IMPLEMENTATION FOR ENHANCING SECURITY OF RFID CARD

Shilpa S. Badhiye1,Prof.Rupali S. Khule2
1 student, Electronics and telecommunication Department, MCOERC, Maharashtra, India
2 Professor, Electronics and telecommunication Department, MCOERC, Maharashtra, India

ABSTRACT

Unauthorized money transaction is a very big problem. The main aim of the proposed system is to build a system that defends against unauthorized transaction in RFID. Although a variety of security solutions exist, many of them do not meet the constraints and requirements in terms of efficiency, security, and usability. In an attempt to address these drawbacks, the proposed system is used. In the proposed system on the server side a secure transaction verification scheme is designed which decides whether to make transaction successful or block the card. Many researchers proposed different techniques for unauthorized transaction but all of them required some auxiliary devices to carry with users. In the proposed work there is an interrogation session between reader and user with addition of extra security for secure transaction and according to the behaviour of the transaction theft can be determined.

Keyword: - *RFID, unauthorized transaction, security*

1. INTRODUCTION

RFID is a technology which uses radio frequency to identify objects or peoples. A typical RFID system consists of tags, readers, and backend servers. Tag consists of small microchip with an antenna attached to it. It contains identification number that store information about their corresponding subject and these information is usually sensitive. The tag will broadcast its identification number to any nearby reader and these causes threat to consumer privacy. RFID tags are sensitive to ghost and leech relay attacks. In this type of an attack, an enemy called a ghost transfers the information secretly read from a legitimate RFID device to a leech which combine secretly to plan and prepare a harmful action [2]. The leech can then transmit the forwarded information to a corresponding reader and viceversa, thus a ghost and leech pair can succeed in attack without actually possessing the device, which disturbs the security. Therefore there is a need to work on security and privacy of RFID card. This sensitive information can be used in order to track the owner of the tag or to clone the tag. RFID cards are more durable but in RFID the credit card number and expiry date are not encrypted which presents a security problem. Due to this unauthorized reading it results in fraud. Different authors proposed different solutions for this unauthorized reading like use of blocker tag [3], Faradays cage, motion detection[4], vibrate to unlock[5] and distance bounding protocol[6]. All of these required some auxiliary devices to carry with users and it also affects the original usage model. In the proposed system we build a system which gives location validation and transaction verification. By using this technique we enhance the security in RFID credit card.

2. PROPOSED SYSTEM

The main aim of the proposed system is to enhance security. Security level is enhanced in the proposed system in 5 ways.
Way 1: Interrogation Questions
Way 2: Addition of 3D image
Way 3: Verification code sent to registered email address
Way 4: For invalid location message sent to registered mobile number.
Way 5: From the transaction of customer behaviour can be decided

The proposed system consists of smart card with RFID tag attached to it. RFID reader required to read data from it. The data read by reader is then sent to laptop through UART. The block diagram of the proposed system is shown in Figure 1.

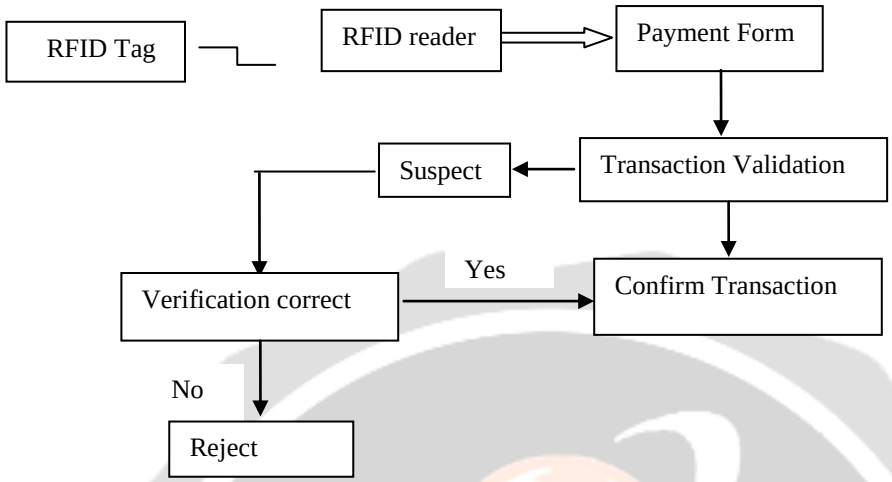

Fig -1: Block Diagram of Proposed System

3. METHODOLOGY AND IMPLEMENTATION

The RFID reader reads the identification number of tag. This tag ID is used as a card number for further process. The RFID reader reports the received tag ID to application software which can interpret the information contained in the tag ID.

