International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT206356

Usability and Security Issues in the Implementation of E-Commerce Website

Pratap Kumar Kumar[1], Sashank Kumar[2], Biresh Kumar[3]

[1,2]**B.Tech Scholar,** Department of Computer Science and Engineering, Amity University, Jharkhand, Uttar Pradesh, India
[3]**Assistant Professor,** Department of Computer Science and Engineering, Amity University, Jharkhand, Uttar Pradesh, India

ABSTRACT

E-commerce (electronic commerce) or EC is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. These business transactions occur either as b to b (business-to-business), b to c (business-to-consumer), c to c (consumer-to-consumer) or c to b (consumer-to-business).It is the trading or in products or services using computer networks like Internet or online social networks. Here the Business conducted through the use of computers, telephones, fax machines, barcode readers, credit cards, automated teller machines (ATM) or other electronic appliances without the exchange of paper-based documents or physically moving to a shopping mall. It includes activities such as procurement, order entry, transaction processing, online payment, authentication, inventory control, order fulfillment, shipment, and customer support. When a buyer pays with a bank card swiped through a magnetic-stripe-reader, he or she is participating in e-commerce. E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e- commerce including of Data security and other wider realms of the Information Security framework. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security-Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability. Ecommerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats, hackings. Therefore it is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. Due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions. In this paper we discussed with Overview of security for e- commerce, various steps to place an order, Security purpose in E-commerce, various security issues in E-commerce, guidelines for secure online shopping etc.

Keywords : E-commerce, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability.

I. INTRODUCTION

Security in E-commerce is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security. E-commerce needs high security components that affect the end user through their daily payment interaction with business. E-commerce required a reliable infrastructure and framework to enable a secure and successful e-commerce.

Today, privacy and security are a major concern for electronic technologies. M-commerce (Mobile – Commerce) shares security concerns with other and organizations engaging with ecommerce. On the web e- commerce applications that handle payments like online banking, electronic transactions or using debit cards, credit cards, PayPal, E-cash, prepaid cards,

master cards, visa cards or other tokens have more compliance issues, technologies in the field. Privacy concerns have been found, revealing a lack of trust in a variety of contexts, including commerce, electronic health records, e- recruitment technology and social networking, and this has directly influenced users. Security is one of the most important factors that restrict customers and organizations engaging with ecommerce.

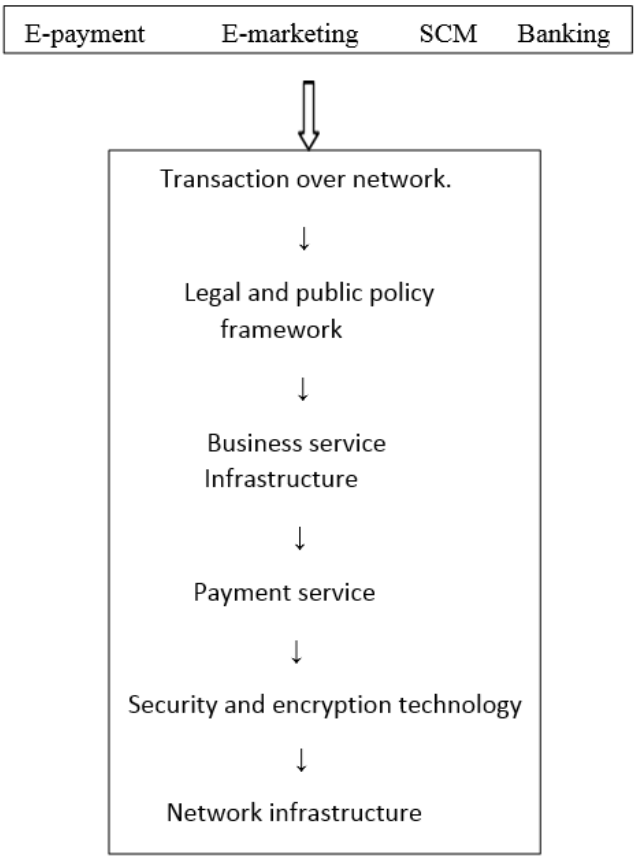

Fig 1:- Basic infrastructure of E-commerce

The e-commerce now addressing slowly for the security issues on their internal networks. There is such kind of guidelines for securing systems and networks available for the ecommerce systems personnel to read and implement. As most of the customers those are using online shopping some are literacy and some are illiteracy so to Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture. Virus, worms, Trojan horse programs launched against client systems pose the greatest threat to e-commerce because they can bypass or subvert most of the authentication and authorization mechanisms used in an ecommerce transaction. These programs can be installed on a remote computer by the simplest of means: email attachments.

