Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Transaction Security for Internet E-commerce Application

Khandare Nikhil B.
Department of Computer Engineering
Veermata Jijabai Technological Institute,
Mumbai, India

Abstract-In the 21st century, any entity that does business or maintains customer data will do it online. The 'e' in eBusiness has already become redundant. There are already well understood practices and standards in place for user authentication, data encryption, and credit card transactions. Security of online electronic transaction is major issue in today'slife which need to be taken care of. Various methods are proposed for the security of online transaction but it may fail in one or the other way, secure electronic transaction SET protocol is also proposed. The operation of SET depends on software that implements a series of protocols installed in the workstations or servers of four kinds of people and organizations. These are Cardholders (Buyer) Merchants (Seller), Payment gateways/acquirers, Issuer.Paper is divided into Intoduction which introduces reader about topic, Second part is literature survey which in brief describes the current research done on the topic by various authors, Third part is Proposed work and Proposed System which is divided in four modules and working of system and finally conclusion.

Keywords: M-commerce,seller,buyer,e-commerce,cardholder,Merchant,Security

I. INTRODUCTION

The success or failure of an e-commerce operation hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations. Security is on the mind of every e-commerce entrepreneur who solicits, stores, or communicates any information that may be sensitive if lost. An arms race is underway: technologists are building new security measures while others are working to crack the security systems. One of the most effective means of ensuring data security and integrity is encryption

II. LITERATURE SURVEY

The Internet is dramatically changing the way that goods (tangible and intangible) and services are produced, delivered, sold, and purchased. Due to this development, trade on the Web comesan essential requirement for enterprises. From e-commerce to m-commerce, which has become a major service nowadays, every enterprise works hard to find out a way to sell and buy that cansatisfy its requirements.

1.1 E-commerce security requirements

Recently, the use of e-commerce systems has grown at a phenomenal rate. A large spectrum of products (tangibles and intangibles) is sold on the Internet, with payments made essentially by debit or credit cards. In addition, there is an increasing concern related to the security of the payment systems used to process online transactions. Confidentiality of payment card information due to disclosure of this information to malicious adversaries could enable them to perform fraudulent transactions at the customer's expense

1.2 General form of the e-commerce process

Payment transaction model has the interactions of four roles:

Payer – The payer is an authorizer of a payment means supported by an issuer. Ordering apayment may be done using a card, a token, or a certificate. The payer is the customeror buyer in an electronic commerce scenario.

Payee – The payee is a merchant providing goods, services, and/or information and receiving electronically the payment for something purchased by the payer. Usually, the payeeis simply referred to as the vendor, merchant, or seller in an electronic commerce scenario.

Issuer – The financial instrument that supports issuing payment cards (or means) by usingcryptographic technologies which guarantees the association with "real money." Its role is to provide the payer and the payee with instances of monetary value which areused in payment protocols to transfer "real money" from the payer to the payee.

Acquirer – This is a financial institution (a bank, for example) which transforms the cryptographic objects involved in the payment into "real money" on behalf of the payee

1.3 Security Requirements

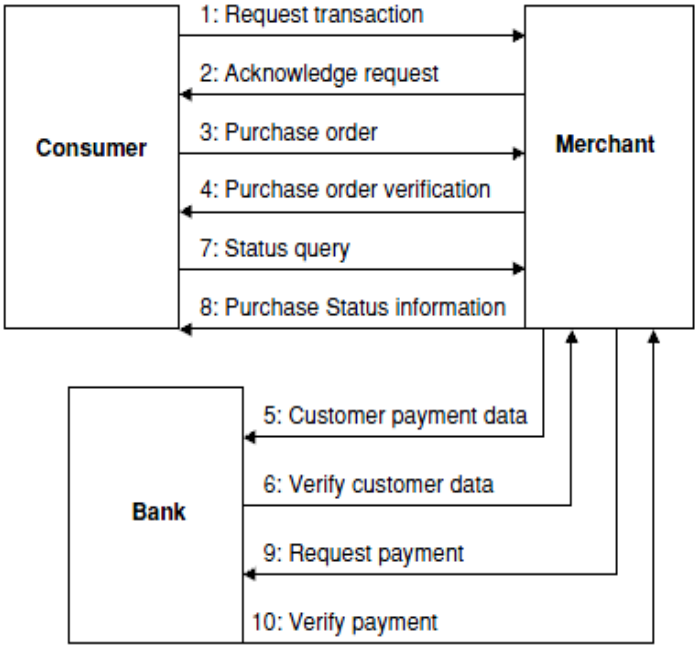
The security requirements vary from one role to another.However, it appears that acquirer and issuer have very close requirements. In the following we examine individually the requirements of each role. Client Transaction confidentiality, especially the information occurring in the payment card, is a major security need for a client. The nature of the transaction may require confidentiality. Various security protocols have been developed for e-commerce. The major protocolsinclude:

1. The Secure Socket Layer (SSL) protocol SSL was developed in 1994 by Netscape to provide secure communication betweenWeb browsers and Web servers. SSL provides server authentication, data integrity, and client authentication.
2. The Transport Layer Security (TLS) protocol This was introduced by the Internet Engineering Task Force in 1995 (Dierks and Allen, 1999).
3. The Secure Electronic Transaction (SET) protocol SET was developed by Visa, MasterCard, and other companies to facilitate secure electronic commerce transactions and provide confidentiality of payment card information, data integrity, authentication of both merchant and cardholder, and authorization of transactions.
4. The 3-D Secure Protocol This has been developed by Visa recently (Visa, 2002). It provides cardholder authentication for merchants using access control servers and the Visa Directory Server.

