# An RFID Enabled Authentication System for Transaction and Abridgement of ATM Card Blocking and unblocking Intricacies

Ms. S. Kumari
Assistant Professor,
Dept. of I.T.,
Panimalar Engineering College,India
*sudhakar.kumari@gmail.com*

M. Nivetha
Dept. of I.T.,
Panimalar Engineering College,
Chennai, India
*mahtevin@gmail.com*

N. Paarkavi
Dept. of I.T.,
Panimalar Engineering College,
Chennai, India
*paaru1618@gmail.com*

M. Archana
Dept. of I.T.,
Panimalar Engineering College,
Chennai, India
*archana.m144@gmail.com*

D. Geetha Yazhini
Dept. of I.T.,
Panimalar Engineering College,
Anna University, India
*yazhini.mathu3@yahoo.com*

***Abstract***— In the modern world, everything has become online and work gets completed in a quick span of time. The flexibility of credit and debit card transactions has led to increase in number of users and also has cautioned us on security risks. The prevailing complications associated with blocking and unblocking of ATM cards involves a tedious interactive processes. In order to overcome the blocking intricacies and transaction liabilities, a three level authentication scheme involving IMEI, One-time password and Graphical pattern is used with the help of RFID (Radio Frequency Authentication). Here OTP is transmitted from mobile to ATM system which is achieved by Bluetooth. The implementation of this takes the help of RFID card, RFID reader housed in ATM, Microcontroller and Bluetooth. The proposed system is thus cost effective which also ensures faster transactions and blocking/unblocking along with tight security.

***Keywords****-ATM, Blocking of ATM Card, Bluetooth, IMEI, Microcontroller, One-Time Password, RFID.*

*****

## I. INTRODUCTION

An increasingly common problem involving blocking and unblocking of ATM cards is handling a tedious interactive process with customer care services. In order to overcome this difficulty, we describe system using a technology called RFID to enforce security for transaction as well as for blocking and unblocking ATM cards with ease. A significant advantage of RFID devices is that the RFID technology enables tag reading from a longer distance, even in harsh environments with no precise line of sight to be maintained. We're all familiar with the difficulty that a cashier sometimes has in making sure that a barcode can be read and that prices of items can be scanned. And obviously, credit cards and ATM cards must be swiped through a special reader.

RFID devices will work within a range up to 20 feet for high-frequency devices of the scanner. For example, you could just put all of your groceries or purchases in a bag, and set the bag on the scanner. It would be able to query all of the RFID devices and your total purchase immediately.

The conventional card blocking and unblocking processes tend to be cumbersome and time consuming. Our system was designed both to overcome security issues and to additionally eliminate common inconveniences by facilitating blocking of cards and unblocking of cards from ATMs nearest to the user. The associated intricacies are eliminated and security is achieved by three level authentications. Essential functioning of our proposed system involves 4 key processes enumerated below:

A. Registration
B. Login
C. Transaction using RFID
D. Blocking of ATM cards
E. Unblocking of ATM cards

The rest of the paper is organized as follows- Section 2 discusses related works and relevant derivatives used in our system. Section 3 describes the proposed methodology, detailed processes involved, and various supporting features and their implementations. Section 4 concludes the paper with future work and comments on implementation details and the system’s advantages over contemporary counterparts.

## II. RELATED WORKS

Using references [1] to [5], we derived various design aspects used in our system, primarily featuring novel usage of NFC. Each of these sources are mentioned below along with their derivatives in our system summarily explained Nara Ida Joslin *et al* [1], suggests a methodology utilizing RFID technology for identifying a specific client. Here the identification is done by comparing serial number of the user RFID tag with the stored data in the system. If the serial number of the RFID tag is matched with the stored data, the system generates one-time password (OTP) to a particular client through GSM module. The false entry of OTP more than three times will activate the buzzer and stops the transaction. This outputs us a secured and authentic transaction achieving goals of privacy.

Anusha Mandalapu *et al* [2], enforces the usage of NFC technology and promotes abridgment of blocking intricacies. Three level authentication is promoted by means of secure NFC tag reading, OTP and pattern matching. The implementation is done for both NFC enabled and non-enabled phones.

K. Santhosh Kumar *et al* [3], suggests the usage of GSM (Global Systems for Mobile communications) as it the only type of cellular service available. For providing security at ATMs, GSM Module are controlled by using Microcontroller. Once the user verifies their identity, a message is sent requesting for PIN and amount which the user sends via message. This ensures a secure authentication.

Mrs. S. P. Balwir *et al* [4], describes GSM technology for performing transactions. Using GSM, the OTP is sent to user where the user can accept or reject the transactions. The user can also respond to ACTION command when their ATM card is under illegal use.

