www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 12 Issue 01, January 2023, Page No.25633-25640
ISSN: 2319-7242 DOI: 10.18535/ijecs/v11i01.4671

A Multi-Factor Biometric Authentication Framework to User for Securing Digital Transaction

A.K. Panpatte#1
(Research Scholar)
#School of Computational Sciences,
Swami Ramanand Teerth Marathwada University, Nanded, Maharashtra, India.
Dr. S.D. Khamitkar#2
(Professor)
#School of Computational Sciences,
Swami Ramanand Teerth Marathwada University, Nanded, Maharashtra, India.
Dr. H.S. Fadewar#3
(Assist. Professor)
#School of Computational Sciences,
Swami Ramanand Teerth Marathwada University, Nanded, Maharashtra, India.

Abstract— The recent growth of digital transactions over the internet is high. This is the newest topic which is to be implemented as well as need to study related with the security. The development of technology we need to improve and build the safe authentication scheme over the internet. The safe authentication scheme is protecting the user valuable information against security threats. While performing digital transactions over the internet, the protection is turn into high importance and demand for authentication is more necessary than before. In the traditional authentication there are so many problems such as username, password & so on. Also, intruders will crack various ways of hacking user information, passwords including brute force attack, shoulder surfing, dictionary attacks, etc.

This paper is useful to performing a secure authentication scheme using different fusion techniques for digital transactions. The propose system approach here combines user details as like user name, password, OTP and biometrics (traits as like fingerprint, face & iris) fusion verification for a more valid user authentication. Our proposed point of view has been initiating to improve security benefits for various forms of invasion & authentication layers turn on password-based attacks.

Keywords— Single, two, Multi-factor authentication, Digital transaction, biometric fusion, security

INTRODUCTION:

In the digital world, people are regularly performed different digital transactions over the internet. These interchanges are frequently virtual economical instruments. Due to its big position in the current worldwide trade, digital transaction system has acquired significant attention in the last two decades. The users generally need username, password and OTP (One Time Password) for authentication to system for the digital transaction but their credential is easily susceptible to various online attacks [9 & 10]. The various organizations are using the SMS service for authentication, it initiates with the identification codes when the user performing the financial transaction that time required phone number to perform different kinds of authentication process, while this is one of the good authentications and it comes under the one-factor authentication. But recently this phone authentication is obtained by illegal methods that is comes under telecommunication fraud [1-2].

Therefore, the two-factor verification approach of system or user is still insecure [3]. Now a days the biometric identification system is implemented in the various digital or electronic transaction while performing payment. The biometric system consists different features that were special and hard to duplicate as well as never lost in digital transaction [11]. The single factor authentication system has no longer authentication [13], that's why we recommend to implement the multimodal biometric system in the various authentication mechanism with digital transactions that will giving enough guarantee to protect the user information. Therefore, the existing system which is currently in working with the digital transaction need to adopted multi-factor authentication mechanism to improve as well as increase the security of digital transaction or electronic payment system. This research paper is in five parts. The first part is introduction of digital transaction and related study of authentication framework and payment system which is already discussed. In the second part, we cover the review of existing research work in this area and elaborate with the proposed idea and need to find out the research gap in the following section. The third part is on the proposed methodology, that focused on the ideas of system with the fusion of different biometric traits. The fourth part is the discussion & analysis the existing system with the proposed model that deeply examines it. Finally, the conclusion is determining the whole research idea of this paper in section five.

LITERATURE REVIEW

To protect the digital transactions through different authentication methods were developed to establish the security, till there are no. of ways of digital transactions authentications are used. But now a days, the sensitive information is stored on internet or virtually [12]. The verification pattern that provides their users details as like username and password more than a secure interconnection used by several websites over the internet. The user's name is used to find out the users online account that means it knowing that what kind of account used by user although the password is confirming the identity of user. However, it seems secure in concept several passwords even now wind up being affected [13] & [16]. To stop this kind of password attacks the two-factor authentication considered to solving and securing digital transactions. And it also recognizing the individual and giving access to the system. The authentication of any system using password that bother no. of different safety problems. But user desire to select password which is easily remember at well as easily recognize and the same password for multiple accounts and it can store on their system [9]. Therefore, intruders test different method to hack or steal password [10] such as snooping, social engineering [14], sniffing etc.

