Multi Account Embedded ATM Card

GOKUL.R, GODWIN ROSE SAMUEL.W, ARUL.M, SANKARI.C
gokul.petit@gmail.com, godwingrs22@gmail.com, arulmohan07@gmail.com, san_nad3@yahoo.co.in

Abstract— The idea behind this work is that to add more than one bank account in an ATM card, so that the user need not carry more cards with them and complication of handling passwords. Here in this one, we embed more than one bank account so that the user can transact as he wish with a single swipe. For security we use pin password with a cipher key generated during the card authentication time.

Index Terms— ATM, banks, card authentication, cipher key, embedding accounts, user authentication, pin.

1 INTRODUCTION

ATM is an abbreviation of Automated Teller Machine. It is introduced in the year 1959 for encouraging self service in retail banking. This makes people to deposit, withdraw and transfer amount without the help of banking personnels and it can be done at anytime and anywhere. At first, the ATM was made to tansact for the particular bank customers but later on the ATMs are connected to interbank network, so that it enables people to deposit, withdraw and transfer amount from the ATM machines not belonging to that particular bank (i.e.) any one can access any banks ATM machine to carry out their transactions. ATMs rely on authorisation of a financial transaction by the card issuer or other authorizing institution via the communication network. This is often performed through an ISO 8583messaging system. Many bank charges ATM usage fees from the customers for the transactions.

At present every customer has an individual ATM card for each and every bank in which he/she maintains account. So handling the cards, their passwords play a major role here. So to overcome these difficulties we embedded more than one bank account of the user in a single ATM smart card, so that the user can swipe the card and can select the bank from which he/she are interested to carry out transaction.

- *Mr.Gokul.R currently pursuingbachelors degree program in computer science engineering in GKM College of Engineering and Technology, Chennai, India. E-mail: gokul.petit@gmail.com*
- *Mr.Godwin Rose Samuel.W currently pursuingbachelors degree program in computer science engineering in GKM College of Engineering and Technology, Chennai, India. E-mail: godwingrs22@gmail.com*
- *Mr.Arul.M currently pursuingbachelors degree program in computer science engineering in GKM College of Engineering and Technology, Chennai, India. E-mail: arulmohan07@gmail.com*
- *Mrs.Sankari.C currently working as a ASSISTANT PROFESSOR in , GKM College of Engineering and Technology, Chennai, India. E-mail: san_nad3@yahoo.co.in*

2 EXISTING SYSTEM

An automated teller machine (ATM) or cash machine is an electronic device that allows a bank's customers to make cash withdrawals and check their account balances without the need or human teller. Many ATMs also allow people to deposit cash or cheques, transfer money between their bank accounts, top up their mobile phones prepaid or even buy postage stamps.

In most modern ATMs, the customer identifies him or herself by inserting a plastic card with magnetic strip or plastic smart card with a chip that contains his or her account number. The customer then verifies his or her identity by entering a passcode (i.e.) personal identification number (PIN) of four digits. If the number is entered incorrectly several times consecutively (usually three), most ATMs will retain the card as a security precaution to prevent an unauthorized user form discovering the PIN by guesswork and so on. Moreover there is a limitation in transaction for the other bank customers in using the ATM of some other bank crossing the limit they have to pay transaction fees.

3 LITERATURE SURVEY

3.1 Smart Card & Security Basics

This Paper gives a overview of basics of smart card and its application and how it is used in various sectors.It also deals with security algorithm during encryption and decryption of data's.This Paper tells us that why smart card is preferred for banking system than other type cards.

A Smart card is type of chip card embedded with computer chip that stores and transacts data between users. It was introduced in Europe nearly three decades ago to pay phone bills.Smart cards greatly convenience and security of any transaction.They provide tamper proof storage of user and account identity. Smart cards systems have proven to be more reliable than other machine-readable cards.

The card is made from PVC, Polyester or Polycarbonate. The card layer are printed first and then laminated in a large press. The next step in construction is the blanking or die cutting.The card consists of several layers to prevent from card damage.

Tools used for implementation are Fishbowl-To contain, isolate and monitor an unauthorized user and IDIOT(Intrusion Detection In Our Time)-A system that detects intrusions using pattern-matching.