Kopparapu Srivatsa *et al* [5], proposed a secure contactless credit card (RFID credit card) to enable secure online transactions using RFID Readers and microcontroller attached to it. When the RFID ATM card is brought into the vicinity of the ATM system, the reader reads the details of card holder and his account number. Then this information is sent to the computer through a microcontroller. Here details are checked for genuineness and a message is sent to the card holder with the help of hyper terminal whether or not to proceed the transaction.

## III. PROPOSED WORK

This section presents the proposed system, setup, and detailed explanation of essential processes involved. The system architecture is shown in Fig1.

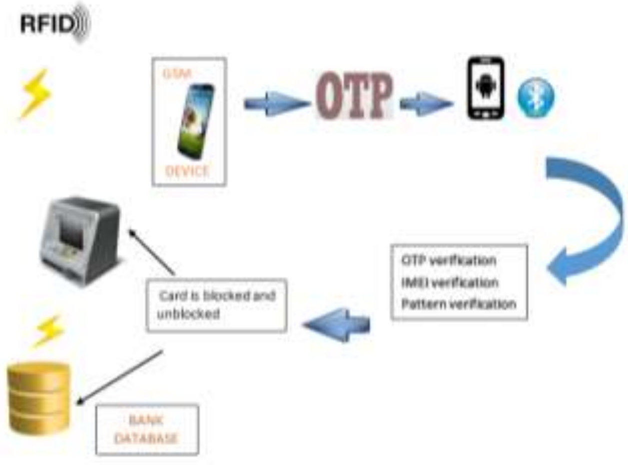

Fig.1. Architecture diagram

### A. Registration Process

The process of registration to enable transactions and blocking and unblocking of cards using RFID involves the following procedures:

1) A page for registration is developed for registering the personal details of the user.

2) For registration process, the user has to register himself with personal details like name, RFID tag number (card number), PIN, phone number, IMEI and a Pattern Password which acts as an authentication key. The pattern is drawn by clicking on buttons which are arranged in the form of 3x3 matrix.
3) Since pattern forms the main part of authentication, the registration page asks the user to confirm the pattern by redrawing it. In order to prevent shoulder surfing, the pattern is made invisible as the user draws it.
4) On submitting all these details, the user will be returned with a password which is used for login purpose, to do transactions and blocking and unblocking.

### B. Login

Logging in is the process by which an individual gains access to a mobile device, database or computer system by identifying and authenticating themselves.

1) The user has to authenticate by providing user name and password. User name is same as the name used in registration process and password is the one that is generated as a result of registration.

2) On logging in, the main menu opens. The main menu has features for transaction, blocking, unblocking with details such as card number (read by RFID reader), PIN and mobile number needs to be entered.

## *C. Transactions using RFID*

This process aims at faster and reliable dealings with banks and ensures ease of use for ATM users. This process is further divided into two sub segmented processes:

The first level of authentication involves ATM card swiping. Here the RFID tag is used instead of ATM card.

1) The tag has the card number stored in it. The RFID reader emits EM waves continuously such that when a tag of RFID is placed in front of it, the EM waves hit the tag and sends the card number information to the reader. The reader in turn sends this information to the ATM system.

2) For performing transaction card number and PIN are validated. The user can also perform cash withdrawal or deposit.

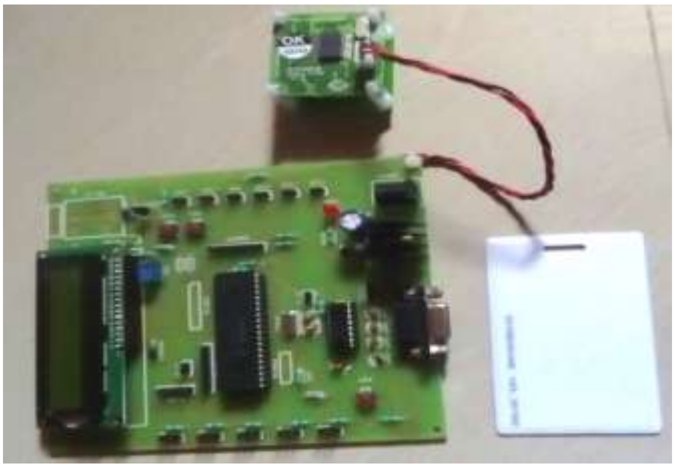

Fig.2. Microcontroller connected to RFID Reader.

Typically, 15 digits long, the IMEI number is unique for every mobile set. It provides information about a phone, such as its origin, serial number, model and manufacturer, to the mobile network that the phone is connected to. The principal purpose of IMEI number is to identify mobile devices and has no relation to the subscriber. The generated OTP is fed to the ATM system through an app that turns on Bluetooth. This will automatically retrieve the IMEI of mobile phone and validates the IMEI.

