

## High-Security Online Shopping Website Using Web Programming and The Network Security Technology

Joel Kabangu Kabobo<sup>1\*</sup>, Shaikh Mohammad Bilal Naseem<sup>2</sup>

<sup>1</sup>Department of Computer Science

Somaiya Vidyavihar University Mumbai, India

<sup>2</sup>Assistant Professor, Dept of Computer Science/IT Somaiya

Vidyavihar University Mumbai, India

<sup>1</sup>[joelkabobo@gmail.com](mailto:joelkabobo@gmail.com), <sup>2</sup>[mohammadbilal@somaiya.edu](mailto:mohammadbilal@somaiya.edu)

### Abstract

*Nowadays, lifestyle of people is changed. People don't like waste time going to the markets and make a long line. So, E-shopping is a benefit as it saves a lot of time. Online shopping is a process that helps easily and directly to buy products from a merchant without an intermediary service over the Internet. Customers can visit web stores from their house or wherever they are and shop by sitting in front of the computer or mobile. One of the most advantages of shopping online is particularly during the holiday season, it alleviates the need to wait in long lines or search from a store for a particular item. So, most Ecommerce are hacked and users' data and transactions are used by hackers for trying to steal users' money with the user's bank detail hacked, and sometimes even the business owner is hacked and lose the information of his E-commerce store. So, online shopping required high-security technology to protect the user's data and transactions, and to secure the company against all types of misused actions from the hacker side over the internet.*

**Keywords:** Website, E-commerce, Web Programming, Network Security, Cyber Security.

### 1. Introduction

The development of high-security online Shopping will play a huge role in the safety of the users and the company owner while using an online shopping website.[10].

In this technological time, the majority of people prefer to shop online in front of their computer, smartphone, or tablet. So, if the online shopping website is not secured from hacking and fraud then the business owner may have to pay a big price in terms of the stealing of personal information and loss of customers. hence hacking and fraud are becoming a real problem for e-commerce websites from both the user and the business point of view. [2]

I am also a victim of hacking. I used one e-commerce named “Shopcloues” for buying a t-shirt and because of the lack of security in that e-commerce, the hacker collects my information from them and wanted to steal me money. they called me and told me that I won a prize of 14,80,000.00 Indians rroupis for the competition game Lucky Draw organized by “Shopcloues” for his customer and they sent me one link for checking whether I won or not. The first thing I remark is the site was not secure, there was not the letter ”s” in the Hypertext transfer protocol (Http) of this link which is used to show if the website is secure or not. if it is secured it will be “https”. So by that, I got the doubt. and secondly, I remarked that in the URL of this website it is written “Shopclouse” instead of the real “Shopcloues”.

By this second remark, I come to know that they are hackers. So, you need to be careful to pay attention to these types of details they just interchanged the last two letters of the name of the real “Shopcloues” and they wrote “Shopcloues”. And the worst thing is inside this fake website if I write my mobile number as they asked me, all my profile information such that name, mobile number, address and order that I did in the real “Shopcloues” appear there, and they confirmed me that I won the prize. They even called me by my phone numbers and told me to transfer them 6500rs for government tax and registration then in five minutes, I will receive my prize what I did not do because I recognized their fraud.[3] So, one of the most important things when building an ecommerce site is your site security. Because You’re collecting sensitive information from your customers, including their mailing address and credit card information. If a hacker steals any of those data, your reputation as a secure, trustworthy business is going to take a huge hit, and you’re likely to lose many customers. [1].

