International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-1 Issue-4, April 2012

Different Data Encryption Methods Used in Secure Auto Teller Machine Transactions

Navneet Sharma , Vijay Singh Rathore

Abstract— Data security is an important issue in current scenario of banking financial operation specially with transaction of secure and confidential data. It must be send with high security at the time of communication. In this paper we will discuss various types of encryption methods and standards which are used in secure banking data transmissions to make more data security. Specially here we discuss the communication security methods used between Auto teller machine and bank server banking financial operations, When we transmit data from an Auto Teller Machine to bank server it must send in encrypted form so that an unauthorized user cannot access the secure information directly at the time of data communication. using this paper I will try to explain different data security that how the data transactions can make more secure with different security techniques used in ATM transactions. Various security levels of data and encryption standard used in banking data transaction security. Encryption methods are built into the communication network to prevent unauthorized transactions that could protect the data from unauthorized access. This paper focuses on Data Encryption Standard and Advanced Encryption Standard, these are the encryption standards used by the banks to protect the data and for secure data transmission.

Keywords — Auto Teller Machine, Encryption, DES, 3DES, AES, RC4, EPP.

I. INTRODUCTION

In competitive market globalization, increased competition, the demand for innovative products, and new technology implementation, the banking industry is changing at least as fast as any other industry. Auto Teller machine is one of the important innovation of banking competition which provides the banking operations out side the bank premises. it mainly used to withdrawal money from it. To provide the security at user level it works on a single pin security for secure banking operation at user level. But it is not sufficient to protect the information which are send by the ATM to bank server and vice versa .

There are three types of securities provided by the banks to protect the ATM .these are : (a) Physical security

(b) Software security

(c) Communication security

In this paper we will discuss only the communication security. At the time of data communication from an Auto Teller Machine to bank server the rise of the banking system becomes a more and more important security issue; In order to make communication security from ATM to Bank and from Bank to ATM a new level of security emerge.

Normally ATM verify the authentication of a user with single key pin security but this is not sufficient to protect this information in a network transaction. to protect this type of secure data bank follows various encryption methods to protect their transactions. Data encryption is one of them. Data Encryption is the cryptographic algorithm in accordance with established expressly to sensitive data transformation into ciphertext data is difficult to identify, through use a different key, the same encryption algorithm used to encrypt the same plaintext into cipher text.

here we will discuss these encryption standards and various methods used by banks for safe data transmission.

Manuscript published on 30 April 2012.

* Correspondence Author (s)

Navneet Sharma*, Sr. Asstt. Professor, Dept. Of Computer Sc. & IT The IIS University, Jaipur, Rajasthan, India (E-Mail: navneetsharma1977@gmail.com).

Dr.Vijay Singh Rathore, Director**,** Shri karni College, Jaipur, Rajasthan, India, (E-mail:vijaydiamond@gmail.com).

II. DATA ENCRYPTION METHOD FOR SECURE DATA COMMUNICATION IN BANKING AND ATM TRANSACTIONS

In auto teller machine for secure data communication, various data encryption methods are used.

DES is the standard for data communication .DES (Data Encryption Standard) is the transformation of data to a form which is impossible to read without the appropriate knowledge or key. The Data Encryption Standard (DES) was developed to provide data security in network by an IBM team around 1974 and adopted as an international standard in 1977. Data Encryption Standard (DES) is a standard cryptographic system with the type and mode symmetry algorithm. Cryptographic algorithms used in DES – which is called the Data Encryption Algorithm (DEA) – is the processing of bits in the form of block cipher (Cipher block). DES is a block cipher using 64-bit blocks and using external key length of 64 bits as well (same with a block size). In DES, the process data encryption (plaintext) using the internal key or sub-key along 56 bits are generated from an external key.

The procedure is done by algorithm DES is as follows:

Step 1: plaintext block was permutated by initial permutation matrix (Initial permutation / IP)

Step 2: To block the initial permutation proficiency level in these enciphering process (Encryption) to do 16 rounds (Round). In this process used internal keys for different each rotation.

Step 3: The results of the enciphering process will be permutated using reversal permutation matrix (the inverse initial permutation/IP-1)

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

3DES is a revised variation of DES due to the need for higher levels of security. all the banks are using this encryption standard for secure data communication in a public network. 3DES is a variant development of DES (Data Encryption Standard) – previously referred to as "multiple DES" basically due to the triple DES merely repeated use of DES; in this case repetition performed three times. Triple DES is generally known as TDES or by the term stands 3DES.

Security concerns in the use triple DES, is still possible there assault with the use of 2^{32} Known-plaintexts, 2^{113} steps, 2^{90} DES-solving ,and 2^{88} memory capacity.

III. ADAVANCED ENCRYPTION STANDARD (AES)

The National Institute of Standards and Technology (NIST) has 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. Will but the use of triple DES is still enough encountered due to the quickness of the cos large enough to switch to the technology new. In addition, when compared with AES, triple DES implementation is felt more suitable for application on the device hardware, such as network system communications, VPN network devices or at an ATM.

DES40 algorithm, available internationally, is a variant of DES in which the secret key is preprocessed to provide 40 effective key bits. It is designed for use by customers outside the USA and Canada who want to use a DES-based encryption algorithm. This feature gives commercial customers a choice in the algorithm they use, regardless of their geographic location.

RSA RC4 is a Highly Secure, High Speed Algorithm The RC4 algorithm, developed by RSA Data Security Inc., has quickly 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. This provides strong encryption with no sacrifice in performance when compared to other key lengths of the same algorithm.

IV. ENCRYPTED PIN PAD (EPP)

With normal keypads, the PIN entered by the customer is sent in "raw" state via a cable to a separate circuit card module containing encryption integrated circuits. For most countries, this arrangement was satisfactory because the cable and circuit card are located within the secure chest area of the ATM. In order to decrease PIN theft fraud, VISA and MasterCard are now requiring an encrypted PIN pad (EPP) in place of the keypad. The EPP is a sealed module that immediately and locally encrypts the PIN after entry. There are no "raw" PIN numbers accessible to electronic hackers either by physically tapping onto wires within the ATM or remotely sensing electromagnetic radiation emitted through ATM wiring. Any tampering of the EPP causes it to permanently disable itself.

V. CONCLUSION

In this paper I have tried to define various types of data encryption methods for communication security. Using these methods banking industries can secure their data with ATM and bank server data transmission. using these encryption methods . 3 DES and AES are more safer foe data security mostly bank are now using the AES to protect their data from hackers.

REFERENCES

1. Oracle Advanced Security Administrator's Guide Release 8.1.5 A67766-01
2. Enterprise Tape Encryption Requirements for the Banking Industry By: Jon Oltsik Enterprise Strategy Group August 2006
3. http://www.ehow.com
4. Xie Baoxiu Shi Bing. Encryption in e-commerce application [J] Computer and Digital Engineering 12, 2005
5. Zhao Lili. RSA algorithm and the speed improvements [D] Shenyang University of Technology 2007
6. Cai Jiren. Information Security Cryptography [J] Network Security 2003
7. W. Stallings, Cryptography and network security, Prentice Hall, 2006, New Jersey, United State
8. R. Sililiano, ATM Security threats Aug. 2010
9. Xie Baoxiu Shi Bing. Encryption in e-commerce application [J] Computer and Digital Engineering 12, 2005
10. Zhao Lili. RSA algorithm and the speed improvements [D] Shenyang University of Technology 2007
11. http://www.bankersonline.com/vendor_guru/diebold/diebold-pin.html.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)