Abstract-- E-commerce is buying and selling through the Internet where the payment process is electronic. Electronic payment (e-payment) is the critical support phase of e-commerce contains sensitive data in transactions and consequently, it must be secure. Therefore, a security protocol (cryptographic protocol) is used in the transaction between parties, and it must be satisfy security properties. In this paper, we study e-payment phase in SET protocol. We found it still has problems of huge and complex transactions processes and not fully satisfy security properties. We introduced an enhanced model that represent the all participants in e-payment phase and functions for each, our model presented sequence diagram for transactions, which reduce the numbers of transactions steps from thirty five to fifteen steps. The functions of removed steps are handled by a “controller agent” working in parallel with these transactions. Such control agent is able to make decisions in an automated way according to the interactions and capable of terminating the process in case of fraud or attack.

1.1 INTRODUCTION

The growth of Internet, as a medium of transaction, has made it possible for the economic transformation in which commerce is becoming electronic. Besides, the success for every e-commerce activity is one of the critical factors for the security of the transaction. The payment phase is the support phase contains sensitive data and bank accounts. The payment processes takes place in several methods.

There are three types of payment: e-cash, stored value and e-credit card. Credit card is the most common means used in e-commerce. Credit card represents an account that extends credit to consumer that permits consumers to purchase goods while deferring credit payment. Visa and MasterCard issue the credit cards and process transaction and act as financial intermediaries minimizing the risk on transaction parties.

Participants description in e-payment phase, functions for each participant and steps of payment between these participants to success the payment operation described thoroughly in this paper. Moreover, enhancement models for e-payment SET protocol called Enhanced SET (E-SET) protocol. After designing the model it is described informally by using graph and sequence diagram.

The enhancement in the model (E-SET) was done by reducing the number of transactions procedure to fifteen steps with controller agent. It works concurrently with transaction as arbitrator to verify and authenticate transactions. It also contains evaluation function to verify and validate the contents of transaction.

1.2 SET protocol

The payment in e-commerce can take place using different means; some are popular; while others are not used. Table 1.1 [1] shows the best method for payment in e-commerce transactions. As shown in the table, the use of credit card in payment for e-commerce was the most frequent method (35% compared to other payment methods).

To ensure the success of e-commerce that include large companies and small retailers, we must understand the various success factors of payment in e-commerce and consider them before introducing and implementing e-payment for e-commerce. In Table 1.2 [1], we present some factors that give a measure of the use of e-commerce.

<table>
<thead>
<tr>
<th>E-Commerce Payment Systems</th>
<th>Percentage</th>
<th>Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card</td>
<td>35</td>
<td>1</td>
</tr>
<tr>
<td>Debit Card (Smart Card)</td>
<td>26.5</td>
<td>2</td>
</tr>
<tr>
<td>Cash on Delivery</td>
<td>23.5</td>
<td>3</td>
</tr>
<tr>
<td>Bank Transfer</td>
<td>9</td>
<td>4</td>
</tr>
<tr>
<td>Money Transfer</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Postal Transfer</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Prepaid Card</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Payment Through Convenience Store</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>0</td>
</tr>
</tbody>
</table>

From the table 1.2, one can see that the most affective factor in the payment process is security, and studies and researches built protocols to protect the transaction payment. Such protocols must satisfy integrity, non-repudiation, authenticity, confidentiality, privacy and availability. These protocols as Secure Socket Layer (SSL), Highly Enhancement Secure Socket Layer (HESSL), Secure Electronic Transaction (SET), and Internet Keyed Payment protocol (iKP) are commonly developed for this purpose.