So some Privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for e-Commerce providers.

II. RELATED WORK

Security is one of the crucial part restrict customers and organizations engaging with e- ecommerce. The aim of this paper is to explore the perception of security in e- commerce basically on business to customer B2C and customer to customer C2C websites from both customer and organizational perspectives.

With the rapid growth of global market in E-commerce, security issues are arising from people's attention. The security for the online transaction is the core and key issues of the development of E-commerce. This paper about the security issues of Ecommerce activities put forward solution strategy from two aspects that are I. technology and system, so as to improve the environment for the development of E-commerce and ii. Promote the further development of E-commerce.

Web applications increasingly integrate third-party services. The integration introduces new security challenges due to the complexity for a web application to coordinate its internal states with those of the component services and the web client across the Internet.

Now a days the owners of Ecommerce web site are thinking of how to attract more customers and how to make the visitors feel secured when purchasing goods on the site, on the other side how the end users should rate an ecommerce website and what they should do to protect themselves as one among the online community. The main objective of writing this research analysis journal is to make the readers to get clarity of thoughts on the web technology which will help all the online customers to do secure transactions along with safety tips and tricks. There for the online ecommerce site owners, have to make their online visitors to be of much comfort or Trust an ecommerce site via Trust marks, and by their security strategies.

Every a transaction applies on the E-commerce has a security measures.

a. E-commerce transaction phases

a) Information phase
b) Registration phase
c) Negotiation phase
d) Payment phase
e) Delivery or shipment phase

Viruses, worms, Trajan horse are the biggest problems in the e-commerce world. They only disrupt e-commerce operations and should be classified as a Denial of Service (DoS) tool. Trojan horse programs allow data integrity and fraud attacks to originate from a seemingly valid client system and can be extremely difficult to resolve. A hacker could initiate fraudulent orders from a victim system and the ecommerce server wouldn_t know the order was fake or real. Password protection, encrypted client-server communication, public private key encryption schemes are all negated by the simple fact that the Trojan horse program allows the hacker to see all clear-text before it gets encrypted.

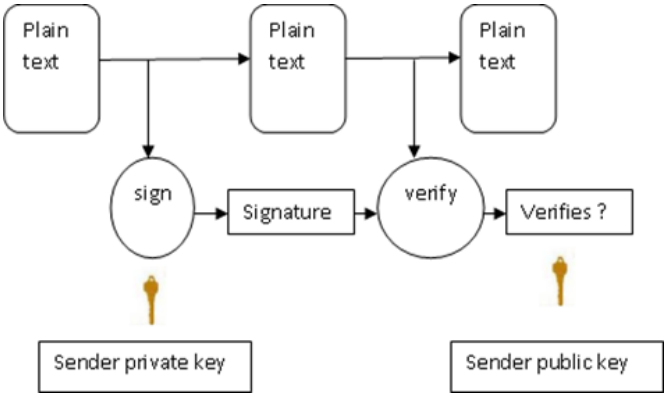

Fig.2:- Public/Private key process

The traditional authentication mechanism is based on identity to provide security or access control methods. To avoid this kind of problem some traditional encryption and authentication algorithm require for high computing power of computer equipment. How to improve the authentication mechanism and optimize the traditional encryption and authentication algorithm may be the focus of peer to peer (P2P) e-commerce.

All the E-Commerce transactions offer the banking industry with a great opportunity, but at the same time it creates a set of new risks and problems such as security threats. Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. As the money transactions are very important factor for e-commerce they require a coordinated match of algorithm and technical solutions.

