IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Design and Analysis of Access Control and Security Model in E-commerce System

Nikhil Pareek

Amity University Uttar Pradesh, India

Abstract: E-commerce Security is a division of a data security structure and is mainly applied to the components that have an effect on e-commerce that contain Data security, Computer Security and other wider area of the Information safety structure. E-commerce safety is one of the principle clear security instruments that impact the end client through their day by day instalment collaboration with business. It is the declaration of e-trade assets from unapproved use alteration, affirmation or decimation. The vital E-business procedure is fundamental used for the effective operation and administration of E-trade conduct. One of a procedure is security and access control. Ecommerce must set up common secure access and confidence among the gatherings in e-trade operation by validating customers and implementing safety features. E-business sites must then approve the right of entry to those elements of the site that an individual customer needs to finish his or her specific transactions. In this way, person will be accessible to all assets of an E-trade webpage aside from added individuals' records, limited group information, website admin organization sector. Other security process ensures the asset of an E-business site from dangers, for example, programmer assaults, burglary of passwords or card numbers, and system breakdown.

Keywords: Security measures, E-Commerce Security Issues, Access control, Availability.

I. INTRODUCTION

One of the most significant issues that should be considered to make sure achievement of e-commerce is security. The minimal effort and extensive accessibility of Internet to organizations and customers has effected a revolution of e-commerce [2].

Today, privacy and security is the main challenges for electronic technologies. Security of system is one of the major and long-term concerns which control clients and organizations engage with ecommerce[1].

Payments handle by web e-commerce application like(electronic transactions, PayPal, online banking or using credit cards, debit cards or other token) have more completion problems[8]. Safety issues are implemented slowly on the internal networks by ecommerce industry[3].

The most genuine component of the ecommerce security is educating the consumer on safety measures but it is still on the initial stage.

With the rise of individuality theft privacy has turn out to be a major fear for consumers, and some distress for customers should be care for as a major concern for the e-Commerce supplier.

II. SECURITY IN E-COMMERCE FIELD

The effective working of E-business security relies on upon a composite relationship among various applications improvement stages, database administration frameworks, frameworks programming and system base. Security measures are present in each stage of E-commerce.

Phases of E-Commerce Operation			
Information phase	Negotiation phase	Payment phase	Delivery phase
Security Measures			
Confidentiality Access control Integrity Check	protect contract Identification Digital signatures	Encryption	protect Delivery Integrity Checks

Fig1:Phases of E-commerce operation [5]

Phases:

1. Information phase: In this phase, the parties try to discover their partners, do comparison, elucidate their trading relations, and specify products that are to be exchanged. These measures are not officially binding.
2. Negotiation Phase: This phase focus on the selection of partners according to the decision criteria of the party and signing of agreement regarding trade relations.
3. Delivery Phase: Finally, in delivery phase, payment and delivery is made and finally a new transaction is arranged.

Some key measurements of e-business security:

- Access Control
- Security/Privacy
- Non Repudiation
- Availability
- Integrity
- Authentication

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

E-commerce Security
In E-commerce security, classification of trust models is done into three categories:

1) Hierarchical
Here, the hierarchy is based on the series of CA establishment that are set on a predefined rules and conventions. However, failure of a single CA can lead to corruption of the complete trust model and all the certificates signed by it.

2) Distributed
No involvement of CA is there in this model. Throughout the transaction, there is no involvement of trust party. This model lacks in carrying out well into the web based e-commerce because every party is left on its own device to establish the trust level with other parties.

3) Direct
This model is also referred to as peer to peer trust model. It is utilized as a part of symmetric input based frameworks. No involvement of trusted third party is there. Direct trust model is not considered appropriate for web based e-commerce.

III. ACCESS CONTROL

The first network security concern addresses access control. Access control perform restriction for the access to a building, a property or a area to trained people in the physical security[8]. Through mechanical means like lock and key or through industrial means such as card entry system, Physical access control can be achieved[5].

Access to intranet and web assets can be utilized through several technologies[1]. Access control involves authorization, authentication and audit.

It in corporately measures, for example: gadgets, including metal locks and biometric scanning, hidden ways, encryption, social boundaries, and observing by people and robotized frameworks[10].

In any entrance control demonstrate, the elements that can perform activities in the framework and are called subjects, and objects are the entities representing assets to which right of entry may need to be prohibited[9].

Access control frameworks give the vital administrations of recognizable proof and verification (I&A), approval, and responsibility where:

a) Authentication and Identification: determining who can access a organization and involvement of customers in the software issues that they are able to control in form of login.
b) Authorization: figures out what a subject is supposed to do.
c) Accountability: recognizes or keep in record what a subject did.

