SURVEY ON CREDIT CARD SECURED TRANSACTION USING OTP

P.MEENAKSHI , B.VINODH KUMAR

Abstract – **The main objective of the research work is to develop an embedded system, which will be for Credit Card secured transaction. This paper describes a method of implementing two way authentications. The person has to provide access during transaction by triggering the text message. While swapping the Credit card the system will send authentication message to the person mobile number by the GSM modem connected to the ARM microcontroller. The message will be delivered based on the database of every individual. After receiving the message the person can continue the process by entering the four digit PIN number which is already exist in the Credit Card, after this process OTP (One Time Password) or a dummy password will be given to the user. By using One Time Password the person can continue the further transaction. After the transaction is over the password cannot be reused. A new OTP password will be generated for each and every transaction.**

Keywords – **Credit Card, Two way authentication, One Time Password (OTP), Text message, GSM modem.**

Manuscript received March,2015.

P.MEENAKSHI[1]*,PG Scholar, M.E. Embedded System Technologies, Department of ECE, Anna University, Sri Shakthi Institute of Engineering and Technology Coimbatore, India.*

B.VINODH KUMAR[2]*,(Ph.d) HOD, Department of Electronics and Communication, Sri Shakthi Institute of Engineering and Technology Coimbatore, India.*

I.INTRODUCTION

Now-a-days, in the self-service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. This is usually done by the insertion of an Credit card which contains a unique card number and security information such as a PIN number which is unique to every user. Anybody can be in the possession of the card and the person may have knowledge of the users PIN. This makes this approach vulnerable to Credit card fraud. The two way authentications are many in use for cash withdrawal in Credit card transaction. By using mobile phone, a One Time Password (OTP) or Mobile Phone Authentication Approval is the second step authentication. Because of its multiple step to authenticate the user, the system complexity get increases but it provides higher level of security.

II. RELATED WORK

In the paper [3], proposes a new multilayered detection system complemented with two additional layers: communal detection finds real social relationships to reduce the suspicion score, and is tamper resistant to synthetic social relationships. Spike detection finds spikes in duplicates to increase the suspicion score, and is

ISSN: 2278 – 909X

probe-resistant for attributes. Results on the data support the hypothesis that successful credit application fraud patterns are sudden and exhibit sharp spikes in duplicates. Although this research is specific to credit application fraud detection, the concept of resilience, together with adaptively and quality data are general to the design, implementation, and evaluation of all detection systems. In the paper [4], proposes to detect fraudulent transaction through the neural network along with the genetic algorithm. Genetic algorithm are used for making the decision about the network topology, number of hidden layers, number of nodes that will be used in the design of neural network for our problem of credit card fraud detection. For the learning purpose of artificial neural network we will use supervised learning feed forward back propagation algorithm. In the paper [5], to the classification of credit applications that has the potential to adapt to population drift as it occurs by Adaptive online algorithm. It a novel methodology for the classification of credit applications that has the potential to adapt to population drift as it occurs. This provides the opportunity to update the credit risk classifier as new labelled data arrives. Assorted experimental results suggest that the proposed method has the potential to yield significant performance improvement over standard approaches, without sacrificing the classifier's descriptive capabilities.

III. SYSTEM ANALYSIS

A. Existing System

There is no security layer is implemented in the credit card except PIN number. Credit card's have not only changed the banking perspective of the world, but a general perspective as well. But in an era where security threats consistently hover around business processing and day to day activities, Credit card's around the world lack security aspects in a more generic sense. If one was to have their Credit card misplaced to be found by someone who is able to crack the PIN code or knows it already, there is no such facility in the currently used Credit card's to determine whether the event of identity theft is taking place or not until it is has already taken place. Nowadays some advanced techniques are used in some Credit card sectors like retina scan or fingerprints for money transaction purposes, but that is something which would turn out to cost the banks and Credit card vendors quite a fortune to be implemented throughout the network, as hardware enhancement cost is likely to be greater than a software enhancement cost. So the advanced technique is failure in such cases.

B. Proposed System

In this paper it is analyzed what are the problem people faced in the existing technology. Especially Biometric method provides more complexity to the user. This project helps to overcome the problem of complexity and provides easiest way to secure the Credit card transactions. Whenever Credit card is inserted into the Credit card slot, the system requires PIN to authenticate in the user mobile. If PIN gets verified, it reply OTP (One Time Password) as a authentication message to the user's mobile. If the user proceed by the received OTP to make a transaction, then transaction process takes place. Otherwise the transactions get terminated. The proposed system uses GSM modem for sending authentication message to the user.

