International Journal of Research in Engineering, Science and Management
Volume-3, Issue-6, June-2020
www.ijresm.com | ISSN (Online): 2581-5792

Virtual ATM Card - The Next Generation Security

A. Mahammad Shafi[1], U. S. Sagar[2*], Jayashree Ganapathi Naik[3], R. Tejas[4]
[1,3,4]*B.Tech. Student, Department of Computer Science and Engineering, Srinivas Institute of Technology, Mangaluru, India*
[2]*Assistant Professor, Department of Computer Science and Engineering, Srinivas Institute of Technology, Mangaluru, India*
*Corresponding author: sagar.udupa@gmail.com

***Abstract*: Credit card deception is a common problem in today's world. Financial institutions have registered major loses till today due to users being exposed of their credit card information. Based on the data, the bank convoyed a community to simple transaction payment in the market. Bank just used a debit card or a credit card for carrying out the transaction or other ATM services, the banks need more investment for infrastructure and, it is very expensive. Based on that cause the bank needs another solution for low-cost infrastructure. Obtained from solutions that, the bank implementation QR Code authentication online is one solution that fulfills. This application is used for carrying out transactions or other banking service purposes by the account holder. The transaction permits in this study lie in the encryption, or decryption transaction permission and QR Code Scan to uplift communication security and transaction data.**

***Keywords*: Banking, Android app, security, QR code scan.**

1. Introduction

The digital virtual ATM card plays an influential character in securing the account of the customer. Credit card dishonesty is a common problem in this today's world, we see Shoulder-surfing or observation attacks, including skimming and video recording with the tiny hidden cameras while the users perform PIN-based authentication at ATM termini is one of the common threats for common users. Researchers have strived to come up with reliable solutions for secure PIN authentication. In this paper, we introduce Security PIN Authentication for providing security for account holders by using virtual ATM cards and connecting Smart Phones. QR Code is the label for a type of matrix barcode. A QR code is a machine-readable optical label that holds information about the item to which it is imputed. Security PIN Authentication allows a user to scan a QR code from the screen of a point-of-service termini and connects to the bank's server. Security PIN Authentication server to obtain secure one-time-use PIN templates. Here, a PIN template is a sequence of digits with marked positions for the user to enter the actual PIN code. The QR code scanning is done using mobile devices. The virtual ATM card is also used in Security PIN Authentication service that are used via smartphones.

2. Proposed System

The customer uses an android application for the transaction. The bank uses the website to track the customer transaction. Both the user and bank are linked to the same database. When the users scan the QR code in the ATM, Bank server provides secure authentication and asks for security pin to user in android application. After verifying the pin automatically allows the user to access the ATM. After this transaction database automatically update the card number so that the security increases.

3. Literature Survey

A. *Electronic Payment System*

Electronic payment refers to the mode of payment, which doesn't include physical cash or cheque. It includes debit cards, smart cards, credit cards, etc. It provides encryption, and requests for more identification in case of doubts. Compare the credit card issuing bank's country with billing address country. The risk in electronic payment is the theft of payments data, personal data. The successful implementation of EPS depends on how the security and privacy dimensions perceived by consumers as well as the seller adequately managed [1].

B. *Mobile Wallet*

Leveraging new technologies connects directly to a productive software experience in the customer's hand to help enhance their experience and educate them. A customer can utilize all of their stored information only by opening an app on their phone. Entering a pin, password or fingerprint and then selecting the information they need to access. The app will utilize information transfer technologies such as Near-field communication to interact with mobile wallet ready payment techniques. This results in reduced fraud since mobile wallets are harder to steal or duplicate than cards. A disadvantage is that only mobile-service people can use such services [2].

C. *Biometric Detection*

This paper examines policy regarding the biometric approaches towards automated teller machine (ATM) for

trustworthy and secured transactions. This project provides a breakthrough against current technology in ATM and able to provide reliable protection for upcoming future ATM and Adds a GPS model. This increased security and proposed a method to find a way to replace the current model of ATM and PIN [3].

D. Electronic ATM

A self-service technology in functional service delivery usually adopted by functional institutions to reach their customers outside the banking hall. This paper presents the conceptual framework of design, specification, and model of the EATM system that uses no card. This enhances the use of ATM by banking customers. ATM fraud and criminal activities can be reduced or eliminated altogether. It will eliminate financial burden placed on customers for issuance and maintenance of the ATM card [4].

