A Critical Study: Secure Gateway in Payment System for Electronic Transaction

Gangadhar Sajjanar[1], Akram Pasha[2]

[1] M.Tech Scholar, Department of Computer Science and Engineering,
Reva Institute of Technology and Management, Bangalore, India

[2]Associate Professor, Department of Computer Science and Engineering,
Reva Institute of Technology and Management, Bangalore, India

Abstract: ***In this paper the attempt of studying a Secure Gateway in payment system for Electronic transaction is made. The current research and development shows that the electronic payment system for such an electronic transaction is to be secure for participants such as Payment Gateway Server, Bank Servers and Merchant Servers, on Internet. The security architecture of such systems are designed by using various Security Protocols and Techniques, not only to safeguard but eliminate the fraud that occurs in such a transaction with stolen credit card/debit card payment information and customer information. Electronic commerce involves the tremendous exchange of some form o f money for trade of goods and services over the Internet, and it is evident from the studies that the Internet is an insecure and unreliable media in many ways in such a trade. The primary goal of this paper is to review the asymmetric key crypto-system methodology that uses Security Protocol, the Secure Communication Tunnel Techniques that protect conventional transaction data such as account numbers, Card number, amount and other information, and to finally provide secure implementation for such an electronic transaction on the Internet.***

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

1. Introduction

Online shopping by card is not new in the current e-commerce applications in our society today. The ease of purchasing and selling products over the Internet has helped the growth of e-commerce and as a result the e-payment services have proved to be the convenient and efficient way to perform financial transactions. In a nut shell, Electronic commerce involves the exchange of some form of money for goods and services over the Internet but associated with the issues and risks of insecurity and unreliable media. Therefore, in the work proposed, we focus on the following e-commerce scenario: a customer wishing to purchase goods online; Electronic Payment Methods-Electronic Fund Transfer (EFT) involved in such a transfer, Financial EDI, Credit Cards, Digital Cash, Online Stored Value Systems, and Smart Cards.

The major focus of this work is to explore the method of payment involved by means of a credit card/ Debit card, and subsequently, to address methods that are to be adapted to ship the goods physically. A considerable need for secure and efficient payment systems that can operate over Internet has been created. Most people have tried at least once or twice to purchase something online. Purchasing online, whether services or products, requires that a customer have a valid credit card or International debit card or finance account such as Pay Pal but most online purchases use credit cards. Due to the increasing crime on the Internet, the customers still have second thoughts over allowing others to view their credit account information.

Due to the nature of Internet, security and authenticity of payments and participants cannot be guaranteed with technologies that are not specifically designed for e-commerce. We need an e-payment system that would not only provide secure payments but should also have properties like online customer and merchant authentication, unforgivable proof of transaction authorization by the customer both to the merchant and the bank, privacy of customer and transaction data. To some it provides a sense of uncertainty and taking risks when purchasing online. Over the years there is lot of e-commerce technology that has been developed. This helps the customers in many ways in terms of convenience and accessibility. But still the security of their hard earned money is left unanswered. This led to the development of Secure Payment System in the e-commerce domain. It is a mode of operation wherein the security of financial transactions done on the Internet is ensured to be safe and confidential.

This application of an online store is an important service that keeps the customers of an online company coming back because they view the online store as safe and reliable. In a way also it provides them a sense of safety and security of their financial-transactions.

Under this type of e-commerce technology is SET or the Secure Electronic Transaction. The SET uses the unique process of encrypting the information obtained between the customers and the online-store. Transaction Participants scenario assumes the existence of three participants a customer (the payer), a merchant (the payee) and a financial institution (e.g. a bank).

All the participants are connected with communication links as shown in figure-1. In order to perform the purchase, the participants need to exchange certain information over those links. If the information is transmitted over the links in plain text, there is a possibility of eavesdropping. Anyone listening to the network traffic could gain access to sensitive information, such as card numbers, card type and or the

complete details of the card holder. Credit card-such as a Visa or Master, has a preset spending limit based on user's credit limit. Debit Cards –withdraws the amount of the charge from the card holder's account and transfers it to the seller's bank. In electronic payment system, server stores records of every transaction. When the electronic payment system eventually goes online to communicate with the shops and the customers who can deposit their money and the server uploads these records for auditing purposes.

