Extraordinary Authentication and Security to Credit/Debit Cards with Biometric and Two Step Verification: Review

Dr. Rahul Mapari[*1], Rahul Parbat [#2], KiranNapte [*3]
[#*]Department of E&TC Engineering, PCCOE&R, Ravet,
Savitribai Phule Pune University, Pune, Maharashtra, India
[2]rahul.parbat@pccoer.in
PCCOE&R, Ravet, SavitribaiPhule Pune University, Pune, Maharashtra, India
[1]rahul.mapari@pccoer.in
[3]kiran.napte@pccoer.in

***Abstract*—In this paper, a strong authentication and security to credit/debit cards with biometric verification along with emergency-mode for Automated Teller Machine (ATM) cash payment withdrawal gateway and point of sale (POS) based payment gateway for commercial and business banking applications are exposed. When consumer with biometric based credit/debit card is willing to make a cash payment withdrawal, then he is allowed to make self-authentication by means of finger print verification. After successful verification of finger print credentials, ATM machine will ask to enter the PIN for successful cash withdrawal of individual user. If credit/debit card is used by the siblings of account/card holder then they can be authenticated for cash withdrawal based on their biometric registration at bank or using the emergency mode under the one time password and/or web based security code acknowledgement capability. Two step web based verification also provided in case of accessing the credit/debit card by joint account holders. If any one of account holder willing to make a transaction then withdrawal can be acknowledged by sending the verification code to another account holder by means of one time password or verification code alert. Transactions can be declined in case of unforeseen cash withdrawal request by terminating verification code. If more than two fraudulent transactions are identified then, system will allow marking the response and sending the fake transaction details to bank for further constabulary's processes.**

Keyword - Biometric ATM, Joint Account Holders, Two Step Verification, Fraudulent Transactions.

I. INTRODUCTION

A credit/debit card is more secure to carry than money. In existing cash withdrawal methods using credit/debit cards, the RFID based proximity cards are being used along with the 16-digit card identification number and information with card verification value (CVV) numbers [1]. Credit/debit cards can work in two way mode including cash withdrawal at ATM machine and purchasing a things and goods by means of point on sale (POS) [2].

Currently monetary organizations will attempt and shield their client from credit/debit card misrepresentation. Current systems uses the magnetic strip based identification and personal identification number (PIN) solution to debit money from ATM machine or purchase things at POS point of customer interest [3]. Now, PIN number secures the transaction as PIN is provided for personal use of credit/debit card. Current systems also allow Unified Payment Interface (UPI) with highly encrypted UPI PIN's and OTP based security for online money transfer and bill payments at point of sale. This UPI system always asks the credit/debit card information to interface with the customer and merchants [4]-[5].

Finger impression based ATM machine is an application where biometric finger print mark of the client is utilized as a validation and confirmation at automated teller machine while willing to cash withdrawal. Rather than utilizing credit/debit card fingerprint based automated teller machine is more secure and protected. There is no stress of losing credit/debit card and no compelling reason to convey credit/debit card in your wallet [6]. Most monetary institutions will try and protect their customer from debit card fraud. Section of ISO 7816 indicates safety allied recommendations to be utilized for individual authentication and verification of biometric techniques in coordinated credit/debit cards. It likewise embodies the authentication data structure and access techniques for utilization of the card for the biometric reference and additionally as the gadget to execute status of cardholder's biometric test [7].

II. METHODOLOGY OF PROPOSED INVENTION

Current running ATM systems are not using the biometric recognition and emergency mode. Using credit card and password, system cannot verify the client's identity exactly. In recent years, the algorithm that the fingerprint recognition continuously updated and sending the four digit code by the controller which has offered new verification means for us, the original password identification technology verify the clients' identity better and achieve the purpose that use of ATM machines improve the safety effectively [8]-[9].

The use of fingerprints as biometric is both the oldest mode of computer-aided, personal identification and the most prevalent in use today. In the world, today, fingerprint database is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examinations, operation of bank accounts among others.

