Enhancement of Two-Tier ATM Security Mechanism: Towards Providing a Real-Time Solution for Network Issues

Syed Anas Ansar[1], Satish Kumar[2], Mohd. Waris Khan[3], Amitabha Yadav[4], Raees Ahmad Khan[5]
Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India[1, 2, 5]
Department of Computer Application, Integral University, Lucknow, India[3]
Department of Software Development and e-Governance[4]
National Post Graduate College, Lucknow, India[4]

***Abstract*—In the current scenario, the crime rate has tremendously increased with respect to the Automatic Teller Machine (ATM). During the last few years, criminals are becoming more sophisticated and paid more attention to ATMs. The majority of ATMs in India are working on a single authentication technique. The attacks, such as skimming, shimming, card cloning, card swapping, shoulder surfing, etc. works due to the use of minimal authentication in ATMs. So, the concern about the security of ATMs is reached to its peak level. Nowadays, banks have moved towards the two-tier authentication level. Recently in India, some banks have adopted the One Time Password (OTP) mechanism along with a UID number to perform the transaction in ATMs. In such a case, dependency on the cellular network for OTP is also a significant concern. To overcome these types of issues researcher proposed a two-tier authentication mechanism. The paper addresses the recent problems and their solution with the help of a two-way authentication method. To resolve the network issue, the researcher also proposed a novel technique, i.e., Security Question-based verification mechanism.**

***Keywords*—ATM-fraud; security: Unique Identifier (UID); shoulder surfing; shimming; trapping**

I. INTRODUCTION

In this digital world, information and computer technology has built up its approach in almost every aspect of life. We are observing that the world is witnessing tremendous growth in the use of the internet, online transactions, data transfer, and information technology tools. Nowadays, the prime user of online transactions and the internet are banking and insurance sectors as well as financial organizations. They use this technology for making payments, transferring cash, and some additional services related to remittance. But recently, cybercrime is becoming a big issue. News headlines always frightening us about the fraud cases related to cash withdrawals, debit/credit card scams, information breach, and data theft, etc. These have a noticeable relation with the electronic system as well as the banking system. We know that maximum data and information are being online, and there is a massive chance that this information being attacked by cybercriminals. Cyber fraud has become so prevalent in the banking system, and with this, it leads to an enormous loss of money every year [1].

In the current decades, debit card has made the most remarkable evolution in the retail industry and as well as in consumer banking. The debit cards have become one of the most favored noncash retail payment gadgets after their introduction in the late 1970s. It is apparent from last decades that the growth in both as in the number of the transaction, as well as value, is multiplying (i.e., approx. 15 percent annually) [2]. At present, the use of debit cards is dominant/ruling in almost everywhere. This technology also enhanced the dispensation of cash via Automatic Teller Machines (ATMs) in order to avoid bank cash counter withdrawals. This card provides authentication of the customer on their account more effectively and securely as compared to their alternatives like cheques and passbooks [3].

As we know, on in one hand, the use of debit cards is continuously increasing, and on the other side, cardholders are facing high- profile security breaches [4]. To resist security breaches and plastic card fraud, the major payment card networks have generated their security programs such as Visa Card Information Program (CSIP), JCB Data Security Program, Master Card Site Data Protection (SDP), and American Express Data Security Operating Policy [3,4]. As these payment card network has built one more security layer on their cards to protect it from breaches and frauds. But on the other hand, attackers have found other techniques for fraud, such as skimming, Physical threats to ATM hardware, and ATM software threat.

For banking institutions, ATM Security has been consistently a significant issue because it is an inexhaustible resource of assets for attackers/cybercriminals. As we know, the problem related to the security of ATMs is becoming more acute. As any cybersecurity expert tries to patch one point but on the other hand, fraudsters find the others way because they are becoming more sophisticated in their techniques. So, security analysts have to protect the whole network rather than a single endpoint [5].

The paper proceeds as follows: related work about the topic is included in Section 2. Section 3 describes the development of plastic cards & their usage and different types of fraud techniques. Recent fraud in India is demonstrated in Section 4. The major finding is mentioned in Section 5. Section 6 includes a proposed security framework &

algorithms, along with the flowchart. At last, the paper is concluded with the conclusion and future work.

II. Related Work

In the current scenario, the research in the area of the secure transaction is going worldwide.

Adrian Fernandes (2020) has proposed an ATM that is based on biometrics. In the proposed work researcher uses biometric technology for the authentication of the account holder in place of the traditional authentication process, i.e., PIN. To perform transaction user is verified through biometric (i.e., fingerprint). The captured biometric is verified with stored biometric in the Aadhar server and after successful authentication transaction is performed. Besides, the researcher suggests that such systems must be constructed to protect the financial institution as well as customers from frauds [6].

