

## Design and Implementation of Secured E-Commerce System

Buthainah Fahran Abed, Rafah Shihab Al-Hamadani, Saja Ghassan Mohmmed

Computer Department, College of Education for Women/ University of Baghdad, Iraq, Dean of Informatics Institute for Postgraduate Studies/ University of Information Technology & Communications,

---

**Abstract :** E-commerce involves the process of buying, selling, and exchanging of products, services, and information via computer networks, primarily the Internet. The objective of this paper is to identify obstacles that facing the implementation of e-commerce system and providing security solutions to protect sensitive information. In the practical part the paper presents the design and implementation of secure site that allow the customers to search and buy products at anytime and anyplace through the Internet. All data are archived and stored in the proposed system, so that the administrator can easily search and retrieve information at any time and can make changes to them.

**Keywords:** Security, Safety, Encryption, E-commerce, Site, Attacker

---

### I. Introduction

E-commerce helps countries improve trade effectiveness and facilitates the integration of developing countries into the global economy. It allows businesses and entrepreneurs to become more competitive. This style of trading is canceled many of the limitations of traditional business. Existence of virtual markets, passages and stores that have not occupy any physical space, allowing access and circulation in these markets for a moment and anywhere in the world without leaving home is possible. Select and order goods that are placed in virtual shop windows at unspecified parts of the world and also are advertising on virtual networks and payment is provided through electronic services. The main components of E-commerce are: communication systems, data management systems and security. [1, 2] The programming languages that are used to develop the system are PHP and CSS. a.PHP: It is one of the most popular programming languages currently used in the creation of web applications. The web server does the interpretation and implementation of the code then sends the result to be displayed in the client browser. Because the web server is the one who interprets and executes its own code, it is so-called server-side scripting language. [3]

b.CSS (Cascading Style Sheets): It is a simple design language intended to simplify the process of making web pages presentable. CSS handles the look of a webpage, such as the color of the text, the style of fonts, the spacing between paragraphs, and how columns are sized and laid out. It provides a powerful control over the presentation of an HTML (XHTML) document. [4]

### Introduction to E-commerce

E-commerce is the business process such as buying and selling between the parties (buyer and seller) on the transfer of the right to use the goods or services over the internet networks with certain electronic mechanism. The electronic approval between the seller and the buyer to hold the sale or purchase is the essential element in defining the concept of E-commerce. [2] There are types of E-commerce are Business-to-Business (B2B), Business-to-Consumer (B2C), Consumer-to-Consumer (C2C), Peer-to-Peer (P2P) and Mobile commerce (M-commerce). [5, 6, 7]

- a. Business-to-Business (B2B): focus on selling to other businesses, an E-commerce company can deal with suppliers or distributors or agents, these transactions usually carried out through Electronic Data Interchange (EDI).
- b. Business-to-Consumer (B2C): online businesses attempt to reach individual consumers. Portals (Yahoo.com, MSN.com) offer users useful Web search tools and many services by charging advertisers for add placement, collecting referral fees for steering customers to other sites and charging for premium service portals can generate massive revenue. Besides that, content providers are a part of B2C business models. Content providers make money by charging subscription fees in distributing information content, such as digital news, also provides music, photos, video and artwork over the Web. This type has been used in the practical part of the proposed system.
- C: Consumer-to-Consumer (C2C): provides a way for consumers to sell to each other, with the help of an online market maker and promotes the opportunity for consumers to transact goods or services to other consumers. The rules of this community to compete are operated by the customer itself, check and decide his own basic

transaction prices. In C2C, the consumer depends on the market maker to provide a catalogue and search engine.

- d. Peer-to-Peer (P2P): enables Internet users to share files and computer resources directly without having to go through a central Web server.
- e. Mobile Commerce (M-commerce): refers to the use of wireless digital devices to enable transactions on the Web. Many types of transaction can be conducted by mobile consumers, including stock (trade, price comparisons, banking), which enabled by Computer-mediated networks.

