Analysis of Security mechanism in E-commerce transaction

Miss Nikita A. Rathi
Dr. S. R. Gupta

Abstract:- Now a days E-commerce is important because most of the business are done online. Example of e-commerce are like flipkart , amazon ,olx etc as business are done on e-commerce many transaction are done so it is important to provide security. There are three main security issues relevant to doing business online: verifying the identity of the person through which doing business, ensuring that messages sends and receive have not been tampered performed .Cryptography is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity , authentication and non-repudation, Application of cryptography include ATM cards,computer passwords and electronic commerce. Aim is to optimize the security levels of the existing system used in e-commerce transaction by using a new and more secure encryption technique which will reduce time required for transaction because security will be optimized than the security used in existing system also compare the algorithms used in existing system with new proposed algorithm based on some parameters.

Keywords - E-commerce, Transaction, Security, Cryptography.

I. Introduction

E-commerce (also written as e-Commerce, eCommerce), short for electronic commerce, is trading in products or services using computer networks, such as the Internet. E-commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern Ecommerce typically uses the World Wide Web for at least one part of the transaction's life cycle, although it may also use other technologies such as e-mail.It covers a range of different types of businesses, from consumer based retail sites, through auction or music sites, to business exchanges trading goods and services between corporations. It is currently one of the most important aspects of the Internet to emerge. Ecommerce allows consumers to electronically exchange goods and services with no barriers of time or distance[2] E - commerce has expanded rapidly over the past five years and is predicted to continue at this rate, or even accelerate. In the near future the boundaries between "conventional" and "electronic" commerce will become increasingly blurred as more and more businesses move sections of their operations onto the Internet. People use the term "ecommerce" or "online shopping" to describe the process of searching for and selecting products in online catalogues and then "checking out" using a credit card and encrypted payment processing.

An agreement between a buyer and a seller to exchange goods, services or financial instruments[1]. In accounting, the events that affect the finances of a business and must be recorded on the books. Transactions are recorded in what are known as "journal entries." Each entry describes a single transaction and states its date and amount.

E-commerce Transaction Mechanism Steps

1. The buyer uses its own private key and the seller’s public key to encrypt the order, and then use its own private key and the bank’s public key to encrypt the payment instruction. This ensures that the seller can only obtain the order information and the bank can only obtain the payment instruction delivered by the seller. This mechanism can keep the buyer’s account information secret to the seller. In addition to signing the order, the buyer should encrypt the order information.

2. The seller confirms the order after receiving the buyer’s order and signs the confirmation information with private key of customer. Then the buyer can validate the signature by seller’s public key. So the buyer can acknowledge that the seller has received his order formally.

3. The seller delivers the payment instruction to the bank after the order confirmation. The bank use the buyer’s public key to identify the buyer and use its own private key to check the secrecy of the payment instruction.

4. If the buyer's account is adequate for the deal, the bank sends accredit information to the seller and obligates the required money of the deal so as to transfer to the seller after the all transaction process.

5. The seller delivers the goods to the buyer according to the order.

6. The buyer signs on the Receipt Ticket for the seller when receive and check the goods according to the order and then uses its private key t o sign the information of Receipt Ticket and deliver it to the seller.

7. The seller sends the Receipt Ticket signed by the buyer and the transfer instruction to the bank, the information of which is signed with the seller's private key and is encrypted with the bank's public key

8. The bank transfers the money of the deal from the buyer's account to the seller's account and gives notice to the seller, and the notice is encrypted with the bank's private key , so the receiver can identify the reliability of the information by the bank's public key .

9. The bank sends bills periodically to the buyer. The bills are encrypted with the bank's private key , so the receiver can identify the reliability of the bills by the bank's public key , and the buyer will acquaint with the change of his account.

Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework[3]. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security-Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability[4]. E-Commerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats. Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. Still, its definition is a complex Endeavour due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions.[5] Security is one of the principal and continuing concerns that restrict customers and organizations engaging with ecommerce in e-commerce B2C and C2C websites from both customer and organizational [6].

