E-Commerce Security for Website and Firewall using HTTP and SSL: A Review and Survey

Ved Parkash[1], Roshan Lal[2]

[1]Computer Science and Engineering Department, CDLSIET Panniwala Mota, Haryana, India.

[2]Computer Science Department, Pt. Chiranji Lal Sharma Govt. P.G. College Karnal, Haryana, India.

[1]vpbhukal24@gmail.com

[2]roshanhiranwal@gmail.com

Abstract

In modern days, Internet technology growing exponentially day by day. From past few years, online business comes in trend and grow rapidly. Nowadays E-Commerce system is used by so many people and it provides the availability of the best resources to the users at their place and overwhelmed by the customer. With the rapid growth of E-Commerce system, there is a security issue in this process. In this research article, the authors address the popular security issue with the E-Commerce, also address the Core characteristics of E-Commerce security and a possible way of providing the security for E-Commerce Transaction.

Keywords: *SSL, SET, Eavesdropping, Secure HTTP, Digital Signature, Digital Certificate*

1. Introduction

In this modern era, people always prefer the situation where things are ease-of-access. Due to the development of Internet technology E-Commerce came in existence and progress significantly in the past few years. E-commerce change the way of business, In E-Commerce people purchase and sell items over the Internet. Day by day E-Commerce is increasing exponentially and with its development, the interaction between the companies and department is increasing or we can say that it is a type of Customer to Customer (C2C) business model. For the banking industry E-Commerce provide the great opportunity. For example, online banking allows the customer to access their bank details from home, transfer fund and pay the bill etc. E-Commerce improved the market efficiency by the low cost and time management. IBM has defined it as "the transformation of key business processes through the use of Internet technologies". E-Commerce is a trade over the Internet but one of the problems or issue with E-Commerce is Security, Especially in case of e-payment. For a reliable E-Commerce system security issue must be resolved.

Security measures involve the hardware, software, and users. A good security system must need to focus on physical security, human security, protection from the disaster and some legal implication along with hardware and software. For E-Commerce system, the designer must address all the security concern for providing better service like a good network, in which security service depends on the encryption rule of that particular country. Eavesdropping, Snooping, Interception, Replay Attacks, Back-door Attacks, Denial-of-Service attacks, Man-In-middle attacks are some possible type of attack in the E-commerce system.

One of primary concern with E-Commerce system is security. The security in E-Commerce is important for both the customer and service providers' perspective. The main key issue regarding the security concern in E-Commerce is security for the transaction.

Session Security Management in E-Commerce System is discussed by Bing XU and Shiyi XIE [1], in this research article the authors discussed the web service session security and session management and come up with the solution. It is based on WS-Security and WS-Conversation. Peer-to-Peer (P2P) E-Commerce gives the flexibility and convenience to E-business but one of the problems with this is security threat of business activity, for resolving the issue a new trust model of P2P e-commerce, which is based on voting agreement discussed by WANG Yu et. al. [2], a new trust model work according to the recommendation of peers and two-side trading experience.

An aspect-oriented approach to separating security and application concern at architecture level is proposed by [3]. E-Commerce security based on cryptography is proposed by Shazia Yasin et. al. [4], and the purpose of the paper is to describe the importance of security in E-Commerce based on secure E-Commerce protocol, digital signature, certificate-based cryptography, and public key infrastructure. Elliptic curve cryptography based E-commerce security approach is proposed by Khaleel Ahmad and md Shoaib alam [5]. A conceptual Risk management framework for E-Commerce is proposed by Wu Yanyan [6].