Most of the e-commerce Transactions occur between buyers and sellers. This kind of transactions in e-commerce includes requests for quotation of prices, information, payment, delivery of orders, and finally services after receiving of the product to customer. The high degree of confidence needed in the authenticity, confidentiality, and timely delivery of such transactions can be difficult to maintain where they are exchanged over the Internet.

On e-commerce the Privacy and security can be viewed as ethical questions. At the same time the privacy and security area attracts a large amount of attention from the commercial sector because it has the potential to determine the success or failure of many business ventures, most obviously commerce activities.

In online shopping of e-commerce the payment function is the key issue to ensure that, the consumers or buyers are fast and convenient, there the safety and secrecy of the parties to a transaction, which requires a complete electronic trading systems.

III. PURPOSE OF E-COMMERCE STUDY

There are several kind of problems may arises over the e- commerce.

- ✓ Registering properly in an online portal
- ✓ Credit or debit card details
- ✓ Proper delivery addresses
- ✓ Loss or damage of products etc. so we need to give more focus on the below

a. Study the overview security of e-commerce
b. Understand the online shopping by giving proper information for delivery the products
c. Security of online payments
d. Discuss various issues in e-commerce
e. Understand the secure online shopping guidelines

IV. THE LIFE CYCLE OF A DIGITAL E-COMMERCE

Now a day‘s millions of people using online shopping because of easier and convenient. Instead of moving a physical shop customers use to buy at virtual shop because of saving of time, choice of various products, less price, delivery of product to customer door etc. Almost anything Can be bought such as music, toys clothing, cars, food and even porn. Even though some of these purchases are illegal we will be focusing on all the item_s you can buy legally on the internet. Some of the popular websites are eBay, iTunes, Amazon, HMV, Mercantile, dell, Best Buy, Flipkart, Snapdeal and much more.

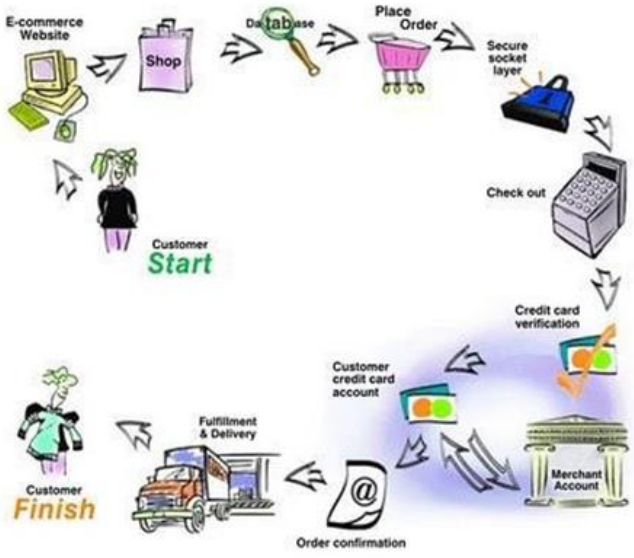

Fig 3:- E-commerce life cycle

Fig 4:- Online shoping phases

Online shopping to place an order

Start -> buyer -> e-commerce website->shop ->product database ->place order ->secure socket layer->check out->redirect to bank or link with bank-> credit or debit card verification-> buyers

account->payment made to seller-> redirect to again online site-> product delivery-> product received to customer

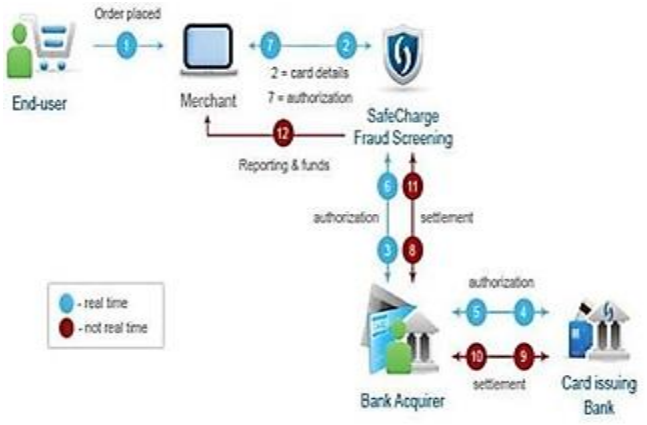

Fig 5:- E-Commerce steps to place an order and Digital Payment methods in E-commerce

V. SECURITY TOOLS FOR E-COMMERCE

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. There are various dimensions of e-commerce security.

