

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Security Issues and Solutions in E-Payment Systems

Amitesh Yadu¹

(Author)

Computer Science Department,
School of Information Technology,
MATS University,
Raipur, C.G., India.

Dr. Vaibhav Sharma²

(Guide)

Computer Science Department,
School of Information Technology,
MATS University,
Raipur, C.G., India.

Abstract: *Today, through e-commerce, we are adopting several methods of payment, so that we have been prioritizing the cash less system in our business and in our shopping, this method of payment is giving us a very convenient experience when you buy goods and services, you pay online those using electronic means. This method of payment without using Real cash or check is called e-commerce payment system and is also known as online or electronic payment systems. Today e-commerce is giving us the opportunity to use many new technologies. In which we can using internet banking, mobile payment, debit card, credit card, QR scanning and e-check smart card, e-wallet, e-cash, and ATM machine through bank services. We can do tasks like exchange and payment very easily. The purpose of this study is to identify the issues and challenges of electronic payment systems and to present some solutions to improve the quality of e-payment systems.*

Keywords: *Cyber Cash Digital Signatures; e-Cash; Electronic Payments; Encryption; First Virtual Holdings; Net Bill; Issues and Challenges; Electronic Payment System.*

I. INTRODUCTION

An electronic payment system is a method of payment over an electronic network such as the Internet. In other words we can say that e-payment is a method in which a person can pay online without physical transfer of cash and check, regardless of time and place. Electronic payment system is the basis of on-line payment and on-line payment system development is a high form of electronic payment. It makes electronic payments at any time via the Internet to manage the e-business environment.

In the real world we have two different types of payment systems

A. Internet –Based payment system

There are four models of Internet-Based payment system:

1. Credit Card
2. E-cash
3. Smart Card
4. Debit Card

B. Electronic Transaction-Based payment system

1. Cyber Cash
2. Net Bill

3. First Virtual Holdings
4. Secure Electronic Transaction

II. OBJECTIVES

- To create awareness about various frauds of electronic payments.
- Creating awareness about various methods of online payment systems.
- To motivate people to use online payments systems.
- To make online payments safe and secure.

III. PAYMENT SYSTEM OVERVIEW

A. Credit Card

A credit card is a plastic card issued to users to lend money to purchase goods and services. The customer types the card number, expiry date and billing address on the order form and the seller can verify the details and be confident about the payment.

Credit card payments on online networks can be classified into three types:

1. Payment using plain credit card statement
2. Payment using encrypted credit card details
3. Payment using third party verification.

B. E Cash

E-Cash is a truly software-based, anonymous, inaccessible, online token payment method, available on the Unix, Windows and Macintosh platforms. When the token purchased by the customer, e-cash software stores the digital money on the customer's personal computer which is signed by the bank. Users can easily spend digital money at any shop that accepts e-cash without giving credit card details to the shopkeeper. And an example of the cash less method.

C. Smart Card

It is a thin, credit-card-sized portion of plastic with a half-inch square area that serves as the card's input-output system. A smart card was first created by Motorola in 1977. Smart card consists of a programmable and compact chip, a combination of RAM and ROM storage. And it can be self-connected by connecting it to the bank. This is known as a smart card because the chip's quality of storing information in its memory makes the card smart.

D. Debit Card

A debit card is a banking card that is enhanced with automated teller machines and point of sale features so that it can be used at merchant locations. A debit card is linked to a person's bank account, allowing funds to be withdrawn at the ATM and point of sale without writing on the check. A debit card holder pays for his purchases directly through the bank. It replaces physical cash and checks. In the debit card system, customers deposit in advance with the bank and withdraw at the time of purchase. There are two types of debit cards that are used in the real world:

1. Online Debit Card
2. Offline Debit Card

E. Cyber Cash

Cyber cash is a web-based service that automatically processes and verifies the customer's credit card information and then electronically credits the customer's account. Cyber cash servers act as a gateway between the Internet and the merchant's secure financial network. This system uses digital signatures for the purpose of security in electronic payment systems

F. Net Bill

Net Bill is a micro payment system. Net bill payment systems use the Internet to purchase goods and services and make secure and affordable payments for them. The net bill server maintains an account for both consumers and merchants, which allows merchants to pay to deliver goods to customers. Goods are delivered digitally. There is money tool software that verifies the receipt of goods. So, the electronic payment net bill system enables communication between money tools, merchant servers and net bill servers.