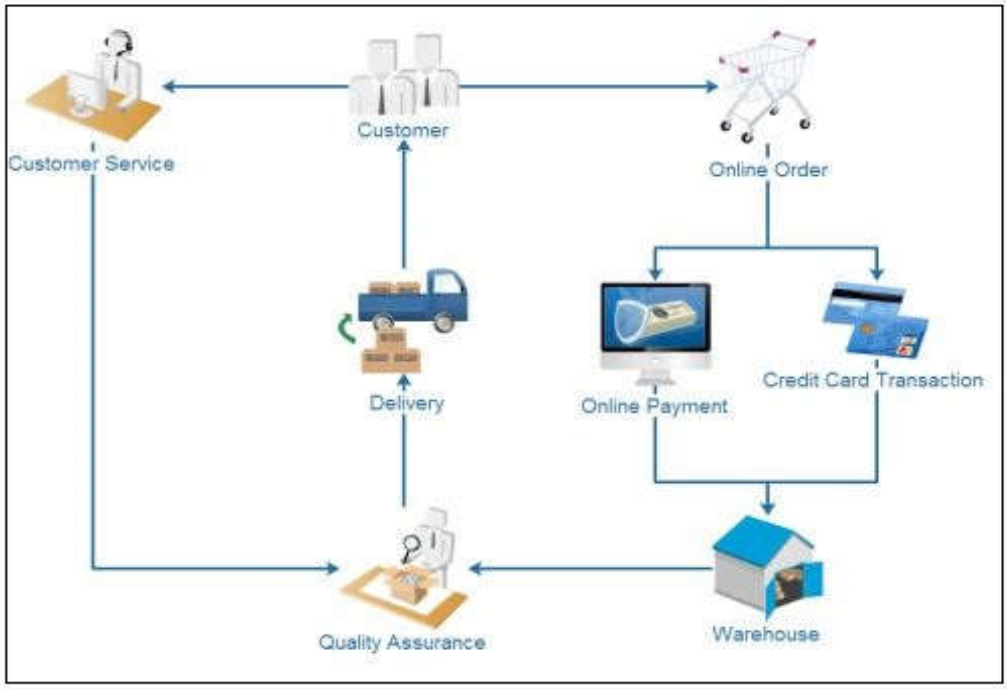

Figure 1. Illustration of general E-Commerce process [7].

The further Section of the Paper is described as Section 2 is about the security issue in E-commerce, Section 3 is about the core characteristic of e-commerce security, Section 4 address the security feature in E-Commerce transaction and finally section 5 is about the conclusion.

2. E-Commerce Security Issue

For concerns about the security for E-Commerce, there must need some safety protocol for e-commerce transaction and it is important for protecting the companies and customer from threats like the fraud using credit and debit card etc and ensure safe payment processing.

One of the most important and crucial features for electronic commerce is Cyber-security and if there is no proper protocol design there always be a chance of payment risk and due to this risk one out of five small business retailers fall victim and out of those due to this approx 60 to 65 percent close within some time.

Apart from the hacking, accepting the fraudulent payment is an also a serious problem. When we talk about the E-Commerce security, it is a set of protocol which provides safety for E-Commerce transaction. Some of the important security issue with E-Commerce address here and the brief description as follows [8]:

I) *Eavesdropping:* In such case the private communication network can be attacked by an unauthorized user. It can be done in the telephone line, emails, cellular network or in another private instant messaging. In case of a network, eavesdropping attack is focused on capture the small packets present in that message. One simple way of preventing the network-based eavesdropping is used https instead of HTTP.

II) *Illegal Access:* One of the problems with the online system of an E-commerce system is Illegal Access of the System it is generally misusing the device without having a right to access.

III) *Mutual Authentication:* In Mutual authentication process before any type of communication the authentication must require from both the parties at a same time. There are two types of mutual authentication one is certificate based and the other one is user-name and password based. For secure communication and e-business the mutual authentication must be needed. If we consider the network environment case here needed an authentication of the server from the client and vice-versa and it is helpful for the minimizing the e-commerce online fraud. Some web-based mutual authentication is done using Transport Layer Security (TLS) protocol.

IV) *Reply Attack:* Sometime this type of attack known as playback attack, it is a type of network attack where data is repeated by fraud. In a real-world scenario like text-dependent speaker verification, this type of attack found. One time password for the particular transaction is a good method for prevention from Reply Attack in an E-Commerce system.

V) *Uncertain Identity:* In this scenario the attackers steal the identity of the authorized user after that actively participate and get the benefit.

VI) *Phishing Attacks:* This is the common method through which the hackers or attacker act as a trusted entity and get the login credentials or the credit card information and harm the user financially.

VII) *Credit Card Fraud:* When we used the E-Commerce sites for shopping there might be a possibility of several intrusion points for attackers to get the users confidential information. A common type of possible Fraud done by hackers or attackers using ATM withdrawal or through E-Commerce transaction.

