# Improving CIA Triads In ATM Using Quick Response Code

**S.R.Kirthiga[1], S.Janani[2], D.Vetriselvi[3]**
[1, 2, 3] Dept of Computer Science and Engineering
[1, 2, 3] Jeppiaar SRR Engineering College, Chennai.

***Abstract-*** *The way of using smart card for money related transactions in ATM has adverse problems on authenticating and maintaining confidential assests of a user. Therefore through the use of peeping assails and shoulder-surfing attacks, the secret code is robbed and even bargained through phishing. And so, we mediate to refine a validation theory to banks which in turn helps to protect the user's data. We tend to make a system that a Quick Response Charter where the user's information are encrypted and a Mobile Application in the user's Mobile device is used to decrypt the information. This process involves sending etiquette quick response information to the server, thereby the transaction is done. Now the customer can easily enter information to transfer money securely by scanning the QR Cryptograph on the ATM mechanical machine. Here encoding and decoding process is done by 3DES Algorithm.*

***Keywords***- security, ATM, privacy, authentication, trust, Quick Response Charter;

## I. INTRODUCTION

The major scope of the proposed project is that a user's assests are secured and maintained confidential without the risk of peeping assails in Automated Teller Machine(ATM). In today's world, banks are immovable part of our life and ATMs can be used to deposit, withdraw and so on. ATMs are more utilized as it paves way for using numerous bank accounts of different branches on a same ATM mechanical machine. Therefore while transferring through ATM machines, it authenticates the authorized user. This process of authentication has various problems in using Personal Identification Number(PIN). Sometimes by shoulder-surfing attacks this private PIN code is stolen. The pattern acknowledgement approach is used to analyze the next higher level of data. Thereby, the Quick Response(QR) charter is utilized for easy and convenient verification and validation process. Hence the transaction in the ATM is being kept secured from phishing and peeping assails in turn protecting user's private data.

## II. EXISTING SYSTEM

The existing system comprises of the conventional method of using Automated Teller Machine i.e., ATM which we use nowadays. It has various security while making transaction. As far as money related transactions are concerned, they should be very secured and the confidentiality of user data is the major requirement. Only the user will have reliability and confidence to transfer money through banks.

Even it has the setback that the customer's personal information is leaked through phishing sites and spyware such as keylogger. This causes vulnerability to the customer. And in some cases the user is unaware of their personal private data from being stolen. So the idea in providing a secure transaction is to allow only the authenticated user to perform transaction. The major issue lies in validating the user that he/she is a legitimate user or not.

The system which we use currently has some security attacks prevention mechanisms like the use of OTP number, SMS banking. These techniques are used to send information to the user. OTP is the One Time Password which is valid for only a particular time period within which the password persists. After that the password gets expired, as this secret code has the vulnerability of being hacked or stolen by unauthorized users. In order to be precautious to this, one time passwords are sent to user's personal mobile device and this code is asked to enter at the time of validating the particular user. This one time password is either sent to user via SMS or through a voice call. Once the enters the secret code is received by them on their personal device, it is verified whether the user is a legitimate user or not.

The another aspect of alerting the user is sending messages to the user's mobile device through Short Message Service called SMS. For this purpose, the user need to register his mobile with his/her account no. with the bank. When the user withdraws or deposits and if any transaction is made on the account, the user is notified by sending a SMS.

If some unauthorized person uses his account, the user becomes aware of it when he/she comes to know that

some manipulation is being in their bank account. So that they could take appropriate steps to bring their account under their control.

Sometimes one time password is sent through messages to unlock the locked user account. These are the problems we faces in today's situation in dealing with logging as an authenticated user to our account. So the way of giving privileges to the authorized user and authenticating the user plays a vital role in providing security to the account. They are the strategy to render privacy to the user. Therefore maintaining the user's private data like their personal information and bank account details are kept confidential. And the user will have reliability on the bank to provide their data fearlessly.

## III. PROPOSED SYSTEM

The proposed system consists of a Quick Response charter in the ATM mechanical machine. Once a customer enters the ATM, he/she is allowed to scan the encrypted QR code using a mobile application. And if the user is a legitimate user, it decrypts the code and shows the corresponding user's information on the ATM monitor screen. This Quick Response code is the separate one for each and every user who enters the ATM to make transaction from time to time. This code is generated by dynamic token generator.

### *A. Setbacks with the existing system*

In the existing system, people used to go to the ATM for withdrawing money and they will be allowed to swipe the smart cards of any bank or from any branch. Once the card is swiped, the customer is authenticated using PIN number, which is given to the user at the time of issuing the card by the bank.

Here, when the user enters PIN number into the ATM mechanical machine, their secret code can be stolen by means of peeping attacks.