SET is an open protocol used in e-payment. [2], [3], [4],[5], [6], [7], [8], [9], [10] developed Visa and MasterCard on February 1996 with a collaboration from leading Microsoft, IBM etc. The SET protocol is
Table 1.2
Factors affecting E-Payment (Singh, 2009)

<table>
<thead>
<tr>
<th>Factors</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concerns about security</td>
<td>70</td>
</tr>
<tr>
<td>Difficulties to enter information</td>
<td>9</td>
</tr>
<tr>
<td>Do not have credit cards/smart cards etc.</td>
<td>7</td>
</tr>
<tr>
<td>Do not like interest charge</td>
<td>6</td>
</tr>
<tr>
<td>Purchase value is too small</td>
<td>4</td>
</tr>
<tr>
<td>Exceeded personal limit</td>
<td>4</td>
</tr>
</tbody>
</table>

The common protocol in electronic transaction, which utilizes cryptography for protecting the privacy and ensuring the authenticity of electronic transaction [6].

When comparing the SSL and SET protocol for security properties as the table 1.3 [4] below shows, we will find that the SET protocol is better than SSL protocol in security and in online transaction.

SET was developed to guarantee the requirements that allowing confidentiality of information. This ensures integrity of all transmitted data, authentication cardholder that he/she is a legitimate user of branded payment, and authenticate merchant to accept payment card.

In a typical SET transaction, there is information where privacy between the customer and the merchant (such as the items being ordered) and other information that is private between the customer and the bank (such as the customer’s credit card number) is secured. SET allows both kinds of private information to be included in a single digitally signed transaction. A dual signature is used to accomplish this partial sharing of information while allowing all parties to be confident that they are handling the same transaction as information intended for the bank is encrypted using the bank’s public key whilst information for the merchant is encrypted with the merchant’s public key. This means that the merchant has no access to the credit card details; thus, a source of fraud is eliminated. Cardholder signs the hashes of both the order information and the payment information. Each party can confirm that the hashes in their possession agree with the hash signed by the cardholder. In addition, the cardholder and merchant compute equivalent hashes for the payment gateway to compare. Cardholders confirm their agreement on the details withheld from him.

Table 1.3
Comparisons between SSL and SET (A.Koponen, 2006)

<table>
<thead>
<tr>
<th></th>
<th>SSL</th>
<th>SET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol type</td>
<td>Secure communication protocol (end to end)</td>
<td>Secure payment protocol (multi party)</td>
</tr>
<tr>
<td>Entities</td>
<td>Buyer to seller</td>
<td>Cardholder, merchant</td>
</tr>
<tr>
<td>Authentication</td>
<td>Only merchants authorization</td>
<td>Mutual authentication</td>
</tr>
<tr>
<td>Privacy</td>
<td>No privacy</td>
<td>Good use dual signature</td>
</tr>
<tr>
<td>Ease of use</td>
<td>Good</td>
<td>Consumer credit card certification required</td>
</tr>
<tr>
<td>Mobility</td>
<td>Good can be used on way on any machine</td>
<td>Fair restricted on computer installed SET certificate</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Good</td>
<td>Fair due to complex cryptographic</td>
</tr>
<tr>
<td>Population</td>
<td>Very adopted</td>
<td>Not very adopted</td>
</tr>
</tbody>
</table>

A SET protocol involves six parties: cardholder, merchants, issuing bank, acquiring bank, payment gateway and authentication centers. Each participant entity is given an electronic certification. The cardholder presents the card to the merchant, and then an electronic message containing the card number and amount is sent to the issuing bank via payment gateway, with which the cardholder is associated and issuing payment card. After that, the issuing bank checks the available credit limit on the card and sends back an authorization. Finally, this authorization travels all the way back.

Based on the studies of researchers in SET protocol at e-commerce, SET protocol can be classified into three phases as summarized as follows:

**Registration phase**
The registration phase is the simplest phase in e-commerce. All participants must be registered before starting the transaction process, so as to obtain a certificate that is important for authentication.

**Purchase phase**
The purchase phase is the next step after the registration phase and is related to the payment phase (the next phase). In this phase the buyer browses the merchant’s site and selects what he wants. After the buyer decides to buy goods and services from a merchant, the merchant will transfer these goods and services to the buyer and the buyer will transfer cash or payment information back to the merchant.
Payment phase
The payment phase is the most important phase and represents the core of e-commerce transactions. This phase allows monetary exchanges using transactions that are done on the websites. The payments processes are done in several ways [1], [7]; such as, internet banking, e-payment card as credit card payments, micro payments, e-cash and other real time money transfers. Electronic payment should be secured in order to be sure that these transactions are secure and safe from any information breach.