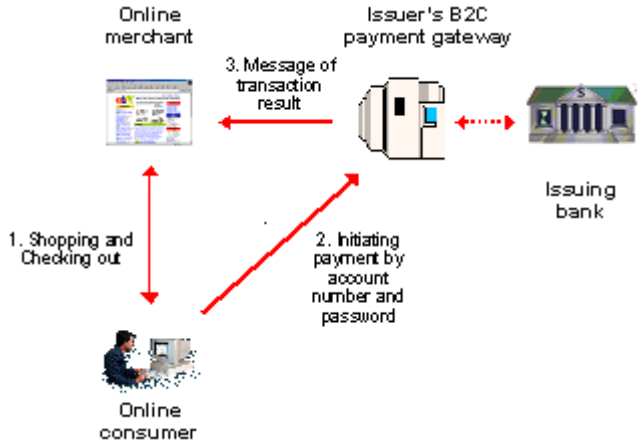

Figure 1: A typical e-commerce scenario and Gateway Payment

We review Secure Payment System for such an Electronic Transaction. Secure electronic payment system uses different cryptographic algorithms and techniques to achieve: privacy, integrity, authentication and non - repudiation. In this work, we discuss various attacks and the important security requirements such a payment system must incorporate and satisfy, so as to be considered a safe and secure system. Initially, this work discusses some of the existing secure systems, how those systems work, their advantages and disadvantages. Subsequently, we compare and contrast the various existing solutions. Finally, we conclude this paper by showing the most efficient technique that must be incorporated for such a payment system in an electronic transaction.

2. Background & Related Work

With the increasing impact of intangible merchandise in worldwide economies and their immediate delivery at small cost, traditional payment systems tend to be more costly than the modern methods. Online processing can be worth of value smaller than the smallest value of money in the manual world. However, there are two methods of running e-payment systems.

- Online payment: in which vendor checks the payment send by purchaser with a bank before serving the purchaser.
- Offline payment: in which over spending must be detected, and consequently, no online link to the bank is needed.

The e-payment schemes can be sub-divided into two groups according to the online assumptions.

a) Payments by transaction method: in which Single payment does not need previous arrangements between purchaser and vendor.
b) Payments by account method: in which purchaser and vendor should have system account with bank and certain type of agreement between both before carrying out the real payment transaction.

The payment by transaction can further be divided into two subgroups

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

II. The e -payment by small value transactions on service: This is acquiring certain interest from the area of research. A number of important services of e-payment are e-publishing and multimedia service. In these services, due to the small transaction amount, the merchant acquires relatively shopping mall revenue from every transaction

As a result, expensive calculations such as digital signature should be limited in order to reduce the investments in software applications. In the recent years, e-payments offering a relatively key improvement in the online revenue malls. The foundation of e-payments is to take benefit of the high level of viewers by p resent content for a low price. Other alternative of this thought is to rating fractions of cents for equally fractional contents sums.

The main features in e-payment protocol are less charges of payment amount and high occurrence of transactions on the e-commerce system.

2.1Secure E-payment Protocol

An e-payment process is a sequence of actions that involves a business task. There are mainly two kinds of payment transactions: i) Atomic payment transaction-single payment transaction and single payment and ii) Composite payment transaction-single payment transaction and multiple payments. Usually, a composite payment transaction involves multiple atomic transactions. Each atomic transaction supports the traditional ACID properties and must either fully commit or fully rollback. However, the classical ACID properties do not hold when a single payment transaction involves multiple atomic payments, especially when a failure occurs in any atomic payment transaction. Since atomic transactions use a two-phase commit protocol, a coordinating process is required to manage and synchronize the composite e- payment services within a given payment transaction. for example, consider a composite payment transaction. An organization has to pay Ethiopian Birr 10,000 for electricity board, Birr 20,000 for Telephone Office, Transports office-Birr 10,000 and Birr 4,000 to Water Board. At the time of issuing a debit instruction using e-check payment instrument with Birr 44,000 assume that by the time the e-check is cleared, the last date for payment towards Water Board is over and the organization has to pay a penalty of Birr 200. Since the balance after the two payments is not sufficient, it is not

possible to transact the water board payment.

Though, the payment instruction toward the electricity and telephone was successful, the complete transaction has to roll back due to insufficient amount. This complete reversal based on nothing-or-all protocol may in turn lead to late payment to other successful utility services. Hence, the nothing-or-all protocol as described above is not sufficient to handle composite e-payments. It can result in loss of confidence and trust in the e-payment services

Payments on the Internet' [6] can therefore refer to either the particular type of electronic money that involves a software product (although at the moment there is no such product in general use) or to electronic access products (via a card reader and a computer), or to both of these. Systems are also emerging that will allow the use of electronic (prepaid) money to be used over a network, by allowing the cash balance of the prepaid card to be drawn in accordance with the value of the goods or services purchased. Internet payments systems cover transactions both wholesale (between companies) and retail (between consumers and companies). Methods of payments include: bank transfers, cheques, credit and debit cards, and prepaid debit cards.