This work is committed to succeed extraordinary authentication and security to credit/debit cards with biometric and two step verification (emergency-mode) for automated teller machine. In our system, Emergency mode is included when the owner of ATM card is not actually available at the time of accessing his own account. The service of Emergency mode is having proper cost and limitation according to rules of bank, so anyone cannot misuse this facility. When third person wants to access ATM card without having presence of owner, then it has to press Emergency Mode button, after inserting ATM card. After pressing Emergency button one text box will be open where a third person has to give his own mobile number. Then bank will send a message to the owner of ATM card and ask whether authentication to the third person has to provide or not.

ATM owner will reply to bank and reply can be of following type:

- If owner gives positive reply then account is accessible to third person.
- If owner gives negative reply then alert message will be send to bank and appropriate action will be taken on third person.
- If owner does not give any reply to bank then alert message will send to owner of ATM and bank and appropriate action will be taken on third person.

Debit Card/Credit Card Views including Front View and Bottom Views illustrating the Magnetic Strip, Fingerprint Scanner, Power Supply Slots and RFID Tag is shown in figure 1 relating: 1: relates to Front View of Card, 11: relates to Power Slot for Biometric Sensor, 12: relates to Power Slot for Magnetic Strip, 13: relates to Magnetic Strip, 14, relates to Biometric Sensor, 15: relates to Card Owner Information, 16: relates to Power and Data Pins for Biometric Scanner, 17: relates to Power and Data Pins for Magnetic Strips, 18: relates to Power Lines for Biometric Scanner, 2: relates to Back View of Card [3]-[4].

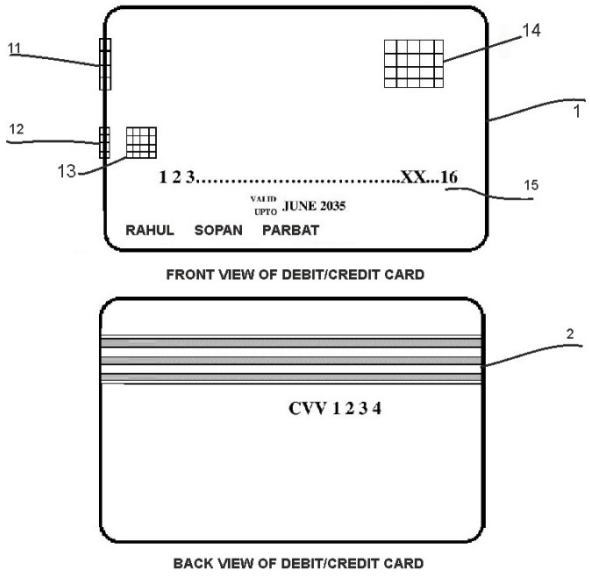

Fig. 1. Debit Card/Credit Card Views

Fig. 2 shows Power Supply, CPU, Memory Interfacing with ATM tray in which 16: relates to Power and Data Pins for Biometric Scanner, 17: relates to Power and Data Pins for Magnetic Strips, 18: relates to Power Lines for Biometric Scanner, number 19: relates to Power Lines for Magnetic Strips [3]-[4].

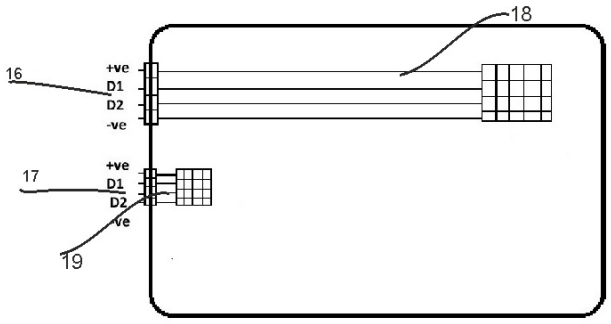

Fig. 2. Debit Card/Credit Card Power and CPU interfacing Considerations

A. Terminology

1) *Power Slots and Power Lines:* SLOT I and SLOT II are used to power supply, Read/Write operation for finger print scanner and to magnetic strip. Slots avails the power form ATM holder Tray to carry out the functioning form card. Power can be supplied with integrated technologies.

