

IMPLEMENTATION OF PAYMENT GATEWAY IN AN E-COMMERCE WEBSITE USING SET PROTOCOL

Project report submitted in partial fulfillment of the requirement for the degree
of Bachelor of Technology

In

Computer Science and Engineering

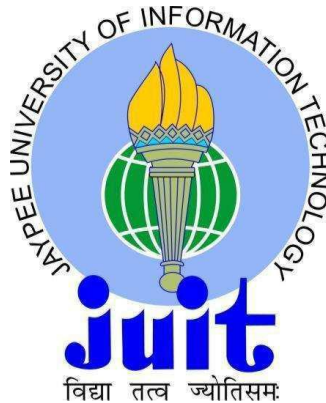
By

Vivek Guleria (151388)

Under the supervision of

Prof. S.P. Ghrrera

To



Department of Computer Science & Engineering and Information Technology

**Jaypee University of Information Technology Wagnaghat, Solan-173234,
Himachal Pradesh**

Candidate's Declaration

I hereby declare that the work presented in this report entitled “ Implementation of payment gateway in an E-commerce website using SET Protocol” in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology Waknaghat is an authentic record of my own work carried out over a period from August 2018 to December 2018 under the supervision of (Prof. S.P. Ghrera) (HOD Department of Computer Science & Engineering and Information Technology).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Vivek Guleria, 151388

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

(Supervisor Signature)

Prof.S.P.Ghrera

Head of department (CSE)

Computer Science And Engineering Department

Dated:

ACKNOWLEDGEMENT

I am using this opportunity to express my gratitude to everyone who supported me throughout the course of this project.

I am thankful for their aspiring guidance, invaluable constructive criticism and friendly advice during the project work. I am sincerely grateful to them for sharing their truthful and illuminating views on a number of issues related to the project.

I express my warm thanks to my project guide **Prof. S.P. Ghreera** from the Computer Science Department for their continuous support and guidance.

I would also like to thank the lab in-charge for their cooperation and all the people who provided me with the facilities being required and conducive conditions for my project

Vivek Guleria

TABLE OF CONTENTS

CONTENT	PAGE NO.
	iii
ACKNOWLEDGMENT	v
LIST OF ABBREVIATIONS	vi
LIST OF FIGURES	vii
LIST OF GRAPHS	viii
LIST OF TABLES	
ABSTRACT	ix
CHAPTER 1 INTRODUCTION	
Payment Gateway in E-commerce	
1.1 Introduction	x
1.1.1 What is ecommerce	x
1.1.2 Security in ecommerce	x
1.1.3 SET protocol	x
1.1.4 Encryption in ecommerce	x
1.1.5 SSL certificate	x
1.1.6 Payment Gateway	x
1.2 Problem Statement	xi
1.3 Objectives	xii
1.3.1 Confidentiality	xii
1.3.2 Integrity	xii
1.3.3 Availability	xii
1.3.4 Authentication	xii
1. 3.5 Non Repudation	xii
1.4 Methodology	xiii
CHAPTER 2 LITERATURE SURVEY	xiv
CHAPTER 3 SYSTEM DEVELOPMENT	xxviii
3.1 SET Specifications	xxviii
CHAPTER 4 ALGORITHMS	xxxiii
CHAPTER 5 TSET PLAN	xxxvi
CHAPTER 6 RESULTS AND PERFORMANCE ANALYSIS	xli
CHAPTER 7 CONCLUSIONS	xliv

List of Abbreviations

C :	Cardholder
M :	Merchant
PG :	Payment Gateway
IB :	Issuer Bank or Cardholder Bank
CA:	Certificate authority
Vshop :	Virtual Shopping Site
PAN:	Card Number
CVV2:	Card Verification Value or Crypto (three digits)
ExD:	Expiry date of the card
OI:	Order Information
PI:	Payment Instructions
OIMD:	OI Message Digest
PIMD:	PI Message Digest
POMD:	Payment Order Message Digest
K:	Symmetric key generated randomly
Kum:	Public key of merchant
Kupg:	Public key of payment gateway
Kuis:	Public key of issuer bank
Krm:	Private key of merchant
Krpg:	Private key of payment gateway
Kris:	Private key of issuer bank
S:	Sign
E:	Encrypt
D:	Decrypt
V:	Verify signature
H:	Hash
:	Concatenation
#:	Disconnect
Eq:	Equal

LIST OF FIGURES

S.No	Title	Page
1.	Figure 1: Entities in a Secure Electronic Transaction (SET) system	xiv
2.	Figure2: Icons used for items representation	xvi
3.	Figure3: Merchant registration is the same as cardholder registration.	xviii
4.	Figure4: : Dual signature	xviii
5.	Figure5: Purchase Request	xix
6.	Figure6: Authorization request and PI verification	xix
7.	Figure7: Authorization response and capture token	xx

S.No	Title	Page
8.	Figure 8: Capture request and capture token	xxii
9.	Figure9: Capture response	xxiii
10.	Figure10: Data element encryption.	xxv
11.	Figure11: : Homepage	xxxvii
12.	Figure12: Search Page	xxxvii
13.	Figure14: Product details page	xxxviii
14.	Figure15: Shopping cart page	xl

LIST OF GRAPHS

S no.	Title	Page
1.	Eexecution Time Graph	xliii
2.	No. of Concurrent users	xliii
3.	Payment transaction time in single-threaded model	xliii
4.	A comparison of single-threaded and multi-threaded model	xliii
5.	Single-threaded model on the payment transaction time	xliii

ABSTRACT

Secure Electronic Transaction (SET) protocol was developed by Visa and MasterCard as a method to protect the security of payment card transactions over open networks, but it failed to be widely promoted.

Based on our research about Secure Electronic Transaction (SET) protocol, we designed and implemented a suite of e-commerce system which was improved from Secure Electronic Transaction (SET) protocol.

Our main contributions are: firstly, apply the proper network technologies of thin client to build the E-commerce model, secondly, develop a method of database encryption to protect the security of sensitive transaction information, thirdly, give support to debit card payment; also we change the payment process of transaction flow for the aim of practicability and atomicity.

Chapter-1 INTRODUCTION

1.1 Introduction

E-commerce is the way of buying or selling of products over the Internet. Electronic commerce uses various technologies such as internet marketing. Electronic funds transfer, mobile commerce, supply chain management, online transaction processing, inventory management systems, and automated data collection systems.

Modern e-commerce mainly makes the use the World Wide Web for at-least single part of the transaction's life cycle however it also use other technologies such as email. Typical electronic commerce transactions include the purchase of online items (such as Amazon services) and also music purchase (music download in the form of digital distribution such as iTunes Store), and to a less extent, customized and personalized online liquor store services.[1] There are three major fields of e-commerce: electric markets, and online auctions ,online retailing. Electronic commerce is basically supported by electronic business.

Secure Electronic Transaction (SET) is a protocol or system which ensures integrity or security of electronic transactions held using credit cards. It is not some system that enables payment but it is a security protocol which is applied on those payments. SET uses various encryption and hashing techniques to secure online payments carried through credit cards. SET protocol was developed and supported by major organizations like MasterCard and Visa and Netscape which provided technology of Secure Socket Layer (SSL) and Microsoft which provides its secure transaction technology (SST).

SET protocol regulates unveiling of credit card details to merchants thus keeping thieves hackers at bay. SET protocol allows Certification Authorities for make use of standard digital certificates like e.g. X.509 Certificate.

1.2 Problem Statement

Is ecommerce safe?

A large number of consumers adopt online shopping; in ecommerce security is a major priority for both consumer and merchants alike. Customers must always verify the merchants with whom transactions are held whether he is legal or not before entering to any financial transaction, while merchant can have multiple security layers to keep valuable data confidential.

What is cryptography in ecommerce?

The cryptography is a method of encrypting data into an unreadable and invisible format, called as cipher text termed as cryptography techniques. Mainly used for the data protection, e-mails or payment information, only for those who have a secure key to decrypt the data or message into readable plain text?

What is SET protocol in ecommerce?

Secure electronic transaction protocol (SET) is a standard protocol in ecommerce which includes three-way transaction between the merchant, user and bank using standard protocols.

What is encryption in ecommerce?

Encryption is a way of encoding data, to ensure that the user data can be securely held over the internet. This is one of the effective ways in reducing ecommerce security issues to secure the data integrity.