3. Security Requirements For Secure Payment System

The primary goal of cryptography is to secure important data as it passes through a medium that may not be secure itself. Usually, that medium is a computer network. There are many different cryptographic algorithms, each of which can provide one or mo re of the following services to applications. It is generally accepted that, in order to be considered secure, a payment system must satisfy the following fundamental security requirements

3.1 Authentication

The assurance that the communicating parity is the one that is claims to be prevents the masquerade of one of the parties involved in the transaction. Both parties should be able to feel comfortable that they are communicating with the party with whom they think they are communicating. Applications usually perform authentication checks through security tokens or by verifying digital Certificates issued by Certificate authorities. Cryptography can help establish identity for authentication purposes

3.2 Access Control

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do.)

3.3 Data Confidentiality (Secrecy)

Data Confidentiality is the protection of data from unauthorized disclosure. Confidentiality is an essential component in user privacy, as well as in the Protection of proprietary information, and as a deterrent to theft of information services. The only way to ensure confidentiality on a public network is through strong encryption. Data is kept secret from those without the proper credentials, even if that data travels through an insecure medium.

3.4 Data Integrity (Anti -tampering)

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no medications, insertion, deletion, or replay) and prevents the unauthorized medication of data. Financial messages travel through multiple routers on the open network to reach their destinations. We must make sure that the information is not modified in transit.

3.5 Non-Repudiation

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of communication.
• Non-repudiation, Origin- Proof that the message was sent by the specified party.
• Non-repudiation, Destination- Proof that the message was received by the specified party.
Non-repudiation is usually provided through digital signatures and public key certificates.

4. Types of Attacks on Insecure System

4.1 Network Attacks
These simple services can be used to stop a wide variety of network attacks, including

4.1.1 Snooping (passive eavesdropping)
An attacker watches network traffic as it passes and records interesting data, such as credit card information.

4.1.2 Tampering
An attacker monitors network traffic and maliciously changes data in transit (for example, an attacker may modify the contents of an email message)

4.1.3 Spoofing
An attacker forges network data, appearing to come from a different network address than he actually comes from. This sort of attack can be used to thwart systems that authenticate based on host information (e.g., an IP address)

4.1.4 Hijacking
Once a legitimate user authenticates, a spoofing attack can be used to "hijack" the connection.

4.1.5 Capture-replay
In some circumstances, an attacker can record and replay network transactions to ill effect. For example, say that you sell a single share of stock while the price is high. If the network protocol is not properly designed and secured, an attacker could record that transaction, and then replay it later when the stock price has dropped, and do so repeatedly until all your stock is gone.

4.1.6 PIN-guessing attack
An attacker can fake the digits and use the user authentication code (UAC) to launch a PIN-guessing attack.

4.2 Cryptographic attacks

In order to define the security level o f a cryptosystem we have to specify the type of attack we are assuming (the power of the adversary) and the type of breaking which we wish to prevent (what tasks should the adversary be able to perform as the result of the attack) Given these specifications, we have to show that breaking the cryptosystem with the specified attack is as hard as performing a certain computational task. The types of attacks are

4.2.1 Cipher text-only attack
Cipher text-only attack in which the adversary sees only cipher texts.

4.2.2 known-plaintext attack
Known-plaintext attack in which the adversary knows the plaintexts (messages) and the corresponding cipher texts transmitted.

4.2.3 chosen-plaintext attack
Chosen-plaintext (CP) attack; where the adversary gets to pick (adaptively); plaintexts of his choice and by exploiting the encryption mechanism he sees their encryption value.

4.2.4 chosen-cipher text (CC) attack
Chosen-cipher text (CC) attack - where in addition to access to the encryption mechanism the adversary can pick (adaptively) cipher texts of his choice and by using the decryption mechanism (as a black box) he gets the corresponding plaintexts.

5. Issues of Security Approach to Secure Payment System

5.1 Secure Sockets Layer (SSL) protocol
Netscape Inc. originally created the Secure Sockets Layer (SSL) protocol. On account of its popularity and acceptance, it is now implemented in all web browsers. SSL has two main objectives:

1. To ensure confidentiality, by encrypting the data that moves between the communicating parties (client and the server).
2. To provide authentication of the session partners using RSA algorithm.

