International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Location Aware and Safer Cards: Enhancing RFID Security and Privacy during Money Transaction

Pooja J. Deshmukh[1], Bharati Patil[2]

[1]PG Student, Electronics and Telecommunication Engineering, G.H. Raisoni COE &Management, Wagholi, Pune, Maharashtra, India

[2]Associate Professor, Electronics and Telecommunication Engineering, G.H. Raisoni COE &Management, Wagholi, Pune, Maharashtra, India

Abstract: ***Because of the several advantageous of RFID like its low cost, small in size also the objects are identified by the computer, use of RFID in many application is increasing today. But RFID may undergo various types of attacks like ghost-leech attack. Attacker has gained access to the information stored in tag. So we need to apply security measures against this. Security measures like RFID enabled smart card, one time password, location sensing and face identity (biometric). There is up gradation from two factors to three factor authentication and now to four factor authentications. In this paper we have taken money transaction application and applied improved four factor authentication scheme which addresses the problem related to RFID.***

Keywords: RFID, FPGA, biometric, one time password, location sensing

1. Introduction

RFID system consists of RFID tag and reader consisting small antenna. There are two types of RFID tags available in the market active tag and passive tag. Reader sends electromagnetic waves. RFID tag is nothing but the small microchip consist of antenna is tuned to receive these signals. While the passive RFID uses the power from field created by the reader. This power from the reader is used to power the components on the microchip. Generally, any reader can read the information stored in the tag which is not desirable. Because tag contains private information like owner information, PIN, password, secure key. So, malicious user or unauthorized user can gain access to this information. To prevent this unauthorized access in the RFID enabled systems we need to apply security measures to enhance the RFID security [5]. There are many applications of RFID e.g. In military application, toll collection in vehicle system, in money transaction, etc.

In this paper we discussed one of the applications of RFID as secure money transaction (ATM). Here we are using RFID enabled smart card. FPGA is an Reconfigurable system. It provides the performance benefits of ASICs and also the flexibility of processors. FPGA is a Field Programmable gate Array. It is the collection of programmable gates embedded in it. It consist of programmable interconnect. An FPGA provides a balance between performance and flexibility, so they are preferred in many embedded system applications. In real time application speed is important factor need to be considered so, FPGA is used for processing instead of microcontroller. FPGA is a Reconfigurable System has ability to provide the performance benefit of ASICs. Also the flexibility of processors ASIC like microcontroller. FPGA combines the programmability of processors with that of the performance of custom hardware. FPGAs become the primary source of computation in many complex or critical embedded systems because they are able to provide a useful balance between performance and flexibility. FPGAs avoid the high initial cost, the lengthy development manufacturing and cycles, and the intrinsic inflexibility of conventional ASICs.

The organization of paper is as follows: in section 2 we discuss review on literature. Section 3 discusses cryptography in short. Section 4 shows the overall system block diagram. Section 5 describes system block diagram. Section 6 describes its algorithm. Section 7 shows the experimental setup. Section 8 shows the results. Section 9 concludes the paper. What we can add and make improvement is described in short in section 10.

2. Review On Literature

We gone through the various papers and research work it seems that previous work assumes that the communication channel between an RFID reader and its server is secure and concentrate only on the security improvement between the RFID tag and RFID reader But the privacy destruction problems at reader side will become a matter of great concern for individuals and organizations, once RFID reader modules gets extensively deployed in consumers' handheld devices. If the future communication environment for RFID systems is in wireless then there is possibility of increasing the insecurity among the three roles. We have to achieve message security, ambiguity, accessibility and protection of information from being stolen or else tamper with it. In various RFID application systems, handheld device, such as mobile phone, embedded RFID reader modules will be situated everywhere and operated with many RFID tags.

Ref [1] discussed security and privacy issues. Unprotected tags may be susceptible to eavesdropping, traffic analysis, spoofing or denial of service attacks. Approaches for tackling security and privacy issues like Password Protection on Tag Memory, Physical Locking of Tag Memory, active jamming, personal privacy.

Ref [2] discussed attacks at physical, network layer and application layer. Approach to avoid tag and reader collision using anti-collision protocol like ALOHA, TDM/FDM. Using AT commands only authenticated user can perform transaction.

Fan-Lin scheme which consists of three phases initialization, registration, login and authentication discussed in ref [4]. The proposed protocol for biometric authentication is and the reader would imply the presence of attacks. In other words, both the legitimate tag (credit card) and legitimate reader may transmit their locations to a centralized authority. This centralized authority can then compare the information received from both entities that is from valid tag and reader and reject the transaction if the two mismatch. Provably secure because this protocol does not reveal any information about the biometric sample to the authentication server. The proposed scheme consists of client side, terminal side and server side. Even though the scheme achieved privacy protection, it couldn't withstand password attack. Also server side attack is another crucial issue in such remote authentication schemes.