3. E-Commerce Security Core Characteristics

As security is more important in E-Commerce system there are some core characteristics like Integrity, Authentication, confidentiality, Availability, controllable, Non-repudiation briefly described here:

I) *Integrity:* From unauthorized prevention and exchangeability E-Commerce transaction require all information. Integrity means the information received by the receiver is same as it sends by the sender and conclude that the there is no damage in the sending information [9].

II) *Authentication:* Before prior communication or trade start online in case of E-Commerce authentication of sender and receiver must require and it prevent from the different possible attacks. For the implementation of the authentication process digital signature is one of the key methods [10].

III) *Confidentiality:* For protecting the transaction from unauthorized reading confidentiality must require and it can be achieved by some encryption technique. when we talk in terms of E-Commerce confidentiality ensure that the information obtain from users is only use for intended purpose and for that purpose most of e-commerce website have the terms and conditions which is agreed by the customer at the time of registration [11].

IV) *Availability:* It is one of the important characteristics of E-Commerce which ensures the effectiveness and efficiency of E-Commerce. It provides easy access to users and ensures stable service to the user. It can be affected by a denial of service attack and reduce the performance of normal computer processing [11].

V) *Controllable:* In an E-Commerce system, it must ensure that the system is out of the access of unauthorized users and set some safety requirements. It ensures that only legitimate user used the system.

VI) *Non-repudiation:* It is a very important feature which needs to address during E-Commerce service, especially during the payment process. It ensures that sender and receiver deny the already transmitted message one way to prevent by repetition of the old message is either through the session management for transaction or other which is commonly used now a day's which is One Time Password (OTP) [12].

4. Security in E-Commerce Transaction

In entire E-Commerce system the important step is payment of purchase and hence security in this case must require because any threat makes the retailer and the

customer in trouble of financial losses. Some of the safety measures for E-Commerce transaction is briefly discussed here:

I) *Secure Socket Layer (SSL):* One of the important methods of securing the channel is Secure Socket Layer (SSL). It is based on the TCP/IP protocol. SSL provides the services like the authentication for the server, authentication for the client, encryption of data and most important is message integrity for TCP/IP. It is useful for the prevention from eavesdropping or forgery of the message when communication takes place between the two devices over the Internet.

Once the SSL certificate is used for communication the information which we send is unreadable to everyone except for the server to whom the information sent. It is very useful in case of online payment purpose because if there is not an SSL certificate anyone between the user and server can fetch the information like credit/debit card information, username, and password etc.

II) *Secure Electronic Transaction (SET):* During the transaction process through credit/debit card SET is required. Enabling the payment security, confidentiality for payment data and authentication of the cardholder and merchant, are the three primary objectives of SET. Because in the e-commerce system there are different vendors and platform and for all of them interoperability must require and it is ensured by SET.

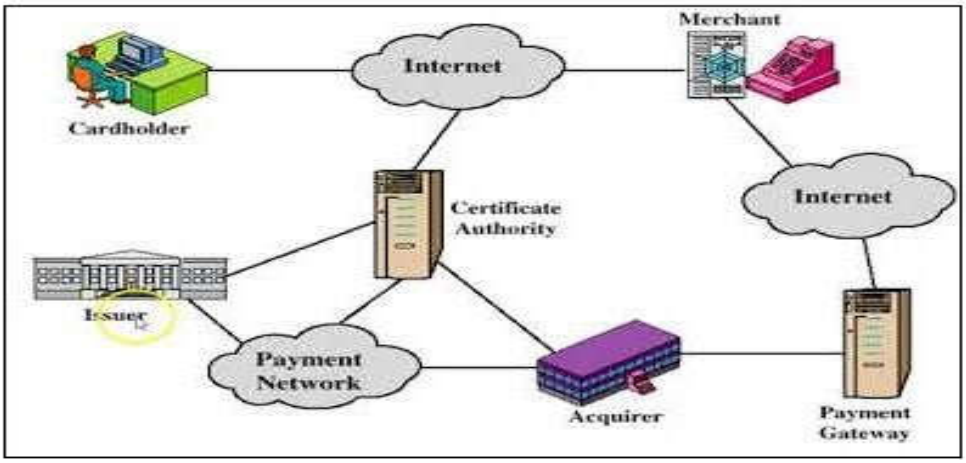

Figure 2. Illustration of general E-Commerce process [14].