A. The SSL Handshake protocol, in which the communicating parties (client and the server) authenticate themselves and negotiate an encryption key. One point to note here is that the SSL there is significant additional overhead in starting up an SSL session

B. The SSL Record protocol, in which the session data is exchanged between the communicating parties (client and the server) in an encrypted fashion. SSL is a great boon to the traditional network protocols, because it makes it easy to add transparent confidentiality and integrity services to an otherwise insecure TCP-based protocol. It can also provide authentication services, the most important being that clients can determine if they are talking to the intended server, not some attacker that is spoofing the server. SSL is currently the most widely deployed security protocol. It is the security protocol behind secure HTTP (HTTPS), and thus is responsible for the little lock in the corner of your web browser. SSL is capable of securing any protocol that works over TCP. An SSL transaction starts with the client sending a handshake to the server. In the server's response, it sends its certificate. As previously mentioned, a certificate is a piece of data that includes a public key associated with the server and other interesting information, such as the owner of the certificate, its expiration date, and the fully qualified domain name associated with the servers

5.1.1 Problems with SSL
SSL is an excellent protocol. Like many tools, it is effective in the hands of someone who knows how to use it well, but is easy to misuse. There are many pitfalls that people fall into when deploying SSL, most of which can be avoided with a bit of work.

a) The merchant cannot reliably identify the cardholder. In cases where customers use stolen credit cards to initiate e-commerce transactions, merchants are responsible for card not present transaction charge backs. While SSL/TLS does provide the possibility of client authentication with the use of client certificates, such certificates are not obligatory and are rarely used. Furthermore, even if the client possesses a certificate, it is not necessarily linked with his cred it card. This means that the client might not be authorized to use the credit card in question.
b) SSL/TLS only protects the communication link between the customer and the merchant. The merchant is allowed to see the payment information. SSL/TLS can neither guarantee that the merchant will not misuse this information, nor can it protect it against intrusions whilst it is stored at the merchants' server.
c) Without a third-party server, SSL/TLS cannot provide assurance of non-repudiation. So SSL protocol does not provide facilities for non-repudiation.
d) SSL/TLS in discriminately encrypts all communication data using the same key strength, which is unnecessary because not all data needs the same level of protection.
e) M ITM attacks: MITM attacks pose a serious threat to many relevant SSL/TLS-based applications, such as Internet banking and remote Internet voting's.

5.1.2 Efficiency
SSL is a lot slower than a traditional unsecured TCP/ IP connection. This problem is a direct result of providing adequate security. When a new SSL session is being established, the server and the client exchange a sizable amount of information that is required for them to authenticate each other and agree on a key to be used for the session. This initial handshake involves heavy use of public key cryptography, which, as we've already mentioned, is very slow. It's also the biggest slowdown when using SSL. On current high-end PC hardware, Open SSL struggles to make 100 connections per second under real workloads. Once the initial handshake is complete and the session is established, the overhead is significantly reduced, but some of it still remains in comparison with an unsecured TCP/IP connection

5.2 Secure Electronic Transaction (SET) Protocol

To carry out transactions successfully and without

compromising security and rust, business communities, financial institutions and companies offering technological solutions wanted a protocol that works very similar to the way how a credit card transactions work Visa and MasterCard, leading credit card companies in the world formed a consortium with computer vendors such as IBM and developed an open protocol which emerged as a standard in ensuring security, authenticity, privacy and trust in electronic transactions.

The main business requirements for SET are:

1. Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
2. Ensure the integrity of all transmitted data.
3. Provide authentication that a cardholder is a legitimate user of a branded payment card account.
4. Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring Financial Institution.
5. Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
6. Create a protocol that neither depends on transport security mechanisms nor prevents their use.
7. Facilitate and encourage interoperability among software and network provider

The goal of SET is to ensure that the payment process is private, convenient and most-important-of-all-secure.
SET ensures that the order and payment information of the customers are kept confidential. SET also has the capacity to authenticate the customer is the legitimate user of the credit account. The payment process is easy and simple. When the customer made a purchase, the SET will authenticate the credit card against the details provided by the customer, and then the merchant which is the online store will send the order details to the bank. Transaction will occur between the two for the approval of the purchase. When approved the bank will digitally sign and an authorization will be given to the merchant who can then process the order. This type of e-commerce technology is truly a breakthrough in online shopping and-transactions. The e-commerce technology developed are very important in the online e-commerce especially the secure payment system. It provides the customers a piece of mind when doing Internet transactions. Now customers will be safe against scams. A reliable e-commerce technology is truly what we need.