In this paper, we will study e-payment phase in SET protocol. We found that it still has problems of huge and complex transactions processes and not fully satisfy security properties. In this paper our main concern will be the study for this phase which it has six steps shown in figure 1.4. The following transaction processes is a summarized version of the thirty-five transactions process stated in [11].

The merchant sends payment request to payment gateway.

The payment gateway will verify the digital certificates of both the merchant and the cardholder and decrypt the message to access the card number and the amount, and then it will be sent to the issuing bank.

Then, the payment gateway will interface with the legacy systems of the acquiring bank to send the transaction to the card brand, which will then send it to the issuing bank for authorization.

When receiving payment request, issuing bank checks validity of cardholder credit card, then verifies if he/she have sufficient money in account. If yes, the bank will take the specific money and send it to the acquiring bank.

Acquiring bank will receive the money and adds it to his account, and sends response to the issuing bank about receiving money and sends it to payment gateway acknowledgement to tell merchant that his account is larger now by adding the payment money.

Issuing bank sends response to payment gateway and this authorization response is then encrypted in the usual fashion and sent to the merchant, who, in turn, will validate the message and store the response. Then, the merchant will arrange to ship the goods.

1.3. Our model of the E-payment in SET protocol
In this section, we will explain the standard components as shown in figure 4.5 which is usually used in payment transactions where the complete descriptions for each component can be as follows:

Cardholder
The cardholder is a consumer who owns the credit card given by issuing bank that has account for consumer. The consumer is making request for something from E-payment merchant online, and buyers represent the major target of all electronic payment system. They decide whether they want to use an electronic payment system to buy a certain thing.

Merchant
The person, company, or retailers receiving E-payment exchange applications for goods or service. Merchants are shop owners selling goods or services to buyers and receiving the money from the buyers in exchange of goods and services. They can choose the electronic payment systems to set up in their shop (or website) and hope that these electronic payments system can help them to have more convenient methods to get payment from the buyers. In some special cases, the user who receives money from other users in an electronic payment system is also seen as the Merchant.

Issuing bank
The bank issues the credit card to consumer who has account in it and has privilege to sell anything according to his account and verifies that cardholder have sufficient money in his account.

Acquiring bank
This bank is financial institution creating merchants account which store their money before and after the transaction. Nowadays, there are many banks which also provide the electronic payment system by themselves (such as internet banking from ABN Ambro).

Payment gateway
The payment gateway is an intermediate between banks and ETC. It transmits the transaction for payment safely and controls the transaction occurring between banks.
ETC (Electronic Transaction Center)
ETC is the application of controlling the transactions between consumer, merchant and payment gateway, and defines certificate for request and approval and support the identity for cardholder, merchant and payment gateway, the ETC add time stamp for each ordering and authenticate from each transaction and contain the region Certificate authority (CA) function.

Figure 1.5 shows the fifteen steps in the current model in contrast with Boping and Shiyu model [11] that contains thirty-five steps. These long steps give hackers a time required to penetrate in the system and also increases the complexity in transactions steps. Whereas, Xu Yong and Liu Jindi [12] were facing long time to finish transaction.

On the other hand, current SET protocol do not fully satisfy main security properties (privacy, authentication, and non-repudiation[12] and [9] argued that SET protocol has authentication problems such as that payment information is sent to the banks by unreliable merchant who is not trusted to deal with or send sensitive information. Moreover, lack time term information leads each party to denial transaction done by users.

[13] also argued the authentication problem are found in the encryption algorithm. This algorithm has insufficient capability since it will break successfully and results in denial transaction.

[14] faced authentication and privacy problems. In his work the security of online data transmission and the identification verification for each party were not guarantee. [10] found problem of privacy and non-repudiation. Problems of saving and checking payment information were not solved.

