International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 8 (2015) pp. 19167-19179

https://dx.doi.org/10.37622/IJAER/10.8.2015.19167-19179

An Enhanced Framework of Hybrid Secure ATM Banking System for Developing Countries

M. Syed Shahul Hameed[1] and Dr. N. Kannan[2]

Research Scholar, Manonmaniam Sundaranar University
Tirunelveli, Tamilnadu, India

Principal, Jayaram College of Engineering and Technology
Pagalavadi, Trichy-621014, Tamilnadu, India

Abstract:

Password Based Authentication is the most widely using identification mechanism in un-trusted machine like ATM Banking. Behind this password, most secret in formations are available. Once this password is hacked by the intruders, they can do as they want. To avoid such intruders, skimmers and their tampering works, this system is proposed to enhance the security level by incorporating different authentication standards. Also, users are authenticating by sending one time password through their mobile communication or authenticating by Biometric authentication. Such this proposed system improves the security levels and avoids intruders in ATM banking process.

Keywords—Biometric Authentication, Fingerprint, AES algorithm, Super Secure Hash (SSH) Algorithm.

INTRODUCTION

Automated Teller Machine (ATM) is the un-trusted mechanical device that is designed to work as a client based communication device connecting to their banking server. This ATM mechanism is established in most of the banking system world widely. This is the best, cheapest and convenient processes for both customers and bank. Privacy and security is the basic concern for these kinds of un-trusted machines. Once the privacy and security levels are reachable by hackers and skimmers, they can do as they want. Crime at ATM‟ s has become a nationwide issue that faces not only customers, but also bank operators [1]. To avoid and protect the system from hackers,

cryptography provides secure authentication in customer's transactions. Sometimes, even the cryptographic authentication systems cannot assure the identity of the legitimate users. It can only identify the owner based on their belongings (card) and what the information (Password, PIN) they are remembering. Almost of the banking system follows the above authentication methods which are not optimally secured. There are three main categories suggested by authentication standard. 1. Authentication by Ownership: requires that the user possesses an object. Example: smart cards, magnetic strip cards, symmetric key and asymmetric key cryptography. 2. Authentication by knowledge: entails that the user supplies specific information or answers questions. Example: password based authentication. 3. Authentication by characteristics: requires that the authentication device measures physical characteristics of the person being verified. These techniques include biometrical mechanisms such as face recognition, fingerprints, voiceprints, retina scans, keystroke patterns and signatures. All authentication devices share the principal goal of preventing the two main types of errors. Type 1: Failing to correctly identify a legitimate user. Type 2: Allowing access to the intruders. The most effective way to provide the secure computing is possible by combining two or three methods [2][3].

FLAWS IN EXISTING BANKING SYSTEM

Intruders are the persons keep watching the other person's works and trying to capture their information without their knowledge. Such intruders are monitoring banking ATM system and trying to capture the password of the users.

Skimmers are another kind of persons those who involves the PIN capturing of the users. Skimming is a method where criminals capture the data from the magnetic strip on the back of ATM cards. The most common methods of capturing the PIN are either by a very small video camera, or with another keypad which picky backs on top of the original keypad.

SECURITY REQUIREMENTS

In this proposed system, participants are not having physical verification for their transactions. However, in financial transaction trust should be established between each participant. The general cryptography concepts can be used to accomplish the trust between each participant [4].

Authentication:

Authentication is the process of proving user identification. One party which involves in transaction needs to make sure that counter-party is the one he is interested to communicate with.

Integrity:

Assuring the receiver that the received message has not been altered in any way from the original message.

Confidentiality:
Ensuring that no one else can read the message except the intended receiver.

Non-repudiation:
A mechanism that ensures to prevent that the counter- party later on rolls back the transaction.

Availability:
System Availability is whether (or how often) a system is available for use by its intended users. This is an integral component of security.

