**International Journal of Engineering Research and Development**
*e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com*
*Volume 11, Issue 08 (August 2015), PP.19-24*

# Analysis of Security Algorithms used in E-Commerce and ATM Transactions

Raghav Sethi
*Student Department Of Computer Science Engineering,*
*Mukesh Patel School Of Technology Management and Engineering, NMIMS UNIVERSITY, MUMBAI, INDIA*

**Abstract**: E-commerce is trading ofproducts or services using computer and Internet. It mainly revolves around the Internet for it's functioning. Virtual mall, buying selling websites or domains, providing secure business transactions, collection and use of demographic data comes under e- commerce. E-commerce security is an important part for the framework and it is applied to the components that affect the vendor and the end user through their daily payment and interaction with business. Since it involves various transactions, E-commerce offers the banking industry a great opportunity but it also creates various risks and security threats. We can say in the near future people would like to carry their transactions though mobile devices instead of carrying currency in their wallets. Due to this the security of sensitive customer information is necessary. Thereare many security protocols and algorithms used in securing credit card transactions over the Internet and we will discuss and analyze the major ones**.**

**Keywords: -**E-Commerce, Security, SET, Verification, Transactions, Biometric, Key Algorithm, Analog data, Selection, Symbolic data, ATM

## I. INTRODUCTION

In the coming future the transactions would be done on smartphones/mobile devices rather than PCs. The existing online banking system has several drawbacks. Firstly hacking, from the Internet any one can hack the username and password and the result is third person gets access to owner account. And it is not feasible to carry laptops every time to make the online payment. The existing online transaction system is secure but there are various flaws in it.

To overcome these flaws Biometrics comes into picture. Biometric authentication technologies such as face, finger, hand, iris, and speaker recognition are commercially available today and are already in use. A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the context, a biometric system may operate either in verification mode or identification mode.

With rapid development of e-commerce industry more security issues are arising. The security of transaction and privacy of the customer is the key for the development of the e-commerce industry. The web applications are increasingly integrating third party modules and due to this the security challenges are increased. The complexity for the application to coordinate its internal states and the new module increases. Viruses and attacks by hackers for stealing private data or disrupting the services has increased as there is competition in the industry, for the proper growth of e-commerce industry, it should be secure and it should be customer friendly.

Transactions between buying and selling in e-commerce includes request of information, quotation of prices, order placement, payment and after sales services. Clearly an online transaction requires the customers to disclose very sensitive information to the vendor over the Internet i.e. bank details and personal information. Thus a secure system is required to build the customers trust.

Security protocols in E-commerce servers' aims at providing some basic guarantees to their clients these include as

- Confidentiality: the service provider does not learn about the data of the customer
- Integrity: if any changes are made by the cloud storage server, that should be easily detected by the customer
- Availability: Customer can access it's data from anywhere from any system
- Reliability: Data properly backed up
- Efficient Retrieval: Data should be easily retrievable
- Data Sharing: Customer can easily share its data with other parties

## II.SET MODEL ALGORITHM

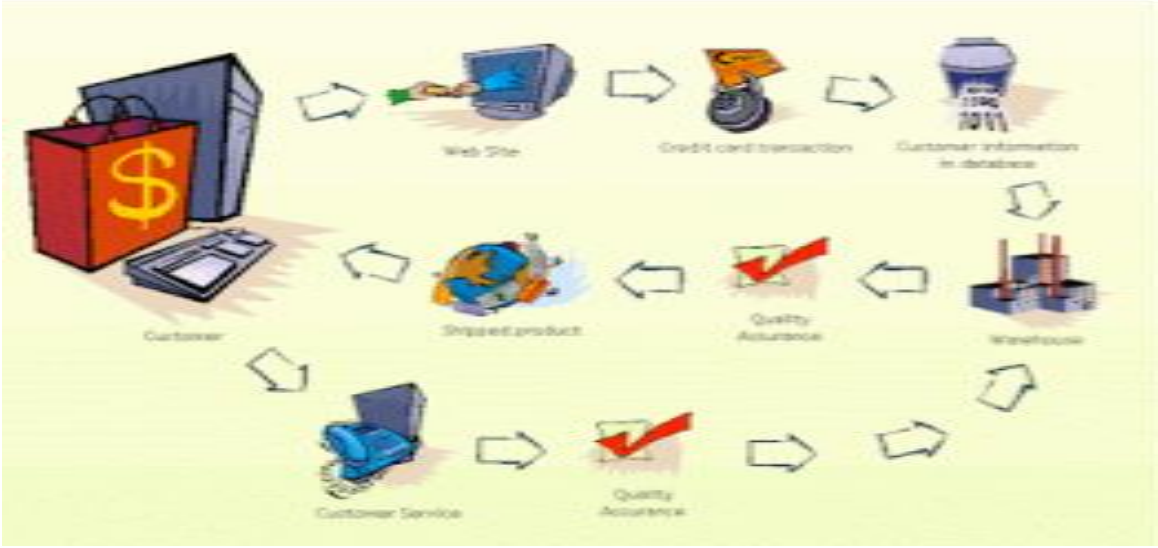
The two models that are mainly improvement to the existing SET model:

A. SET Algorithm
B. Modified SET Algorithm

### A. SET ALGORITHM-

The steps modified are:

1) The customer requests to the merchant.
2) Merchant provides all the product details to the customer.
3) Customer order, the order is processed and digitally signed by the customer.
4) The merchant decrypts the above data to recover the certificate and the public key certificate of the customer and then it is verified whether the customer places the order. The merchant encrypts the digital certificate and the payment gateway certificate; this involves the identification and all the details of the product [1].
5) The customer decrypts and confirms that the merchant sends the data. Then, customer produces symmetrical key K stochastically, used to encrypt data The account information of customer, (name, credit card number and so on) and K are encrypted with the Public keys and the payment gateway. Customer carries on the signature on and then transmits all these information to the transaction authentication center CA [2].
6) Transaction authentication center CA decrypts all the data and the transaction is recorded in the database. The CA generates a digital signature and then transmits to the payment gateway [1].
7) The payment gateway decrypts the data and confirms whether it is sent from the CA similarly it checks for the customer and the merchant. The public key of the customer is decrypted and sent to the credit card company through a safe network.
8) The credit card companies check about the customer in their database and confirm.
9) The payment gateway issues notice to the merchant [4].
10) The merchant decrypts message and confirms that it is sent by payment gateway and the goods will be delivered to the customer.



### B. Modified SET Algorithm-

In the modified version of SET, the customer details, product details, payment details and other information is encrypted and decrypted every time and used in all the steps

The SET protocol makes use of cryptography for its process and the main purpose for implementing SET protocol is:

1) Provide confidentiality
2) Ensure integrity
3) 3.Authenticate both customer and the merchant

There are mainly four entities in this system:

1) The customer
2) The merchant
3) Payment gateway
4) Issuer (Bank of the cardholder)

For initiating the process both the merchant and the cardholder must obtain a digital certificate for their public keys. The main flow of the SET protocol described by the author is as follows:

1) Customer selects the product from the merchant's website.
2) Merchant sends the information of the product and bill; during this the merchant also sends a digital certificate [4].
3) Authorization is done in both the banks and confirmation is sent to the merchant.
4) The merchant completes order.
5) The merchant captures the transaction
6) The customer receives payment notification.

## III. TIC AUTHENTICATION ALGORITHM

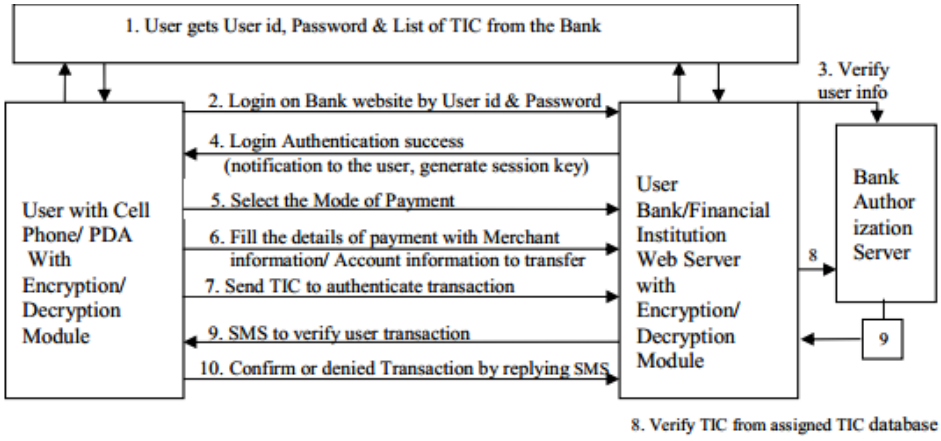
- The TIC codes are issued by the bank or financial institutes to its customer.
- An 8bit or 16 bit Pseudo code is generated [1].
- It can be a digit sequence or combination of numeric and alpha numeric characters.
- The TIC codes is secured and stored in the users smartphone.
- The bank keeps a track of issued TIC codes to its customers and matches the same code during internet transaction.
- The bank can also decide to designate a valid time period of TICs according to its standard organizational issue policies [2].

