecting and securely storing the user's biometric data in a database, the next step is to authenticate the user's identity by performing operations on the stored biometric data. The process of authenticating the user's identity typically involves comparing the user's biometric data to the stored data to verify their identity.

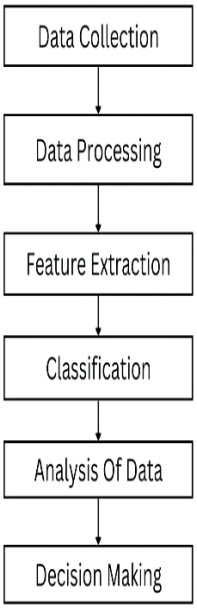

Fig 2: Flowchart of Authenticate user data

Here are some key points to consider when authenticating user data:

- Matching algorithms: Biometric authentication systems use various algorithms to match the user's biometric data to the stored data. These algorithms can be based on statistical or mathematical models, and they typically calculate a similarity score or distance metric between the user's biometric data and the stored data.

- Thresholds: To determine whether the user's biometric data matches the stored data, the system uses a threshold value that represents the level of similarity required for a match. If the similarity score exceeds the threshold, the system considers the user's identity to be authenticated.

- Error rates: Biometric authentication systems are subject to error rates, such as False Acceptance Rate (FAR) and False Rejection Rate (FRR), which represent the likelihood of incorrect authentication decisions. It's important to choose an appropriate threshold value that balances the FAR and FRR to achieve high accuracy and reliability[15]

- Continuous authentication: Some biometric authentication systems also incorporate continuous authentication, which involves periodically re-authenticating the user's identity during a session to prevent unauthorized access.

  Here is an example of a formula for calculating the similarity score or distance metric between the user's

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

biometric data and the stored data, based on the Euclidean distance algorithm:
Euclidean distance = sqrt ((x1 − y1)^2 + (x2 − y2)^2 + … + (xn − yn)^2) [16]
In this formula, x1 through xn represent the features or characteristics of the user's biometric data (e.g., the pixel values of a fingerprint image), and y1 through yn represent the corresponding features of the stored data. The formula calculates the Euclidean distance between the two sets of features, which represents the overall similarity or difference between the two biometric samples.[16]

It's important to note that the formula for calculating the similarity score or distance metric is just one component of the authentication process, and other factors such as threshold values and error rates also play a critical role in determining the accuracy and reliability of the system.

D. Username and password

Upon completing the biometric authentication, the user is required to enter textual username and password for authentication, the system typically prompts the user to enter their username and password using a text input field. The username and password are then stored in a database, often in an encrypted form, and used for comparison during the authentication process. If the password is correct, they are granted access to the 3D virtual environment. Otherwise, access is denied.

Here is an example of a formula for encrypting passwords using a hashing algorithm:

hashed_password = hash_function (password + salt) [17]

In this formula, the password is concatenated with a random salt value and passed through a hash function, which generates a fixed-length string of characters. The hashed password is then stored in the database, along with the salt value, to prevent attackers from easily recovering the original password [17].

E. Entering into 3d environment

Upon completing the biometric authentication, In the 3D environment, such as virtual or augmented reality, the user is prompted to create a 3D password by selecting and manipulating objects within the environment to create a unique gesture or pattern.[3]

Here is an example of the process for entering the 3D environment for authentication:

- The user successfully completes the biometric authentication and is prompted to enter the 3D environment for the next stage of authentication [3]
- The system loads the 3D environment and presents the user with a set of objects and interactions that can be used to create a 3D password [3]
- The user selects objects from the environment and manipulates them in a specific manner to create a unique gesture or pattern. This may involve rotating, scaling, or moving the objects in a specific sequence or order [3]
- The system records the user's 3D password and securely stores it in a database for future authentication attempts [3] By utilizing a 3D environment for authentication, the system can create a unique and secure password that is difficult for hackers to replicate. Additionally, the use of biometric authentication and 3D passwords adds layers of security to the overall authentication process

E. Connect user to bank

After successfully completing the biometric and 3D password authentication process, the user needs to input their payment information. The system then creates an encrypted key that combines the payment data and user data. This key is used to establish a secure connection between the user's bank account and the payment system. To ensure the confidentiality and integrity of the transmitted data, secure communication protocols such as HTTPS or SSL/TLS are used.

The connection can be initiated either by the user or the system, depending on the specific implementation. Once the secure connection is established, the user can securely access their bank account information and perform payment transactions. The system can also employ additional security measures like two-factor authentication to further enhance the transaction's security.

While there may not be specific formulas or diagrams related to connecting a user to their bank account, including diagrams or flowcharts that illustrate the payment integration process, including the steps involved in establishing a secure connection to the bank, could be beneficial. These visual aids could help users understand the complex processes involved in securing their financial transactions.

F. Approve payment

In a biometric and 3D password-based payment system, approving payment involves verifying the user's identity through encrypted keys and confirming payment details before completing the transaction. Once the user connects to their bank account, the bank system decrypts the key and compares it with the data in its database. If the verification process succeeds, the transaction is completed; otherwise, it fails.