What is an SSL certificate?

SSL certificate make use of small files of data to safeguard cryptographic key to company's file. On the web server when an SSL certificate is installed on a web it makes the use of specific protocols to provide a reliable connection from the server side to a browser.

What is online credit card fraud?

Internet or online transactions using credit card fraud uses hacking, phishing attacks or malware to copy or exchange financial data or information for fake transactions.

What is a payment gateway?

Payment gateway is an ecommerce platform or application which enables merchants to authenticate credit card payments done by various customers over internet for online purchase.

1.3 Objectives

- **Confidentiality**: Ensures that the information is accessible only to those who have the valid authenticity.
- **Integrity**: Ensures that there is no change in data or information during any transaction held between merchant and customers and information send by both is received completely with accuracy.
- **Availability**: Allows accessibility of information to authorized users whenever required.
- **Checking authenticity (authentication)**: Involves verification of user passwords or identity or personal identification numbers (PINs) and many others.
- **Non-Repudiation**: Ensures that transaction must occur completely without any halt in between.
- **Authorization**: Both merchant and customer should have digital certificates for verification of each other.

1.4 Methodology

Secure Electronic Transaction (SET) protocol was widely practised in late 1990's as the credit card payment standard over open networks. It was developed to satisfy business requirements but failed to win market share. Thus, we have much work to do with secure electronic transaction protocol. We can modify the Secure Electronic transaction protocol as following:

We use the web browser/server technology with the ActiveX control to reduce the burden on the client side and to help cardholder to manage her security information.

We also design method to support both encryption of database or any query over encrypted database. This method was used in our solution to ensure the security of information of the sensitive transaction data.

We change the process of payments of transaction flow to ensure the atomicity of goods and certified delivery atomicity.

To support the use of debit card for more cardholders we add the choice of inputting or not inputting or not inputting (PIN) of debit card, that is, if cardholder use debit card she can choose to input the PIN.

Chapter-2 LITERATURE SURVEY

SECTION 1.

The fast development of web has changed our very life, and it also no doubt made a deep influence towards the progress in civilization. Against this big background, a new thing named online payment get up huge waves in the ocean of internet. It has changed big and efficient ways towards the e-commerce. However, these ways are not as safe as we thought, and they are risky and pitted with peril.

In order to get rid of the growing hacking concerns and change the way for this growth of online payment on the internet. RUPAY, MasterCard, VISA etc and some other leading companies created this Electronic Transaction (SET). “On February 1st, 1996 these companies announced a technical standard for safeguarding the payment card purchases made over open networks. This standard is called the Secure Electronic Transaction (SET) specification.”

Our secure Transaction setup has the following things (see figure 1). The definitions of these entities and the relationship between them are defined in [1], [2], [3].

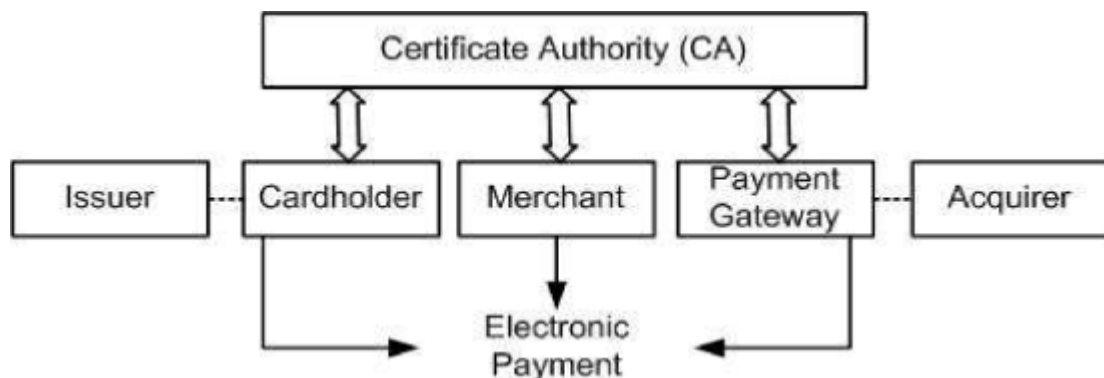


Figure 1: Entities in a Secure Electronic Transaction (SET) system

It was developed to satisfy business requirements but failed to win market share. Thus, we have much work to do with Secure Electronic Transaction (SET) protocol. In this paper we improved the Secure Electronic Transaction (SET) protocol as following:

We use the web browser/server technology with the ActiveX control to reduce the burden on the client side and to help cardholder to manage her security information.

We design a method to support database encryption and query over encrypted database. This method was used in our solution to ensure the information security of the sensitive transaction data.

Improvisation of payment style is to guarantee that goods atomicity of certified delivery unity.

In order to support the use of debit card for more cardholders we add the choice of inputting or not inputting PIN of debit card, that is, if cardholder use debit card she can choose to input the PIN.

The specifications of the rest of the paper are as follows. We start off with the specification of our suggested e-commerce model in Section 2. In section 3, we define the essential technical implementation detail of the system. We conclude with a summary and directions for future work in Section 4.

SECTION II.

Specification of Our Suggested E-commerce Model:

For the convenience of written expression, we have used some notational conventions in this paper as mentioned before in the abbreviations page.

We also created some icons to represent a certain item as following:









- : Data Item
- : Algorithm
- : Data Operation
- : Local Disk
- : Symmetric Key
- : Public or Private Key
- : Certificate
- : Random Source

Figure 2: Icons used for items representation

Observe that throughout the text I use female pronouns to refer to cardholders.

Our Secure Electronic Transaction (SET) transaction flow includes:

Cardholder, payment gateway and merchant should register and get certificates from certificate authority (CA) before both of them involve in the Secure Electronic Transaction (SET). Cardholder browses for items and selects items to be purchased from a merchant (V Shop). Cardholder gets an order which contains the list of items and the price.

Cardholder receives the order information and then chooses payment method of Secure Electronic Transaction (SET). After enters the payment instructions cardholder creates a dual signature of the PI and OI, then sends these information to merchant. Merchant verifies the order and transmits encrypted authorization request and encrypted PI to payment gateway (VBR). After payment gateway verifies cardholder's payment instructions, it transmits encrypted authentication response and send capture token to the merchant. Merchant verifies authentication response and then sends capture token to cardholder. Cardholder verifies the capture token. Merchant ships the goods to cardholder; if buyer satisfies with the products she should send encrypted information and capture token to payment gateway within stipulated time. Payment gateway verifies capture request and capture token, ensures consistency between capture request and the capture token and then sends capture request through a financial network to cardholder's financial institution to transfer the money from cardholder's account to merchant's account, or else the transaction will be canceled.

Finally, payment gateway transfers the captured response to the vendor. Although browse, product selection, ordering, selection of payment and shipping of goods are not included in the Secure Electronic Transaction (SET) protocol we still design and implement the whole phases to show an entire process of secure electronic transaction (SET) protocol in our project. In the following, we only describe the payment process details of Secure Electronic Transaction (SET) protocol.

A. Cardholder Registration:

Cardholder logs in VBR and select certificate registration, and then she is redirected to Certificate Authority (CA). In Certificate Authority (CA), cardholder needs to fill in the registration form (including Country Name, Province Name, Location Name, Common Name, Organization Name and Organization Name Unit etc.). After finish of the registration form she click submit button to send the form. (Submit button activates the ActiveX control at cardholder's browser to generate one pair of keys (public key K_{Uc} and private key K_{Rc}) randomly, K_{Rc} is stored local and K_{Uc} along with registration form are sent to Certificate Authority (CA), see figure 3)

Certificate Authority (CA) generates certificate, keep a copy and offer the link of downloading certificate to cardholder. Cardholder can download her certificate into a folder and she can use IE to help her to manage the certificate.