IV. CYCLE OF DIGITAL E-COMMERCE

Security is essential in online purchasing locales. Now days, gigantic sum is acquired on the web, as it's less demanding and extra reasonable[6]. Practically everything can be purchased, for example, toys, attire, music, etc. Some of the most prevalent sites are iTunes, dell, eBay, HMV, Amazon, Best Buy and many more. The point of this explanation is to make others aware, especially young students that the electronic commerce might be dangerous thus at the same time might be useful[11]. The rise of the digital economy does not change the the issue of good and bad, but rather it enhances the client's entrance to purchasing and offering products, which amplifies the issue of illicit exercises[1].

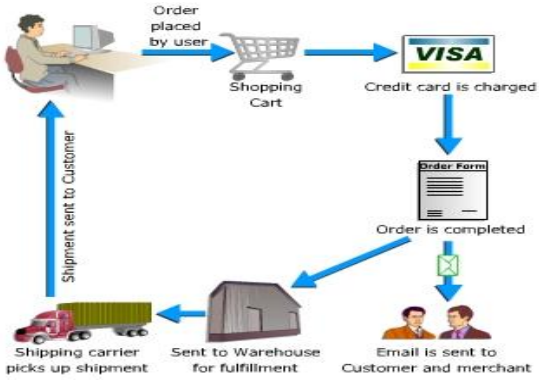

Fig2:Digital E-commerce cycle [12]

V. TOOLS OF E-COMMERCE SECURITY

- Firewall – related to software and hardware
- Open Key framework
- Encoding of encryption
- Digital credentials
- Digital signatures
- Biometrics – fingerprints, voice, retinal scanning, etc
- Passwords
- Locks(network operations centers)

Fig3. E-Commerce Security Strategy [12]

VI. REASONS FOR SECURITY

1. Confidentiality of Information – encryption and decryption techniques are used for this..
2. Identification and conformation – digital signatures are responsible for guaranteeing that someone is who they claim to be.

DOI 10.17148/IJARCCE.2016.5548

3. Access Control – oversees what resources a client may access and utilizes extensive IDs and passwords.
4. Data Integrity – guarantees that data has not been distorted and is executed by hashing or message process.
5. Non-denial – do not deny a sale or purchase implemented with digital signatures.
6. Plaintext – a message that common people could understand.
7. Cipher text – illegible to humans, uses encryption.
8. Reverse process is known as decryption.

VII. ISSUES RELATED TO SECURITY

E-commerce security provides the security to assets of e-commerce from the illegal access, use modification, or damage. Although security features will not assure a secure system but they were necessary to construct a secure system[4].

Categories of Security System:

1) Authentication:- It is responsible for the Verification of who the user declare they are. It assures that only a particular user is the one allowed to have access to their Internet banking account.
2) Authorization:- It is responsible for allowing the user to control or operate their resources in particular ways. This can prevent them from exceeding the balance of their account or a bill deletion.
3) Encryption:- It is responsible for hiding of information and also ensures that you are not spying on others during banking transactions.
4) Auditing:-It is responsible for keeping a trace of operations. Auditing helps merchants in proving that you bought particular merchandise.
5) Integrity:- It provides avoidance of illegal data alteration.
6) Non repudiation: It ensures that one party does not renege on an agreement.
7) Availability: It ensures that there are no delays of data or their removal.

A. SOME WAYS TO PROTECT US:

1) We should change our passwords time to time.
2) Try to choose passwords which includes numbers, both upper and lower case, should be at least 8 digitals long and should have some special characters as well (!*&).
3) We should not keep our sensitive or secluded files in folders having fascinating name.
4) Try not choosing same password that we are already using anywhere else.
5) Whenever available, we should try applying updates to our shopping cart.
6) We should apply security patches to our shopping cart when accessible.
7) We should always try to use the https while navigating by our admin area.
8) If we get an option to delete all details of our credit card after purchases, use the opportunity.
9) We should try to sign up with a firewall service, these services generally appear with an icon or symbol that can be put in our store as they help in boosting sales. They are paid and not free.
10) We should try choosing a shopping cart that has the feature of recording IP address in admin and store section.

B. SO CAN We FEEL SAFE WHILE SHOPPING ON-LINE?

Yes, we can surely feel safe by following some simple rules. If we are new to the Internet or a usual shopper online, there are some guidelines that should be followed:

1) We must be sure that we are aware of the rate of exchange, if we are not confident about the current rates, discover before buying a product[3].
2) Always uncover the delivery cost before the placement of our order and also the time they will be taking to deliver. Mostly shopping websites are using courier services to deliver the products and delivering across overseas can be somewhat expensive[3].
3) We should always check the feedback of buyers and sellers before making a bid at eBay.
4) If new to a site, always read FAQ section first.
5) We should always say no to a cash payment. Use of our credit cards to make the payment can protect us from fraud activities because credit card companies make sure to refund accounts where fake activity or fraud transaction takes place.
6) We should always have a look at contact information of a buyer and ensure that they have given their postal address. If not, no dealing with them.
7) We should not get conscious of asking our queries to the seller, genuine sellers should be helpful.
8) Always read and check the full terms and conditions as well as the privacy policy of the website.
9) On being unsure about a website, search for it on Google or any other search engines.

