AN RFID FEATURED THREE LEVEL AUTHENTICATION SYSTEM FOR TENABLE TRANSACTION AND ABRIDGMENT OF ATM CARD

[1]BHAGYA K
[1]Professor

[1]Department of Computer Science & Engineering

[1]HKBKCE, Bangalore, India

*Abstract :**The flexible use of credit and debit card transactions has become increasingly ubiquitous and so have the associated vulnerabilities that make them a common target for cyber criminals. Furthermore, a prevalent complication associated with blocking of ATM cards involves tedious interactive processes and even possibly long waiting times during interaction with customer care services. Using a three factor authentication scheme employing RFID Involving One- time password, we describe and quantify the potential to overcome common transaction liabilities (brute force attack, shoulder surfing, skimming of ATM cards, etc.). The auxiliary feature of blocking ATM cards is implemented using a QR code authentication scheme and RFID technology. The proposed system, therefore, ensures both secure usage of ATM cards and cost effectiveness by utility of novel and increasingly common technology, when also simultaneously proving to be user friendly.***

IndexTerms -**ATM transaction, Blocking of ATM Card, RFID, One-Time Password, Negative Pattern Password, Bluetooth, RFID-Transmitter, RFID-Receiver, Microcontroller**.

I. INTRODUCTION

A fairly and increasingly common loss involving theft in digital commerce is stealing or skimming of ATM cards. Unlike most other means of theft, this is an innate vulnerability of the ATM system and network itself. In order to over come this inherent weakness, we describe system using a relatively new technology called RFID to enforce security during transaction and usage.This paper's methodology aims at using both RFID-enabled and non-enabled cell phonesfor designing a dedicated application that can communicate with the ATM machine. Our proposed system eliminates the requirement of a password or a PIN, which is entirely pivotal to keeping to memory or safe storage of an authentication key.

Since conventional card blocking processes tend to be cumbersome and time consuming, our system was designed both to overcome afore mentioned security issues and to additionally eliminate common inconveniences by facilitating blocking of cards from ATM near the user. This is implemented by QR code authentication. Essential functioning of our proposed system involves 4 key processes enumerated below:

a) To provide Secured ATM transactions usingRFID

b) To provide Blocking and Unblocking of lost ATM cards

c) To provide RFI dregistration

d) To provide Authentication by negative pattern password andOTP.

The rest of the paper is organized as follows- Section II discusses related works and relevant derivatives used inour system. Section III describes the proposed methodology, detailedprocessesinvolved,andvarioussupportingfeatures and their implementations. Section IV analyses and compares performance results obtained from both simulationsandexperimentsconductedinrealtime.Section V concludes the paper with future work and comments on implementation details and the system's advantages over contemporarycounterparts.

II.RELATEDWORKS

We derived various design aspects used in our system, primarily featuring novel usage of RFID. Each of these sources are mentioned below along and their derivatives in our system summarily explained suggests a methodology utilizingORcodeasapasswordauthenticationtechniquethat simple read images and transmits them to the server. Its effectiveness against several attacks such as brute-force attack, man-in the-middle attack and keyboard hacking are examined and degrees of vulnerabilities arecompared.

Hung-Min Sun *et al* [2], proposes a method which leverages a user's cell phone and short message service to thwart password stealing and password reuse attacks. Through *oPass*,usersonlyneedtorememberalong-termpasswordfor login on all websites. Evaluations of the *oPass*prototype concluded the system as being efficient and affordable compared with the conventional web authentication mechanisms.

BlakeRoss*etal*[3],describesabrowserextension,*PwdHash*thattransparentlyproducesadifferentpasswordfor eachsite, improving web password security and defending against password phishing and otherattacks.

Chris Karlof*et al* [4], proposes a novel technology called dynamicpharming.Dynamicpharmingenablestheadversary to eavesdrop on sensitive content, forge transactions, sniff secondary passwords, etc. To counter dynamic pharming attacks, they proposed two locked same-origin policies for web browsers.

MinWu*etal*[5],presentsasolutiontotheproblemofreusing passwords saved in computers using mobile phones as hand-heldauthenticationtokens,andasecurityproxywhichallows the system to be used with unmodified third-party web services to develop a system that is both secure and highly versatile.