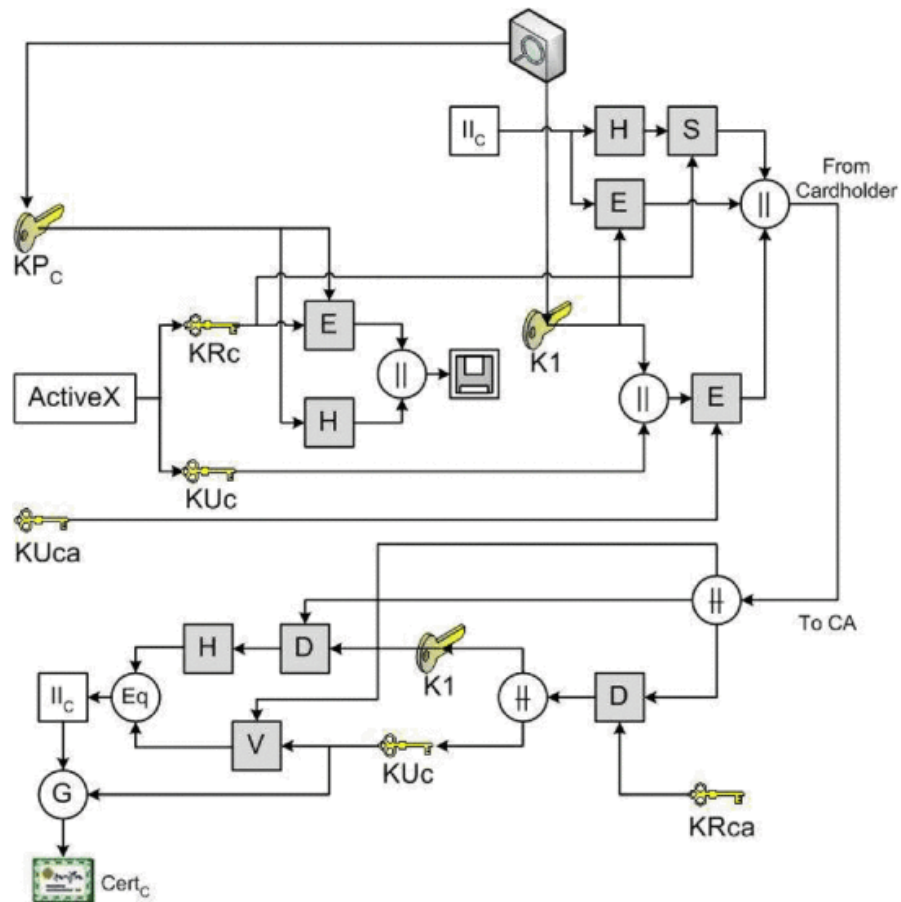


Figure 3: Merchant registration is the same as cardholder registration.

B. Purchase Request

Cardholder generates OI and encrypted PI in dual signature (see figure 4), then prepares purchase request for the vendor, as shown in figure 5. Merchant verify the cardholder dual signature and OI. After the OI has been processed merchant sends a response to cardholder.

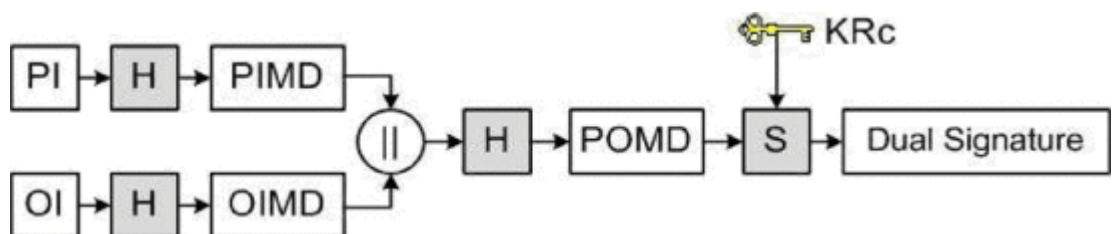


Figure 4: Dual signature

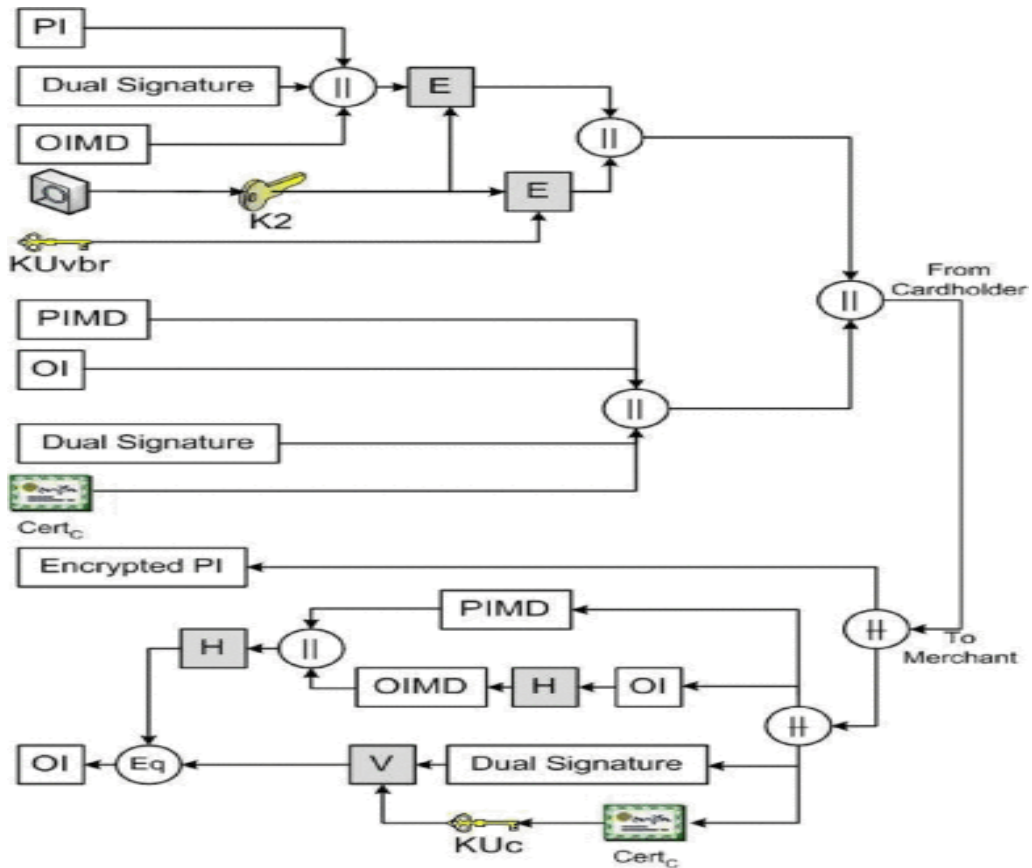


Figure 5: Purchase Request

C. Payment Authorization

Merchant signs authorization request and encrypts authorization request using a randomly generated symmetric key, and this key is then encrypted using the public key of payment gateway.

Merchant transfers encrypted authorization request and encrypted PI to the payment gateway (Encrypted PI is from the cardholder). Payment gateway verifies the cardholder's dual signature and PI, as shown in figure 6.

After the PI was processed payment gateway transfer encrypted authorization response and capture token to vendor. Vendor decrypts and verifies authentication response and sends token to cardholder, as shown in (figure 7). Merchant ships the goods to cardholder.