PROPOSED ENHANCHED HYBRID SECURE ATM BANKING SYSTEM

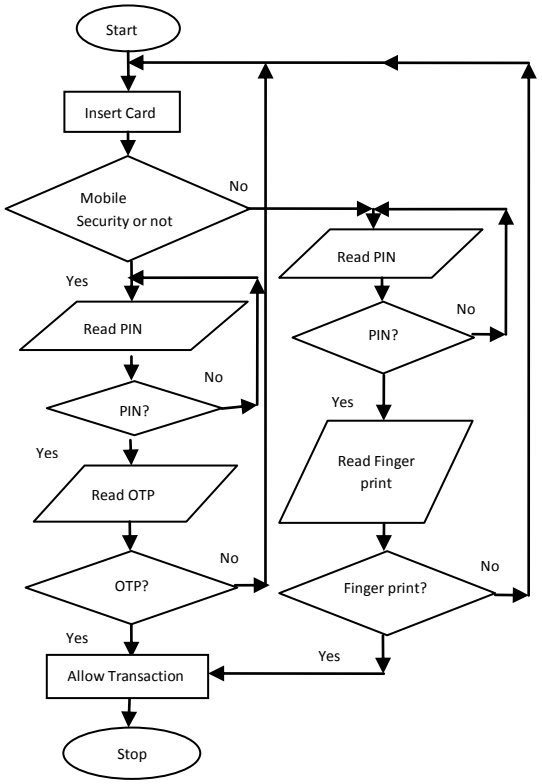

Figure 3: The detailed flowchart of the proposed system

A. System Architecture

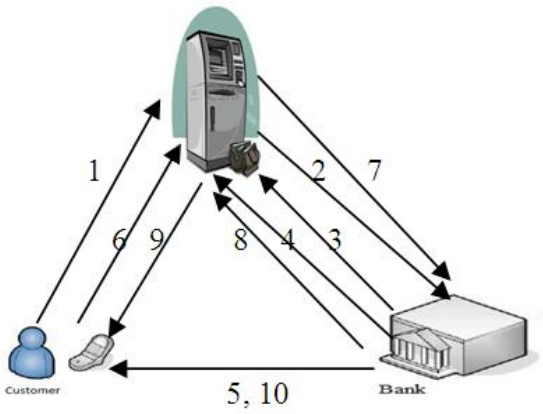

Figure 4: System Architecture.

ATM machine accessing steps:

1. A customer inserts the ATM card and types his PIN. The ATM machine reads the information from card.
2. ATM machine communicates with Bank Server and verifies the details.
3. Bank Server verifies the information and sends the approval to ATM machine.
4. Bank server issues One Time Password (Confirmation Number) to ATM machine.
5. Another OTP (Transaction Number) is send to the customer.
6. Customer type the OTP (Transaction Number) in ATM machine.
7. ATM machine send both Confirmation Number and Transaction Number to the Bank server.
8. Bank server verifies the relation between both numbers.
9. If the relation is correct, Bank server allows ATM machine to deliver the money.
10. Customer gets the information about transaction.

Similar steps are followed for the Finger print authentication. Instead of having OTP the users are verified by their Finger Print Pattern.

B. System Roles

There are three main actors and AES algorithm on the screen of the proposed system.

Customer:

A customer is a person who needs to perform an ATM transaction. The local users should have a bank account and suitable mobile phone to receive an OTP. The entire customer's ATM card should embed with unique Account number and Card number.

ATM:
The ATM machine should have a high speed communication with their bank server and accomplished with the finger print recognizer.

Bank Organization:
Bank should have high speed servers capable of sending Confirmation number to ATM machine and Transaction number to customer's mobile phone. In addition to that the bank servers should maintain the customer's details such as Account number, PIN, Card number, Mobile number, and Finger print pattern.

AES Algorithm:
Here the module uses AES (Advanced Encryption Standard) for encryption algorithm due to its standardized availability, strength and speed over other techniques like DES, etc … 128 bit long key is just enough to secure the operation against cryptanalytic attacks for data having average privacy requirements, for more sensitive data longer key lengths should be used [5].

SYSTEM WORKING

Almost of the world wide banking still using the PIN based security mechanism in ATM machine authentication. To enhance this current idea, our system incorporates the entire authentication standard in this proposed frame work. Authentication by ownership is achieved by One Time Password of mobile security. Authentication by knowledge is achieved by PIN based security. Authentication by characteristics is achieved by biometric authentication such as Finger print security. There are two cases of security method followed in the proposed system. Case 1: PIN based and OTP based authentications are combined. Case 2: PIN based and biometric based authentications are combined. Case 1 is mostly recommended for local users. Case 2 is recommended for international users.

***A. Authentication by Knowledge (PIN Based)*:**
Customer enters his PIN number into the ATM. By using SSH algorithm ATM will prepare a hash code based on PIN, Card number and A/C number. The generated hash code is used as the key for the AES encryption algorithm to encrypt the customer related information at the client side. According to the assumption mentioned above, the bank generates a Hash Code using SSH algorithm based on the Customer PIN number, Card number and the A/C number and keeps it in bank's database and uses the generated hash key to attempt decrypting the received encrypted message from the customer.

