Journal for Research| Volume 02| Issue 02 | April 2016
ISSN: 2395-7549

QR based Card-less ATM Transactions

Meenu Jacob
Department Computer Science & Engineering
Amal Jyothi College of Engineering Kanjirappally, Kerala, India

Nikhil Mathew
Department Computer Science & Engineering
Amal Jyothi College of Engineering Kanjirappally, Kerala, India

Rose Merin Jose
Department Computer Science & Engineering
Amal Jyothi College of Engineering Kanjirappally, Kerala, India

Seba Siby
Department Computer Science & Engineering
Amal Jyothi College of Engineering Kanjirappally, Kerala, India

Prof. Neethu C Sekhar
Department Computer Science & Engineering
Amal Jyothi College of Engineering Kanjirappally, Kerala, India

Abstract

In the present scenario ATM transaction are carried out with the help of ATM cards which have to be physically swiped at the ATM machine. The present cash withdrawal system involves swiping the ATM card at an ATM Machine and then input a four digit pin into the terminal for verification. This method is susceptible to many types of attacks such as shoulder surfing, replay attack and ATM card skimming. In this paper, we are proposing a system in which a QR code is used as an alternative to the physical ATM card based authentication. This system can be incorporated in smartphones and other wearable device thereby eliminating the need for carrying ATM cards. QR codes are generated in the wearable device as well as the ATM machine to carry out User Authorization. An eight-digit long pin is generated to make the system more secure than present one. A background server is used to generate unique 8 digit pins for each transaction. This background server also manages transactions and links them to a user's bank account when a transaction is underway. This scheme protects the user from shoulder surfing or observation attacks, replay attacks and partial observation attacks.

Keywords: ATM, credit card, ATM card, security, QR code, PIN security, attacker, cyber criminal's

I. INTRODUCTION

ATM transactions have become a basic activity in a person's daily life. Several factors such as queue length, distractions, length of time for the interaction, urgency, physical hindrance memorization of PINs, co-located user display, speed of interaction, and the environment are all the problems faced by card users [1][2]. As the card system is ageing, the fraudsters are finding more methods to attack this system.

These cards contain magnetic strip which stores the information about the PIN and authentication details. Now-a-days, it is easy to clone the magnetic strip [4] with cheap card readers to avail the information. Uses of chips embedded in the cards are more secure but there is still the presence of a physical card entity.

II. EXISTING SYSTEM

The existing system is based on physical entities i.e. magnetic cards that are read at an ATM terminal in order to identify and authenticate a user. A four-digit pin is used as a level of authentication, this pin is known only by the user and the bank. The credit card, being a physical entity can easily [3] be stolen, and the number of combinations for the pin are limited [5], and if the attacker can acquire the user's ATM pin, then the user's bank account is compromised. The pin can be acquired using shoulder surfing, card skimming, replay attacks or by analysing the users pattern (how he thinks).

III. PROPOSED SYSTEM

The purpose of our system is to make ATM transactions more secure and lucid. Here we are using QR codes for authentication and an eight-digit long PIN for securing it.

All rights reserved by *www.journalforresearch.org*

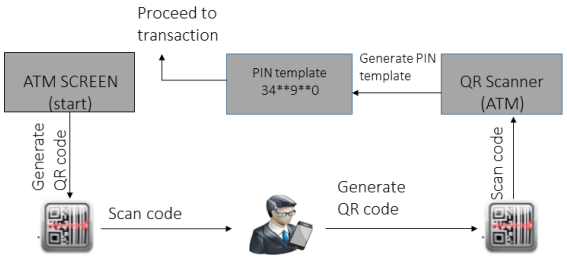

Fig. 1: System flow diagram

The server coordinates the functions and data in the wearable device, ATM machines and the user data stored in the database of the banks.

A. SERVER:

The server authenticates the user and the ATM. It generates the transaction id and validity of the current transaction when it receives the request id from the client on initiation of a transaction. The transaction id is generated using a SHA-512 hashing algorithm and hence is unique as one of the components used in the generation of the transaction id is the timestamp of the moment that the transaction was initiated on the client. This unique transaction id is logged to the database and also sent to client terminal for creation of the ATM QR code.