2.4 Transaction security with SET

Once registration is done, cardholder and merchant can start performing their transactions, which involve five basic steps in this protocol:

1. The customer browses thewebsite and selects the goods to purchase. Then the customer sends the order and payment information, which includes two parts in one message: the purchase order (say part a) and the card information (say part b). While the former information part is for the merchant, the latter is for the merchant's bank only.
2. The merchant forwards part b to its bank to check with the issuer for payment authorization.
3. On receipt of the authorization from the issuer, the merchant's bank sends it to the merchant.
4. The merchant completes the order, sends confirmation to the customer and captures the transaction from his/her bank.
5. The issuer finally prints a credit card bill (or an invoice) to the customer.SET relies on cryptography and digital certificate to ensure message confidentiality and security. Message data is encrypted using a randomly generated key that is further encrypted using the recipient's public key.



1. The customer opens an account
   The customer obtains a credit card account, such asMasterCard or Visa, with a bank that supports electronic payment and SET.
2. The customer receives a certificate
   After a suitable verification of identity, the customerreceives an X.509v3 digital certificate, which is signed by the bank. The certificateverifies the customer's RSA public key and its expiration date. It also establishes arelationship, guaranteed by the bank, between the customer's key pair and his/her creditcard. A merchant who accepts a certain variety of cards must be in possession of twocertificates for two public keys: one for signing messages and one for key exchange.The merchant also needs a copy of the payment gateway's public-key certificate.

3. The customer places an order
   This is a process that may involve the customer firstbrowsing through the merchant's Web site to select items and determine their prices.The customer then sends the list of the items to be purchased from the merchant, whoreturns an order form containing the list of items, their individual prices, a total price,and an order number.
4. The merchant is verified In addition to the order form, the merchant sends a copy ofhis certificate, so that the customer can verify that he/she is dealing with a valid store.
5. The order and payment are sent
   The customer sends both an order and paymentinformation to the merchant, along with the customer's certificate. The order confirmsthe purchase of the items in the order form. The payment contains credit card details.The payment information is encrypted in such a way that it cannot be read by themerchant. The customer's certificate enables the merchant to verify the customer.
6. The merchant requests payment authorization
   The merchant sends the paymentinformation to the payment gateway, requesting authorization that the customer's availablecredit is sufficient for this purchase.
7. The merchant confirms the order
   The merchant sends confirmation of the order to the customer.
8. The merchant provides the goods or service The merchant ships the goods or providesthe service to the customer.
9. The merchant requests payment
   This request is sent to the payment gateway, whichhandles all of the payment processing.

2.5 Securing Electronic Payment

The objective of an electronic payment system is to transfer a monetary value from the payer to the payee by using a payment protocol and a financial institution or network which links the exchanged data to some economic real world value. The financial network may be built of individual financial institutions (i.e., banks or authorized service providers).
Five key phases can be identified in a commercial transaction
1. Getting means of payment -This phase entails using the appropriate means of paying for objects and obtaining digital cash in a given currency.
2. Service discovery -During this step, the client discovers the available services and selectsone or some of them based on a set of factors including price.
3. Payment negotiation When an e-service has been selected by a customer, the client can negotiate payment based on specific parameters such as payment means and authentication mechanism.
4. Service utilization -During this phase, the customer utilizes the selected service, while making on-going payments.
5. Termination -This phase includes the action performed after the utilization of service has ended. Actions involve reclaiming any unspent money or obtaining a proof of payment and service use.

2.6 M-commerce and security

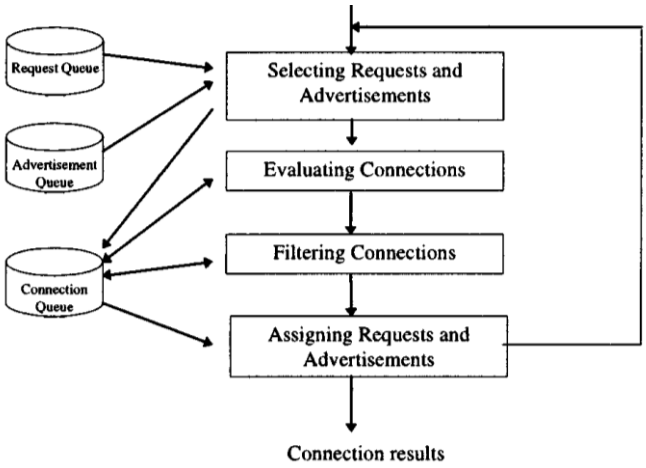
Recent advances in wireless technology have increased the number of mobile devices and have given speed to the rapid development of e-commerce activities using these devices. These advances have also contributed to the creation of new transaction processes that are made through wireless communications and wired e-commerce technologies, which are called m-commerce systems.
1. Ubiquity -This is an essential advantage of m-commerce. Customers can acquire any information whenever and wherever they want, regardless of their location.
2. Reachability -Business entities are able to arrive at customers anywhere anytime. With a mobile terminal, a customer can however limit his/her reachability to particular individuals or at particular periods of time.
3. Localization -The knowledge of the customer's location at a particular moment can add significant value to m-commerce since many location-based applications or services can be provided.
4. Personalization - M-commerce applications that are accessible may need to be personalized in ways appropriate to users. This can reduce the amount of information stored in the mobile device.
5. Dissemination Information can be distributed to a large set of customers since the wireless infrastructure supports simultaneous delivery of data within a given geographic area

2.7 A Brokering Protocol for Agent-Based E-Commerce

The goals of Brokering Protocol for Agent-Based E-Commerce are to
Design and implement an algorithm that connects buyer and seller agents.

