Received: March 22, 2023. Revised: April 9, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Online Financial Transactions in India: A Study of Its - Significance, Frauds and Security Models to Counter Frauds

Md. Irshad Hussain B.[1]* **Mohamed Rafi[2]**

[1]*Department of Master of Computer Applications,*
University BDT College of Engineering, A Constituent College of Visvesvaraya Technological University, India
[2]*Department of Studies in Computer Science and Engineering*
University BDT College of Engineering, A Constituent College of Visvesvaraya Technological University, India
* Corresponding author's Email: ihctdc@gmail.com

Abstract: In India, online digital transaction has become prominent means of financial transaction in everyone's day-to-day life as per reserve bank of India's (RBI) reports. Presently, Indian banks protect users' online transactions with only username and password, CAPTCHA, and dynamic 6 or 8-digit one time passwords (OTPs), which are not very secure. According to literature, this straightforward method of authentication is easily vulnerable to numerous threats. The time offered to enter the OTP with numerical pattern is more than 100 seconds, which is in defiance of RBI guidelines and can be used by fraudsters to commit fraud. In this paper we are suggesting a novel 3-Level authentication which is in-line with RBI authentication guidelines along with the authenticator assurance standards of National Institute of Standards and Technology of the United States and the European regulation for electronic payment services, for securing the users online transactions aided by username and password, OTPs and biometrics. At Level-3 user is verified with biometrics or by OTP. For biometric authentication, we have chosen facial trait, a hybrid algorithm for face detection and recognition is designed, implemented and tested on a standard dataset of VTU-BEC-DB. Suitable OTP and time constraints were identified with the implementation of proposed algorithm being tested by conducting series of trials involving 200 participants with age group of 22 to 55 years. Based on online-survey, we are suggesting for the use of fall-back authentication technique powered by security question, in-case the authentication is only on the basis of OTP. We have achieved 98.20% recognition success rate for facial recognition. The significant time to enter dynamic 6 digit OTP and dynamic 8 character alpha-numeric OTP with time limits of 45 and 60 at Level 2 and 3 is 33.82±1.10 and 45.31±0.92, respectively.

Keywords: Biometrics, Fallback authentication, Intensity equalization, Principal component analysis, Retention, Time-based one time password, Viola-Jones algorithm.

1. Introduction

The gravity of online financial transactions performed in India is more and is thought of as a replacement/alternative to the cheque system. Our extensive analysis of records pertaining to reserve bank of India (RBI) - India's central bank and regulatory organization that is in charge of overseeing the country's financial sector; and national crime records bureau (NCRB) - in charge of gathering and examining data on crime, primarily in accordance with Indian penal code (IPC), has revealed in identifying the importance, volume, and frauds associated with online digital transaction. Indian banking system constitutes of 12 public sector banks, 22 private sector banks, 43 regional rural banks, 1,484 urban cooperative banks, and 96,000 rural cooperative banks [1]. In India, the RBI and the government are attempting to reduce the economy's reliance on cash by promoting digital/payment devices, such as prepaid instruments and cards [2]. The goal of a "less cash" society is what the RBI hopes to achieve through promoting these innovative types of payment and settlement systems. India's - "Digital India" initiative, aims to

Received: March 22, 2023. Revised: April 9, 2023.

make India a nation with strong digital infrastructure [3]. With that the Indian customers' today have access to a variety of platforms that allow them to make payments electronically via cards and other means, with the help of smart devices [4].

Currently, the user is authenticated by username and password, completely automated public turing test to tell computers and humans apart (CAPTCHA – is a challenged response program that distinguishes between robot computer programmes and humans) and one time passwords (OTP) to perform transactions, which are not secure. Passwords and OTPs can be compromised. According to the RBI's annual reports over the past five years the growth in transaction volume is proportional to rise in online frauds. Online transaction fraud during the fiscal year 2021–2022 accounted for 39.50% that resulted in a loss of Rupees (Rs.) 1550 Million (i.e., 19.37 Million US Dollars). As per NCRB's most recent statistics (i.e., February 2023) accessible on the NCRB portal was up to 2021, that recorded highest OTP frauds by 61.75%.

With our work, we are proposing a multimodal based security for online transaction with 3 Levels of authentication, which follows RBI's authentication procedures and incorporate three fundamental "factors" [5] when verifying a user for online transaction - Factor 1: Anything the user is already aware of, for instance - password, PIN, etc. In our system the password satisfies the requirement of factor 1.; Factor 2: Anything that the user already possesses, such as - a credit card, a mobile phone, an ID document, ATM card, smart card, etc., in our system the use of Mobile satisfies the requirement of factor 2.; Factor 3: Something the user is, for instance - biometric characteristic, such as a fingerprint, iris, face, voice etc. In our system the authentication of the customer through Facial recognition satisfies the requirement of factor 3.

These afore said factors also satisfies the authenticator assurance standards of national institute of standards and technology (NIST) of the united states second payment services directive (PSD2), of the European regulation for electronic payment services.

At Level 1 the users are authenticated with their registered username and password, the password is encrypted with strong hashing technique. At Level 2 user is verified with the Dynamic 6 Digit OTP (D6DOTP) with time constraint of 45 Seconds. At Level 3, user has to choose one of the two ways to authenticate themselves – First way by using the biometrics, where the customer is authenticated based on face recognition.

Table 1. Online transaction in India as per RBI (#11 Months data from Jan. to Nov.)

Sl. No.	**Year**	**No. of Transactions (In Billions)**	**Transacted Amount (In Trillion Dollars)**
1	2018	20.24	**19.19**
2	2019	28.38	**20.92**
3	2020	39.08	**17.08**
4	2021	67.21	**20.61**
5	2022#	86.81	**20.32**

The second way by means of OTP recognition, in this case the user is first authenticated with a security question based on a fallback authentication technique, which is then followed by a dynamic 8 character-alpha-numeric OTP (D8CANOTP). The transaction completes only after the successful verification of user at all 3 Levels. The developed application prototype, ensures a safer means of user's online transaction and we assert that the system would guarantee that the transaction is actually carried out by the authenticated user, which in turn take care of significant online transaction frauds.

2. Literature review

As per RBI, the customers are performing bulk of online banking transaction in terms of these 3 modes - national electronic fund transfer (NEFT), real time gross settlement (RTGS) and mobile transactions, the detailed analysis of RBI data reported in 59 reports [6] shows that the transactions are inflating every year, as depicted in Table 1.

With these numbers of transaction, banks are very much responsible for ensuring that the online banking services they are offering to their customers are safe digital payment systems.

The following facts were discovered after studying the previous authors' works [2, 7, 8, 9, 10, 11] in the area of online transactions and frauds: There is certainly increase in digital transaction; identified types of online transactions; high risk of identity thefts in online digital transactions; loss of phone lead to loss of transaction or lead to fraud, as most of the transaction and confidential information is present with the users mobile; availability and confidentiality(unauthorized access) are also the issues of concern; proper end-to-end encryption credentials, etc., which enabled us to identify the key challenges of online transactions.

2.1 Challenges of digital transactions

There are number of challenges that have

Table 2. Comparison of ODF vs. OTBF (to name a few forgery of cheques, stolen cheque, demand draft fraud, fraudulent loans, accounting frauds, credit card fraud, stolen payment cards, etc.,) [TFL- Total Financial Loss in Million Dollars]

Financ-ial Year	OBF	OTF	OTBF	TFL-OBF	TFL-ODF
2017-18	5916	**2059**	3857	13.69	**4.76**
2018-19	6798	**1866**	4932	8.92	**2.45**
2019-20	8703	**2677**	6026	16.12	**4.96**
2020-21	7359	**2545**	4814	14.87	**5.14**
2021-22	9103	**3596**	5507	19.37	**7.65**