Even it has the setback that the customer's personal information is leaked through phishing sites and spyware such as keylogger.

### *B .Architecture Diagram*

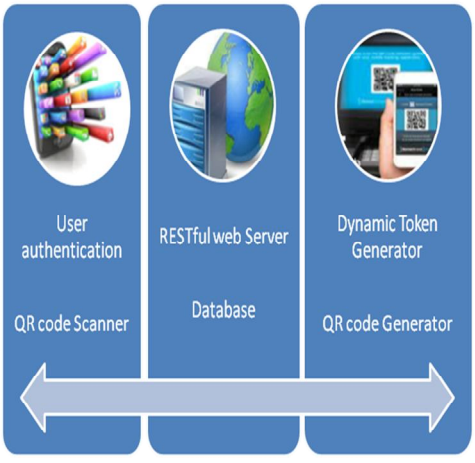
The system constitutes an architecture of an ATM machine, web server, database of bank storing credentials and an android mobile application. This involves the interaction of android mobile application with ATM machine through a web server. The mobile application has two tasks to perform namely authenticating the user and scanning the QR code displayed on the ATM. And ATM machine generates separate code for each and every user dynamically using dynamic token generator algorithm.

This dynamic token is the same for all users, it varies to different users. The web server links with the database and bank website for making the authentication process. It provides a collaborative service of interfacing the android application on the mobile device and ATM mechanical device.

This strategy allows the user to register their account in the bank database. Initially the user is given with the account number and the user need to install the mobile application in his/her mobile device and an OTP is used to verify the user while in the registration process. Then the user can change the password accordingly. These are the steps that involves for registering firstly.

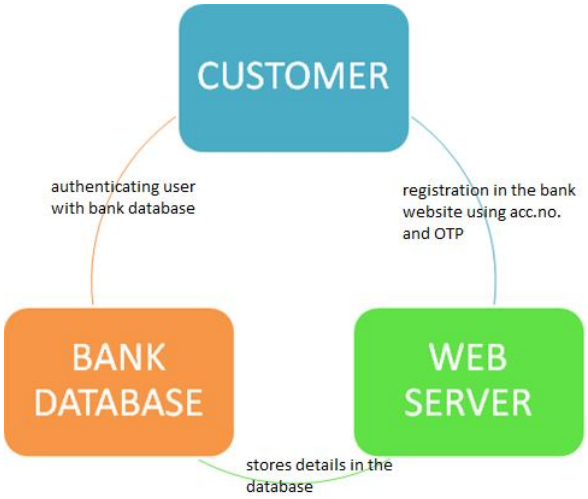
Now the user can withdraw money for ATM using their own authenticated mobile device. When the user enters the ATM, the person need to scan the QR charter from the monitor in the display screen. This in turn links with the bank database and web server for fetching user credentials to validate the user. It paves a way to decrypt the charter which is scan through mobile device. The mobile device is used to scan the quick response code which is in encrypted form. Only when the user is verified, the user is allowed to perform transaction otherwise not. This quick response code along with the user's data is validated at the server side. After these validation and verification process, the user is displayed with their details. But the user is unaware of the encryption and decryption process being done on the server side.

The architecture diagram given below represents the overall view of the proposed approach. Its functions are stated as above.



*C. Authenticating user*

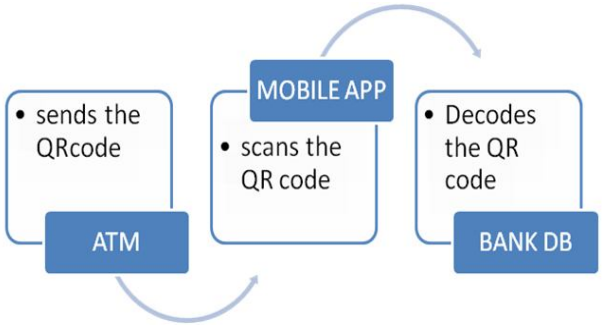
The way of authenticating the user consisting of registering the user details in the bank database as a first step. The user is provided with an account number and OTP which is valid for single time at that moment of registration in the database. This is the step takes validating the user with the mobile application. The web server acts as an interface with the customer and database. Here the database of the bank stores the details of user. Whenever the user attempts to make money transfers using Automated Teller Machine, the encrypted quick response code is made to scan using mobile device. As soon as the user is found legitimate, his/her details are shown on screen. So that he/she could make transactions. Thereby the intruders cannot make transactions or view account details of the customer. And also the user credentials are protected from being theft by unauthorized persons. This approach involves decrypting the encrypted quick response charter at the backend that was scanned.