Also, this information may be altered or used in illegitimate way. None of the party’s guarantee that the others are trusted to deal or send sensitive information and dose not guarantee the privacy among parties.

Finally,[8], [9], [11] were unable to protect cardholder and merchant because there is no guaranteed privacy among parties. They also did not know how to store or destroy data safety. Consequently, none of the parties guarantee that the others are trusted to deal with or send a sensitive and cause denial of service.

In our model of enhanced e-payment SET protocol, by adding control agent to behave as an arbitrator is used to solve the above issues.

The authentication problem is solved by using evaluation function done by control agent to verify authentication properties by time-stamp, hash function, identification and digital signature. Its work as an arbitrator, which allows transacting after the authentication and judgment. This shall increase authentication and decrease non-repudiation.

The privacy problem is solved using public and private key and adds special value through evaluation function in control agent. It checks if any intruder accesses, the content of transaction information stops operation.

1.4 The Transaction Steps
In this section, the simplified transactions between all parties in the E-SET model as a sequence diagram are shown. First, it shows every transaction between two parties that have a relationship between them, and then shows the sequence of model E-SET as a whole.

1- Transaction between cardholder and merchant
Figure 1.6 stated the transaction between cardholder and merchant by the following:

The user, who owns credit card and uses computer connected by internet, browses the website, which belongs to merchant. When he accesses it, he puts his/ her own identity (UID) with time stamp, his/ her certificate, expiration date for certificate and his/ her secret key by hashed and digitally...
signed and encrypted with a merchant secret key message. Then the requested good and services will be chosen.

The evaluation process performed by the internal agent that will check the validity of the transaction, first it evaluates the process of encryption, then the agent will evaluate the time stamp by ensuring that it is a valid, not reused and did not change during the running process. At the end agent will check the expiration date of the user certificate to ensure any vendor that valid amounts will be paid-off before expiration date. The agent will evaluate the set of messages and the freshness of the set of names, which are bounded by this transaction process. Then the agent evaluates received the encrypted messages and the substitution function.

The merchant store user identity (UID) and user certificate. Then the selected items will be determined by the user. Cost will be sent back to the user encrypted and hashed message containing merchant identity (MID), merchant certificate, total cost of selected items, merchant account, list of selected items and expiration date at merchant certificate. Evaluation function checks the validity of each sent items in this transaction.

When user receives message from ETC, he/she decrypts and controller agent evaluate it. The transaction identity (TID) will be stored. Then generates the payment information (PI) which contains transaction identity, cost of selected items (Ct), merchant account (Mac), and user account (Uac). It also generates order information which contains the following: Selected item (SI), transaction identity (TID) and cost of selected items (Ct). After that the OI, PI, time stamp, UID and certificate of user (Uc). All messages are signed digitally and hashed with encryption of ETC public key, then encrypted with a user secret key.

Merchant receives message from ETC decrypts message and controller agent evaluate and extracts information. When the merchant checks the information, it sends a message to the user. The merchant informs the user that the payment transaction was successfully containing transaction identity TID, time stamp Ts and cost of selected item Ct. All message is signed digitally and hashed with encryption of ETC public key, then encrypted with a user secret key.

The evaluation function for the expressions equality and encryption/decryption can be performed for all the sent element specifically for the time-stamp and for cost of selected items this can be done by applying the evaluation function on equality expression between two times, where first time denote the time stamp freshly generated earlier and by second time means the time-stamp which had been sent back from the merchant to the user. The function will ensure that the time-stamps by both transactions are the same, otherwise will terminate the process. The same way for the cost of selected items sent earlier by the user and the some are returned by the merchant for equality expression will ensure that both values in such bi-transaction are equal.

By ensuring that the encrypted set of messages and not disclosed to any other party, the privacy of the message is guaranteed, it is done by applying the evaluation function of a guard to encryption/decryption process. The past of that can be followed same as in step 1. By such evaluation we can proof that no intruder has interfered during the transaction between the user and merchant, which lead us to explicitly state that the authentication of both parties are guaranteed.

