Privacy and Security Issues in E-Commerce: A Survey

Ms. Ruchi Oberoi  
Assistant Professor, MCA  
Institute of Management Studies, Ghaziabad

Ms. Sharmistha Dey  
Assistant Professor, MCA  
Institute of Management Studies, Ghaziabad

Shourabh Sholliya  
Assistant Professor, MCA  
Institute of Management Studies, Ghaziabad

ABSTRACT

Electronic commerce (or e-commerce) refers to buying and selling of goods and services through the internet. At the time of doing e-commerce transactions, confidential or personal information is stored in the database and also can be communicated through network channels. Hence Security and Privacy are the major concern while doing e-commerce transactions. E-commerce applications are also susceptible to various security threats which will lead to loss of customer’s confidence while doing online shopping. In this paper we have discussed about various privacy and security issues related to e-commerce, purpose of security in e-commerce, security tools used in e-commerce and also various guidelines to be followed when shopping online.

Keywords  
E-commerce, Privacy, Security, Authentication, Confidentiality, Security Threats

INTRODUCTION

E-commerce refers to doing shopping over the Internet. Security and privacy are the major concern that restricts the customers and organizations doing online shopping. In E-commerce, various payment applications like online banking, debit card, credit card, PayPal, PayUMoney and other tokens are at increasing risk of being misused and there is a greater chance of loss and modification of data. Due to the increasing growth and usage of E-commerce, privacy has become an increasing concern for the users, providers, technologist and policy makers. The transaction will not be completed by the user of e-commerce, if it does not provide confidential information and to protect that information from propagating is another very complex task for the providers, technologist and policy makers.

LITERATURE REVIEW:

As security and privacy of the confidential information is one of the major concern that restrict the customers doing online shopping. The main aim of this paper is to explore the perception of security and privacy in e-commerce from both the customers and the organizations point of view[1]. Due to the growth of e-commerce, security and privacy issues are also taken into consideration as the security of the transaction is the foundation for the growth of e-commerce. This paper promotes security solutions from point of view of technology and system which will help to promote and expand e-commerce further.

On one hand owners of the E-commerce websites think of how to attract more customers so that they feel more secure when working on the website and on the other hand in what way the end – users should rate an e-commerce website and in what way they can protect themselves as one among the online community. The main aim of writing this research paper is to make the reader understand about the technology that helps them do various online transactions securely along with the safety tips and in what way owners of the e-commerce website can make their online visitors more comfortable and trustful using various Trust marks [2].
Due to the increase in various security and privacy breaches such as identity theft and financial fraud and also online customers are aware of the fear of performing online transactions; e-commerce has not been able to achieve its full potential. Most of the customers are still reluctant to perform online transactions and relate that to lack of trust and fear of their confidential information getting misused[3].

The traditional authentication mechanism is based on identity to provide security or access control methods; besides this, traditional encryption and authentication algorithm require high computing power of the computer equipment. Thus, in what way we can improve the authentication mechanism and optimize the traditional encryption and authentication algorithm can possibly be the focus of P2P e-commerce[4].

Information security is therefore an essential management and technical requisite for any efficient and valuable payment transactions done over the internet. Still, its meaning is a complex endeavour due to the constant change in the technological and business requirements and also requires a coordinated match of the algorithm and its technical solutions[5].

**DIGITAL E-COMMERCE CYCLE**

Security is considered very significant in doing online shopping. Nowadays anything can be purchased over the internet such as apparels, music, toys, books, TV’s, cars, grocery items, cosmetics though various websites like Amazon, Myantra, Flipkart and many more.

![Fig 1: E-Commerce Payment system [6]](image)

In the above figure, the user enters the data in the computer; if all the information is correct then the next step is done. In the next step the user enters the credit or debit card information for making the payment. Once the order is complete, the e-mail is sent to the customer and the merchant. In the next step, the company sends the product which is ordered to the customer’s address.