*D. Quick Response Charter Scanning*

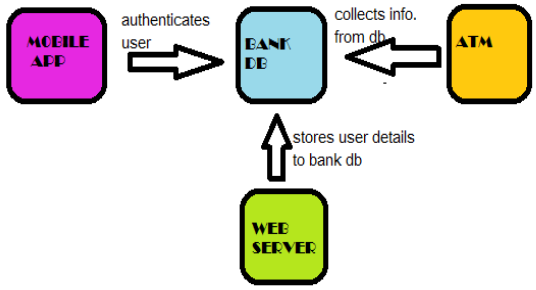
On account of making ATM money transfer, the proposed system uses a new method for authentication that uses quick response charter. Once the user enters the ATM, he/she is allowed to scan the QR code that was generated for that particular user. This way of authentication provides security and privacy for the user's confidential data from being stolen or misused by assails. This QR code is used as the way to the mechanism of authentication, as it has the major advantage that can't be stolen by shoulder-surfing assails.

The overall process is as depicted below. This involves android mobile application to mediate between the database of the bank and teller machine. This plays a important role in making the interaction process efficient and effective.




*E. Web Server interaction*

This web server serves as an intermediate which collaborates and makes the entire task to appear simple to the user. It plays an important role in mediating the entire operation of making money transfers. The customer may not be aware of the manipulations performed inside the server. But it operates with the scanned QR code and user's account details. It also does the task of decoding the encrypted quick response information.




## IV. CONCLUSION

To conclude, the proposed system reduces the vulnerability of the data and money theft from the user side and in turn provides a strong security to user's personal and bank details. This proposed system is purposed to provide powerful authentication services to the user and the bank. Our generation is moving towards cashless transaction via digitalization in each and every fields in current trend. Moveover, implementing this project paves way to cardless transaction. Even it prevents user data from shoulder-surfing attacks. And unauthorized user won't be able to access any information.

## V. FUTURE ENHANCEMENTS

This system needs a mobile device to make payment. Without the use of smart phone, this technique is somewhat tidy. And unsophisticated users won't be able to make transaction effectively. This technique can be implemented in various fields involving digital transaction for the process of

authentication. This can be further simplified make the project more and more efficient.

## REFERNCES


[1] Aayushi Mishra, Manish Mathuria, "Multilevel Security Feature for Online Transaction using QR Code &Digital Watermarking," IEEE Transactions, vol. 6, pp. 48-51, December 2017.

[2] Lin, Pei- Yu. "Distributed Secret Sharing Approach with Cheater Prevention based on QR Code," IEEE Transactions. Vol. 12(1):384 -392, Feb 2016.

[3] Tkachenko.I, Puech.W, Destruel.C, Srauss.O, Gaudin.J.M and Guichard.C, " Two level QR code for private message sharing and document authentication," IEEE Transactions. Vol. 11(3) :571- 583, March 2016.

[4] Lin SS, Hu MC, Lee CH, Lee TY. "Efficient QR Code Beautification With High Quality Visual Content. Multimedia", IEEE Transactions,vol.17(9):1515-24., . Sep 2015.

[5] Samir Pakojwar, Dr.N.J. Uke. Security in Online Banking Services – A Comparative Study. Internagtional Journal of Innovative research in Science, Engineering and Technology. Vol. 3, Issue 10, October 2014.

[6] Md. Syeful Islam. An algorithm for Electronic Money Transaction Security ( Three Layer Security):l A new Approach International Journal of Security and Its Applications Vol.9, No.2 (2015), pp.203-214.

[7] Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo, Hoon Jae Lee. Online Banking Authentication System using Mobile-OTP with QR-code.

[8] Sonia Sharma. A detail comparative study on e-banking VS traditional banking. International Journal of Applied Research 2016.

[9] Chiang JS, Hsia CH, Li HT. High density QR code with multi-view scheme. Electronics Letters . Vol49(22):1381-3. Oct 2013.

[10] Khan SH, Akbar MA, Shahzad F, Farooq M, Khan Z. Secure biometric template generation for multi-factor authentication. Pattern Recognition.vol. 48(2):458-72. Feb 2015.

[11] Leu JS, Hsieh WB. Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards. Information Security, IET.;Vol 8(2):104-13. Mar 2014.

[12] Mohan Durvey, Devshri Satyarthi. A Review Paper on Digital Watermarking. International Journal of Emerging Trends & Technology in Computer Science ( IJETTCS). Volume 3, Issue 4, July-August 2014.

[13] Petrlic R, Sorge C. Establishing user trust in automated teller machine integrity. Information Security, IET. Vol8(2):132-9;Mar 2014.

[14] Prabakaran G, Bhakkiyalakshmi R. Transmission of Data Using Arm Based Privacy Protection QR-code. InInternational Journal of Engineering Development and Research (Vol. 2, No. 2 (June 2014)). IJEDR.June 2014.