E. Fraud Currency Detection System

Nowadays, we are aware of the ATM, which makes the task of money withdraw more flexible, but to deposit money into a bank account, we have some traditional methods like the manual procedure of deposit in a bank and a modern method of e-banking. The goal of this project is to construct a simulation model to deposit money to an account in ATM itself. This Secure as user login is validated. It performs all banking transactions with a single click and also is Portable and hence can be accessed wherever available. Currency checking makes MTA more efficient. (MTA-money to ATM) [5].

F. Unified Payment Interface

Demonetization there was a massive requirement for currency notes, but government was unable to provide required quantity of currency notes, and also Indian government wanted to promote cashless transactions. Unified Payments Interface (UPI) is a payment system launched by National Payments Corporation of India and regulated by the Reserve Bank of India, which facilitates the instant fund transfer between two bank accounts on the mobile platform. UPI is built over Immediate Payment Service (IMPS) for transferring funds using Virtual Payment Address (a unique ID provided by the bank), Account Number with IFS Code, Mobile Number with MMID (Mobile Money Identifier), Aadhaar Number, or a one-time use Virtual ID. A MPIN (Mobile banking Personal Identification Number) is required to confirm each payment. Excitement over the growth of mobile payments perpetuated the phenomenon of disconnected Islands and disjointed experiences. With UPI there is no need for any other payment app at all [6].

G. Automated Teller Machine

We have surveyed different ATM of various banks to check the existing protocol and working of existing machines. It is based on two points, A) Facility or services like cash withdraw, balance inquiry, card to card payment, and other services provided by ATM & B) How user's privacy is secure when he does the operations on ATM? According to a well-known ATM manufacturer Die bold, these have 4 threats- Fake ATM, Shoulder surfing, Skimming Devices, and Fake keypad overlay attack. We have considered 5 banks- State Bank of India, Punjab National Bank, IDBI Bank, ICICI Bank, and City Bank. Attacks on ATMs such are Fake ATM, Shoulder Surfing, Skimming Devices, Fake key-pad overlay attacks.

4. System Implementation

This proposed system is designed in a way that the user can use the virtual ATM card for online transactions such as paying bills or fund transfers as shown in figure 1.

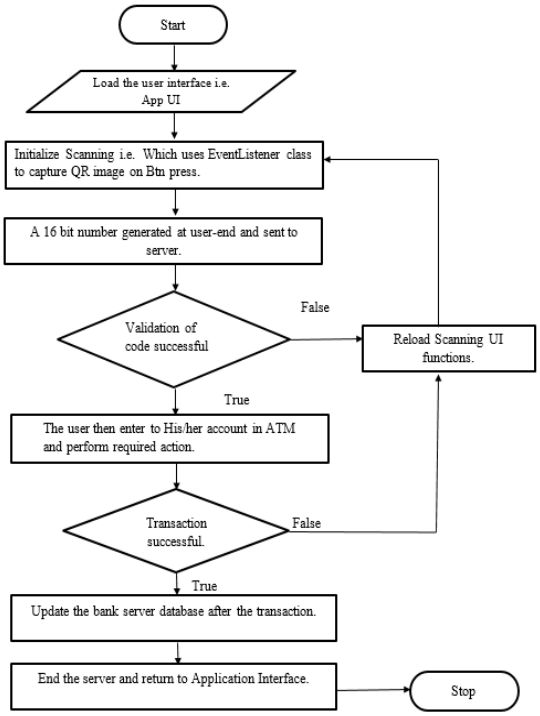

Fig. 1. System Implementation of Virtual ATM Card

A Secure PIN Authentications Service enables obscured PIN authentication for ATM using personal mobile. Implementation is done in 3 phases. The first phase including the design of the GUI for the end-user to scan the QR image in the ATM, the second phase deals with the implementation of a formation of 16-bit Random digit and third phase involves in connection to the server by entering the pin, the bank server checks the authentication and process the transaction. The user to scan a QR code from the screen of a point-of-service terminus and connects to the bank's server to obtain secure one-time-use PIN templates. Here, a PIN template is a sequence of digits with marked positions for the user to enter the actual PIN code. The QR code scanning is done using mobile devices. The protocol is immune to observation attackers and ensures resistance against relay and replay attacks. The bank server will authenticate whether He/she is a legitimate user by challenge-response technique to verify the bank account holder. After

reading the QR code, the system will load and validate the QR code. The user identity is matched then the user will get the pin entry option. Then the customer can perform the requisite activity that He/she wishes to achieve. After the transaction Bank system updates the customer's account details in the database. If the Identity is not matched, the user account and android application will be blocked.