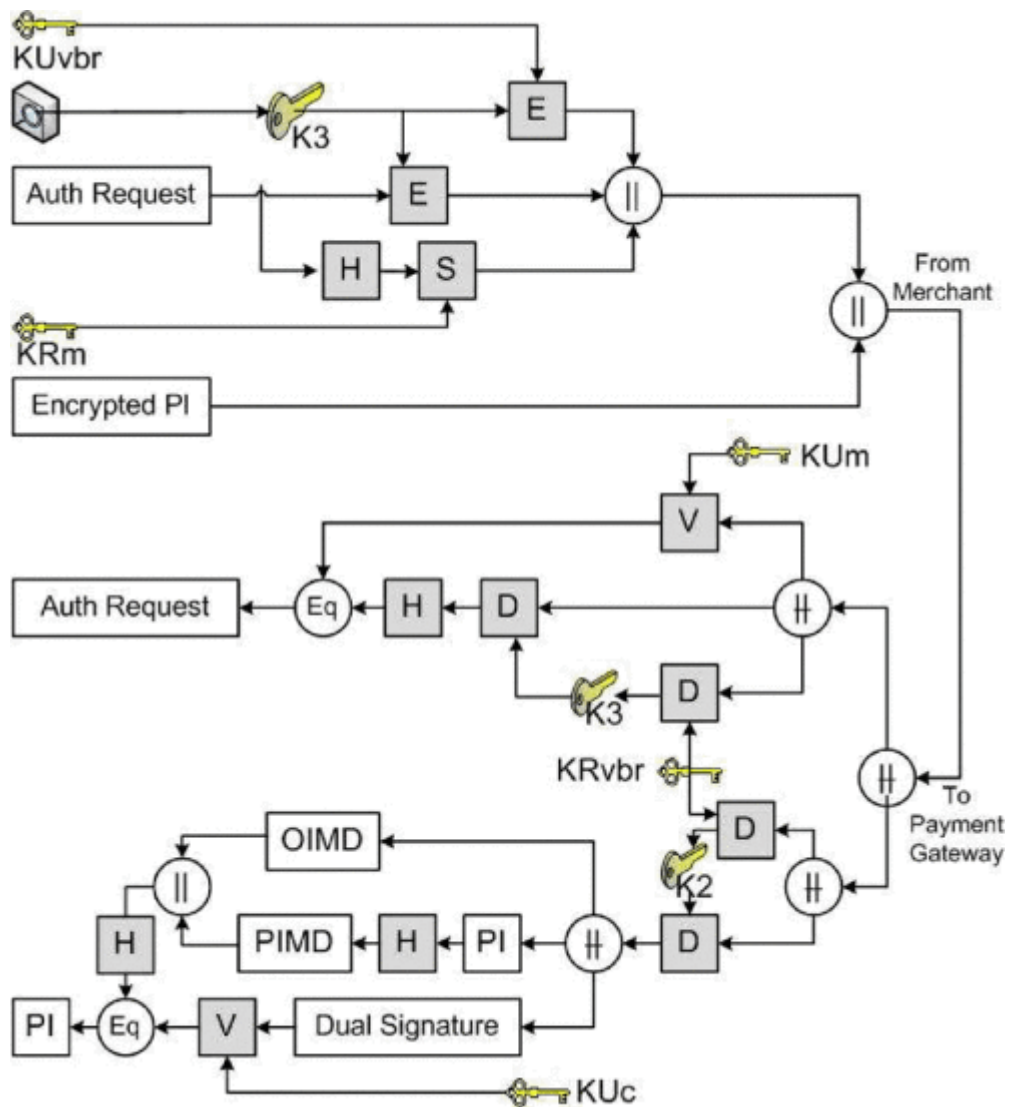


Figure 6: Authorization request and PI verification

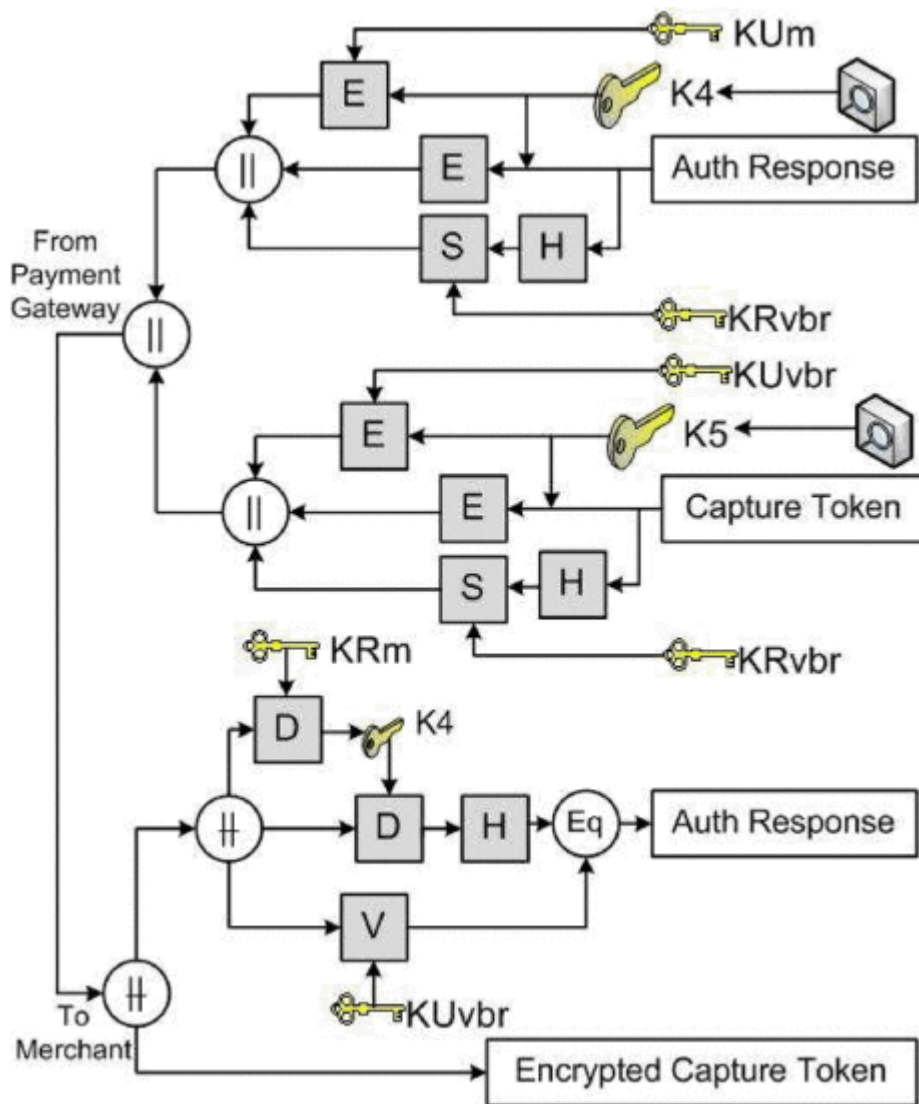


Figure 7: Authorization response and capture token

D. Payment Capture

If buyer satisfies with the products she should send encrypted capture token and capture request to payment gateway within stipulated time. If cardholder forgets to submit the system will process automatically. Payment gateway verifies capture request and capture token, results consistency between capture token and the capture request, as shown in figure 8.

Payment gateway transfer capture request using a financial network to buyer's financial institution to transfer money from buyer's account to merchant's account. Payment gateway transfer encrypted capture response to merchant, as shown in figure 9. Vendor verifies received response.