G. First Virtual Holdings

The first virtual is one of the first Internet payment systems that offered a third-party verification method to make payments over the Internet. The first pragmatic payment system is unique in the sense that it does not use encryption. A fundamental philosophy of payment systems is that some information should not travel on the Internet because it is an open network. This information is basically related to credit card information. Instead of using a credit card number, the transaction is completed using a virtual PIN first issued by the virtual company. These PIN numbers can be sent over the Internet as it acts like an ID and no merchant can charge a user's account without receiving an email with them.

H. Secure Electronic Transaction

Secure electronic transactions are a system of online payment to ensure the security of financial transactions over the Internet. The SET specification is an open, technical standard for commerce, invented by Visa and MasterCard. It provides facility to secure payment card transactions over the Internet. The digital certificate makes a change in the confirmation of the entire transaction, cardholders and merchant validity.

I. Online Check/Electronic Fund Transfer

While transacting with an online check, a buyer enters the digits or numbers found on the check. This is done for the purpose of authorization whereas in electronic fund transfer, there is a financial house, called an Automated Clearing House (ACH), which completes the transaction from the buyer's or promoter's account to the seller's recipient or recipient's accounts is responsible for transferring funds.

IV. ISSUES AND CHALLENGING REGARDING ELECTRONIC PAYMENT SYSTEM

A. Lack of Usability

Electronic payment systems require large amounts of information from end-users or make transactions more difficult using complex detailed websites interfaces. For example making a credit card payment through a website is not the easiest way because this system requires a large amount of personal data and contact details in a web form.

B. Various Issues With E-Cash

The main problem of e-cash is that it is not universally accepted as it is necessary that business establishments accept it as a payment method. Another problem is that when we make payments using e-cash, customers and salesmen have accounts in the same bank that issues e-cash. Payment is not valid in other banks.

C. Lack of Security In E Payment System

The online payment system for the Internet is an easy target for stealing money and personal information. Customers must provide credit card and payment account details and other personal information online. This data is sometimes transmitted in a non-secure way, (Kolkata and Winston, 1997). Providing these details by mail or over the telephone also increases security risks (Gutman, 2003, Loudon and Traver, 2002).

D. Lack of Trustiness

Electronic payments have a long history of fraud, misuse and low credibility as well as a new system without establishing a positive reputation. Potential customers often refer to the risk of why they do not trust paid services and therefore do not purchase the Internet (Littaire, 2002)

E. Lack of Awareness

Paying online is not an easy task. Even educated people face problems in paying online. Therefore, they always prefer the traditional way of shopping rather than online shopping. Sometimes there is a technical problem in the server, customers try to pay online, but they fail to do so. They avoid it as a result.

F. Online Payments Are Not Suitable In Rural Areas

The population of rural areas is not very educated and those who are few rural literates are also not able to operate computers and mobiles. Since they are unaware of technological innovations, they are not interested in online payment. So online payment system is not possible for the villagers.

G. User Perception About Acceptance Of Electronic Payment Systems

User acceptance is an important factor determining the success or failure of any information system project. (Davis, 1993), several studies on information technology report that user information and human factors are important aspects influencing the success of any information system (Davis, 1989, Burckhardt, 1994, Rice & Edin, 1991). According to Dillian and Morris (1996), users' acceptance is a "willingness to work within a user group that is willing to employ information technology for tasks that are designed to support it". Electronic payment systems are no exception. This means that they are not successful without the approval of the users. Electronic payment system is an innovative method for online payment. Issues are not easily accepted due to lack of security in the changing business environment. There is a need for improvement of information technology in online payment systems. The failure of electronic payment systems depends on the factor that ignores the needs of users and the market.

H. Highly Expensive and more Time Consuming

The electronic payment system is highly expensive because it includes set costs, machine costs, management costs etc. and this mode of payment will take longer than the physical mode of payment.

V. E-COMMERCE SECURITY TECHNOLOGY SYSTEM

A. Physical System Security

According to national standards, information security level and financial status, the security, the location hosting your E Commerce applications (usually a data center) needs to be physically secure and with development of appropriate physical security requirements and the construction and management to achieve the relevant standards. In addition to application security and network proper secure operating procedures. The main system must be resources (including hosting, application server, security, GAP and other equipment), communication circuitry, as well as physical media (soft / hard disk, CD-ROM, IC card, PC card, etc.). Security measures such as encrypted, electromagnetic shielding, etc. should be kept in a physically safe place.

Computers that host web servers and database servers must be physically located in a secure facility, typically a secure data center.

B. Network Security

Network security refers to the security of operating systems and servers. Hackers can gain some control over your operating system or server by discovering flaws in the operating system and server software. To ensure smooth progress of e-commerce transactions, stable and reliable e-commerce platforms should be able to provide services without any hindrance. An e-commerce system may not function as a result of any system interruption (eg hardware, software errors, network failures, viruses, etc.) Barring business data, in determining the effectiveness of time and space, cannot often be guaranteed, often causing great economic losses.