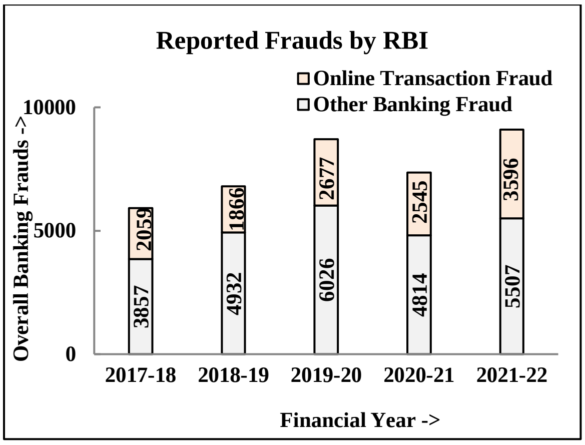


Figure. 1 Chart depicting the comparison of OTF and OBF

Table 3. Online transactions fraud recorded as per NCRB. (Credit Card/ Debit Card + Online Banking + OTP Frauds)

Year	FCR	PFC	Cases in Current Year		
			Total (C2+C3)	Dispo-sed	Pend-ing
C1	**C2**	**C3**	**C4**	**C5**	**C6**
2017	1533	626	**2159**	691	**1465**
2018	1596	1465	**3061**	1047	**2024**
2019	3009	2024	**5033**	1475	**3567**
2020	6334	3567	**9901**	2485	**7461**
2021	8475	7461	**15936**	5254	**10710**

prevailed over time in the field of online digital transactions and pose a threat to the security offered by username and password as well as the OTP. The following are some significant threats:

(i) Social Engineering attacks [11] - It can be categorized into two variations: 1) Computer based fraud - the fraudsters use the technology to trick the victim into providing the data required to impersonate the authenticated user. Phishing attack can be considered as one of the example. 2) fraud with human-interaction strategy the fraudsters get the confidential information of the victims through their interpersonal communication skill. Spoofing attack and vishing can be considered as the candidates for the human-interaction strategy to commit the fraud.

(ii) Packet Sniffing Attacks [12] - Data thefts brought on by the unauthorized access and reading of unencrypted data by capturing network traffic via packet sniffers. Eavesdropping can be considered as one of the candidate in this type. Eavesdropping refers to the possibility that an attacker will connect to or intercept a communication medium and obtain access to the data without authorization.

(iii) Password Cracking Attacks [13] - It is the term used to describe the process of recovering a lost or forgotten computer or network resource password, but the culprits use this technique to gain illegal access to the victim's credentials. Though, it is of several forms, the major forms are – a) Brute force attack, b) Rainbow attack, c) Guessing, and d) Dictionary attack.

(iv) Un-verified Mobile Applications [14] - In this attack the fraudsters dupe the victim to click the link that downloads the unverified malicious applications, through which the fraudsters gains the complete access to the victim's device and thereby to the victims sensitive information.

(v) Subscriber Identity Module (SIM) jacking [15] - In this attack the fraudster takes full access of the victims mobile transactions from the victims existing SIM to another SIM at his/her end.

(vi) SIM cloning [15]- In this attack, the fraudster using the software as a means create a duplicate SIM from the original one, thereby gains complete control of the mobile device and hence to the confidential data.

2.2 Online frauds in India

The fraud analysis on basis of reports from the RBI and NCRB sources, are as follows:

2.2.1. Reserve bank of India (RBI)

As per RBI's annual reports of past five financial years, it shows that the online transaction frauds (OTF) are gradually increasing [16], which can be analyzed from the Table 2, the contribution of OTF to overall banking fraud (OBF) has increased from 34.80% (2017-18) to around 39.50% (2021-22).

The chart represented in Fig. 1 depicts there is increase in online transaction fraud in comparison to the OBF (summation of OTBF and OTF).

Received: March 22, 2023. Revised: April 9, 2023.

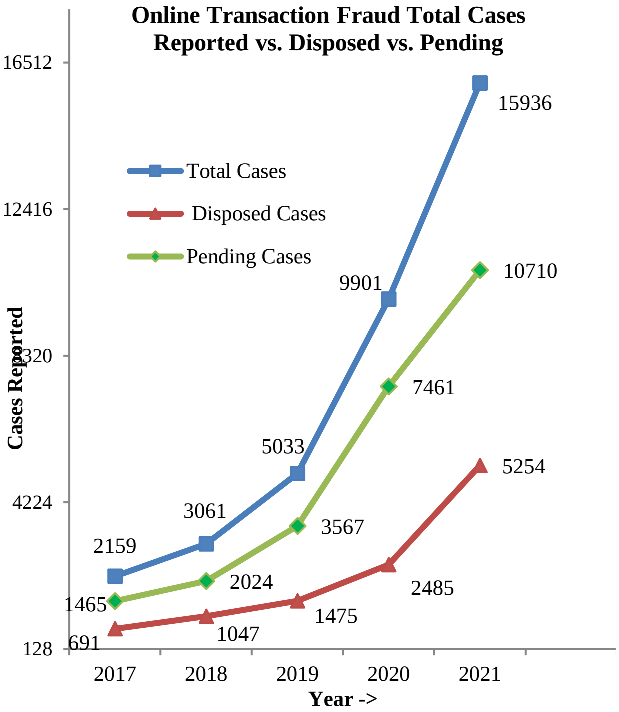


Figure. 2 Chart representing the cases reported against online digital transaction frauds as per NCRB

Table 4. No. of OTP frauds recorded in past 5 years

Year	FCR	PFC	Cases in Current Year		
			Total (C2+C3)	Dispo-sed	Pend-ing
C1	C2	C3	C4	C5	C6
2017	334	106	**440**	174	**266**
2018	319	266	**585**	210	**376**
2019	549	376	**925**	309	**621**
2020	1093	621	**1714**	497	**1217**
2021	2028	1217	**3245**	1168	**2080**

2.2.2. National crime records bureau (NCRB)

(a) Online frauds reported

As per the NCRB data the online fraud in India is increasing every year, as represented by the following Table 3 and Fig. 2. One can infer that the cases reported by NCRB in terms of online digital fraud are increasing every year.

From the Table 3, total online transaction fraud cases in current years (C4) are the sum of fresh cases recorded (FCR - C2) in current year and the pending fraud cases (PFC - C3) of previous year.

(b) OTP frauds in online transactions

To overcome online transaction frauds most of the existing systems are adopting a two-factor authentication (TFA) concept to authorize an authenticated user. The literature survey we did, pointed out that the OTP is one of the suitable way to perform TFA and, almost every platform that supports online transactions is ultimately using OTP to authenticate and complete a transaction. But, as per the NCRB [17] reports there are significant OTP frauds recorded in online transaction frauds as depicted in the Table 4 and Fig. 3.

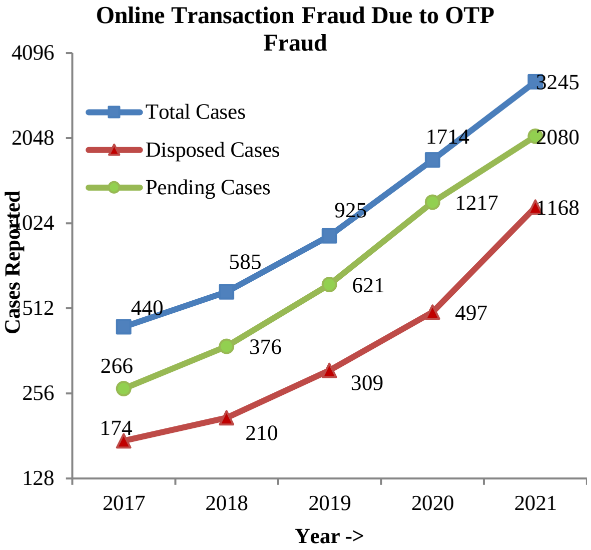


Figure. 3 Chart representing total No. of OTP frauds recorded in 5 years

From the Table 4, total OTP fraud cases recorded in current years (C4) is the sum of fresh OTP fraud cases recorded (C2) in current year and the pending OTP fraud cases (C3) of previous year. The total cases against OTP frauds reported were 61.75% more than the previous year.

From Tables 3 and 4, one can observe that the total cases are increasing in constant rate but the disposals of cases are not at the same rate.

With the study we have identified the gravity of the online transactions, various challenges associated with it and OTP fraud as a major threat. To counter this OTP fraud we are proposing the Time-based OTP (TOTP) with suitable OTP pattern and time frame for the OTP. We are suggesting two TOTP's that are best suited for two different levels to authenticate a user, along with a fallback mechanism of secured question at the final level to perform secured transaction.