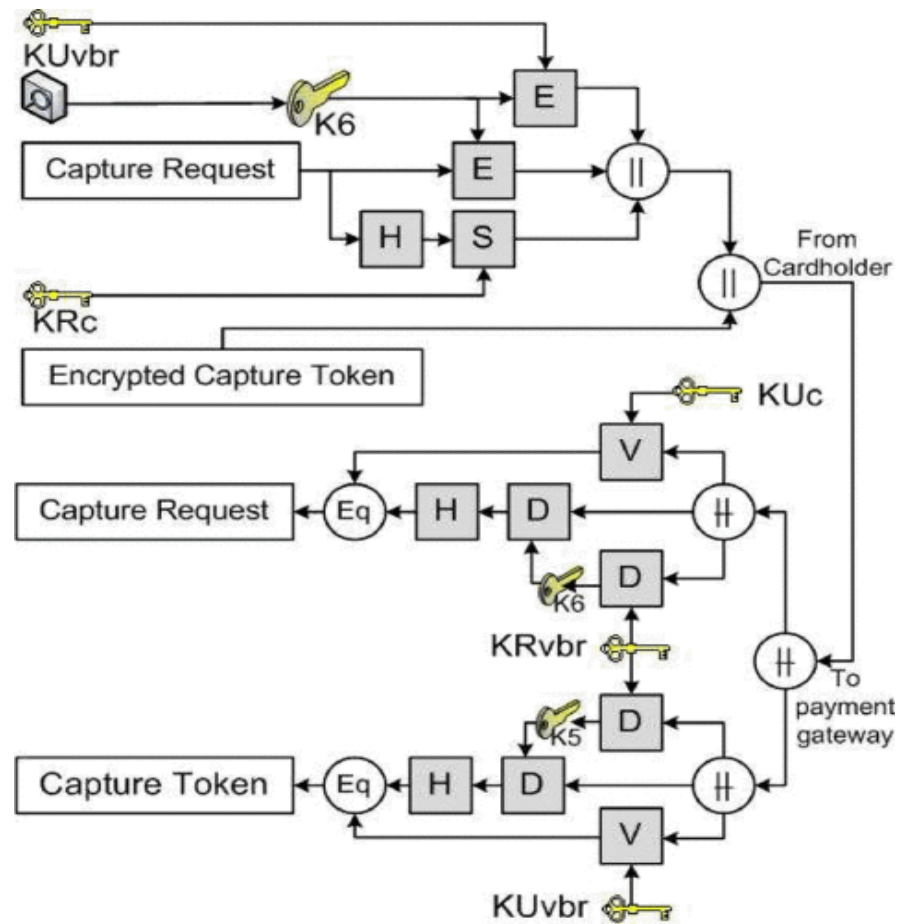


Figure 8: Capture request and Capture token

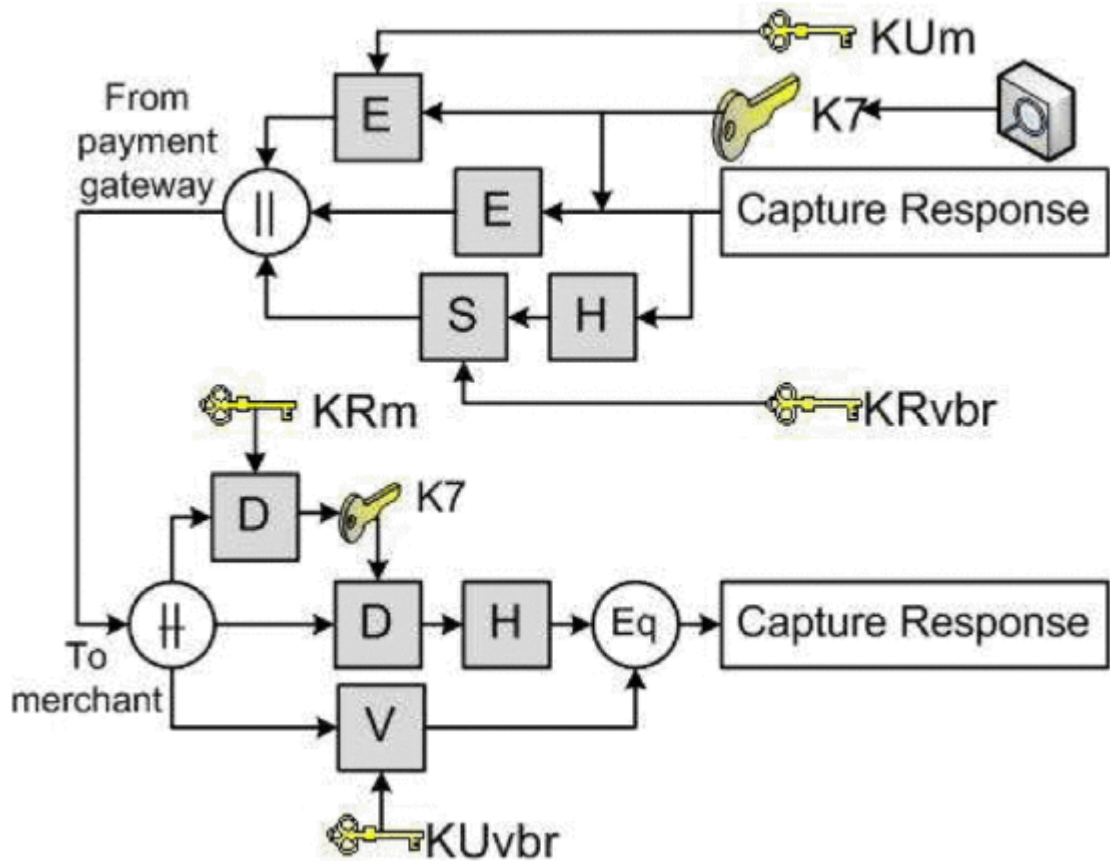


Figure 9: Capture response

SECTION III.

Implementation:

There are four key techniques in the course of development of our e-commerce system. We use ActiveX security control to deal with all cryptographic operation for cardholder. To protect the sensitive information of cardholder and merchant we find a way to encrypt query and database over encrypted database. We exchange the way of payment transaction flow to guarantee certified delivery atomicity and better atomicity, two important properties of e-commerce. In order to setup a Certificate Authority (CA) to give registration for cardholder and merchant, we use Open SSL to develop a light weight Certificate Authority (CA).

A. ActiveX Security Control

We use ActiveX security control to deal with the data encryption and data interaction, which makes us to realize two goals: help the cardholder to control data transfer between different websites and protect the security between client and server. We realize the following functions in our ActiveX control:

Protect the use of private key of cardholder: As shown in Figure 2, the private key KRc of cardholder is protected by KPc. When anyone wants to use cardholder's private key KRc ActiveX control will ask her to enter KPc to make sure the user is legitimate (KPc is the symmetric key used to protect cardholder's private key KRc, see figure 3).

Cryptographic operation: ActiveX control does all operation of encryption, decryption, signature and verification for the cardholder.

B. Protect Sensitive Data

The transaction information in Secure Electronic Transaction (SET) include a lot of sensitive data, such as, buyer's identification information, product detail and credit card number etc., this data is stored in the database of bank and merchants. To protect the useful data, encrypting the data is an important technique [11]. With data is encrypted in database, [7], [12], [13], [14] shows some solutions of query on encrypted database.

We refer to the solution in [7] to design and implement an improved way to encrypt database and query in the encrypted database. In our solution, before sensitive data is stored in database it will be encrypted. Whenever the user has a question or query, then query is converted to one or more messages that are transferred to the database. When receiving the message(s), the databases search the best encrypted data elements and returns to the user. Finally, the users decrypt the received data elements. It verifies that the plain text of the useful data only can be seen by the user and the useful data in the network or database will all be encrypted.

We review the database represented by Table T (we assume that the confidential data is stored in T) and store the database-encrypted Table T' and discuss the queries made in T'. Suppose T has n rows and m columns. T_{ij} is a data element at the intersection of row i and column j of table T, the result of T_{ij} encoding is T'_{ij} . We assume that each TIME data element in a simple text table is an L1-bit string, and when encrypted, a random L2-bit

string will be added to plain text. Therefore, the input of the encryption algorithm is the string of bits L_0 , where $L_0=L_1+L_2$. Our method is based on symmetric encryption (see Figure 9), so the output of the encryption algorithm also consists of L_0 -bit strings. For convenience, we use the following classification conventions (see Figure 9): SE: Symmetric Encryption, H: Hash function, K_1 , K_2 : Symmetric Keys.

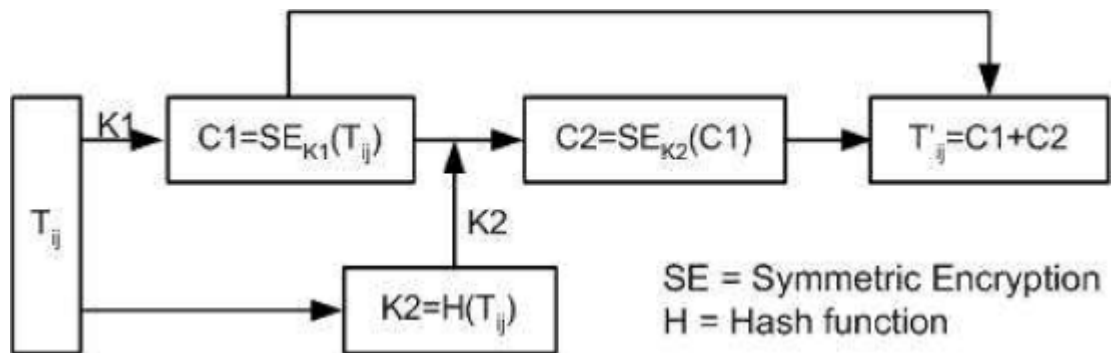


Figure 10: Encrypt data element T_{ij}

The grain size in our encrypted database is the grain size of the data element. Figure 9 shows the encryption of each T_{ij} sensitive data item. For each T_{ij} data element, the encrypted $T'_{ij}=C_1+C_2=SE_{K_1}(T_{ij})+SE_{H(T_{ij})}(SE_{K_1}(T_{ij}))$ element consists of two parts. A Part one $C_1=SE_{K_1}(T_{ij})$ is a simple symmetric T_{ij} encryption using SEC block encryption and K_1 symmetric key; Part two $C_2=SE_{H(T_{ij})}(SE_{K_1}(T_{ij}))$ - is a checksum, which, together with the first part, allows you to check whether the item meets the order condition.