If this is a success it means that the hash key stored in the bank database is equal to the hash key generated by the customer. Therefore bank can authenticate the customer. Also, encrypted version of the customer message provides the integrity and the confidentiality of the customer information.

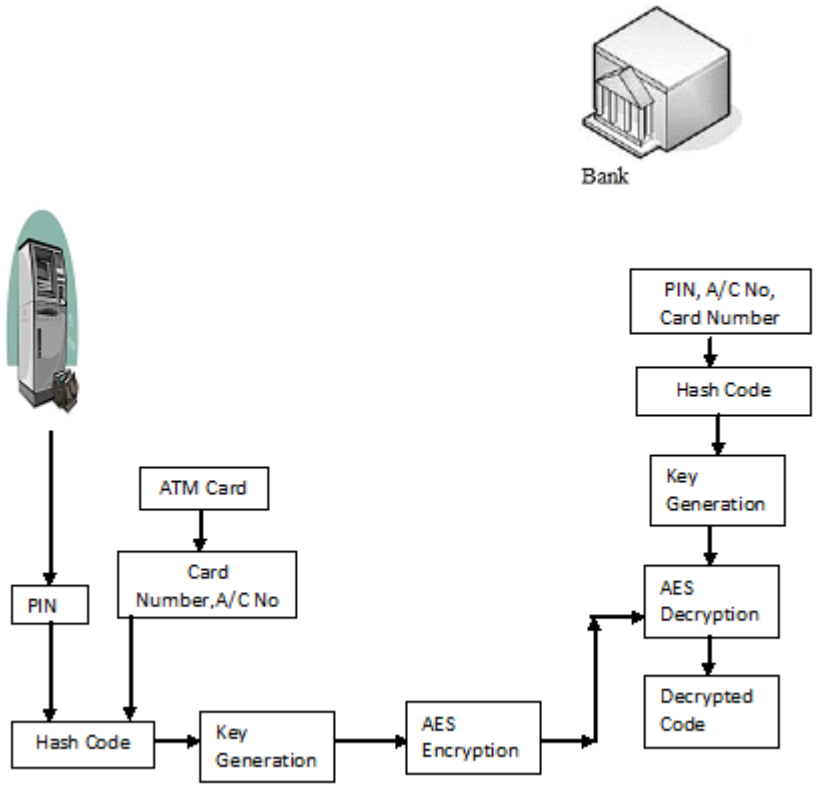

Figure 5: Authentication by Knowledge.

B. Authentication by Characteristics (Biometric Authentication):
Customer enters his Finger Print pattern into the ATM. By using SSH algorithm ATM will prepare a hash code based on Finger Print pattern, Card number and A/C number. The generated hash code is used as the key for the AES encryption algorithm to encrypt the customer related information at the client side. According to the assumption mentioned above, the bank generates a Hash Code using SSH algorithm based on the Finger Print pattern, Card number and the A/C number and keeps it in bank's database and uses the generated hash key to attempt decrypting the received encrypted message from the customer. If this is a success it means that the hash key stored in the bank database is equal to the hash key generated by the customer. Therefore bank can authenticate the customer strongly by his Finger Print pattern. Also, encrypted version of the customer message provides the integrity and the confidentiality of the customer information.

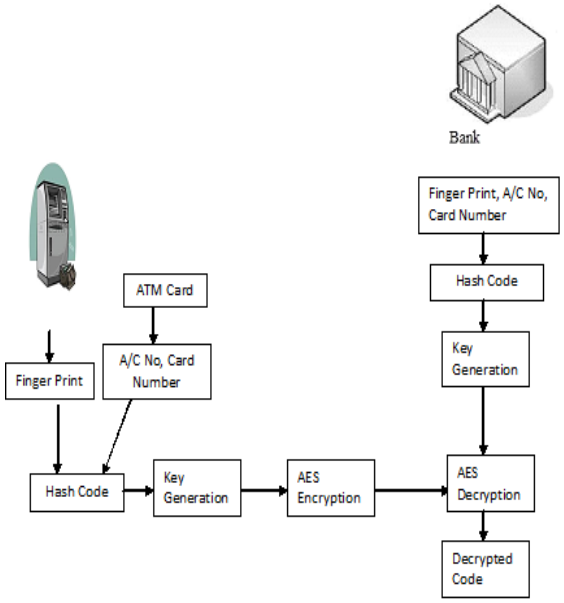

Figure 6: Authentication by Characteristics.