2.2.3. Face recognition as a biometric

The automated ways of identifying people based on their physiological and/or behavioral traits are known as biometrics [18]. Comparison of some prominent Biometric traits [19, 20] are made in Table 5.

Received: March 22, 2023. Revised: April 9, 2023.

Table 5. Comparison of biometric traits [H – High, M – Medium, L – Low, VH-Very High]

Popular Biometric Traits	Parameters			
	Ease of Use	Accu-racy	User Acceptance	Cost
Fingerprint	H	H	M	M
Face	H	H	H	M
Voice	H	M	H	M
Signature	H	L	H	M
Retina	L	VH	L	H
Iris	M	VH	L	H
Palmprint	H	M	H	L
Gait	H	M	L	L

For comparison on popular biometric traits, we have considered four parameters – ease of use by the user, accuracy in recognition, user acceptance and the cost of implementation. From Table 5, in terms of accuracy the retina and iris traits are highly accurate in recognizing an individual but have a poor user acceptance and the implementation is high. The palmprint and gait traits bear low implementation cost but the accuracy of both the traits is medium; ease of use is high for both traits; the user acceptance is high for palmprint but low form gait trait. Like this when we we compared all the traits we found that the use of Face as biometric trait is more suitable as out of four parameters only the cost of implementation is medium, but ease of use, accuracy and user acceptance are high. Hence we are proposing to use the face as biometric at Level 3 to authenticate an individual.

The following are some earlier authors' works in facial recognition:

Borkar et'al [21]: They have used principal component analysis (PCA) and linear discriminant analysis (LDA) to recognize an individual. They have used AT&T face dataset, that consists of 40 subjects and claim a recognition rate of 97.00%.

Al-Ghrairi et'al [22]: In their work, for face detection they have used Viola-Jones algorithm (V-JA) and PCA to recognize an individual. They have used file exchange interface (FEI) databases dataset with sample size of 35 individuals and claim an accuracy of 96.00%.

Siswanto et'al [23]: In their approach they have used PCA to recognize an individual, they have used proprietary dataset and claim an recognition rate of 90.00%.

Asha et'al [24]: In their work they have used PCA to extract features from the source images and have used artificial firefly swarm optimization technique(AFSOT) for matching the query image with source image. They have used their own proprietary dataset with sample size of 90 subjects and claim an accuracy of 80.60%.

Rama et'al [25]: They have used PCA to recognize an individual. They have used AR dataset with sample size of 136 subjects and claim an accuracy of 80.00%.

Sharmila et'al [26]: They have used PCA and linear binary pattern histograms (LBPH) to recognize and individual. They have proprietary dataset and claim a recognition rate of 70.00%.

3. Proposed system

We are proposing a system that enhances the security feature in online digital financial transactions. In our proposal we are authenticates a user at multiple levels, as shown in Fig. 4, which is a flow chart representing the proposed system.

At Level 1 the users are authenticated with their registered username and password. The password is encrypted with strong hashing algorithm. If the users fail to validate themselves then they are given two more chance to verify themselves as authenticated users. Once the users are verified as authenticated user, then the user can select the beneficiary from the list of beneficiary to whom they wish to transfer the amount. If suppose the beneficiary is not in the list, the user can add up the beneficiary and exit the process of amount transfer and wait for the bank verify and respond. If beneficiary is already in the list then the user can enter into Level 2 of authentication.

At Level 2 the user has to raise a request for a D6DOTP from bank server, on receiving the OTP the user has to enter the exact OTP within a time frame of 45 seconds, if not the user will be given 2 more chances to prove themselves as the authenticated user. On successful entry of the right OTP within 45 seconds marks the passing of Level 2 of authentication. Then the users need to enter the amount they want to transfer to the beneficiary, once the amount is entered the balance is verified by the bank server, if the balance is sufficient then the users will be taken to the Level 3 authentication.

At Level 3, they will be presented with two ways to authenticate themseslves, out of wihich user has to choose one method, as shown in Fig. 5.

3.1 Level 3 authentication with face biometrics

At Level 3, one of the way for user to authenticate is to use face biometrics. We have proposed a hybrid algorithm that uses Viola-Jones algorithm [27] for face detection and principal

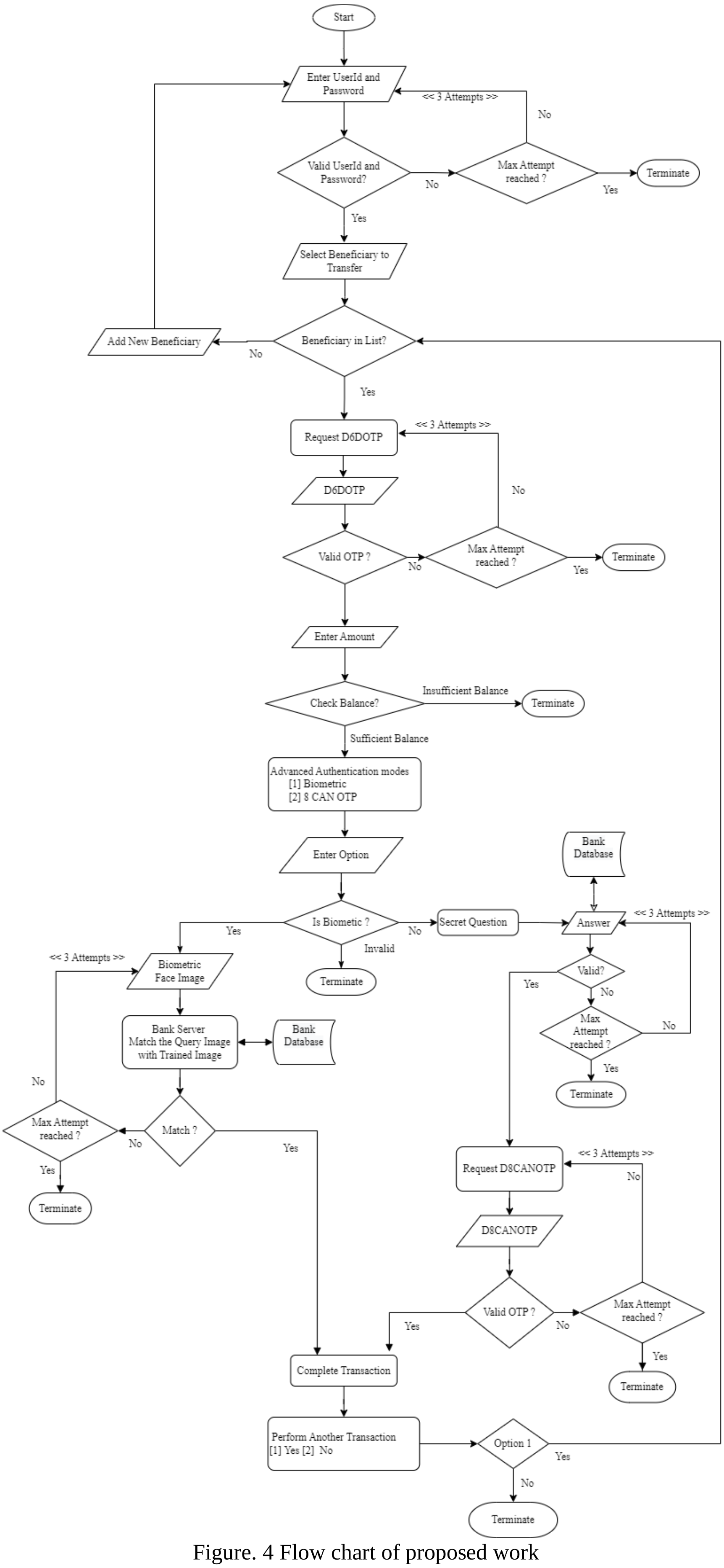
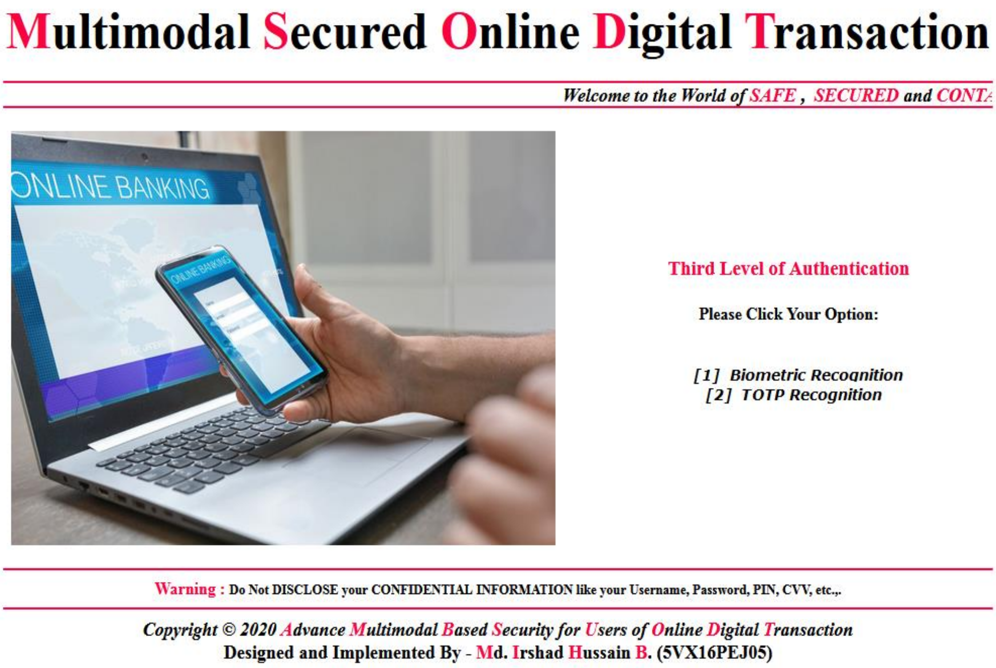