- ✓ Integrity: prevention against unauthorized data modification
- ✓ No repudiation: prevention against any one party from reneging on an agreement after the fact
- ✓ Authenticity: authentication of data source
- ✓ Confidentiality: protection against unauthorized data disclosure
- ✓ Privacy: provision of data control and disclosure
- ✓ Availability: prevention against data delays or removal

There are various security measures to be taken for online shopping like

- ✓ Firewalls – Software and Hardware
- ✓ Public Key infrastructure
- ✓ Encryption software
- ✓ Cryptography
- ✓ Security certificates
- ✓ Digital Signatures
- ✓ Passwords
- ✓ Biometrics – retinal scan, fingerprints, voice
- ✓ Locks and bars – network operations centers
- ✓ Secured protocols

VI. VI.PURPOSE OF SECURITY

1. Data Confidentiality – is provided by encryption/decryption.
2. Authentication and Identification – ensuring that someone is who he or she claims to be is implemented with digital signature.
3. Access Control – governs what resources a user may access on the system. Uses valid IDs and passwords.
4. Data Integrity – ensures info has not been tampered with. Is implemented by message digest or hashing.
5. Non-repudiation – not to deny a sale or purchase Implemented with digital signatures.

Plaintext/Clear text – message humans can read. Cipher text – unreadable to humans, uses encryption.

Reverse process is call decryption. A cryptographic algorithm is called a cipher. It is a mathematical function. Most attacks are focused on finding the –key.

VII. SECURITY THREATS/PROBLEMS

The Distributed Denial of Service (DDoS):

This type of attack makes an attempt to prevent legitimate users from accessing some services or resources, which they are eligible for. DDoS attack affect the availability of site to users as server is overwhelmed with fake requests generated by attackers. No actual damage is done to the victim site.

SQL Injection:

Because the present encryption protection only can guarantee the security of data transmitting on the internet, but cannot check the content of data content filled by the user, and sent to the web server. If the attacker has filled the data that include the vicious SQL query instruction in the web page form, these query instruction together with HTML file will drill through the firewall and reach at to web server. When it is executed on the server, the vital information will be compromised.

Price Manipulation:

The total payable price of the purchased goods is stored in a hidden HTML field of a dynamically generated web page. In this attack an attacker can use a web application proxy to simply modify the amount that is payable, when this information flows from the user's browser to the web server. The final payable price can be manipulated by the attacker to a value of his choice.

Session Hijacking:

Session hijacking refers to taking control of a user session after successfully obtaining or generating an authentication session ID. The attacker mostly uses brute force or reverse engineered session IDs to get control of legitimate user's web application session while that session is still in progress.

Security Solutions to protect an E-Commerce System

The security of sensitive information such as credit card from attackers must get highest priority and every precaution must be taken to ensure security of online transactions through credit card by including the following solutions:-

Personal Firewalls: When connecting our computer to a network, it becomes vulnerable to attack. A personal firewall helps protect our computer by limiting the types of traffic initiated by and directed to our computer.

Secure Socket Layer (SSL): Secure Socket Layer is a protocol that encrypts data between the shopper's computer and the site's server. When an SSL-protected page is requested, the browser identifies the server as a trusted entity and initiates a handshake to pass encryption key information back and forth. Now, on subsequent requests to the server, the information flowing back and forth is encrypted.

Digital Signatures and Certificates: Digital signatures meet the need for authentication and integrity. A plain text message is run through a hash function and given a value: the message digest. This digest, the hash function and the plain text encrypted with the recipient's public key is sent to the recipient. The recipient decodes the message with their private key, and runs the message through the supplied hash function to that the message digest value remains unchanged. Very often, the message is also time stamped by a third party agency, which provides non-repudiation.