Authors	Approach	Observation	Issue or Complication
Abhishek Arvind, Pradyumna Mahajan, and Rishikesh Chalke [4]	Password & Time-based OTP	In this study password & time-based OTP is used for authentication.	In this many securities related issue occurred. Password is stolen or break by intruder in many ways, known as password-based attack.
J.Santos,M.Antunes,J.Mangana,P.Santos&J.Casal [5]	Email & Password	This study performs the security testing platform for mobile wallet, named as "weWallet", in this testing is performed using wireless communication technology, mobile wallet software and the cloud framework.	This approach also comes under the single factor authentication as email and password scheme is highly at risk to operate. This method is also forgot, shared and stolen.
E.Benli,A.Ulak& S. Bahtiyar [6]	Password & Fingerprint	In this research work biometric trait is used for authentication the system for digital wallet. In this user is primarily	First few steps user is allowed to use the system by default. During these steps, user can conduct the

		register their biometric credential on the database & then it is authenticated by the system. The advantage of proposed system has recovery mechanism that means if user lost his phone, then it also recovers the data or credential.	number of transactions without their identity being approved. Therefore, it could be unsafe and occurred different kinds of fraud.
D. S. Islamiati, D. Agata, and A. R. Anom Besari [7]	Username & Password	This research work is measuring the payment system efficiency in ten days for users (It is performed using mobile app, web server & E-commerce application). It shows that the system is performing payment of user and it is tested.	This approach comes under the single factor authentication as username & password scheme is highly at risk to operate, this method is prone to password-based attacks and thus it is not useful to user. It can forget, shared and stolen.

Table 1: - Related Work

To avoid different kinds of password-based attacks at the authentication methods, the two-factor authentication method is granting the alternative method to secure digital transaction as well as identifying the system. The use of two-factor authentication will largely reduce the fraud but the fraud is not fully relieved [16]. When we use two-factor authentication method it extremely needs various tokens such as copying the information, cost & shed [18] that makes suspected. In the multifactor authentication system is a secure system that users can easily transfer through various authentication standards. In this, users are appeal to giving the minimal information and use the minimum three valid simple authentication [17] & [25] factors and that helps to make it difficult to any intruder to invalid the identity of the genuine user.

PROPOSED METHODOLOGY:

The proposed scheme is divided into three phases named as Login phase, Verification phase & Transaction phase. This proposed methodology is established for system application using three-factor authentication grouping namely as traditional login details (username and password), biometric fingerprint and face. The figure 1. Describe each step-in detail.

The user must register with their login details during first phase i.e., login phase before using the system. The verification is initiate to recognize the user's information which is entered by user. And the payment or financial transactions are exchanged via transaction phase. The three phases during the proposed methodology, the technique is completed with the system and the complete process flowchart is reviewed.

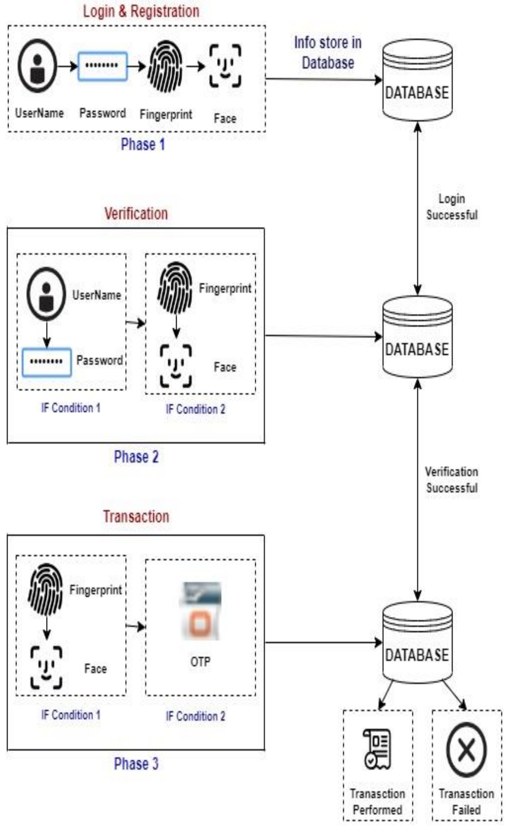


Fig: - A framework of Proposed Methodology

- **Login Phase: -**

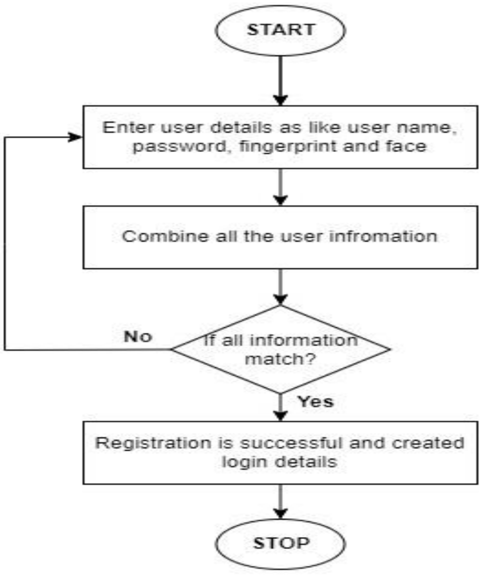
To access the system, firstly the user needs to register on the system by providing user details. Then user login the system by entering details, after that the server test the user whether it is a valid person or not. The following figure show the proposed pseudocode of the login phase with the user registration.