N. Provos*et al* [6], identifies the four prevalent mechanisms used to inject malicious content on popular web sites: web server security, user contributed content, advertising and third-party widgets. For each of these areas, they present examples of abuse found on the Internet. They also present the state of malware on the Web and emphasize the importance of the threat.

III.PROPOSEDWORK

This section presents the proposed system, setup, and detailed explanation of essential processes involved.

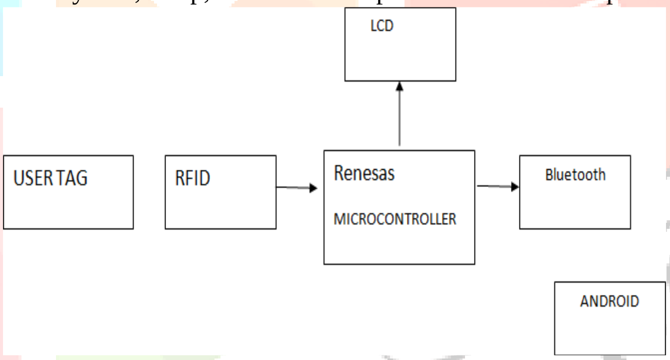


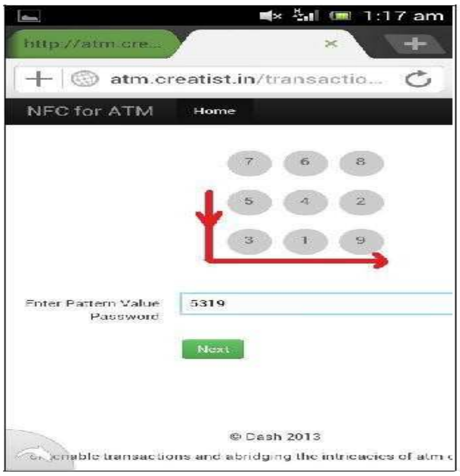
Fig.1.An overview of the system

a) Secured ATM transactions usingRFID

This process aims at faster and reliable dealings with banks andensureseaseofuseforATMusers.Thisprocessisfurther divided into two sub segmentedprocesses:

1) The first level of authentication involves ATM card swiping or manual ATM card number entry in case of card detection failure, damage to the card, or just its absence. The latter is suggested as an optional method to avoid ATM card skimming.

2) ThesuccessiveprocessfeaturestheuseofanRFIDenabled cell phone having access to Internet. The user is required to taptheRFIDcardontheRFIDreader.UponsuccessfulRFID tagging, a webpage on the Cell phone’s browser requests for a pre-registered phone number as a user input. Followingthis step, the user is required to enter a Pattern Password that was previously registered online during the registration processto use RFID, discussed in Section III (C). The pattern password (Fig.2.),appearsasarandomsetofnumbers.TheOTPisthen generated on a subsequent page, which is then entered on the Andriod screen before a presettimeout.



1:17 am

http://atm.cre...

atm.creatist.in/transactio...

NFC for ATM Home

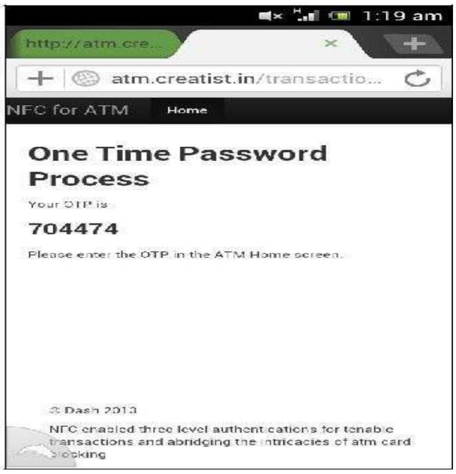
Enter Pattern Value Password: 5319

Next

© Dash 2013

...enable transactions and abridging the intricacies of atm c

Fig. 2.Pattern generation



1:19 am

http://atm.cre...

atm.creatist.in/transactio...

