Wireless Serial Data Synchronization Methodology for Secured Money Transaction Using Multi Account Embedded ATM Card

[1]Rakhee Patil,[2]Gayathri S,[3]PradeepKumar,[4]Soumya K

Department of E&I , RYMEC , Ballari

Abstract*- The need of money can only be satisfied when you are carrying money with you. That also increases the risk of getting robbed. This research focuses on how to enhance security of transactions in Automatic Teller Machine system using a multi-factor authentication system (PIN and Fingerprint). This research proposed a highly secured Automatic Teller Machine banking system using an optimized Advanced Encryption Standard (AES) algorithm. This research proposes two levels of security. Firstly we consider the security level at the client side by providing biometric authentication scheme along with a password of 4-digit long. Biometric authentication is achieved by considering the fingerprint image of the client. Secondly we ensure a secured communication link between the client machines to the bank server using an optimized energy efficient AES processor. The fingerprint image is the data for encryption process and 4-digit long password is the symmetric key for the encryption process. To get a low power consuming Automatic Teller Machine, an optimized AES algorithm is proposed in this research. In this system biometric and cryptography techniques are used together for personal identity authentication to improve the security level.

1.INTRODUCTION

In most modern ATMs, the customer identifies himself 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 pass code (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 from 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.

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.

2.LITERATURE SURVEY

In the existing system, 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 propose a system to embed more than one bank account of the user in a single ATM smart card, so that the user can swipe the card and will be able to select the bank from which he/she is interested to make a transaction [1].

Personal identification number (PIN) is a common method to authenticate a user for various devices including automatic teller machines (ATMs), mobile phones, and so on. However, if someone observes the input procedure by using a tiny camera, he can easily get the PIN. This kind of attack is called ‘shoulder surfing attack’ (SSA).

We presenting new pin entry method, it contains two parts that is four digit with one symbol which is given by user of the account. We adopt a completely different approach to the existing problem, and present a secure and practical PIN entry method. According to our experiments, the proposed method significantly reduces the error probability. The Principle idea behind this is instead of bank setting the new password user can set the new password to avoid the card blocking procedure taken up by the banks if the user enters the wrong password more than three times [2].

Existing measures adopted by financial institutions require ATM card holders to optionally subscribe to financial transactions message alerts through Short Message Services (SMS) (debit and credit transactions) and the use of posters pasted in banking halls to warn customers on the need to protect PIN numbers from unauthorized users. These measures are purely informative and do not adequately deal with the problems in real time. In this proposed research work, we introduce a Real Time Instructive SMS-Based scheme called MophTem (Mobile phone Text message) scheme which compels

all customers to subscribe to SMS alerts as a basis for initiating transactions on their account.

Every time the user's account is accessed, a message will be sent to the registered mobile number to authorize the transaction. Only after the user's confirmation is received, the transaction is processed [3].

Cloud computing is a key technology to provide security for any advanced systems. In the scenario we are depicting, we leverage the use of the Cloud technology to reproduce real world scenarios encompassing distributed systems, e.g., several ATM centres belonging to the same system and deployed over different cities. we propose the adoption of a Private Cloud Infrastructure model to build up an advanced ATM system that will replace the existing systems by overcoming the problems which are there in the current systems and then to apply proposed methodology, after assessing the vulnerabilities of the system[4].

3.BLOCK DIAGRAM

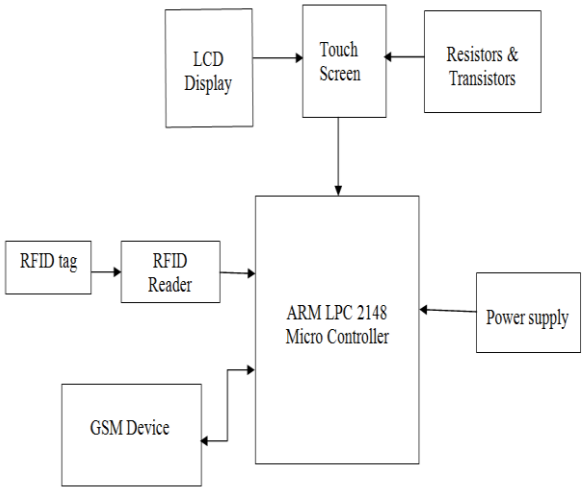


Figure : Model block diagram

Hardware Requirements:

- Microcontroller – ARM LPC2148
- GSM modem
- RFID reader and cards
- 7812/ 7805 voltage regulators for power supply
- Power supply circuit
- Fingerprint Reader

Software Requirements:

- Embedded c
- Keil-c compiler
- Flash magic burner software

4.IMPLEMENTATION

In our proposed work we are using RFID cards as ATM cards. When user brings RFID card near RFID reader then on the touch screen authentification page will display. If correct user name and password is entered then security password will be sent to user mobile, then user has to enter the received number(OTP) on the screen.

After successful login, all bank symbols will be displayed on the screen, and then user has to select the corresponding bank to perform transaction. Before any transaction again security number is sent to confirm the transaction.