II. Background

By definition, ecommerce is the utilization of computer tool and telecommunication network in order to buy sell products service of all kind[4][8][7]. For many Americans, ecommerce is something we participate in on a daily basis, like online bill payment or purchasing from an e-tailer. Nowadays the thought of living without ecommerce seems unbeliveable and an inconvenience. It wasn't until only a few years ago that the idea of ecommerce had even appeared. Ecommerce was introduced 40 years ago and, to this day, continues to grow with new technologies, innovations, and thousands of businesses entering the online market each year. The convenience, safety, and user experience of ecommerce has improved exponentially since its inception in the 1970's.

Currently, Amazon offers not only books but DVDs, CDs, MP3 downloads, computer software, video games, electronics, apparel, furniture, food, and toys. A unique characteristic of Amazon's website is the user review feature that includes a rating scale to rate a product. Customer reviews are now considered the most effective social media important for driving sales. The company attracts approximately 65 million customers to its U.S. website per month and earned revenue of 34.204 billion in 2010.

In 2001, Amazon.com launched its first mobile commerce site. Another major success story of the dot com was Ebay, an online auction site that debuted in 1995. Other retailers like Zappos and Victoria Secret followed suit with online shopping sites; Zappos being a web only operation. Also in 1995, was the inception of Yahoo followed by Google in 1998, two leading search engines in the US. These successful web directories began their own ecommerce subsidiaries with Google Shopping and Yahoo! Auction, in following years. Global ecommerce company, PayPal, began its services in 1998 and currently operates in 190 markets. The company is an acquired bank that performs payment processing for online vendors, auction sites, and other commercial users. They allow their customers to send, receive and hold funds in 24 currencies worldwide. Currently, PayPal manages more than 232 million accounts, more than 100 million of them active.

As more and more people began doing business online, a need for secure communication and transactions became apparent. In 2004, the Payment Card Industry Security Standards Council (PCI) was formed to ensure businesses were meeting compliance with various security requirements. With mobile commerce gaining speed, more users are purchasing from their hand.The market for mobile payments is expected to be increased by 2014, reaching $630 billion in value. Total sales in ecommerce have grown from $27.6 billion in 2000 to $143.4 billion in 2009 and are expected to continue its growth for the foreseeable (to predict) future.

Transaction security in E-commerce is important in todays century so that we get to know what and how much work is done in this field. As this field is intresting part to discuss.Follwoing are some researcher work in this field let see what work these people have done. Pradnya B.Rane and Dr. B.B.Mehsram[1] have done work on "Transaction security for E-commerce application". As web based application efficiency matters a lot for this application. As transaction in E-commerce faces problems such as database exploits, log data mining etc can be resolved by using different security measures so security is important in E-commerce application. They have secure E-commerce by integrating security technologies into trust infrastructure. The work done by them was first step in establishing trust to make transaction secure. Houssam E Ismaili, Hanane Houmani[6] have done work on " A Secure Electronic Transaction payment protocol Design and Implementation". Based on research done on security schemes and requirement of electronic payment they have design secure and efficient E-payment SEP Protocol. This SEP Protocol offers extra layer of protection for cardholder and merchant. SEP Protocol is good transaction protocol for credit card payment. [6] design system how well SEP protocol meets E-payment security implementation and identified end user implementation requirement. Khalid Haseeb, Dr. Muhammad Arshad, Shoukat ali, Dr. Shazia Yasin[7] have done work on " Secure E-Commerce Protocol " . [7] present system that has token based secure E-commerce protocol. [7] have paradigm that is capable of satisfying security objectives by using token based security mechanism. [7] done work on secure transaction so that both parties will get transaction token and can communicate with each other. There are many security E-commerce protocol like SSL , PGP , SET . [7] have used SET (Secured E-commerce Transaction) to provide protection against security threars. There are some steps that need to be performed between customer and merchant. SET provide security aspect in E-commerce like Authentication , Non Repudiation , Integrity, Replay Attack, Man In Middle Attack. Due to some issues in E-commerce Transaction they have used SET to provide protection against attack. SET present security mechanism to increase level of security objectivies using simple cryptographic technique. Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries)[7]. More generally, it is about constructing and analyzing protocols that block adversaries; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Ankur Chaudhary , Khaleel Ahmad, M.A.Rizvi[7] have done work on "E-Commerce Security through Asymmetric Key Algorithm" . In this [7] have proposed model of E-Transaction based on PGP. It have shown how secure payment and customer order of information will be efficiently handled by PGP based on dual signature. [7] proposed model focused on some drawback of DES because it generates many cycle and took much time to process data in verification so they have implemented RSA algorithm which is most secure and take less time. It has alo control all encryption and decryption with help of private and public key of sender and receiver.

