IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 11, Issue 1, Ver. IV (Jan. - Feb .2016), PP 01-04
www.iosrjournals.org

Technical Review On Secure Banking Using RSA And AES Encryptor Methodologies

Abhilesh S. Jadhao[1], Shital B. Kumbhalkar[2]
[1]*Dept. of Electronics and Communication Engineering, Ballarpur Institute of Technology, Bamni, Ballarpur (M.S.), India*
[2]*Dept. of Electronics and Communication Engineering, Assistant Professor, Ballarpur Institute of Technology, Bamni, Ballarpur (M.S.), India*

Abstract : *One of the key challenges faced by the information communication network while sharing resources is its security. Due to the increased online transactions, issue of data security became vital. This paper presents a technical review on secure banking using RSA and AES encryption methodologies. We will discuss the data communication security methods used between Auto teller machine and bank server during its financial operations. Since multiple security attacks can be attempted during the transaction to gather the precious information and gain unauthorized access, various data security levels and encryption standards are used for secure banking transactions. This paper focuses on Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES), encryption standards used by the banks for secure data transactions.*
Keywords: *Auto Teller Machine, Authentication, Cryptography, Security, One Time Password.*

I. Introduction

In the world of globalization, the demand for innovative products, and new technological advancements, banking industry is no exception as far as competition is concerned. Auto Teller Machine is one of the prime innovations for the banking industry which provides the facility for banking operations outside the banking premises. One of the main functions of the ATM is withdrawal of money. Currently, security which has been provided to the user for secure ATM transactions works on the principle of single Pin security. A three way security is provided by the banks to protect ATMs. These are:

- ✓ Physical security
- ✓ Software security
- ✓ Communication Security

Physical security includes protection of physical aspects of the ATM machine like lock mechanism of ATM Entrance door, CCTV surveillance, etc. **Software Security** includes protection to the operating system on which ATM runs. **Communication security** follows the security to the online transactions pertaining to the ATM. Multiple security attacks can be attempted during the ATM transactions to gain unauthorized access to the precious information and use the same information against clients. In order to prevent such cybercrimes, various data security levels and encryption standards are used for secure transactions.

We will discuss the data communication security methods used between Auto teller machine and bank server during its financial operations. This paper focuses on Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES), encryption standards used by the banks for secure data transactions.

II. Literature Review

Sistu Sudheer Kumar, A. Srinivas Reddy (May-2015) [1] Authentication is a critical part of any trustworthy computing system which ensures that only authorized individuals can log on to the system. Here, ATM Security has always been one of the most prominent issues. ATM machines generally authenticates by using ATM card and PIN number to perform transactions. This paper discusses design of ATM system that will improve the authentication of customer while using ATM. Here is possible scenario that an individual's ATM card falling into wrong hands by knowing PIN number and forget ATM card is difficult to perform ATM transaction. So to clear all these problems we are implementing this system using "One Time Password (OTP)" and "Personal Identification Number (PIN)" combination in order to improve authentication of customer using ATM machine to perform transaction without having any ATM cards.

Ezeofor C. J, Ulasi A. G. (December 2014) [2], this paper presents an analysis of network data encryption and decryption techniques used in communication systems. In network communication systems, exchange of information mostly occurs on networked computers, mobile phones and other internet based electronic gadgets. Unsecured data that travels through different networks are open to many types of attack and can be read, altered or forged by anyone who has access to that data. To prevent such an attack, data encryption and decryption technique is employed. In order to visualize the effect and evaluate the performance of the

encryption and decryption of each technique used in communication systems, Visual Basic simulation program that encrypt and decrypt data were developed, written and tested. Different data block sizes were captured and plotted against total time response taken during data encryption using Microsoft Excel. The graph result shows the superiority of RSA and AES algorithms over other algorithms in terms of the processing speed and time. DES has worm holes in its security mechanism whereas Blowfish, AES, and RSA do not have any. Further analysis was made based on the graph result obtained on each data encryption techniques.

Siva Kumar T, Gajjala Askok (August 2013) [3], the idea of designing and implementation of Security Based ATM theft project is born with the observation in our real life incidents happening around us. This project deals with prevention of ATM theft from robbery. So to overcome this drawback found in existing technology, this project can be implemented. Here, vibration sensor is used which senses the vibrations produced by the ATM machine. This system uses ARM controller based embedded system to process real time data collected using the vibration sensor. Once the vibrations are sensed, various parameters start responding like the buzzer starts sending signals in the form of beep, DC Motor starts closing the door of ATM and Stepper motor leaks the gas inside the ATM to bring the thief to unconscious stage. Camera is always in processing and sending video signals continuously to the observatory and will be saved in computer. Real Time Clock is used to capture the robbery occur time and send the robbery occur time with the message to the nearby police station and corresponding bank through the GSM. Here LCD display board is used for showing the output of the message continuously. This will prevent the robbery and the person involving in the act can be easily caught. Keil tools are used to implement the idea and obtaining the results. keil tools are also used for run the DC motor and stepper motor for automatic door lock and leak the gas inside the ATM respectively.

