INVESTIGATING AND DEVELOPING SECURE ELECTRONIC PAYMENT PROTOCOL FOR MOBILE PAYMENT SYSTEM

Ms. Mansi Patel [1], Mr. Hitesh R Chhikaniwala[2]

[1] *Masters of Engineering Student, Computer Science and Engineering, GTU PG School, Gujarat, India*

[2] *Associated Professor, Adani Institute of Infrastructure Engineering, Ahmedabad, Gujarat, India*

ABSTRACT

The exposure of mobiles and wireless technologies has made the entrance of electronic commerce possible with the new applications and research subject: Mobile commerce, mobile commerce can be defined as the exchange or buying and selling of commodities, services, or information on the Internet through the use of mobile devices. Still there are few big challenges like lack of consistency in security and payment methods and an absence of consensus on technology standards for the growth of M-commerce. So there have been many security and payment technologies proposed and applied, which are highly diverse and broad in the m-commerce application. Many sensitive information transfer through insecure network like Credit Card number, PIN and some other personal information transfer through insecure network in Mobile commerce transaction. To solve issues like interception or eavesdropping of the data during payment transaction there have been many protocols with cryptographic algorithms developed in the past for secure payment system. Secure Electronic Transaction (SET) is an open standard protocol for protecting the privacy of electronic transaction and it ensures authenticity and integrity of data.

Keyword: - *E-commerce, Secure Socket Layer (SSL), Secure Electronic Transaction (SET).*

1. INTRODUCTION

Today, E-commerce is widely used on an internet for payment. Payment over an internet is one of the big Security issues. E-commerce payment is done either by credit card or by debit card and for that customer has to provide his /her credit card/ debit card information for the payment [1]. Hence, In E-commerce transactions transfer credit card information and personal information through internet. An internet is insecure and entrusted communication network so possibility of eavesdropping, Phishing, Fake information, Man-in-middle attack , Intercepting of personal information of cardholder, merchant and sensitive information like PIN and credit card number. To maintain the security of data with E- commerce transactions secure payment system protocols are accessible. Secure transaction payment protocols are SSL, iKP (i=1,2,3), SET which maintain communication synchronization between cardholder, merchant and payment gateway. SET protocol is also providing data security. There are mainly three participants in E-commerce transaction: Customer(C), Merchant (M), and Bank (B). These participants are connected with a communication link [3].

Figure 1: Typical E-Commerce Scenario [3]

Some other issues are also possible during E-commerce other than above discussed.

- "Merchant (M) needs to ensure that customer(c) are authorized to use credit card."
- "Customer(C) has to trust on Merchant (M) and Bank (B) both."
- "Merchant (M) and Bank (B) would not to see the details of Payment and Order information respectively. These might be a business secret of Merchant and a privacy respect for Customer.

The important Security requirements for a successful E-commerce transaction are discussed below:

1.1 Security Requirements

Confidentiality: It mainly required ensuring the confidentiality of the data not to be lost due to unauthorized access of data. To prevent interception and eavesdropping of the data during transmission system need to be encrypting it using different cryptographic algorithms.

Integrity: In simple term, Integrity means no modification. Completeness of the information is requires the electronic payment recipients should verify the received Information is true and complete or not being changed during transmission.

Authorization: To prevent fraud both sides should able to confirm the authenticity of each other's identity to ensure that the data to be transferred was, in fact generated by the signed author.

Non repudiation: It ensures that the client and server are who each claims to be, so they cannot deny for the transaction which they have did. For satisfied Non- repudiation, use Digital signature.

Availability and Reliability: During the E-commerce all parties' transaction requires the ability to make or receive whenever necessary. So software and hardware components of the E-commerce should be availability and reliability.

2. MOTIVATION AND OBJECTIVES

2.1 Motivation

In the 21st century the use of internet is exponentially increasing day by day, especially in the business transaction, in that the share of the developing countries like India, Brazil, South africa, etc steep raise in using of World Wide Web(www) with short period. The internet provides the virtual link between people, which has helped the banking and government sector's service more easy by providing services like E- banking, E- voting, E-governance, etc. These electronic services are cheaper and faster to carry out business transaction on an internet. The online services which provides the virtual excess to the people requires various securities to protect the data of the users and provide reliable usage internet medium among them. Among all online services E-commerce service is catering the most (active) users on the internet. E-commerce services are the most vulnerable against the online transaction and internet based payment system, so the security is key issues here. Currently there are many threats present on the internet which affect the security system of E-payment transaction and risk of data breach of users. As a scope of the dissertation we have measured the overhead for the message security and calculate speed of the transaction in mobile payment system.