Figure. 4 Flow chart of proposed work

Received: March 22, 2023. Revised: April 9, 2023.



Multimodal Secured Online Digital Transaction

Welcome to the World of SAFE , SECURED and CONT

Third Level of Authentication

Please Click Your Option:

[1] Biometric Recognition
[2] TOTP Recognition

Warning : Do Not DISCLOSE your CONFIDENTIAL INFORMATION like your Username, Password, PIN, CVV, etc.,.

Copyright © 2020 Advance Multimodal Based Security for Users of Online Digital Transaction
Designed and Implemented By - Md. Irshad Hussain B. (5VX16PEJ05)

Figure. 5 Level 3 Authentication with two choices for user

componenet analysis algorithm [28] for face recognition, in between these two we have included a intermediary step of intensity equalization.

Algorithm for face detection and recognition

```
Step 1: Get the Source image $s(x,y)$
Step 2: Convert the Source image $s(x,y)$ to Gray scale image $g(x,y)$
Step 3: Apply Viola-Jones Algorithm to image $g(x,y)$.
If Face is detected in the source image
    Extract the Face image $e(x,y)$ from $g(x,y)$.
Else
    Exit
Step 4: Change the dimension of image $e(x,y)$ from $M \times N$ to $N \times N$ forming $f(x,y)$
Step 5: Apply Intensity Equalization to $f(x,y)$
• Divide the image $f(x,y)$ into sub-regions

  $f(x,y) = \sum_{i=1}^{n} f_1(x,y), f_2(x,y), \dots\dots\dots\dots, f_n(x,y)$   (1)
  Where, $f_i(x,y)$ a sub-region of $f(x,y)$

• Apply Histogram stretching for each region to equalize the intensity

  $H = Ƕ(f_i(x,y))$   (2)
  Where, Ƕ is the histogram function
• Join the sub-regions $f_i(x,y)$ to form $f(x,y)$
  $f(x,y) = \bigcup_{i=1}^{n} f_1(x,y), f_2(x,y), .., f_n(x,y)$   (3)
Step 6: Apply Principal Component Analysis to $f(x,y)$ to recognize the image

If a Match is found between image $f(x,y)$ and trained image, then
    Image is Recognized
Else
    Image is NOT Recognized
```

In this approach, the source image $s(x,y)$ will be the aquired image, this acquired image is pre-processesed by converting the image into a gray scale image $g(x,y)$. The obtained image $g(x,y)$ is subjected to Viola-Jones algorithm, which is used to detect objects in the image, in our case the object is the face that has to be detected. If the face is detected in the image then it is extracted forming the image $e(x,y)$ and passed to intermediate step otherwise the process is terminated. If the image is detected then in the next step the facial part is extratced from the image $e(x,y)$, and the dimension is set from $M \times N$ to $N \times N$ dimension, forming image $f(x,y)$. Then the face image $f(x,y)$ subjected to intensity equalization.

During intensity equalization, the face image $f(x,y)$ is first disintegrated into sub-regions ($f_1(x,y)$, $f_2(x,y)..f_n(x,y)$). Then, each sub-region is subjected to histogram stretching using histogram function $Ƕ(f_i(x,y))$ to equalize the intensity. Finally, when equalization of all sub-regions is performed then all the subregions $(f_1(x,y), f_2(x,y)..f_n(x,y))$ are joined to form the face image $f(x, y)$.

For face recognition, the image $f(x, y)$ is subjected to principal component analysis algorithm, where image $f(x, y)$ is compared with the trained images if a match is found, leads to successful image recognition otherwise mark the failure of image recognition.

Using an Intel Core i5-2540M processor clocked at 2.60GHz and 4GB of RAM, the system was developed using MATLAB R2016b running on a 64-bit operating system platform of Windows 7. We have used Visvesvaraya Technological University's VTU-BEC-DB [29] multimodal biometrics database that has 100 subjects and five orientation of each subjects, to model the system.

3.2 Level 3 authentication with secret question and OTP

In this approach the user has to identify their authenticity with a secret question based on hashed fallback authentication technique then with D8CANOTP. The secret question is framed by the users at the time of online account registration. On correct entry of the answer to the secret question, the users will be navigated to the page from where they can raise a request for D8CANOTP, on receiving the TOTP from the server. The users need to enter OTP within 60 seconds of time restriction, to successfully complete the amount transfer to the beneficiary.

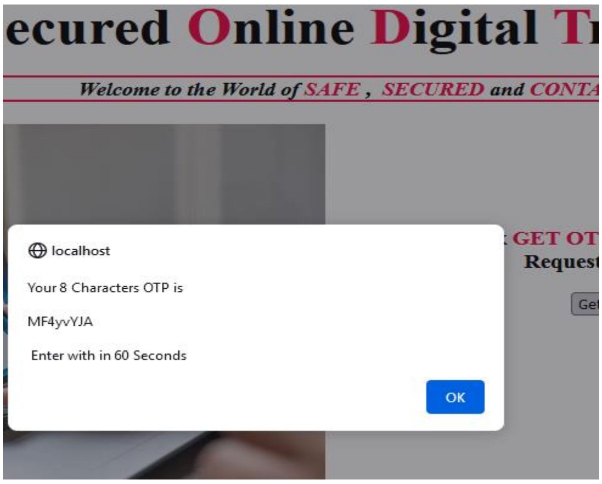
The following algorithm is used for generating a combination of different OTP pattern and time constraints on the OTP.

Algorithm: Generate pattern for OTP and time constraint

```
//I=[A-Z][0-9][a-z], OTP, l=8, generate_rand, rand_index, otp_gen _time, otp_sub_time, Year, Month, Day, Hr, Min, Secs
Step 1: Initialize I
Step 2: Find D the length of I
Step 3: Choose a character from I and add them to OTP every iterations for L times, doing so until the length is exhausted.

For c in range (1, L)
        $generate\_rand = get\ a\ vlaue$
                $between\ 0\ and\ 2^{31} - 1$
        $rand\_index = generate\_rand$ -
            $[D \times Floor(generate\_rand \div D)]$
        $OTP = substr(I, rand\_index, 1)$

Return OTP
```



Your 8 Characters OTP is

MF4yvYJA

Enter with in 60 Seconds

Figure. 6 Dynamic 8 character Alpha-Numeric OTP generation with time bound of 60 seconds (OTP Generated – "MF4yvYJA")

```
Step 4: otp_gen _time = Save the OTP generation's current date and time stamp.
Step 5: Submit OTP
Step 6: otp_sub_time = Save the OTP submission's current date and time stamp.
Step 7: Get the time difference between otp_sub_time and otp_gen _time
Step 8: Decide the Authentication based on time

If (Year = 0 and Month = 0 and Day = 0 and Hr=0 and Min = 0 and Secs <= 45)
        If Entered OTP = Submitted OTP Then
                SUCCESSFUL Authentication
        else
                Entered OTP is Invalid
        end if
else
        OTP Expired
```

The algorithm above, generates a D8CANOTP with time restrictions of 45 seconds. The same algorithm can be used to generate a D6DOTP, by setting variables I = [0-9] and L = 6; the time restriction can be varied to 30 or 60 Seconds by setting the variable "Secs" value to 30 or 60.