5. Working

Fig. 2. shows the system architecture of Virtual ATM Card. We have provided a mobile application and a website. The customer can download the app or the website according to their convenience. The customer after downloading this application /app into their mobile phones, they are asked to scan the QR code present in the ATM. When the customer scans the QR code, a 16-digit number is generated, which is matched with the number which is already stored in the bank server. This happens in the validation process of the QR code, to get connected the bank system. Then the bank system provides the authentication to the customer, only if their numbers gets matched. So then the customer will be allowed to perform transactions.

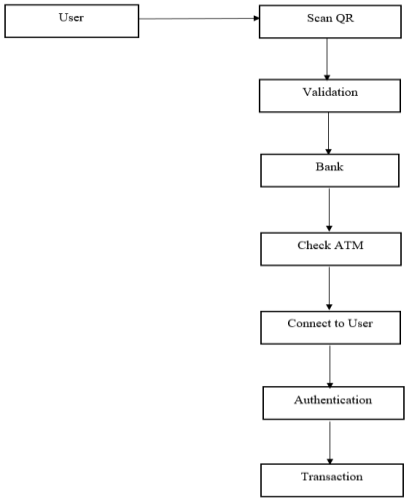

Fig. 2. System architecture of Virtual ATM Card

After the transaction Bank system updates the customer account details. The acknowledgement regarding the transaction is sent to the customer so that the customer gets to know whether it's a successful or failed transaction. On a successful transaction, customer's account details gets updated in the bank system. On a failed transaction, the customer details are not updated, where the system reloads the UI function. After finishing all the process the customer can logout of the application. Using this same app the customer can also do online shopping, where the customer can do the transaction using the Virtual ATM Card technique itself.

6. Results

We have prepared an application and a website that will help the customer to do the transaction without the use of an ATM card. The output of this web application and app is as shown below.

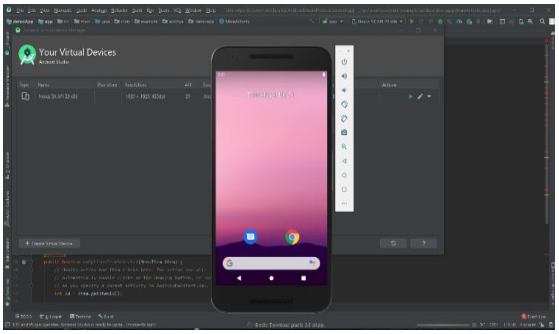

Fig. 3. QR code scanner app

Fig. 3, shows the App interface developed using android studio tool that is used scanning the QR code present in an ATM screen for carrying out transaction by the customer.

Fig. 4. System home page

Fig. 4, shows the system home page for visiting the customer account in a web interface.

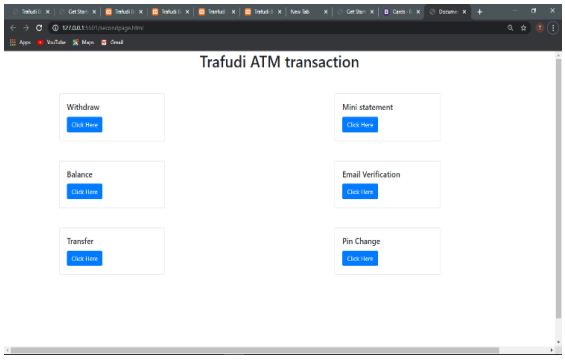

Fig. 5. Customer account option

Fig. 5, shows the system providing an option for a customer to take action concerning His/her account such as cash to withdraw, mini statement, etc.

Fig. 6, shows the virtual card details of the account holder, card holder name, CVV, card expiry, and 16-bit random number generated by the system that will be used for authentication during transactions.