C. Authentication by Ownership (One Time Password):

Bank server issues Confirmation number to customer's mobile number and Transaction number to the ATM machine. Bank server only knows the relation between these two numbers. At the time of transaction, customer will receive the Confirmation number and enters the same into the ATM. At the same time ATM machine will receive the Transaction number from Bank server.

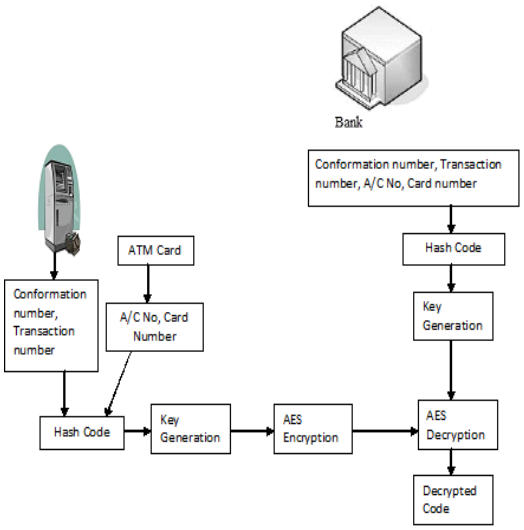

Figure 6: Authentication by Ownership.

By using SSH algorithm ATM will prepare a hash code based on Transaction number, Confirmation number, Card number and A/C number. The generated hash code is used as the key for the AES encryption algorithm to encrypt the customer related information at the client side. According to the assumption mentioned above, the bank generates a Hash Code using SSH algorithm based on the Transaction number, Confirmation number, Card number and the A/C number and keeps it in bank's database and uses the generated hash key to attempt decrypting the received encrypted message from the customer. If this is a success it means that the hash key stored in the bank database is equal to the hash key generated by the customer. Therefore bank can authenticate the customer strongly by the Transaction number and Confirmation number. Also, encrypted version of the customer message provides the integrity and the confidentiality of the customer information.

D. Hash Function

Hash function is mainly used for integrity check and improving the validity of digital signatures. Hash functions resistant to collision attacks can be developed by combining the MD-5 and DES algorithms. It may be particularly applicable to environments where these security requirements have made the implementation of certain security services prohibitively expensive[6]. The four secure algorithms such as SHA-1, SHA-256, SHA-384, and SHA-512 were proposed with iterative one way hash functions that can be process a message to produce a condensed representation called hash or message digest. MD5, SHA-1 and RIPEMD are the most commonly used message digest algorithms. A detailed review over the cryptographic hash functions has been carried out in [7]. Hash functions also called message digests and one-way encryption, are algorithms that use no key [8]. The MD6 Message digest algorithm uses a Merkle tree structure to allow for immense parallel computation of hashes for very long inputs. SHA-3 uses sponge construction in which message blocks are XOred into the initial bits of the state, which is then invertibly permuted. RIPEMD-160 is a bit message digest algorithm. There exist 128,256 and 320 bit versions of this algorithm, called RIPEMD-128, RIPEMD-256, and RIPEMD-320 respectively.

According to the research of hash function, a secure hash function should meet the following conditions [9].

1. Hash function H, should accept a block of data of any size as input.
2. The length of the input string is fixed. It takes 128 bits at least according to the current computer technology in order to resist attacks from the network.
3. H should produce a fixed-length output no matter what the length of the input data is.
4. It is very easy that calculating hash value of the output for each given input.
5. Don’t find that any two different input messages can have the same hash value.

The proposed algorithm has been designed to suit the requirements of a good hash function algorithm. In addition to matrix multiplication operation, logical

operations have been included to perform bit-wise manipulations. The proposed algorithm involves less complex operations and hence easily be implemented. The main aim of the proposed algorithm development is the design of hash algorithm which consumes less memory and less collision rate. A use of non-invertible matrices has been suggested for the practical one way hash function. The present algorithm Super Secure Hash (SSH) uses non-invertible matrix which can be used as multiplication matrix in Hill cipher technique for one way hash algorithms [10].

E. Super Secure Hash (SSH) Algorithm:

In order to improve the efficiency of batch verification and speedup the process, our system proposed a Super Secure Hash (SSH) algorithm. The sender's file is fragmented into packets and each packet size is 256 bits.

SSH Algorithm:

***Step 1*:**

Each packet source message is converted into 256 bits decimal digit. By using the ASCII code, each character is represented in decimal number. If the packet size is less than 256 bits, then copy and connect the string until the string length is equal to 256 bits.