5.2.1 Disadvantages of SET are as follows

1. Implementing SET is more costly than SSL/TLS for merchants as well. Adapting their systems to work with SET is more complicated than adapting them to work with SSL/TLS. Furthermore, merchants must have accounts opened at business banks capable of handling SET transactions.
2. Business banks must hire companies to manage their payment gateways, or install payment gateways by themselves.
3. Despite being designed with security in mind, SET also has some security issues. In a variant of the SET protocol, the merchant is allowed to see the customer payment information. Just as with SSL/TLS. There are also some other, minor security issues in this protocol
4. SET employs complex cryptographic mechanisms that may have an impact on the transaction speed.
5. Despite being very secure, SET has not been a success in e-commerce environments. The reasons attributed are the overheads associated with SET are heavy.
6. For a simple purchase transaction:
7. Four messages are exchanged between the merchant and customer
8. Two messages are exchanged between the merchant and payment gateway.
9. 6 digital signatures are computed.
10. There are 9 RSA encryption/decryption cycles.
11. There are 4 DES encryption/decryption cycles and four certificate verifications.
12. It has been argued by merchants that they have to expend lot of money in order to process SET transactions. From consumer's point of view, they have to install appropriate software.
13. Inter-operability problem has not been solved.
14. With SET, while the payment information is secure, order information is not secure.

5.3.3 D Secure

The main advantage over SSL/TLS is that 3-D Secure provides credit card authorization and non-repudiation. 3-D Secure is built upon the relationships between three domains, named the acquirer, the issuer, and interoperability domains .The acquirer domain covers the relationship between the merchant and the acquirer. The issuer domain covers the relationship between the cardholder and the issuer. The interoperability domain supports the relationship between the acquirer and issuer domains. To protect the security of communication between the various entities, 3-D Secure requires the following links to be protected using SSL/TLS: cardholder merchant, cardholder-ACS, merchant Visa Directory, and Visa Directory-ACS (access control sever)

Disadvantages

The merchant still has access to the payment information, and all information is encrypted using the same key strength. The main advantage over SSL/TLS is that 3-D Secure provides credit card authorization and non-repudiation. On the other hand, prior customer registration is required

5.4 Cyber Cash

The Cyber Cash provide several separate payment services on the Internet including credit card and electronic cash. Cyber Cash uses specialized software on the merchant and customer's sides of the connections to provide secure payments across the Internet.

5.5 The Secure electronic payment system using secure communication tunnel.

Secure electronic payment system consists of four system participants (segments). The communication between the participants goes through secure communication tunnels.

5.5.1 Secure Communication tunnel

Means provide a secure way for communication between two or more parties or segments, i.e., Customer to merchant and merchant to payment gateway.

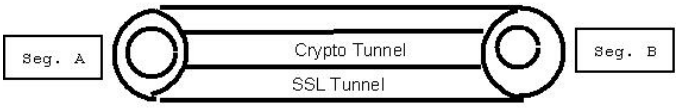

Figure 2: Secure communication tunnel consists of SSL and nested crypto tunnel.

Secure communication tunnel consists of SSL and nested crypto tunnel, which is created by employing cryptographic algorithms and techniques on the information that are transmitted between parties. The SSL is based on session key and Crypto tunnel is based on public key cryptosystem. These Secure communication tunnel are work between customer to merchant and merchant to payment gateway and transfer data securely.

5.5.2 Working of Tunnel

The customer decides to buy something and open the merchant's web site. Customer sees many item of merchant web site. At this time web server and our browser communicate through HTTP Protocol. To be securing this system, secure communication tunnel and key cryptosystem is used to protect conventional transaction data such as account numbers, amount and other information.

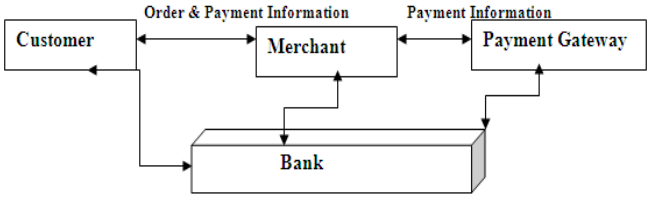

Figure 3: Secure Communication tunnels between Customer, Merchant and payment gateway

The web payment segment creates two messages
1.The first message contains order information
2.The second message contains payment information- credit card number and other information like credit card type and expiration date. The order information is encrypted using symmetric session key and digitally signed using customer's private key. The payment information is double encrypted, first time using payment gateway public key and second time using symmetric session key. Merchant cannot peek the payment information because of the payment information is also digitally sign with the customer's private key.