**SECURITY TOOLS**

- **Public Key Infrastructure (PKI)**: It is a technology that can be used to establish identities, encrypt information and digitally sign the document. It identifies and manages relationship of the parties in an electronic exchange serving a wide range of security needs that includes access control, confidentiality, integrity, authentication and non-repudiation. It uses unique digital certificates to secure e-commerce transactions.

- **Proxy Servers**: When a proxy server receives a request for an Internet (Web page), it looks in its local cache. If it finds the page in the cache, it returns it to the user without forwarding the request to the Internet. If the page is not to be found in the local cache, the proxy server uses one of its own IP addresses to request the page from the server on the Internet. Once the page requested for is returned, the proxy server relates the page returned to the original request and forwards it the user. In an
enterprise, proxy servers are mainly used for security purpose, administrative control and also provides for caching services. In personal computer, proxy servers are used to achieve user privacy and anonymous surfing.

- **Encryption Software**: it is software that uses cryptography to prevent unauthorized access to the digital data. In encryption, the electronic data is translated into cipher text, so that it cannot be easily understood by anyone except the authorized person.

- **Digital Certificates**: It is a data structure which is used in the public key system which can be used to securely bind an authenticated individual to a particular public key. Digital certificates are issued by a third party who is known as a Certification Authority such as VeriSign. The responsibility of the third party certification authorities is to confirm the identity of the certificate holders and also guarantees the website visitors that the website is trustworthy and is capable of serving them in a trustworthy manner. Thus Digital Certificates provides an electronic means of identifying someone’s identity and it is used in conjunction of the encryption, it provides more complete solution.

- **Digital Signature**: It is an electronic signature that provides verification to the recipient that the price has come from the person who has sent it, and has not been altered since it was signed. Thus Digital Signature secures electronic transactions by including authentication, confidentiality, integrity and non-repudiation.

- **Firewall**: A Firewall is a device or a group of devices, that controls access between networks. It consists of gateways and filters. Normally Firewall runs a monitoring software that can be used to detect and prevent external attacks on the site and can be used to protect internal corporate networks.

**PURPOSE OF THE SECURITY [7]**

- **Data Integrity**: Data Integrity refers to trustworthiness of data or resources. Data integrity is used to ensure that the message has not been tempered with after it leaves the sender but before it reach the receiver. It is implemented using message digest or hashing.

- **Access Control**: Access control governs what resources users can access on the system. Proper Valid ID’s and passwords are needed to be used.

- **Data Confidentiality**: It refers to limiting access and disclosure of information to authorized user and preventing access or disclosure to unauthorized users. This is done using Encryption/Decryption technique.

- **Authentication and Identification**: It helps in verifying the identity of the user, by using specific credentials like passwords, locks, token etc. It guarantees that someone is who he or she claims to be is implemented with digital signatures.

- **Non-repudiation**: It prevents either sender receiver from denying a transmitted message. Thus when a message is sent, the receiver can prove that the alleged sender has actually sent the message. Similarly when a message is received, the sender can prove that alleged receiver has in fact received the message.

**SECURITY ISSUES:**

E-commerce security refers to protection of e-commerce assets against unauthorized access, use, modification or destruction. Online privacy and security of the confidential information are the major components of E-commerce. Privacy is connected with legal requirements and good practices regarding the management of personal data and security refers to the technical aspects of the management and protection [8]. Protecting user data from online fraud cannot be achieved without proper security. Security features are therefore necessary to build a secure system but they does not always guarantee a secure system.

There are certain security features which are considered important. They are:
• **Integrity**: Data Integrity guarantees that the data which is transmitted is correct and consistent and has not been altered during transmission.

• **Authentication**: It refers to establishing the identity of one party to the other. Once the authentication to a system is performed correctly, the user is authorized to perform further actions. In e-commerce, the customer has to prove his identity by giving personal information (credit card number etc.)