## 1V. SMS AUTHENTICATION ALGORITHM:

- SMS can also be used to validate user transaction.
- Since the users will be carrying their phones most of the time, so for the online transactions security codes can be sent using SMS.
- After receiving the SMS the user can acknowledge the choices i.e. either YES/NO [4].

Thus multifactor authentication consists of the following:

1) Web based authentication
2) TIC authentication
3) SMS authentication




## V. PUBLIC KEY ALGORITHM

In the e-commerce industry, three parties are involved in all transactions.

- Firstly, the customer,
- Secondly Trusted Third Party (TTP) and
- Lastly the merchant.

For the above transactions, we are going to apply the new public key algorithm based on the linear block cipher [3]

Customer request to TTP for token consider as a message or plain text.

Modular function*:*

(a +b) mod n = [(a mod n) + (b mod n)] mod n

(a-b) mod n [(a mod n) – ( b mod n)] mod n*)* [1]

(a * b) mod n = [(a mod n) x (b mod n)] mod n*)*

Now customer has one key issued by the TTP and Merchant that has o decryption. The customer key is a square matrix issued by the Trust Party and the inverse of square matrix is Merchant key [3].

In order to provide quick and simple encryption/decryption, the bits s secret key has to be effectively [4]. For encrypting small amount of data, there should overhead to the encrypting system as well as there should not be any compromise security level.
Thus an optimized size of 64 bits is chosen.

**I.** Request for the token from TTP -

**II.** Assume the customer sending message about product and asking TTP's Consider here product or message or plain text is 'INDIA' i.e.9,14,4,9,1

**III.** TTP calculating customer message with key Here we are selecting the key as e=$^{21}45$

**IV.** Invertible is (2 * 5) – (1 *4) = 6 is no common faction in Z37.

**V.** Selected matrix is 2x2, so makes a message as a 2 blocks i.e. (9,14), (4,9), (1, 37) used for blank space.

**VI.** Now we are calculating message with selected key i.e. 'e'Customer Token = (m * e) mod 37

| | | | | |
|---|---|---|---|---|
| 9 | | *21 | mod 37 = mod37 | 3 = 2 1 8 |
| 1 4 | | 45 | | 3 2 |
| | | | | |

Therefore message (9,14,4,9,1,37) will becomes (32,32,17,24,2,4)
Customer send the encrypted message i.e (32,32,17,24,2,4) to Merchant iv) TTP generate the private key i.e inverse of 'e' is known as $e^{-1}$[4].
C11$[-1]^{1+1}$ x[5]=$[-1]^{2}$ x[4]=5C12$[-1]^{1+2}$ x[4]= $[-1]^{3}$ x[3]=-4C21$[-1]^{2+1}$ x[1]=$[-1]^{3}$ x[1]=-1 C22 $[-1]^{2+2}$ x [2] = $[-1]^{4}$ x [2] = 2[4].

| | | | | | |
|---|---|---|---|---|---|
| | | mod 37<br>-1 e= = - 6 * | 5 7-1 | 6 | |
| -4 | | | 2 4 | 2 5 | |
| | | | 2 | | |
| | | | 6 | | 3 M2 o d 3 7 * = 7 9 |
| | 24 | | 2 5 | | 32 14 |

## VI. MESSAGE AUTHENTICATION ALGO

Message Padding- The message can be of variable length. SHA-1 digests the message in the form of message blocks each of 512bits. To be able to break the message into multiple blocks of equal length, we must pad the message. SHA-1 sequentially processes these blocks of 512bits each. The message can be padded by putting a "1" on the right or 'n' number of "0"s [4].

**Computing the Message Digest-**
There are two main methods, which SHA-1 adopts to obtain the message digest:
**Method 1:**

- First the message is padded before digesting as described before.
- It involves two buffers, each of which have five 32bit words.
- It also involves a sequence of eighty 32bit words. • The words of the first 5-word buffer are named A,B,C,D &E.
- The words of the second 5-word buffer are named H0, H1, H2,H3& H4. • The words of the eighty word sequence are named W(0),W(1).....W(79).
- To obtain the message digest, the individual message blocks of 512bits each processed in order.