## *D. Blocking of lost ATM cards*

For blocking initially PIN and mobile number are validated. The blocking process involves three level authentication. The following are the details used for this authentication:

a) International Mobile Station Equipment Identity(IMEI)

The IMEI (International Mobile Station Equipment Identity) is a serial number that uniquely identifies a GSM or UMTS mobile phone.

b) One Time Password (OTP)

OTP, a four-digit number is generated on the mobile screen with a timeout which is valid only for few seconds, say 30 seconds. This is a password that is valid for only one login session or transaction and is also stored in database. If it exceeds the timeout, then a new OTP is generated. The OTP has to be entered on the ATM screen. If both the passwords match, the user can continue his process henceforth. This corroborates the second-level of authentication.

c) Pattern Matching

During registration process, the user is asked for a pattern which is similar to the pattern used in mobile phones for unlocking applications. This pre-registered pattern will be asked once OTP is successfully verified. The users need to draw the correct pattern to proceed further with the blocking of their ATM cards. This confirms the third level of authentication.

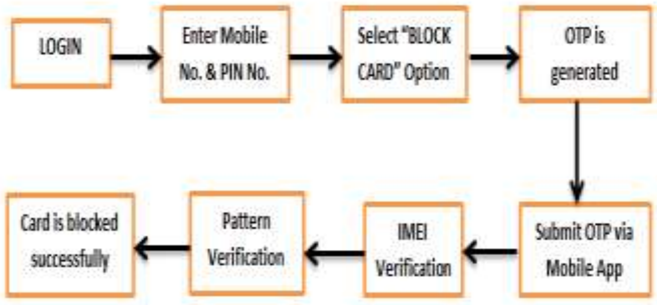
LOGIN
Enter Mobile No. & PIN No.
Select "BLOCK CARD" Option
OTP is generated
Submit OTP via Mobile App
IMEI Verification
Pattern Verification
Card is blocked successfully

Fig.3. ATM Card blocking overview

An overview of the methodology implemented to facilitate easy blocking of cards is shown in Fig. 3. Elaboration of the steps involved in the process follows below:

1) An ATM card blocking function is made available on the ATM home screen with the requirement of having to log in for usage.
2) After logging in, the user is required to enter his

registered mobile number and Personal Identification Number (PIN). On validation of the mobile number and PIN, an OTP code is generated by the server. This OTP code is sent as a message to pre-registered mobile number. This OTP is fed to the ATM system via an application. The application will automatically turn on the Bluetooth of the mobile phone and transmits the OTP to the system. The ATM system will have its Bluetooth switched on at all times. Thus there is no need to facilitate the switching on of the system's Bluetooth. Through this process, the OTP and IMEI of mobile phone are verified against those details stored in database.

3) After the validation of IMEI and PIN is performed, the ATM system asks for pattern from the user. In this step, the user is required to draw the same pattern that has been used for registration. The pattern has to be drawn on the ATM screen.
4) The verification of pattern confirms the final level of authentication and with this the card is blocked successfully. This is also intimated to the bank.

### E. *Unblocking of ATM cards*

The process of unblocking cards using RFID is same as that of blocking. This process also promotes three level authentication that is, verification of OTP, IMEI and pattern, similar to that in blocking process. There is also an additional requirement when unblocking of cards is concerned. The user is required to have his/her RFID tag (ATM card) to be in hand. This requirement ensures that only the correct person or owner is unblocking the card. An overview of the methodology implemented to facilitate easy blocking of cards is shown in Fig.4.

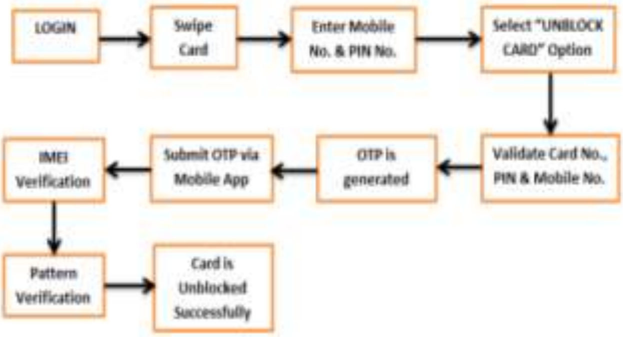
LOGIN
Swipe Card
Enter Mobile No. & PIN No.
Select "UNBLOCK CARD" Option
Validate Card No., PIN & Mobile No.
OTP is generated
Submit OTP via Mobile App
IMEI Verification
Pattern Verification
Card is Unblocked Successfully