Nentawe Y. Goshwe (July 2013) [4], one of the principal challenges of resource sharing on data communication network is its security. This is premised on the fact that once there is connectivity between computers sharing some resources, the issue of data security becomes critical. This paper presents a design of data encryption and decryption in a network environment using RSA algorithm with a specific message block size. The algorithm allows a message sender to generate a public keys to encrypt the message and the receiver is sent with a generated private key using a secured database. An incorrect private key will still decrypt the encrypted message but to a form different from the original message.

Sneha K. Patel, Dr. D. C. Joshi (June 2013) [5], the present era of information and technology is quickly revolutionizing the way of transactions. Human involvement in handling and authenticating day to day activities is being increasingly replaced by electronic gadgets/systems. This growth in electronic transactions results in a rise of demand for fast and accurate user identification and authentication system. Access codes for buildings, banks accounts and computer systems often use PINs for identification and security clearances. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Total security system may solve this problem since a face; speech; fingerprint; palm print etc. are undeniably connected to its owner. This system can compare scans to the records stored in a central or local database or even on a smart card. The main aim of this paper is to construct mathematical model based on cryptography for total security system using qualitative and quantitative data of human.

Shun Wong (April 2005) [6] ATM also known as Automatic Teller Machine is simple and yet secure banking service. The basic concept is that an ATM allows an authorized cardholder to conduct banking transaction without visiting a branch. They are well known for its convenience to the customers, cost-effectiveness to the bank and most importantly it is one of the secure banking methods. ATMs rely on authorization of a transaction by the bank via a secure communications network. Encryption methods are built into the communication network to prevent unauthorized transactions that could result in loses. This paper focuses on Data Encryption Standard and Advanced Encryption Standard, these are the encryption standards presently adopted by the banks across the globe.

III. Generalized Concept

RSA Algorithm

RSA is an internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the web browsers from Microsoft and Netscape. The encryption system is owned by RSA security. The technologies are part of existing or proposed Web, Internet and computing standards. The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public key encryption methods. RSA RC4 is a Highly Secure, High Speed Algorithm The RC4 algorithm, developed by RSA Data Security Inc., has rapidly become the de-facto international standard for high -speed data encryption. Despite ongoing attempts by cryptographic researchers to "crack" the RC4 algorithm, the only feasible method of breaking its encryption known today remains brute-force, systematic guessing, which is generally infeasible. RC4 is a stream cipher that operates at several times the speed of DES, making it possible to encrypt even large bulk data transfers with minimal performance consequences. RC4_56 and RC4_128 RC4

is a variable key-length stream cipher. The Oracle Advanced Security option release 8.1.5 for domestic use offers an implementation of RC4 with 56 bit and 128 bit key lengths [7]. This provides strong encryption with no sacrifice in performance when compared to other key lengths of the same algorithm. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

AES Algorithm

The National Institute of Standards and Technology (NIST) have created AES, which is a new Federal Information Processing Standard (FIPS) publication that describes an encryption method. AES is a privacy transform for IPSec and Internet Key Exchange (IKE) and has been developed to replace the Data Encryption Standard (DES). AES is designed to be more secure than DES: AES offers a larger key size, while ensuring that the only known approach to decrypt a message is for an intruder to try every possible key. AES has a variable key length —the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key. AES able to process six times faster compared with the triple DES for the same processing capacity.

ATM (Automated Teller Machine)

The first ATM in Korea was installed by Korea exchange Bank in 1975, and once installation of ATM by Shinhan Bank in 1982, the civilian will use the ATM of varied banks with beginning of operation of common CD network that is controlled by Korea Financial Telecommunications & clearings institute. The quantity of put in ATM machine has shown the trend of skyrocketing unceasingly with the high increasing quantitative relation within the half of year 2000s, and gradual increase once the year. Particularly external ATM machine has been accrued unceasingly.

An Automated Teller Machine (ATM) is used to electronically withdraw money from and deposit it to your bank account [9]. ATM communicates with central host processor by Internet Service Provider has a gateway where all ATM networks available to user. Here ATM machines connected to central host processor are by telephone lines or normal phone line using modem. When customer wants to perform transaction provide PIN details and ATM card. ATM machine forwards to central host processor, where ATM request to customer's bank. If customer request cash, central host processor initiates electronic funds transfer from customer bank to ATM central host processor account. Once transfer complete to central host processor, it sends approval code to ATM machine to dispense cash.