B. Saranraj et al. (2020) have proposed a mechanism for the enhancement of ATM security by using Arduino. In the proposed methodology, researchers used two processes, i.e., Arduino Nano along with fingerprint and OTP mechanism. Users can perform transactions either by entering OTP (in the absence of original account holder) or through biometrics (in the presence of original account holder). In addition, researchers have mentioned that it will increase security by placing a two-way authentication mechanism and provides high proficiency as well as maintains a strategic distance from the illicit exchanges [7].

Ogata Hisao et al. (2019) have proposed an ATM security framework focused on avoiding jackpotting with the help of peripheral equipment. In the proposed work, the dispenser validates the reliability of the command obtained from PC for distribution of cash through ATM. In addition, all the transaction facts are recorded via a card reader. This framework fulfills three conditions and is based on the protection of peripheral equipment, and it can act as a safeguard if the PC is conciliated [8].

S. Shuka et al. (2018) have proposed an ATM security mechanism where they use a random keyboard and face resignation system for the authentication of users. In the proposed method, for making any transaction, the user has to go through a two-way security procedure. When a user goes for the transaction, a new page appears in the form of the random keyboard on the screen if the user is already registered if not then a link is provided on that page for the registration. The layout of the random keyboard is shuffled after every transaction. After that user has to enter the PIN for performing balance inquiry, withdrawal, and PIN change followed by facial recognition [9].

K. Sangeetha et al. (2018) have developed a security feature for the enhancement of ATM security by using RED-TACTON. RED-TACTON is a wireless network/human area networking technology that is consisting of transmitter and receiver sections. It has a fast data transfer rate of about 10 Mbps, and here data is transferred through the human body. In this procedure, initially, the user has to verify identity through a biometric, i.e., fingerprint scan if it matches then the PIN/password is transferred through RED-TACTON by touching the ATM to complete the transaction. They have also provided a way to perform the transaction with the help of others. In that case firstly, the other user passes the password through RED-TACTON after that the primary user will get an authentication message; if the primary user passes yes, then the transaction will take place [10].

K. T. Rayudu and M. Aravindan (2017) have proposed a security mechanism for enhancing the security of Automatic Teller Machines. Where they use One Time Password and Biometrics (i.e., finger vein biometric) with the help of Elliptic Curve Cryptography (EEC) technology to improve the surety of ATM. Elliptic Curve Cryptography is used to generate keys. Here they used a finger vein and RFID card to validate users after that; it will send a One Time Password (OTP) with the help of Bluetooth to complete the transaction [11].

Moses O. Onyesolu and Amara C. Okpala (2017) have proposed a security technique by using a Three-Tier Authentication mechanism for Automatic Teller Machine (ATM). Here they use three layers of authentication method; firstly, the user password followed by the biometric identification, and finally the user gets a One Time Password (OTP) on their mobile number (which is linked to their account number). In addition, they also introduced a new keyboard for the existing system with some unique character keys and alphabet keys. The authors also stated that all these authentication techniques must be in affirmative prior granting access to the user 12].

M. Dutta et al. (2017) have proposed a security procedure for the ATM transaction with the help of fingerprint recognition. In proposed work, they have used the fingerprint of the users as the password followed by traditional Personal Identification Number (PIN) in order to overcome the security issues in ATM money transactions. Here fingerprint module generates a four-digit code as a text message, which is sent to the registered mobile number. After the validation of the code, the user is allowed to complete the transaction [13].

N. Ahmad et al. (2016) have proposed an Advanced Encryption Standard (AES) card less Automatic Teller Machine biometric security system. The proposed security is developed by using a Field Programmable Gate Array (FPGA). The proposed system is consisting of the fingerprint scanner, multi touch screen display, RS-232, FPGA DE2-115 board with cyclone IV, and PS/2 keyboard. Here in the proposed system user has to enter identification number followed by the biometric scan, i.e., fingerprint as an input to the ATM. Advanced Encryption Standard (AES) is used to encrypt the identification number as well as a fingerprint scan. After that, the encrypted information is sent to DE2-115 and matched with the stored data for authentication [14].

Amala et al. (2016) have proposed a modified biometric authentication technique, where they used a modified Radial Basis Function Network (RBFN) to discriminate between face patterns and non-face patterns. In addition, they reduced the complexity of the RBFN with the help of Principal Component Analysis (PCA). PCA to obtain the Eigen Vector; the RBFN network takes these vectors as input for training and reorganization [15].

III. BACKGROUND

John Shephard-Barron was invented ATM (Automatic Teller Machine) in 1960, and it is a computerized telecommunication device. It starts its functioning by inserting a plastic card, i.e., a credit/debit card. This card is encoded with the user's banking information on a magnetic stripe, i.e., Personal Identification Number (PIN) and account number etc. [16]. This device permits banking as well as financial institutions and their customers to gain access to their accounts by means of a secure method of communication. The main aim of ATM is to reduce the workload of the banking sector. This device acts as a self-service terminal, which provides facilities like a dispensation of cash as well as accepts cash [17].

