International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 10, Issue 5, May 2021 **ISSN 2319 - 4847**

SECURED CONTACTLESS ATM TRANSACTION DURING PANDEMICS WITH FEASIBLE TIME CONSTRAINT AND PATTERN FOR OTP

Md. Irshad Hussain B[1] and Dr. Mohamed Rafi[2]
[1,2]University BDT College of Engineering, Davanagere, Karnataka, India
[1]Visvesvaraya Technological University, Belagavi, Karnataka, India

ABSTRACT

Currently the users operate the Automated Teller Machine(ATM) in-contact mode with Single Factor Authentication (SFA), usually with a static 4 Digit Personal Identification Number (PIN), which is not safe and secure. The ATMs often suffer from attacks and frauds. In this paper we are proposing a novel solution to overcome the ATM frauds and attacks. ATM can be operated in contact-less, Multimodal and Two Factor Authentication (TFA) mode, that enables transactions highly secured and provides safety to user in this COVID-19 pandemic. The work carried out is strictly in conjunction with RBI Authentication guidelines. The application that has been designed verifies a customer at three different levels. The application is designed and tested out with 200 samples with these considerations: i) Success rate of OTP with two Patterns - Digit and Alpha-numeric along with time restriction ii) Total Success rate of Authentication at Second and third levels using TOTP by memorizing or by writing it or by any other means marking completion of Authentication. A detailed survey of RBI reports is also made to bring out the usage of ATM transactions and number of ATM frauds committed. The work also identifies suitable pattern and time to be used for OTP and make it more secured.

Keywords: OTP, TOTP, PIN, Two Factor Authentication, Retention.

1. INTRODUCTION

At the beginning of evolution, in the absence of monetary medium, the transactions were carried out with barter system. The introduction of monetary medium led to the banking system, which dates back to 2000 B.C., as per the loan records obtained from temples of Babylonia [1]. Now a day, the monetary medium used is termed as 'Currency'. Banks play very vital role in any country's economic affairs. The bank facilitates the essential services of depositing, currency exchange and loaning to the citizens in need. The ATM was invented by John Shepherd-Barron in year of 1960. The ATM is a self-service banking terminal that accepts deposits and dispenses cash. ATM facilitates the customers in such a way that, they need not visit the bank for withdrawal of amount. It provides a customer with round the clock i.e., 24 hours of uninterrupted services, hence sometimes it is fondly called Any Time Money machine. As per The RBI data [2], Table 1 and Fig. 1 infers that the usage of ATM across India has drastically increased, in past 5 Years(Statistics of 60 Months) i.e., from 2016 to 2019 and there is slight dip in usage in 2020 due to COVID19 Pandemic.

Year	**2016**	**2017**	**2018**	**2019**	**2020**
No. of ATB	7.95	8.48	9.5	9.6	6.31
AWAT	□22.38	□27.oo	□32.65	□34.54	□31.38

Table 1: Actual Transactions in Billions(ATB) and Actual Amount withdrawn from ATM in Trillions(AWAT) [Source : RBI]

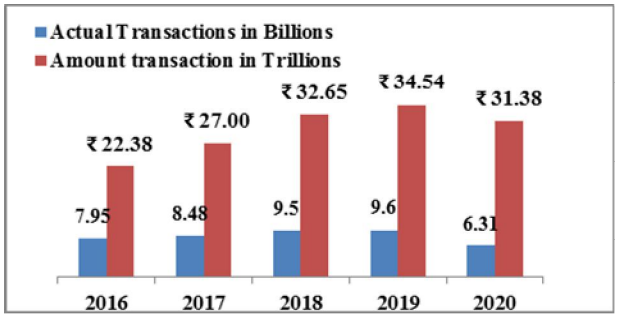

Fig. 1: Chart of ATB and AWAT [Source: RBI]

ATM is vulnerable to attacks and frauds, which have been categorized in to 3 variations Physical attack, ATM Fraud and Software Attack. Physical attack is an attack on ATM machines physically with a clear intention of gaining access to the cash in it. Software Attack is an attack on ATM by gaining unauthorized access of the ATM Machine. ATM Fraud pertains to the gaining of bank card information of the authorized customer and using it unlawfully. The most common ATM frauds are– Eavesdropping, Phishing and Spoofing, and Skimming. As per the RBI Annual Reports[3][4], the ATM fraud attacks on ATM machine is increasing every year, which is shown in Table 2 and represented in Fig. 2;

Year	2017 -18	2018-19	2019-20	Apr – Jun 2020
No. of Frauds	2,059	1,866	2,678	530
Amount (In Millions)	□ 1,095.60	□ 713.80	□ 1,950	□ 270

Table 2: ATM Fraud attacks in past 3 years.