### **Advantages and Disadvantages Of E-Commerce**

#### **Advantages of an E-Commerce System [5, 6, 7]**

- Buying 24/7:** everyone can sell and buy any time, night or day, 365 days a year.
- Decrease Transaction Costs:** the buy and sell from online store, can cut many unnecessary costs.
- Conduct a Business Easily:** we do not need to physically involve in company or crowds. We can buy from our house comfortable and easily choose goods from various electronically procedures without moving around physically.
- Comparison in Prices:** Everyone can easily compare fees among the various web sites and usually earn discounts on fees when compared with normal shop fees.

#### **Disadvantages of an E-Commerce System [5, 6, 7]**

- Security:** Everyone good or bad can easily open a web site, and there are many bad sites, which their aim is user's money.
- Guarantee:** there is no guarantee for product quality, orders might be damage in the post or things may look different online to what you actually receive.
- Social Relationships:** E-commerce allows users buying and selling goods without geographic limitations but no social contacts with other persons.
- Impact:** E-commerce and electronic business have impact on many districts of business for instance, economics, marketing, business law and ethics.
- Marketing:** The raise of information technologies and computer networks has many effects in business especially in field of marketing. In this case, they can decrease cost of operations and catch new markets for selling and transactions.

### **E-Commerce Challenges**

- Infrastructure requirements & Cost:** E-commerce systems require new technologies that can touch many of a company's core business processes, therefore significant investments in hardware, software, staffing, and training is required.
- Value: Businesses companies want to know that their investments in E-commerce systems will produce a return.**
- Diversity of providers:** The delivery of services is carried out by a large number of providers, some of which are charitable or nonprofit organizations, others are commercially established.
- Security:** A company's assets must be protected against misuse, whether accidental or malicious but that protection should not compromise a site's usability or performance nor make its development too complex.
- Existing Systems:** Companies need to be able to harness the functionality of existing applications into E-commerce systems therefore Internet E-commerce systems integrate existing systems in a manner that avoids duplicate function and maintains usability, performance, and reliability.
- Interoperability:** The linking of trading partners' applications in order to exchange business documents and must work together well in order to achieve business objectives. Interoperation between businesses reduces costs and improves performance and enables the implementation of more dynamic value chains.
- Multiple relationships among providers:** The Department purchases services on behalf of consumers from many provider organizations but the agency from which services are purchased is not necessarily the agency which provides the services.
- Governmental and political complexity:** The provider field is not the only one characterized by only diverse stakeholders and complex arrangements. The Government sector itself is divided along many lines.

### **Security Obstacle**

In E-Commerce system security hardware, software, and environment are the main critical and vulnerable points. Hardware security includes any devices used in running the E-Commerce website like network devices, web servers, database servers and client's computer. Securing the network with a properly configured firewall device that is only allowing ports needed for accessing the E-Commerce website which is an essential part of network security. The web server and database server should be isolated from other networks

using a network DMZ (demilitarized zone) to reduce possible intrusion from compromised computers on other networks behind the firewall. A DMZ is a separate network added between a protected network and an external network, in order to provide an additional layer of security. Software and routinely released patches should be regularly updated to fix holes in security. Website pages, where confidential information is being entered, should be secured with strong cryptography algorithm [10]. The secure an E-Commerce website is a dynamic process where new threats crop-up every day. To build a secure E-commerce application, the following five security features must be included [11, 12, 13]:

- Authentication:** to establish proof of identities and ensures that the origin of an electronic message or document is correctly identified.
- Integrity:** message should not be tempered in transit.
- Non repudiation:** non repudiation does not allow the sender of a message to refute the claim of not sending that message.
- Access control:** determines who should be able to access what.
- Availability:** resource should be available to authorized parties at all times.

**Security Problem**

-**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.

-**Cross-site script (XSS):** Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems they rely on. Exploiting one of these, they fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user as shown in figure 1.

