International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 06 | June 2019 www.irjet.net p-ISSN: 2395-0072

Ecommerce Transactions: Secure Gateway in Payment System

Jaiganesh Kalbande

PG Student, Department of Computer Science & Engineering Wainganga College of Engineering and Management, India

---

Abstract — In this paper describe a study of Electronic transaction which made using Secure Gateway in payment system. Electronic payment system for an electronic transaction is to be secure for participants such as Payment Gateway Server, Bank Servers and Merchant Servers, on Internet shown in current research and development. By using various Security Protocols and Techniques security architecture of such systems are designed, to make not only safeguard but avoid/eliminate the potential attempts of frauds that may occurs in such a payment transaction with stolen cards payment information and information of customer. Ecommerce has some form of money for services and goods over the Internet involved. It can be clearly intercept from the research/studies, The Internet is bit less secure and unreliable way to make any such a trade. The main aim of this paper is to review the description of asymmetric key crypto-system methodology that mainly uses a Security Protocol, the Techniques of Secure Communication Tunnel that prevent conventional transaction information such as account and Card number, amount and other information, and eventually secure electronic transaction implementation over the Internet.

Keywords: SET Protocol, Symmetric / Asymmetric Methodology, Communication Tunnel techniques, TCP/ IP Protocol, SSL / TLS, Dual Signatures, 3DES, AES

I. INTRODUCTION

In our society today, Online shopping by credit card or Debit Card is most common in the current ecommerce applications. The main reason of growth of e-commerce transaction is due to ease of buying and selling products over the Internet which is now a day convenient and efficient way to perform financial transactions tag has been achieved by e-payment services. In a few words, Ecommerce accompany with the issues and risks of insecurity and unreliable media during the exchange of some form of money for goods and services over the internet. Therefore, Paper focus on the following e-commerce scenario: a customer wishing to purchase goods online. Online Stored Value Systems, Financial EDI, Digital Cash, Credit Cards and Smart Cards Electronic Payment Methods are involved in Electronic Fund Transfer (EFT).

The major focus of this work is to explore the method of payment involved by means of a credit card/ Debit card, and subsequently. Secure and efficient payment systems that can operate over internet has been created a considerable need. To purchase something online most of the people have tried at least once or twice. Whether services or products, requires that a customer have a valid credit card most customer use credit cards purchasing online.

As increasing crime over the Internet, The customers still feel insecure to view their credit account information over allowing others. As nature of Internet, participants cannot be guaranteed with technologies that are not specifically designed for ecommerce for authenticity and security of payments. Demand of the situation to have a e-payment system that would not only allows to make potential secure payments but should also have feature of merchant authentication, transaction authorization by the customer of both merchant and the bank, privacy of transaction data. Lot of e-commerce technology has been developed over the years. It provides convenience and accessibility to customers in many ways. However security would be on stake.

This led to development in ecommerce domain of Secure Payment System. It is a step of operation to ensure financial transactions to be safe and confidential over the internet. This service plays vital role in application an online store that retained customers to keep doing transaction, as it build reputation of online services to be safe and reliable. In other way it provides them safe financial-transaction. E-commerce technology SET or the Secure Electronic Transaction is good in this type of services. Encrypting the information obtained between the customers and the online-store is called as SET, It has the unique process.

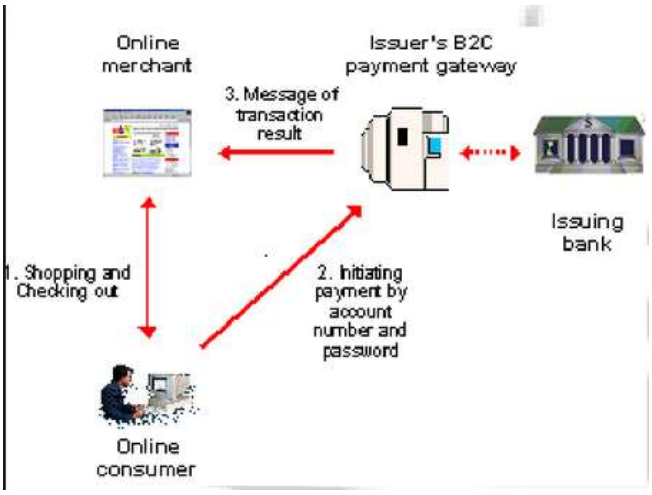

Fig. 1: Conventional e-commerce method with payment gateway.