6. Comparison of Security Schemes For Secure Payment System

Table 1: Comparison of SSL, SET 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 table-1 above outlines the key differences and similarities of major security schemes for any secure payment system.

6Encryption: AES versus Triple-DES

As depicted in the table-2 below, all Good Link messages are encrypted end-to-end using the Advanced Encryption Standard (AES). AES is a Federal Information Processing Standard (FIPS) selected by the U.S. National Institute of Standards and Technology (NIST) for its combination of resistance to attack, ease of implementation, efficiency, and scalable design. All Good Link clients (Mobitex, Palm OS, and Microsoft Windows Mobile 2003) support Good's implementation of AES.

Table 2: AES versus Triple-DES

	AES	Triple-DES
Description	Advanced Encryption Standard	Triple Data Encryption Standard
Timeline	Official standard since 2001	Standardized 1977
Type of algorithm	Symmetric	Symmetric
Key size (in bits)	192	168
Speed	High	Low
Time to crack (assume a machine could try 255 keys per second - NIST)	149 trillion years	4.6 billion years
Resource consumption	Low	Medium

7. Conclusion

The work proposed reviews the Secure Electronic Payment schemes through SSL, SET, and Secure communication Tunnel. The security techniques are incorporated to provide security for the customers to be able to purchase the desired items on the Internet through Electronic Transaction. The system shall ensure the security of such a transaction, making it a reliable and an efficient solution to any E-business model. The primary benefits of such a Payment System over Internet are many folds: it uses strong cryptographic and authenticity checking models, thus improving the security; the merchant is prevented from seeing payment information, thus improving the privacy; as a result the customer has the freedom to use the system safely. Additionally, as the customers can use such a system

without having the additional software installed, he / she can rely on these secure payments or can rely to have a digital certificate. It is evident from the literature that with the use of security principle for secure communication channels, it provides the significant level of protection over unsecured communication channels.

References

[1] Yin, Y. "The RC5 Encryption Algorithm: Two Years On." Crypto Bytes, winter 1997.
[2] ELECTRONIC CASH AND SET, Paper presented at the conference: Internet Crime held in Melbourne, 16-17 February 1998.
[3] Yin, Y. "The RC5 Encryption Algorithm: Two Years On." 1997.
[4] Gary C.Kessler, N.Todd Pritsky,"Internet Pay ment Systems: Status and Update on SSL/TLS, SET and IOTP" Information Security Magazine August 2000.
[5] 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.
[6] Z. Dju ric, Securing money transactions on the Internet, 2005.
[7] Z. Djuric, Secure internet payment System "ITCC-2005.
[8] Yann Glouche1, Thomas Genet1, Olivier Heen2, Olivier Courtay2, a Security Protocol Animator Tool for A VISPA, 2005.
[9] 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
[10] Baja and Nag, "E-Commerce" TM H Publications.
[11] W .Stallings, 1998 "Cryptography and Network Security", Th ird Ed ition, 2006.
[12] Kaliski Jr, B.S. and Yin, Y. L., September 1998. "On the security of the RC5 Encryption Algorithm",2006.
[13] Yun Ling, Yiming Xiang, Xun Wang "RSA-BASED SECURE ELECTRONIC CASH PA YM ENT SYSTEM" Proceedings of the 2007 IEEE IEEM .
[14] Z. Djuric, Ognjen Maric "Internet payment System", Journal of University computer Science-2007
[15] A R Dani1, P Radha Krishna and V Subramanian "An Electronic Pay ment System Architecture for Composite Pay ment Transactions" 2007.
[16] Pyae Hun,"Design and Implementation of Secure Electronic Pay ment System (Client)" World Academy of Science, Engineering and Technology 48, 2008.
[17] 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.
[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
[19] 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 ".

Author(s) Profile

Gangadhar Sajjanar received Bachelor of Computer Science Engineering from Visvesvaraya Technological University, Belgaum, Karnataka. He is now pursuing Master of Technology in Computer Network Engineering. His research interests are Secure Gateway in Payment System for Electronic Transaction.

Akram Pasha, Associate Professor, Department of Computer Science and Engineering, Reva Institute of Technology and Management, Bangalore, India.