1) The payment form consists of registration process which contains registration of users, interrogation question, and points on 3D image. It completes the registration process.

2) In transaction validation if all the data i.e. username, card number, expiry date, passwords and registered location and points on 3D image are correct then only transaction is successful otherwise system assume it as a suspect and starts asking interrogation question , points on 3D image and verification code is sent to registered email address.

3) For invalid location, verification code is sent to registered mobile number. If answers of interrogation questions were wrong then the card will be blocked for 24 hours. Similarly if 3 attempts are failed for 3D image then also the card will be blocked and email is sent to registered email address.

4) Depending on the last 10 transactions, according to HMM algorithm [7] behaviour of the user is decided as low, medium and high. If behaviour is wrong then it gives alert as user category wrong and asks security questions.

5) In this way the proposed system provide security, location validation, payment validation and transaction validation.

3.1 Hardware Requirements

The hardware required for the proposed system is RFID reader module and laptop.

3.1.1 RFID Reader Module

RFID Reader Module [8] is a low frequency (125Khz) RFID reader with serial output with at range of 8-12cm. It is a compact units with built in antenna and can be directly connected to the PC using RS232 protocol. Tag consists of microchip and an antenna is attached to it.The tags used are read only tags. In read only tags Tag ID is assigned at the factory during manufacturing and can never be change and no additional data can be assigned to the tag. The tag used is passive tag. One of the advantage of passive tag is it not required battery. It uses harvested energy to switch on. For communication between tag and reader near field communication is used which uses electromagnetic field.

Fig -2: RFID Reader Module

Table -1: Specifications of RFID Reader Module

Parameter	Value
Operating Voltage	5V
Current	<50mA
Read Distance	10cm
Operating Frequency	125Khz

3.2 Software Description

Software used for the proposed system is java and platform used is netbeans IDE 7.0.1.

3.2.1 JSP

JSP is java server pages.JSP used for developing web pages. JSP consists of html and java code. The implicit objects of JSP like responses, request, out and session are used for developing security business logic.

3.2.2 JDBC

JDBC is used to connect java programs to sql database. The database used is mysql and Tomcat apache server is used.

4. RESULT AND DISCUSSION

For enhancing RFID security for smart cards we have concluded that the proposed system provides location validation, payment validation and security in transaction.

4.1Result for location validation

If latitude and longitude of particular location are same then it will verified it and go further otherwise it will give message not detect. If answers of interrogation questions were wrong then system will block our card and a messege is sent to registered email address.

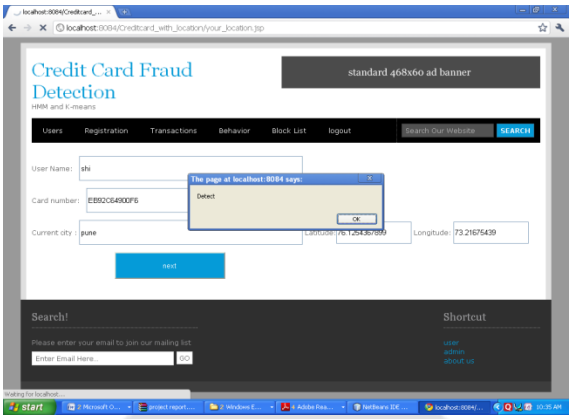

Fig -4: Result for location validation

4.2 Result for Payment Validation

If balance is sufficient then only transaction is successful and if balance is low then it will give alert as your balance is low.