Transaction Participants scenario Lets consider the three participants the payer, a merchant and a bank as financial institution. Figure-1 shows the all participants are connected by communication links.

To execute the transaction, Participants need to transfer certain information with the help of links over the internet. There is a possibility of eavesdropping, if information is transmitted in plain text over the links. If somebody want to listen to the network message could get access to confidential information, such as card type, card numbers and other complete details of the card owner. The amount of the charge from the card holder's account and transfers it to the seller's bank, this withdraws operations perform by debit cards.

Server stores records of every transaction, in electronic payment system. To communicate with the shops, when electronic payment system eventually comes up online, Customers can deposit money and for auditing purposes server uploads these records. Secure Payment System has been for an Electronic Transaction. Different cryptographic algorithms and techniques to achieve Secure electronic payment system. Various attacks has been shown in this paper and a payment system must incorporate satisfy, so as to be considered a secure system.

This paper has compared and contrasts the various existing solutions. Most efficient technique that to be incorporated in payment system in an electronic transaction has concluded in this paper.

II. LITERATURE REVIEW

Many researches and works have been done on secure payment system; following are some of them,

Newman, Simon; Sutter, Gavin et al. [1] has proposed an approach in three parts examines the legal issues raised by the development of the smart card. It explores contractual, liability at intellectual property rights issues and assesses whether a suitable legal framework exists in which smart card use can flourish and grow.

Sheng-Uei Guan; Feng Hua et al. [2] has proposed a multi-agent mediated electronic payment architecture in this paper. It is aimed at providing an agent-based approach to accommodate multiple e-payment schemes. Through a layered design of the payment structure and a well-defined uniform payment interface, the architecture shows good scalability. When a new epayment scheme or implementation is available, it can be plugged into the framework easily.

Flanigan, Paul D et al. [3] has reports on the findings of a research into consumers' online payment preferences in the United States. The electronic payments and expedited payments, commonly known as convenience payments, are gaining in popularity.

Sanayei, Ali; Rabbani, Hamed et al. [4] has discussed the e-banking evolution and explain the emerging of e-banking services, Epayment system as well as legal, risk management challenges, and have presented necessary suggestions for managing e-banking.

Wonglimpiyarat, Jarunee et al. [5] is concerned with the business strategy in managing payment innovations. Particularly, the study looks at the smart card - electronic cash (e-cash) innovation in the financial service industry. The

smart card e-cash has yet to overcome obstacles to its diffusion.

Cotteleer, Mark J. et al. [6] has proposed review the future of corporate payments and how businesses plan to address the challenges of integration, security, and remittance standards.

Singh, N. P [7] proposed the trends of major activities of the phishing across globe specifically in the banking sector. In addition, author analyzed the reasons for increase in phishing activities, types of phishing techniques, and process of phishing.

Bland, Vikki et al. [8] focuses on the benefits and

risks of electronic payments. Statistics NZ revealed that the value of total electronic card transaction (ECT) series had increased 0.8% at a value of $4.5 billion in September 2008 compared to August 2008.

Flatraaker, Dag-Inge et.al. [9] describes how some

banks and banking communities in the last two decades, especially in the Nordic area, have been able to take advantage of technology and new payments channels to re-engineer their payments business, and how they interact with their customers.

Bruce Jay; Huszar, W. Alison et al. [10] provides

information on banks' information security programs that are useful for consumers.

Sausner, Rebecca et al. [11] present information on a new firewall desktop used by the Community Bank for online security. According to the bank's information security officer Aaron Friot, the system offers intrusion prevention without the constant sitting of the employees, and is user interactive.

Mookerji et al. [12] explored that internet banking is fast becoming popular in India. Nevertheless, it is still in its evolutionary stage. They expect that a large sophisticated and highly competitive internet banking market will develop in future.

Joseph et al.[13] examined the influence of internet on the delivery of banking services. They found six primary dimensions of e-banking service quality such as convenience and accuracy, feedback and complaint management, efficiency, queue management, accessibility and customization.