To prevent fraudulent transactions and unauthorized payments, a final confirmation step is presented to the user. This step ensures that the user approves the correct payment amount and recipient

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

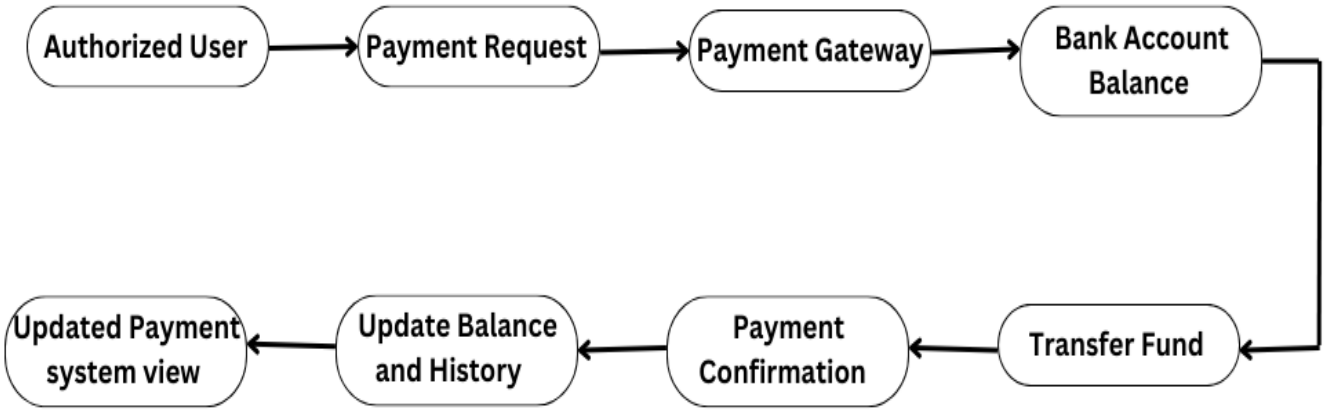

Fig 3: Steps for payment

before the transaction is completed. One possible formula for the final confirmation step could involve calculating the total payment amount and presenting it to the user for confirmation. For instance:

Total Payment Amount = Payment Amount + Transaction Fee

The user must then confirm that the total amount is correct before the payment can be completed. This step helps to ensure the accuracy and legitimacy of the transaction.

V. ADVANTAGES OF USING VIRTUAL 3D PASSWORD IN BIOMETRIC PAYMENT SYSTEM

The use of 3d password in biometric payment system provides advantages in terms of safeguarding and Enhanced user satisfaction that cannot be obtained from traditional password- or token-based authentication methods.

A. Safeguarding

Biometric traits are extremely difficult to forge, unlike traditional payment methods like cards, which can be cloned or copied. Biometric payment methods employ distinct physical or behavioral attributes of an individual, like fingerprints, facial features, or iris scans, to identify and verify the user. Even identical twins would have different fingerprints [18]. In biometric payment system there is a risk of losing biometric templates, biometric data is very crucial so once it is compromised it will be lost forever. The incorporation of 3D password technology in a biometric payment system enhances the system's security by providing increased complexity and multi-factor authentication. Additionally, it includes features like real-time intrusion detection and blocking of unauthorized access attempts, which further fortify the system's security. it helps in preventing fraud by detecting and blocking unauthorized access attempts. This makes it an ideal solution for biometric payment systems where the risk of fraud is high.

B. Enhanced user satisfaction

In contrast to conventional password-based systems, 3D password technology eliminates the need for users to memorize intricate passwords or PINs. with the use of virtual 3d password user can remember their password like a story. This results in a quicker and more user-friendly authentication process[14]. Thus, the use of 3D password technology in biometric payment systems can improve the user experience by providing a more secure, convenient, and streamlined authentication process.

VI. DISADVANTAGES OF USING VIRTUAL 3D PASSWORD IN BIOMETRIC PAYMENT SYSTEM

The virtual 3D password technology offers potential advantages in biometric payment systems, it is crucial to take into account the possible obstacles and complexities that may arise during the implementation and adoption stages. The user acceptance of 3D password technology in biometric payment systems may face some challenges due to its novelty, which can result in reluctance or resistance from some users to adopt the technology[10]. Furthermore, creating and remembering complex 3D passwords may prove to be challenging for some users, leading to frustration and difficulties in completing payment transactions. The applicability of the 3D password technology in some payment systems may be limited by compatibility issues with certain biometric devices[5]. This can pose a challenge as it may prevent some users from accessing the payment system or force them to switch to a different authentication method.