## **2. Problem Statement**

### *A. Statement of Problem*

As security is most important in an e-commerce website, I wanted to build a strong security e-commerce website where the business owner and users will be secure from all attacks of hackers on the internet. So, our system will consist of online shopping for clothes on the internet. In this e-commerce, users can search for Clothes type and chose the desired one and choose also the colour and the number of clothes that he chose. Once the choice is made, the customers need to login for placing an order. If login is done then the user has to place the order and choose the payment method by cash or card. If by cash, the customer will see the order confirmation details, and if by card he has to fill the card details and confirmed the payment, thus he will see the confirmation message of his order on the screen, and the date and address of the shipment. So, our system will be implemented in such a way that all these operations like user information and transaction and the entire website will be secure in a manner that the hackers cannot steal any data

### *B. Existing Systems*

Nowadays, Online shopping is becoming increasingly popular for a variety of reasons. There are certainly other reasons like augmentation of gas price, difficulty in finding and going to traditional stores often associated with shopping malls, and other traditional stores to contribute to the increased interest in online shopping [4]. There are many online shopping websites in today world which help people to shop online however the most popular are Amazon, eBay, Etsy, InspireUplift, Overstock, Wish, Alibaba, Aliexpress, etc. [5] and some of those systems are implementing various technologies to secure their system for the satisfaction of the user and the safety of their business. Like Amazon the most popular e-commerce, to secure their system makes use of the service socket layer ( SSL) to keeps traffic between their customer and the website; Amazon obscured header information to prevent hackers from quickly narrowing down the attack routes; amazon secure cookies to prevents the client malware from impersonating the customers; amazon uses Emails and DNS protection to verify emails and web addresses are real.[6]

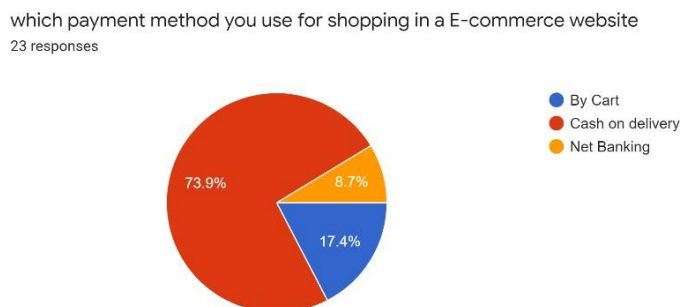
### 3. Survey Analysis

For a better overview of the audience about the impact of Online Shopping website in today's world, I decided to create a google form which will help to determine the statistic of people using Ecommerce for shopping, the payment method that they use, and the problem they are facing for lack of security in the system. Please notice that the opinion of 23 persons was taken into consideration and produce the following results:



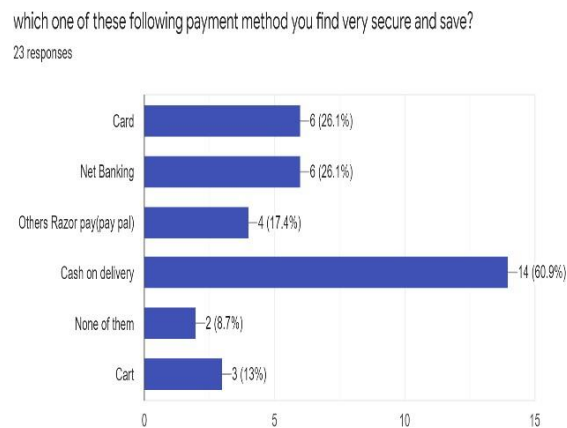
**Figure No. 1**

The given figure shows us that 100% are the people who already used an e-commerce website for shopping. This static proves that there is not a single person among 23 who have never used the e-commerce website for shopping.



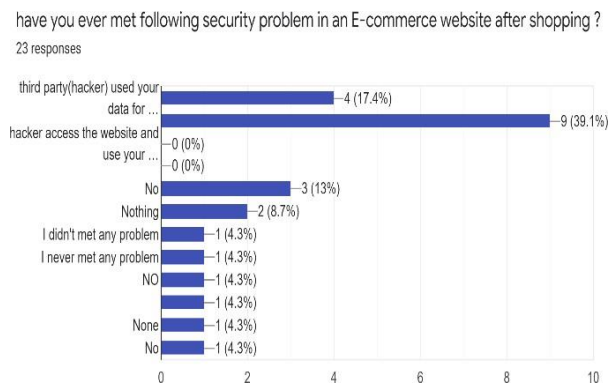
**Figure No. 2**

This question helps to see which payment method customers use to order. We can see that in figure2, 73.9% of the people use cash on delivery to pay their orders. 17.4% use Net Banking to order and 8.7% used cards. This given chart shows us that majority of people prefer to pay cash on delivery of their order.