The question remains: how to set an encrypted table T' . $T'_{1s}...T'_{ws}$ (Table T' has in in $T_1s...T_ws=C_1+C_2$) corresponds to $SE_v(C_1)$ in Table T' . If the equation is saved, the database returns C_1 from $T_{x1}... T_{xN}(1 \leq x \leq N \leq w)$ to the user. The user decrypts each received element with the symmetric key K_1 and rejects the endpoint of the plain text bit L_2 .

The advantage of our method is as below:

- We use symmetric encryption and hash function because their operating efficiency is higher than other cryptographic techniques.
- Our database is encrypted at element level, this means that we can only encrypt sensitive data not all data in the database.
- We append a random string to every sensitive data element to make the cipher text different, it means that if there is two or more plain text in the database is the same the cipher text is different, or when you input the same plain text at different time the cipher text is also different. This makes the database intruder much more difficult to break the database.
- We do not need to decrypt before we query on the encrypted database.

B. Atomicity

Product atomicity and certified atomicity of delivery are important properties that any e-commerce protocol must meet. Product atomicity means that when we pay, we must receive the product, and when we receive the product, we must pay for it. A certified delivery address means that the trader and the customer want to prove the exact content of the delivered goods [6].

In the original Secure Electronic Transaction (SET) protocol, once the cardholder's orders have been processed, the merchant may request a token capture and capture at the payment gateway to receive payment for the goods before the cardholder receives the goods [3]. This means that the Secured Electronic Transactions Protocol (SET) does not take into account the atomicity of the goods and the atomicity of the certified delivery. To ensure this, we have made changes to the Secure Electronic Transactions (SET) payment process. As part of the payment authorization process, we send the cardholder a merchant capture ID. Then, during the payment interception process, only after the cardholder is satisfied with the goods does he send the interception request and the interception token to the payment portal. If you do not allow the cardholder to forget or not to send these instructions, we will specify a fixed period within which the cardholder and the merchant

will be able to solve the problem with the goods, but after that the system will be processed automatically.

D. Use Open SSL to Setup Certificate Authority (CA)

Open SSL is a powerful secure open library for secure communication, and it has the excellent cross-platform performance [9]. We use Open SSL to develop a light weight Certificate Authority (CA). This light weight Certificate Authority (CA) can only issues certificate. There are four major steps when we use Open SSL to generate certificate:

- 1) Use V c8 c 1 compiler of Visual Studio to compile the Open SSL in the environment t of Windows.
- 2) Use a 1024 bits RSA algorithm which was implemented by us to produce a pair of keys, and then put the key pair into EVP _ PKEY of Open SSL for future generation of certificate. (Open SSL support us to put public key into certificate, this is good for us to control the Cipher Strength of the Certificate Authority (CA))
- 3) Use request to generate certificate request file which includes the public key and the user's information, then use it to generate certificate for the user.
- 4) Generate certificate according to the certificate request.

For the above-mentioned techniques we implement our e-commerce system. This system is used for our teaching, as it is just a teaching system, we've only developed a light weight CA, it does not have some function, such as certificate revocation, certificate backup etc.

The sensitive data can be encrypted before it is stored in the database and the query can be executed over the encrypted database, but our method does not support Fuzzy Query and aggregate functions of SQL.

Chapter-3 SYSTEM DEVELOPMENT

This is a systemised industry wide protocol principals and specification delegate to ensure the security of payment transactions and verifies the parities which are involved in any type of transaction using Internet. MasterCard and Visa developed some standard of SET protocol with cooperation from essential software companies such as Netscape, RSA, Microsoft, and other.

Using SET protocol we can provide the trust required by consumer. The protocol use digital certificates and cryptography algorithms to ensure confidentiality of the information verifies merchants, banks and cardholders during SET transaction and ensure payment integrity.

SET Specifications:

- SET make the use of RSA data security public key cryptography algorithm to decrypt and encrypt transaction messages along with the help of dual signature and digital certificates to verify all the parties to the validation and transaction that information can not been tampered with.
- With the help of digital certificates SET makes online transactions even safer to verify that both merchants and consumers are authenticated to accept and use Visa cards. It's equivalent for both consumer and merchant that consumer is asking for a Visa decal in a store window of vendor, and also vendor verifies the signature of buyer on the back of a Visa card.
- To protect the privacy of financial and personal information SET incorporates the use of public key cryptography. As a result, by using SET all the information related to consumer's payment is protected from financial institution. The information is not visible or read by merchant during payment transaction.
- With use of SET, cardholders can verify that the merchant with whom he is dealing is permissible through vendor digital certificate SET software

automatically verifies that both vendor and financial institution have trusted relationship through certificate. Therefore SET provides confidence to consumer that their payment transactions are handled with legal Visa promise.

Advantages of SET Protocol

- 1) Various standards and formal methods are used to ensure the authenticity of data ,data integrity ,confidentiality, these may help to build trust between both merchant and customer
- 2) By using SET payment gateway public key SET prevents vendors from seeing the payment information of customer, customer payment information is not visible or read by the vendor during SET transactions.
- 3) Also too ensure the vendors information privacy; SET avoids the payment gateway from seeing the order information.

Drawbacks of SET

- 1) For handling the SET transactions customer must install additional software.
- 2) User or buyer should have a valid digital certificate.
- 3) Implementation of SET is costlier than that of SSL for vendors.
- 4) Implementing the system to work according to SET is very complicated as compare to work with SSL
- 5) To manage payment gateways business banks must hire companies, or install gateway systems by themselves.
- 6) Along with concept of security in user mind, SET also has some security drawbacks. As a other type of the SET protocol, the vendor have access to see the customer payment information same as SSL.
- 7) Due to complex cryptographic mechanisms of SET the transactions speed may reduce.

8) The given algorithm can be used for the project.

CAs before beginning with any transaction

Categorically

Customer gets credit card acc. number

Selected Category then

Adding CategoryId

Choose the SubcatID also

Select list of items of selection category

If Selected (Item)

Then also

{Showing detail about selected item}

Buying Phase is started

If {you want to purchase the selected product}

Then also select

{Add this to order database}

or

{Going previously to category}

Ordering phase is started

If selection of add form of order

Then

AddingToOrder(SubCatId)

It go to

Ordering form and also inserting required fields which includes CR card No,
Expiry date also

and mobile , Address

Select

{Submitted}

{Encrypt}

or

{Carry on shopping}

or

Back}

Authenticate

If selected enter

Go to authentication page

{

if credit card data is true

Then print

"This customer has been verified from Bank."

or

"This customer is unauthorized from Bank. }

if verified

Transfer Money

Decryption of credit card number

Then do

Request for payment via gateway

Response is then. Redirect("Payment Gateway")

Do

Request for payment to issuer }

Then

Payment transfer to vendor account

View

"Payment is transfered to vendor bank

last

Chapter-4 Algorithms

Here we combine Purchase request and Payment authorization, comprises of six-step protocol.

Initial Shopping -Agreement

The merchant and the cardholder agree on OrderDesc and PurchAmt, this stage of the agreement between the two parties is called the SET startup process because this programming guide is not part of the SET and takes place immediately before it.

Purchase Initialization Request

The cardholder sends the merchant a freshness challenge (Chall C) and a local transaction identifier (LID M).

1: C! M: LID M; Chall C

Purchase Initialization Response

The seller responds with an authorized message containing a perishable ability call (M call) and generates a Nonce, which serves as the world's only transaction identifier 1 XID. Instead, the public key certificate is issued to the payment platform, which is also defined by the bank of the seller and the card brand. In our opinion, a certificate is a message containing the name and public key of the agent, signed by the primary certifying authority.

2: M! C: SignpriSKM(LID M; XID; Chall C; Chall M)

Purchase Request

This is a very important and interesting message from SET. The advertiser and payment portal should understand the cardholder's answer to the purchase, although each of them has only partial information: The advertiser has no information about the card and the payment portal also does not know what is being bought. To achieve this goal, SET uses

the double signature method: In this cardholder you authorize the association of labels to make payments.