Web Server Firewall: A web server or web application firewall, either a hardware appliance or software solution, is placed in between the client end point and the web application. Web application firewalls protect cardholder data because all web layer traffic is inspected looking for traffic that is meant to exploit known vulnerabilities as well as patterns that may suggest a zero day exploit being launched against the application. A firewall ensures that requests can only enter the system from specified ports, and in some cases, ensures that all accesses are only from certain physical machines. A common technique is to setup a demilitarized zone (DMZ) using two firewalls. The outer firewall has ports open that allow ingoing and outgoing HTTP requests. A second firewall sits behind the E-Commerce servers. Another common technique used in conjunction with a DMZ is a honey pot server. A honey pot is source placed in the DMZ to

fool the hacker into thinking he has penetrated the inner wall.

Password policies: Ensure that password policies are enforced for shoppers and internal users. They ensure that passwords are sufficiently strong enough so that they cannot be easily guessed.

Installing Recent Patches: Software bugs and vulnerabilities are discovered every day. Even though many of them are discovered by security experts, rather than hackers, they may still be exploited by hackers once they became a public knowledge. That's why it is important to install all software patches as soon as they become available.

Intrusion Detection and Audits of Security Logs: One of the security strategies is to prevent attacks and to detect potential attackers. This helps understand the nature of the system's traffic, or as a starting point for litigation against the attackers. We should also lock any attempted unauthorized access to the system.

Technical Obstacles

a. The need to have a private networks and infrastructure for seller and buyer.
b. Robberies of bank accounts through the computer.
c. Tools for software development are constantly changing and quickly.
d. The lack of security system or confidence in the transactions.
e. Low numbers of Internet users because of high prices with a low individual income.

Non-Technical Obstacles

- High implementation costs
- Fear of providing personal data
- The inability of the consumer to see the product visually before buying it online.
- The proliferation of commercial fraud

VIII. SECURE ONLINE SHOPPING GUIDELINES

A. Use Familiar Websites

Use a trusted site rather than shopping with a search engine. Search results can be rigged to lead you stray, especially when you drift past the first few pages of links. If you know the site, chances are it's less likely to be a rip off. Beware of misspellings or sites using a different top-level domain (.net instead of .com, for example)—those are the oldest tricks in the book. Yes, the sales on these sites might look enticing, but that's how they trick you into giving up your info.

B. Look for the Lock

Never ever buy anything online using your credit card from a site that doesn't have SSL (secure sockets layer) encryption installed—at the very least. You'll know if the site has SSL because the URL for the site will start with HTTPS:// (instead of just HTTP ://). An icon of a locked padlock will appear, typically in the status bar at the bottom of your web browser, or right next to the URL in the address bar. It depends on your browser. Never give anyone your credit card over email.

C. Don't Tell All

No online shopping store needs your social security number or your birthday to do business. However, if crooks get them, combined with your credit card number for purchases, they can do a lot of damage. The more they know, the easier it is to steal your identity. When possible, default to giving up the least amount of information.

D. Check Statements

After successful shopping regularly during the holiday season and look at electronic statements for your credit card, debit card, and checking accounts. Make sure you don't see any fraudulent charges, even originating from sites like PayPal. (After all, there's more than one way to get to your money.)If you do see something wrong, pick up the phone to address the matter quickly. In the case of credit

cards, pay the bill only once you know all your charges are accurate. You have 30 days to notify the bank or card issuer of problems, however; after that, you might be liable for the charges anyway.

E. Use Strong Passwords

The best practice over online shopping is to change the passwords in periodically. Our tips for password can come in handy during a time of year when shopping around probably means creating new accounts on all sorts of e-commerce sites.

F. Think Mobile

Most of the young generation when they are going to purchase any product from online they start compare the products from various sites. The National Retail Federation says that 5.7 percent of adults will use their mobile devices to do comparison shopping before making a purchase. (And 32.1 percent will comparison shop online with a computer, as well.) For more complete information, be sure to also read our tips for shopping safely on a mobile device.)