III) *Encryption:* It is a process of transfer the data from its present form to another form without changing its actual meaning and in technical term cipher text. The primary purpose of encryption is securely stored information, secure the transmission process.

IV) *Secure HTTP:* It is a secure communication protocol for message transfer. It is used for sending the message securely where SSL is used for creating a secure connection between the two computers. S-HTTP is designed to provide security for HTTP (Hypertext transfer protocol).

V) *Digital Signature and Digital Certificate:* It is a digital way of authenticating the document. It is a unique digital code for the person (for sender or receiver) and very easy for verification it is basically a hash function value of a message and the encryption is done using the private key of the document owner basically. On the other hand, the Digital Certificate is a document which is issued by the

trusted third party and the certificate contain the information like certificate serial number, expiration date, issuance date, digital signature certificate, and other authentic information. This certificate is signed using the private key of Certification Authority. The authenticity of the certificate can be confirmed using the public key of the Certification Authority.

5. Conclusion

For buying and selling the items online E-Commerce is widely used and exponentially increasing from past few years and play an important role in online retail marketing. Security is one of the primary concerns in E-Commerce and it is very important for prevention from unauthorized access, destruction. For prevention from transaction against threats integrity, confidentiality and non-repudiation are important dimensions. Apart from this the current E-Commerce security issue related to other areas like the legal system, people's moral regulation, and other factors. The important applications are mentioned in the previous works [15]-[48]. In the future, E-commerce security for firewall and website with more secure protocols.

References

[1]. Xu, Bing, and Shiyi Xie. "Research of session security management in E-Commerce system." Information Engineering and Electronic Commerce, 2009. IEEC'09. International Symposium on. IEEE, **(2009)**.

[2]. Wang, Yu, Yue-long Zhao, and Fang Hou. "A new security trust model for peer-to-peer e-commerce." Management of e-Commerce and e-Government, 2008. ICMECG'08. International Conference on. IEEE, **(2008)**.

[3]. Yang, Chunhua, and Jiancheng Wan. "An approach to separating security concerns in e-commerce systems at the architecture level." International Symposium on Electronic Commerce and Security. IEEE, **(2008)**.

[4]. Yasin, Shazia, Khalid Haseeb, and Rashid Jalal Qureshi. "Cryptography based e-commerce security: a review." International Journal of Computer Science Issues (IJCSI) 9.2 **(2012)**: 132.

[5]. Ahmad, Khaleel, and Md Shoaib Alam. "E-commerce security through elliptic curve cryptography." Procedia Computer Science 78 **(2016)**: 867-873.

[6]. Yanyan, Wu. "Research on e-commerce Security based on Risk Management Perspective." International Journal of Security and Its Applications 8.3 **(2014)**: 153-162.

[7]. E-Commerce work flow Diagram: "https://www.edrawsoft.com/template-e-commerce-workflow.php." **Accessed on 5/11/18**.

[8]. E-Commerce Security Systems: "https://www.tutorialspoint.com/e_commerce/e_commerce_security.htm." **Accessed on 28/10/18**.

[9]. J. H. Matsuura, "Security, rights, and liabilities in e-commerce.", **(2002)**.

[10]. C. Hay-Hurst, "Careers in e-commerce security and encryption.", **(2001)**.

[11]. H. Bidgoli, "Electronic commerce: principles and practice.", **(2002)**.

[12]. M. Bushry, "E-Commerce." **(2005)**.

[13]. Maurya, Santosh Kumar, and Nagendra Prata Bharati. "Cyber Security:

Issue and Challenges in E-Commerce.", *NagendraPratap Bharati* 5.1 **(2016)**.

[14]. E-commerce security: "https://www.bigcommerce.com/ecommerceanswers /why-online-security-so-important/". **Accessed on 30/10/2018.**

[15]. Krishan Kumar, Deepti D. Shrimankar, F-DES: Fast and Deep Event Summarization, IEEE Transactions on Multimedia (TMM), 2017.