The technologies that we have used for experimentation are: Scripting language – PHP (Hypertext Preprocessor) 7.3.12 and JavaScript; Markup language - HTML5.0; Web server - WAMP 3.2.0; database - MySQL 5.0.12 and Style Sheet language - CSS (Cascading Style Sheets). In search of secured OTP and suitable time restriction for the OTP expiry, experiments were carried with 200 subjects with age group ranging from 22 years to 55 years. In this pursuit, algorithm was proposed that can be used to set different OTP patterns and time restriction [30]. We have carried out three

Received: March 22, 2023. Revised: April 9, 2023.

experiments in form of three tests in two phases with three trials respectively, the first experiment was with D6DOTP pattern with varying time limits, second was with D8CANOTP pattern with varying time limits and the third was in sequence authentication i.e., first the user has to enter the D6DOTP with the defined time bound at Level 2 of authentication, on successful entry of OTP within the defined time bound the user will be taken to Level 3 of authentication, where the user has to enter the D8CANOTP with specified time bound (Fig. 6), on successful entry of the OTP within specified time bound, marks the successful authentication of the user.

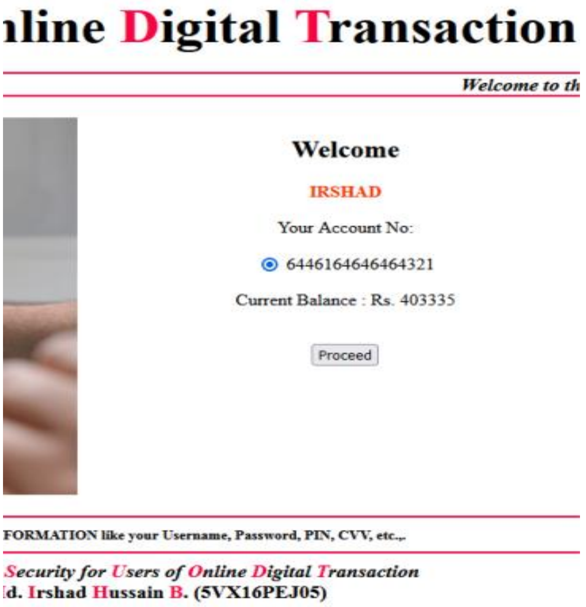
4. Results and discussion

4.1 Hashed password at Level 1

In Level 1, we are using strong hashing algorithm with random salt to encrypt the password, which further secures the online transaction from packet sniffing and variations of password cracking attacks. Even if the secured database that stores the credentials is hacked, it will be very difficult to decrypt the original password from the stored. For instance the user has assigned a password as “tiger@1”, then its hashed version stored in database will be –

“[redacted]2Mm/[redacted]7R6CVbZ[redacted]L.ljbxOs[redacted] k/b[redacted]FJ3a6l7afm[redacted]”.

After successful verification of user at Level 1, the user will be navigated to the welcome page which displays the user’s Account details as shown in Fig. 7.



ıline **Digital** **Transaction**

Welcome to th

Welcome

IRSHAD

Your Account No:

● 6446164646464321

Current Balance : Rs. 403335

FORMATION like your Username, Password, PIN, CVV, etc.,.

Security for Users of Online Digital Transaction

ḍ. Irshad Hussain B. (5VX16PEJ05)

Figure.7 Successful verification and display of account details

4.2 Identification of Suitable patterned TOTP

Each test of three trails with 200 participants whose age ranged between 22 to 55 years, for different patterns and time windows were conducted in two phases, in phase-I users have to use their retention power to remember the OTP received and has to enter within the time limit enforced to verify themselves whereas in phase-II the user can use any means to enter the received OTP within the time frame enforced.

4.2.1. With varying patterns and time window

Table 6 represents the dynamic 6 digit OTP pattern and varying time limits of 30, 45 or 60 Seconds.

Table 7 represents the time taken by the subjects to enter a dynamic 8 character Alpha-Numeric OTP - within 30, 45 0r 60 Seconds.

Table 6. Result of mean time taken with standard error (SE) for dynamic 6 digit pattern with variable time windows [PI RT – Phase-I Retention Time, PII OTRT- Phase-II Other than Retention Time]

Phase Type	**Trial 1**	**Trial 2**	**Trial 3**
	Mean ± SE	**Mean ± SE**	**Mean± SE**
Test 1: Pattern - 6 Digit and Time Window – 30 Secs.			
PI RT	18.14±0.59	**18.40±0.61**	18.28±0.52
PII OTRT	**19.66±0.55**	19.21±0.49	19.29±0.52
Test 2: Pattern - 6 Digit and Time Window – 45 Secs.			
PI RT	24.85±0.87	25.24±0.84	**25.46±0.85**
PII OTRT	26.45±0.81	**26.49±0.85**	26.11±0.87
Test 3: Pattern - 6 Digit and Time Window – 60 Secs.			
PI RT	**32.75±1.16**	32.02±1.13	31.97±1.15
PII OTRT	**33.82±1.10**	33.40±1.09	32.77±1.09

4.2.2. Sequential experiment

After the experimentation of different patterns at different time intervals, another experiment was carried where a randomly generated 6 digit OTP with different time window was used at Level 2 and challenge based 8 character lengths Alpha-Numeric OTP with different time windows were used at Level 3. In this experimentation the users have to successively enter the OTP for both levels in succession to authenticate themselves, the time taken is depicted in Table 8.

Table 7. Result of mean time taken by 200 subjects for dynamic 8 character Alpha-Numeric pattern with variable time windows

Phase Type	Trial 1	Trial 2	Trial 3
	Mean ± SE	**Mean ± SE**	**Mean± SE**
Test 1: Pattern – 8 Character Alpha-Numeric OTP and Time - 30 Seconds.			
PI RT	25.39±0.53	27.50±0.81	**27.91±0.82**
PII OTRT	28.63±0.53	**28.76±0.46**	28.11±0.54
Test 2 : Pattern – 8 Character Alpha-Numeric OTP and Time - 45 Seconds.			
PI RT	32.95±0.76	33.19±0.75	**33.77±0.72**
PII OTRT	36.06±0.55	36.90±0.54	**38.02±0.57**
Test 3 : Pattern – 8 Character Alpha-Numeric OTP and Time - 60 Seconds.			
PI RT	42.37±0.95	**43.89±0.97**	43.60±1.04
PII OTRT	44.98±0.89	**45.31±0.92**	45.28±0.81

Table 8. Result of mean time taken by 200 subjects for authenticating with dynamic 6 digit OTP at Level 2 and dynamic 8 character Alpha-Numeric pattern OTP at Level 3 with variable time windows

Test No.	Phase Type	Trial 1	Trial 2	Trial 3
		Mean ± SE	**Mean ± E**	**Mean± SE**
Level 2 - 6 Digit OTP and Level 3 - 8 Character Alpha-numeric OTP Time Frame of 30 Seconds for each Level				
Test 1	Phase I - Retention Time			
	Level 2	19.17±0.52	**19.96±0.52**	19.28±0.53
	Level 3	20.80±0.93	**21.40±0.96**	21.30±0.93
	Phase II - Other than Retention Time			
	Level 2	20.03±0.47	**20.98±0.40**	20.26±0.40
	Level 3	22.31±0.77	22.50±0.70	**22.73±0.76**
Level 2 - 6 Digit OTP and Level 3 - 8 Character Alpha-numeric OTP Time Frame of 45 Seconds for each Level				
Test 2	Phase I - Retention Time			
	Level 2	**27.68±0.83**	27.09±0.81	27.50±0.82
	Level 3	29.06±1.05	**29.43±1.02**	29.16±0.97
	Phase II - Other than Retention Time			
	Level 2	**29.27±0.77**	28.32±0.71	27.24±0.71
	Level 3	29.75±0.86	**30.50±0.76**	29.58±0.78
Level 2 - 6 Digit OTP and Level 3 - 8 Character Alpha-numeric OTP with Time Frame of 45 and 60 Seconds				
Test 3	Phase I - Retention Time			
	Level 2	29.05±0.80	28.52±0.73	**29.29±0.74**
	Level 3	**41.74±1.16**	40.03±1.18	40.15±1.14
	Phase II - Other than Retention Time			
	Level 2	30.16±0.69	**30.31±0.66**	29.22±0.62
	Level 3	**41.14±1.09**	39.43±1.09	40.61±1.07