G. Avoid Public Terminals

Hopefully we don't have to tell you it's a bad idea to use a public computer to make purchases, but we still will. If you do, just remember to log out every time you use a public terminal, even if you were just checking email.

H. Don't Fall for "Phishing" Messages

Identity thieves send massive numbers of emails to Internet users that ask them to update the account information for their banks, credit cards, online payment service, or popular shopping sites. The email may state that your account information has expired, been compromised or lost and that you need to immediately resend it to the company. a

Some emails sent as part of such –phishing‖ expeditions often contain links to official-looking Web pages. Other times the emails ask the consumer to download and submit an electronic form. For more information on phishing, visit www.antiphishing.org, and www.onguardonline.gov.

I. Count the Cards

Gift cards are the most requested holiday gift every year, and this year will be no exception. Stick to the source when you buy one; scammers like to auction off gift cards on sites like eBay with little or no funds on them.

J. Use Shopper's Intuition

Look at the site with a critical eye. And heed the old adage,

"If it looks too good to be true, it probably is." If any of These questions trigger a warning bell in your head; you will be wise to find another online merchant:

- Are there extraordinary claims that you question?
- Do the company's prices seem unusually low?
- Does itlooks like the merchant is an amateur?
- Are there alot of spelling or grammar errors?
- Does the company's phone go unanswered.
- The use of a post office box might not send up a red flag, but a merchant who does not also provide the company's physical address might be cause for concern.

IX. HOW PEOPLE SAFE WHEN SHOPPING ON-LINE

When a customer is a regular to online shopping he/she must be follow the following guide lines.

1. Before purchasing the goods on global sites make sure about the currency or exchange rates.
2. Find the cost of delivery charges and whether the product is delivered to your location or not.
3. If you are bidding on E-bay check out the buyers and sellers feedback. This should become standard before you ever place a bid.
4. Find the FAQ‘s on the online shopping sites for more information and their rules, acts and regulations.

5. If someone demands cash for a payment, –say no‖. Use your credit card to make your payment; this will protect you against fraud. Credit card companies refund accounts where fraudulent activity transpires.
6. Read the full term and conditions briefly before placing an order and also privacy policy of the e-commerce web site.
7. If you are unsure about a site, try doing a search with Google or any of the other search engines. You may find comments posted about the shopping site from other customers.

X. CONCLUSION

E-commerce is widely considered the buying and selling of products over the internet, but any transaction that is completed solely through electronic measures can be considered e-commerce. Day by day E-commerce and M- commerce playing very good role in online retail marketing and peoples using this technology day by day increasing all over the world. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security; Integrity: prevention against unauthorized data modification, No repudiation: prevention against any one party from reneging on an agreement after the fact. Authenticity: authentication of data Source. Confidentiality: protection against unauthorized data disclosure. Privacy: provision of data control and disclosure. Availability: prevention against data delays or removal.

XI. 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 Security Issues". 2008 International Seminar on Business and Information Management.

[3]. Biswajit Tripathy, Jibitesh Mishra. "Protective measures in ecommerce to deal with security threats arising out of social issues a framework" iaeme -issn 0976 – 6375(online) volume 4, issue 1, January- February (2013),

[4]. Shazia Yasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012

[5]. Abdulghader.A.Ahmed.Moftah."Challenges of security, protection and trust on e- commerce: a case of online Purchasing in Libya". issn: 2278-1021-ijarcce vol. 1, issue 3, May 2012.

[6]. A Sengupta, C Mazumdar "e-commerce security – a life cycle approach" sadhana vol. 30, parts 2 & 3, April/June 2005

[7]. Biswajit Tripathy, Jibitesh Mishra. "Protective measures in ecommerce to deal with security threats arising out of social issues – a framework" iaeme -ISSN 0976 – 6375(online) volume 4, issue 1, January- February (2013)

Cite this article as :

Pratap Kumar Kumar, Sashank Kumar, Biresh Kumar, "Usability and Security Issues in the Implementation of E-Commerce Website", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 3, pp.249-257, May-June-2020. Available at
doi : https://doi.org/10.32628/CSEIT206356
Journal URL : http://ijsrcseit.com/CSEIT206356