2) *RFID TAG:* Card has total size of 85.60mm × 53.95 mm with 15.82 mm of RFID tag zone.

3) *Magnetic Strp:* Magnetic strip is used to avail the Point-on-Sale (POS) service for making the payments.

4) *Biometric Sensor:* A biometric gadget is a security authorizations and confirmation tool. Such gadgets are utilized in in the invented system for confirming or perceiving the individual dependent on a physiological trademark.

In the invented system our main aim is to improve the authentication in ATM system by providing the extreme security. Main advantages includingbiometric finger print reader is placed over the credit/debit card and can be energized by utilizing the ATM holder tray of automated teller machine. Also we are allowing credit/debit card to operate in two stages: one stage for user verification by means of biometric identification; second stage for account validation linked to the card.

III. Summary of Operations and Discussion

Proposed Debit/Credit card shown in fig. 1 is identical to the ATM card in the market and has biometric scanners and magnetic strips When the ATM owner wants to withdraw money, he will take his ATM card and go to the ATM premises. While operating, user has to go for their own verification by putting his card on ATM holder in the tray and wait for his verification for. Fig. 3 shows the Pass I of operations showing holding mechanism of card while fig. 4 shows Pass II of operations showing holding mechanism of card.

The user biometric data of bank account/ATM card holder is already registered at bank side during the opening of bank account and it is stored on shared database of bank to ATM network. User needs to select the one of mode operation within 3rd party emergency mode and/or sibling biometric authentication mode for self-authentication process to be carried out. While transaction is to be process, user has to put his finger on the ATM's biometric sensor and put the card in the ATM holder tray of ATM machine. The biometric sensor and RFID TAG collaboratively energized by the power lines and the slots available on the ATM card. Proper interfacing can be done with power slots of ATM tray by means of connectors. User is allowed entering a half portion of card into ATM holder tray for biometric verification process.

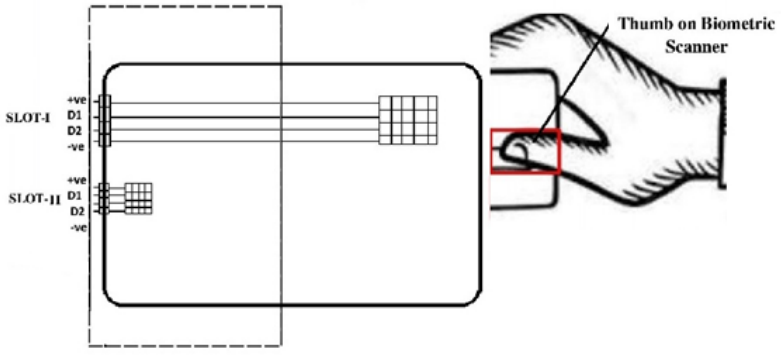

Fig. 3. Pass I of operations showing holding mechanism of card

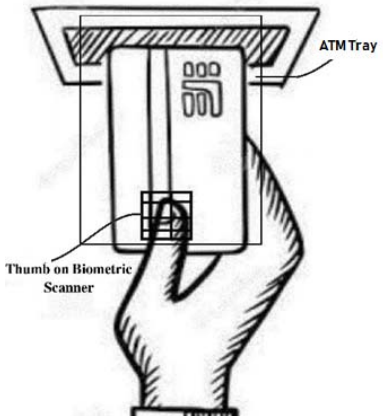

Fig. 4. Pass II of operations showing holding mechanism of card

If the user who uses the ATM card has a valid fingerprint of the same, then the system will allocated that user with the machine and acknowledge him against biometric authentication and will get permission for further processes of transaction.