1) Devise a brokering protocol for specifying and structuring the interactions among electronic intermediaries and trading (buyer and seller) agents.

- Design and engineer a testbed that models and simulates some of the activities of information brokering in the domain of securities trading.
- Algorithm uses multiple criteria to match buyers and sellers based on prespecified user profiles.
- The process of matching and connecting buyers and sellers are divided in four stages
  - *selection,*
  - *evaluation,*
  - *filtering* and *assignment*



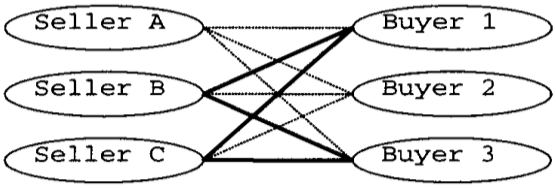
The algorithm prefers to select requests and advertisements

1) That are not expired or withdrawn;
2) With profiles and preferences that are closely matched;
3) That have not been previously assigned.

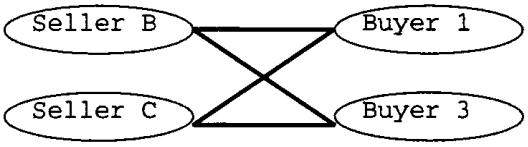
- Criterion 1) ensures that only valid advertisements (requests) are selected. This is because advertisements (requests) can be withdrawn at anytime and housekeeping jobs are normally done periodically in batch.
- By preferring advertisements (requests) that are not expired or withdrawn in the early stage saves system resources in connecting invalid buyer or seller agents and avoids recommending invalid connections to users

Connection with and without criteria 1 (check weather expired)

- Suppose there are three seller A, B, CAnd three Buyer 1, 2, 3
- Suppose that A's advertisement is expired and request from buyer 2 is withdrawn



- Without criteria 1,nine connection are formed out of which only four are valid
- With criteria one, only four connection are formed. less resource is required in handling these four (when compared to nine) connection is expected.

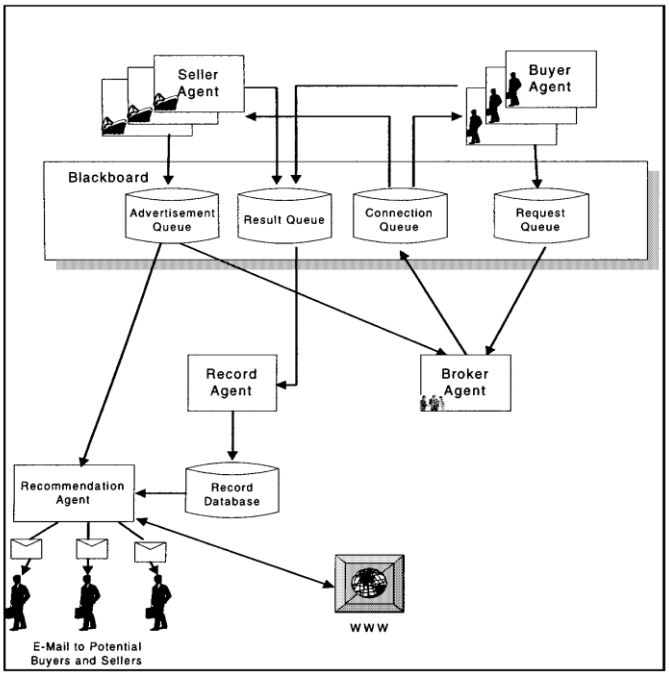


2.8 Agent-Based Information Brokering Test bed

- Enabling buyers to post requests and sellers to post advertisements
- Connecting buyers and sellers.
- Maintaining and documenting user profiles.
- Documenting successful connections.
- Making recommendations to potential buyers or sellers

Entities involved in Agent-Based Information Brokering Test bed

1. Buyer Agent: Buyer agents provide user interface for the users of the testbed. They post requests to or withdraw requests from the blackboard, view results of each request, and make purchase decisions.
2. Seller Agent: Seller agents are similar to buyer agents but act on behalf of human sellers.
3. Broker Agent: The broker agent connects buyer and seller agents together using the connection algorithm. In addition, it manages and controls the transactions and accesses to the blackboard.
4. Record Agent: The record agent documents and records the transaction histories of users in the record database. Using the information in the database, user profiles can be traced and determined.
5. Recommendation Agent: By accessing documented transaction histories, the recommendation agent proactively seeks potential buyers (sellers) when there is no matching sellers (buyers) or when the buyer to seller (seller to buyer) ratio is too large.
6. Blackboard Database: The blackboard accepts 1) requests from the buyer agents in the request queue and 2) advertisements from the seller agents in the advertisement queue



Information Brokering Protocol Stages

STAGE 1)

- Buyers send *requests* and sellers send *advertisements* to the broker agent to specify their profiles and preferences.
- Buyers and sellers may also withdraw requests or advertisements previously sent.
- For securities trading, buyers' specifications may include the type of products (for example, stocks of banks) and the broker agent attempts to match them with actual product names based on Information stored locally.
- Sellers' specifications may include the product name (for example, stocks of Citibank)

STAGE 2)

- The broker agent attempts to connect buyers and sellers by matching the specifications of requests and advertisements. It determines the rating of each connection made and filters out those with rating lower than a predefined cutoff point. Multiple connections for a request or an advertisement are also possible.