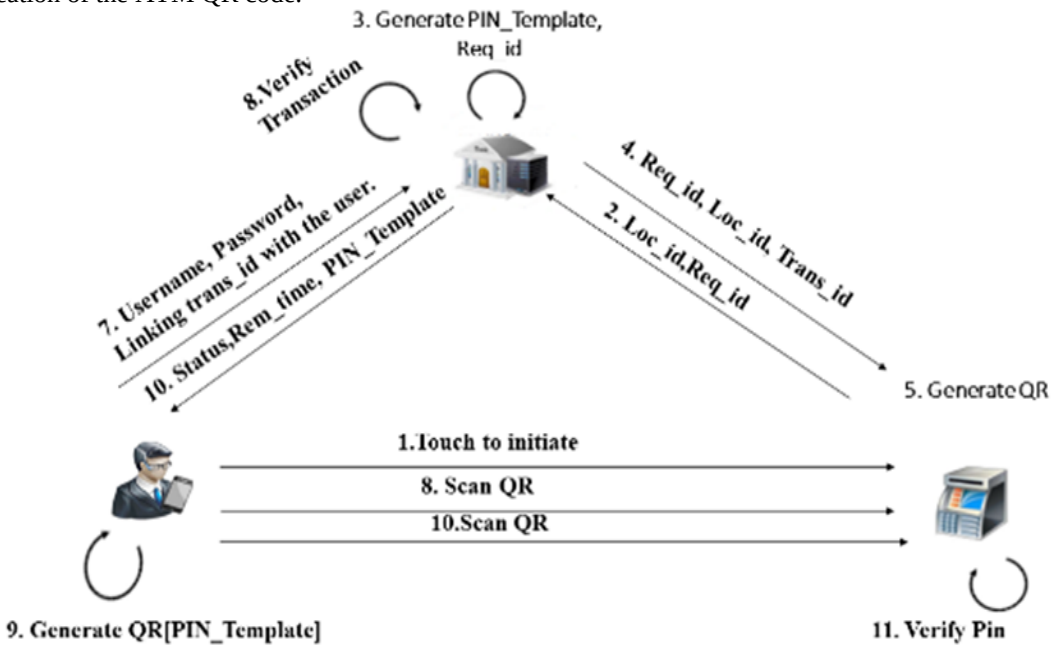

Fig. 3.1: System Overview

When an Android sends a scanned transaction id the system links the ownerless transaction identified from the QR code containing the transaction id, to the user that scanned the QR code. This transaction is now linked to a user.

The server then receives the transaction details from the android application that the user enters. A PIN-template is generated and sent to the Android app which will act as an extra layer of security. The PIN template will consist of eight or more digits in which four of them are positions for the user's ATM pin and the rest are generated and positioned randomly in the template [1].
The client then sends an authentication request when the user enters the pin template completed with the user's private ATM pin into the terminal. The server then sends the transaction details to the client and the appropriate action is taken at the client terminal, e.g. Withdrawal of money, mini statements etc.

The transaction id is marked as used in the server immediately after the transaction completes or after a timeout so that it cannot be misused by an attacker.

B. ATM Machine:

The ATM machine generated a request id when a transaction is initiated. The request code, the ATM machine's identification and the current time are sent to the server to generate a transaction id. The client receives the transaction id from the server and renders it as a QR code. This is scanned by the Android client.
The ATM client the scans the QR generated by the phone, verify the entered pin template and complete the transaction.

All rights reserved by *www.journalforresearch.org*

C. Bank:

The bank manages the user details on a central server, the details of the user, ie. The user's bank account no and debit card no are linked to their email id, making Android login easier to implement. It also stores the details of the ATM machine located at each location and provides real time monitoring of the ATM Machines' status. The Server is linked to the Bank Database which contains the actual account database.

D. Android Application:

The android application provides the platform for the user to interact with the system. The users have to login in the app. This application consists both a QR generator and a QR scanner. The user when enters the ATM he scans the QR code on the ATM screen. This links the transaction id to this user. The pin template is shown on the app. Then the user enters the transaction details and the amount to be withdrawn. After this the app will generate a QR which have to be scanned by the ATM. A final stage of verification, i.e. Entering the pin template completed with the user's pin into the ATM client. The cash can be only be withdrawn if the final authentication is successful.

IV. SYSTEM PROTOCOL

The interactions and message passed is explained as follows:

1) Step 1: The user enters the ATM along with his personal mobile device. He touches the ATM screen to initiate the transaction.
2) Step 2: A transaction request is send to the server along with the parameters such as the location of the ATM and the corresponding request id generated by the ATM.
3) Step 3: A transaction id and PIN template is generated and sent back to the ATM client.
4) Step 4: The ATM client generates a QR code using this transaction id.
5) Step 5: The QR generated will be scanned by the android device.
6) Step 6: The Server links the transaction id with the user that scanned the QR.
7) Step 7: The user inputs his transaction details into his device, at the same time he receives a pin template from the server.
8) Step 8: A QR code will be generated in the android application which have to be scanned by the scanner embedded in the ATM machine. The ATM terminal gets the transaction details from the user's device.
9) Step 9: The user enters the pin template completed with the user's personal pin. This completes the Authentication.
10) Step 10: After the authentication, the amount can be withdrawn from the ATM.

V. CONCLUSION

The system is designed in such a way that it can be more resistant to attacks such as card-skimming, observation attacks, replay attacks and relay attacks. This system is more efficient and secure than the existing ATM system. No malpractices can be done in the case of this system.

VI. FUTURE SCOPE

Modifications and new features can be added to this project. A biometric authentication be used instead of one QR scanning.

REFERENCES

[1] SEPIA:Secure-PIN-Authentication-as-a-Service for ATM using Mobile and Wearable Devices. Rasib Khan, Ragib Hasan, and Jinfang Xu SECRETLab, Department of Computer and Information Sciences.
[2] "Secure mobile-based financial transactions," S. N. White , Feb 2013, US Patent 8,374,916
[3] "Understanding credit card frauds," T. P. Bhatla, V. Prabhu, and A. Dua Cards business review, vol. 1, no. 6, 2003.
[4] "Cloning credit cards: A combined pre-play and downgrade attack on emv contactless." M. Roland and J. Langer, in Proceedings of The 7th USENIX Workshop on Offensive Technologies, 2013.
[5] R. Anderson, "Why cryptosystems fail," in Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM, 1993

All rights reserved by *www.journalforresearch.org*