**Figure No. 3**

In figure NO.3, it was asked people which payment method they find secure and safe. And the result of the statistic shows us that 60.9% find cash on delivery very secure and save, 26.1% use Card or Net Banking and others used razor pay like PayPal, Paytm or google pay. This statistic shows us that many find cash on delivery secure and save as they pay only if they receive their order and it needs no transaction through the internet, it's hand to hand.



**Figure No. 4**

When I asked about the security problem that people already met on an e-commerce website, I found that 39.1% of people their information was hacked from the e-commerce that their use and their mobile number was collected by hackers who called them to try to swindle them. We found also 17.4% of people their data like account details were hacked from the e-commerce and the hacker steal their money or change their order or do some modification without their permission. This statistic proves to us that 12 persons out of 23 met the problem because of security issue in the e-commerce system what it has to be solved

#### 4. Methodology

This is a fundamental process that appears in figure5. That shows how the system will work. The people can access the website everywhere if he's having the internet in his portrait. He can navigate through the website, and see which product the site offer and which products are available. So, the system is for the following stakeholders:

##### 1) Admin:

The admin can access and navigate through the website without login but if he wants to do any other process, he has to login with his unique identifier number et his password. Once done, he has now the right to manage the Store. He can add, delete or modify a category of product; he can add, delete or modify the product; he can manage order even it is canceled; he can manage the payment for better transparency; he can check feedback of customers and reviews; at the end, the admin will give report all whatever operation he did. and in the last, he will stop the system.