Login Phase

```
1) Start the registration or user on the system
2) Initialize the system
3) Enter valid details of user
4) Generating the login details as like user
   name & password
5) Login the system with these details
6) If condition is initiated and check
7) If condition match?
     Access to the system
8) Else
     Error message & Exit
9) END
```

Fig – The pseudocode of Login Phase

Fig: - Flow chart of login Phase Proposed Method


START
Enter user details as like user name, password, fingerprint and face
Combine all the user infromation
No
If all information match?
Yes
Registration is successful and created login details
STOP

- **Verification Phase: -**

In this phase, the user is verified by the verification server of system if the user details are true then it successfully authenticates by the system and give privileges to access the system. In the verification phase user must enter login detail with approved password, fingerprint and face or other combination of biometric trait to verification of the user and after the login in to the process, the person can able to access the account. The following figure shows two proposed verification pseudocode and flowchart.

Verification Phase

```
1) Start the verification of the user
2) Enter user password
   IF password match? Then
       Go to step 3
   ELSE go to step 1
3) Enter user fingerprint and face
4) Compare with the existing information
5) IF Fingerprint + Face match?
       Go to step 6
 ELSE go to step 2
6) Verification successful and ready for digital
   transaction
ELSE   Unsuccessful and Go to step 4
7) END
```

Fig – The pseudocode of verification phase proposed method

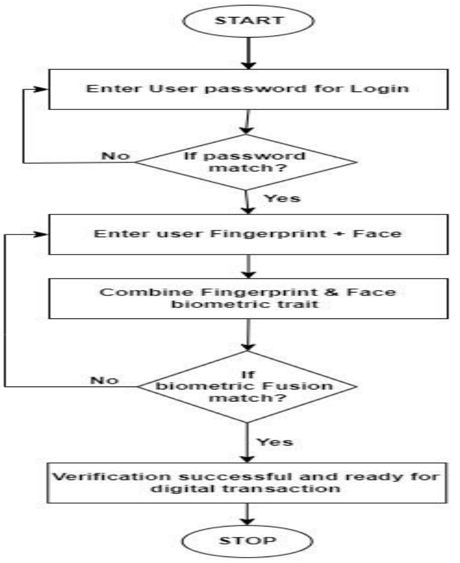

START
Enter User password for Login
No
If password match?
Yes
Enter user Fingerprint + Face
Combine Fingerprint & Face biometric trait
No
If biometric Fusion match?
Yes
Verification successful and ready for digital transaction
STOP

Fig: - Flow chart of verification Phase Proposed Method

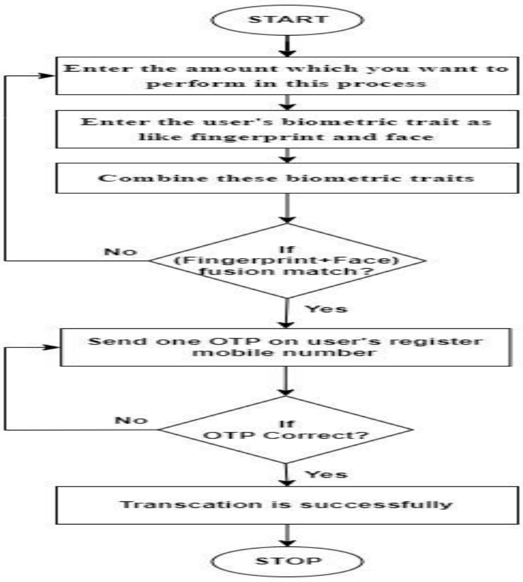
- **Transaction Phase: -**

In this phase the actual money transfer is done. This phase is authenticating the secure transaction of user with biometric trait authentication is performed. After successfully authenticate the user, the transaction process is concluded and sending one OTP (One time Password) to the user's register mobile number. The following figure shows the pseudocode and flowchart of transaction phase.