Wool, Avishai et al.[14] discusses the failure of security standards in computer systems. Working on a standard has its own set of challenges. A standards body involves many parties with conflicting agendas, many of them powerful corporations. Furthermore, a standard is not measured by excellence.

Backhouse, James et al.[15] describe addresses the role of power and politics in setting standards. It examines the interaction of external contingencies, powerful agents, resources, meaning, and membership of relevant social and institutional groupings in generating successful political outcomes.

Owen, Michael et al.[16] describe discusses the Payment Card Industry Data Security Standard, also known as the PCI DSS. This standard has been assembled by the PCI group as a security baseline for all processors, handlers, or collectors of cardholder data bearing the mark of any of the members of the PCI.

Garry, Michael et al. [17] reports on the move of credit card industry in the U.S. to take some rigid steps that can help retailers improve security of their data cards. According to the article, through the sector's Payment Card Industry (PCI), the group is giving retailers greater predictability to their audits. In addition, it states that several states have already started enacting the in-transit data encryption system

Morrison, David et al. [18] reports on the examination of the data security standards of the credit card industry in the U.S. Congress. The examination concluded that if the credit card industry cannot address its

own fraud risks, the Congress might step in with federal legislation.

III. EXISTING METHODOLOGY

Conventional payment systems tend to be more costly than the modern methods, As with increasing impact of

intangible merchandise in worldwide economies and delivery in low cost, As smallest value of money in the manual world, Online processing could be worth of value. However, running e-payment systems are divided into two methods

- Payment in Online Mode: A bank before serving the purchaser in which vendor checks the payment send by purchaser.
- Payment in Offline Mode: No online link to the bank is needed.

According to the online assumptions, The e-payment schemes sub-divided into two parts

a) Transaction Payments Method: Previous arrangements between purchaser and vendor does not need in Single payment.

b) Account Payments Method: system account with bank by purchaser and vendor. The real payment transaction Agreement between both before carrying out transaction and amount.

The transaction payment can be further divided into two subgroups below

I. The transaction of credit card payment: Some hundreds or even thousands of dollars is tailored for large charge of payment. In contrast, low value payment of net money transaction is usually with difficult transaction online features and cost, similar as e-payment transaction. The drawback of the creed it, There will be fee of transactions of card payment transaction, mainly from the vendor perspective that has to pay some invoices for clearing house according to the agreement. This will certainly have straight impact on possible users.

II. Value transactions on service by e-payment: E-publishing and multimedia service are a number of important services of e-payment. In these services, due to the small transaction amount, shopping mall revenue from every transaction can relatively acquire by the merchant.

IV. PROPOSED WORK

The major focus of this work is to explore the method of payment involved by means of a credit card/ Debit card, and subsequently. Secure and efficient payment systems that can operate over internet has been created a

Considerable need. To purchase something online most of the people have tried at least once or twice. Whether services or products, requires that a customer have a valid credit card most customer use credit cards purchasing online.

In the project we use Secure Sockets Layer (SSL) protocol, Secure Electronic Transaction (SET) Protocol, D Secure and Secure communication tunnel algorithm to match the security result

- Secure Sockets Layer (SSL): Secure Sockets Layer (SSL) protocol originally created by the Netscape Inc. It is now implemented in all web browsers on account of its popularity and acceptance with best result. SSL has two main objectives: 1. Confidentiality Ensuring, by providing potential encrypting between the communicating parties (client and the server). 2. Use RSA algorithm to provide authentication of session partners.
- Secure Electronic Transaction (SET) Protocol: To carry out transactions successfully and without To drive transactions without compromising business communities companies are proposing technological solutions, Need a protocol that should works very similar way how a credit card transactions work Visa and MasterCard. The world formed a consortium with computer vendors such as IBM and developed which were Leading credit card companies for open protocol to emerged a standard in ensuring privacy, security and authenticity with trust in electronic transactions.
  - Secure Communication tunnel : Responsible to provide a secure way for communication between i.e., Customer to merchant and merchant to payment gateway which help to communicate two or more parties securely.

A. Flowchart

The below flowchart describe that we start the program by taking the input from user credential. Flow start mainly with user or admin module, on the right hand side of diagram Admin module can be referred. Admin would be responsible Managing Category.

