



ISSN: 2319-5967

ISO 9001:2008 Certified

International Journal of Engineering Science and Innovative Technology (IJESIT)

Volume 2, Issue 2, March 2013

TM Fortification and Facile Approach Based on GSM and RFID

Sharadha.M, Gokul Saravanan.T, Suresh Kumar.V, Priya.S

Department of Electronics and Communication Engineering Angel College of Engineering and Technology

Abstract - Currently, security is becoming a prime factor in the society. It's becoming a challenge for everyday activities such as access control, cash terminals, public transport, internet etc, where the user authentication is required prior to giving access to confidential information, RFID in conjunction with GSM technologies bring a solution to such necessitate. The usage of ATM card is increasing day by day, at the same time it paves way for many other Malpractices(card or cash being stolen, hacking of passwords). In order to overcome this, RFID based ATM smart card will yield enhanced results. This project describes the hardware and software co-design of a RFID and GSM. RFID(Radio Frequency Identification), a contactless smart card is used for accessing ATM terminal, the random code generated is sent to the mobile which is entered in the ATM terminal then the code undergoes verification process, , if the code matches then the regular process begins, if there is mismatch of codes then the access is denied. These initial steps will help in cash withdrawal in an easy and secured manner against forges.

Index Terms— RFID, GSM, ATM.

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. Using the ATM (Automatic Teller Machine) which provides customers with the convenient banknote trading is very common. However, the financial crime case rises repeatedly in recent years; a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. 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. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. Using credit card and password cannot verify the client's identity exactly. This paper includes RFID and GSM for security and easy access. The RFID will be integrated in the ATM, so when the person enters in to the ATM terminal with ATM card, the ATM machine will identify the account and bank of the user. Then the user selects the account then random code generated password from the code generator is sent to the mobile (GSM) of the customer. Then the customers have to type the code from the mobile send by the server after which the password undergoes verification process. If the password is not matched the access will be denied. If the password is matched then the further process of cash withdrawal begins. One more advantage in our system is that after the user left the ATM terminal the account will get involuntarily closed. This will ensure safe as well as easy access of ATM in the terminal.

II. LITERATURE SURVEY

The paper [1] describes one of the oldest biometric techniques is the fingerprint identification. Fingerprints are used as a means of positively identifying a person as an author of the document and are used in law enforcement. Fingerprint recognition has a lot of advantages such as the fingerprint is compact, uniqueness for every person, and stable over the lifetime. A predominate approach to fingerprint technique is the uses of minutiae see Figure 1 The traditional fingerprints are obtained by placing inked fingertip on paper; now compact solid state sensors are used. The solid state sensors can obtain patterns at 300 x 300 pixels at 500 dpi, and an optical sensor can have image size of 480 x 508 pixels at 500 dpi. The paper [2] proposes several hand parameters can be used for person identification such as Hand shape pattern Blood vessel pattern, Palm line pattern. The image obtained from the CCD camera is a 640 x 480 pixels color photograph in JPEG format. Not only the view of the palm is taken, but also a lateral view is obtained with the side mirror. To extract features, the image is first converted into black and white, and spurious pixels are also removed at this point. Rotation and resizing of image are also done to eliminate variations caused by position of camera. This is follow by Sobel edge detection to extract contours of the hand.

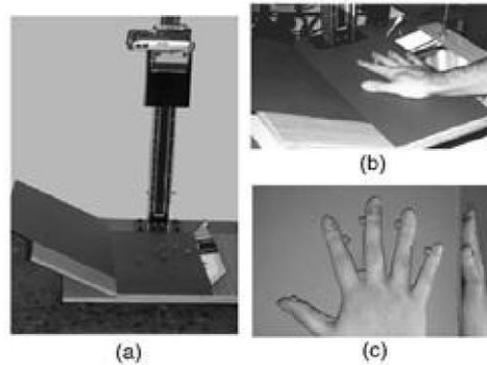


Fig. 1 Hand Geometry



Fig. 2 Minutiae, ridge endings and ridge bifurcations.

