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

Theft Identification and Remote Information of ATM Card by a Unique System

Ayesha Khatoon R. Syed[1], Vijay R. Wadhankar[2]

[1]Research Scholar, R.T.M. Nagpur University, Agnihotri College of Engineering, Nagthana Road, Wardha, Maharashtra, India

[2]H.O.D. Of E & C Dept, Agnihotri College of Engineering, R.T.M. Nagpur University, Nagthana Road, Wardha, Maharashtra, India

Abstract: ***The main objective of this project is to detect the loss of ATM card and to send a message. In this Project Access to the ATM is given by using the Smart Card Technology. In this system, the Smart Card, which contains the tagged data of the object generates a signal containing the respective information which is read by the card reader, which then may pass this information to a processor for processing the obtained information for that particular information. Based on the information from the tags access can be given or denied. In this project to display the permission status LCD is used.***

Keywords: Automatic Teller Machine (ATM), One Time Password (OTP), Personal Identification Number (PIN), GPS, SMS.

1. Introduction

Security of persons and information has always been a major issue. We need to protect our homes and offices; and also the information we transmit and store. Developing embedded systems for security applications is one of the most lucrative businesses nowadays. Security devices at homes, offices, airports etc. for authentication and verification are embedded systems. Encryption devices are nearly 99 per cent of the processors that are manufactured end up in~ embedded systems. Embedded systems find applications in. Every industrial segment- consumer electronics, transportation, avionics, biomedical engineering, manufacturing, process control and industrial automation, data communication, telecommunication, defense, security etc. used to encrypt the data/voice being transmitted on communication links such as telephone lines. Biometric systems using fingerprint and face recognition are now being extensively used for user authentication in banking applications as well as for access control in high security buildings.

An embedded system is a combination of software and hardware to perform a dedicated task. Some of the main devices used in embedded products are Microprocessors and Microcontrollers .Microprocessors are commonly referred to as general purpose processors as they simply accept the inputs, process it and give the output. In contrast, a microcontroller not only accepts the data as inputs but also manipulates it, interfaces the data with various devices, controls the data and thus finally gives the result.

2. Implementation

Smart Card contains the code which is unique for each user and whenever a person wants to access his Smart Card, he should enter the correct PIN number to access it. This password is programmed in the microcontroller in advance, so if the given password does not matches with the existing one a massage is delivered to the user of the card using GSM modem.

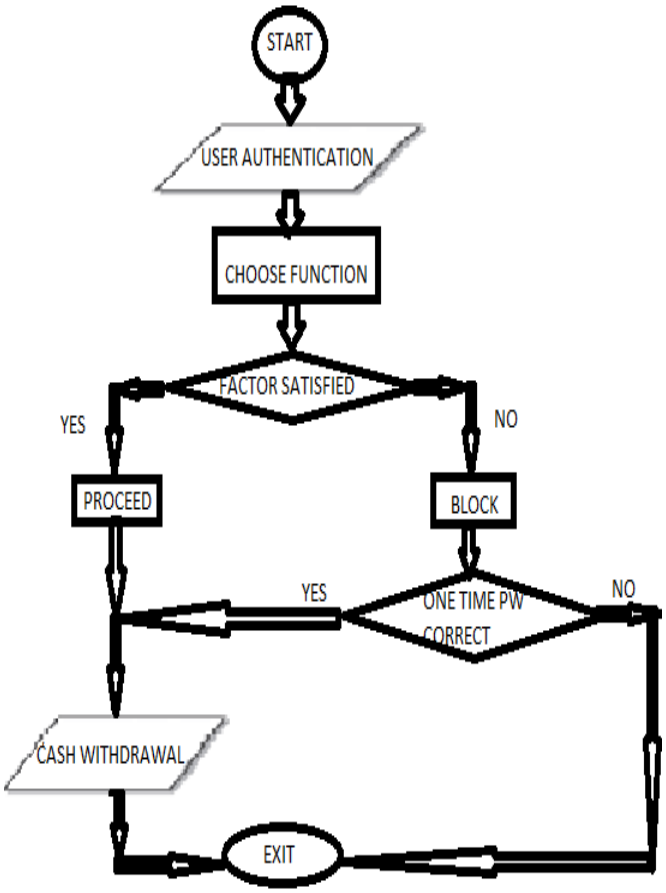


Figure 1: Functioning of the program

We need to send OTP as well as GPS location if OTP doesn't matches, GPS location send to the user through GSM. GSM as well as GPS also works on serial communication but we have only two RX (P3.0) and TX (P3.1) pins for controller for serial communication.