During the transaction process, the ATM sends the information provided by the user to the banks' server, and after its verification, the user is allowed to complete the transaction. The cardholder (i.e., user) and the host processor (i.e., server) are communicating with each other with the help of a gateway (i.e., Internet Service Provider ISP). And then the whole transaction details are sent to the bank's server. The plastic card is secured with Personal Identification Number (i.e., PIN), which is encrypted with the help of some standard encryption technique. There is no technique or process to get a PIN from the plastic card. ATMs are of two types; the basic one is to dispense cash only on the other hand, the second one is more complicated, which accepts as well as dispense cash. It consists of two input devices (i.e., Card reader and keyboard) and four output devices (i.e., Display Screen, Receipt Printer, Cash Dispenser, and a Speaker) [18].

Nowadays, news headlines are always frightening about the frauds related to Automatic Teller Machines, and in the current era, it has become a hot button issue. The fraudsters have become more sophisticated in their method to find the loophole. So, security experts have to protect the whole network rather than a single point. Some common ATM security treats are:

- The most straightforward and preliminary ATM treat; Physical threat to ATM.
- A fraud technology used to capture the details of plastic cards and then transferred to the duplicate cards: Skimming.
- Threat to ATM Network Software.
- Jackpotting.
- Shimming.
- Card and Cash Trapping.
- Transaction Reversal.

Physical Attacks: In physical attacks, the attackers rob the ATM and take cash from the safe with the help of heavy tools like cutting torch or explosive. This type of attack is also comprising of solid and liquid explosives as well as the removal of ATM from its location, and then they use some methods to get access to the safe [19].

Skimming: In this process, the skimmers use a small skimming device that fits over the actual ATM card reader slot. When the user swipes their card from it, the data and information are captured from the card and stored on the device. In addition, the skimmers place an undetectable camera to record the PIN [19].

Threat to ATM network software: In this type of attack, security criminals breach the ATM network to get control over the ATM server, where they install malware with the help of improved code. With the help of this code, they gain access to the internal command of the ATM. And now, the ATM server will act like a Command & Control (C & C) server, which commands various infected endpoints to dispense cash [5].

Jackpotting: It is the technique through which cybercriminals manipulate hardware and software vulnerabilities in ATMs that result in spitting heaps of cash from the machine. ATM jackpotting was firstly spotted in the European country in 2016, and now it was continuously spreading throughout the world. In this technique, a tiny bore is made next to the keyboard through which a cable is inserted to connect the laptop. Once attackers access a certain port, they made complete control on the machine and instructed them to dish out the cash. With the help of this technique, attackers can dispense and clears all cash from ATMs in just a few minutes.

Shimming: It is similar to skimming, where the attackers use paper-thin in the card reader to steal data from chip-enabled cards [20].

Card Trapping: In this method, the attacker hacks the ATM by installing a gadget inside the card slot. In this process, they use the most common device (i.e., Razor-Edged spring), with the help of this, the attackers trap the card and stop it from ejecting. Besides that, the attacker acts as a fellow customer and memorize the PIN trough shoulder surfing or offers to help and suggests to re-enter PIN and complete the transaction again. Then all the thief needs to do once the victim has gone is to retrieve the card from the ATM [21].

Cash Trapping: It is one of the most prominent techniques in which attackers put a gadget (i.e., glue-trap) into the ATM physically to trap the cash. In addition, a bogus dispenser is allocated in the place of original, and on the other hand, the installed device traps the allocated cash [22].

Transaction Reversal: It is one most sophisticated technique used by cybercriminals to lift cash from ATMs, where they use stolen or skimmed cards to refrain from detection. Generally, ATM is jammed by the attackers by reversing the logic of the host application. This process requires a chain of sequences for fabricating promiscuous error codes, as well as the reversal of the unwanted transaction. This type of fraud is only exercisable to those ATMs that support Motorized plastic cards [23].

IV. RECENT FRAUDS IN INDIA

On 9 December 2019, Kolkata police had cracked Kolkata ATM fraud case (skimming) of siphoning money from the account of around 71 users of ATM. The police claimed that they had arrested the accused Siliviu Florin Spiridon (28)

precisely after 8 days from Greater Kailash Delhi. The accused had started withdrawing money from November-30 to December-3 using skimmed data from Kolkata. In addition, they said that the accused used to visit India 3 times this year via tourist visa firstly on 14 March, 19 July and 14 October. They have collected around 12 sunglasses, 24 caps, a huge collection of clothing, and costly mobile phones and skimming devices [24].