2.2 Objectives

As we all know the importance of data security and processing speed in electronic payment system. Different secure payment system protocols are designed based on the requirement of data security. For that various cryptographic algorithms are used in the protocol. In between some of the protocol provides high level of security but if security is high its overhead is also high. And if data overhead is high than it decreases the overall performance of the payment system. In SET protocol RSA 1024 bit key size is used for data confidentiality and SHA-1 hashing algorithm is used for the data integrity.

In the proposed method alternate of RSA public key algorithm is presented which is Elliptic Curve Cryptography (ECC) that provides same level of security with small key size, so it increase the processing speed which reduce the data encryption overhead and also increase overall performance. For the data integrity checks the performance of MD5 and SHA-1 both and observe the results which one is fulfill our requirement and improves the performance of our system.

3. BACKGROUND THEORY

Cryptographic techniques are providing the confidentiality, user authentication, non repudiation, information integrity. All the method of cryptographic algorithms to provide security requirements. Oldest and very popular data security scheme is secure socket layer. SSL runs above TCP/IP and below high-level application protocols. Its secure point- to- point links at session layer. In this section we have understanding the available protocols and cryptographic algorithm for secure payment transaction.

3.1 Secure Socket Layer (SSL)

SSL Protocol is developed by Netscape. In SSL, Server authentication is requisite but client authentication is optional. SSL include two sub-protocols are the SSL Record Protocol and the SSL Handshake Protocol. Session keys are used to encrypt and decrypt information exchange during the SSL session and to verify its integrity using hash value. SSL uses public key cryptography to provide authentication. SSL also use secret key cryptography and digital signature to provide privacy and data integrity. SSL alone does not enough to provide non repudiation. It is vulnerable for the Man-In-Middle Attack [4]. SSL's transparency, less complexity, eases of use it is used for any secure application.

3.2 Secure Electronic Transction (SET)

SET is an open standard protocol for protecting the privacy of electronic transaction and it ensure the security and integrity of online transactions and purchases. The main objective of SET is to provide secure payment using credit cards over an Internet. SET transactions include the participants: the customer, the merchant and the payment gateway. SET provides many security aspects like:

Confidentiality of payment information.

Authentication of the Cardholder, Merchant and the Payment Gateway.

Integrity of the protocol messages.

Parting method of Order and Payment information to maintain privacy.

Message Flow between three participants: Cardholder, Merchant, Payment gateway of the SET as shown in figure

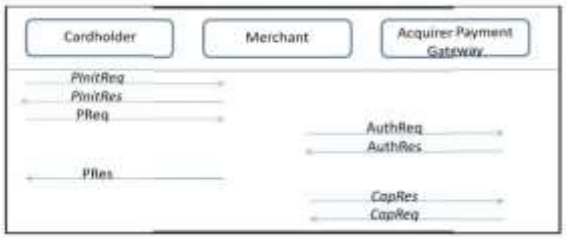


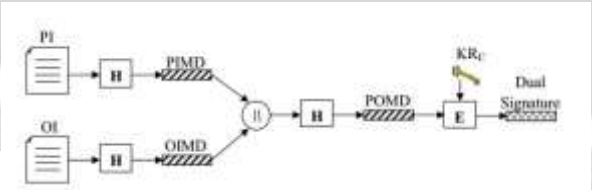
Figure 2: SET message flow [5].

In this figure, PInitReq and PInitRes messages are used to exchange certificate between Cardholder and Merchant. But they are optional. These messages are helpful for providing non repudiation security requirement.

Actual transaction is start from PReq message, which contain order and payment information. Order information is for Merchant and allow him to verify cardholder is agrees on order. Payment information is only for Payment Gateway because of it is encrypted by public key of Payment gateway. Now, Merchant forward encrypted PI to Payment Gateway using AuthReq message. The payment gateway responds with an AuthRes message to notify the merchant about the result of the authorization request. After receiving response, merchant forward it to the cardholder as PRes message. Merchant may include Capture request as CapReq in the Authentication request message to inform the clearing process to be performed directly.