Fig.4. ATM Card unblocking overview

The procedure involved in the above block diagram is shown below:

1) The ATM card blocking function is made available on the home screen with the requirement of having to log in for usage.
2) After logging, the first step that is different from the blocking of cards is that, the ATM system asks user to swipe the card, i.e. the user has to feed the card number by using his RFID tag. This is initial step of authentication as anyone may unblock the card if the system does not demand the usage of ATM card for unblocking.
3) The user is required to enter the registered mobile number and Personal Identification Number (PIN) and then select unblock card option.
4) On validation of mobile number and PIN, an OTP code is generated by the server. This OTP code is sent as a message to preregistered mobile number. This OTP is fed to the ATM system via an application. The application will automatically turn on the Bluetooth of the mobile phone and transmits the OTP to the system. The ATM system will have its Bluetooth switched on at all times. Thus there is no need to facilitate the switching on of the system's Bluetooth. Through this process, the OTP and IMEI of mobile are checked with stored information in the database.
5) After validation of IMEI and PIN is performed, the ATM system asks for pattern from the user. In this step, the user is required to draw the same pattern that has been used for registration. The pattern has to be drawn on the ATM screen. Thus confirming the unblocking procedure.

## IV. CONCLUSION

This new proposal establishes abridgement of intricacies in blocking and unblocking ATM cards. Generally, blocking ATM card involves a tedious process of attending longer customer care call where the representative questions the user for all details like PIN, account number, etc. For unblocking, the user will have to pass a letter to higher authority, which after clearances, will lead to unblocking. This may take more time. Moreover, the card holder has to visit the office for this purpose which may be located far away from card holder's location. Introduced here is an essential feature that alleviates user's anxiety for blocking of ATM cards by approaching the nearest ATM. This cuts down the waiting time of the user on the customer care line, who may also be in a sense of grief.

The RFID technology is more advantageous than normal barcode reader or swiping mechanisms. RFID can transmit over longer distances and since the limit of area is confined to ATM cabin, the process of reading

RFID tags is much easier than swiping as swiping can sometimes result in card detection failure. The usage of RFID tags cuts down any attempt to seize the card holder's information by means of skimming.

The verification of IMEI and pre-registered pattern will strengthen the confirmation of legitimate user. This scheme not only presents an advantage to the user, but also aids the bank. The IMEI will change as the user changes his/her mobile phone. But the proposed system also facilitates the changing of IMEI, PIN, mobile number and login password. The user need not remember his previous IMEI (in case of changing mobile phone), as it is automatically retrieved on selecting Change IMEI option.

Above all, the proposed system does not require the user to have an internet connection in his or her mobile phone. The existing system provides cash withdrawal and deposits to be done on different machines. Here all the facilities are combined in a single machine and encourages users to do all their jobs on their own with ease.

Further proposals on enhancement would be the usage of another password like MPIN (Mobile PIN) instead of IMEI, which can be returned on registration. This MPIN may be provided by banks and can be made unique for each user. This will enable users to change their phones without having the need to change IMEI.

The proposed work shows all its implementations in a normal PC system. This can be further enhanced by extending the forms to mobile platform. The registration can be facilitated by means of website so that the user can register himself at home. The password which is returned as a result of registration can be sent in email of user along with a Negative Pattern Password (NPP) which can be used for blocking and unblocking purpose

## ACKNOWLEDGMENT

The authors want to heartily thank Dr. B. Annie Princy Project Coordinator, Professor and Ms. S. Kumari Project Guide, Assistant Professor of IT, Panimalar Engineering College of Tamil Nadu for their critique discussion and valuable suggestions.

## REFERENCES

[1] Nara Ida Joslin and B.Vamsi Krishna," Secured ATM Card Accessing System Using RFID", IJCSME-Volume- 2-Issue-11, November 2015.

[2] Anusha Mandalapu, Daffney Deepa V, Laxman Deepak Raj and Anish Dev J, "An NFC featured three level authentication system for tenable transaction and abridgment of ATM card blocking intricacies", IEEE ,October 2015.

[3] K. Santosh Kumar and G.Vinay Kumar," RFID and GSM Based ATM Money Transfer Prototype System", IJAREEIE Vol. 3, Issue 11, November 2014.

[4] Mrs.S.P.Balwir, Ms.K.R.Katol, Mr.R.D.Thakare Mr.N.S.Panchbudhe and Mr.P.K.Balwir (2014),"Secured ATM Transaction System Using Micro-Controller", IJARCSSE Volume 4, Issue 4,April 2014.

[5] Kopparapu Srivatsa, and Madamshetti Yashwanth, "RFID & Mobile Fusion for Authenticated ATM Transaction", International Journal of Computer Applications, (0975–8887)Volume3,June2010.