In May 2018, a 16-year-old girl named Nisha was cheated with Rs. 29,000 by two people on an ATM at Dwarka Sector 14, and after a day that girl was reportedly committed suicide. She had visited the ATM to withdraw some money for the medical treatment of her father, but due to lack of awareness she handovers her two debit cards to the person who was there at that time to withdraw the amount. During the process, they swiped the cards and made the fraud very smartly without letting her know, and a huge amount of money was falsely transferred. She hanged herself because she blamed herself for the loss of money [25].

In April 2018, a person JINTO JOY who runs a firm for the exchange of money at tourist spots of Varkala at Thiruvananthapuram. He uses a small hand-held device and a camera of the size and a small led bulb to steal the money from his client. He was arrested for reportedly siphoning money from a French man's (Francois Mousis) bank account by cloning his card, where he uses a camera to capture the password. In contrast, his staff uses a small skimming device to steal information on the card [26].

In April 2018, a doctor was arrested from a government institution for his involvement in skimming and ATM fraud. According to the report, firstly the doctor had made a firm and acquired five Point of Sale (POS) machines for the firm. The gang involves in the skimming and ATM fraud by using the POS machine for siphoning the money their client account. The money was deposited in the account of the doctor who takes more than 30% of the whole money, and the rest of the money was distributed among the gang member [27].

On 9 September 2017, a man named Darshan Patil has swiped his card for a toll tax of Rs. 230 at Khalapur toll plaza around 6:27 pm. By 8:34 pm, a total of 87000 have been drawn from his account. As per the record (reported at Hadapsar Police Station Pune), he doesn't receive any OTP for the transactions. Cybercriminals have performed more than 5 transactions for siphoning the amount from Patil's account. One of the security experts have explained during the swapping process; we give our card to another person for the transaction. During this process, our card is until in machine until the bill came out from the machine, and it provides enough time for a cyber-criminal to steal data from card [28].

V. Major Findings

1) Majority of ATM users does not follow the rules described by banks:

- Not more than one person in an ATM chamber for the transaction.
- A huge number of people performing transactions while using caps, sunglasses, and handkerchiefs on their faces, etc.
- Maximum numbers of ATM having no security guards to care of rules provided by the banks or to instruct the users.
- A considerable number of ATM having distorted gates, alarm systems, cash dispensers, keyboards and jammed keys etc.

2) All the points mentioned above will increase in the ATM fraud rate, i.e., by shoulder surfing, card cloning, password stealing, keyboard-jamming, and card/cash trapping etc.

3) Many ATMs have equipped with finger printer sensors and voice recognition systems; even after having such features, they are working on a single level authentication factor.

4) Recently, few banks implemented a 2FA (Two Factor Authentication) mechanism based on OTP to withdraw a certain amount. But they didn't provide any solution in case of network issues, device is lost or damaged, and any kind of accidental issues.

VI. Proposed Security Mechanism

Nowadays, there is a tremendous increase in numbers of ATM users due to the advancement in digitalization. As a result, the financial sector has moved from cash to cheque and currently towards the plastic cards [29, 30]. From the last decade, plastic cards emerged as a widely accepted mode of transactions across the world [31].

According to the times of India, there is around 9% growth in fraud rate on ATM from the year 2017-18 to 2018-2019 and causes a loss of about 21.4 crores. In addition, there is a rise in the ATM fraud case, but due to improvement in security features of ATMs or plastic cards (i.e., chip-enabled mechanism) the country has witnessed a huge decline in terms of money loss, i.e., around 305% from the last year [32].

The ease and convenience of ATM have made the financial users rely and trust on it. But at the same time news headlines are threatening about the frauds related to ATM, i.e., skimming, shoulder surfing, card swapping, and password-stealing etc. To avoid all these bluff techniques, researchers have proposed a two-tier security model. Recently some banks in India are using the OTP feature to avail cash, but they did not provide any solution in case of any failure in a particular network or any accidental issue (i.e., cell phone damage and stolen etc.), which lead to transaction failure. In the proposed framework, there is an alternative feature to avoid these types of issues by choosing the random security question from the database. The details of the framework are elaborated in the subsequent sections.

A. Working Procedure of Proposed Security Mechanism

Firstly, the bank's personnel collect the client's information, i.e., name, aadhar and e-mail, etc. In addition, they collect an activated mobile number and at least four

security questions as well as their answers. After collecting all the information from the customer, a unique database for bank clients is prepared with a unique ID. The registration process and the creation of the client's database are shown in "Fig. 1".

The proposed framework is divided into two phases. In the first phase, the authentication process is done. Whenever the bank's client needs to perform a transaction firstly, the client has to insert the card and enter the unique UID/PIN provided by the bank after that client has to select the desired transaction process. The outline of the process is mentioned in "Fig. 2".