- After processing, the message digest is the 160bit string given by the 5 words H0 H1 H2 H3 H4 [4].
- It has a much lesser execution time than Method 2 as the address computations are comparatively simpler.
- Uses more storage than Method 2.

**Method 2:**

- In this method, instead of using 80 32bit words we use only W (0),....,W(15).
- Here the 16 32bit words form a circular queue. • The message digest is given by words H0 H1 H2 H3 H4[1].
- Thus, using the second method saves 64 32bit words of storage.
- But the execution time is much more than Method 1 due to the complexity of address computations.

**PROPOSED SECURED FINGERPRINT PAYMENT SYSTEM**

- The solution involves the use a biometric authentication mechanism.
- A payment application would be installed onto a android device, for authentication finger print is taken at run time [3].
- The finger print template would be captured by the phone and compared against a stored template on a database server.
- The fingerprint template is encrypted by using the RSA algorithms and sends it to the host server (i.e.. Bank ). Fingerprint is used for the login purpose for the bank application on mobile.

## VII. INFERENCE

We infer from all the different algorithms, the research has given a general idea of the threats which are targeted to an e commerce website, different security issues are also discussed but solution to these issues are not addressed properly.

SET Model - The review paper has discussed two models i.e. the normal SET model and the modified SET model. In the modified SET model additional data is encrypted and decrypted at every step, which increases the time required for the completion of the process.

The security of the e commerce websites and the online transaction will be improved, which will create customer trust. The customer trust will act as a catalyst, which will help in the steady growth of the e commerce industry

## VIII. CONCLUSION

Thus we can say that the threats to a website particularly an ecommerce website is very high. Since the industry is growing rapidly, to get the customer's trust for steady growth of the industry the transactions and sensitive customer data should be secured. By implementing a secure transaction web application we can use the security of the system.

The SET model provides security to the online transactions but by using the modified SET model the no. of encryption and decryption steps are increased which increases the time required for the completion of the transaction. The computational time is increased with the increased number of encryption and decryption steps.

The SET model provides security to the online transactions but by using the modified SET model the no. of encryption and decryption steps are increased which increases the time required for the completion of the transaction. The computational time is increased with the increased number of encryption and decryption steps.

By implementing biometrics in online transactions, the security can be further enhanced. It is difficult to replicate a biometric pattern. Authentication request and reply are in the encrypted form. This gives the better level of security mechanism for mobile payment system. The proposed system can be used in mobile banking and M-commerce.

## IX. FUTURE SCOPE

In the coming future the transactions would be done on smartphones/mobile devices rather than PCs. The existing online banking system has several drawbacks. Firstly hacking, from the Internet any one can hack the username and password and the result is third person gets access to owner account. And it is not feasible to carry laptops every time to make the online payment. We can say in the near future people would like to carry their transactions though mobile devices instead of carrying currency in their wallets. Due to this the security of sensitive customer information is necessary. This gives the better level of security mechanism for mobile payment system. The proposed system can even be used in mobile banking and M- commerce.

## REFERENCES


[1]. Niranjanamurthy and, Dr. DharmendraChahar," The study of E-Commerce Security Issues and Solutions"International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013.

[2]. Hassan M. Elkamchouchi ,Eman F. Abu Elkhair2 and YasmineAbouelseoud " AN IMPROVEMENT TO THE SET PROTOCOL BASED ON SIGNCRYPTION" in International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 2, June 2013.

[3]. AyuTiwari, SudipSanyal, Ajith Abraham, Svein Johan Knapskog and SugataSanyal "A MULTI-FACTOR SECURITY PROTOCOL FOR WIRELESS PAYMENT- SECURE WEB AUTHENTICATION USING MOBILE DEVICES" .

[4]. American National Standards Institute. 1994. Accredited Standards Committee X9 Working Draft: Public Key Cryptography for the Financial Services Industry: Management of Symmetric Algorithm Keys Using Diffie-Hellman. ANSI X9.42-1993

[5]. Zhang Jian, "Analyzes based on the SET agreement electronic commerce safety mechanism", Netinfo Security, 2006(10),pp:9-11.

[6]. G. Eschellbeck, "Active security a proactive approach for computer security systems", Journal of Network and Computer Applications, vol. 23, (2000).

[7]. G. Antoniou and L. Battern, "E-commerce: protecting purchaser privacy to enforce trust", Electronic commerce research, vol. 11, no. 4, (2011).

[8]. Zhang Yifei,(20-22 aug,2010) ,"Research on online payment pattern and security strategy of e-commerce" ,IEEE Internet Technology and Applications pp 1-4.