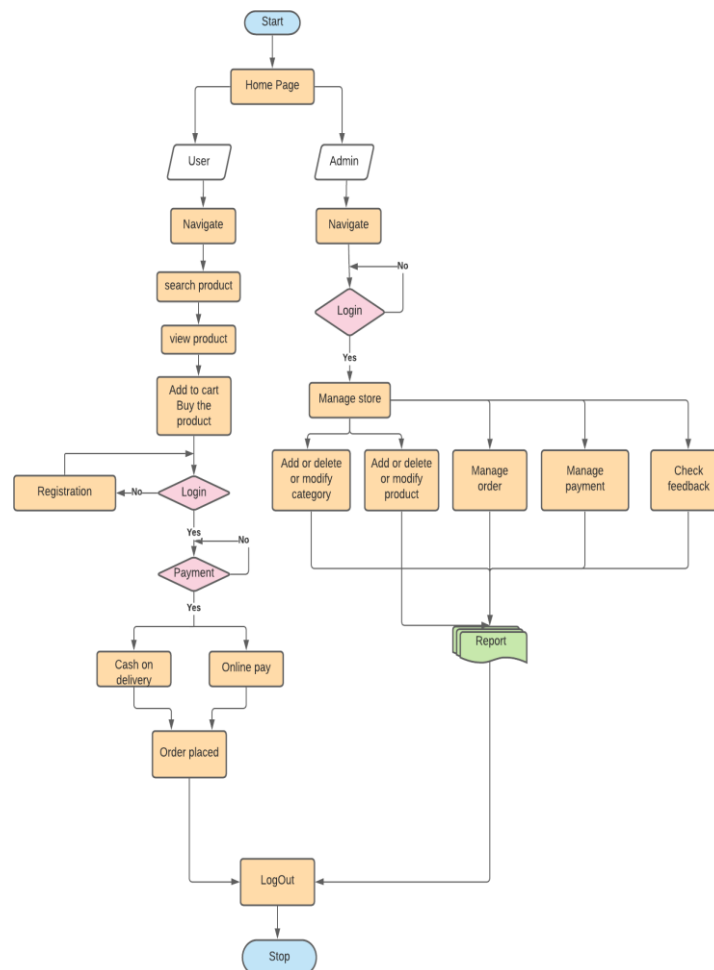


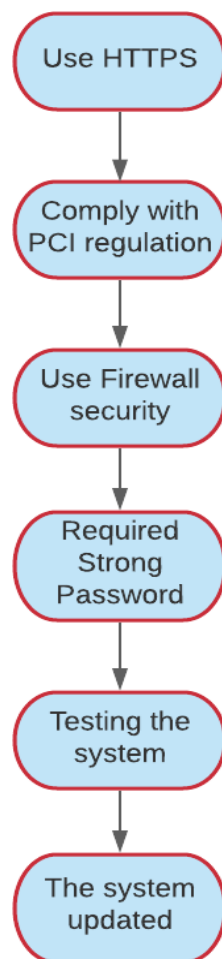
Figure No. 5. The flow diagram of the system

##### 2) User:

The user can access the website and navigate through the home page without login in; he

can search for a particular product, add the product to the cart and place his order for buying

the product. but he needs to login first before making the payment. If he is a new user, the system will ask him to register as shown in figure9 with a strong password. once he login, he becomes a customer member. He can now proceed to the payment. and for payment, the system will trigger him which payment method he wants. So, he has the choice between going for online payment or going for cash on delivery. once the payment process is chosen and completed, the order will be placed and the user will receive the confirmation. Hence the order is done. The user can do the same procedure for other orders or he can logout and stop the system.



**Figure No. 6. Diagram of security algorithm of the system**

As security is the most important field of my system, we will implement some technologies in my system to secure customers, business owners, and our entire system from hackers. So those techniques are shown in progression in Figure 6. And will be explained in the following section:

### 1) HTTP with SSL = HTTPS

The use of HTTP (hypertext transfer protocol) with SSL (secure socket layer) which is the standard security technology between a web server and a browser offers more security to my system. as SSL ensures that all data passed between the web server and browsers remain private and integral. SSL helps the system to ensure the protection of sensitive financial and personal information throughout the process. So, HTTP with SSL is known as HTTPS (hypertext transfer protocol secure).

this secure aspect will help protect personal user data like credit card numbers, passwords, and addresses.[7]

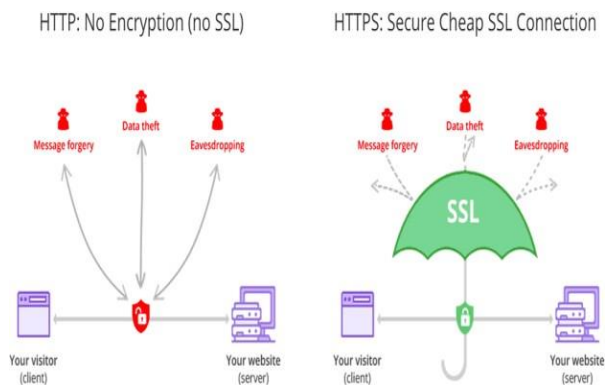


Figure No. 7. Web secured with SSL

### 2) Comply with PCI regulations

Like my system will accept credit or debit cards, it must comply with the regulations outlined by the PCI (payment card industry) Security Standard Council. These regulations make sure that any financial data stored by the business is secure. If you're not complying with all of the PCI regulations, you may face large fines in addition to leaving customer information vulnerable to hackers [1].