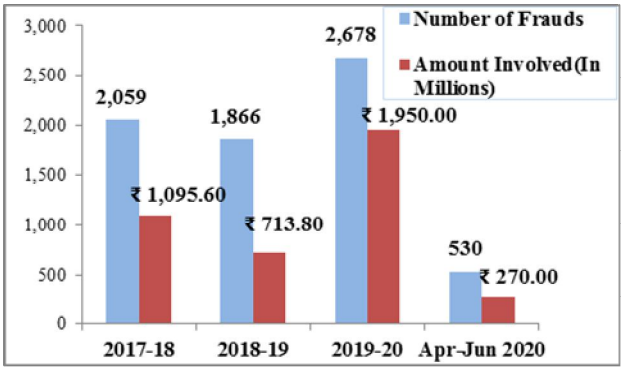

Fig. 2: ATM Fraud Attack (Source: RBI)

The above depiction of graph shows there is surge in fraud and the amount; this is due to weak authentication in the existing technology. Existing technology is based on SFA which needs a customer to punch the static 4-digit PIN after inserting the ATM card, the ATM calls up the banks computers to verify the authenticity of that customer, checks balance, and dispenses the cash and the completion of transaction is accomplished with acknowledgement on display of ATM, it might also dispense receipt on user's request and also with an SMS (Short Message Service) [5]. One of the RBI Authentication practices[6] suggests to involve three basic 'factors' in authenticating a customer for transaction - Factor 1: Something the user knows for e.g., password, PIN, etc. ; Factor 2: Something the user has for e.g., ATM card, smart card, etc.; Factor 3: Something the user is for e.g., biometric characteristic, such as a fingerprint, iris, face , voice etc.

In the proposed technology, all the three factors are used to authenticate a user at different levels with multifactor authentication, which enhances the security of the transaction. In this approach, the user has to insert the ATM card (Factor 2), then the user has to use the PIN (Factor 1), as password, then the user is verified with a 6-Digit TFA TOTP, followed by biometric authentication (Factor 3) or by 8 Character alpha-numeric TFA TOTP – a Customer's Family and Friends (CFF) feature – these multifactor authentication creates difficulties to fake the identity of the user[7]. Traditionally, the ATM user is authenticated with static 4-digit PIN as provided by the bank. The user can change this

PIN, this raises a great concern of how much the PIN is secured? The customer for ease of remembrance often changes the PIN to their date of birth or use weak PINs such as 1234[8] and also sometimes write it down which may be compromised as they are static in nature. So, to enhance the security a mechanism of TFA TOTP and biometric or CFF feature are needed. CFF feature has been added keeping in mind that if customer cannot operate the ATM due to critical illness or physical absence. The usage of TOTP and CFF feature is supported by prototyping different types of OTP (One Time Password) that are currently used in various applications.

2 LITERATURE SURVEY:

Some of the work that has been proposed that tackles one or more of the 3 frauds are surveyed and summarized in Table 3.

The survey revealed that the works proposed so far, requires physical contact of user to perform ATM transactions. Some proposed work uses weak SFA PIN or passwords to authenticate a user; some uses OTP - that remain unexpired, resulting in security concerns. The proposed system overcomes all these issues.

2.1 Need for strong TOTP:

The TFA TOTPs are much stronger than the SFA PIN/OTP, but they too have a downside, the OTPs are difficult to memorize [21] by human beings. The studies have revealed that retention capabilities of a person with speak abilities is of 7 ± 2 number span and that of signers is only 5 ± 1 [22]. In general, the banks use 4 to 6 Digits PIN or OTP for the transactions and the RBI security measure [6] emphasizes on having challenge-based and TOTPs for strong security and also recommends a an time window of not more than 100 Sec. to lower the risk of OTP misuse. Considering all these factors an application is developed that simulates to authenticate a user in three different scenarios, the first scenario is a 6-Digit TOTP with a time constraint of 30 Sec. at II level, the second and third scenario is a challenge-based 8-Characters alpha-numeric TOTP at 30 and 45 Sec., respectively for III level CFF authentication, in case of biometric fails [23] of the customer himself or if the transaction is performed by his/her friend or family member. The application was tested by accounting into the factors of retention and time constraint.

Authors	Levels	Advantages	Limitations
Mithun Dutta & et'al[9]	I : Fingerprint (FP) II: OTP	Alert Message sent to user phone. Enhancement of the existing system.	Transaction in-contact mode. No proposed algorithm.
Paschal A. Ochang & et'al [10]	I: PIN II : FP	Eliminate the need for a debit card	Transaction in-contact mode. Fails Factor 2 [6]
Shivam Mishra & et'al[11]	I:PIN II: FP III: OTP	After 3 failures sends SMS to user and to nearest Police station	Transaction in-contact mode.
Kavita Hooda[12]	I: PIN II: Face	Face image is acquired from 3 different angles	No face algorithm proposed.
Sowmya Ravikumar & et'al[13]	I: FP	FP as a biometric measure to enhance the security	Uses only one factor to authenticate a user.
Muhammad Bello B.L. & et'al [14]	I: PIN II: OTP	Enhancement to Existing system. Proposed a Novel algorithm	No Physical Presence of user. Transaction in-contact mode.
Avinash Kumar Ojha [15]	I:Pass-word II: FP	The same hardware platform can be used for iris trait.	No clarity of I Level authentication.
Deepa Malviya [16]	I: PIN II: Face	Face image is acquired from 3 different angles	No face algorithm was proposed
Savita Choudhary [17]	I: FP	Each transaction generates a key which is verified from the database	The proposal was not built in context to the existing system
Jaydeep Shamdasani & et'al [18]	I: FP II:4 digit OTP	For every transaction new OTP is generated	No FP Algorithm is proposed. Not discussed dynamic