The observation we made was that the time taken at Level 3 in these tests was significantly less than the time consumed by the subjects in the previous study we made, it was due to the fact that some subjects failed at Level 2 itself and do not turn themselves to Level 3. Hence, we are considering Tables 6 and 7 for the identification of suitable TOTPs at different Levels, as per Table 6, the maximum time taken by the user to enter a D6DOTP was 33.82±1.10 which was more than 30 seconds but less than 45 Seconds, hence we suggest for enforcement of 45 seconds time window for D6DOTP. As per Table 7 the maximum time taken by the user to enter an D8CANOTP was 45.31±0.92, which was almost nearer to 46 seconds but less than 60 seconds, hence we suggest for the enforcement of 60 seconds time window for D8CANOTP. The total time of 105 seconds to enter the OTP at both levels almost adheres to the RBI's [5] suggestion of including a time constraint of 100 Seconds on the OTP. The user on successful verification at Level 2 is taken to the next step where the user has to choose the beneficiary to whom the amount has to be transferred. Once the user enters the amount, the amount is verified for sufficient balance, if balance is sufficient then the user is navigated to Level 3 authentication to complete the transaction.

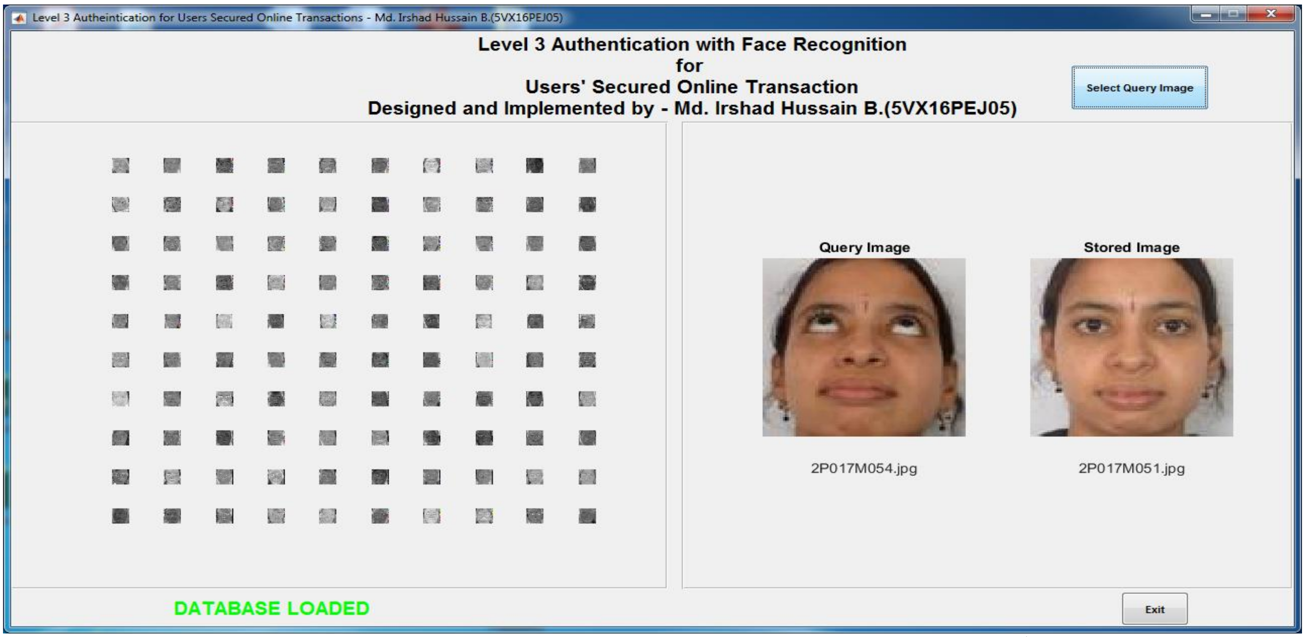
4.3 Authentication at Level 3

As said earlier, the user is authenticated in one of the two ways:

4.3.1. Facial recognition

The VTU-BEC-DB dataset consists of 100 subjects, each subject's image is captured in 5 orientations where the subject is asked to pose looking front, left, right, up and down. All the poses were captured under the controlled setup with white background. In Matlab the application is designed in such a way that, if the query image matched with the stored image than both the images are showed in sequence first the query image followed by stored image (Fig. 8), if no match is found than only query image is displayed with no match found message.

In order to compare our work to that of the previous authors, we focused on two things: first, the database should contain at least 100 subjects embedded with restrictions of at least position and lighting; second, have employed PCA for facial recognition with either one or both of them satisfied. [21, 23] has reduced image dimensionality using PCA, then the image is projected onto eigen space



Level 3 Autheintication for Users Secured Online Transactions - Md. Irshad Hussain B.(5VX16PEJ05)

Level 3 Authentication with Face Recognition
for
Users' Secured Online Transaction
Designed and Implemented by - Md. Irshad Hussain B.(5VX16PEJ05)

DATABASE LOADED

Figure. 8 Successful recognition of a subject where, the query image of the subject posing in 4th Orientation i.e., looking upwards is matched with stored image

Table 9. Comparison of previous work on face recognition using PCA for face recognition

Sl. No	Authors	Method Adopted	Face Dataset	No. of Subjects	Recognition Rate
1	**Proposed Method**	VJ-A and PCA	**VTUBEC-DB**	**100**	93.60%
		VJ-A with Intensity Equalization and PCA			**98.20%**
2	Borkar et'al [21]	PCA and LDA	AT&T	40	97.00%
3	Al-Ghrairi et'al [22]	V-JA and PCA	FEI	35	96.00%
4	Siswanto et'al [23]	PCA and LDA	Proprietary	NA*	90.00%
5	Asha et'al [24]	PCA and AFSOT	Proprietary	90	80.60%
6	Rama et'al [25]	PCA	AR	136	80.00%
7	Sharmila et'al [26]	PCA and LBPH	Proprietary	NA*	70.00%

Table 10. Face recognition with respect to VTU-BEC-DB dataset

Sl. No.	Total No. of Images	No. of Images Correctly Identified	Images Not Identified	Recognition Rate
1	500	491	09	**98.20%**

using linear discriminant analysis (LDA). [22] has used Viola-Jones algorithm for face detection and PCA for face recognition. [24] have used PCA for extraction of facial traits and for matching and decision making have used artificial firefly swarm optimization technique. [25] have used PCA for face recognition and [26] have used PCA and Linear Binary Pattern Histograms (LBPH), that uses haar cascade for face recognition. Nevertheless, [21-23, 26] utilised Euclidean distance metric for comparison of trained and query images, while in our work we have employed Mahalanobis distance metric.

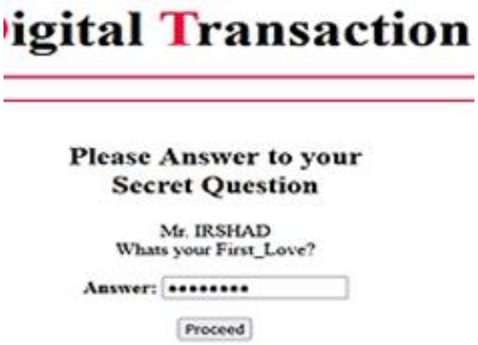
With the help of the Viola-Jones method and principal component analysis, we were able to recognize faces with a rate of 93.60%. Including an intermediate stage of intensity equalization between face detection and face recognition, we were able to get a recognition rate of 98.20%, which is high compared to current approaches as depicted in Table 9 [31].