2- Transaction between cardholder and ETC

Figure 1.7 stated the transaction between cardholder and ETC by the following:

![Fig. 1.7. The transactions between cardholder and ETC](image)

The user receives the message from merchant, decrypt it, after that, controller agent evaluates the message. The user then checks if he accepts the cost of selected items. If yes, the identity of merchant and his/her identity will be checked. Then the selected item and the cost will be shown. If the user authenticates, the merchant identity, list of selected items, time stamp, user identity, merchant certificate and it's expiration date, and user certificate with its expiration date with encrypted will be sent.

All messages are signed digitally, and hashed with encryption of an ETC secret key then encrypted with a user a public key and send to ETC.

The main security properties; authentication and privacy can be proved in this transaction by applying the evaluation function on each of the sent elements, this can be explicit done as in previous steps

![Fig. 1.8. Transaction between merchant and ETC](image)

When ETC receives the message from user it decrypts it. Then controller agent evaluates the message. ETC
checks the certificate and identities the user and merchant with certificate and identity stored and expiration date for both. If agreement is achieved, it generates transaction identity (TID), store it and send with time stamp to user by all messages are signed digitally, and hashed with encryption of ETC public key then encrypted with a user a secret key.

The authentication and privacy can be proved by applying the evaluation function on each of the sent element, by that the user can evaluate the received element by equality expression to ensure that the time-stamp generated earlier by him/her is the same as the one received by ETC, the same for transaction identity. Proof explicitly can be done in previous steps.

3- Transaction between merchant and ETC

Figure 1.8 stated the transaction between merchant ETC by the following:

Merchant receives the message, decrypts it, controller agent evaluate message and merchant extracts information from it. Then, he checks merchant identity and user identity. If yes, he sends message contain OI, PI, MID, merchant certificate (Mc), UID, Uc and TID ETC. All messages are signed digitally, and hashed with encryption of merchant public key then encrypted with a user secret key. Explicitly same process of evaluation for proving authenticity and privacy properties can be followed as in earlier steps.

ETC receives message from payment gateway, decrypts it and evaluate by controller agent. It sends message to merchant contains transaction identity TID, time stamp Ts, list of selected items SI, cost of selected items Ct, merchant identity MID, and merchant certificate Mc. All messages are digitally singed and hashed.

4. TRANSACTION BETWEEN ETC AND PAYMENT GATEWAY

Figure 1.9 stated the transaction between ETC and payment gateway by the following:

ETC on receiving the message from merchant decrypts it and controller agent evaluates it. It extracts information from it. After that, it verifies the TID, MID, Mc, UID and Uc. If it approves, it sends UID, PI, Ts, list of selected items, MID, by encrypted and hashed message to payment gateway. Singed digitally and hashed with encryption of merchant public key then encrypted with ETC secret key.

Explicitly it can be followed as in previous steps, by applying the evaluation function, for validating each message carried in the transaction. At the other side, the payment gateway will evaluate the received message by evaluating each message and check it is valid or not to decide whether to proceed to next transaction or terminate the processes.

When payment receiving two messages from issuing bank and acquiring bank, it decrypts these messages and the controller agent evaluates them and checks the two equivalent messages. If agrees, it sends to ETC messages that response pay men containing, payment information PI, time stamp Ts, identity of user UID and identity of merchant MID. All messages are hashed and encrypted.

5. TRANSACTION BETWEEN PAYMENT GATEWAY AND ISSUING BANK

Figure 1.10 stated the transaction between payment gateway and issuing bank by the following:

The payment gateway receives the message from ETC, decrypts it and the controller agent evaluates the messages and after that extracts information. These includes Ts, PI (Ct, Uac, Mac, TID), UID, MID, with expiration date for both cardholder and merchant checks the certificate and identity for merchant and user. If exist, then he sends message include PI (Ct,Uac,Mac,TID), list of selected item, time stamp and identity for user and merchant to issuing bank. Where all messages are hashed and digitally signed.