NFC for ATM Home

One Time Password Process

Your OTP is

704474

Please enter the OTP in the ATM Home screen.

© Dash 2013

NFC enabled three level authentications for tenable transactions and abridging the intricacies of atm card blocking

Fig. 3. OTPgeneration

The above mentioned sub-segment processes (2) makes use of the following procedures which are elaborated below:

a) RFID Tagreading

The user reads the RFID–TAG, by swiping the RFID card over the RFID reader. The tag is designed for secured password input through the mobile device.

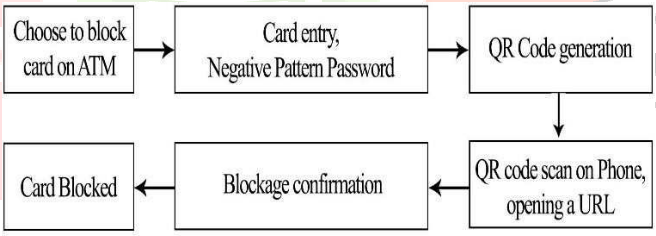
b) Pattern Generation

Afterthefirststepissuccessfullyverified,itasksfornew pattern generation, once the pattern is created successfully it forwards to the OTP generation, if the pattern generation is unsuccessful it will not allow the user for next step of authentication.

c) One Time Password (OTP)

Once the second step is successfully verified, a four digit One-Time Password (OTP) is generated on themobile screen with a timeout which is valid only for few seconds, say 60 seconds as in Fig. 3. If it exceeds the timeout, then a new OTP is generated. The OTP has to be entered on the second screen of the ATM which appears after swiping or entering the ATM card number. If both the passwords match, the user can continue his transactions henceforth. This corroborates the third-level ofauthentication.

b)Blocking of lost ATMcards



Choose to block card on ATM
Card entry, Negative Pattern Password
QR Code generation
QR code scan on Phone, opening a URL
Blockage confirmation
Card Blocked

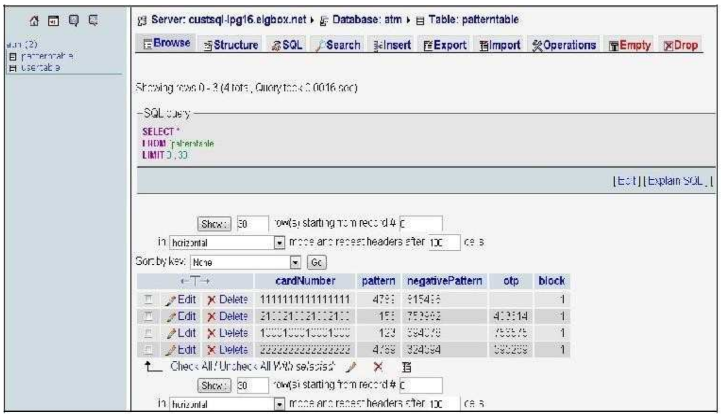
Fig. 4. ATM Card blocking overview

An overview of the methodology implemented to facilitate easyblockingofcardsisshowninFig.4.Elaborationofthe steps involved in the process followsbelow:

1) AnATMcardblockingfunctionismadeavailableonthe ATMhomescreenwithouttherequirementofhavingtolog in forusage.

2) Upon its activation, the user is required to enter the registered Card number and Negative Pattern Password (NPP). The NPP is sent by the bank server during registration (as discussed in Section III C) of the pattern as in Fig.5.

OnvalidationofthePVP,aQuickResponse(QR)codeis generatedontheATMscreen.TheQRcodeisscannedin the phone and a unique URL is generated. After opening itinthemobilebrowser,aconfirmationpageisrequested to the user. On user confirmation, a success screen is displayed. Simultaneously, the intimation of this request to block the card is sent to the bank server. Account ownership can be ensured through phone callverification by the bank once the request is registered. Further steps are taken to deactivate the account as per bankrules.