In paper [3] the signature differs from above mentioned biometric system, it is a trait that characterize single individual. Signature verification analysis the way a user signs his or her name. This biometric system can be put into two categories, on-line and off-line methods. On-line methods take consideration of signing features such as speed, velocity, rhythm and pressure are as important as the finished signature's static shape. Whereas, off-line classification methods are having signature signed on a sheet and scanned. People are used signatures as a means of transaction-related identity verification, and most would see nothing unusual in extending this to encompass biometrics. Signature verification devices are reasonably accurate in operation and obviously lend themselves to applications where a signature is an accepted identifier. Various kinds of devices are used to capture the signature dynamics, such as the traditional tablets or special purpose devices. Special pens are able to capture movements in all 3 dimensions. Tablets are used to capture 2D coordinates and the pressure, but it has two significant disadvantages. Usually the resulting digitalized signature looks different from the usual user signature, and sometimes while signing the user does not see what has been written so far. This is a considerable drawback for many (inexperienced) users.

In paper [4] the face recognition technology has applications in many wide ranges of fields, including commercial and law enforcement applications. This can be separate into two major categories. First is a static matching, example such as passport, credit cards, photo ID's, driver's licenses, etc. Second is real-time matching, such as surveillance video, airport control, etc. In the psychophysical and neuro scientific aspect, they have concerned on other research field which enlighten engineers to design algorithms and systems for machine recognition of human faces. A general face recognition problem can be, given still or video images of a scene to identify one or more persons in the scene using a stored database of faces. With additional information such as race, age and gender can help to reduce the search.

Drawbacks of Existing System:

In the above mentioned systems there are many drawbacks which paves way for other malpractices like there is Less probability for preventing theft, The existing process is very tedious, it involves lengthy procedure and comparatively cost wise expensive. In case of numerous Comparing with Biometrics features such as face, fingerprint, hand geometry and signature RFID technology is more stable and reliable.

III. PROPOSED SYSTEM

One's 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 loss to customer. The ultimate solution for avoiding this problem is to integrate the GSM with Smart Card. This Primary System uses the RFID embedded with the existing ATM card to have secure

money transaction. So that the ATM can involuntarily identify the presence of the user by this technique the theft of the card can be avoided. By identifying the card the server sends the code to the concerned mobile of the user (GSM) from the random code generator. The respective code is typed in the terminal to continue with the further process. If the code is matched then the cash withdrawal takes place if not the access will be terminated. Hence secure as well as easy access of ATM usage can be made.