Instructions (PIData) and customer order information (OIData). It combines these two elements with PAN Data card data, including PAN and other confidential numbers, Cards Secret and PANS Secret used for verification. The consumer then encrypts everything with the public key of the payment gateway, the pub. It transmits them to the seller, including information about orders and payments.

Instructions. As a result, a lot of information is copied so that different parties can authenticate quick access labels.

3: C! M: PIDualSign; OIDualSign

Here, C has computed

HOD = Hash (OrderDesc; PurchAmt)

PIHead = LID M; XID; HOD; PurchAmt;M;

Hash (XID; CardSecret)

OIData = XID; Chall C; HOD; Chall M

PANData = PAN;PANSecret

PIData = PIHead;PANData

PIDualSign = SignpriSKC(Hash(PIData); Hash(OIData));

CryptpubEK P (PIHead; Hash (OIData);PANData)

OIDualSign = OIData; Hash (PIData)

An authenticated purchase request does not contain a combination of hash and digital signature. Check the user for compliance with the PANS Secret hash value. This does not guarantee an electronic signature yet, but it is even more effective than sending the card data to the seller.

Authorization Request

The merchant requests confirmation of payment processing through the payment gateway after receiving the purchase request from the customer. First, merchants check the double signature using the hash of the payment instructions. It also checks the order data of the

cardholders. Use the payment instructions (which you can read) and link them to the transaction identifiers and the hash value of the order information. It checks and encrypts it with the gateway public key.

4: M ! P : CryptpubEK P (SignpriSKM(LID M; XID; Hash(OIData);HOD; PIDualSign))

Authorization Response

In this double signature, the payment portal checks with the order form, the double signature checks whether the seller and the cardholder agree with the purchase amount and order description, comparing the hash value and finally the validity of the cardholder's secret account data with the cardholder's certificate. If he is satisfied, he confirms the verification with the merchant by signing a detailed message containing the purchase amount and transaction identifier.

5: P! M: CryptpubEKM(SignpriSK P (LID M; XID; PurchAmt; authCode))

Purchase Response

Then similar signed message is sent by the merchant to cardholder. This message contains hash value of the purchase amount, which must be verified by the cardholder.

6: M! C: SignpriSKM(LID M; XID; Chall C; Hash(PurchAmt))

In this model, we offer signed and unsigned versions of authorization requests, authorization responses and purchase requests.

Chapter-5 Test Plan

E-Commerce Testing Checklist

The following are important segments and examples of e-commerce site testing.

#1) Homepage – Hero Image:

The following few things are to be test:

- Auto scrolling?
- Yes, at what interval in which image is refreshed?
- When customer hovers over it, scroll to the next one?
- Hovered on effect?
- Clicked on effect?
- If true, it will take you to the right deal and right page?
- Is rest of content seen?
- Rendering the same way in different screen resolutions and different browsers?

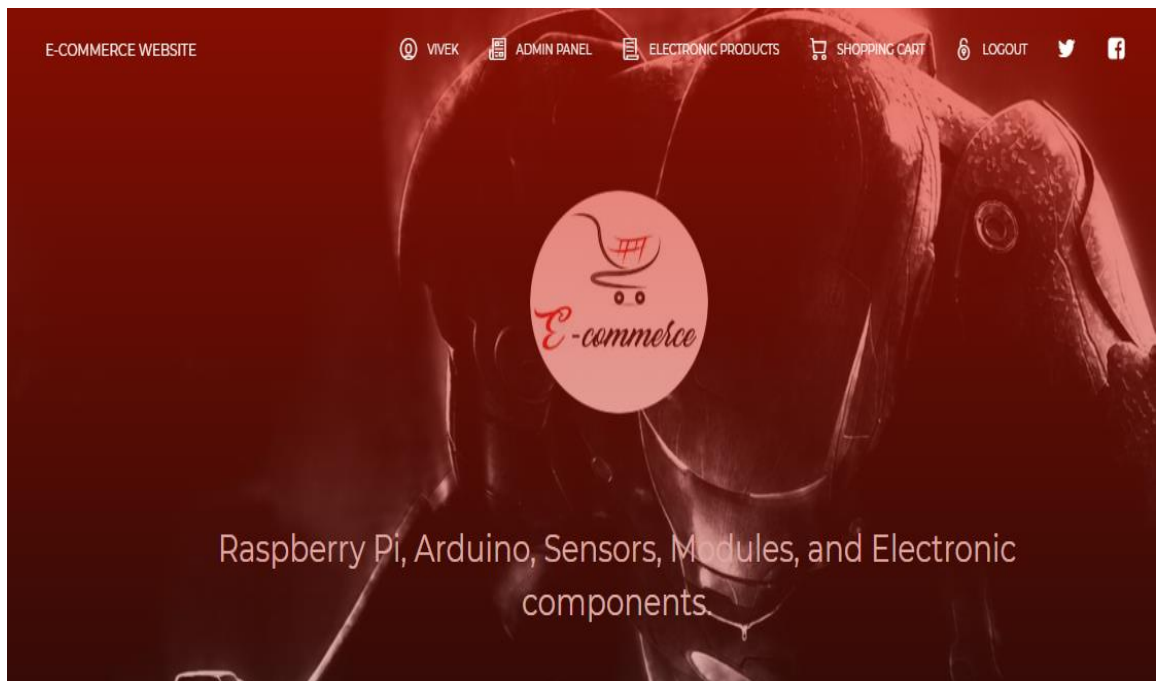


Figure 11: Homepage

#2) Searches:

Common tests are:

- Search Results on brands/products.
- Sorting options based on brand/price etc.
- Number of results display per page?
- Option of navigation for multiple pages.

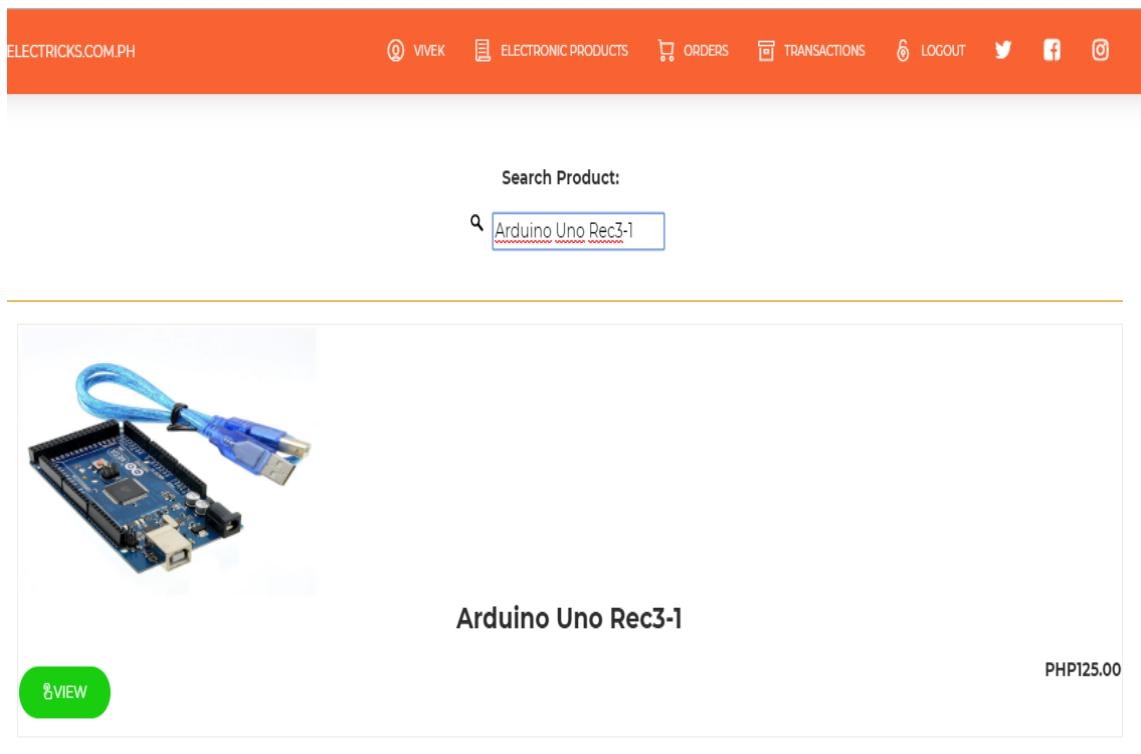


Figure 12: Search Page

#3) Product Details Page:

Check:

- Image of product
- Price
- Product characteristics
- Reviews on product
- Option checkout
- Options for delivery
- Product delivery information
- Stock information
- Variety of products



Serial number: 1122330099

Product name: Arduino Uno Rec3-1

Description: Small Arduino Uno Blue

Type: Arduino

Price: Php125.00

Product Sold Out!