ISSN: 2278 – 909X

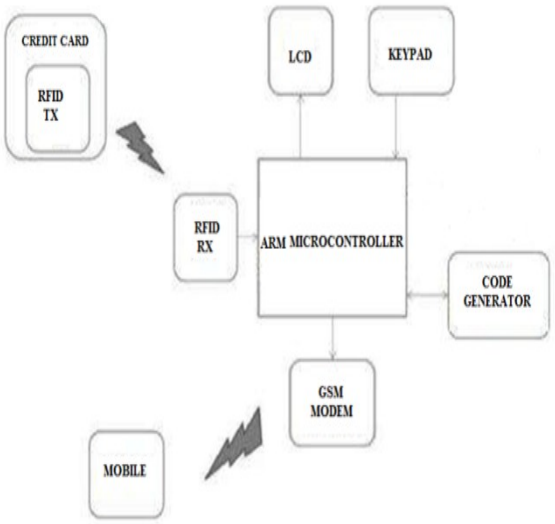

Fig 1 : Block diagram of proposed system

IV. SOFTWARE DESCRIPTION

A. MPLAB IDE

MPLAB IDE is a Windows-based Integrated Development Environment (IDE) for the Microchip Technology Incorporated PICmicro® microcontroller (MCU) families. MPLAB IDE allows you to write, debug, and optimize PICmicro MCU applications for firmware product designs. MPLAB IDE includes a text editor, simulator, and project manager. MPLAB IDE also supports the MPLAB ICE 2000 emulator, MPLAB ICD debugger, PICSTART® Plus and PRO MATE® II programmers, and other Microchip or third party development system tools. The MPLAB X IDE is the new graphical, integrated debugging tool set for all of Microchip's more than 800 8-bit, 16-bit and 32-bit MCUs and digital signal controllers, and memory devices.

B. Proteus

Proteus 8 is best simulation software for various designs with microcontroller. It is mainly popular because of availability of almost all microcontrollers in it. So it is a handy tool to test programs and embedded designs for electronics hobbyist. Now simulate the programming of microcontroller in Proteus 8 Simulation Software. After simulating the circuit in Proteus 8 Software can directly make PCB design with it so it could be a all in one package.

C. Embedded C Programming

The 'C' Programming Language was originally developed for and implemented on the UNIX operating system, by Dennis Ritchie in 1971. One of the best features of C is that it is not tied to any particular hardware or system. C is often called a middle-level computer language as it combines the elements of high-level languages with the functionalism of assembly language. To produce the most efficient machine code, the programmer must not only create an efficient high level design, but also pay attention to the detailed implementation.

V. RESULT & ANALYSIS

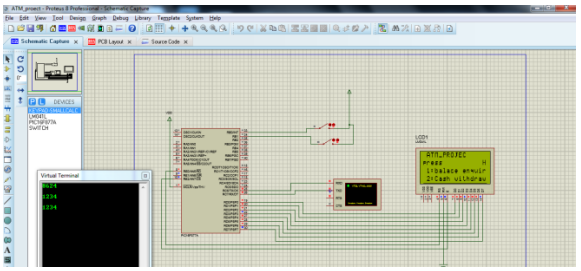

Fig 3 : Simulation window

The output window for starting the simulation is shown in the above figure. In this window the initial stage for starting the transaction can be done by using the run command to execute the terminal window.

ISSN: 2278 – 909X

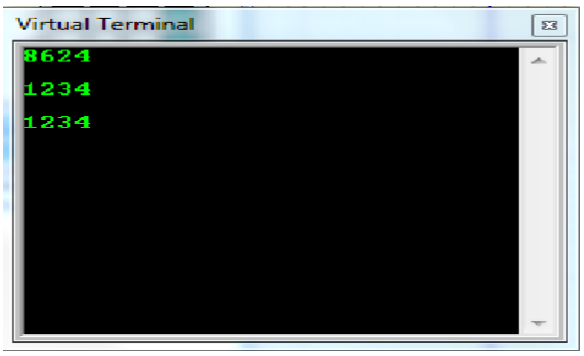

Fig 4 : Virtual terminal window

The virtual terminal window will act as a mobile. In this window original PIN (8624) should be entered and send to start the transaction. Then we will receive the dummy code which is the One Time Password(OTP) (1234) is received and the code is used to proceed the transaction.

VI. CONCLUSION

The proposed system based on microcontroller is found to be more compact, user friendly and less complex which can readily be used in order to perform the transaction. In this paper we have implemented a new mechanism named OTP generation technique which will provide more security for accessing like automatic perception of account details with message alert via GSM modem, comparative code authentication and automatic termination of session. If some authorized person uses the Credit card we may be able to identify them. Due to the probability of high technology (GSM) used this "Credit card Secured transaction using OTP" is fully software controlled with less hardware circuit. The feature makes this system is the base for future systems.

REFERENCES

[1] June 2014, Advanced Security Model for Detecting Frauds in ATM Transaction by Vivek V. Jog Nilesh R. Pardeshi.

[2] January 2014, Abhijeet S. Kale Sunpreet Kaur Nanda "A Review Paper on Design of Highly Secured Automatic Teller Machine System By Using Aadhaar Card And Fingerprint"

[3] "Resilient Identity Crime Detection"- Clifton Phua, Member,Kate Smith-Miles, Senior Member,Vincent Lee, and Ross Gayler,2011.

[4] NG Pavlidis, DK Tasoulis, NM Adams and DJ Hand," Adaptive consumer credit classification "Journal of the Operational Research Society (2012).

[5] Linda Delamaire , Hussein Abdou , John Pointon ," Credit card fraud and detection techniques: a review", Banks and Bank Systems, Volume 4, Issue 2, 2009.

[6] I Martin,"Too Far ahead of its Time:Barclays, burroughs and Real Time Banking,"Annals of Historyof Computing,IEEE Volume.

[7] " A Password Strectching method using specific Salts". Changhee Lee, Heejo Lee.

[8] "J. Kelsey, B.Schneier, C.Hall,andD.Wanger, Secure applications of low-entropy keys". Lecture Notes in Computer Science,1396:121-134,1998.

[9] "Stronger Password Authentication Using Browser Extensions, Proceedings" of the 14thUsenix Security Symposium, 2005.Blake Ross, Colin Jackson, Nicholas Miyake, Dan Boneh and John C.Mitchell.

ISSN: 2278 – 909X