			OTP.
V.Padmapriya & et'al [19]	I: PIN II:FP III:4 digit OTP	Scope for a nominee user to perform transaction on behalf of the real user.	Discordances between the user and the nominee.
Vaibhav R. Pandit and et'al[20]	I: 4 digits PIN. II: FP	1) The system can be deployed with any application to enhanced security. 2) Low power consumption	No FP algorithm was proposed.

Table 3: Details of Previous work

3 METHODOLOGY:

The proposed system is a three level verification system as shown in the Fig. 3, flowchart representing the proposed system. The customer has to insert the ATM card into the ATM, if he does not key in the PIN within 5 Sec., then by default the system is thought of being operated in contactless mode, which is followed by three level authentication of customer.

At first level the customer of the bank has to login to the application using the registered user identifier along with PIN as password. When the customer passes through this first level of verification, he/she enters in to second level of verification where a unique 6 digit TOTP will be generated and received. The customer has to enter this TOTP correctly within 30 Sec. for successful verification.

After successful verification at second level the customers enter into third level of verification, here the customer is provided with two options; first to the biometric verification. Any of the biometric verification which is contactless with the likes of face recognition, iris recognition, voice recognition, etc., should be embedded in the verification process. This biometric verification speeds up the recognition process and brings out the inference the physical presence of the user there by concluding that the rightful user is performing the transaction. Secondly, a special feature CFF that aid in operating of ATM on behalf of the Customer. When CFF mode is opted an 8 characters alpha-numeric TOTP will be generated and the received TOTP has to be correctly entered within 45 Sec. On successful third level verification the customer will be given access to do transaction at ATM.

If the customer is performing transaction with in-contact or regular mode, he/she will enter the PIN within 5 Sec. of insertion of ATM card. On successful verification, he/she will be taken to second level and rest follows as said above.