VII. DISCUSSION

The research paper on biometric payment integration with 3D password aims to address the security issues associated with traditional payment methods and biometric authentication.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 06, June-2023

Traditional payment methods such as cash, credit cards, and e-wallets are vulnerable to hacking and phishing attacks [13]. On the other hand, biometric authentication is a promising solution that uses unique physiological and behavioral characteristics of the user to provide more secure authentication. However, biometric data is sensitive and raises privacy and ethical concerns [2]. To address these issues, the research paper proposes integrating biometric authentication with 3D password, a multifactor authentication scheme that creates a 3D virtual environment in which the user interacts with objects to create a unique password [10]. The combination of biometric authentication and 3D password provides a more secure, convenient, and streamlined authentication process. This paper provides an additional layer of security to prevent unauthorized access to user accounts. Biometric authentication ensures that only the authorized user can access their account, while the 3D password provides an additional layer of protection against brute-force attacks and phishing attempts [5]. The 3D password is difficult to guess or crack since each user has a unique password that they can remember like a story. Biometric data is sensitive and raises privacy and ethical concerns. The research paper should address how to securely store and transmit biometric data to prevent unauthorized access and how to address privacy and ethical concerns associated with using biometric data. The proposed approach of biometric payment integration with 3D password has the potential to enhance the security of online transactions and make them more convenient for users [3]. Additional advancement are required to tackle these challenges and enhance the efficiency and user-friendliness of this methodology.

VIII. CONCLUSION

This proposes integrating biometric payment methods with 3D password authentication to provide a more secure and convenient online payment experience. The integration of biometric data and 3D password authentication offers a higher level of security, making it difficult for hackers to gain unauthorized access. The proposed payment method involves performing biometric authentication first, followed by 3D password authentication. If both are matched, the encrypted payment and user details are passed to the bank for verification. If the user details are accurate, the payment will proceed, otherwise, the payment will fail. Each user having a unique and memorable password so ethical concerns regarding biometric data collection and storage should be addressed to ensure the privacy and protection of user data. This study has highlighted the potential of integrating biometric payment methods with 3D password authentication, and its advantages over existing payment methods. It is a more streamlined and secure payment method, addressing the limitations of existing payment methods.

IX. REFERENCES

[1] Yang, J. (2010). Biometrics Verification Techniques Combing with Digital Signature for Multimodal Biometrics Payment System.
[2] Yang, W., Hu, J., Yang, J., Wang, S., & Shu, L. (2013). Biometrics for securing mobile payments: Benefits, challenges and solutions. In International Congress on Image and Signal Processing. https://doi.org/10.1109/cisp.2013.6743950
[3] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik “Three-Dimensional Password for More Secure Authentication” 2008
[4] Nath, Dev & Ray, Saurav & Ghosh, Sumit. (2011). Fingerprint Recognition System : Design & Analysis.
[5] Ye, H., Pei, R., Mo, Z., Zheng, Q., & Chen, H. (2020). Comparison on the Security of Biometrics. Journal of Physics, 1607(1), 012120. https://doi.org/10.1088/1742-6596/1607/1/012120
[6] Priyanka Kamboj, Shashi Bala “Review Paper on Enhancing Palm Print Recognition System” 2015
[7] Manivannan, Nadarajah & Noor, Azad & Student, Phd & Memon, Shahzad & Memon@brunel, Shahzad & Uk,. (2011). Fingerprint Biometric for Identity management. 2. 39-44.
[8] Chanchal S. Khandelwal, Shilpa R. More, Sai S. Phalke, Prachi J. Kamble, 2013, Tracking of Unauthorized Access Using Face Recognition, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 02, Issue 01 (January 2013)
[9] Francisco D. Guillén-Gámez & Iván García-Magariño & Sonia J. Romero, 2015. "Analysis of the Perception of Students about Biometric Identification," International Journal of Web-Based Learning and Teaching Technologies (IJWLTT), IGI Global, vol. 10(3), pages 1-18, July.
[10] Yu, Z., Olade, I., Liang, H., & Fleming, C. B. (2016). Usable Authentication Mechanisms for Mobile Devices: An Exploration of 3D Graphical Passwords. In International Conference on and Service. https://doi.org/10.1109/platcon.2016.7456837
[11] Garg, R., & Garg, N. (2015). Developing secured biometric payments model using Tokenization. In Soft Computing. Axel Springer SE. https://doi.org/10.1109/icscti.2015.7489549
[12] Bharti S. Yerne, Fazeel.I.Z.Qureshi “Design 3D Password with session based technique for login security in Smartphone”(2016)
[13] Praveen Kumar Singh, Neeraj Kumar and Bineet Kumar Gupta “A survey on biometric fingerprints: The cardless payment system” 2019
[14] Lee, Mun-Kyu & Kim, Jin Bok & Franklin, Matthew. (2015). 3DPIN: Enhancing security with 3D display. 2014 IEEE 3rd Global Conference on Consumer Electronics, GCCE 2014. 129-130. 10.1109/GCCE.2014.7031090.
[15] “False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics” Danny Thakkar biometric technology, biometric terminology, biometrics comparison
[16] Pornpanomchai, C., & Phaisitkulwiwat, A. (2010). Fingerprint Recognition by Euclidean Distance. 2010 Second International Conference on Computer and Network Technology. doi:10.1109/iccnt.2010.100
[17] Shi-Qi Wang , Jing-Ya Wang , Yong-Zhen Lia, “The Web Security Password Authentication based the SingleBlock Hash Function” 2013
[18] A. K. Jain, S. Prabhakar, and S. Pankanti, "On the similarity of identical twin fingerprints" 2002