VIII. CONCLUSION

E-commerce is extensively measured the export and import of goods above the internet, except any operation which is completed solely by electronic procedures will considered as ecommerce[11]. Gradually M-commerce and E-commerce plays fine role in online trade marketing also with this technology increased day to day over the globe. E-commerce safety is the protection of e-commerce resources from the illegal access use , destruction or alteration. Different dimension of e-commerce safety; Integrity: avoidance beside illegal data alteration, No Authenticity: authentication of data source. Disclaimer: barrier beside any single party from renege onto the contract following the verity. [8]. Privacy: terms of data manage and revelation. Confidentiality: security against illegal data revelation. Availability: avoidance against information delay or elimination[11]. Fraud people are frequently seems to take benefit of online shoppers prone to building beginner errors. general mistakes that leave users defenseless contain shopping on websites which is

not protected, providing the full personal information, and leaving the computers for the virus[2]. In this document we were discuss E-commerce safety problems, Digital E-commerce Online Shopping, Security Threats, Security measures and procedure for secure and safe online shopping by the shopping websites[10].

REFERENCES

[1]. Mohanad Halaweh, Christine Fidler - " Security Perception in Ecommerce: Conflict between Customer and Organizational Perspectives".Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 – 449, ISBN 978-83-60810-14-9- 2008-IEEE
[2]. Yuanqiao Wen, Chunhui Zhou "Research on E-Commerce SecurityIssues". 2008 International Seminar on Business and Information Management.
[3]. Rui Wang, Shuo Chen "How to Shop for Free Online Security Analysis of Cashier-as-a-Service Based Web Stores". IEEE S&P'11 proceedings.
[4]. V.SRIKANTH "ECOMMERCE ONLINE SECURITY AND TRUST MARKS". IJCET ISSN 0976 – 6375, Volume 3, Issue 2, July- September (2012),
[5]. Shazia Yasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012
[6]. Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues"Proceedings of the 35th Hawaii International Conference on System Sciences - 2002
[7]. Rashad Yazdanifard, Noor Al-Huda Edres "Security and Privacy Issues as a Potential Risk for Further Ecommerce Development"International Conference on Information Communication and Management - IPCSIT vol.16 (2011)
[8]. Seyyed Mohammad Reza Farshchi "Study of Security Issues on Traditional and New Generation of E-commerce Model" International Conference on Software and Computer Applications-IPCSIT vol.9 (2011)
[9]. RAJU BARSKAR, ANJANA JAYANT DEEN"The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology"(IJCSIS)-Vol. 8, No. 1, April 2010.
[10]. Dr. Nada M. A. Al-Slamy, "E-Commerce security"IJCSNS - VOL.8 No.5, May 2008
[11]. W. Jeberson, Prof. (Col.). Gurmit Singh. "Analysis of Security Measures Implemented on G2C Online Payment Systems in India" MIT International
[12]. Journal.International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013.
[13]. International Journal of Security and Its Applications Vol.8, No.3 (2014), pp. 153-162 http://dx.doi.org/10.14257/ijsia.2014.8.3.17.
[14]. Deepu Raveendran et al, "A Study on Secure and Efficient Access Control Framework for SOA", International Journal of Computer Science and Telecommunications, Vol.-3, No.-6, Pg. No. 71-76, June 2012.
[15]. Dr. S. K. Dwivedi, Ashish kr. Luhach, Dr. Jitender Kumar, "Enterprise Transformation to Service Oriented Architectures", 2015IEEE International Conference on Computational Intelligence andComputing Research, 2015.
[16]. Li Xiong-Yi, "Research and application of SOA in B2B electronic commerce", 2014 International Conference on Computer Technology and Development, 2014.
[17]. Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues"Proceedings of the 35th Hawaii International Conference on System Sciences - 2013
[18]. Rashad Yazdanifard, Noor Al-Huda Edres "Security and Privacy Issues as a Potential Risk for Further Ecommerce Development"International Conference on Information Communication and Management – IPCSIT vol.16 (2011)
[19]. Seyyed Mohammad Reza Farshchi "Study of Security Issues onTraditional and New Generation of E-commerce Model" International Conference on Software and Computer Applications-IPCSIT vol.9 (2013)
[20]. RAJU BARSKAR, ANJANA JAYANT DEEN"The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology"(IJCSIS)-Vol. 8, No. 1, April 2014.