Fahime Javdan Kherad, Mohammad V. Malakooti, Hamid R. Naji, Payman Haghighat [8] have done work in "*A New Symmetric Cryptography Algorithm to Secure E-Commerce Transactions"* . In this research we have proposed a new self-developed symmetric algorithm called FJ RC-4, which isderived from RC4. Our studies shown that KSA is thevulnerable stage of RC4, whereas a new self-developedsymmetric algorithm, FJ-RC4, is an attempt to increase thesecurity of RC4 by introducing the new algorithm for the KSAstage. We have investigated and compared the robustness of the RC4 and FJ-RC4 and shown that FJ-RC4 is stronger thanRC4 against the attacks. In addition, it takes more time to findkey in FJ-RC4 and requires more resources. Thus, it wouldlead us to a more secure algorithm in addition to the fact thatFJ-RC4 keeps RC4 simplicity in the core algorithm, PRGA. Inaddition this idea can be more efficient if KSA and PRGAstages are conducted concurrently.

III. Working of Optimizing security through cryptography algorithm

The objective to design this system is to optimize the security level that is applied during transaction so that user can make the transaction fast. E-commerce is important because most of the business are done online. Example of e-commerce are like flipkart , amazon ,olx etc as business are done on e-commerce many transaction are done so it is important to provide security. There are three main security issues relevant to doing business online: verifying the identity of the person through which doing business, ensuring that messages sends and receive have not been tampered performed . Cryptography is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity , authentication and non-repudation, Application of cryptography include ATM cards,computer passwords and electronic commerce. Using cryptography security level is integrated and Using RC6 algorithm and Kerbores level 3 proposed system is optimizing the security in E-commerce Transaction. First user will signup and add the services provided by them, these services can be provided by the sellers to the portal. The user login is common for both sellers and buyers.Kerbores level 3 authentication is used at this steps. It checks from database whether user is valid if not gives error and return to login page. If user is valid then user is passed to kerbores level 2 at this step it check whether timeout is expired or not. Timeout is used to avoid any viruses in the system so that user can login securely. If timeout is less than it will proceed further checking and if all is fine it will pass to kerbores level 3. In kerbores level 3 Key is generated and ticket is issued so that user can perform E-commerce transaction now. To perform E-commerce transaction three service is provided that are