• **Non-repudiation**: It refers to the ability to ensure that the parties that are engage in e-commerce do not deny their online actions. E.g. the customers ordering products online and later denying that he or she has done so.

• **Encryption**: deals with Information hiding through the use of mathematical formulas’ or keys. It ensures that you cannot spy on others during internet banking transactions.

• **Privacy**: Information exchanged must be kept from unauthorized parties.

• **Available**: It ensures that access data or computing resources needed by the appropriate personnel are both reliable and available in a timely manner.

• **Auditing**: Merchant use auditing to prove that you bought specific merchandise.

**SECURITY THREATS [9]**

A security threat is an object, person or other entity that represents a constant danger to an asset. Management must be educated about different kinds of threats that are faced by the organization. Management can effectively protect information through policies, education, training and technology by investigating each type of threat. There are various threats to e-commerce security. Despite of latest technologies and many issues with the websites, there is still no way to make your e-commerce website completely secure.

• **Authentication Attacks**: It refers to the type of attacks that occurs when a user changes system resources or gains access to system information without authorization by either sharing logins or passwords or using an unattended terminal with an open session. Password attack refers to the method of repeated attempts to identify the user account and the password. These repeated attempts are called brute-force attack. These types of attacks are performed using the program that runs across a network and attempts to login into a shared resource such as a server.

• **Integrity Attacks**: In this type of an attack, the attacker can change, add or remove the message while it is in transit between the sender and the receiver. It requires root access to the router or the system. If the program does not check the buffer limit, while it is reading or receiving the data, this opening can be misused by an attacker and he can add any arbitrary data into the program or a system. Hence while running, this data gives the intruder root access to the system. This integrity attack can cause a delay as data will be unavailable for a certain period of time or either it will be held. The attacker floods the network with useless traffic, because of that system becomes tremendously slow to serve the customers and in extreme case, causes the system to crash down. They could also cause the data to be discarded before the final delivery. Both the delay and denial attacks can cause denial of service (DOS) to the network user.

• **Confidentiality Attacks**: Even if network communicates in parallel but network computers communicate serially and contain limited immediate buffers, data and information are transmitted in small blocks called packets. Hackers use a verity of methods to attack the computers. With the use of loads of shareware and freeware packet sniffers available, the attacker would capture all network packets and also the user login names, passwords and also their accounts. Most of the times, the attackers are successful in gaining access to the corporate sensitive and confidential information. The attackers also take advantage of the human tendency e.g. using the small password for the multiple accounts. Some snooping attacks place the network interface card in promiscuous mode, while other packet sniffers capture the first 300 bytes of all the telnet, file transfer protocol (FTP) and login sessions.
• **Viruses**: They are the most widely known security threats. Viruses are computer programs that are written by devious programmers [11]. These programs are designed to replicate themselves and infect specific computer when triggered by a specific event. E.g. viruses called macro viruses attach themselves to the files that contains macro instructions (routines that can be repeated automatically) and are then activated every time whenever the macro runs. But some viruses can be very frustrating causing interruptions like displaying some comical message when pressing a certain letter on the keyboard. Other types of viruses are very destructive and can cause problems such as deleting files from the hard-disk or slowing down a system. A network can also be infected by virus only if the virus enters the network through the outside source e.g. through an infected pen-drive or files downloaded from an internet. When one computer on the network becomes infected then other computers on the network are also vulnerable to contracting the virus[10].

• **Trojan Horse**: It is a program that appears to the user as harmless, it is in fact malicious which means that it requires users to invite in, and is therefore disguised as something else. A Naïve users will allow Trojan in to their machine through a harmless and routine task, only to have their system compromised. This malicious code is hidden within some program. E.g. An email alert regarding a new security patch. The e-mail might provide a link, inviting the user to click on to it, download and install the patch. When the unsuspecting user clicks on the link, this malicious code gains access to the user’s computer and then executes its programmed task. With Trojan horse a hacker can gain access to a large network or a secure system so that it can use for its own personal gain[11].