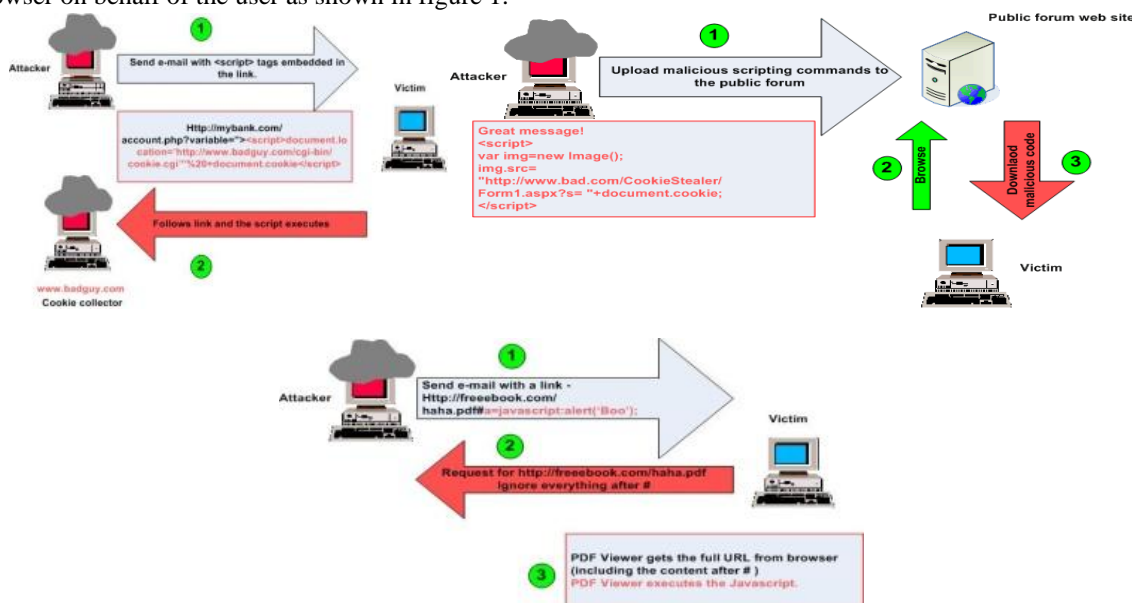


Fig.1. Cross Site Scripting

### **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 [10, 11, 14, 15, 16, 17, 18, 19]:

**-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 [19]**

- 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
- The low level of awareness and knowledge about the E-commerce.

### **The Proposed System**

- The proposed system presents the solution against security obstacle that e-commerce system faced when using sensitive information. The site is designed and the implementation allows the users to search and buy products through the Internet. All data are secured and stored in the proposed system, so that the administrator can easily search, retrieve and change information at any time. The proposed system using Internet in the implementation which is almost universal access therefore the site is protected against misuse, whether accidental or malicious through the use of multiple security strategies (such as user name and password) to prevent unauthorized access, and provide safety against the intruders. The sensitive information is encrypted to prevent a malicious attack on the system. The proposed system has been designed with online search and buy of

electronic products as shown in figure 2. The user can access to the E-commerce system homepage to buy a product by using his Visa-ID. After the user enters the VISA\_ID the system will check it this ID is correct or not. In case it's true the system redirect the user to purchase page else the system will show message that this ID is not correct. In purchase page the user will enter the quantity and confirm the purchasing process. After that the system will check if there is enough quantity in store and enough amount of money in VISA to complete the purchase process. The Database is designed by using WAMP server (Windows Apache MySQL/Php) as shown in figure 3 and it consist of four tables.

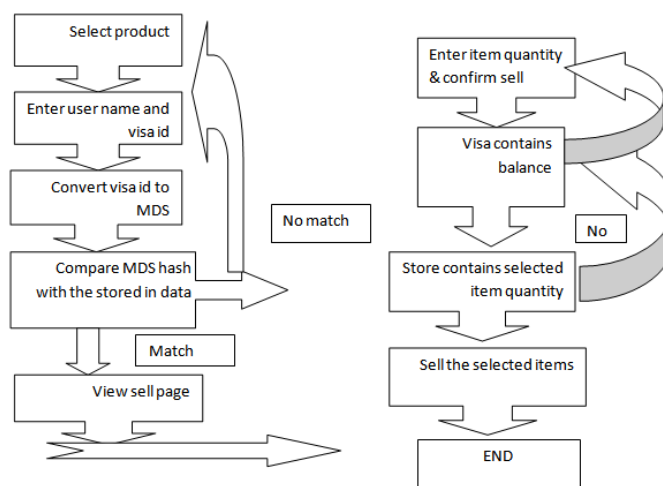


Fig.2. E-Commerce System Diagram

Fig.3. Database Design

Table (1) Items table

Field name	Field type	Field Description
Id	integer	Id of Item
Code	Text	Code of Item
It_name	Variable Character	Name of Item
P_id	Integer	Id of product that the item related to
Qty	Integer	Quantity of item in store
Price	Integer	Price of Item
Desc	Variable Character	Description of Item