- BUY

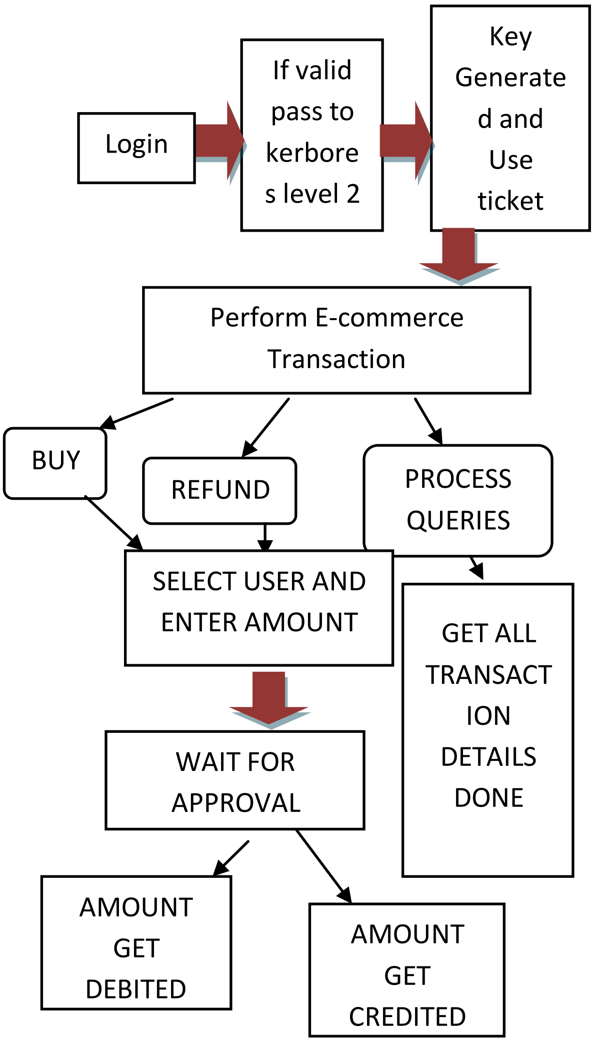
If user wants to buy user will select the user from whom user want to buy and will enter amount for item. User will wait till the other user(from whom user want to buy that item) approve it. If approved entered amount will be debited from the user wants to buy.

- REFUND

If user wants to Refund amount user will select other user to whom user have to refund and enter amount user have to refund. Will wait for approval and after approving the transaction the amount will be debited from user who want to refund and credited to user who accepted the transaction

- PROCESS QUERIES

In this user will get all the details of transaction have made on which date, time, amount(credited, debited).


Login
If valid pass to kerbores level 2
Key Generated and Use ticket
Perform E-commerce Transaction
BUY
REFUND
PROCESS QUERIES
SELECT USER AND ENTER AMOUNT
GET ALL TRANSACTION DETAILS DONE
WAIT FOR APPROVAL
AMOUNT GET DEBITED
AMOUNT GET CREDITED

IV. Conclusion

The conclusion is that it optimize E-commerce Transaction security using Kerbores and RC6 algorithm. Proposed model focused on some point like time consumption etc. In proposed model existing algorithm is removed i.e RSA because it generates many cycles and takes too much time to process data in verification but proposed system used RC6 algorithm which is most secure and less time consuming also proposed system use RC6 help all encryption and decryption with help of public and private key of public and private key of sender and receiever. At last comparison is done of algorithm used in existing and proposed system.

In future integrate proposed security system to existing E-commerce websites and also extended the concept of M-commerce for further security improvement.

References

[1]Pradnya.B.Rana,Dr.B.B.Meshram "Transaction security for E-commerce application," published in IJECSE,ISSN-2277-1956

[2] Brian Thomas, "Recipe for Ecommerce," published in IEEE December 1997, pp 72-74

[3] Hassler,"Security fundamentals for Ecommerce," published in IJCSI 2001

[4] Li Yuewen, "Research on E-commerce secure technology," published in IEEE computer society, 2010

[5] Dai Wei,Ji wei, "Research on the security of an improved E-commerce model," published in International conference on E-business and E-goverment of IEEE,2010,pp2354-2357.

[6] Houssam E Ismaili, Hanane Houman, "A secure electronics transaction payment protocol design and implementation," published in IJACSA 2014

[7] Ankur Chaudhary, Khaleel Ahmad, M.A.Rizvi "E-commerce security through asymmetric key algorithm," published in IEEE 2014

[8] Niranjana Murthy M, Dr. Dharmendra Chahar,"The study of E-commerce security issues and solutions ," published in IJARCE 2013, ISSN-2278-1021

[9] Khalid Haseeb,Dr. Muhammad Arshad, Shoukat Ali, Dr. Shazia Yasin, "Secure E-commerce protocol,"published in IJCSS 2011

[10] Fahime Javdan Kherad, Mohammad V. Malakooti, Hamid R. Naji, Payman Haghighat, " A New Symmetric Cryptography Algorithm to Secure E-Commerce Transactions, " published in International Conference on Financial Theory and Engineering, 2010