IV. BLOCK DIAGRAM

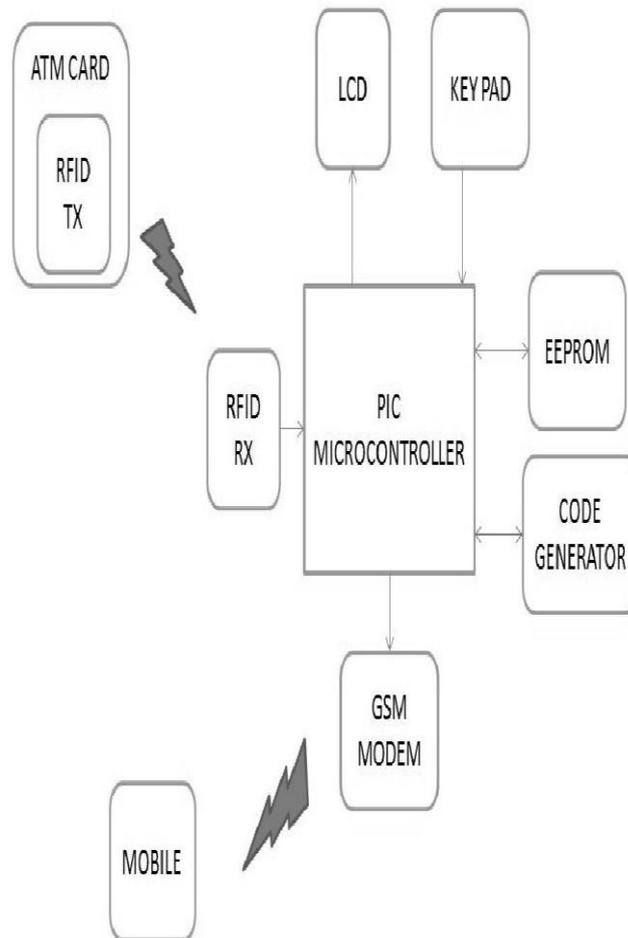


Fig. 3 Block Diagram

The methodology is, when the person enters the ATM terminal with the proposed RFID tag (contact less smart card), the tag holds the details of the user and its account details. Automatically the RFID receiver detects and identifies the particular individual and displays it on the LCD. Now the random code generator generates the random code and sends it the individuals mobile (GSM) via GSM MODEM. The code should be entered by the user using the keypad. The code is authenticated by comparing the entered code and the code generated, if the code is matched then the user can withdraw the cash otherwise the process gets terminated.

V. FLOW DIAGRAM

The flow chart signifies the overall process, the card is brought to the ATM terminal, the card is read by the reader and hence forth identifies the individual and the random code generator generates the random code and sends it to the user mobile, the code has to be typed by the user in the terminal.

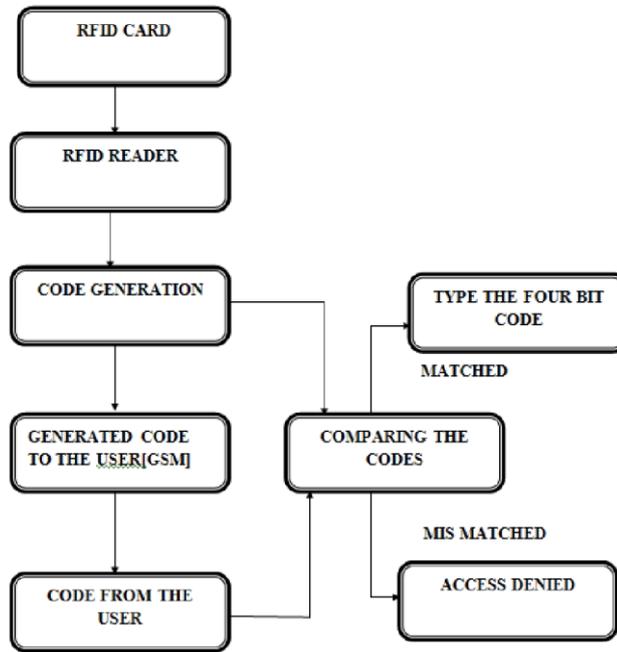


Fig. 4 Flow Diagram

Now the verification process begins the entered code is verified with the code generated, if the code is matched then withdrawal of cash can be made otherwise the access will be denied

VI. COURSE OF ACTION

A. Contact less Smart Card: A contact less smart card contains an embedded antenna that communicates via RF technology. The card communicates with the card reader when it is placed within the reader's magnetic interface. The lack of physical contact makes the contact less card more robust than the contact version.

B. RFID Transmission: The RFID contact less smart card contains the user and the account details which is used to access the ATM terminal, the signal transmitted will be received and read by the RFID reader.

C. RFID Reception: The information in the RFID card will be read by the RFID receiver and authenticates the individual.

D. Random Code Generator: After the authentication the random code generator generates the corresponding password and sends it to the user mobile.

E. GSM Module: The GSM MODEM is used to send the password to the corresponding user

F. Verification: The code from the GSM should be entered in the ATM terminal and the code undergoes verification process with the generated code if the code gets verified then the process of cash withdrawal begins otherwise the process will get terminated.