STAGE 3)

- The protocol does not assume that connections for requests and advertisements will always be made. If advertisements (requests) with matching specifications cannot be found, the recommendation agent proactively 'push' e-mail recommendations to trading agents by accessing the record database to determine their profiles and transaction histories.

STAGE 4)

- Buyers and sellers review connections made by the broker agent.

STAGE 5)

- Buyers and sellers complete the transaction. In this stage, trading agents can either take or reject recommendations made by the broker agent.

2.9 Model Checking for E-Business Control and Assurance

- Model checking is a promising technique for the verification of complex software systems. As the use of the Internet for conducting e-business extends the reach of many organizations, well-designed software becomes the foundation of reliable implementation of e-business processes
- These issues take on added importance as new business models and architectures such as Internet auctions, web services and the semantic web offer broad support for loosely coupled, e-commerce transactions where buyers and sellers may not have any prior trading experience with one another
- Variation in execution of concurrent processes in nonstop, nondeterministic systems increases the potential for automation failures.
- Automation failures occur when an automated system behaves differently than its stakeholders expect.
- Model checking can trace through all relevant states with respect to any given requirement.
- Some of the most compelling features of model checkers are summarized as follows

1. They help delimit a system's boundary or the interface between the system and its environment.
2. They precisely define a system's desired properties.
3. They characterize a system's behavior more accurately. Most current methods focus on functional behavior only (e.g., "What is the correct answer?") but some can handle real-time behavior as well (e.g., "Is the correct answer delivered on time?").

4. They can aid in proving that a system meets required specifications. By providing counterexamples that show how specifications are not satisfied, model checkers can pinpoint the circumstances under which a system does not meet its specifications. This can also help to correct the system.

These features of model checkers aid stakeholders in two important ways.

1) Through specification, by focusing a system designer's attention to crucial questions, such as:

- What is the interface?
- What are the assumptions about the application's environment?
- What is the system supposed to do under this condition or that condition?
- What happens if that condition is not met?
- What are the system's invariant properties?

2) Through verification, by providing additional assurance. Relying on proof that a system meets its security goals is better than relying on opinion—even expert opinion.

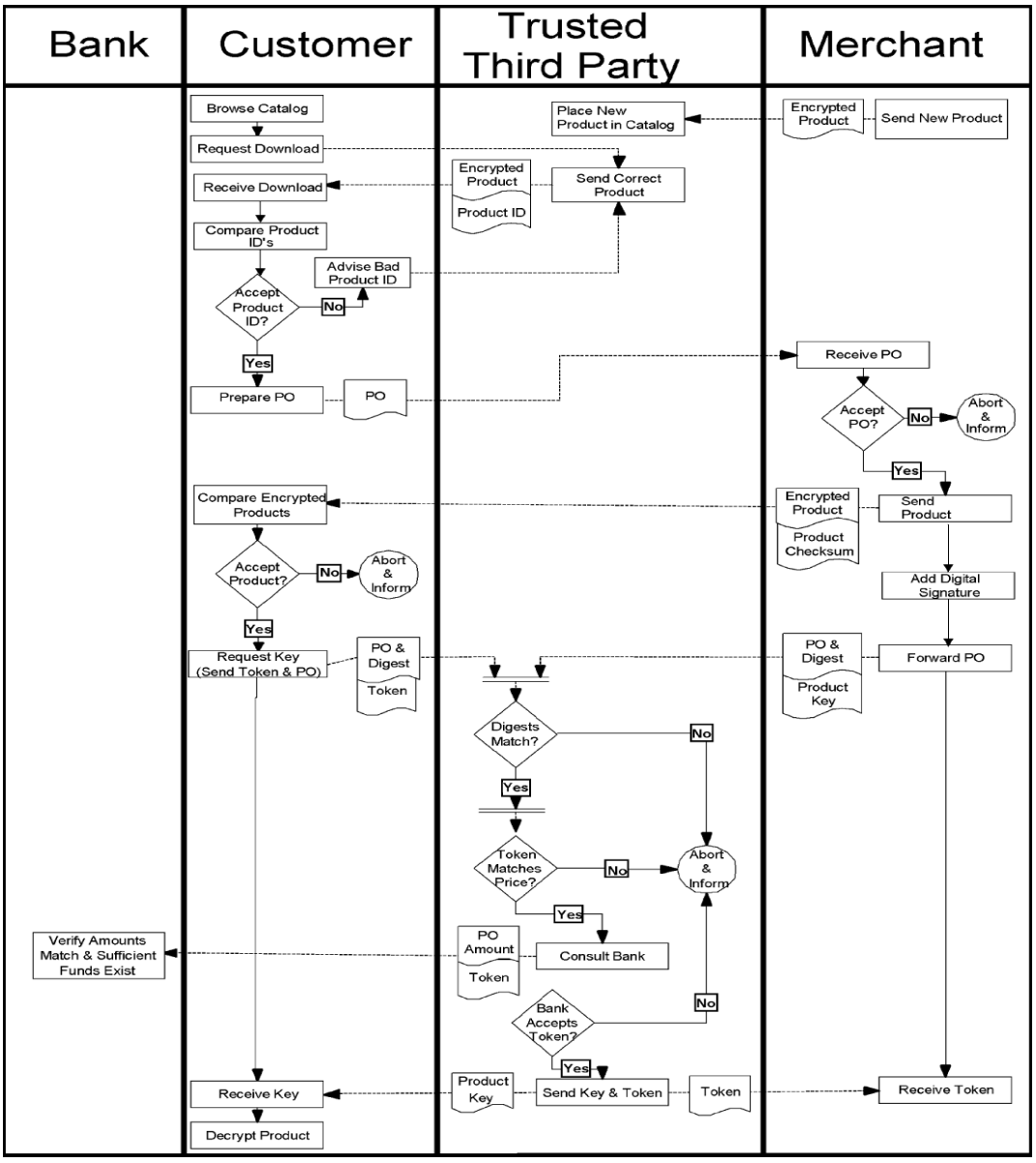
The process of proving entails three actions:

First, the system of interest must be modeled. A mathematical model is constructed that expresses the semantic structure of an e-business implementation.

Second, all properties to be guaranteed in the implementation are formally specified. In an e-business context, one such specification might be that goods must always be received before payment is initiated.

Third, a proof is provided. Typically, a proof relies on induction over traces of the e-commerce communication and transaction operations.

Model checking was originally developed for validating highly Complex integrated circuits and software packages but it has recently been adopted to tackle the complexity of e-commerce transactions. Sequence Diagram for e-business protocol



III. PROPOSED SYSTEM

3.1 Statement of Problem

In our system only certified sellers and buyers can participate,this will ensure the security because only legitimate users will be able to take part in the online electronic transactions sellers and buyers will be certified by the certifying authority. Certifying authority will certify the user when user may be seller of buyer wants itself to get certified, and hence participate in the transactions. The username or passwords which the buyer enters may be credit card number or online banking username and password should be secure and no one else should be able to read the sensitive information hence we use multiple encryption scheme for the security of information.We also check for the hacking or attacks on the e commerce application and the sensitive information sent over the network.

Modules of the Proposed System

There are four modules in the proposed system may be stated as

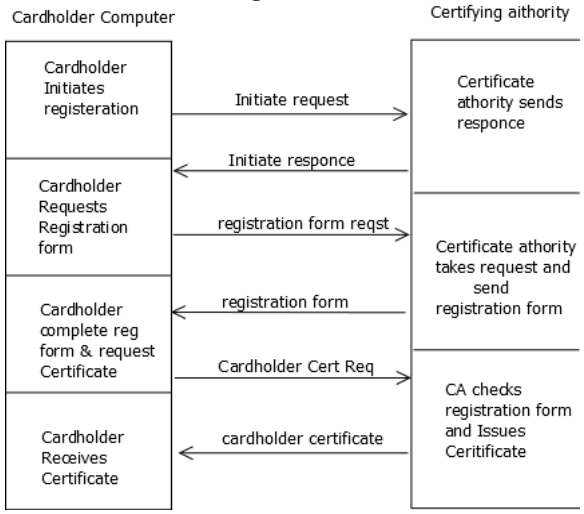
- Certification of Entities Participating in online Electronic Transaction
- Encryption of Sensitive Information Using Multiple Encryption Scheme
- Checking for the hacking or attacking on application and sensitive information sent over insecure channel
- Defense Mechanism used for the attack on web application

3.1.1 Certification of Entities Participating in online Electronic Transaction

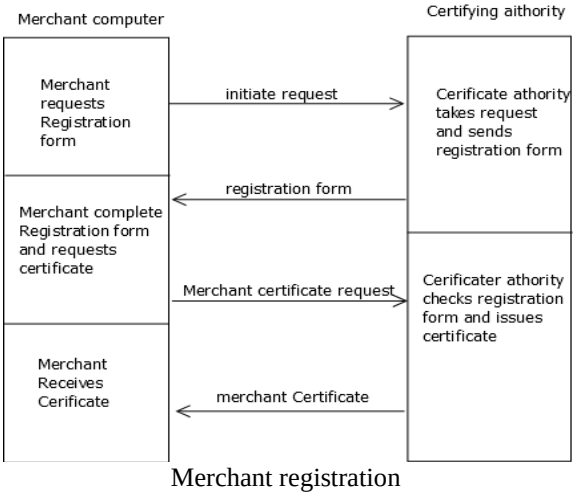
Everyone normally pay for goods purchased over the Internet by giving the merchant their credit card details. To prevent this information from unwanted people from stealing the card number, the message undergoes a session of the secure sockets layer (SSL) protocol. In this arrangement the cardholder and merchant should trust each other. That requirement is undesirable even in face-to-face transactions, but over the internet it has risks.

- The cardholder is protected from eavesdroppers but not from the merchant itself. Some merchants are dishonest. They do not protect the sensitive information.
- The merchant also needs to be protected and should have some protection against dishonest cardholders who supply an invalid credit card number.