3. Text Message

The lack of encryption on SMS messages is an area of concern that is often discussed. This concern sometimes

arises within the group of the bank's technology personnel, due to their familiarity and past experience with encryption on the ATM and other payment channels. The lack of encryption is inherent to the SMS banking channel and several banks that use it have overcome their fears by introducing compensating controls and limiting the scope of the SMS banking application to where it offers an advantage over other channels. SMS banking services are operated using following two types of messages.

3.1 Pull Messages

Pull messages are those that are initiated by the customer, using a mobile phone, for obtaining information or performing a transaction in the bank account. Examples of pull messages for information include an account balance enquiry, or requests for current information like currency exchange rates and deposit interest rates, as published and updated by the bank.

3.2 Push Messages

Push messages are those that the bank chooses to send out to a customer's mobile phone, without the customer initiating a request for the information. Typically push messages could be either Mobile marketing messages or messages alerting an event which happens in the customer's bank account, such as a large withdrawal of funds from the ATM or a large payment using the customer's credit card, etc.

The SMS banking channel also acts as the bank's means of alerting its customers, especially in an emergency situation; e.g. when there is an ATM fraud happening in the region, the bank can push a mass alert (although not subscribed by all customers) or automatically alert on an individual basis when a predefined 'abnormal' transaction happens on a customer's account using the ATM or credit card. This capability mitigates the risk of fraud going unnoticed for a long time and increases customer confidence in the bank's information systems.

Another type of push message is One-time password (OTPs). OTPs are the latest tool used by financial and banking service providers in the fight against cyber fraud. Instead of relying on traditional memorized passwords, OTPs are requested by consumers each time they want to perform transactions using the online or mobile banking interface. When the request is received the password is sent to the consumer's phone via SMS. The password is expired once it has been used or once its scheduled life-cycle has expired.

Figure 2: SMS from ATM to Cell Phone

4. One Time Password (OTP) Implementation

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as something a person knows.

The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

Third Party Screen
Welcome ICIC Bank
Welcome Ayesha
Enter PIN

****

Success…OTP has been generated and send to your mobile 0123456789

Enter OTP

****

Transaction Successful…

Figure 3: Simulation Result I: For correct OTP

Third Party Screen
Welcome ICIC Bank
Welcome Ayesha
Enter PIN

****

Success…. OTP has been generated and send to your mobile 0123456789

Enter OTP

****

Entered OTP is Incorrect
Transaction Fail…

Figure 4: Simulation Result II: For Incorrect OTP

Third Party Screen
Welcome ICIC Bank
Welcome Ayesha
Enter PIN

****

Entered PIN is Incorrect
Transaction Fail…

Figure 5: Simulation Result III: For Incorrect PIN

4.1 How OTP's are Generated and Distributed

OTP generation algorithms typically make use of pseudorandomness or randomness, making prediction of successor OTPs by an attacker difficult, and also hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed below:

- Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time)
- Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).
- Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter.

There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security tokens that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as SMS messaging. Finally, in some systems, OTPs are printed on paper that the user is required to carry.

4.2 Methods of Delivering the OTP's

4.2.1 Text messaging

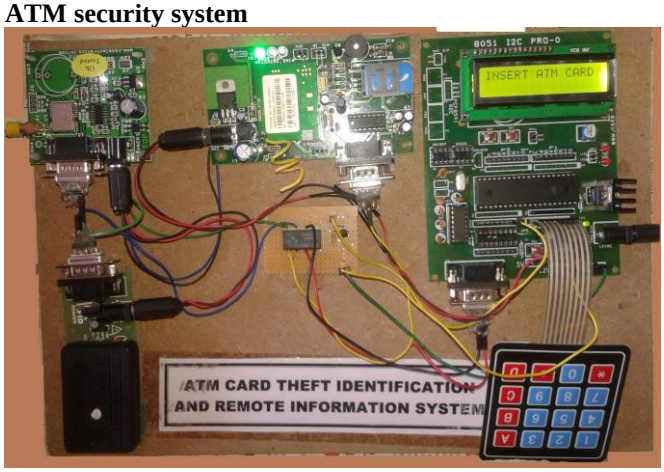
A common technology used for the delivery of OTPs is text messaging. Because text messaging is a ubiquitous communication channel, being directly available in nearly all mobile handsets and, through text-to-speech conversion, to any mobile or landline telephone, text messaging has a great potential to reach all consumers with a low total cost to implement. However, the cost of text messaging for each OTP may not be acceptable to some users. OTP over text messaging may be encrypted using an A5/x standard, which several hacking groups report can be successfully decrypted within minutes or seconds, or the OTP over SMS might not be encrypted by one's service-provider at all. In addition to threats from hackers, the mobile phone operator becomes part of the trust chain. In the case of roaming, more than a single mobile phone operator has to be trusted. Anyone using this information may mount a man-in-the-middle attack.