VII. CONCLUSION

Here, the RFID based contact less smart card is used as the user's ATM card. The RF transmission and reception is done using RFID reader. There are separate RFID transmitters for individual user accounts. If the RFID is brought before the ATM terminal, the RFID reader will read the card number and the account details of the user automatically. Now the random code is generated using the random code generator and the password is sent to the user mobile through GSM MODEM. The code is authenticated by comparing the entered code and the code generated, if the code is matched then the user can withdraw the cash otherwise the process gets terminated.

VIII. FURTHER ENHANCEMENTS

To implement the random code generation random code algorithm is to be created in the random code generator by which the password will be generated and sent to the user mobile phone, the password should be typed in the ATM terminal for further verification process.



ISSN: 2319-5967

ISO 9001:2008 Certified

International Journal of Engineering Science and Innovative Technology (IJESIT)

Volume 2, Issue 2, March 2013

REFERENCES

- [1] Lin Hong, Wan Yifei, Anil Jain. Fingerprint image enhancement: algorithm and performance evaluation [J]. IEEE Transactions on Pattern Analysis and Machine intelligence. 1998, 20(8): 777-789.
- [2] J.Hashemi and E. Fatemizadeh, "Biometric identification through hand geometry," in Proc. Int. Conf. Comput. Tool, 2005, vol. 2, pp.1011– 1014.
- [3] X. Boyen, "Mesh Signatures: How to Leak a Secret with Unwitting and Unwilling Participants," Advances in Cryptology-Euro crypt 2007, M. Naor, ed., vol. 4515, pp. 210-217, Springer Berlin/Heidelberg 2007.
- [4] M. Bichsel and A.P. Pent land, "Human Face Recognition and the Face Image Set's Topology," CVGIP: Image Understanding, vol. 59,pp. 254-261, 1994.
- [5] S.Piramuthu (2007), "Protocols for RFID tag/reader authentication", decision support systems 43, pp.897-917.
- [6] Qinghan Xiao, Senior Member, IEEE, and Mario Savastano , Proceedings of the 2007 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY 20-22 June 2007,| An Exploration on Security and Privacy Issue of Biometric Smart ID Cards|.
- [7] M. Ibrahim and M. Youssef, "A hidden Markov model for localization using low-end GSM cell phones," in Proc. ICC, 2011.
- [8] M. Y. Chen, T. Sohn, D. Chmelev, D. Haehnel, J. Hightower, J. Hughes,A. Lamarca, F. Potter, I. Smith, and A. Varshavsky, "Practical metropolitan-scale positioning for GSM phones," in Proc. 18th Int. Conf.Ubiquitous Comput., 2006.

AUTHOR BIOGRAPHY



Sharadha.M is currently pursuing her bachelor's degree in Electronics and Communication Engineering at Angel College of Engineering and Technology, Tiruppur. Area of interest includes embedded systems, Computer networks and Communication systems. Her area of research is application of embedded system using communication systems. She is a member of IETE.
E-mail ID: sharadha.2508@gmail.com



Gokul saravanan.T is currently pursuing his bachelor's degree in Electronics and Communication Engineering at Angel College of Engineering and Technology, Tiruppur. Area of interest includes embedded systems, Computer networks and Digital electronics. His area of research is application of embedded system using communication systems. He is a member of IETE.
E-mail ID: gokulsaravanan.t@gmail.com



Suresh kumar.V is currently pursuing his bachelor's degree in Electronics and Communication Engineering at Angel College of Engineering and Technology, Tiruppur. Area of interest includes embedded systems, Computer networks and Digital Electronics. His area of research is application of embedded system using communication systems. He is a member of IETE.
E-mail ID: sk.san91@gmail.com



Priya.S is working as assistant professor of electronics and communication department in Angel College of Engineering and Technology, Tiruppur. She has completed her masters in the field of communication, her areas of interest includes communication, network security, image processing. She has presented 2 papers in National and International conferences. She is a member of IETE.
E-mail ID: mailtopriya.sri@gmail.com