It seems contrary to popular belief that it is the merchant who has the most to lose from fraud. Law in many countries protects the cardholder. The aspect of registration of merchant as well as cardholder is dealt with here. First figure shows the registration of cardholder and the second one show registration of merchant.



Cardholder registeration



Merchant registration

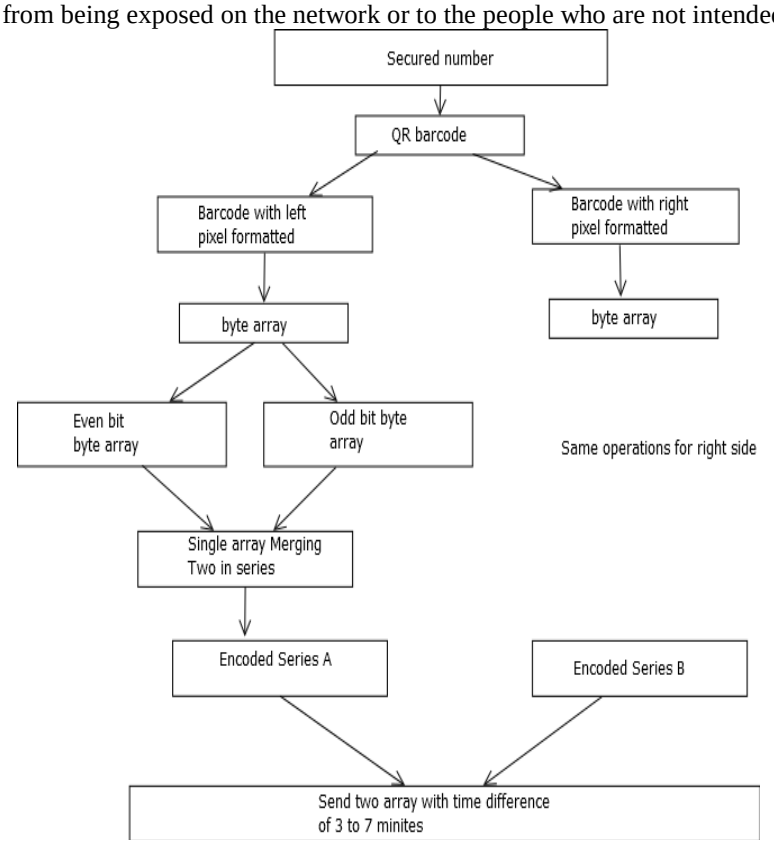
3.1.2 Encryption of Sensitive Information Using Multiple Encryption Scheme

In the study of barcodes work related to sensitive data transfer secure (SDTS) algorithms is proposed by many authors for security and applications of the same. The revised model of SDTS is below provides the benefits of the following.

Firstly, this makes the system more complex because the changes made are at byte level and thus, it is very difficult to predict by the hackers that what exactly is happening.

Secondly, this provides tightly coupled security because the complexity of the system is increased to larger extent.

SDTS model is converting the secure information into barcodes first, this information converting can be done by pixel manipulations and then convert the barcode image into byte arrays they may be even odd byte array. Finally, it encrypts the bytes using standard RSA algorithm. The detail view of the model is shown in figure is the revised model. With reference to the online transaction processing apps, the information to be processed is not sent over the network in unsecured manner, but a security key corresponding to the information is picked from databasetable to secure the real time data or information from being exposed on the network or to the people who are not intended to view it.



3.1.3 Checking for the hacking or attacking on application and sensitive information sent over insecure channel.

Here we check for the various attack that can happen over the web application and security of the same is dealt with here and we can check the hacking of sensitive information sent over the insecure channel i.e. over the internet, the probability of attack is reduced as the user is certified and also seller,information has least probability to be hacked as it is encrypted multiple times,for more security we add this module to our system.

3.1.4 Defense Mechanism used for the attack on web application

Various Defense

1. Analyze the Application
   - Identify Functionality
   - Identify Data Entry Points
   - Identify the Technologies Used
   - Map the Attack Surface

2. Test Client-Side Controls
   - Test Transmission of Data via the Client
   - Test Client-Side Controls over User Input
   - Test Thick-Client Components
   - Test Java Applets
   - Test ActiveX controls
   - Test Shockwave Flash objects

3. Test the Authentication Mechanism
- Understand the Mechanism
- Test Password Quality
- Test for Username Enumeration
- Test Resilience to Password Guessing
- Test Any Account Recovery Function
- Test Any Remember Me Function
- Test Any Impersonation Function
- Test Username Uniqueness
- Test Predictability of Auto-Generated Credentials
- Check for Unsafe Transmission of Credentials
- Check for Unsafe Distribution of Credentials
- Test for Logic Flaws
- Exploit Any Vulnerabilities to Gain Unauthorized Access

4. Test the Session Management Mechanism
- Understand the Mechanism
- Test Tokens for Meaning
- Test Tokens for Predictability
- Check for Insecure Transmission of Tokens
- Check for Disclosure of Tokens in Logs
- Check Mapping of Tokens to Sessions
- Test Session Termination
- Check for Session Fixation
- Check Cookie Scope

5. Test Access Controls
- Understand the Access Control Requirements
- Testing with Multiple Accounts
- Testing with Limited Access
- Test for Insecure Access Control Methods