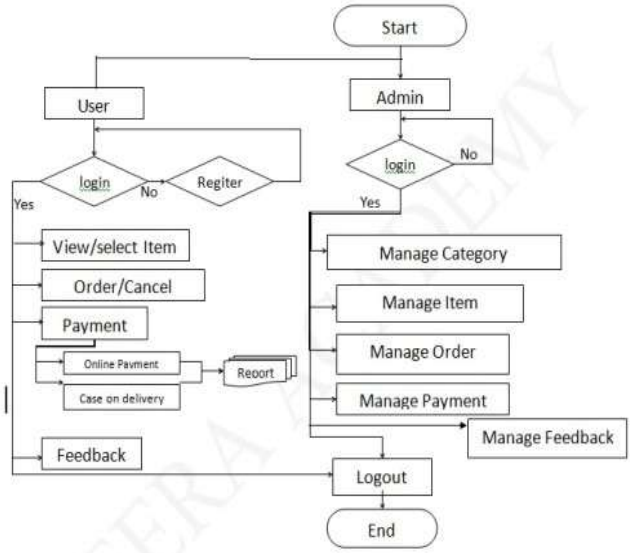

Fig. 2: Flow Chart.

User can select the item, Can be added in the cart for checkout purpose. All item can then later on checkout and proceed further for payment. Integrated payment gateway would be responsible for taking care of deduction of money from customer and credited to Merchant account. Any security criteria failed to meet prescript conditions would lead to unsuccessful transaction.

B. System Flow

1: Create user account.
2: Login to account.
3: Complete remaining details in user profile.
4: Search for products to buy.
5. Add them to cart.
6: View manage Cart.
7: Click on buy product.
8: Confirm customer address.
9: Processs route it to PayuMoney payment Gateway.
10: Enter Card details to proceed for payment.
11: Payment Gateway confirm card details with bank.
12: Details confirm with card neteworking undert fruad checking criteria.
13: Bank confirm user authentication.
14: PayuMoney would debit desired money from customer account and credit it to Merchant account.
15: User get confirmation of order along with communication of transaction from bank.
16: Proceed for checkout

C. Data flow diagram

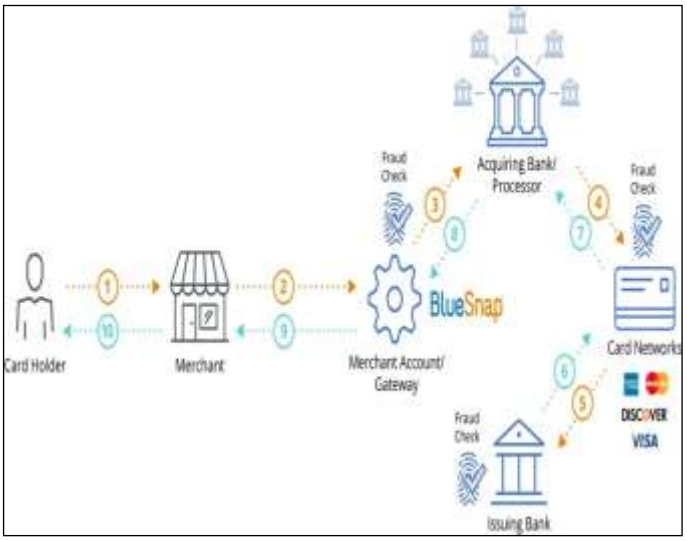

Fig. 2: Flow Flow Diagram.

As a customer, a payment gateway seems simple and straightforward. You visit an ecommerce site, select the items you want, add them to your cart, and checkout. You enter your payment information and confirm your order.

Behind the scenes, however, it's a little more complex.

The customer places an order and enters their payment information. An online the transaction will be processed. Again, this may result in a higher processing rate. Once this info has been submitted, it's encrypted, and then sent on its way. The encrypted data is first sent to the merchant's processor, which is simply the company that actually processes the transaction. The processor routes the transaction data to the credit card association. Visa, MasterCard, Discover, or American Express are credit card associations. These card associations charge an interchange fee for each transaction.