[16]. Krishan Kumar, Deepti D. Shrimankar, Deep Event Learning boosT-up Approach: DELTA, Springer Multimedia Tools and Applications, 2018

[17]. Krishan Kumar, Deepti D. Shrimankar, Navjot Singh, Eratosthenes sieve-based key-frame extraction technique for event summarization in videos, Springer Multimedia Tools and Applications (MTAP), 2017.

[18]. Krishan Kumar, Deepti D. Shrimankar, ESUMM: Event SUMMarization on scale-free network, IETE Technical Review (TITR), 2018.

[19]. Krishan Kumar, Manish Kurhekar, Sentimentalizer: Docker container utility over Cloud, In Proc. IEEE 9th International Conference on Advances in Pattern Recognition (ICAPR 2017), Dec. 2017

[20]. Krishan Kumar, Deepti Shrimankar, Navjot Singh, Event BAGGING: A novel event summarization approach in multi-view surveillance videos, In Proc. IEEE International Conference on Innovations in Electronics, Signal Processing and Communication, (IESC 2017), Apr. 2017.

[21]. Krishan Kumar, Deepti Shrimankar, Navjot Singh, Key-Lectures: Keyframes extraction in video Lectures, In Proc. Springer International Conference on Machine Intelligence and Signal Processing, (MISP 2017).

[22]. Krishan Kumar, Anurag Kumar and Ayush Bahuguna, D-CAD: Deep and Crowded Anomaly Detection, In Proc. ACM 7th International Conference on Computer and Communication Technology, ICCCT- 2017, Nov. 2017

[23]. Krishan Kumar, Deepti Shrimankar, Navjot Singh, V-LESS: a Video from Linear Event SummarieS, In Proc. Springer 2nd International Conference on Computer Vision & Image Processing (CVIP-2017), Sept. 2017

[24]. Krishan Kumar, Deepti Shrimankar, Navjot Singh, SOMES: An efficient SOM technique for Event Summarization in multi-view surveillance videos, In Proc. Springer 5th International Conference on Advanced Computing, Networking and Informatics (ICACNI 2017), Sept. 2017

[25]. Shikhar Sharma, Piyush Kumar, Krishan Kumar, LEXER: LEXicon based Emotion analyzeR, In Proc. Springer 7th International Conference on Pattern Recognition and Machine Intelligence (PReMI 2017), Dec. 2017

[26]. Krishan Kumar, Shambhavi Sinha, Piyushi Manupriya, D-PNR: Deep license Plate Number Recognition, In Proc. Springer 2nd International Conference on Computer Vision & Image Processing (CVIP-2017,) 2017

[27]. Krishan Kumar, Deepti Shrimankar, Navjot Singh, Equal Partition based Clustering approach for Event Summarization in Videos, In Proc. IEEE 12th International Conference on Signal-Image Technology & Internet-Based Systems, SITIS 2016, Nov. 2016

[28]. Krishan Kumar, Manish Kurhekar, Economically Efficient Virtualization Over Cloud Using Docker Containers, In Proc. IEEE 5th International Conference on Cloud Computing in Emerging Markets (CCEM) Nov. 2016

[29]. Krishan Kumar, Rishab Bamrara, Prakhar Gupta, Navjot Singh, M2P2: Movie's trailer reviews-based Movie Popularity Prediction system, In Proc. 3rd SoCTA (Soft Computing: Theories and Applications), Dec. 2018.

[30]. Krishan Kumar, Manish Kurhekar, Abhay Mishra, Dynamic Behavior of Coupled Neurons and Contact Processes on Scale Free Networks, In Proc. International Conference on Aerosols, Air Quality & Climate Change (AAC-2018), Oct. 2018.

[31]. Shubham Kumar, Krishan Kumar, LSRC: Lexicon Star Rating system over Cloud, In Proc. IEEE 4th International Conference on Recent Advances in Information Technology (RAIT'18).

[32]. Shikhar Sharma, Krishan Kumar, Navjot Singh, D-FES: Deep Facial Expression recognition System, In Proc. Conference on Information and Communication Technology, (CICT 2017), Oct. 2018.

