Security Issues, its Solutions & Protocols in E-Commerce: A Review

Pooja[1]

[1]Assistant Professor, Department of Computer Application (BCA), Vaish College of Engineering, Rohtak (Haryana)

balhara.pooja2@gmail.com

Shruti Balhara [2]

[2]Research Scholar, Haryana School of Business, Guru Jambheshwar University of Science & Technology, Hisar, Haryana.

sbalhara24@gmail.com

Abstract

In today's competitive and changing environment the emergence of network technologies plays an important role in E-Commerce. Now days, the role of e-commerce is gaining more importance because this system is used as online business for buying and selling of goods and services over the network of computers. The e-commerce business can take place in variety of forms such as B to C (Business to consumers), C to C (Consumers to Consumers), B to B (Business to Business), and C to B (Consumers to Business). This paper aims to study the various security issues faced by consumers in E-Commerce like data integrity, confidentiality, availability, authenticity, privacy, non-reputability & auditability. This paper also suggested solutions & protocols used in E-Commerce security for users.

Keywords: E-Commerce (EC), security issues, security solutions, security protocols.

Introduction

The issues such as security and privacy emerged as a major obstacle for users to deal with online trade of goods and services over the network of computers. The security issue in E-Commerce is considered essential segment of information security framework. So, the E-Commerce requires the highly security segment for users that don't affect their deals with businesses over the network of computers. The transfer and exchange of goods and services to the end-users over the network of computers is called E-Commerce. In today's time of competition many users or consumers wants to purchase the goods over the online websites to save time, transportation cost etc with the help of E-Commerce. The biggest retail stores have online business, banks also use online services to transfer credits, buy securities etc. So

the issue of security should be maintained properly for the consumers to carry out their functions properly. The important aspect which limits the customers and various organizations to deal with E-Commerce is security issue (Ackerman et al., 1999). The various software which put efforts to prevent the users for securities issues such as biometric software's (H, Abrishami Moghaddam & M. Ghayoumi, 2006). For full growth of digital business, the organization needs to raise the confidence and trust level to customers for the security and privacy of online transactions (Adams, C., & S. Farrell, 1999). As the more security is provided to the user's, more will be transactions electronically and the business will grow. Many individual users and organizations are facing by computer viruses and hackers to steal and corrupt their information. For avoiding this situation various companies spend enormous income to protect the customers from harm (Anderson, R., & M. Kuhn, 1997). Another study talked about the two privacy and security issues faced by customers. The first issue is about access by unauthorized person to steal their personal data and the second concern is about sharing their personal information to third parties (Culnan, M. J., & Armstrong, P. K, 1999).

Security issues in E-Commerce

For E-Commerce websites, the major issue faced by users is security to lose their secured privacy data and their records (Brands, Stefan., 1996). So the purpose of E-Commerce security is prevention of frauds from unauthorized users and access of data. The security requirements for safe payment electronically are:

1. **Confidentiality** - The protection of information should be done from unauthorized users, hackers etc.
2. **Integrity** - During the transmission it ensures that information will not be alerted or destroyed to end- users.
3. **Availability** - Whenever need arises the information should be available to users across the communication network.
4. **Authencity** - The method to verify or validate the buyer's identification before the payment is authorized.
5. **Privacy** - The right to control over one's personal information.
6. **Non- repudability** - To protect against customers denial of order placed and against merchant's denial of payment mode.

7. **Auditability** - Data which will be audited must be recorded in a way that specifies confidentiality and the integrated requirements are met.

Security Solutions for E-Commerce

1. Security certificates
2. Digital signature
3. Encryption

Security Certificates: they provide the identification in the electronic world named by the organization certificate authorities that issues security certificates. The role of certificate authority is to validate the security certificate holder's identity and to sign the certificate so that certificate cannot be tempered with. Once, a Certificate authority has signed a certificate to network resources, websites, people etc. it is a unique digital identity that can be used to verify the identity of an individual & always include name of identity, public key, an expiration date, name of certificate, digital sign of certificate authority and a serial number.

Digital Sign – An electronic sign whose authority is generated through password and encryption.

Encryption – control against network threats. It is an effective and practical way to safeguard data transmitted on the network which is done by encryption. The process require an encryption device for converting the original message into a code as well as decryption device for translating the code back into recognizable text

Protocols used in E- Commerce security:

1. **Secure Socket Layer (SSL)**
2. **Secure Hypertext Transfer Protocol (SHTP)**
3. **Secure Electronic Transaction (SET)**

Secure Socket Layer (SSL) – To provide privacy and security to the users, this protocol is being used. This protocol met the security requirements named encryption, integrity, authentication and non- repudiation .This was developed by Netscape communication during a communication session for providing a security.

Secure Hypertext Transfer Protocol (SHTP) – It provide the current HTTP with public key encryption, digital signature and authentication over World Wide Web server on the network

of computer. It also allows people to send secured data, payment and signatures over the network of computers.

Secure Electronic Transaction (SET) – The more secured protocol called SET was developed jointly by VISA and master card.

Conclusion

This paper concluded that E-Commerce is considered as an essential tool for buying and selling of goods and services over the networks of computers but the issue of security is of vital importance which prohibits the user to trade with online websites. So this paper founded that various protocols emerged as an E-Commerce security such as SSL, SHTTP and SET to protect the users from fraud of their personal information.

References

- Ackerman, Mark S., Lorrie Cranor, and Joseph Reagle (1999). Privacy in ECommerce: Examining User Scenarios and Privacy Preferences. *Proceedings of the ACM Conference in Electronic Commerce*, 1-8.
- Adams, C., and S. Farrell. (1999). Internet X.509 Public Key Infrastructure certificate management protocols. *Internet RFC 2510.*
- Anderson, Ross, and M. Kuhn. (1997). Low Cost Attacks on Tamper-resistant Devices. *Proceedings of the Security Protocols, 5th International Workshop*,125-136.
- Brands, Stefan. (1996). Electronic Cash. Invited talk. *RSA Cryptographers' Colloquium.*
- Culnan, M. J., and Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1),104-115.
- Ghayoumi, M. (2016). Review of security & privacy Issues in E- Commerce. International conference e- learning, e- Bus., EIS, & E-gov. ISBN:- 60132-432-4,CSREA Press corporation.
- H. Abrishami Moghaddam and M. Ghayoumi (2006). Facial Image Feature Extraction Using Support Vector Machines *Proc. VISAPP,Setubal, Portugal.*
- Nariya, H. & Gohel, C. (2013). E-Commerce system: A Review on Security Challenges & Indian Perspective. *Journal of Information and Research in Computer Engineering,* Vol. 2(2), 451-457.
- Patrol, P., Padhy, N, & Panigrahi, R. (2016). Security Issues over E-Commerce & their solutions. *International Journal of Advanced research in Computer and Communication Engineering,* Vol. 5(12), 81-85.