3.3 Dual Signature

The objective of dual signature is to link two messages that are planned for two recipients. As we have seen OI is for Merchant and PI is for bank. The merchant does not know the customer's secret personal information and bank does not need to know customer's order. To provide privacy the customer keeps these two items different. Both the items must be linked in such that can be used to resolve controversy, and customer can prove that this payment is planned for this order and not for some other goods or services [6]. So to provide the link of two messages dual signature is used and the construction of dual signature is as shown in figure ([3][5]).



Where, PI= Payment information, OI= Order information=Hash function, ||=Concatenation, PIMD= PI Message Digest, OIMD= OI Message Digest, POMD= Payment Order Message Digest, KRc= Customer's Private Signature Key.

Figure 3: Diagram of Dual Signature [3].

4. PROBLEM DESCRIPTION

SET protocol family uses ***RSA*** public key cryptography algorithm for secure data transfer with ***SHA1*** to provide integrity. ***RSA*** with key size less than 1024 bits can be compromised because of high processing power. In ***RSA***, different key size can provides the required level of security. But, larger key size can increase the data security overhead. For required security level in E-commerce transaction ***MD5*** hashing algorithm has been used for data integrity. But ***MD5*** algorithm is no more secure with new cryptanalysis tools and fast processing power. It is also

not collision resistant thus it can be possible to generate the file having the same hash as of the original file eavesdrop by an intruder during the payment transaction through an internet and this violates the data security. In ***SET*** protocol, ***DES*** algorithm is useful for symmetric key cryptography. But, ***DES*** is no more secure in Symmetric key algorithm.

5. PROPOSED SOLUTION

We have proposed an approach of ***SET*** protocol for E-commerce system. In that, we have use ***ECC*** instead of ***RSA*** because of ***ECC*** can provide the same level of security with the lower key size as compare to ***RSA***. So it can improve the performance of existing protocol in terms of speed, level of security and also decrease the overhead of the protocol. We will applied experiments on different input with different key size and analyze the result in different parameters like speed and security. Not only ***RSA*** has been replaced with ***ECC*** within ***SET*** for possible performance improved, we have also studied the performance of ***SHA-1*** over ***MD5***, for integrity aspect. Study suggested that ***SHA-1*** is less vulnerable to provide integrity compared to ***MD5***. And we have also check the performance of ***AES*** over ***DES***, for symmetric key cryptography. ***AES*** is more secure compare to ***DES*** and ***3DES***.

6. EXPERIMENTAL SETUP AND RESULTS

Secure Electronic Transaction (SET) protocol provides privacy, confidentiality, non-repudiation, authentication and integrity on the information which is transfer through insecure network during payment transaction. SET is mainly use to provide secure payment using credit cards over an open network such as internet. SET protocol consists: 1) Customer 2) Merchant 3) Payment Gateway. These three entities are communicated secretly with each other. In SET protocol, RSA 1024bit used for data encryption/decryption and SHA1 hash is for data integrity. Java JDK 1.8 is chosen as implementation tool. An implementation of this system because java is object oriented characteristics makes the implementation easy to be managed and it also provides the socket programming for communication between different parties. Java cryptography Extension provides the cryptographic engines such as encryption & decryption, digital signature. Java also provides keytool to generate certificate. The platform of our experiment is windows 8.1 pro, running on Intel core i5- 5200u CPU 2.20 GHz processor with 8 GB RAM.

6.1 Experimental Results and Analysis

In this section contains the test results of our experiments for an existing and proposed approach. It shows encryption and decryption time taken by various file size with the framework of SET protocol. In SET protocol DES algorithm is use for symmetric key, RSA algorithm is use for asymmetric key and SHA1 is to check the integrity of data. In our proposed work we take different combinations of algorithms for integrate the whole system and this system provides privacy, confidentiality, non repudiation and authentication between different parties. For that, DES and AES is use for symmetric key algorithms, RSA and ECC is use for asymmetric key algorithms and also check the integrity with MD5 as well as SHA1. As shown in our experimental results for smaller message both hash algorithms value is approximately same. For this reason to provide higher security in our system SHA1 hash algorithm is use for check the integrity instead of MD5 because SHA1 is more powerful than MD5. Table 1 show the encryption and decryption time for different file size taken by RSA algorithm with 1024 bits key size, ECC algorithm with 160 bits key size and for symmetric key we use DES 56 bits and AES 128 bits. While we are running these algorithms in single time it is not give you a satisfied value. So each operation for every test parameter was run by 10 times in order to reach a satisfactory level. These test results are an average of encryption time and decryption time for different file size. As we can see in table 1 the major time difference in between RSA and ECC because of ECC provides the same level of security with smaller key sizes as compare to RSA. For small file size, ECC takes a minor decryption time. Thus, it reduce the processing overhead of the system.