***Step 2*:**

To get a non-zero number in the source message, replace the 0 with the numeric string such as like 123456789123456789…

***Step 3*:**

Divide the string of 256 bits into 16 blocks data of 16 bits such as m1,m2,m3,…,m16.

***Step 4*:**

Adjacent two blocks of data is multiplied and retain the highest 16 bits(or the lowest 16 bits). The result of multiplication may overflow. Take the absolute value if the result is negative. Example: take the highest 16 bits from the result of m1xm2 into new m1. Perform the same between m2xm3, and so on. At last m16Xm1 and find the highest 16 bits as the new m16.

***Step 5*:**

Consider a Key matrix (K) of order 4x4 of 64 bits, whose inverse does not exist.

***Step 6*:**

Rewrite the blocks of messages in the form of 4x4 matrixes. m1,m2,m3,m4 are grouped in the name of G1 matrix of 64 bits, m5,m6,m7,m8 are grouped in G2 matrix of 64 bits, m9,m10,m11,m12 are grouped G3 matrix of 64bits and m13,m14,m15,m16 are grouped in G4 matrix of 64bits.

***Step 7*:**

The following transformation function is repeated for four times on the group

matrixes with different F functions.

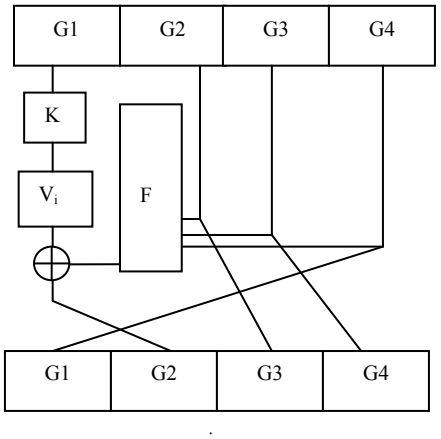

Figure 7: Transformation Function

$$V_i = G_i \times K \bmod 16$$

The function F is different in each round

$F_1(x,y,z) = x \oplus y \oplus z$

$F_2(x,y,z) = (x \wedge y) \vee (\neg x \wedge z)$

$F_3(x,y,z) = (x \vee \neg y) \oplus z$

$F_4(x,y,z) = (x \wedge z) \vee (y \wedge \neg z)$

SYSTEM ANALYSIS

A. Strength of SSH algorithm

Super Secure Hash (SSH) algorithm has been developed by keeping in view of providing efficient hash value with minimum operations. The use of non-invertible matrix multiplication operation makes the algorithm one-way and improves the collision resistant property. The proposed method involves bit-wise exclusive-or operations, logical operations which enhances the avalanche effect. Repeated transformation function makes it infeasible to trace the hash value in reverse direction. The padding of checksum helps to increase the confusion property of the algorithm. Thus the algorithm has been designed to incorporate all resistive features to provide data security. The algorithm has been designed to produce 256 bit hash value and hence the method is resistant against brute-force attack.

B. Performance Analysis of SSH

Software implementations of SSH were tested on system with Intel based CPU Core i5 2.67GHz with 4 GB RAM. The comparison is given in the following table for various hash functions tested on 0.8 Mb data file.

Table 1. Comparison of Different Hash Algorithm with SSH

Algorithm	Time(ms)
SSH	300
MD5	312
SHA-256	445
SHA-224	458
SHA512	430
RIPEMD-128	275
RIPEMD-160	275

It shows that SSH has the third fastest output after RIPEMD-128 and RIPEMD-160. In RIPEMD-128 and RIPEMD-160 algorithms produced more collision on the hash values. Specifically SSH shows its strength in dealing with collisions. SSH algorithm tested with different file sizes from 8KB to 1024KB. Whereas N=128, number of collisions is just 2.8% of overall hash values generated that's where number of hash values generated is 16225 hash values. Also in the same case when N=256 number of collisions is just 0.50178% where number of hash values generated is 16225. SSH didn't find any collision after 72 bit hash value length with 4x4 non invertible matrixes. Because of batch processing of group of packets, our proposed system uses a small size of packets which is not very small as well as not very big in the size. On the other hand, SSH algorithm uses a 4x4 non invertible matrix which reduces the conflict rate.