4.2.2 Mobile phones

A mobile phone keeps costs low because a large customer-base already owns a mobile phone for purposes other than generating OTPs. The computing power and storage required for OTPs is usually insignificant compared to that which modern camera-phones and smartphones typically use. Mobile phones additionally support any number of tokens within one installation of the application, allowing a user the ability to authenticate to multiple resources from one device. This solution also provides model-specific applications to the user's mobile.

5. Experimental work

5.1 Complete Hardware development of this project for ATM security system



5.2 RFID Cards

6. Conclusion

This Project provides secure accessing of the smartcard if an unauthorized person access the card, a message will be generated automatically. We can use the two passwords for the better security one password can used to detect the smart card and another password can be used for the transaction. Using this method we can provide the better security for the smart card users. This project entirely depend on RFID and GSM technologies where the RFID read the card information and also accessing and GSM is used to send the SMS to card user when the card is theft.GSM and RFID communicate using serial communication port RS232. This project provides secure accessing of the smart card. If an unauthorized person accesses the card, a message will be generated automatically.

References

[1] T. Phillips, T. Karygiannis and R. Kuhn, "Security Standards for the RFID Market," IEEE Security &Privacy, vol. 3, no. 6, pp. 85 - 89, Nov.- Dec.2005.
[2] C. C. Tan, B. Sheng and Q. Li, "Secure and Server less RFID Authentication and Search Protocols," IEEE Transactions on Wireless Communications, vol. 7, no. 4, pp. 1400 - 1407,April 2008.
[3] R. Weinstein, "RFID: A Technical Overview and Its Application to the Enterprise," IT Professional, vol. 7, no. 3, pp. 27 - 33, May - June 2005.
[4] P. Booth, P. H. Frisch and S. Miodownik,"Application of RFID in an Integrated Healthcare Environment," 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBS '06), pp. 117 - 119,Aug. 30 2006 - Sept. 3 2006.
[5] CASPIAN, Privacy Rights Clearinghouse, ACLU,EFF, EPIC, Junkbusters, Meyda Online, and Privacy Activism, RFID position statement of consumer privacy and civil liberties organizations http://www.privacyrights.org/ar/RFIDposition.htm,2003.
[6] C. D. M. Cordeiro, S. Abhyankar, R. Toshiwaland D. P. Agrawal, "A Novel Architecture and Coexistence Method to Provide Global Accessto/from Bluetooth WPANs by IEEE 802.11WLANs," Proceedings of the 2003 IEEE International Performance, Computing, and Communications Conference, pp. 23 - 30, 9- II April 2003.
[7] Ryder, ATM Security, Part One: Preventing ATM Theft,http://www.securityfocus.com/infocus/1186. July2001.
[8] B. Klinder, ATM Security Guidelines, http://atm.techtarget.com/articles/atmsecurity.htm, November 200 I.
[9] Sivakumar T.1, Gajjala Askok2, k. Sai Venuprathap3" Design and Implementation of Security Based ATM theft Monitoring system" International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 3, Issue 1 (August 2013) PP: 01-07
[10] Vivek V. Jog, Rohan Arora, Darshan Jain, Badal Bhat" Theft Prevention ATM Model using Dormant Monitoring for Transactions" Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT 2013).
[11] Srivatsan Sridharan1, Gorthy Ravi Kiran2, Sridhar Jammalamadaka3"Improvising Authenticity and Security of Automated Teller Machine Services" IJCSMC, Vol. 3, Issue. 2, February 2014, pg.666 – 674.

Author Profile

Ayesha Syed received her B.E. degree in Electronics Engineering from Rajiv Gandhi College of Engineering Research & Technology Chandrapur in 2011 from R.T.M.N.U (M.S.) India. Currently she is research scholar and pursuing her M.Tech from Agnihotri College Of Engineering, Wardha (M.S.) India.

Prof. Vijay R. Wadhankar received his B.E.degree in Electronics Engineering from Bapurao Deshmukh College Of Engineering Wardha (M.S.) India and M.Tech in VLSI from G.H.Raisoni College of Engineering Nagpur (M.S), India. He is working as Head of Dept. in Agnihotri College of Engg. Nagthana Wardha, India.