Table (2) Products table

Field name	Field Type	Field Description
P_id	Integer	Product Id
P_name	Variable Character	Product Name
P_no	Text	Product Number

Table (3) Sell table

Field name	Field type	Field Description
S_id	integer	Sell id
It_id	Text	Item id
U_id	Variable Character	User id
price	Integer	Price of item
qty	Integer	Quantity of item sell

T_price	Integer	Total price of sell
date	Variable Character	Date of sell

Table (4) Users table

Field Name	Field Type	Field Description
id	Integer	User Id
name	Variable Character	User Name
pass	Text	User Password
email	Text	User E-mail
gender	Variable Character	User Gender
Visa_id	Text	User Visa Id
charge	Integer	Visa Charge
address	Variable Character	User Address
age	Integer	User Age

Table (5) Types of Users and Authorization Level

User Type	Authorization Level
Administrator	Add, delete and Edit items and products in e-commerce system
User	Regular user that can access, search and buy products using Visa ID

**Conclusion**

**-Privacy and Security in E-commerce System**

- a. Using user name and password to maintain security for accounts and to prevent unauthorized access. Provide secure account management against automated tools. Also sensitive information like password is stored as an encrypted text and not as a plaintext
- b. Prevent SQL Injection into input fields taken from the forms by using `mysql_real_escape_string( )` which increase the security.
- c. Using cryptography functions by using Message-Digest 5, known simply as MD5, is one of the quickest and simplest ways to add security to the files and messages that send and transfer in order to encrypt the sensitive information. In this paper, MD5 function is used to encrypt the VISA-ID information of the customer to provide more security to this sensitive data and compare it with the encrypted data stored in data base as shown in algorithm 1.

**Algorithm. 1.**

- I. `$visa_id=md5($visa_id1);`
- II. `$query4=mysqli_query($con, "select *from users wherevisa_id='$visa_id'");`
- III. If `visa_id` match with the value of inventory in the database then the customer will directed to sell page otherwise a message will appear to customer to retry the process.

**- Implementation of the Booking System**

The Software tools that used to create and implement the system are: PHP server side script interpreter, WAMP Server that based on Apache server used to provide web, database and ftp services, MySQL data base management system (DBMS) to store and retrieve data. Figure 4 shows the Home page of an E-commerce system

Figure 4 shows the Home page of an E-commerce system



**Fig.4.E-commerce System Home Page.**

Figure 5 shows how the products are selected and presented with some details like product name and price in products page. After the user selects the products, the system redirects the user to the purchase authentication page shown in figure 6. The user enters the username and VISA-ID in the textboxes, if the VISA-ID is correct then the system redirect the user to the sell page to buy the selected products.

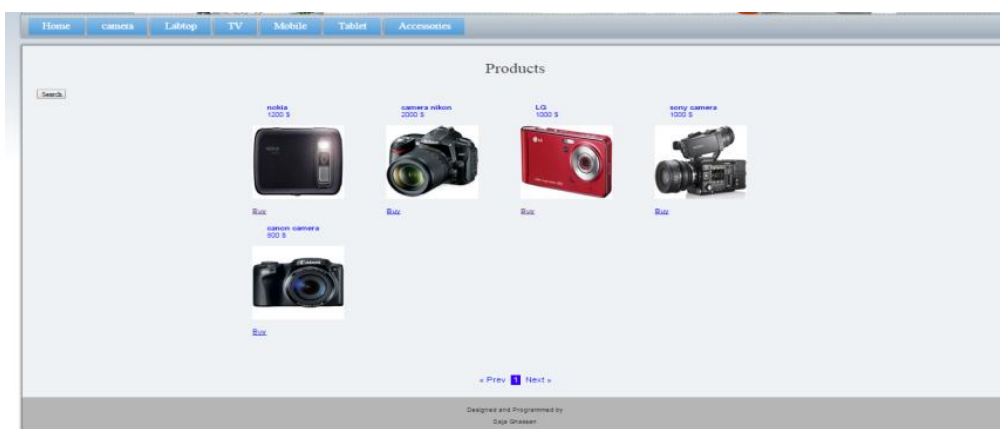


Fig.5. Products Page.