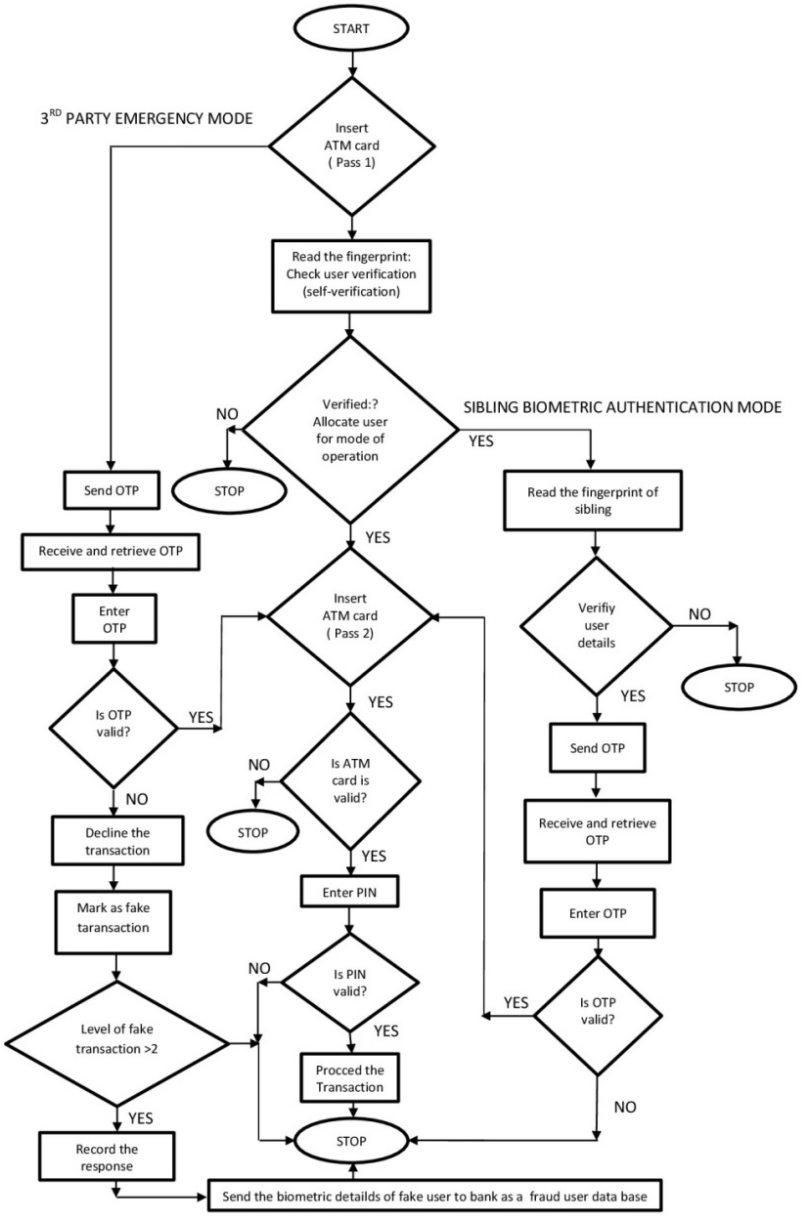

Fig. 5. Flowchart of operations that are carried out in Pass I

As per the authentication status, if user is valid then he can go with its transaction, 3rd Party Mode of Transaction or Sibling Mode of transaction. User has to push the card inside the ATM tray (Pass II of operation) to verify the ATM working status. Once the user has been verified, he can type his ATM PIN and proceeded for withdrawal of money from the ATM machine. Moreover if fingerprint is not verified then it will discard the user transaction.