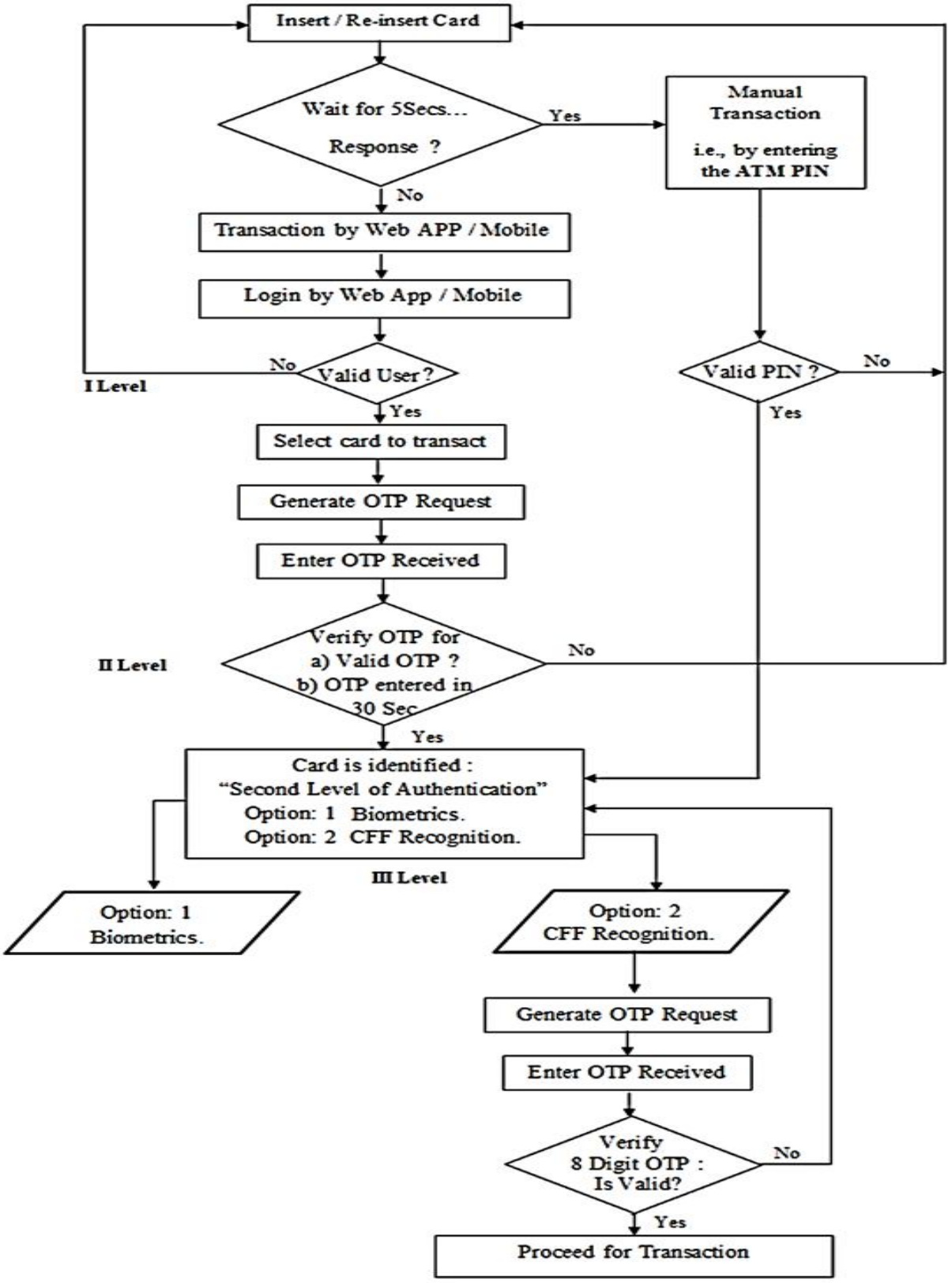

Fig. 3: Flow chart of the proposed system.

3.1Algorithms to generate pattern and set time constraint for OTP:

The following algorithm generates a random alpha-numeric OTP with length of 8 characters.

Algorithm 1: Pattern for OTP generation for CFF
//G="0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz", OTP, n=8, g_rand, mod_opr, otp_gen _time

Step 1: Set default timezone
Step 2: Initialize G;
Step 3: Iterate for n-times and pick a single character/number from G and append it to OTP each time until the length exhausts.

```
for i in range (1, n)
   g_rand=rand()
   r_indx = g_rand – (62 * floor(g_rand/62))
   OTP = substr(G, r_indx, 1);
   return OTP
```

Step 4: otp_gen _time = Store current date_time stamp of OTP generation.

Using the above algorithm and Setting the variable G to string of numbers will generate a random numeric OTP of length 6 Digits.

Algorithm 2: Appending time constraint to OTP for II level and CFF
// otp_sub_time, otp_gen _time, YYYY, MM, DD, Hr, Min, Secs

Step 1: Set default timezone
Step 2: Capture otp_sub_time - OTP Submitted Time Stamp in "Y-m-d H:i:s" format
//2019-10-16 11:51:36 Y- Year in YYYY format, m- month in mm format, d-day in dd format, h-hour, i-minutes and s – Sec..
Step 3: Get otp_gen _time (2020-10-16 11:51:36)
Step 4: Convert otp_gen _time and otp_gen _time into Unix timestamp
Step 5: Get the Years YYYY, Months MM, Days DD, Hours Hr, Minutes Min and Seconds Secs, difference between otp_gen _time and otp_gen _time
Step 6: Time Comparison

```
If YYYY =0 and MM=0 and DD=0 and Hr=0 and Min = 0 and Secs <= 45
   If Entered OTP = Submitted OTP Then
      Display “SUCCESSFUL Verification”
   else
      Display “Invalid OTP”
   end if
else
    Display “OTP Expired”
```

The above algorithm is to set time constraint of 45Sec. and 60Sec. for CFF at III Level and same algorithm can be used by Setting the variable Secs <= 30 or Secs <= 45 to set a time constraint of 30 Sec. or 45 Sec. at II Level.

3.2 Working of application:
3.2.1 Login: I level authentication (SFA):
Login Page acts as a First Level of Verification of the customer. The entry to the system is possible with only registered user id of the bank as Username and the ATM PIN associated with the ATM card as Password. The Login page is subjected to validation checks at client’s end against the Username and Password fields, before the submission of data is made to the server, which are as follows:

- Both fields are checked for empty values.
- Only characters from A to Z, a to z; numerals from 0 to 9 and a period (.) and underscore (_) are considered as valid characters for username field.
- The User name field should be of length 6 to 10 characters.
- The Password field can contain only numeric values.

- The Password field should be entered exactly with 4 numeric characters.

Only after the above validations the request is processed to the server. The entered values of Username and password are verified against stored credentials of the customer in the server. If there is a mismatch of any one of the credentials then the server will display the message as invalid username and/or password and asks the user to retry once again. If the Username and Password entered are verified correctly, then the system fetches the card(s) id associated with that particular customer and waits for customer's instruction to proceed.