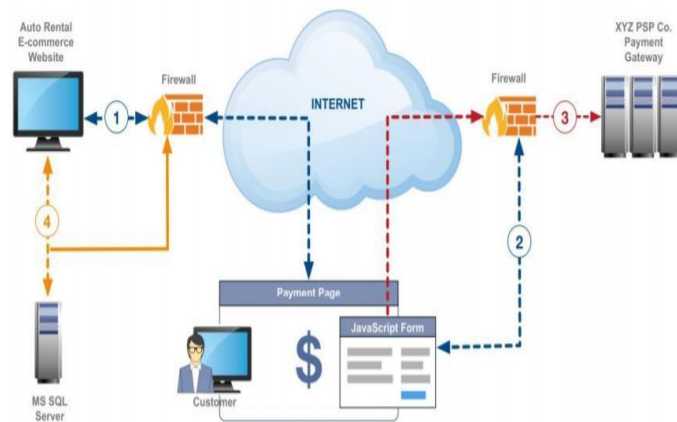
Consider using third-party payment applications that are PA-DSS (payment application data security standard) validated and noted on the List of Validated Payment Applications as "acceptable for new deployments" Note that some payment brands require the utilization of PADSS validated payment applications where third-party payment applications are in use. Merchants should consult their acquirers or the payment brands to know applicable requirements. The correct installation of a payment application is critical to the protection of card data. The payment application's PA-DSS Implementation Guide (obtained from the payment application vendor) should be followed when installing and configuring the payment application to ensure that the product is implemented securely and in a manner that supports PCI DSS compliance.[8]

### 3) Use Firewall security

Many virus attacks will be avoided with a Firewall. A firewall may be a fair layer of your network that alerts you whenever any suspicious events occur on your server. To avoid SQL injection and cross-site scripting attacks, online merchants should have an additional layer of security to a customer's login page, contact forms, and search queries. Firewalls monitor traffic coming onto the server and I can set a predefined access control list to allow only

consented communication [2].

So, I will implement a web application firewall to help block malicious data.



**Figure No. 8. Firewall illustration**

#### **4) Require Strong Passwords**

One-way hackers can gain entrance into your site is to use a brute force hack, which basically starts putting combinations of letters into your site login, hoping to urge lucky and crack your password. Using randomized and long passwords makes this ton less likely. So employees and customers must use strong passwords, a combination of upper- and lowercase letters, numbers, and symbols to register in the system as shown in Figure 9. Also, they will be advised to change their passwords every 6 months, if not more often.[7]