6. Test for Input-Based Vulnerabilities
- Fuzz All Request Parameters
- Test for SQL Injection
- Test for XSS and Other Response Injection
- Test for OS Command Injection
- Test for Path Traversal
- Test for Script Injection
- Test for File Inclusion

7. Test for Function-Specific Input Vulnerabilities
- Test for SMTP Injection
- Test for Native Software Vulnerabilities
- Test for Buffer Overflows
- Test for Integer Vulnerabilities
- Test for Format String Vulnerabilities
- Test for SOAP Injection
- Test for LDAP Injection
- Test for XPath Injection

8. Test for Logic Flaws
- Identify the Key Attack Surface
- Test Multistage Processes
- Test Handling of Incomplete Input
- Test Trust Boundaries
- Test Transaction Logic

9. Test for Web Server Vulnerabilities
- Test for Default Credentials

- Test for Default Content
- Test for Dangerous HTTP Methods
- Test for Proxy Functionality
- Test for Virtual Hosting Misconfiguration
- Test for Web Server Software Bugs

Diagram of Proposed System

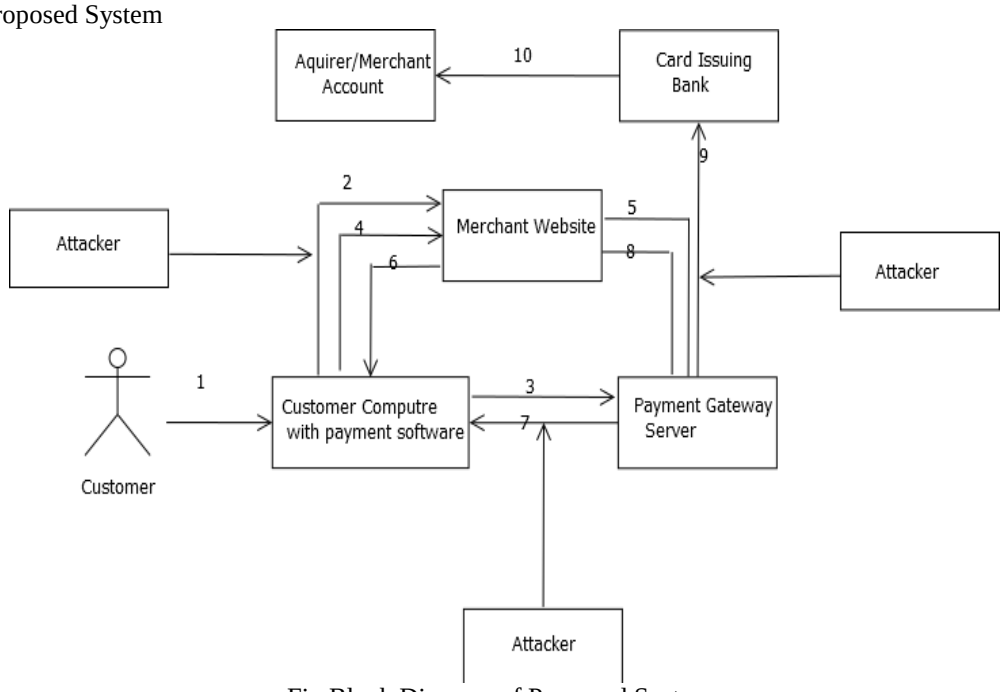


Fig Block Diagram of Proposed System

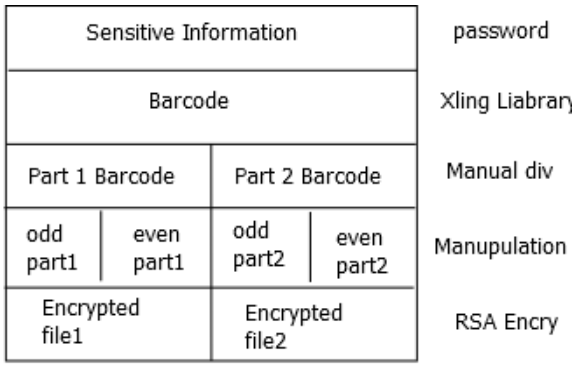


Fig Multiple Encryption Scheme

Algorithm

Steps in the algorithm cam be listed as follows

1. Customer starts Pri-pay on his terminal. He is then prompted to enter a secret password or a PIN to further access the system.
2. After successful entry of the password/PIN, customer opens the Pri-pay browser where he visits the merchant's website and places the order.
3. The OTP system in the Authentication module of Pripay synchronizes itself with the payment gateway server (GS).
4. An initial request draft, ReqDraft is created automatically by Pri-pay and encrypted using the public key of the payment gateway
5. Merchant sends the received ReqDraft to GS. GS after verifying the customer notifies the merchant about authenticity of the customer.
6. Merchant then creates a transaction bill, TransBill which is: TransBill = EnCrypt [(Merchant ID ,Merchant's Acc. No. , Payment details) , PRMER]
7. Customer verifies the order information and then Authentication module of Pri-pay sends T_ID obtained from the merchant to GS for merchant authentication.
8. GS sends T_ID to the corresponding merchant and merchant in turn sends the TransBill to GS. GS decrypts the TransBill using merchant's public key and authorizes the merchant and notifies the customer of merchant's authenticity.