In the second phase (i.e., verification phase), there are two ways to complete the transaction process. Firstly, with the help of OTP or in case there is accidental or some natural issues with the network or device, then the client can use an alternative method to perform a transaction (i.e., security questions). To complete the transaction process client has to authenticate with either OTP or Security Question. If the client wants to perform the transaction with the help of mobile. He/she has to select the authentication process with the mobile option, and an OTP is sent to the registered mobile. After that, a time slot of 90 seconds, as well as a counter of two attempts, is assigned in which the client has to enter the correct OTP. In addition, if the client fails to enter correct OTP in all attempts within the given time and counter, the card has been blocked for 24 hours or the client has to contact with either bank or customer care. The outline of the process is mentioned in "Fig. 3".

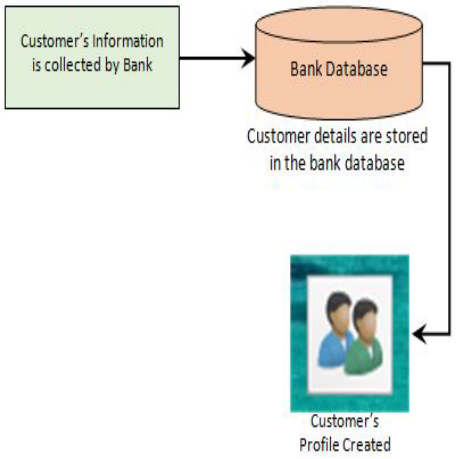

Fig. 1. Registration Process of Bank's Client.

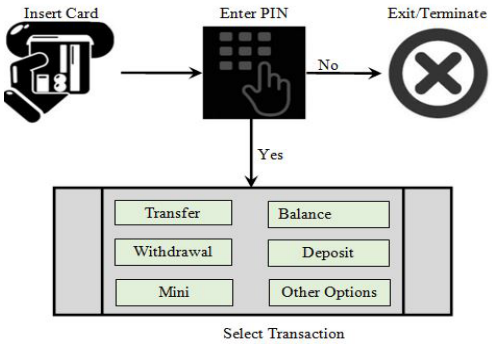

Fig. 2. First Level Authentication Process for Transaction.

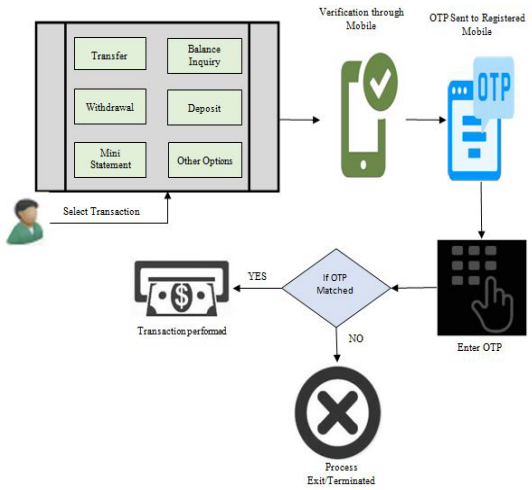

Fig. 3. Authentication Process (Via Mobile) for Transaction.

In the phase second (i.e., verification phase), if the client wants to perform the transaction with the help of a security question, then the client has to go with the security question option. A security question will be displayed on the screen from the client's database. The client has to answer the security question correctly in allotter time as well as in allotted counter to perform the transaction.

Once the security question displays it is stored in the database, either the client answers it correctly or not, it will not display in the next transaction. We have done this to avoid shoulder surfing, card swapping, cloning etc. For the security perspective, researchers have set a timer as well as in the number of attempts to answer the security question. If the client fails to enter the correct answer in all attempts within the given time and counter, the card has been blocked for 24 hours or the client has to contact with either bank or customer care. The outline of the process is mentioned in "Fig. 4".

B. Proposed Flowchart

The complete flow diagram of the proposed ATM security mechanism is outlined in "Fig. 5".

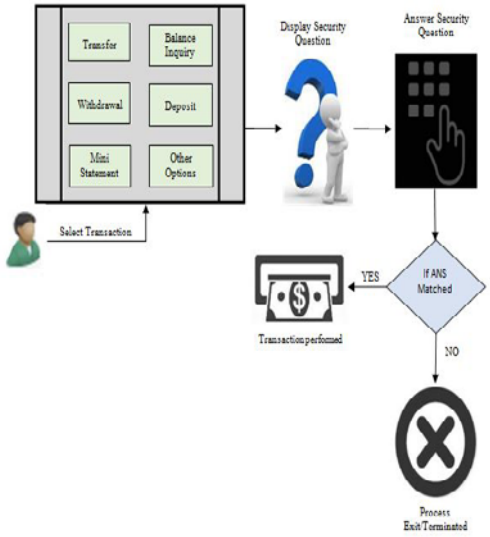

Fig. 4. Authentication Process (Via Security Question) for Transaction.