3.2.2 Get OTP: II level authentication(TFA):

As soon as the customer proceeds further by clicking, "Proceed" button, the system asks the customer to click the "Get OTP" button, to generate the 6 Digit TOTP. As the customer clicks on "Get OTP" button, the request is made to the server to generate a 6 Digit TOTP for the current transaction. The server responds by generating and sending a 6 Digit TOTP. The customer has to enter this 6 Digit TOTP from his end which has popped up on his screen within 30Sec.

3.2.2.1 Verification of 6 digit OTP:

It acts as Second Level of Authentication of the Customer. The User enters the TOTP, which he/she has received from the server: The TOTP is verified for the following:

a) Whether the TOTP has been entered within 30 Sec. of its receipt, if not the system will not process the request, it will simply display the message as TOTP Expired and ask to retry. When opted to retry, the system navigates the user to generate OTP (Get OTP) page.
b) If the OTP is entered within 30 Sec. and if it invalid (or wrong) TOTP, then also the system will not process the request, it will simply display the message as Invalid OTP and ask to retry. When opted to retry, the system navigates the user to generate OTP (Get OTP) page.
c) If the OTP is entered within 30 Sec. and if it is the valid TOTP i.e., same as sent by the server, then the user will be successfully verified at Second level of verification and enters into third level of verification.

3.2.3 Third level of authentication (TFA):

The third level of authentication offers two ways of verifying a customer

i) Biometric Verification: If selected the customer will be diverted to biometric verification.

ii) CFF Recognition: If the customer is unable to carry out the transaction in his physical presence due to physical or medical conditions, in this case, the transaction can be carried out by the Customer Family or Friends.

When this is opted then the following steps comes into existence.

Step 1) Get OTP: The system presents the customer with a "Get OTP" button, to raise a request to generate the 8 Characters alpha-numeric TOTP.

Step 2) As soon as the customer clicks on "Get OTP" button, the request is made to the server to generate an 8 Characters alpha-numeric TOTP for the current transaction. The server responds by generating and sending an 8 Characters alpha-numeric TOTP.

Step 3) the customer has to enter this 8 Characters alpha-numeric TOTP from his end which has popped up on his screen.

Step 4) Verification of 8 Characters alpha-numeric TOTP: The User enters the TOTP, which he/she has received from the server: The TOTP is verified for the following:

a) Whether the TOTP has been entered within 45 Sec. of its receipt, if not the system will not process the request, it will simply display the message as TOTP Expired and ask to retry. When opted to retry, the system navigates the user to generate TOTP (Get OTP) page.
b) If the TOTP is entered within 45 Sec. and if it invalid (or wrong) TOTP, then also the system will not process the request, it will simply display the message as Invalid TOTP and ask to retry. When opted to retry, the system navigates the user to generate OTP (Get OTP) page.
c) If the TOTP is entered within 45 Sec. and if it is the valid TOTP i.e., same as sent by the server, then the user will be successfully verified at this final level of verification and will be given access to perform transactions.

4 TEST RESULT AND ANALYSIS:

The application was developed using PHP: Hypertext Preprocessor scripting language Version 7.3, EXtensible HyperText Markup Language(XHTML) version 5.0, JavaScript version 1.8.5, MySQL version 5.7 Cascading Style

Sheets and WampServer 2.0.
The users were first let to perform a transaction with their retention capabilities and then they were asked to perform by writing down the OTP on a piece of paper or any other means they prefer to. Using this concept a survey of 200 users with an age range of 22 to 55 is carried out, the result of survey is as follows:
Successful Retention (SR) – When user remembers the TOTP and enters correctly within the stipulated time of 30 or 45 or 60 Sec.
Invalid OTP Retention (IOR) - When user tries to remembers the TOTP and enters it incorrectly, within the stipulated time of 30 or 45 or 60 Sec.
OTP Expired Retention (OER) - When user tries to remember the TOTP and submits it, but not within the stipulated time of 30 or 45 or 60 Sec.
Successful Written (SW) - When user enters the TOTP correctly within the stipulated time of 30 or 45 or 60 Sec. by writing down the TOTP or recorded by any other means.
Invalid OTP Written (IOW) – When user enters the wrong TOTP, which has been written down or recorded by any other means, but within the stipulated time of 30 or 45 or 60 Sec.
OTP Expired Written (OEW) - When user enters the TOTP, which has been written down or recorded by any other means, but not within the stipulated time of 30 or 45 or 60 Sec.

4.1 OTP pattern and time variations at II level:

a) 6 Digit OTP in 30 Sec.:

In retention mode: 84% of users remembered and successfully entered the 6 Digit TOTP within 30 Sec., 12% entered wrong TOTP and 4% of Users could not accomplish the task within 30 Sec.
In written or any other mode: 94% of users successfully entered the 6 Digit OTP within 30 Sec., 4% entered wrong TOTP and 2% of Users could not accomplish the task within 30 Sec., as shown in Table 4.