9. GS then sends payment details and customer's details (credit card number) to the issuing bank.
10. Issuing bank after verifying the payment due with the credit card limit of the customer transfers the requested funds to the merchant's account/acquirer and both, customer and the merchant are notified of the transaction status.

Acronym	Meaning
Pripay	Payment software
ReqDraft	Request Draft
TransBill	Transaction bill
EnCrypt	Encryption
PIN	Personal Identification Number

Recent Rule on Debit card by RBI from 1 Dec 2013

- Now every time you swipe your card at a merchant outlet, you will have to enter the personal identification number (PIN) that you use at an automated teller machine (ATM)

Why the change?

- As per Reserve Bank of India (RBI) guidelines, from 1 December 2013, all debit card transactions at retail outlets will need to be validated using the existing ATM PIN. The move was introduced to reduce the incidence of frauds in payment systems
- If you don't punch in your PIN, the bank will decline the transaction. You get three chances to enter the right PIN. If the fourth attempt is also wrong, your card will get blocked. This is similar to the process at ATMs

IV. CONCLUSION

Privacy and Security are the two major factors that affect costumers trust in electronic transaction. Therefore companies or websites or organizations that offer and sell their products or services online should put more efforts in positively influencing their costumer's perceptions of privacy and security. Computer system security is a worldwide problem that is affecting private as well as corporate users of IT. Information technology users should be informed and should take responsibility for the security of resources that they are using and building. Accordingly, they should play an active role in protecting their privacy. All other security systems are generally based on cardholder authentication but ignore the merchant verification which makes the transaction system vulnerable to merchant attacks which should be taken care of and Internet related frauds such as site cloning, merchant collusion etc. In biometric run time fingerprint would be captured for mobile transaction and it should not stored already in the mobile device so it provides more security and not stolen by third party. Authentication request and reply should be in in the encrypted form. This gives the better level of security mechanism for mobile payment system.

REFERENCES

[1] A Brokering Protocol for Agent-Based E-Commerce, KwangMongSim and Raymond Chan
[2] Model Checking for E-Business Control and Assurance Bonnie Brinton Anderson, James V. Hansen, Paul Benjamin Lowry, and Scott L. Summer
[3] Provably Secure Integrated On/Off-Line Electronic Cash for Flexible and Efficient Payment Chun-I Fan and Vincent Shi-Ming Huang
[4] Verifying the SET Registration Protocols Giampaolo Bella, Fabio Massacci, Member, IEEE, and Lawrence C. Paulson
[5] An Artificial Immune System Architecture for Computer Security Applications Paul K. Harmer, Paul D. Williams, Gregg H. Gunsch, and Gary B. Lamont
[6] Exploring Software Partitions for Fast Security Processing on a Multiprocessor Mobile SoCDivyaArora, AnandRaghunathan, Senior Member, IEEE, Srivaths Ravi, Senior Member, IEEE, MuruganSankaradass, Niraj K. Jha, Fellow, IEEE, and Srimat T. Chakradhar, Member, IEEE
[7] Ray, I. Ray, and N. Narasimhamurthi, "A fair exchange e-commerceprotocol with automated dispute resolution," in Proc. 14th Annu, IFIPWG 11.3 Working Conf. Database Security, Schoorl, The Netherlands,Aug. 2000, pp. 27–38.
[8] E. Clarke, O. Grumberg, and D. Peled, Model Checking. Cambridge,MA: MIT Press, 1999.
[9] P. Ryan and S. Schneider, The Modeling and Analysis of Security Protocols:The CSP Approach. Reading, MA: Addison-Wesley, 2001.
[10] H. Schuldt, A. Popovici, and H. J. Schek, "Execution guarantees in electroniccommerce payments," in Proc. 8th Int. Workshop FoundationsModels Languages Data Objects. New York, 1999, pp. 189–198. LectureNotes in Computer Science.
[11] J. Tygar, "Atomicity versus anonymity: Distributed transactions for electroniccommerce," in Proc. 24th Very Large Data Base Conf., NewYork,1998, pp. 1–12.
[12] I. Ray and I. Ray, "Fair exchange in e-commerce," in Proc. Assoc. Computing*Machinery SIGcom Exchange*, vol. 3, May 2002, pp. 9–17.

[13] Iterative Trust and Reputation Management Using Belief Propagation ErmanAyday, Student Member, IEEE, and FaramarzFekri, Senior Member, IEEE

[14] A Family of Trusted Third Party Based Fair-Exchange Protocols Paul D. Ezhilchelvan and Santosh K. Shrivastava

[15] Provably Secure Integrated On/Off-Line Electronic Cash for Flexible and Efficient Payment Chun-I Fan and Vincent Shi-Ming Huang

[16] Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach by MangalaBelkhede, VeenaGulhane, Dr. Preeti Bajaj

[17] Online Transaction Processing using Enhanced Sensitive Data Transfer Security Model SonaKaushik, ShaliniPuri.

[18] Comments on the Security of Fast Encryption Algorithm for Multimedia (FEA-M) A. M. Youssef, and S. E. Tavares, Member, IEEE.

ABOUT AUTHOR

Nikhil Khandare (nikcoep@gmail.com) is Assistant Professor and has B.Tech from College of Engineering Pune M.Tech Computer Engineering from VeermataJijabai Technological Institute Matunga Mumbai, Maharashtra, India