Recognition rate(R) is calculated as follows

$$R = (\Sigma_{TIID} \div \Sigma_{TSI}) \times 100 \qquad (4)$$

Table. 11 Users confidence in application imposed secret questions (NUTSQ - No. of user trusted the secret question)

Sl. No	Security Question	NUT SQ
1	**What is your mother's maiden name?**	**62**
2	What is your favorite teacher's nickname?	31
3	Where did you meet your spouse?	16
4	What year was your father (or mother) born?	45
5	**What was your childhood nickname?**	**103**
6	What is your maternal grandmother's maiden name?	23
7	What is your preferred musical genre?	29
8	**What is the name of the first school you attended?**	**85**
9	What was the last name of your favorite teacher?	34
10	What is your favorite team?	51



Please Answer to your Secret Question

Mr. IRSHAD
Whats your First_Love?

Answer: ••••••••

Figure. 9 Secret question at Level 3 authentication

Where,

$$\sum_{TIID} = Total\ Images\ Identified\ Correctly$$
$$\sum_{TSI} = Total\ Stored\ Images$$

From Table 10, for 100 subjects with five different orientations and total number of images 500, we have attained a recognition rate of 98.20% which is higher than the state-of-art method as proposed by earlier authors in Table 9.

4.3.2. Hashed fallback authentication

One of the key methods used for fallback authentication is the usage of security questions [32] and we are proposing to use this approach for the identification of an individual at Level 3.the identification of an individual at Level 3. With the help of a study, we were able to determine the top 10 questions that are typically used as a secret question to identify an individual when a user registers across the web portals [Table 11].

To determine which among these 10 questions the user would trust the most, with the confidence that they alone know the answer. We conducted a survey with 200 Subjects with age ranging from 22 to 55Years. The subjects were asked to choice maximum of 3 security questions that they feel only they are aware of its answer, the findings of the survey are depicted in Table 11.

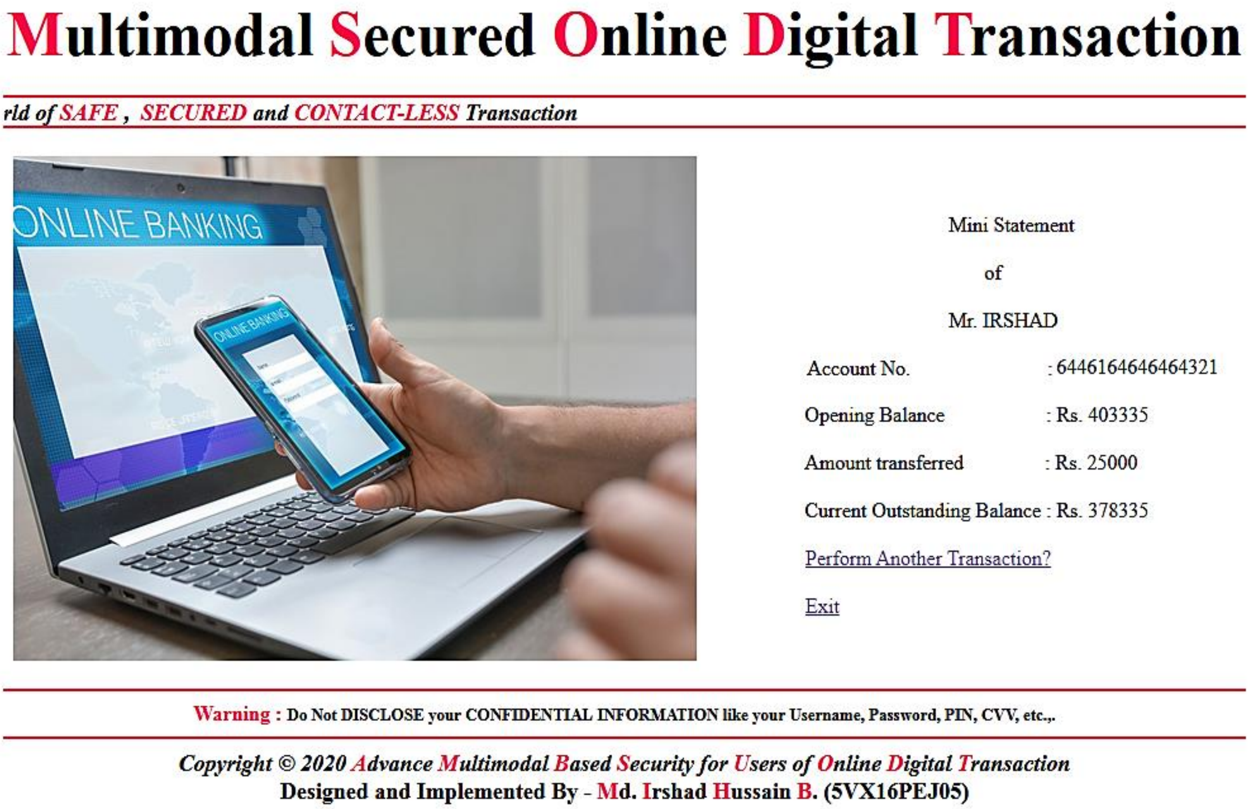
We found that secret question with serial No. 5 topped and users' had most confidence in this question followed by question at serial no. 8 and 1 respectively. However, it has been noticed that using security questions for authentication has serious usability and security issues [33], when the choice of the standard set of questions are posed in front of user. To overcome this issue, we asked the users to frame their own Security question of which only he/she is aware of. We found that most of the users had framed the different security questions which were very personal to them and we are of the opinion that nobody else were aware of the answers to those questions, to name a few questions framed by the users which we opinion that are secured are - What is your desired destination?, What is one feeling which you have not shared with anyone else in this world?, Which is your favorite animated character?, What is the strangest habit you have?, What is the aim in your life?, etc.

With that we incorporated this feature in our work and gave a free hand to the users to frame their own secret question at the time of registration of online transaction account. We also enforced hashing on the answer to secret question to provide more security. For instance the secret question by user was “What’s Your First Love?” (Fig. 9), the answer was “family”.

The answer stored in the database will be -

“[redacted]Z1pAmgTAn[redacted]Ib87/sF.[redacted]4 Futl[redacted]2WeyBDq9F[redacted]”

At Level 3, 2-step verification of user takes place. First the user will be posed with secret question, after answering it correctly the user will be taken to the second and final step of verification where the user has to enter a dynamic 8 character Alpha-Numeric OTP within 60 seconds. The successful completion of verification at Level 3, in one of the two ways discussed above is marked by execution of user’s financial transaction by transferring the amount to the beneficiary and there by displaying a Mini statement of the user account, as shown in Fig. 10.



Multimodal Secured Online Digital Transaction

rld of SAFE , SECURED and CONTACT-LESS Transaction

Mini Statement

of

Mr. IRSHAD

Account No.	: 6446164646464321
Opening Balance	: Rs. 403335
Amount transferred	: Rs. 25000
Current Outstanding Balance	: Rs. 378335

Perform Another Transaction?

Exit

Warning : Do Not DISCLOSE your CONFIDENTIAL INFORMATION like your Username, Password, PIN, CVV, etc.,.

Copyright © 2020 Advance Multimodal Based Security for Users of Online Digital Transaction

Designed and Implemented By - Md. Irshad Hussain B. (5VX16PEJ05)

Figure. 10 Completion of online transaction by transferring amount of Rs. 25,000/- (US Dollars-312) to the chosen beneficiary

The encrypted password with hashing creates secured hashes for the passwords and as well to secret question's answer [34]; this secures the user from packet sniffing and variations of password cracking attacks like brute force attack, rainbow attack and dictionary attack. The hashing will secure the credentials by encrypting them in such a way that, the stored credential will be difficult to decrypt by hackers, even if they illegally access the credentials.

5. Conclusion

We have identified the significance of online transactions in India. With the experimentations we have carried out, we are of the opinion that the online transaction frauds can be encountered with suitable OTP pattern and time restriction. Our experiments revealed that a D6DOTP with time restriction of 45 seconds is more significant at Level 2 of authentication; a D8CANOTP with time restriction of 60 seconds will enforce more security at Level 3 to authenticate a user.