Sl. No.	Test Type	Samples in a Category	Percentage of Result
Retention			
1	SR	168	84.00%
2	IOR	24	12.00%
3	OER	08	04%
Written or Other Mode			
1	SW	188	94.00%
2	IOW	08	4.00%
3	OEW	04	2.00%

Table 4: Result of Sample Testing with 6 Digit OTP in 30 Sec.

b) 6 Digit OTP in 45 Sec.:

In retention mode: 91.50% of users remembered and successfully entered the 6 Digit TOTP within 45 Sec., 6.50% entered wrong TOTP and 2% of Users could not accomplish the task within 45 Sec.
In written or any other mode: 97.50% of users successfully entered the 6 Digit OTP within 45 Sec., 1.50% entered wrong TOTP and 1% of Users could not accomplish the task within 45 Sec., as shown in Table 5.

Sl. No.	Test Type	Samples in a Category	Percentage of Result
Retention			
1	SR	183	91.50%
2	IOR	13	6.50%
3	OER	04	2.00%
Written or Other Mode			
1	SW	195	97.50%
2	IOW	03	1.50%
3	OEW	02	1.00%

Table 5: Result of Sample Testing with 6 Digit OTP in 45 Sec.

c) Challenge based CFF - 8 characters alpha-numeric OTP in 30 Sec.

Sl. No.	Test Type	Samples in a Category	Percentage of Result
Retention			
1	SR	68	34.00%
2	IOR	56	28.00%
3	OER	76	38.00%
Written or Other Mode			
1	SW	124	62.00%
2	IOW	32	16.00%
3	OEW	44	22.00%

Table 6: Result of Sample Testing with Challenge based in 30 Sec.

In retention mode: 34% of users remembered and successfully entered the 8 Characters Alpha-Numeric OTP within 30 Sec., 28% entered wrong TOTP and 38% of Users could not accomplish the task within 30 Sec.
In written or any other mode: 62% of users successfully entered the 8 Characters Alpha-Numeric OTP within 30 Sec., 16% entered wrong TOTP and 22% of Users could not accomplish the task within 30 Sec., as shown in Table 6.

d) Challenge based CFF 8 characters alpha-numeric OTP in 45 Sec.
In retention mode: 44% of users remembered and successfully entered the 8 Characters Alpha-Numeric OTP within 45 Sec., 44% entered wrong TOTP and 24% of Users could not accomplish the task within 45 Sec.
In written or any other mode: 80% of users successfully entered the 8 Characters Alpha-Numeric OTP within 45 Sec., 14% entered wrong TOTP and 6% of Users could not accomplish the task within 45 Sec., as shown in Table 7.

Sl. No	Test Type	Samples in a Category	Percentage of Result
Retention			
1	SR	88	44.00%
2	IOR	88	44.00%
3	OER	24	12.00%
Written or Other Mode			
1	SW	160	80.00%
2	IOW	28	14.00%
3	OEW	12	6.00%

Table 7: Result of Sample Testing with Challenge based CFF in 45 Sec.

e) Challenge based CFF 8 characters alpha-numeric OTP in 60 Sec.
In retention mode: 54% of users remembered and successfully entered the 8 Characters Alpha-Numeric OTP within 60 Sec., 36.50% entered wrong TOTP and 9.50% of Users could not accomplish the task within 60 Sec.
In written or any other mode: 90.50% of users successfully entered the 8 Characters Alpha-Numeric OTP within 60 Sec., 7% entered wrong TOTP and 2.50% of Users could not accomplish the task within 60 Sec., as shown in Table 8.

Sl. No	Test Type	Samples in a Category	Percentage of Result
Retention			
1	SR	108	54.00%
2	IOR	73	36.50%
3	OER	19	9.50%
Written or Other Mode			
1	SW	181	90.50%
2	IOW	14	7.00%
3	OEW	05	2.50%

Table 8: Result of Sample Testing with Challenge based CFF in 60 Sec.

4.2 OTP pattern and time variations at II and III Level marking completion of transaction:
The following are the results obtained, when the overall application was tested by setting
a) 6 Digit TOTP of 30 Sec. at II level and 8 characters alpha-numeric TOTP of 30 Sec. at III Level :

Mode	Success	Error	%ge Success	%ge Failure
Retention	64	136	32%	68.00%

Written or other mode	112	88	56%	44.00%

Table 9: Completion of Transaction at II and III Level

In retention mode: It is observed that only 32% of user could accomplish the task and 68% of users failed to accomplish the task. In written or any other mode: It is observed that 56% of user could accomplish the task and 44% of users failed to accomplish the task, as shown in Table 9.

b) 6 Digit TOTP of 30 sec. at II level and 8 characters alpha-numeric TOTP of 45 Sec. at III level :

Mode	Success	Error	%ge Success	%ge Failure
Retention	72	128	36%	64.00%
Written or other mode	152	48	76%	24.00%

Table 10: Completion of Transaction at II and III Level

In retention mode: It is observed that only 36% of user could accomplish the task and 64% of users failed to accomplish the task. In written or any other mode: It is observed that 76% of user could accomplish the task and 24% of users failed to accomplish the task, as shown in Table 10.

b) 6 Digit TOTP of 45 sec. at II level and 8 characters alpha-numeric TOTP of 60 Sec. at III level :

In retention mode: It is observed that only 59% of user could accomplish the task and 41% of users failed to accomplish the task. In written or any other mode: It is observed that 88.50% of user could accomplish the task and 11.50% of users failed to accomplish the task, as shown in Table 11.