Server: custsql-ipg16.eigbox.net ▸ Database: atm ▸ Table: patterntable

Browse | Structure | SQL | Search | Insert | Export | Import | Operations | Empty | Drop

Showing rows 0 - 3 (4 total, Query took 0.0016 sec)

SQL query

```
SELECT *
FROM `patterntable`
LIMIT 0 , 30
```

[Edit] [Explain SQL]

Show : 30 row(s) starting from record # 0

in horizontal mode and repeat headers after 100 cells

Sort by key: None Go

			cardNumber	pattern	negativePattern	otp	block
□	Edit	Delete	1111111111111111	4793	915436		1
□	Edit	Delete	2100210021002100	153	753962	403514	1
□	Edit	Delete	1000100010001000	123	364078	755575	1
□	Edit	Delete	2222222222222222	4769	324094	590209	1

Check All / Uncheck All With selected:

Show : 30 row(s) starting from record # 0

in horizontal mode and repeat headers after 100 cells

Fig. 5. Database details of cards initiated forblocking

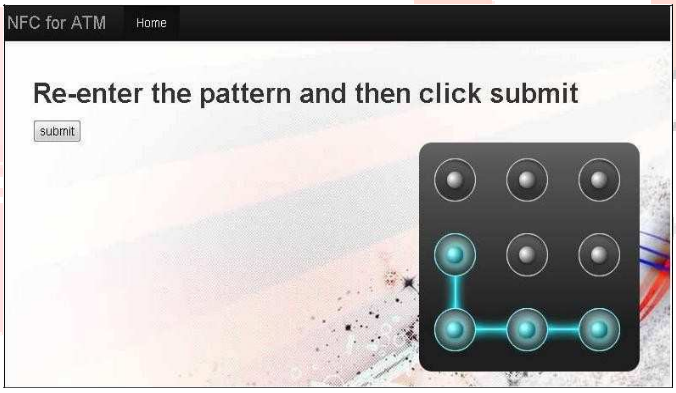
c) RFIDRegistration

The process of online registration to enable transactions using RFID comprise of the following procedures:

1) Awebsiteforregistrationisdevelopedforregistering the personal details of the user.(For experimental studyhttp://atm.creatist.in/register/init)

2) During the transaction process while using RFID,the userhastoregisterthePatternPasswordwhichactsas the authentication key. The pattern is drawn by holdingdownatouchclick,duringwhichthecursoris moved along the path in a single stroke without being lifted until completion[5]. It is the same as drawing the pattern on a mobile device as Fig.6.

Oncompletionofthisprocess,theuserwillreceivean acknowledgement to the registered e-mail id that will contain a negative pin which is a Negative Pattern Password(NPP)inthisdiscussionasFig.6.ThisNPPisused toblocktheATMcard.Inthisway,cardblockingisupgraded to feature greater ease of use and higher levels ofsafety.



Re-enter the pattern and then click submit

Fig. 6. Register pattern.

d) Facilitation of RFID using non-RFID mobilephones

Issues concerning portability of the proposed system onto mobile devices, not having RFID, can be dealt with by a bridging system. A broken down, component-wise description of this system is described below:

1) RFIDTransmitter

A hardware kit which has an RFID transmitter, as given in Fig. 7, has a Microcontroller ARM 2103 and a receiver.

2) RFID Tag(MIFARE ClassicCard)

An RFID MIFARE card is used to write the private URL that the mobile application opens in a browser after RFID tagging. The MIFARE Classic 1K tag (used for study) offers 1024 bytes of data storage.

3) MobileBluetooth

Bluetooth is enabled in the kit once the tag is read and it triggers the Bluetooth of the mobile device. The URL written in the tag now opens in the web browser of the mobile device with an application. The hardware kit with themicrocontrollerandtheBluetoothchipisshowninFig.7.