The inclusion of Level 3 authentication, will verify the user by face biometrics or by hashed fallback security question and D8CANOTP. The two options provided at Level 3 ensure that the rightful user is physically performing the transaction. The recognition rate of 98.20%, achieved for facial recognition was higher than the state-of-art method proposed by earlier authors. Security question framed by the user was unique instead of the routine security question provided by the applications that can be guessed by hackers. The TOTPs ensures that the user has sufficient time to enter OTP; apart from this no one will have sufficient time to hack or steal the OTP and perform illegal transaction, and also justify the RBI's guidelines of authentication.

We suggest to use face biometrics exclusively at Level 3, however in case of biometric failures, the user can choice for the second way of authentication, which is the TOTP recognition. As our work complies with the requirements set forth by the RBI, the NIST's user authenticator standards of the United States, and PSD2 standards for the Europe, any bank in the world can be integrated with our Level 3 authentication for imposing secured online transactions.

Conflicts of interest

The authors declare no conflict of interest

Author contribution

Md. Irshad Hussain B. was responsible for the paper's conceptualization, methodology, software, validation, formal analysis, data curation, writing-original draft, writing-review and editing. The supervision and software administration have been done by Dr. Mohammed Rafi.

References

[1] The Banking Industry Report: https://www.ibef.org/industry/banking-presentation

[2] N. Ramya, D. Sivasakthi, and M. Nandhini, "Cashless transaction: Modes, advantages and disadvantages", *International Journal of Applied Research*, Vol. 3, No. 1, pp. 122-125, 2017.

[3] K. S. Vally and K. H. Divya, "A Study on Digital Payments in India with Perspective of Consumer's Adoption", *International Journal of Pure and Applied Mathematics*, Vol. 119, No. 15, pp. 1259-1267, 2018.

[4] S. Khan and S. Jain, "A Study on Usage of ePayments for Sustainable Growth of Online Business", *IOSR Journal of Business and Management*, pp. 74-81, 2018.

[5] Reserve Bank of India, Authentication Guidelines: https://www.rbi.org.in/hindi1/Upload/content/PDFs/C2292604162.pdf

[6] Reserve Bank of India: https://rbi.org.in/Scripts/NEFTView.aspx.

[7] Rachna and P Singh, "Issues and Challenges of Electronic Payment Systems", *International Journal for Research in Management and Pharmacy*, Vol. 2, No. 9, 2013.

[8] B. U. I. Khan, R. F. Olanrewaju, A. M. Baba, A. A. Langoo, and S. Assad, "A Compendious Study of Online Payment Systems: Past Developments, Present Impact, and Future Considerations", *International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 5, 2017.

[9] K. A. L. Qawasmi, M. A. L. Mousa, and M. Yousef, "Proposed E-payment Process Model to Enhance Quality of Service through Maintaining the Trust of Availability", *International Journal of Emerging Trends in Engineering Research*, Vol. 8, No. 6, 2020.

[10] M. A. Hassan, Z. Shukur, M. K. Hasan, and A. S. A. Khaleefa, "A Review on Electronic Payments Security", *Symmetry*, pp. 1-24, 2020.

[11] B. Atkins and W. Huang, "A Study of Social Engineering in Online Frauds", *Open Journal of Social Sciences*, Vol. 1, No. 3, pp. 23-32, 2013.

[12] R. Tuli, "Packet Sniffing and Sniffing Detection", *International Journal of Innovations in Engineering and Technology*, Vol. 16, No. 1, pp. 22-32, 2020.

[13] S. He, J. Fu, C. Chen, and Z. Guo, "Research on Password Cracking Technology Based on Improved Transformer", In: *Proc. of International Conf. on Artificial Intelligence and Computer Science, Journal of Physics: Conference Series*, Zhejiang, China, pp. 1-9, 2020.

[14] F. Liu, C. Wang, A. Pico, D. Yao, and G. Wang, "Measuring the Insecurity of Mobile Deep Links of Android", In: *Proc. of the 26th USENIX Security Symposium*, Vancouver, Canada, August 2017.

[15] Information Security Awareness - Sim Swapping And Sim Cloning Frauds: https://www.infosecawareness.in/

[16] Reserve Bank of India, Annual Report 2018 to 2022; https://rbidocs.rbi.org.in

[17] National Crime Records Bureau; https://ncrb.gov.in/

[18] A. Jain, R. Bolle, and S. Pamkanti, "Introduction to Biometrics," *in: A. Jain, R. Bolle, and S. Pamkanti (Eds.), Biometrics: Personal Identification in Networked Society*, pp. 1-41, 1999.

[19] K. Mali and S. Bhattacharya, "Comparative study of different biometric Features", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, No. 7, pp. 2776-2784, 2013.

[20] K. Yadav and S. K. Grewal, "A Comparative Study of Different Biometric Technologies", *International Journal of Computer Science & Communication*, Vol. 5, No. 1, pp. 37-42, 2014.

[21] N. R. Borkar and S. Kuwelkar, "Real-Time Implementation of Face Recognition System", In: *Proc. of International Conf. on Computing Methodologies and Communication*, pp. 249-255, 2017.

[22] A. H. T. A. Ghrairi, A. A. Mohammed, and E. Z. Sameen, "Face Detection and Recognition with 180 Degree Rotation Based on Principal Component Analysis Algorithm", *International Journal of Artificial Intelligence*, Vol. 11, No. 2, pp. 593-602, 2022.

[23] A. R. S. Siswanto, A. S. Nugroho, and M. Galinium, "Implementation of Face Recognition Algorithm for Biometrics Based Time Attendance System", In: *Proc. of International Conf. on ICT for Smart Society*, Bandung, Indonesia, pp. 149-154, 2014.

[24] N. Asha, A. S. S. Fiaz, J. Jayashree, J. Vijayashree, and J. Indumathi, "Principal Component Analysis on Face Recognition using Artificial Firefirefly Swarm Optimization Algorithm", *Advances in Engineering Software*,

Vol. 174, 2022.

[25] A. Rama, F. Tarres, L. Goldmann, and T. Sikora, “More Robust Face Recognition by Considering Occlusion Information”, In: *Proc. of IEEE International Conf. on Automatic Face and Gesture Recognition*, Amsterdam, Netherlands, pp. 1- 6, 2008.

[26] Sharmila, R. Sharma, D. Kumar, V. Puranik, and K. Gautham, “Performance Analysis of Human Face Recognition Techniques”, In: *Proc. of International Conf. on Internet of Things: Smart Innovation and Usages*, Ghaziabad, India, pp. 1-4, 2019.

[27] P. Viola and M. Jones, “Rapid Object Detection Using a Boosted Cascade of Simple Features”, In: *Proc. of IEEE Computer Society Conf. on Computer Vision and Pattern Recognition*, Kauai, USA, pp. 1-9, 2001.

[28] M. A. Turk and A. P. Pentland, “Face Recognition Using Eigenfaces”, In: *Proc. of Computer Society Conf. on Computer Vision and Pattern Recognition*, Maui, USA, pp. 586-591, 1991.

[29] S. A. Angadi and S. M. Hatture, “Multimodal Biometrics Database for Person Authentication: VTU-BEC-DB”, In: *Proc. of International Conf. on Intelligent Computing and Sustainable System*, Coimbatore, India, pp. 573-579, 2018.

[30] M. I. B. Hussain and M. Rafi, “Secured Contactless ATM Transaction during Pandemics with Feasible Time Constraint and Pattern for OTP”, *International Journal of Application or Innovation in Engineering & Management*, Vol. 10, No. 5, pp. 20–31, 2021.

[31] M. I. B. Hussain and M. Rafi, “A Secured Biometric Authentication with Hybrid Face Detection and Recognition Model”, *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 3, pp. 48 – 61, 2023.

[32] N. Micallef and N. A. G. Arachchilage, “Changing users’ security behaviour towards security questions: A game based learning approach”, In: *Proc. of Military Communications and Information Systems Conf.*, Canberra, Australia, pp. 1-6, 2017.

[33] A. Rabkin, “Personal knowledge questions for fallback authentication: security questions in the era of Facebook”, In: *Proc. of Symposium On Usable Privacy and Security*, Pittsburgh, USA, 2008.

[34] Sutriman, and B. Sugiantoro, “Analysis of Password and Salt Combination Scheme to Improve Hash Algorithm Security”, *International Journal of Advanced Computer Science and Applications*, Vol. 10, No. 11, pp. 420-425, 2019.