Transaction Phase

```
    1) Start the transaction phase
    2) Enter the amount which you want to perform in this process
    3) Enter the user's biometric trait as like fingerprint and face
    4) Combine these biometric trait
    5) IF Fingerprint + Face biometric trait fusion is match then Go to step 6
ELSE Go to step 2
    6) Send one OTP (One time Password) on user's register mobile number
    7) IF OTP Correct? Go to step 8
ELSE go to step 6
    8) Transaction is performed successfully
ELSE Unsuccessful and Go to step 6
    9) END
```

Fig – The pseudo code of transaction phase proposed method



START
Enter the amount which you want to perform in this process
Enter the user's biometric trait as like fingerprint and face
Combine these biometric traits
No
If (Fingerprint+Face) fusion match?
Yes
Send one OTP on user's register mobile number
No
If OTP Correct?
Yes
Transcation is successfully
STOP

Fig: - Flow chart of transaction phase proposed method

DISCUSSION:

In the digital world, the financial transactions i.e., electronic payment is an important part of digital transaction that mainly used in E-commerce business world over the Internet. There is huge research interest on digital transactions in literature – electronic payment system, e-wallet and related studies. Hence so many authentications method is find out to protect the digital transaction over the Internet. Therefore, the comparison is performed with the existence application of authentication mechanism of system which are used regularly. In the proposed system the user's important information is stored in system securely. Before, there is single-factor authentication system is used for authentication purpose but here we use in proposed system i.e., three-factor or multi-factor authentication system with the biometric fusion, that gives us effective techniques for issuing good security to the system.

Ref	**Verification Type**	**Attacks**				
		Password	**Password Guising**	**Brute force**	**Dictionary**	**Phishing**
[5]	Single-Factor	YES	YES	YES	YES	YES
[8]	Single-Factor	YES	YES	YES	YES	YES
[7]	Single-Factor	YES	YES	YES	YES	YES
[6]	Two-Factor	NO	YES	NO	NO	YES
Proposed sys.	Multi-Factor	NO	NO	NO	NO	NO

Table 2: - Analysis of proposed system with the existing systems.

CONCLUSION:

The proposed system is used the multi-factor or three-factor authentication mechanism to authorize the user and it can securely authorization of users. In this, it recognizes the username, password, fingerprint, face and OTP (one time password). It enhances the authentication method in proposed system as compare to existing system. In our proposed framework we use multi-factor authentication section to verify user during phase 2 i.e., Table 3 shows that the proposed system gives better protection strength in terms of authorization compared with the existing scheme. This multi-factor scheme is providing the protection as well as confidence to perform secure digital transaction over the internet

REFERENCES:

1) V. Khattri and D. K. Singh, “Implementation of an Additional Factor for Secure Authentication in Online Transactions,” J. Organ. Comput. Electron. Commer., vol. 29, no. 4, pp. 258–273, 2019.
2) Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-Factor Authentication: A Survey,” Cryptography, vol. 2, no. 1, p. 1, 2018.
3) Mohammed and Yassin, “Efficient and Flexible Multi-Factor Authentication Protocol Based on Fuzzy Extractor of Administrator’s Fingerprint and Smart Mobile Device,” Cryptography, vol. 3, no. 3, p. 24, 2019.
4) Abhishek Arvind, Pradyumna Mahajan, and Rishikesh Chalke, “TOTP Based Authentication Using QR Code For Gateway Entry System,” Int. J. Eng. Comput. Sci., vol. 9, no. 05, pp. 25023–25028, 2020.
5) J. Santos, M. Antunes, J. Mangana, D. Monteiro, P. Santos, and J. Casal, “Security testing framework for a novel mobile wallet ecosystem,” Proc. - 9th Int. Conf. Comput. Intell. Commun. Networks, CICN 2017, vol. 2018–Janua, pp. 153–160, 2018.
6) E. Benli, I. Engin, C. Giousouf, M. A. Ulak, and S. Bahtiyar, “BioWallet: A Biometric Digital Wallet,” Twelfth Int. Conf. Syst. (Icons 2017), no. April 2017, pp. 38–41, 2017.
7) D. S. Islamiati, D. Agata, and A. R. AnomBesari, “Design and Implementation of Various Payment System for Product Transaction in Mobile Application,” IES 2019 - Int. Electron. Symp. Role Techno-Intelligence Creat. an Open Energy Syst. Towar. Energy Democr. Proc., pp. 287–292, 2019.
8) N. Abu Bakar, S. Rosbi, and K. Uzaki, “E-Wallet Transactional Framework for Digital Economy: A Perspective from Islamic Financial Engineering,” Int. J. Manag. Sci. Bus. Adm., vol. 6, no. 3, pp. 50–57, 2020.
9) O. S. Okpara and G. Bekaroo, “Cam-Wallet: Fingerprint-based authentication in M-wallets using embedded cameras,” IEEE Int. Conf. Environ. Electr. Eng., 2017.
10) O. Alsayed and A. L. Bilgrami, “E-Banking Security: Internet Hacking, , Analysis and Prevention of Fraudulent Activities,” Int. J. Emerg. Technol. Adv. Eng., vol. 7, no. 1, pp. 109–115, 2017.
11) O. Ogbanufe and D. J. Kim, “Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment,” Decis. Support Syst., vol. 106, pp. 1–14, 2018.
12) P. Aigbe and J. Akpojaro, “Analysis of Security Issues in Electronic Payment Systems,” Int. J. Comput. Appl., vol. 108, no. 10, pp. 10–14, 2014.E. Huseynov and J.-M. Seigneur, Context-Aware Multifactor Authentication Survey. Elsevier Inc., 2017.
13) O. Alsayed and A. L. Bilgrami, “E-Banking Security: Internet Hacking, , Analysis and Prevention of Fraudulent Activities,” Int. J. Emerg. Technol. Adv. Eng., vol. 7, no. 1, pp. 109–115, 2017.