Add To Cart

Figure 13: Product details Page


#4) Shopping Cart:

- Add items in cart and continue your shopping
- If adds same product in the cart while continuing to shop, then increase the count in shopping cart.
- Total items must display in cart.
- Taxes applied according to location.
- Changes by user must reflect the same
- Remove product from cart
- Checkout option
- Total cost
- Available coupons
- Without closing the site come back later. The site retain all products in the cart

Vivek's Shopping Cart

 Shop more items

[1] types of item.

Product	Description	Quantity	Price(PHP)	Total(PHP)	Option
	Flame Sensor Flame Sensor 3 Pins	1	455.00	455.00	update qty remove
Total Price				Php455.00	

[Check Out](#)

Figure 14: Shopping Cart Page

#5) Payments:

- Various payment options.
- Existing customer – Login to checkout
- New user must sign up
- If customer credit card information is stored, then ensure security testing of this information to make sure that it is held confidential.
- If user keep signed up for too long, make sure that session period is timed out or not. Different sites have different threshold (10 minutes) or may be different.
- Emails/Text confirmation when order number generated.

razorpay 777777777
[Login as a different user](#)

Select options to pay ₹ 1.00 Cancel Payment

Transaction ID: ORDS44557111

Paytm Balance
(Wallet Balance ₹ 9,803.00)

Money in Your Paytm ₹ 9,803.00	-	Payment to be made ₹ 1.00	Pay Now
--	---	-------------------------------------	---

Remaining balance ₹ 9802

[Saved Details](#) | FIA CARD SERVICES [Remove Card](#)

Figure 15: Payment Page

Chapter-6 RESULTS AND PERFORMANCE ANALYSIS

COMPARISON ANALYSIS

We have examined principal algorithms which are associated with asymmetric cryptography. A comparison table is designed with given attributes in table:

Name of algorithm

- Characteristics
- Problems in computation.
- Key size of encryption.
- Applications

Drawback and Attack

(1)Algorithm-RSA

Features:

- Integer factorization
- Size of encryption key -1024 bit
- Applications: Widely used in the banking
- Method for transaction and security purpose.

Drawbacks and attacks-

- Key size is very large and hence 15 times slower than ecc
- More memory is required, more consumption power and battery in RSA.

(2) Algorithm-DES

Features:

- Discrete logarithm problem: Computational problem
- DES has no encryption key.
- Applications: Used for digital signature.

Drawbacks and attacks-

- Vulnerable DSS design
- The second problem is about size of prime i.e. 512 bits
- Attack: In known message attack, attacker gives valid signature for different type of message which are known to attacker but not chosen by the attacker.

(3) Algorithm- Diffie Hellman

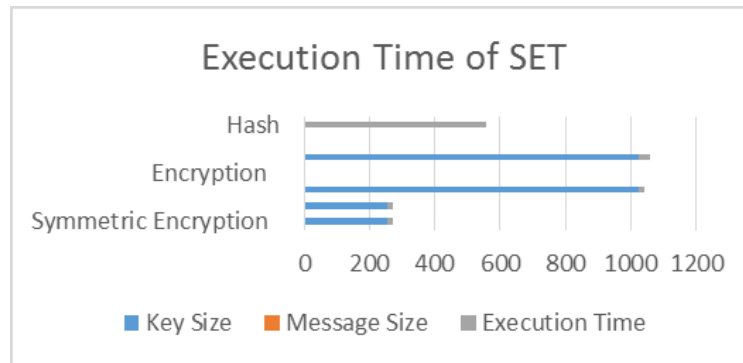
Features:

- Discrete logarithm problem: decision problem and computational problem.
- Key size for encryption is 1024bits
- Application: Exchanging of keys.

Drawbacks and attacks-

- The private key K has smaller value in size which is easily understood and decoded.
- Attack: Used only for key exchange.

Execution Time Graph:



Performance Analysis

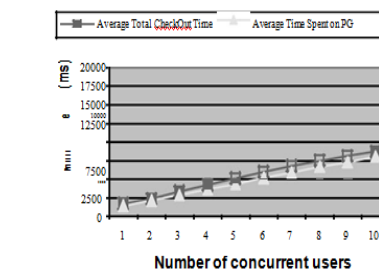
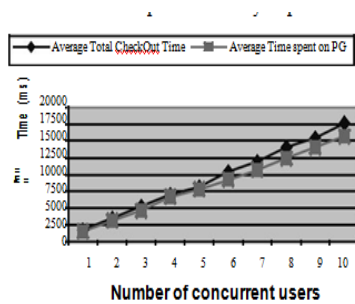


Fig. 4: Payment Transaction Time in Single-Threaded Model

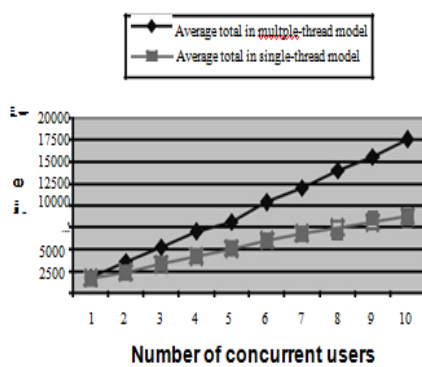


Fig. 5: A Comparison for Single-Threaded and Multi-Threaded Model

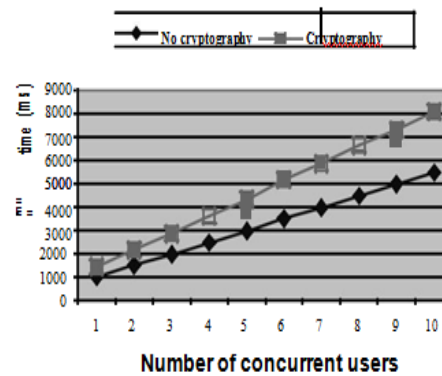


Fig. 6: Single-Threaded Model on the Payment Transaction Time on PG

Figure 16: Execution graph of SET

Chapter-7 CONCLUSIONS

CONCLUSION

Electronic Payment and infrastructure of system is available in many countries but it's not much safe. The defined architecture is also lack in the security feature. That model is made developed securely by implementing secure electronic transaction structure. Just he verified customer will now able to buy products from its vendor's website whose CR no. is valid and credit card contain sufficient amount to purchase the required product. Trustworthy third party apps or system involves who is dealing in all of payment settlements. Merchant can't misuse data of customer credit card details because the info given to him is transfer in encrypted form. The payment gateway can also decrypt customer information and get access to customers' bank. Firstly it is confirmed that weather the customer is authorized one or not then the whole transaction takes place. In this way website is made secure to ensure that any verified customer can very easily depend on site and without any problem make it successful transaction on the internet.

FUTURE WORK/SCOPE

There is lot of scope in secure electronic transactions improvement with the everyday change in technology, we can hope that it will improve with time and the drawbacks of SET technology will be improved.

Applications

When it comes to applications, E-commerce is used in a variety of ways in our world

Some of the examples are as follows :-

1. Amazon
2. Flip kart
3. EBay

And so on.

REFERENCES

- <https://ieeexplore.ieee.org/document/5489099>
- https://www.researchgate.net/publication/273550411_A_Secure_Electronic_Transaction_Payment_Protocol_Design_and_Implementation.
- https://thesai.org/Downloads/Volume5No5/Paper_27-A_Secure_Electronic_Transaction_Payment_Protocol.pdf
- http://www.idc-online.com/technical_references/pdfs/data_communications/Secure_Electronic_Transaction.pdf.
- http://ccc.cs.lakeheadu.ca/set/set_lw.pdf
- <https://pdfs.semanticscholar.org/f05a/290f358b9787c45cfbdc0d1a9b65172019a0.pdf>
- <https://pdfs.semanticscholar.org/173c/819ce3fccafdc4f64af71fd6868e815580ad.pdf>