C. Security Analysis

Our proposed system enhanced the security features of the ordinary ATM mechanism. All the participants are verified by face-face manner, so that all identities are strongly verified. Bank server maintains the customer's financial and authorization details in the databases in encrypted form. Therefore they cannot be illegally accessed by unauthorized individual. AES is a privacy transform for IPSec and Internet Key Exchange (IKE) and has been developed to replace the DES [11][12]. AES is designed to be more secure than DES with variable key length. Combining optimized AES encryption with Biometric authentication such as Finger print pattern capable of safeguard against all known attacks [13][14]. All messages pass through the mobile network are in encrypted form. Thus the system provides the integrity and confidentiality. It is very convenient to have non-reputability for the electronic transactions. According to mobile security through OTP bank generates and sends two random numbers, the confirmation number to the customer and the transaction number to the ATM machine. To complete the transaction, the system design enforces customer to disclose the confirmation number to the ATM machine. Only after that, the ATM machine is authorized to hand over the money to the customer. In the context of the ATM machine, the confirmation number received from the customer is a good evidence to verify that the transaction has happened completely. Very similar to the above described scenario, bank sever accepts the transaction only after

receiving the transaction number and the confirmation number from the ATM machine. Hence, none of the parties can rollback the transaction in illegal way. Moreover, the transaction number received from the ATM machine is good evidence to verify that the ATM machine has completed the transaction. So, the proposed system provides non-reputability for both customer and ATM machine. In order to maintain the system availability, all the resources such as bank server, ATM machine and mobile network should provide the efficient service to customers. Thus our proposed system maintains all the security services.

CONCLUSION

Thus our proposed system successfully addresses the issues in the current PIN based authentication of ATM machine and enhanced the security services. Performance of the proposed SSH algorithm and Security analysis of the proposed system were clearly showing that this framework can be easily implemented.

REFERENCES

[1] Richard. B and Alemayehu. M, "Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons", Journal of Internet Banking and Commerce, vol. 11, no.2. August 2006.

[2] "Authentication Reference Guide" Secure Computing Corporation, Sep 2002.

[3] "Authentication and Directory Services" Statewide Standard, STATE of ARIZONA, Government Information Technology Agency, May 2002.

[4] William Stallings, "Cryptography and Network Security: Principles and Practices", 5thEdition,
January 24, 2010.

[5] Ahmed Ali Karzan and Nadia Erdogan, "Securing Mobile Agent Systems in Which the Agents Migrate via Publish/Subscribe Paradigm", Lecture Notes on Software Engineering, Vol 2, no 1, pp 11-15, February 2014.

[6] Richa Purohit, Yogendra Singh, Dr. Upendra Mishra and Dr. Abhay Bansal, "Strengthening Hash Functions using Block Symmetric Key Encryption" , ,Int.J.Computer Technology & Applications,Vol. 3 no 5, pp 1715-1719, Sept-Oct 2012.

[7] Rajeev Sobti, G. Geetha, "Cryptographic Hash Functions: A Review", International Journal of Computer Science Issues(IJCSI), vol. 9, issue 2, no. 2, pp 461-479, March 2012.

[8] S.G. Srikantaswamy and Dr.H.D. Phaneendra, "Hash Function Design using Matrix Multiplication Ex-Or, Checksum Generation and Compression Technique Approach", International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 3 no 1, pp 115-119, February 2013.

[9] William Stallings, "Cryptography and Network Security: Principles and Practices", 5th Edition, January 24, 2010.

[10] Artan Berisha, Behar Baxhaku and Artan Alidema, "A class of Non Invertible Matrices in GF(2) for Practical One Way Hash Algorithm, International Journal of Computer Applications, Vol. 54 no. 18, pp 15-20, September 2012.

[11] Navneet Sharma and Vijay Singh Rathore, "Different Data Encryption Methods Used in Secure Auto Teller Machine Transactions" , International Journal of Engineering and Advanced Technology (IJEAT), vol. 1, issue 4, April 2012.

[12] Ms. Pratiksha, L. Meshram and Prof. Tarun Yenganti, "Credit and ATM card Prevention Using Multiple Cryptographic Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol. 3, issue 8, pp 1300-1305, August 2013.

[13] Fakir Sharif Hossian, Ali Nawaz and Khan Md. Grihan, "Biometric Authentication Scheme for ATM Banking System Using Energy Efficient AES Processor", International Journal of Information and Computer Science Vol. 2 Issue 4, May 2013.

[14] Sri Shimal Das and Smt. Jhunu Debbarma, "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System", International Journal of Information and Communication Technology Research (IJICT), vol. 1, no. 5, September 2011.