Ref [5] discussed more secure approach via location sensing in addition with three factor authentication scheme discussed above. A difference in the locations of the tag and the reader would imply the presence of such attacks. In other words, both the valid tag and reader may transmit their locations to a centralized authority (issuer bank). This centralized authority can then compare the information received from both entities, if the two mismatches then it reject the transaction.

At present we are using single card or the individual card for the different banks like ICICI, AXIS, HDFC, Etc., The pin number in the Negative Behind the cards. In this system there is a only one pin number. In our scheme we are using pin as well as one time password. Presently cards we are using for transaction is different for different banks. Here we can use the same card for different banks.

3. Cryptography

We know cryptography is the process of encryption and decryption. It is used for the secure data communication. Encryption is the process of converting plaintext into cipher text while decryption is the process of converting cipher text back into plaintext. In Symmetric-key cryptography both the sender and receiver share the same key. Symmetric key ciphers can be implementing as either block. Ciphers or stream ciphers. It is more secure. But the drawback of symmetric key cryptography is the key management especially it is more difficult when number of members in the network are increasing. In asymmetric key cryptography public key is used for encryption while private key is used for decryption. So cryptography technique is used to protect the information from unauthorized user.

4. Overall System Block Diagram

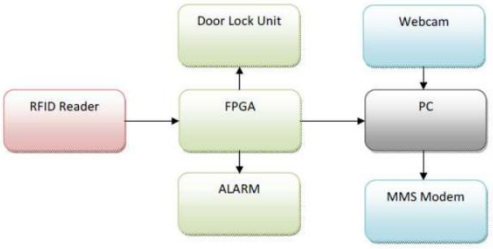

Figure 1: RFID Enabled Money Transaction

5. Description

Hardware used is active RFID tag and reader, FPGA SPARTAN III evaluation board, MMS modem, webcam, PC, buzzer and motor.

SPARTAN III family reduces cost per logic cell because of its low cost it is well suited to a wide range of consumer electronics application. One additional feature over SPARTAN II family is power management, advanced 90 nm process technology combined with, Spartan-3E enhancements, it can deliver more functionality and bandwidth per dollar than was earlier possible. Thus it is setting innovative standard in the programmable logic industry. FPGAs are mainly used in consumer electronics applications, such as broadband access, home networking, display/projection, and digital television equipment, because of their especially low cost; Here in our project we are using active tags because security is important. An active tag supports more bandwidth and therefore larger key sizes. While passive tags have a shorter range and limited in cryptography. Xilinx simulator is used and for coding VHDL is used. FPGA is used for controlling and processing. It receives data from RFID, process it and transmit it to PC. We created GUI in Visual Basic to see the experimental results.

6. Overall System Algorithm

1. Initialize the total design.
2. Read the RFiD information.
3. If location is matched then trigger the web cam.
4. Then capture the image and compare the data base images.
5. Comparison is done depend on the mean, variance and correlation function of the image matrix.
6. Person image is then send to the owner mobile using mms module
7. Owner will give permission using the one time password
8. If person is authorized owner will send positive acknowledgement
9. If positive acknowledgement then login pin will ask
10. If person is not authorized then owner will send negative acknowledgement
11. If negative acknowledgement then alarm will blow and door lock system will on.

In this research work DC motor used as door lock unit. Clockwise rotation of motor will open the door while anticlockwise rotation will close it.