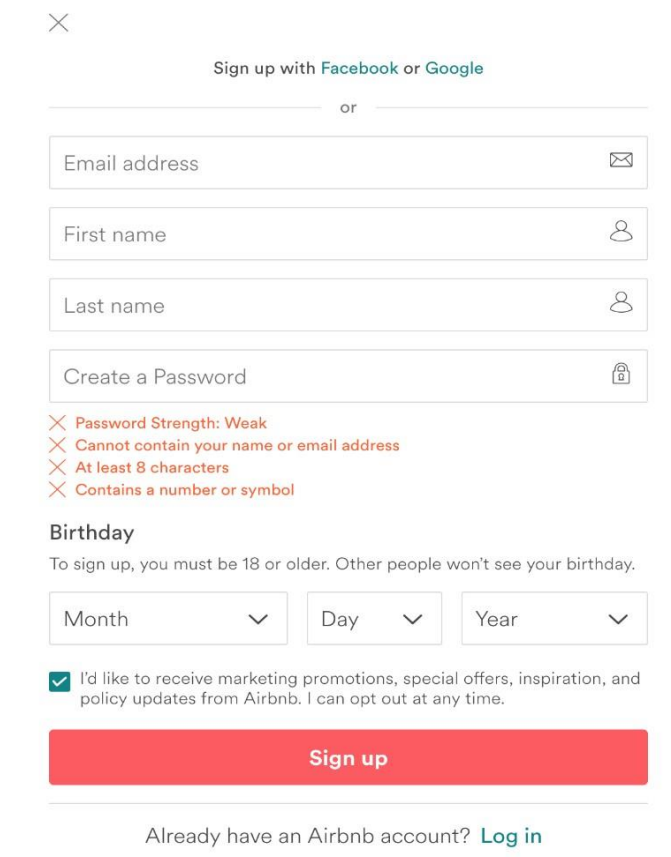
#### **5) Testing the system**

Once you have got your network as strong as possible, you would like to check it by hiring someone to perform penetration testing. This testing, sometimes referred to as ethical hacking, involves someone attacking your e-commerce site as if they were a hacker. If they are ready to gain access to your customer information, you recognize your site isn't as prepared as you'd love it to be. Ethical hacking will give you an idea of all of the weaknesses you still have to shore up and is a vital step before you make your e-commerce website live for customers to use.[1]

#### **6) Keep the system updated**

To avoid being a cyber victim, software companies frequently release the newest versions that also fix bugs in software and supply smooth functionality. Whenever an update is available to my system, I will update it just because cybercriminals always take advantage of those software or systems that are not updated regularly.[2]





The image shows a registration form for a system. At the top, there is a close button (X) and a link to sign up with Facebook or Google. Below this, there is a horizontal line with the word "or" in the center. The form consists of several input fields: "Email address" with an envelope icon, "First name" with a person icon, "Last name" with a person icon, and "Create a Password" with a lock icon. Below the password field, there are four error messages in red text: "Password Strength: Weak", "Cannot contain your name or email address", "At least 8 characters", and "Contains a number or symbol". Below these errors is a "Birthday" section with the text "To sign up, you must be 18 or older. Other people won't see your birthday." and three dropdown menus for "Month", "Day", and "Year". Below the birthday section is a checkbox with the text "I'd like to receive marketing promotions, special offers, inspiration, and policy updates from Airbnb. I can opt out at any time." and a red "Sign up" button. At the bottom, there is a link "Already have an Airbnb account? Log in".

**Figure No. 9. Registration form of my system.**

## 5. Conclusion

This proposed work will provide a website that helps to online shopping of clothes where people can order wherever and whenever he wants without worrying about being hacked and with the assurance of the security of this transaction or payment. As customers now prefer security first, and if your eCommerce website is lacking security measures, then you may say good-bye to your business revenue. From the security measures of my system, ecommerce business owners can protect their online stores from hacking and they can ensure their customers by protecting the e-commerce website with robust security. It is essential to protect your e-commerce website not just for potential revenue but for the sake of your customers [2].

## 6. Acknowledgement

We like to express our gratefulness to M.E, Shaikh Mohammad Bilal N, Assistant professor, Department of Computer Science, Somaiya Vidhyavihar University, Mumbai for providing guidance throughout the project work.

## 7. References

- [1] 10 ways to secure your e-commerce site from cyber-attacks, published by ShipWorks.
- [2] 10 Tips to protect your e-commerce website against hacking and fraud, 18th September 2018, published by Tweak Your Biz
- [3] <http://shopcluse.luckydraw.net.in/>.
- [4] C.K. Sunitha, “ONLINE SHOPPING- AN OVERVIEW”, June 2014, Research Gate.
- [5] 25 Most Popular Online Shopping Sites and Online Stores 2020, 14th July 2020, published by IDEASPLUSBUSINESS.
- [6] How does Amazon handle cybersecurity, 27th Aug 2020, published by UpGuard.
- [7] Jennifer Lonoff Schiff, “7 ways to protect your e-commerce site fraud, hacking and copycats”, 7th November 2016, published by CIO.
- [8] PCI Security Standards Council, “Best Pratique for Securing E-commerce”, April 2017, page 36, 55-56
- [9] Mihir Sanghrajka and Shaikh Mohammad Bilal N, “Analysis over security threats of Mobile Communication”, March 2020, published by Elsevier SSRN
- [10] Tutorialspoint, “E-commerces-Security System”,  
[https://www.tutorialspoint.com/e\\_commerce/e\\_commerce\\_security.h](https://www.tutorialspoint.com/e_commerce/e_commerce_security.h)