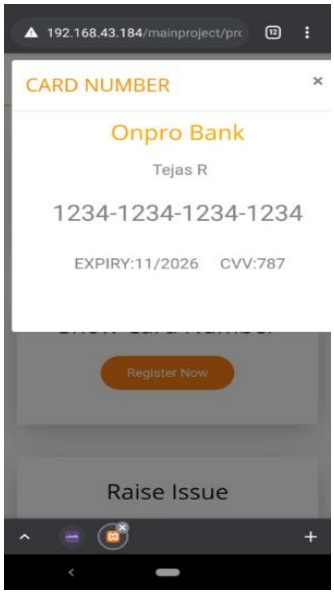

Fig. 6. Customer V-Card details

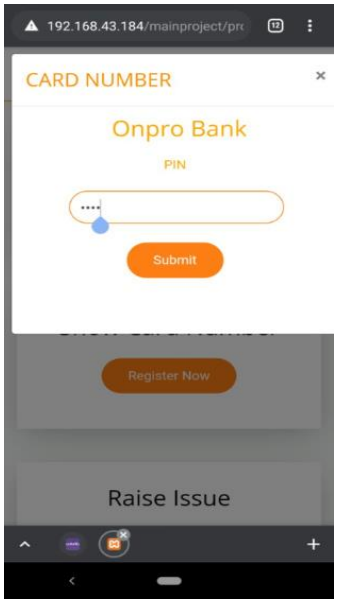

Fig. 7. Customer V-Card details

Fig. 7, depicts the UI for customer to enter the PIN to access His/her account for transaction.

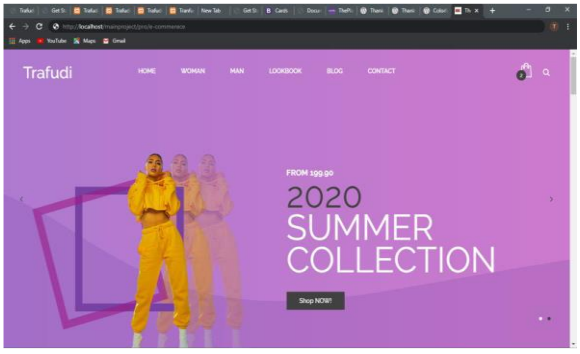

Fig. 8. E-Commerce home page

Fig. 8, shows the E-Commerce Home Page to the customer.

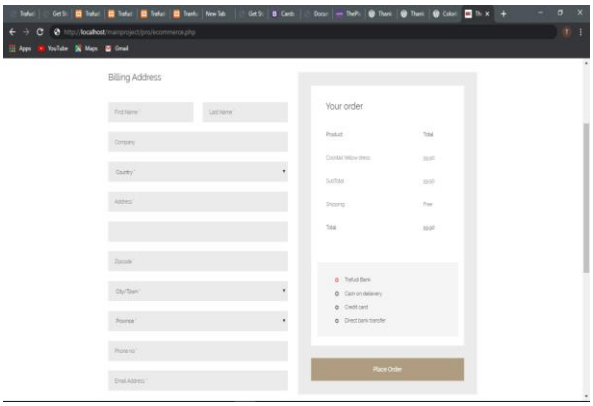

Fig. 9. E-Commerce billing page

Fig. 9, shows the web based platform that allows customer to do online shopping transaction through Virtual ATM Card Techniques.

7. Conclusion

The progress in science and technology is a non-stop process. New things and new technology are being invented. As the technology grows day by day, we can imagine about the future in which things may occupy every place. This project is implemented in a way that the user must carry their phone to the ATM's to do the money transactions. In case the user's phone is lost or hacked, it would be difficult to do the transactions. So the future scope of the project is that, even though we have finger print, iris, speech and face recognition system our phones get hacked through social media's. Hence it may be a problem for the user in the future, if his/her phone is hacked, or maybe even lost, which leads to theft of the money present in user's account. So we can implement a finger print, iris, speech or face recognition system in the application, which makes the application more authentified.

References

[1] Adrian Banarescu, "Detecting and Preventing Fraud with Data Analytics", 2015.
[2] Saleh Al-Furiah, Lamia AL-Braheem "Comprehensive study on methods of fraud prevention in credit card e-payment system", ACM, December 2009.
[3] Pratiksha L. Meshram, Tarun Yenganti "Credit and ATM Card Fraud Prevention Using Multiple Cryptographic Algorithms", IJARCSSE, pp. 1306-1313, Volume 3, August 2013.
[4] Aman Srivastava, Mugdha Yadav, Sandipani Basu, Shubham Salunkhe, Muzaffar Shabad, "Credit Card Fraud Detection at Merchant Side using Neural Networks", IEEE, 2016.
[5] Raghavendra Patidar, Lokesh Sharma "Credit Card Fraud Detection using Neural Network", NCAI2011, Vol. 1, June 2011.
[6] Gabriel Preti Santiago, Adriano C.M. Pereira, Roberto Hirata, "A modelling approach for credit card fraud detection in electronic payment services", ACM, April 2015.