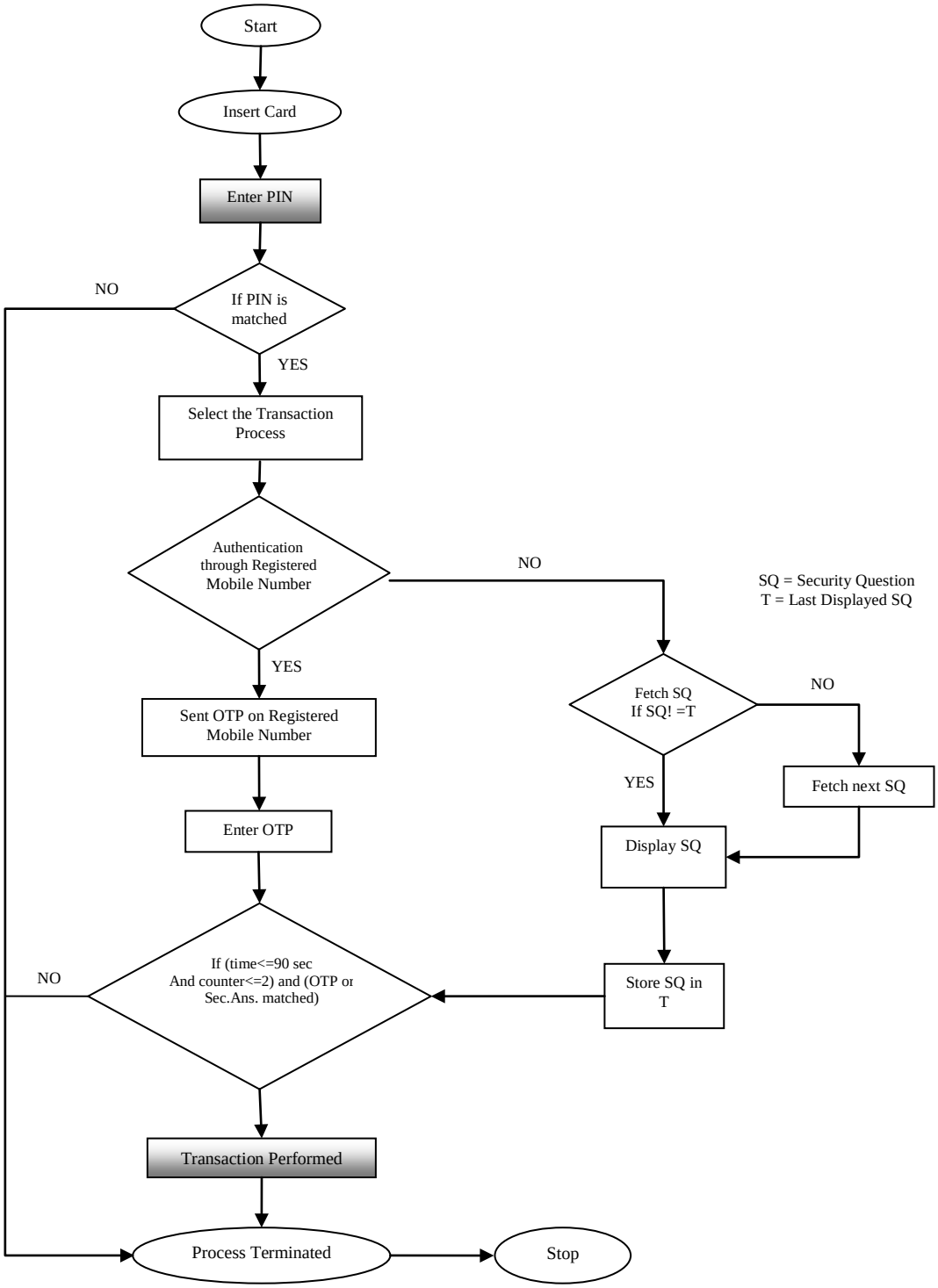

Fig. 5. Flowchart for the Proposed ATM Security Mechanism.