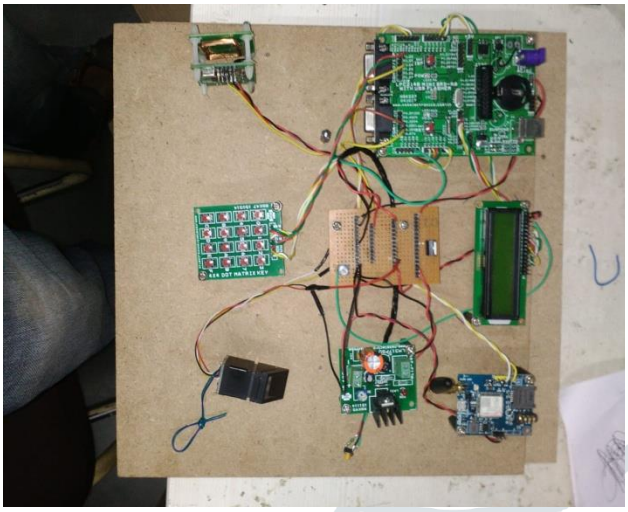
Whenever ATM user enters the ATM machine he/she will get SMS to their mobile indicating their transaction is being started. In reply the ATM user needs to reply by entering their password.

When ATM machine asks for password they have to enter the same password which they have forwarded from their mobile. If the enter any other password other than that transaction will be stopped. Advantage of this system will be every time user can change the password for every transaction made.

When the user enters the amount he/she will get a SMS again to their mobile asking whether cash to be withdrawn or not. If they want they can stop the transaction at this point also. Also, when making purchases, the user will get a notification message saying that a transaction is being made from his account. Only after the user authorization is received, the transaction is allowed. Else the transaction is blocked then and there itself.

Thus the user can manage his/her multiple accounts in various banks with the help of this single smart card which provides easy access. Reduces the complexity of managing more than one ATM card and their passwords. Leads to avoiding transaction charges levied on the users/ customers for transactions done in ATMs other than their respective banks. Production cost of ATM cards can be reduced.

5.CIRCUIT IMPLEMENTATION



6.ADVANTAGES

The proposed method is operationally feasible because here the cost of each device is much lower compared to those products available in the market presently.

7.APPLICATIONS

- Can be implemented on existing ATM systems.
- We can embed a biometric scan in the smart card i.e. multi component card.
- This method can be implemented for:
    1. Office security
    2. Colleges
    3. Hospitals
    4. Parking system

8.CONCLUSIONS

Thus the user can manage his/her multiple accounts in various banks with the help of this single smart card which provides easy access. Reduces the complexity of managing more than one ATM card and their passwords. Leads to avoiding transaction charges levied on the users/ customers for transactions done in ATMs other than their respective banks. Production cost of ATM cards can be reduced.

9.REFERENCES

[1] Gokul.r, Godwin Rose Samuel's, Arul's, Sankari.C**"** *Multi Account Embedded ATM Card***",** International Journal of Scientific and Engineering Research, Volume, Issue 4 APRIL 2013, ISSN 2229-5518

[2] Chang Soon Kim, Mun-Kyu Lee**"** *Secure and User Friendly PIN Entry Method***"**, IEEE, Inchon 402-751, 2010

[3] Ugochukwu Onwudebelu, Olumide Longe, Sanjo Fasola, Ndidi C. Obi and Olumuyiwa B. Alaba **"***Real Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM Systems* **"**, 3rd IEEE International Conference on Adaptive Science and Technology 2011

[4] Antonio Marotta, Gabriella Carrozza, Luigi Battaglia, Patrizia Montefusco, Vittorio Manetti SESM S.C.A.R.L**, "***Applying the SecRAM Methodology in a Cloud-based ATM Environment* **"** IEEE International Conference on Availability, Reliability and Security,2013

[5] Harshal M. Bajad1Sandeep E. Deshmukh Pradnya R. Chaugule Mayur S. Tambade **"***Universal ATM Card System***",** International Journal of Scientific and Engineering Research, Volume 1, Issue 8 OCTOBER 2012, ISSN 2278-0181

[6] Philip K. Chan, Wei Fan **"***Distributed Dam Mining in Credit Cud Fmud Defwdon"* IEEE, NOVEMBER/DECEMBER 1999

[7] Sebastien Jean, Didier Donsez, Sylvain Lecomte "*Using Some Database Principles to Improve Cooperation in Multi-Application Smart Cards*" IEEE, JULY 2001

[8] Ling-Yu Duan. Xiao-Dong Yu, Qi Tian ,Qibin Sun "*Face pose analysis from mpeg compressed video for surveelance applications"*IEEE, MARCH 2003

[9] Vinod Chcrian Joseph, Kyung Hee Lee, Doohyun Kim, Sung Ho Ahn, Ji-Young Kwak "*Embedded ATM Access Point: Optimal Design at Food Court"* IEEE 10th Asia-Pacific Conference on Communication and 5th International Symposium on Multi-Dimensional Mobile Commnications, SEPTEMBER 2004

[10] Jae Hyung Joo, Jeong-Jun Suh, and Young Yong Kim, "*Secure Remote Usim(Universal Subscriber Identity Module) Card Application Management Protocol For W-Cdma Networks*" IEEE,APRIL 2006