An experimental result of SET protocol is shown in table 1. Table 1 contains combinations of different algorithms encryption and decryption time (in millisecond) with different file size (in kb) and also hash calculation time of MD5 and SHA1 (in millisecond).

Table 1: Results of SET protocol

File size	Combination of algorithms	Encryption time (ms)	Decryption time (ms)	MD5 (ms)	SHA1 (ms)
	DES and RSA	405	259.74	0.1273	0.1271
1 KB	AES and RSA	338.62	240.71	0.1273	0.1271
	DES and ECC	373.23	7	0.1262	0.1267
	AES and ECC	377.63	5	0.1262	0.1267
	DES and RSA	412	271.6	0.1156	0.1125
2 KB	AES and RSA	374	240.31	0.1156	0.1125
	DES and ECC	372	11	0.1123	0.1115
	AES and ECC	380.9	7	0.1123	0.1115
	DES and RSA	418	279	0.1181	0.1175
3 KB	AES and RSA	395	261.34	0.1181	0.1175
	DES and ECC	370	12	0.1162	0.1155
	AES and ECC	382.14	8.2	0.1162	0.1155
	DES and RSA	422.47	282	0.1291	0.1293
4 KB	AES and RSA	425.8	264	0.1291	0.1293
	DES and ECC	372.53	13.1	0.1282	0.1279
	AES and ECC	386.6	9	0.1282	0.1279

From the results of above table 1 we can say that combination of AES and ECC provides the higher security with the small key size as compare to other combinations with less amount of time.

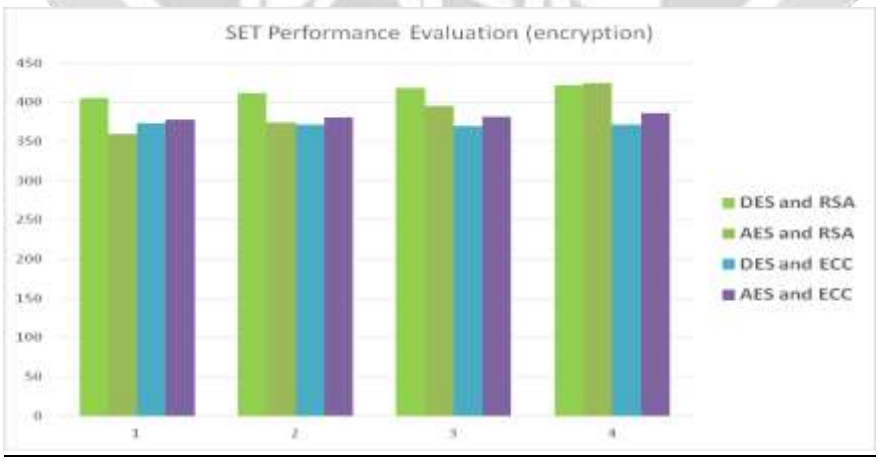


Figure 4: Comparisons of different combination based on decryption time

Figure 4 shows graphical representation of encryption time for different combinations of algorithm with 1 kb, 2 kb, 3 kb and 4 kb file sizes. From the figure 4 we can say that combination with ECC algorithm takes smaller time compare to combination with RSA algorithm. At the end, AES and ECC combination is best in terms of security and time aspect.