3.2 Smart card based Identity Card And Survey

This paper provides an overview of smartcard based ID cards and their security aspects. It tells us about how cards are manufactured and different types of cards.

The use of smart card technology in the banking sector represents a smart first step to preserving and protecting individual privacy while achieving secure, strong identity verification. The system must protect each individual information at all times, including while the information is being stored and while it is being used.Smart cards are credit card- sized, often made of flexible plastic and are embedded with a micromodule containing a single silicon integrated circuit chip with memory and microprocessor.The chip cards are of three types namely contact cards, contactless cards and multicomponent cards.

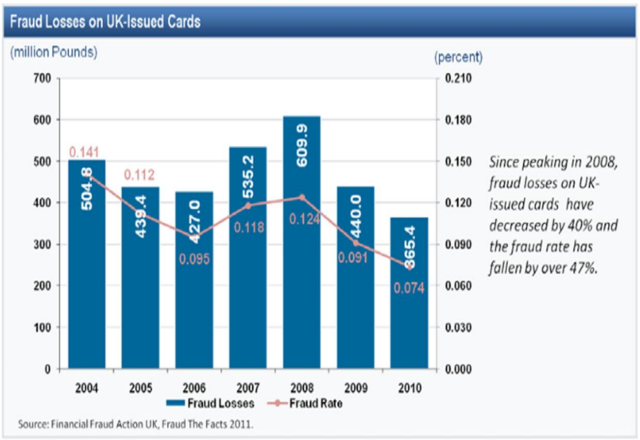
Tools Used For Implementation are Microprocessor Unit-To execute Programmed Instruction, I/O controller-To Manage the flow of data and Read Only Memory(ROM)-To store instructions into the chip.

3.3 Chip-and-PIN: Success and challenges in reducing Fraud from Federal Reserve Bank of Atlanta

Traditional Payment cards have evolved in much of the world and now rely on the EMV (Europay, MasterCard, and Visa) global standard using chip technology.Transaction conducted with EMV chip –embedded cards (smart cards) that uses PIN verification are more secure than transaction conducted using magnetic strip technology.

EMV cards are used globally in which United stated stand apart in experience, chip-and-PIN cards have successfully reduced fraud on face-to-face transactions. However, these cards have less impact on overall fraud levels as fraudsters have shifted their focus to non-chip transactions.

Chart 1: Fraud Losses on UK-Issued Cards



.

Tools Used For Implementation are Session keys-Generated every time when a secure channel is initialised, C-MAC-For securing Messaging and, ALGSCP-Algrothim for identifying the secure channel protocol.

3.4 Examining Smart-Card Security under the Threat of Power Analysis Attacks

This paper examines how monitoring power consumption signals might breach smart-card security.We examine the noise characteristics of the power signals and develop an approach to model the signal-to-noise ratio (SNR)

Cryptographers have traditionally analysed the security of ciphers by modelling cryptographic algorithm as ideal mathematical objects.The input is given to the cryptographic algorithm along with secret key and a cypher text is generated.

3.5 Secure Internet Banking Application

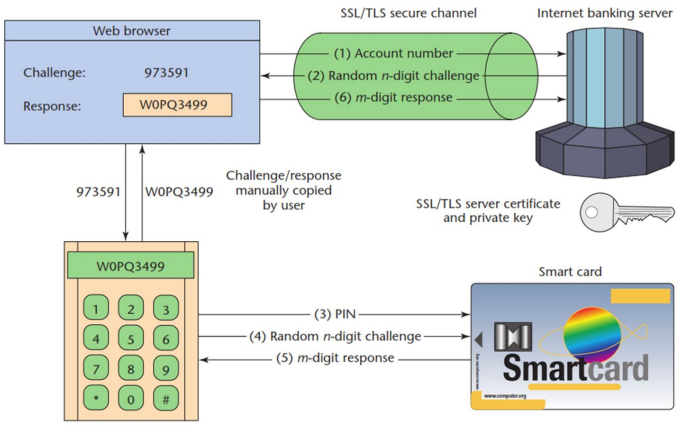
This paper tells about how authentication can be kept safe during malicious software attacks.Here short-time passwords and one on certificate are used to protect the authentication.