• **Worms**: They are malicious programs designed to spread through a computer networks. Worms spread from one computer to another computer but unlike a virus, it has the capability to travel without human intervention. The major threat with the worm is that it has the capability to replicate itself on your system which means instead of sending out a single worm, it would send out hundreds or thousands of copies of itself thus creating a destructive effect. E.g. worm would send a copy of itself to everyone listed in your e-mail address book. They may also open TCP ports to create network security holes for other applications, and they may also attempt to flood the network with spurious Denial of Service(DoS) data transmission. Being embedded inside the network software, computer worms can easily penetrate to most firewalls and other network security measures [11].

• **Database Threats**: E-commerce system stores user’s confidential data and also retrieve product details from the database which is connected to the web-server. Besides storing product details, database connected to the web also contains valuable and private information that could damage the company’s reputation if that information were disclosed or altered. Some database also store username and password pairs in a non-secure way. If someone gets hold of this user authentication information, then he/she can masquerade as a legitimate database user and reveal the personal and valuable information.

**SECURE ONLINE SHOPPING GUIDELINES [12]:**

1. **Shop at secure websites**: Secure websites always use encryption technology to transfer information from your computer to online merchant’s computer. Encryption technology scrambles the information you send e.g. your credit card number, so as to prevent computer hackers from obtaining that information while in transit. Only those persons who have legitimate access privileges can only unscramble the code. There are different ways, you can tell whether you are dealing with a secure website:
   - If you look at the top of the screen where the website address is displayed (Address bar), you should see https://. The “s” that is displayed after “http” indicates that the website is secure. Often you do not see the “s” until you actually move to the order page on the web site.
• Another technique to determine whether the website is secure, is to look for closed padlock displayed in the address bar of the screen. If that lock is open, it means that it is not a secure site.

2. **Research the Website before you order:** Do business with the company you already know. If a company is unfamiliar, check for the privacy policies before buying their products. If you decide to buy something from an unfamiliar company, start out with a less costly order before you learn if a company is really trustworthy or not. Trustworthy companies always advertise their business address and at least one phone number, either customer service or an order line. Call the phone number and ask questions to determine if the business is legitimate.

3. **Read the website's privacy and security policy:** Every website that has a good reputation offers information about how it processes your order. It is usually listed in the section entitled –Privacy Policy. You can find out if the merchant intend to share your information with a third party. You can also learn about what type of information is gathered by the website, and how it shares this information with others. But however be aware that a strong privacy policy does not guarantee that the merchant will protect your privacy forever. Policies can change.

4. **Be Aware of cookies and Behavioural Marketing:** Online merchants as well as other sites watch our shopping and surfing habits by using “cookies” (an online tracking system) that attaches a piece of code to our internet browsers to track which sites we visit as we search the web. “Persistent cookies” remains stored on your computer while “session cookies” expires when you turn off the browsers. Online merchants use cookies to recognize you and speed up the shopping process that next time you visit. You may be able to set your browser to disable or refuse cookies, but doing this will limit the functions you can perform online and possibly prevent you from ordering online. Usually, you need to enable session cookies to place an order.

These simple guidelines should be followed when ordering online.

**CONCLUSION:**

In our study we have seen the general perception of privacy and security in e-commerce. In our study we have talked about e-commerce and its privacy and security issues. As we have seen that E-commerce refers to buying and selling of products over the internet, but any transaction that is completed exclusively through electronic channels can also be called as e-commerce. Slowly and gradually e-commerce and m-commerce are playing very important role in online retail marketing and people using this technology are increasing day by day, all over the world.

**REFERENCES**


[7] The study of E-Commerce Security Issues and Solutions Niranjanamarthy M 1, DR. Dharmendra Chahar 2 Research Scholar, Dept. of MCA, MSRIT, Bangalore, INDIA1