If ATM card user wants to be transitioned from someone close to him, then then he will take the third party's emergency mode of operations to withdraw money from ATM machine with OTP based processes. ATM machine will send out the OTP to the prime card holder under the 3RD PARTY MODE OF OPERATION. The OTP can be POP-UP based flash notification in which there will transaction PROCCED and DECLINE options. If owner of card proceeds the transaction then and then only Pass II operation for money withdrawal can be succeeded, otherwise it will mark as FAKE TRANSACTION and store the response if user done more than two transactions. The stored data of fraudulent user will be sent for bank and ATM owner for further security aspects.

If card owner want to withdraw money from his siblings, then our system has provided the SIBLING BIOMETRIC AUTHENTICATION MODE. The fingerprint verification of card owners sibling also present during the account opening process at the bank. Sibling needs to de his self-biometric verification to be done during the withdrawal of money at the ATM machine. If Pass I of operation has been succeeded then card owner get POP-UP based flash notification in which there will transaction PROCCED and DECLINE options. User can select TEXT based OTP for authorization of his sibling while withdrawing the money form ATM machine. If owner of card precedes the transaction then and then only Pass II operation for money withdrawal can be succeeded, otherwise transaction will be declined.

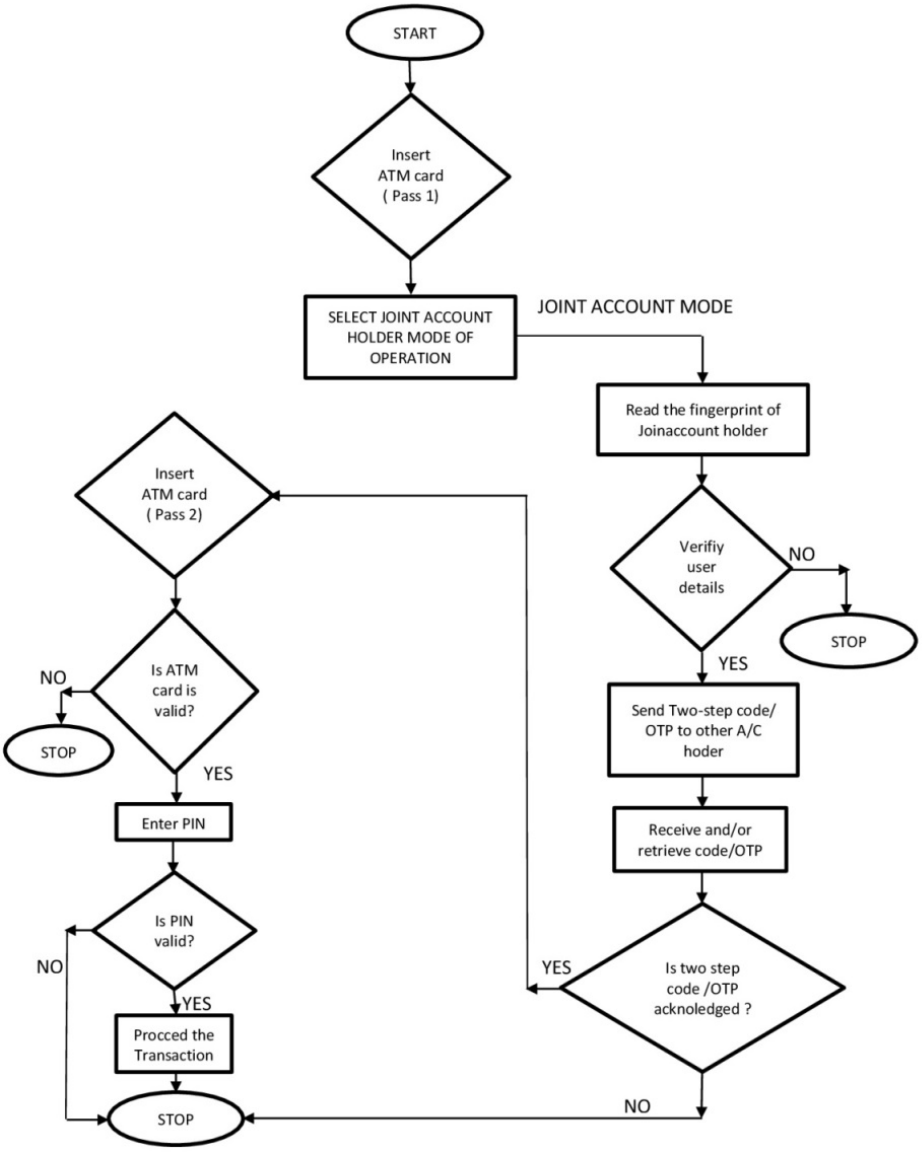

Fig 6. Flowchart of operations that are carried out in Pass II

Detailed flow of operation is summarized in flowcharts shown in fig. 5 and fig. 6. User has to authenticate himself after selecting the JOINT ACCOUNT HOLDER MODE OF OPERATION. After verification of user; two-step code is allowed to send by ATM machine to another account holder as a flash notification/OTP. These codes will be acknowledged by another user to approve the current user to allocate and authenticate card holder for transaction to be done.

IV. CONCLUSION

Biometric based debit/credit card is used in the invented system giving precise and challenging solution against monetary frauds. Biometric finger print reader is placed over the credit/debit card and can be energized by utilizing the ATM holder tray of automated teller machine. In our system emergency mode for third party transaction is provided to authenticate the user transaction. Message alarming feature is proposed with 4-digit