There two types of common attack during internet banking authentication are,

1. Offline credential stealing attacks
2. Online channel-breaking attacks

Here short lived passwords are generated using offline card reader and smart card to manage the authentication.Hence the transaction can be done without any malicious attacks.

Tools used for Implementation are SSL/TLS server certificate and, Private Key.



3.6 Benefits Of Smart cards versus Magnetic Stripe Cards for Healthcare Application

Smart cards have significant benefits versus magnetic stripe cards for healthcare applications. Smart cards are highly secure and are used worldwide in applications where the security and privacy of information are critical requirements.

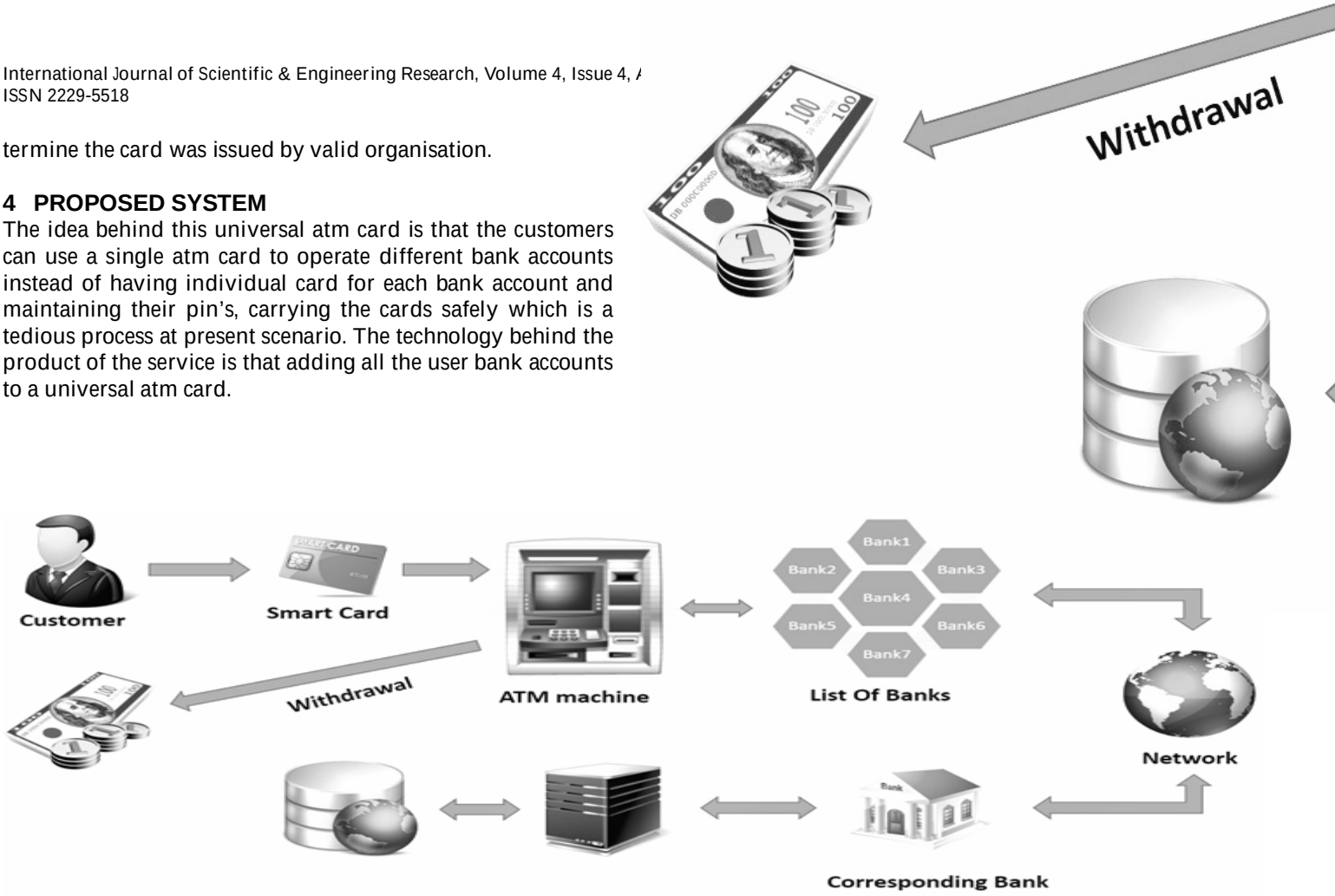
Smart cards embedded with microprocessors can encrypt and securely store information, protecting the patient's personal health information. Smart cards use secure chip technology and are designed and manufactured with features that helps to prevent counter attacks