Mode	Success	Error	%ge Success	%ge Failure
Retention	118	82	59.00%	41.00%
Written or other mode	177	23	88.50%	11.50%

Table 11: Completion of Transaction at II and III Level

5 CONCLUSIONS:

To begin with the literature survey, our study showed that, the ATM usage has increased with that ATM frauds also have increased drastically. So far the work carried out is based on in-contact ATM transactions. The previous works does not talk about the time limits that should be constrained on OTP as per the RBI guidelines. Our work focuses mainly on usage of TOTP, the best duration of time constraint on OTP and which pattern can be successfully used for OTP.

We found that a 6 Digit OTP was most successfully entered by the users within 45 Sec, a success of 97.50% in written or any other mode and 91.50% by retention.

CFF feature helps the user to operate the ATM during biometric failures or if they cannot operate physically. We found that in a Challenge based CFF - 8 Characters Alpha-Numeric OTP when given a time limit of 60 Sec., the success rate was more in retention as well as in written or any other mode against 30 Sec. and 45 Sec. time limit, respectively.

We also found that the user success rate increased in completing the authentication with 6 Digit TOTP of 45 Sec. at II Level and 8 Characters Alpha-Numeric TOTP of 60 Sec. at III Level by 27% by retention and 32.50% in written or other mode against *6 Digit TOTP of* 30 Sec. at II level and 8 characters alpha-numeric TOTP of 30 Sec. at III Level and by 23% by retention and 12.50% in written or other mode against *6 Digit TOTP of* 30 Sec. at II level and 8 characters alpha-numeric TOTP of 45 Sec. at III Level.

Hence, with the analysis we would conclude that a 6 Digit TOTP of 45 Sec. at II Level and 8 Characters Alpha-Numeric TOTP of 60 Sec. at III Level should be used for successful secured authentication. Further, our study revealed that use of Biometrics will enhance the security of transaction at ATMs. So it is suitable to use an ATM card, a PIN, a random TFA 6 Digit TOTP at II Level and at III Level – preferably a contactless Biometric (e.g. Iris, Face, Retina, etc.,) or CFF, a random TFA 8 Characters Alpha-Numeric TOTP will enhance the security of transaction and also completely abide by 3 factors of RBI guidelines [6].

6 FUTURE WORK:

In Future, identification of a feasible Biometric trait for III level, that enhances the security of user transaction and implementation of the same. Also to address the issue of Physical Attack on ATM, this ensures the security of ATM and also the safety of user.

REFERENCES:

[1] Emmanuel N, Roussakis(1997), Global Banking, Origins And Evolution, - Revista de Administração de Empresas, São Paulo, v. 37, n. 4, pp45-53, doi.org/10.1590/S0034-75901997000400006.
[2] Reserve Bank of India, BANKWISE ATM/POS/CARD STATISTICS: https://www.rbi.org.in/Scripts/ ATMView.aspx
[3] Reserve Bank of India, Annual Report (2018-19); https://rbidocs.rbi.org.in/rdocs/AnnualReport/ PDFs/0ANNUALREPORT2018193CB8CB2D3DEE4EFA8D6F0F6BD624CEDE.PDF
[4] Reserve Bank of India, Annual Report (2019-20); https://rbidocs.rbi.org.in/rdocs/AnnualReport/ PDFs/0RBIAR201920DA64F97C6E7B48848E6DEA06D531BADF.PDF
[5] Md. Irshad Hussain, B; Dr. Mohammed Rafi(2019), A Survey On Unimodal And Multimodal Biometric System For Enhancement Of ATM Security, IJRAR, Volume 6, Issue 1,pp1143-1148.
[6] Reserve Bank of India, Authentication Guidelines https://www.rbi.org.in/hindi1 /Upload/content/PDFs/C229260416_2.pdf
[7] M. L. T. Uymatiao; W. E. S. Yu(2014); Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore, IEEE International Conference on Information Science and Technology, Shenzhen, pp225-229, doi: 10.1109/ICIST.2014.6920371.
[8] E. D. Dimaunahan; A. H. Ballado; F. R. G. Cruz; J. C. Dela Cruz(2018), MFCC and VQ voice recognition based ATM security for the visually disabled, 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), IEEE, vol. 1–5, doi: 10.1109/HNICEM.2017.8269516.
[9] Mithun, Dutta; Kangkhita Keam, Psyche; Shamima, Yasmin(2017), ATM Transaction Security Using Fingerprint Recognition, American Journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN : 2320-0936 Volume-6, Issue-8, pp41-45.
[10] Paschal A, Ochang; Paulinus O, Ofem(2017), An Enhanced Automated Teller Machine Security Prototype using Fingerprint Biometric Authentication, Int. J. Advanced Networking and Applications, Volume: 08 Issue: 04, pp3110-3117.
[11] Shivam, Mishra; Aakarsh, Jain; Shivam, Kumar; Ankit, Goyal(2017), Enhanced ATM Security System using GSM, GPS and Biometrics, International Journal of Engineering and Technical Research (IJETR), Volume-7, Issue-8, pp33-37.
[12] Kavita, Hooda(2016), ATM Security, International Journal of Scientific and Research publications, Volume 6, Issue 4, pp159-166.
[13] Sowmya, Ravikumar; Sandhya, Vaidyanathan; B, Thamotharan, S, Ramakrishnan(2013), A new business model for ATM transaction security using fingerprint recognition, International Journal of Engineering and Technology, Vol 5 No 3, pp2041-2047.
[14] Muhammad,Bello B.L.; Alhassan, M.E.; Ganiyu, S.O. (2015), An Enhanced ATM Security System using Second-Level Authentication, International Journal of Computer Applications, Volume 111, No 5, pp8-15, doi: 10.5120/19533-1181
[15] Avinash Kumar, Ojha(2015), ATM Security using Fingerprint Recognition, International Journal of Advanced Research in Computer Science and Software Engineering. Volume 5, Issue 6, pp170-175.
[16] Deepa, Malviya(2014), Face Recognition Technique: Enhanced Safety Approach for ATM, International Journal of Scientific and Research Publications, Volume 4, Issue 12, pp1-6.
[17] Savita, Choudhary(2014), Design of Biometric Based Transaction System using Open Source Software Development Environment, International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 2, pp37-42.
[18] Jaydeep, Shamdasani; Prof. Pravin, Matte(2014), ATM Client Authentication System Using Biometric Identifier & OTP, International Journal of Engineering Trends and Technology, Volume 11, Number 5, pp255-258.
[19] V, Padmapriya; S, Prakasam(2013); Enhancing ATM Security using Fingerprint and GSM Technology, International Journal of Computer Applications, Volume 80 , No 16, pp46-46, doi:10.5120/13957-1735

[20] Vaibhav R, Pandit; Kirti A, Joshi; Narendra G, Bawane(2013), ATM Terminal Security using Fingerprint Recognition, International Journal of Applied Information Systems (IJAIS), 2nd National Conference on Innovative Paradigms in Engineering & Technology, pp14-18.
[21] Dr. K. Mohan, Kumar; G, BalaMurugan(2018), Comparative Study On One Time Password Algorithms, International Journal of Computer Science and Mobile Computing, Vol.7 Issue.8, pp37-52.
[22] Mary, Rudner; Josefine, Andin; Jerker, Rönnberg(2009), Working memory, deafness and sign language, Scandinavian journal of psychology, 495-505.
[23] P, Markert; D. V, Bailey; M, Golla; M, Dürmuth; A. J, Aviv(2020), This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs, 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, pp286-303, doi: 10.1109/SP40000.2020.00100.

AUTHORS

Mr. Md. Irshad Hussain B, is currently working as Assistant Professor on deputation in the Department of Master of Computer Application, University BDT College of Engineering, Davanagere from Visvesvaraya Technological University(Bangalore Region). He is having more than 12 years of Teaching experience. He received his Master's Degree MCA(First Class with Distinction) from Bapuji Institute of Engineering and Technology, Davanagere, affiliated to Visvesvaraya Technological University, Belagavi in the year 2004. Currently pursuing PhD in the area of Image Processing under the guidance of Dr. Mohammed Rafi, Professor, Dept. of Computer Science &Engineering, University BDT College of Engineering, Davanagere, a Constituent College of VTU, Belagavi, Karnataka, India. His research interest includes, Data Warehousing and Mining, Image processing, IoT, Databases and NOSQL. He is a Life time member for ISTE.

Dr. Mohamed Rafi having B.E., M E., and Ph.D. in Computer Science & Engineering. He is having more than 25 years of experience in Teaching & Research. Currently he is working as Professor in Department of Studies in Computer Science &Engineering, University BDT College of Engineering, Davanagere, a Constituent College of Visvesvaraya Technological University, Belagavi. Also serving as member of Board of studies, Bangalore University, Subject expert of Doctoral Committee Bangalore University and BOE member of Computer Science and Information Science Board, VTU. Worked at Universities of Ethiopia& Saudi Arabia. Published more than 100 papers in conferences, & International Journals. His area of Interest Includes Digital Image Processing & Managing Big data.