code as a message to the mobile of the authorized customer without any clatter in order to access the ATM machine. Prime account/card holder is allowed to scan the finger print details of their siblings or family members for accessing the card under emergency mode of operation. Generated OTP under the emergency mode need to be submitted/approve to avail the successful withdrawal capability. Our system provides two-step verification based codes for user verification in case of joint account holders. If user approving the received two-step verification code then and then only transaction is proceeded otherwise our system will mark this as a fraud transaction and thereby transaction declined. Thereby transaction can be followed by user biometric verification then authorizing the user for transaction and allows the emergency mode of operation for non-exclusive user along with two-step verification based security to joint account holders.

REFERENCES

[1] Reserve Bank of India – Report on: Working Group on Securing Card Present Transactions,2011. [Online]. Available: https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/SCP020611FS.pdf
[2] Fumiko Hayashi, Richard Sullivan, and Stuart E. Weiner, “A Guide to the ATM and Debit Card Industry”, Payments System Research Department, FEDERAL RESERVE BANK OF KANSAS CITY, Missouri, USA, 2003.
[3] ISO 20022 Manual: Universal financial industry message scheme, SO 20022 Cards and Related Retail Financial Services messages. [Online]. Available: https://www.iso20022.org/cards_and_retail_messages.page
[4] ISO 3554:1976Cards and security devices for personal identification Committee Report: Credit cards- Magnetic stripe encoding for tracks 1 and 2. [Online]. Available: https://www.iso.org/standard/8957.html
[5] Yun Yang andJiaMi, “ATM terminal design is based on fingerprint recognition”, 2nd International Conference on Computer Engineering and Technology, IEEE, 2010.
[6] Ron Zoka, “Touch Scan Internet Credit Card Verification Purchase Process”, U.S. Patent 2002/0062291 A1, May 23, 2002.
[7] Will Shatford, “Biometric AuthenticationProxmity Card”, U.S. Patent 2008/0028230 A1, Jan. 31, 2008.
[8] Abiodun Daniel walloye, “I-Card (Biometric and Contactless Credit and Debit Cards)”, U.S. Patent 2013/0056539 A1, Mar. 7, 2013.
[9] Christiawan,BayuAji Sahar,Azel Fayyad Rahardian,ElvayandriMuchtar, “Fingershield ATM – ATM Security System using Fingerprint Authentication”, International Symposium on Electronics and Smart Devices (ISESD), pp. 1-6, IEEE, Oct. 2018.