Tools used for Implementation isDigital Signature-To de-

termine the card was issued by valid organisation.

4 PROPOSED SYSTEM

The idea behind this universal atm card is that the customers can use a single atm card to operate different bank accounts instead of having individual card for each bank account and maintaining their pin's, carrying the cards safely which is a tedious process at present scenario. The technology behind the product of the service is that adding all the user bank accounts to a universal atm card.



In this the user swipes his/her smart card in the ATM machine, then it request for authentication in the server side. After the user is authenticated, then it displays the list of all banks that the user is having account. Now the user can select the bank from which he/she is willing to perform transaction. After selecting the bank the request is sent to the corresponding bank through a network and links it with the banks server for accessing the database of the user or customer so that the transaction is processed.

5 Advantages of smart card over magnetic cards

FEATURE	SMART CARD	MAGNETIC CARD
Reduction in fraud	✓	x
Accuracy	✓	x
Positive identification	✓	x
Security	✓	x

6 FUTURE ENHANCEMENT

Since more than one bank accounts are being added, the existing PIN security is not sufficient enough, so we can embed a biometric scan in the smart card i.e. multicomponent card. So that the user holds the card such that the finger rests on the biometric scan reader while he swipes the card and the image is authenticated at the real time. No one other than the user and his/her nominees can use the card. Only if the thumb impression matches the next step is processed otherwise the transaction will not be allowed until the user is authenticated.

7 CONCLUSION

Thus the user can manage his/her multiple accounts in various banks with the help of this single smart card which provides easy access and reduces the complexity of managing more than one ATM card and their passwords. This also leads to lessen the transaction charges that were leived on the users/customers for transaction and decrease in the production of smart cards for each every account the user has. By implementing this the ATM fraud i.e. skimming etc can be avoided.

ACKNOWLEDGMENT

We wish to thank Dr.N.Ramaraj Principal, Mrs.Neelavani HOD/CSE, Mrs.Thangarevathy HOD/IT and other staff members of GKM College of engineering and technology who gave us full support through out our work for making it a great successful one.

REFERENCES

[1] **"Smart Card & Security Basics"-**CardLogix, paper no.:710030 www.cardlogix.com

[2] **"Smart card based Identity Card And Survey"-**White Paper JKCSH (Jan Kremer Consulting Services).

[3] **Chip-and-PIN: Success and challenges in reducing Fraud from Federal Reserve Bank of Atlanta"-**Douglas King, Jan 2012

[4] **"Examining Smart-Card Security under the Threat of Power Analysis Attacks"-**Thomas S.Messaerges member IEEE, Ezzat A.Dabbish member IEEE, and Robert H.Sloan senior member IEEE vol.51, No. 5, MAY 2002

[5] **"Secure Internet Banking Application"-**Alain Hiltgen, Thorsten Kramp

[6] Fingerprint Verification Using Smart Cards for Access Contol Systems, Raul Sanchez-Reilllo, IEEE AESS Systems Magazine , September 2002

[7] **"Benefits Of Smart cards versus Magnetic Stripe Cards for Healthcare Application"-**Smart card Alliance 2011

[8] "On the design of an Embedded Biometric Smart Card Reader" Dong-Sun Kim, Member, IEEE, Seung-Yerl Lee,Member, IEEE, Byuing-Soo Kim, Member, IEEE, Sung-Chul Lee and Duck-Jin Chung, Member, IEEE, VOL. 54, NO. 2, MAY 2008