C. Data Transmission and Application Development

Mainly refers to business transactions appearing in the media in network security issues, including the prevention of theft, tampering, forgery of business information, was to negate the Business Act, namely, confidentiality, integrity, E-commerce to achieve authenticity, non-vengeance. All sensitive information being transmitted must be encrypted. Businesses may choose to refuse customers who cannot accept this level of encryption. Confidential and sensitive information should never be sent via e-mail. If it should, it should also be encrypted.

D. System Administration Security

Primarily to protect the operating system and database system of the host computer. To protect system security, the overall idea is: to address management of security vulnerabilities through reinforced security; and then use security technology and equipment to enhance your security capabilities. System administrators should monitor suspicious activity within the business by inspecting log files and repeatedly researching logon failures. They can also audit their e-business systems and look for any holes in security measures.

E. Safety Management Process Supervision in E-Commerce

It is necessary to strengthen the network planning phase, the creation and management of information security planning. There is a need to invest some amount of manpower, material and financial resources for information security-building. As per the situation to set realistic network security goals and milestones implemented in phases to minimize investment risks.

VI. OVERCOMES OF PROBLEMS IN ELECTRONIC PAYMENT SYSTEM

A. Encryption

Online shopping is very sensitive to the notion that e-commerce is insecure, especially when it comes to online payment. Most online payment systems use an encryption system to add security to the transmission of personal and payment details to conduct all online shopping. There are various encryption schemes to prevent online payment fraud.

B. Digital signature

The parties involved in online payment must use digital signature in the transaction to ensure authentication of the transaction.

C. Firewall

A firewall is a unified collection of security measures designed to prevent unauthorized electronic access to a networked computer system to protect private networks and individuals machines from over-the-Internet threats, with firewalls coming in or out of predefined grounds Can be employed to filter outgoing traffic. The set of rules called firewall policies.

The firewall has 3 policy actions:

1. Accepted: Permitted through the firewall.
2. Dropped: Not allowed through with signs of failure.
3. Rejected: Not allowed through an attempt to notify sources that the packet was rejected.

There are two fundamental approaches to creating firewall policies to reduce vulnerability to the outside world while maintaining the functionality that machines desire in trusted or individual computers. Here are:

4. Black List Approach
5. White List Approach

VII. CONCLUSION

Electronic payment refers to the mode of payment that does not include physical cash or checks. This includes debit cards, credit cards, smart cards, e-wallets, etc. The use of payment methods in e-commerce is the main link for its development online, some of which we have analyzed in this work. This is the risk. Online payment is theft of payment data, personal data and fraudulent rejection on behalf of customers. Therefore, and until the use of electronic signatures is widespread, until then we must use the available technology to guarantee a reasonable minimum level of security on the network. With regard to the payment methods analyzed in this work, it is impossible to say that any one of them is perfect, although each of them has advantages unlike the others. If customers want to maintain privacy, So they choose payment methods that guarantee high levels of privacy such as e-cash or net bill checks. If the priority is security, they should use a smart card. Both consumers and service providers can benefit from the e-payment system, which will increase national competition in the long run. Successful implementation of electronic payment systems depends on how the security and privacy dimensions are handled by consumers as well as vendors, which in turn will improve market confidence in the system.

References

1. Bhasker, Bharat (2013). Electronic Commerce, Framework, Technologies and Applications. McGraw Hill Education (India) Private Limited., p.9.2-9.16.
2. Chhabra, T.N., Suri, R.K., Verma, Sanjiv (2006). E-Commerce. Dhanpat Rai & Co. (P) Ltd. p.306-328.
3. Preeti Dhankar(2012). E-Commerce online payment security issues discussion and analysis
4. http://ecommerce.insightin.com/internet_security/physical_security.html
5. http://ecommerce.insightin.com/internet_security/network_security.html
6. http://en.wikipedia.org/wiki/Electronic_business.html

AUTHOR(S) PROFILE



Amitesh Yadu, received B.IT from Manipal Academy of Higher Education in 2003 and the Advance diploma in Software Engineering in 2003, M.Sc. degree in Information Technology from Guru Ghasidas University(GGU), Bilaspur in 2008 and M.B.A degrees in Management from Sikkim Manipal University in 2010. Since 2009, He is a Computer Programmer in Panchayat State Government Institute. And doing Ph.D. in Computer Science from MATS University, Raipur (C.G.)