14) J. Gualdoni, A. Kurtz, I. Myzyri, M. Wheeler, and S. Rizvi, "Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor

Authentication," Procedia Comput. Sci., vol. 114, pp. 93–99, 2017.C

15) J. Gualdoni, A. Kurtz, I. Myzyri, M. Wheeler, and S. Rizvi, "Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication," Procedia Comput. Sci., vol. 114, pp. 93–99, 2017.B
16) V. Khattri and D. K. Singh, "Implementation of an Additional Factor for Secure Authentication in Online Transactions," J. Organ. Comput. Electron. Commer., vol. 29, no. 4, pp. 258–273, 2019.
17) E. E. Nwabueze, I. Obioha, and O. Onuoha, "Enhancing Multi-Factor Authentication in Modern Computing," Commun. Netw., vol. 09, no. 03, pp. 172–178, 2017M. Harish, R. Karthick, R. M. Rajan, and V. Vetriselvi, A New Approach to Securing Online Transactions—The Smart Wallet, vol. 500, no. January. Springer Singapore, 2019.
18) Rancha and P. Singh, "Issues and Challenges of Electronic Payment Systems," Int. J. Res. Manag. Pharmacy (IJRMP), vol. 2, no. 9, pp. 25–30, 2013.1
19) R. Mohan and N. Partheeban, "Secure Multimodal Mobile Authentication Using One Time Password," Int. J. Recent Technol. Eng., vol. 1, no. 1, pp. 131–136, 2014.2
20) Mohammed and Yassin, "Efficient and Flexible Multi-Factor Authentication Protocol Based on Fuzzy Extractor of Administrator's Fingerprint and Smart Mobile Device," Cryptography, vol. 3, no. 3, p. 24, 2019.V. Shukla, A. Chaturvedi, and N. Srivastava, "A new one-time password mechanism for client-server applications," J. Discret. Math. Sci. Cryptogr., vol. 22, no. 8, pp. 1393–1406, 2019.5
21) K. A. Taher, T. Nahar, and S. A. Hossain, "Enhanced cryptocurrency security by time-based token multi-factor authentication algorithm," 1st Int. Conf. Robot. Electr. Signal Process. Tech. ICREST 2019, pp. 308–312, 2019.C. A. Soare, "Internet Banking Two-Factor Authentication using Smartphones," J. Mobile, Embed. Distrib. Syst., vol. 4, no. 1, pp. 12–18, 2012.
22) Hassan, Z. Shukur, and M. K. Hasan, "An Improved Time-Based One Time Password Authentication Framework for Electronic Payments," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 11, pp. 359–366, 2020.
23) S. F. Tan and A. Samsudin, "Enhanced Security of Internet Banking Authentication with EXtended Honey Encryption (XHE) Scheme," pp. 201–216, 2018.
24) N. Yildirim and A. Varol, "A research on security vulnerabilities in online and mobile banking systems," 7th Int. Symp. Digit. Forensics Secur. ISDFS 2019, pp. 1–5, 2019.
25) M. Harish, R. Karthick, R. M. Rajan, and V. Vetriselvi, A New Approach to Securing Online Transactions—The Smart Wallet, vol. 500, no. January. Springer Singapore, 2019.