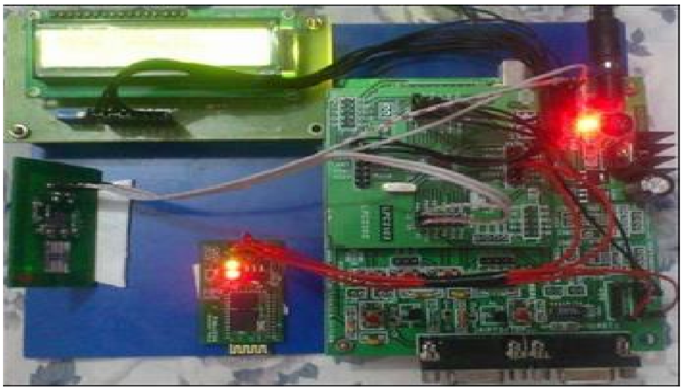
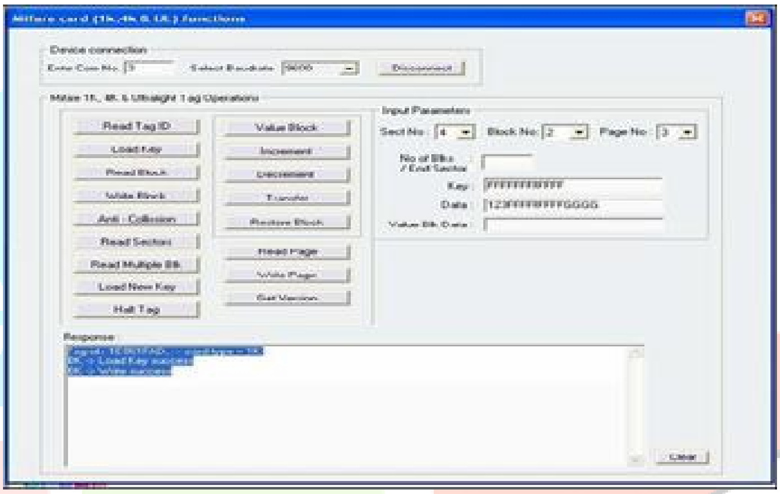


Fig. 7. RFID Transmitter Hardware Kit.

The MIFARE card is written with data using an RFID writer. The one used in our study is a starter kit CD by Digant Technologies that has an installation drive. The drive runs an application that enables to do certain functions as shown in Fig. 8.



Device connection

Select Baudrate: 9600

Input Parameters

Sect No: 4 Block No: 2 Page No: 3

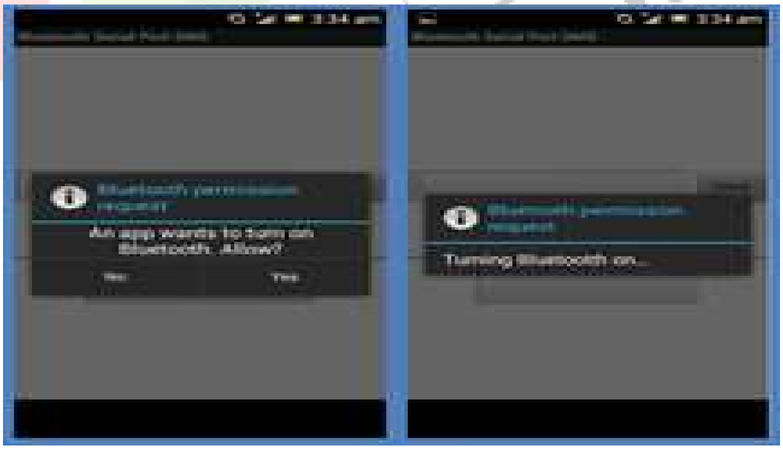
Key: FFFFFFFFFFFF

Data: 123FFFFFFFFFGGGG

Response

Fig. 8. Writing Data into RFID card

The microcontroller is coded in Embedded C programminglanguagetoenableBluetoothoncethetagis read. This Bluetooth will enable to interact with the Bluetooth of the mobile device. A pop up notification is triggered to enable Bluetooth in the mobile phone as in Fig. 9.(a) and 9.(b).



An app wants to turn on Bluetooth. Allow?

Turning Bluetooth on...

Fig. 9(a) Fig. 9.(b)

Once the Bluetooth is detected after making the device discoverable and paired with the phone device, the restrictedATMtransactionURLopensinthewebbrowser with the help of an application. The procedure being the sameasdetailedearlier.TheMIFAREcardscanbeissued to the RFID registered customers to make use of it for secure transactions. These users will need an Android phone, an active internet service, a web browser and a QR code scanner.