The page in figure 6 shows the information of the selected product. The user can enter the quantity required and confirm the sell process buy select confirm selling checkbox. Figure 7 shows the purchase page. Figure 8 shows information about the product purchased by the customer. This information includes the product purchased, the previous charge, current charge, quantity of product purchased and total price.

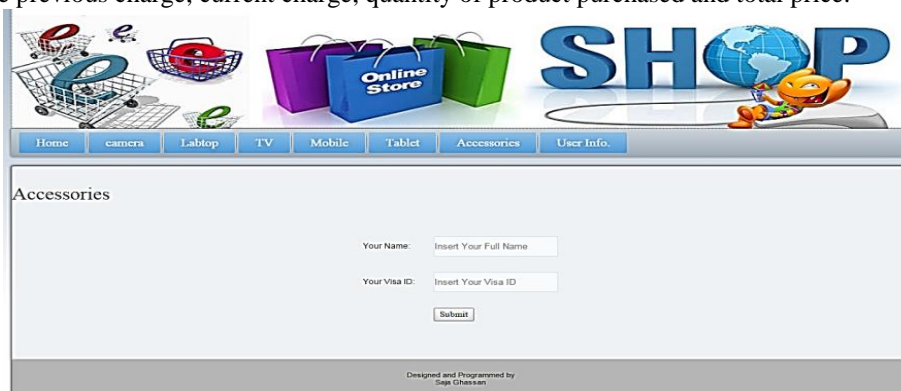


Fig.6. Sell Authentication Page



Fig.7. Purchase Page.

Figure 9 shows the administrator login page. This page allows the administrator of E-commerce system to login to the administration phase. It contains two fields; username and password. The Login information are sent to the server after filling out all fields and the server checks if the user name and password are correct, if correct it send the administrator to the administration phase, otherwise the page show a message to the user that the user name or password error.



Fig.8. Purchase confirmation Page



Fig.9. Administrator Login Page

Figure 10 shows how the administrator can add new item information to the system. This page contains fields such as item name, item quantity, item code, item price and description. In figure 11 allows the administrator to edit items information? Figure 12 shows how the administrator can add new user to the E-commerce system

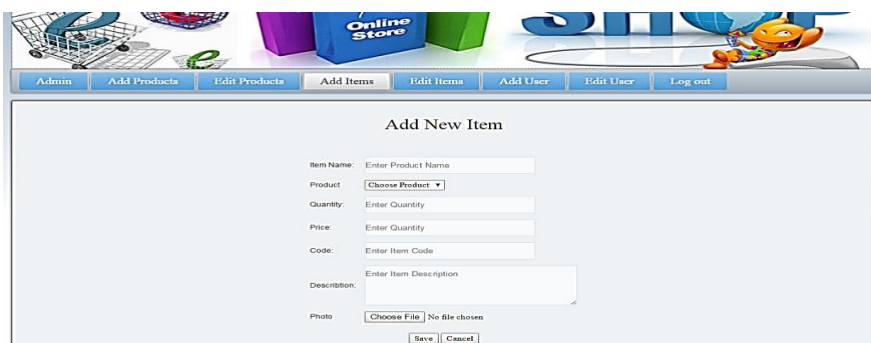


Fig.10. Add New Item Information



No.	Item name	Quantity	Price	Edit
1	nokia	9	1200	
2	camera nikon	26	2000	
3	LG	6	1000	
4	Samsung Mobile	0	500	
5	Samsung taps	5	2000	
6	HP	1	2500	
7	dell	4	2000	
8	sony	3	2300	

Fig.11. Edit Item Information

Fig.12. Add User Page.