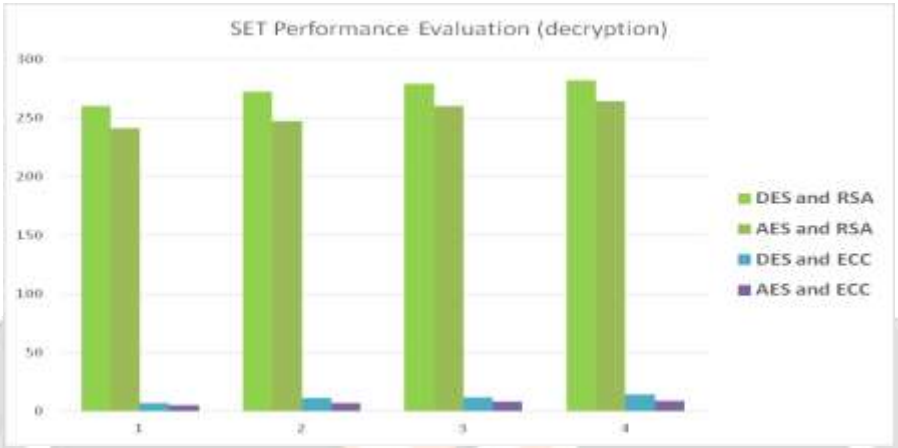


Figure 5: Comparisons of different combination based on encryption time

Figure 5 shows graphical representation of decryption time for different combinations of algorithm with 1 kb, 2 kb, 3 kb and 4 kb file sizes. From the figure 5 we can say that combination with ECC decryption algorithm takes much smaller time compare to combination with RSA decryption algorithm. At the end, AES and ECC is best combination in terms of security and time aspect for decryption.

7. CONCLUSIONS

Secure payment transaction is necessary for all the online business development. E-commerce system is helpful in many ways but it has many complexity issues involved with its transaction. SET is a good transaction protocol for credit card payment but due to its high time complexity which is turn increases overhead. The objective of our proposed framework is to improve the efficiency of the existing secure payment system in mobile environment which has limited available processing power. For that, we have taking different combination of algorithms in our proposed work. In proposed model, we have use ECC in place of RSA because ECC 160 bits provides same level of security as compare to RSA 1024 bits with smaller key size. Along with that for symmetric key cryptography we have apply AES 128 bits instead of DES 56 bits. In general AES takes higher execution time compare to DES but in our algorithms have been tested with only 1 KB to 4 KB file size and for the smaller file size both algorithms execution time difference is minor. We have also check data integrity in terms of MD5 and SHA1. As we above conclude that SHA1 is more secure and powerful than MD5. So we have use SHA1 algorithm to check the data integrity in our system. As processing time reduces significantly with SET using the combination of AES and ECC and SHA1, such approach can be considered for limited processing power devices, mainly for mobile payment.

8. REFERENCES

[1]. Đurić, Zoran, Ognjen Marić, and Dragan Gašević. "Internet payment system: A new payment system for internet transactions." *Journal of Universal Computer Science* 13.4 (2007): 479-503.

[2] Chen, Xing. "Research of the electronic commerce information security technology." *Proceedings of the 3rd international conference on Anti-Counterfeiting, security, and identification in communication*. IEEE Press, 2009.

[3] Y. He, P. Wei and Y. Shi, "The Research on Secure Payment System of E-Commerce", Asia- Pacific Conference on Communication Technology, 2010.

[4] "Secure Sockets Layer (SSL) Protocol Overview" http://publib.boulder.ibm.com.

[5] van Cuijk, Mark. "iKP and SET: a comparison." (2009).

[6] Liu, Xiuhua. "The Study on E-commerce Security Based on ECC and SET." *2011 Third International Conference on Communications and Mobile Computing*. 2011.

[7] Chaudhry, Shehzad Ashraf, et al. "A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography." *Electronic Commerce Research* 16.1 (2016): 113-139.

[8] Zhang, Xuan, Qinlong Huang, and Peng Peng. "Implementation of a Suggested E-commerce Model Based on SET Protocol." *Software Engineering Research, Management and Applications (SERA), 2010 Eighth ACIS International Conference on*. IEEE, 2010.

[9] Yong, Xu, and Liu Jindi. "Electronic payment system design based on SET and TTP." *E-Business and E-Government (ICEE), 2010 International Conference on*. IEEE, 2010.

[10] Tripathi, Devendra Mani. "A note on modified SET protocol for mobile payment." *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*. IEEE, 2011.

[11] Sun, Aifeng. "Optimization Study for Lightweight Set Protocol." *Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference on*. IEEE, 2012.

[12] El Ismaili, Houssam, Hanane Houmani, and Hicham Madroumi. "A Secure Electronic Payment Protocol Design and Implementation." *International Journal of Computer Science and Network Security (IJCSNS)* 15.5 (2015): 76.

[13] van Cuijk, Mark. "iKP and SET: a comparison." (2009).

[14] Li, Yabo. "The design of the secure electronic payment system based on the SET protocol." *Computer Science and Information Technology, 2008. ICCSIT'08. International Conference on*. IEEE, 2008.

[15] Sherif, Mostafa Hashem, et al. "SET and SSL: Electronic Payments on the Internet." *Computers and Communications, 1998. ISCC'98. Proceedings. Third IEEE Symposium on*. IEEE, 1998.