C. Proposed Algorithm

1. Start
2. Enter "Uid" and store in UID
3. If UID is not matched, then Go to step 22 else Go to step 4
4. Select Process
    - Withdraw
    - Mini statement
    - Pin Change
    - Etc.
5. Enter Y or N as the choice to authenticate by mobile.
6. If choice == Y then Go to step 7 else Go to step 12
7. Set the counter C=1.
8. Send OTP to the registered mobile number.
9. Start the timer for 90 seconds and repeat steps 10 to 12. If Time Elapsed, Go to step 21
10. Enter OTP
11. If OTP is matched then complete the TRANSACTION and Go to step 22

    Else if C<3, then set C=C+1. Go to step 8 for the regeneration of OTP else Call Card Block Procedure Go to 22
12. Set counter=1
13. Start Timer of 90 second
14. Repeat steps 15 to 20 till Time is not Elapsed and Counter! =3 else Call Card Block Procedure Go to 22
15. Fetch security question SQ from the database
16. If SQ! = T, then display it
17. Else fetch the next question from the database and display it
18. Enter "Enter Security Answer"
19. Save the question number in T
20. If the answer is wrong, then go to step 21 else complete the transaction
21. Process Terminate
22. Process End

VII. Conclusion and Future Scope

Due to the advancement of technology, the dependency on ATM is continuously increasing, and the banking sector is consistently encountering the risk of privacy and security. The number of cases regarding misuse of plastic cards is endlessly growing, and the security procedures applied by banks are not optimal. From the literature survey, it is revealed that the maximum number of ATM fraud/attacks is occurring at its authentication phase. Many banks have started a two-tier authentication process with the help of OTP. Still, there is an issue; if a client forgets to carry its mobile or if there is any network issue (i.e., network failure, network ban due to some circumstances) then the transaction process will become incomplete.

To avoid all these issues, researchers have presented two-tier security architecture to remove network dependencies. In the proposed framework, there is an alternative feature to avoid these types of issues by choosing the random security question from the database. Before the user is granted access to the transaction, these two authentication methods (a combination of any two, i.e., Personal Identification Number along with One Time Password or Personal Identification Number along with Random Security Question) must be affirmative. In addition, with the adaptation of this security framework, the problem of identity theft, shoulder surfing, card cloning, password stealing and illegal withdrawal of cash will be eliminated. The siphoning of this framework to the financial sector would improve the security of the ATM system and also restore the customer's trust. Future Work: The researcher is planning to further extend the work as well as testing and building a financial machine (ATM), having additional features for serving every kind of disabled person.

References

[1] R.R. Soni and N. Soni," An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Bank," Research Journal of Management Sciences, vol. 2, no.7, pp. 22-27, 2013 ISSN 2319–1171.

[2] B. Kay, M. D.Manuszak, C. M.Vojtech, "Bank Profitability and Debit Card Interchange Regulation: Bank Responses to the Durbin Amendment (2014-08-22). FEDS Working Paper No. 2014-77. Available at SSRN: https://ssrn.com/abstract=2976985.

[3] H. Leinonen,(2011) "Debit Card Interchange Fees Generally Lead to Cash-Promoting Cross-Subsidisation", European Competition Journal, 7:3, 527-557, DOI: 10.5235/ecj.v7n3.527.

[4] J. Liu, Y. Xiao, H. Chen, S. Ozdemir, S. Dodle and V. Singh, "A Survey of Payment Card Industry Data Security Standard," in IEEE Communications Surveys & Tutorials, vol. 12, no. 3, pp. 287-303, Third Quarter (2010).do i:10.1109/SURV.2010.031810.00083.

[5] S. Tchesnokov, "Advanced Approaches to ATM Network Protection" [ONLINE], Available at: https://securityintelligence.com/advanced-approaches-to-atm-network-protection/.

[6] A. Fernandes, "Biometric ATM" International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 8 Issue VI, June 2020, ISSN: 2321-9653.

[7] B. Saranraj, N. Sri Priya Dharshini, R. Suvetha, K. Uma Bharthi, "ATM Security System Using Arduino", International Conference on Advanced Computing & Communication System (ICACCS), pp 940-944, IEEE 2020.

[8] OGATA, Hisao& ISHIKAWA, Tomoyoshi & MIYAMOTO, Norichika& MATSUMOTO, Tsutomu. (2019). An ATM Security Measure for Smart Card Transactions to Prevent Unauthorized Cash Withdrawal. IEICE Transactions on Information and Systems. E102.D. 559-567. 10.1587/transinf.2018EDP7136.

[9] S. Shukla, A.Helonde, S. Raut, S. Salode, J. Zade, "Random Keypad and Face Recognition Authentication Mechanism", International Research Journal of Engineering and Technology, pp:3685-3688, 2018.

[10] K. Sangeetha, P. Jayashri, D. Vanitha, "ATM Security Using Red-Tacton" International Conference on Advancements in Engineering, Technology and Sciences, pp:427-434, 2018.

[11] K.T. Rayudu, M. Aravindan, "Enhancing Security of ATM Machines using One Time Password and Biometrics using Elliptic Curve Cryptography", -International Journal of Engineering Trends and Technology Vol.35, Number 1, pp:6-11, 2016, DOI: 10.14445/22315381/IJETT-V35P202).

[12] M. Onyesolu, A. Okpala, "Improving Security Using a Three-Tier Authentication for Automated Teller Machine (ATM)," International Journal of Computer Network and Information Security, Vol.9, pp:50-56, 2017, doi:10.5815/ijcnis.2017.10.06.