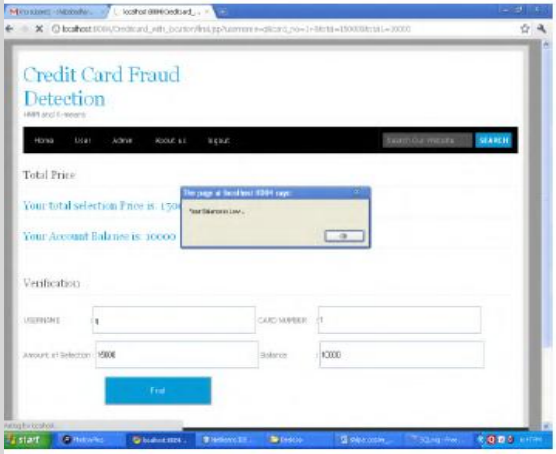

Fig -5: Result for payment validation

4.3 Result for transaction line chart

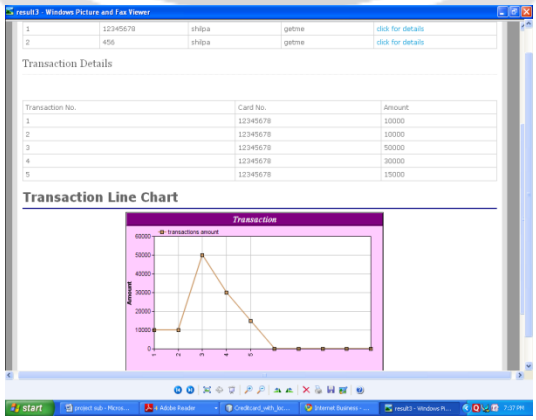

Fig -6: Result for transaction line chart

Figure 6 shows spending profile of all transactions. On x axis number of transactions are taken where as on y axis amount is taken. From the graph it is seen that first and second transaction is of 10,000 where as third, fourth and fifth transaction is of 50,000; 30,000; and 15,000 respectively. From all these transaction behaviour of customer is find out. Since for 0to 50,000 customer comes in low category therefore behaviour of customer is low.

4.4 Result for transaction verification

In transaction verification it shows the user amount balanced in his account and of how much price amount price he is going to purchase. In this way it shows us how much amount is left in users account so that he is able to make payment. In this way it gives transaction verification. Result for transaction verification is shown in figure 7.

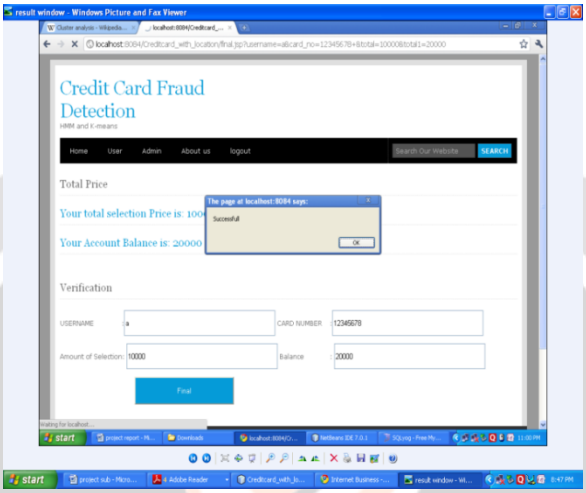

Fig -7: result for transaction verification

5. CONCLUSION

In the proposed work an HMM algorithm is used for detection of RFID card fraud. For security purpose the facility is provided to the user for blocking the card immediately as soon as the answers of interrogation questions is wrong or points on 3D image is wrong for 3 times. The proposed system gives location validation, transaction verification and payment validation. By having all these advantages one of the limitation of proposed system is execution time is surely increase i.e. there is tradeoff between security and execution time.

REFERENCES

[1]Di Ma,NiteshSaxena, Tuo Xiang, and Yan Zhu, "Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing," IEEE transactions on dependable and secure computing, vol. 10, no. 2, pp. 57-69, march/April 2013.

[2] A. Czeskis, K. Koscher, J. Smith, and T. Kohno., "RFIDs and Secret Handshakes: Defending against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications," Proc. ACM Conf. Computer and Comm. Security, 2008.

[3] A. Juels, R.L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," Proc. ACM Conf. Computer and Comm. Security (CCS), 2003.

[4] N. Saxena and J. Voris, "Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model," Proc. Workshop RFID Security (RFIDSec), June 2010.

[5] N. Saxena, B. Uddin, J. Voris, and N. Asokan, "Vibrate-to-Unlock: Mobile Phone Assisted User Authentication to Multiple Personal RFID Tags," Proc. IEEE Int"l Conf. Pervasive Computing and Comm. (PerCom), 2011.

[6] S. Drimer and S.J. Murdoch, "Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks," Proc. 16th USENIX Security Symp, Aug. 2007.

[7]Rabiner R. L. *A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition* Proceedings of the IEEE, Vol 77 (2), pp 257286, 1989.

[8]www.reseachdesignlabs.com