The proof explicitly can be easily followed as in previous steps.

After issuing bank receives acknowledgment from acquiring for deposit of money to payment gateway, decrypt it and controller agent evaluates it then extracts information from message. It sends message about transfer fund containing time stamp Ts, transaction identity TID, user account Uac,
merchant account Mac and user identity UID and merchant identity MID. All messages are digitally signed and hashed by issuing encryption key.

The agent controller will evaluate all of the message elements by evaluation function and decide the validity for each of them. Already the agent controller has enough knowledge of each element of the transaction that makes the evaluation easier to apply. The evaluate function to validate and decide the correctness and completeness of the transaction. The evaluation can be explicitly followed as same as in step 1.

6. TRANSACTION BETWEEN ACQUIRING BANK AND PAYMENT GATEWAY

Figure 1.11 stated the transaction between acquiring bank and payment gateway by the following:

Acquiring bank receives message from issuing bank, decrypts it and takes information about transferring. Then adds to account of merchant the value of the cost of selected items. After that, it sends PI and time stamp to the payment gateway telling it about deposit value to his account from Uac about TID. The messages send hashed and digitally signed by acquiring bank public key.

![Diagram](image)

Fig. 1.11. The transaction between acquiring bank and payment gateway

7. TRANSACTION BETWEEN ISSUING BANK AND ACQUIRING BANK

Figure 1.12 stated the transaction between issuing bank and acquiring bank by the following:

Issuing bank receives the message request fund decrypts it then controller agent evaluate the message and extracts information by issuing bank. Then check if he founds the same account. He checks if it has sufficient money to pay for cost. If it agrees, it sends to acquiring bank PI and time stamp that all messages are digitally singed and hashing using issuing bank public key.

![Diagram](image)

Fig. 1.12. The transaction between issuing bank and acquiring bank

Acquiring bank deposits the amount of money (cost of selected items) then sends acknowledgment to the issuing bank telling it about deposit from it containing time stamp and payment information (PI) all message hashed and digitally signed by encryption key.

All remaining transactions between parties we believe to be followed explicitly as the above.

Figure 1.13 shows transaction steps among parties. Controller agent does not appear since it is implicit in the model which works concurrent with transaction.

The security in the current model starts from the transaction's beginning. The controller agent checks the validity of transaction and time stamp by ensuring that the time is valid and didn't change during the running of the process. It also checks the expiration date for certificate to ensure any part valid before date expiration this entire works parallel by controller agent. Using these steps, transaction will be reduced for each part where each part sends transaction to authenticate information. In transaction, wait until the response will be received about authenticate information and after that transaction will be completed. This shall lead to increase complexity and the time to complete transaction process but in current model controller agent works concurrent with transaction as arbitrator to checks information transaction. This shall lead to reduce transaction steps, complexity and time.

Controller agent also contains evaluation function, that evaluate message encrypted received by evaluation function. To decides its correctness and completeness of transaction this lead to approve privacy property.
1.5 Conclusion

In this paper, we build a suggested model for enhanced e-payment SET protocol (E-SET) informally for easy understanding. It characterizes system’s behavior more precisely and defines the system’s desired properties precisely. It is also applied for each transaction between parties. Security problems by adding control agent work as arbitrator was solved.

The controller agent checks the validity of transaction and time stamp by ensuring that the time is valid and did not change during the running of the process, and checked the expiration date for certificate to ensure any part valid before date expiration this entire works parallel by controller agent. It also contains evaluation function, that evaluate message encrypted received by evaluation function that decided its correctness and completeness of transaction this lead to approve privacy property.

The authentication problem is solved by using evaluation function done by control agent to verify authentication properties by time-stamp, hash function, identification and digital signature. Its work as arbitrator that allows transacting after verifies the authentication and judgment. This shall increase authentication and decrease non-repudiation.

The privacy problem solved using public and private key and adds special value shows through evaluation function in control agent. It checks if any intruder accesses, the content of transaction information stops operation.

REFERENCES