[33]. Shikhar Sharma, Krishan Kumar, GUESS: Genetic Uses in video Encryption with Secret Sharing, In Proc. Springer 2nd International Conference on Computer Vision & Image Processing (CVIP- 2017), Sept. 2017

[34]. Aditya Vijayvergia, Krishan Kumar, STAR: rating of reviewS by exploiting Variation, In Proc. 2nd Conference on Information and Communication Technology, (CICT 2018), Oct. 2018.

[35]. Shubham Kumar, Krishan Kumar, IRSC: Integrated automated Review mining System using virtual machines in the Cloud environment, In Proc. IEEE 2nd Conference on Information and Communication Technology, (CICT 2018), Oct. 2018.

[36]. Abhay Mishra, Krishan Kumar, Parveen Kumar, Prakhar Mittal, A novel approach for Handwritten Character Recognition using K-NN Classifier, In Proc. 3rd SoCTA (Soft Computing: Theories and Applications), Dec. 2018.

[37]. Gagandeep Singh, Navjot Singh, Krishan Kumar, PICS: a novel technique for video summarization, In Proc. Springer International Conference on Machine Intelligence and Signal Processing, (MISP 2017), Dec. 2017

[38]. Shikhar Sharma, Piyush Kumar, Krishan Kumar, A-PNR: Automatic Plate

Number Recognition, In Proc. ACM 7th International Conference on Computer and Communication Technology, ICCCT- 2017, Nov. 2017

[39]. Anurag Kumar, Navjot Singh, Piyush Kumar, Aditya Vijayvergia, Krishan Kumar, A novel Superpixel based Color Spatial feature for Salient Object Detection, In Proc. Conference on Information and Communication Technology, (CICT 2017), Oct. 2018.

[40]. Piyushi Manupriya, Shambhavi Sinha, Krishan Kumar, V-SEE: Video Secret sharing Encryption technique, In Proc. Conference on Information and Communication Technology, (CICT 2017), Oct. 2018.

[41]. Shikhar Sharma, Shiv Naresh Shivhare, Navjot Singh, Krishan Kumar, Computationally efficient ANN model for Small Scale Problems, In Proc. Springer International Conference on Machine Intelligence and Signal Processing, (MISP 2017), Dec. 2017

[42]. Harman Singh, Neeti Dhanak, Haroon Ansari, Krishan Kumar, HDML: Habit Detection with Machine Learning, In Proc. ACM 7th International Conference on Computer and Communication Technology, ICCCT-2017, Nov. 2017

[43]. Kunal Patange, Pushkar Pete, M. Wankhade, A. Chatterjee, Manish Kurhekar, Krishan Kumar, 3E-VMC: an Experimental Energy Efficient model for VMs scheduling over Cloud, In Proc. IEEE First International Conference on Secure Cyber Computing and Communications (ICSCCC 2018), Dec. 2018

[44]. Rama Krishna Koppanati, Saad Qamar, Krishan Kumar, SMALL: Secure MultimediA technique using Logistic and LFSR, In Proc. IEEE International Conference on Intelligent Computing and Control Systems (ICICCS 2018)

[45]. Saad Qamar, Rama Krishna Koppanati, Krishan Kumar, VM-MMT: a novel approach for VM consolidation over openstack cloud using linear regression and Minimum Migration Time, In Proc. IEEE International Conference on Intelligent Computing and Control Systems (ICICCS 2018), Jun. 2018.

[46]. Sandeep Kumain, Maheep Singh, Krishan Kumar, An Efficient Gaussian Noise Reduction Technique for Noisy Images using optimized filter approach In Proc. IEEE First International Conference on Secure Cyber Computing and Communications (ICSCCC 2018), Dec. 2018

[47]. Haroon Ansari, Aditya Vijayvergia, Krishan Kumar, DCR-HMM: Depression detection based on Content Rating using Hidden Markov Model, In Proc. IEEE 2nd Conference on Information and Communication Technology, (CICT 2018)

[48]. Akshay Solanki, Rishab Bamrara, Krishan Kumar, Navjot Singh, VEDL: a novel Video Event searching technique using Deep Learning, In Proc. 3rd SoCTA (Soft Computing: Theories and Applications), Dec. 2018.