### Conclusion

The needs of the citizens should always be under consideration when implementing and improving e-commerce services; because citizens are considered to be at the core of every service and the responsibilities of the authorities. Implementing and developing e-commerce is not free of any obstacles, and barriers. Therefore, in this paper it was discussed and accommodates the solution to security was accommodated in the proposed system.

### References

- [1] "Introduction to Computers", [http://www.b-u.ac.in/sde\\_book/bcom\\_ca.pdf](http://www.b-u.ac.in/sde_book/bcom_ca.pdf)
- [2] Y. A. Nanehkaran, "An Introduction To Electronic Commerce", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2ISSUE 4 , APRIL 2013. ISSN 2277-8616
- [3] R. Lerdorf, K. Tatroe, B. Kaehms, and R. McGredy, "Programming PHP", Published by O'Reilly & Associates, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472. [http://www.tutorialspoint.com/css/css\\_tutorial.pdf](http://www.tutorialspoint.com/css/css_tutorial.pdf)
- [5] M. Niranjnamurthy, D. Chahar, "The study of E-Commerce Security Issues and Solutions", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013, ISSN (Online) : 2278-1021
- [6] N. Shafiyah, R. Alsaqour, H. Shaker, O. Alsaqour and M. Uddin, "Review on Electronic Commerce", Middle-East Journal of Scientific Research 18 (9): 1357-1365, 2013 ISSN 1990-9233, © IDOSI Publications, 2013, DOI: 10.5829/idosi.mejsr.2013.18.9.12421
- [7] D. Pandey, V. Agarwal, "E-commerce Transactions: An Empirical Study", IJARCSSE All Rights Reserved Page | 669 Volume 4, Issue 3, March 2014, ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering, Research Paper Available online at: [www.ijarcsse.com](http://www.ijarcsse.com)
- [8] P. B. Rane , B.B.Meshram, "Transaction Security for E-commerce Application ", International Journal of Electronics and Computer Science Engineering 1720 Available Online at [www.ijecse.org](http://www.ijecse.org), ISSN- 2277-1956 ISSN 2277-1956 /V1N3-1720-1726
- [9] T. Castleman, P. A. Swatman and Craig M. Parker, "Issues in the Implementation of Electronic Commerce in the Human Services: Reflections on the Victorian Initiatives", <http://www.deakin.edu.au/study-at-deakin/find-a-course/business-analytics>
- [10] "E-commerce and Security-1dl018", spring 2008, Uppsala University / Computer Science Division / Uppsala Database Laboratory : E-Commerce and Security - 1DL018, <http://www.it.uu.se/edu/course/homepage/ehandel/vt08/>.

- [11] J. Singh, "Review of E-Commerce Security Challenges", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization)Vol. 2, Issue 2, February 2014, ISSN(Online): 2320-9801
- [12] A. Kahate, "Cryptography and Network security", Tata McGraw Hill Education Private Limited, 2ndedition, 2008.
- [13] "SQL Injection", [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection). <http://www.symantec.com/connect/articles/common-security-vulnerabilities-e-commerce-systems>.
- [15] J. Botha, and C. Bothma , P Geldenhuys,"Manging E-commerce" , Published 2008 by Juta & Company ISBN, 0702173045 (ISBN13: 9780702173042)
- [16] "Critical Threats e-Commerce hosting", <http://www.plaveb.com/blog/3-critical-threats-To-e-commerce-hosting>.
- [17] " E-Commerce site security", <http://www.applicure.com/solutions/eco>. [http://www.tutorialspoint.com/css/css\\_tutorial.pdf](http://www.tutorialspoint.com/css/css_tutorial.pdf).
- [19] M. O. El-fitouri , "E-Commerce in Developing Countries: A Case Study on the Factors Affecting E-commerce Adoption in Libyan Companies" , M Othman El-fitouri Int. Journal of Engineering Research and Applications, ISSN :2248-9622, Vol. 5, Issue 1( Part 1), January 2015, pp.102-115, [www.ijera.com](http://www.ijera.com)