D. Comparison of Security Schemes For Secure Payment System

Below table shows the comparison of SET , SSL and Secure Tunnel

Key Point	SSL	SET Protocol.	Tunnel
Security	Less Secure	More Secure	More Secure
Technique	Encryption /Decryption	Encryption/Decryption-With Dual Signatures	Encryption /Decryption With-Crypto Tunnel
Merchant security	Less	Yes	More
Client Security	Less	Yes	More
Payment Gateway	No	Yes	More
Channel Security	No	Yes	Using Tunnel
Use of Digital Certificates	No	Yes	Yes

The above table outlines the similarities, key differences and state the major security schemes for any secure payment system.

V. CONCLUSIONS

The SSL, SET, and Secure communication Tunnel concepts used in this paper to reviews the Secure Electronic Payment schemes. To make customers should able to purchase the desired items on the Internet through Electronic Transaction, Hence security techniques are incorporated to provide security for the same.

To make transaction reliable and an efficient solution to any Ebusiness model, the system shall ensure the security of such a transaction. The strong benefits of such a Payment System are many folds: it uses strong authenticity and cryptographic checking models, to potential improving the security; payment information access restricted to merchant, thus building the privacy; as a result system safely could be freely use by customer.

Additionally, such a system can be use by the customers without having any adhoc software installed, Customer can be assure on the security of the secure payments or can rely to use a digital certificate. It is easily understandable from the literature, significant level of protection would be provide for secure communication channels by using security principle.

REFERENCES

[1] ELECTRONIC CASH AND SET, Paper presented at the conference: Internet Crime held in Melbourne, 1617 February 1998.

[2] Ajeet Singh, Karan Singh "A Review: Secure Payment System for Electronic Transaction. " March 2012. [20] Prakash Gulati1 and Shilpa Srivastava "The Empowered Internet Payment Gateway ".

[3] P. Jarupunphol, C.J. M itchell, Measuring “3-D Secure and 3D SET against e-commerce end-user requirements”, Proceedings of the 8th Collaborative Electronic Commerce Technology and Research Conference, 2003, 51–64.

[4] Yin, Y. “The RC5 Encryption Algorithm: Two Years On.” 1997.

[5] Gary C.Kessler, N.Todd Pritsky,”Internet Pay ment Systems: Status and Update on SSL/TLS, SET and IOTP” Information Security Magazine August 2000.

[6] Baja and Nag, “E-Commerce” TM H Publications.

[7] Z. Dju ric, Securing money transactions on the Internet, 2005.

[8] Yun Ling, Yiming Xiang, Xun Wang “RSA-BASED SECURE ELECTRONIC CASH PA YM ENT SYSTEM” Proceedings of the 2007 IEEE IEEM .

[9] Z. Djuric, Secure internet payment System ”ITCC- 2005.

[10] Z. Djuric, Ognjen Maric “Internet payment System”, Journal of University computer Science-2007

[11] Ro lf Oppliger, Ralf Hauser b, 1, Dav id Basin c, SSL/TLS session- aware user authentication or how to effectively thwart the man-in-the- middle. 23 March 2006.

[12] A R Dani1, P Radha Krishna and V Subramanian “An Electronic Pay ment System Architecture for Composite Pay ment Transactions” 2007.

[12] W .Stallings, 1998 ”Cryptography and Network Security”, Th ird Ed ition, 2006.

[13] Yann Glouche1, Thomas Genet1, Olivier Heen2, Olivier Courtay2, a Security Protocol Animator Tool for A VISPA, 2005.

[14] Kaliski Jr, B.S. and Yin, Y. L., September 1998. “On the security of the RC5 Encryption Algorithm”,2006.

[15] Pyae Hun,”Design and Implementation of Secure Electronic Pay ment System (Client)” World Academy of Science, Engineering and Technology 48, 2008.

[16] Ajeet Singh, Gurpreet Kaur, M.H Khan, Manik Chandra, Shahazad, National Conference on Information, computational Technologies and e- Governance (NCICTG 2010) in Laxmi Devi Institute of Engineering & Technology, Alwar (Raj), India,”The Secure Electronic Pay ment System Using SET Protocol Approach. 19 to 20 Nov- 2010.

[17] Yin, Y. “The RC5 Encryption Algorithm: Two Years On.” Crypto Bytes, winter 1997.

[18] Ajeet Singh, M.H Khan, ManikChandra,Shahazad “Implementation of Payment System for Internet Transaction” International conference on concurrent Techno and Environ search-in Bhopal, India, 4th -5th Dec. 2010