IV.RESULTS

The entire process from swiping the card to entering the OTP on the screen was tested under simulation. Real time testing was conducted on a test bed machine possessing average home computer hardware specifications and runningonWindows7.Thecellphoneusedduringthetest was furnished with internet connectivity having a connection speed of 2.14 Mbps.

V.CONCLUSION AND FUTUREWORK

This new proposal is put forward to diminish the concept of PIN as a password for the process in an ATM system. As the future is still vulnerable to password attacks such as Peeping attacks, Brute-Force attack, Retrieving passwords from the systems, Skimmers, etc, all these aspects are oppressed by imparting this new method. On using RFID, it is easy to open a webpage without the wastageofbrowsingtime.Bytheuseofdummypassword,i.e. PVP, the level of security is escalated and avoids the slightest percentage of attacks. Usually the acknowledgement of OTP through the erstwhile text messagingcausesdelayinreceivingit.Toevadethisissue, we generate an OTP on the webpage with a Timeout. Introducedhereisanessentialfeaturethatalleviatesuser's anxiety for blocking of ATM Card by approaching the nearest ATM. This cuts down the waiting time of the user on the customer care phone line, who may also be in a sense ofgrief.

The QR code generation is also reliable as it generates a unique URL in accordance to the card number. The Negative Pattern Password will strengthen the confirmation of the legitimate user. This scheme not only presentsasanadvantagetotheuser,butalsoaidstheBank. The intimation received to them from the proposed interface, can provide to deactivate the user's account by placing an additional phone call for confirmation. As a result, the RFID technology and the Dash Matrix concept can be subsequently used for many relative fields. Thus, RFID usage is less time consuming, feasible, reliable and also cost efficient, given the cost of a single RFID MIFARE card being between $1.75 to $ 2.0 (1000units).

Future proposals on enhancement would be the usage of NTag21x family of tags, which is the latest advancement with more security features and faster read capacity. Also MIFARE DESFire EV2, MIFARE SAM AV2 cards can

be used as they provide AES and secure storage for cryptographic keys. The tags can be tested for the RFID enabled phones while the latter can be used for non-RFID mobile devices.

The propose system consist of RFID technology and password authentication using TAC. RFID is used to uniquely identify a user and TAC is used to add extra security which is a 4 digit code and that will be sent to user's cell phone number using GSM service, after entering TAC transaction will be done. So in this paper with the help of Password authentication and RFID identificationthesystemwillbesimple,cost-effectiveand security level will get increase in an ATM transaction, as cell phone number is unique to everyuser.

REFERENCES

[1].Young-Gon Kim and Moon-Seog Jun, "A design of User Authentication system using QR code identifying method", 6thInternational Conference on *Computer Science and Convergence ,Information Technology, IEEE Transactions*, pp. 31-35, Nov-Dec2011.

[2].Blake Ross, C. Jakson, N. Miyake, D. Boneh, and J.C. Mitchell, "Stronger password authentication using browser extensions," in *SSYM'05: Proc.14thConf. USENIX Security Symp.*, Berkeley, CA, pp. 2-2, USENIX Association,2005.

[3]. ZhengmingLi,LijieXueandFeiTan,"Facedetectionin complex background based on skin color features andimproved AdaBoost Algorithm" *Progress in Informatics and Computing (PIC), 2010 IEEE International Conference*, Vol. 2 , pp. 723-727, Dec.2010.

[4]. Chris Karlof, U. Shankar, J. D. Tygar and D. Wagner, "Dynamic pharming attacks and locked same- origin policies for web browsers" in *CCS'07:proc.14thACM Conf. Computer Communications Security*, New York, 2007, pp. 58-71,ACM.

[5].Min Wu, S. Garfinkel and R. Miller, "Secure Web authentication with mobile phones" in *DIMACS Workshop usable Privacy Security Software,* Citeseer,2004.

[6]. N.Provos,D.Mcnamee,P.Mavrommatis,K.WangandN.Modadugu,"Theghostinthebrowser:AnalysisofWeb based Malware" *Proc. 1st Conf. Workshop Hot Topics in Understanding Botnets*, Berkeley, CA, 2007.