7. Experimental Setup

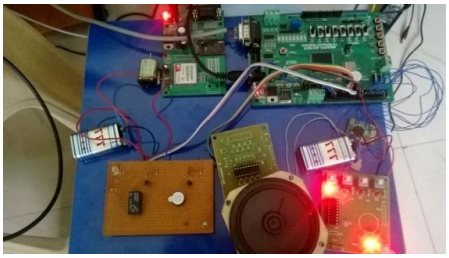

Figure 2: Experimental Setup

8. Results

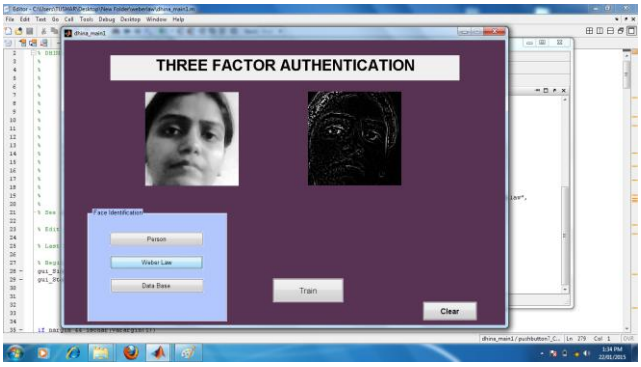

Figure 3: GUI result 1 in MATLAB

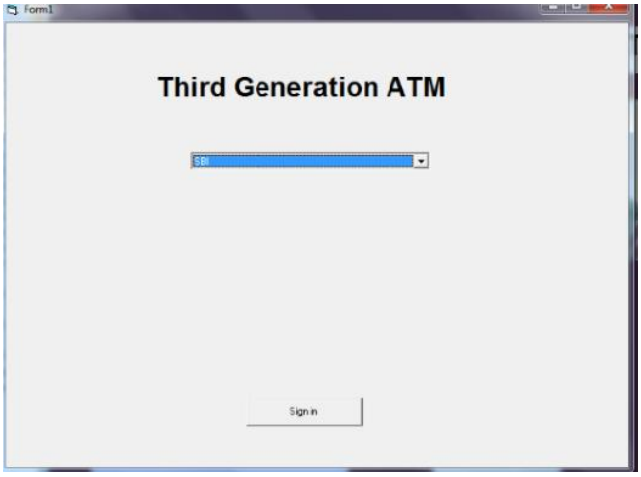

Figure 4: GUI result 2 in VB

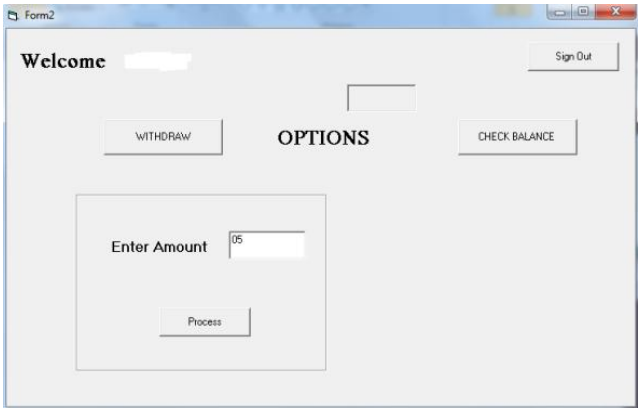

Figure 3: GUI result 2 in VB

9. Conclusion

While the use of RFID technology is increasing across a range of different industries, the associated security and privacy issues need to be carefully addressed. In real time application, accuracy and speed is important. We used MATLAB, Xilinx and Spartan3 evaluation kit. Using PCA technique we checked whether person is authorized or not. Thus this is one of the factor using which we can improve the security in money transaction. This is a high level model for the modification of existing ATM systems using both security protocols as PIN, One Time Password, Biometric face recognition strategy and GSM technology. Using this four factor authentication scheme we can definitely addressed problems which are in the present ATM system. For real time application we can use same card (RFID enabled smart card) for accessing different banks like HDFC, ICICI, AXIS, etc. Hence our system will definitely solve the aspect of transaction security to a precise and great extent. This is helpful to society.

10. Future Work

As use of credit card, debit card is increasing today in the application like online mobile payment system, online shopping, and online billing. But present system is not as secure. Here we implement a system to enhance the security in money transaction using ATM. Based on this, the concept can be extend to the online mobile payment billing systems. In online mobile payment system bank is used as a server and requires JAVA programming. So we can address to the problems during the online transaction. Also we can use more improved method for the face recognition. In future the same can be enhanced with 3D camera and motion capturing technologies for achieving best results.

References

[1] The Government of the Hong Kong Special Administrative Region, "RFID Security", Feb 2008
[2] Madamshetti Yashwanth, A. Parvathy, Kopparapu Srivatsa "RFID & Mobile Fusion for Authenticated ATM Transaction", International Journal of Computer Applications (0975 – 8887), June 2010
[3] RFID security and Privacy, RFID, "Hierarchical ECC based RFID Authentication Protocol", Sec2011 Springer
[4] Harlay Maria Mathew, S. Benson Edwin Raj, "An Improved Three-Factor Authentication Scheme Using Smart Card with Biometric Privacy Protection", IEEE TRANSACTIONS 2012
[5] Di Ma, Member, IEEE, Nitesh Saxena, Member, IEEE, Yan Zhu and Tuo Xiang, "Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing", IEEE Transactions On Dependable And Secure Computing. 10, No. 2, March/April 2013.
[6] Jian Yang, David Zhang, Senior Member, IEEE, Alejandro Jing-yu Yang and F. Frangi, , "Two-Dimensional PCA: A New Approach to Appearance Based Face Representation and Recognition", IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 26, No. 1, .JANUARY 2004
[7] Vikas Kumar, Navneet Jindal, "Enhanced Face Recognition Algorithm using PCA with Artificial Neural Networks", International Journal of Advc Research in Computer Science and Software Engineering (IJARCSSE) Volume 3, Issue 6, June 2013

Author Profile

Pooja J. Deshmukh Received B.E. degree in electronics and telecommunication from Modern College of Engineering, Pune, Maharashtra in 2013 and pursing M.E. (VLSI & ES) in G. H. Raisoni College of Engineering and management Pune, Maharashtra, India 2014-15. She also worked as a lecturer in the same institute. Her area of interest is communication and embedded system.