[13] M. Dutta, K. K. Psyche, and S. Yasmin, "ATM transaction security using fingerprint recognition" American Journal of Engineering Research (AJER), Vol.6, Issue: 8, pp- 41-45, 2017.

[14] N. Ahmad, A. A. M.Rifen, M. H. A. Wahab, "AES Cardless Automatic Teller Machine (ATM) Biometric Security System DESIGN using

FGPA Implementation" International Engineering Research and Innovation Symposium, IOP conference series: materials science and engineering, pp: 1-10, 2016.

[15] A. A. S. Rexlin, K. Venkatesh, M.Varatharaj, "A modified Biometrics Authentication Techniques Based on Image Processing," International Journal of Research in Electronics Vol. 3, Issue 3, pp: 14-18, 2016.

[16] K. Curran, D. King, "Investigating the Human-Computer Interaction Problems with Automated Teller Machine (ATM) Navigation Menus," Interactive Technology and Smart Education, Vol.1, No.2, pp:59-79. 2008, doi: 10.1108/17415650810871583.

[17] "How ATMs Work?" [ONLINE], Available at: https://www.elprocus. com/automatic-teller-machine-types-working-advantages.

[18] "ATM Machine" [ONLINE], Available at: https://www.pcmag.com/ encyclopedia/term/38117/atm-machine.

[19] O. Wild, "Six Types of ATM Attacks and Fraud" [ONLINE], Available At: https://www.ncr.com/company/blogs/financial/six-types-of-atm-attacks-and-fraud.

[20] S. Engelbrecht, "Latest Threat to ATM Security," [ONLINE], Available at: https://www.securityweek.com/latest-threats-atm-security.

[21] Security Information, " Card and Cash Trapping" [ONLINE], Available at: https://www.ca-nextbank.ch/en/en/security-informations/card-and-cash-trapping.html

[22] Arun Thomas, "Beware of ATM Cash Trapping" [ONLINE], Available at: https://medium.com/@netsentries/beware-of-atm-cash-trapping-9421e498dfcf

[23] Arun Thomas, "Transaction Reversal Fraud (TRF) — Don't be the next Target", " [ONLINE], Available at: https://medium.com/@netsentries/ transaction-reversal-fraud-trf-dont-be-the-next-target-a948f5a3205#:~:text=Transaction%20Reversal%20Fraud%20(TRF)%20is,by%20criminals%20to%20avoid%20detection.

[24] D. Ghosh, "Kolkata ATM fraud accused held after auto chase through Delhi Lanes" [ONLINE], Available at: https://timesofindia.indiatimes .com/city/kolkata/atm-fraud-accused-held-after-auto-chase-through-delhi-lanes/articleshow/72447447.cms.

[25] S. Bhardwaj, "Cheated of Rs 29,000 by ATM thieves, Delhi girl hangs self", [ONLINE], Available at: https://timesofindia.indiatimes.com /city/delhi/cheated-of-rs-29k-by-atm-thieves-teen-hangs-self/articleshow/64086408.cms.

[26] TOI., "Varkala ATM fraud: All they had was a skimming device and a hidden cam," [ONLINE], Available at: https://timesofindia.indiatimes .com/city/thiruvananthapuram/varkala-atm-fraud-all-they-had-was-a-skimming-device-and-a-hidden-cam/articleshow/63720572.cms

[27] B. Dominique, "Doctor arrested for ATM fraud", [ONLINE], Available at: https://timesofindia.indiatimes.com/city /puducherry/doctor-arrested-for-atmfraud/articleshow/ 63911 782. cms

[28] NDTV., "Card Fraud: Man Loses Rs 87,000 After Swiping At Pune-Mumbai Toll Plaza" [ONLINE], Available at: https://www.ndtv.com/mumbai-news/card-fraud-man-loses-rs-87-000-after-swiping-at-pune-mumbai-toll-plaza-1749098

[29] F. Twum, K. Nti, &M. Asante, "Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication" International Journal of Science and Engineering Applications, 5(3), pp. 126-134, 2016.

[30] Mohd Waris Khan, D. Pandey and S. A. Khan, "Test Plan *Specification* using Security Attributes: A Design Perspective," ICIC Express Letters, no.12 (10), pp. 1061-1069, 2018.

[31] D. O. Mahony, M. Peirce, &H. Tewari, "Electronic Payment Systems for E-Commerce." 2nd edition. Boston, London: Artech House, 2001.

[32] S. Bhardwaj, "Maharastra tops in ATM frauds, Delhi second" [ONLINE], Available at: https://timesofindia.indiatimes.com/india /maharashtra-tops-in-atm-frauds-delhi-econd/articleshow/70322347.cms