IV. Proposed Methodology

Authentication of ATM during transaction is unsecure because with help of clone of original cards by replicas of ATM machine card slots with built-in magnetic strip readers. The reader capture data embedded in the magnetic strip and store it. By placing small wireless surveillance cameras in ATM center to track the PIN to cash withdrawal. To come up with stolen card and tracked PIN for cash withdrawal. To overcome this, I am proposing ATM transaction using combination of One Time Password and PIN to authenticate the ATM during transactions.

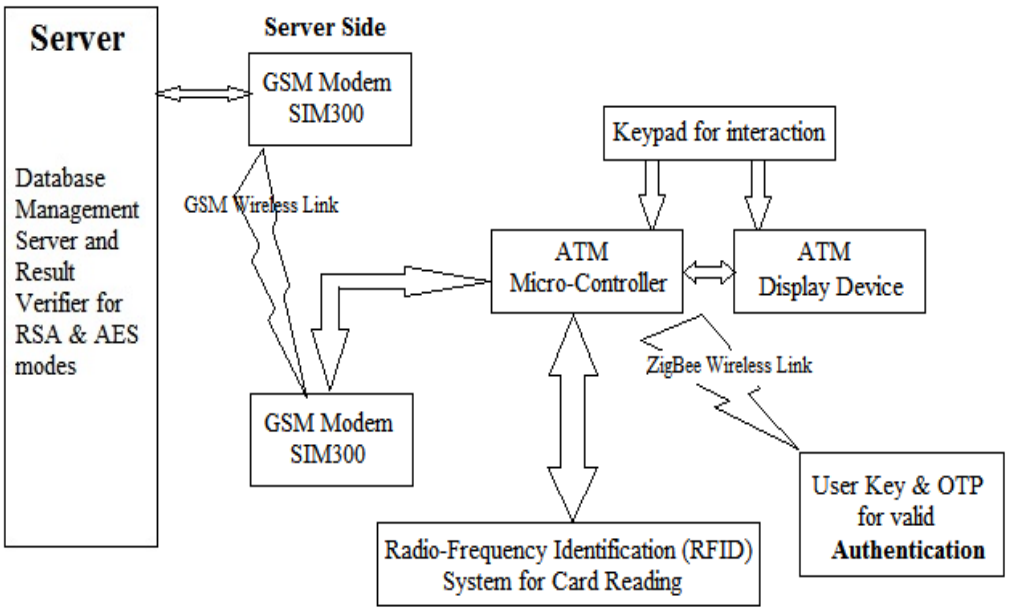

Fig.1. Basic block diagram of proposed system

Above figure consists of three nodes, one node is master which is connected to the personal computer and other two nodes are the slave nodes connected with wireless module which is ZigBee & RFID.

V. Conclusion

The last few decades has witnessed various kinds of card and currency fraud. The security procedures followed by the banks are archaic, thus making it less secure and leaves scope for possible attacks and frauds. Implementation of varied kinds of encryption strategies like RSA and AES cryptography methodologies will not only make the transactions secure but also increase the trust among the employees, clients and partners for the banks and online transactions.

References

[1] Sistu Sudheer Kumar, A. Srinivas Reddy , May-2015, " A survey on theft prevention during ATM transaction without ATM cards", eISSN: 2319-1163 | pISSN: 2321-7308 Volume: 04 Special Issue: 06 | NCEITCS-2015 | May-2015.
[2] Ezeofor C. J, Ulasi A. G., December 2014, "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems " International Journal of Innovative Research in Science Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 12, December 2014 ISSN: 2319-8753.
[3] Sivakumar T, Gajjala Askok, k. Sai Venuprathap, August 2013, " 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.
[4] Nentawe Y. Goshwe , July 2013, " Data Encryption and Decryption Using RSA Algorithm in a Network Environment" IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013.
[5] Sneha K. Patel, Dr. D. C. Joshi, June 2013, "Mathematical Model Based Total Security System with Qualitative and Quantitative Data of Human", Int Jr. of Mathematics Sciences & Applications Vol.3, No.1, January-June 2013 Copyright Mind Reader Publications ISSN No: 2230-9888.
[6] Shun Wong, April 2005, "The Encryption Technology of Automatic Teller Machine Networks", Software Engineering 4C03 Winter 2005.
[7] Oracle Advanced Security Administrator's Guide Release 8.1.5 A67766-01
[8] RSA SecurID Authentication, A Better Value for a Better ROI.
[9] Http://www.ehow.com/how-does_4900119_how-atms-work.html.
[10] AES Encryption, AES Encryption and Related Concepts.