A NEW MODEL METHOD TO SECURE AN E-COMMERCE WEBSITE

TECHNICAL ANSWERS FOR REAL WORLD PROBLEMS (CSE3999)

REPORT

Winter 2020-21

by

18BCI0179 - Shouya Maheshwari

18BCI190 - Laksh Gupta

18BCI0197 - Nimish Shah

18BCI0214 – Mihir Srivastava

in partial fulfillment for the award of the degree of

B. Tech

in

Computer Science and Engineering

School of Computer Science and Engineering

May, 2021

Title

A NEW MODEL METHOD TO SECURE AN E-COMMERCE WEBSITE

Abstract

We looked into the security design of many websites both e-commerce related and other websites, we noticed some deficiencies. So in this project we have decided to come up with a new approach to securing a website, we also plan to implement this new technique on a sample e-commerce website that we will create.

The scope of the website would be:

> We wish to show the users all the shops close to them and allow them to search for the products that they want through the options provided on our website. They should be able to create a cart that contains all the items they wish to buy. Then the website should show the user a comparative analysis of the prices at each shop and the approximate final price for the whole cart for every shop available nearby. The website should also notify the user if a product is not available.
>
> There is also a feature for the customer to send their list to the shop so that the shopkeeper can keep the items ready so that the customer can only pick the groceries quickly.

After we apply this new method on our website w then also plan to test this website against standard tools like Burp Suite and nessus.

Literature survey (Summarize five papers most relevant to your problem)

[1] *Cyber Security; Issue and Challenges in E-Com*

Online business refers to the trading of products and ventures over the Internet. Shopping through web based business has entered all fragments of merchandise going from food supplies to electronic products and even vehicles. Fast development in versatile registering and correspondence innovations has encouraged the prevalence of internet business. The primary

hindrance in development of online business is **digital misrepresentation and data fraud**. Programmers are individuals who commit cybercrime. Consequently, helpless security on web based business web workers and in clients PCs is a central issue to be settled for quick development of internet business. **This paper gives bearings to online business security in order to improve client trust in internet business shopping.**

[2] *E-Commerce Security Challenges: A Taxonomy*

With the rise of the Global Economy, and with a steadily growing degree of buyers doing their business generally by methods for on the web or mobile phones, electronic exchange, web business, is rapidly being seen as the best methodology worldwide at the piece of a catch. In this way, developing a fruitful Web based plan of action is getting fundamental for any front line business. Regardless, an **association should address assorted new security challenges and make certain to keep up the best assumptions for electronic business security, to guarantee both themselves and their customers**. A powerlessness to hold quick to serious web business security can achieve **lost data, compromised trade information**, just as the appearance of the customer's money related data. This can prompt legal and budgetary danger, similarly as a negative impact on the association's reputation. These new security challenges are the results of the use of the new advancement and correspondence medium, and the movement of information from large business to undertaking, from enormous business to buyers, and moreover inside the endeavor. **This paper presents the particular development and determined pieces of the electronic business generally speaking, and perceives and arranges the different kinds of security challenges standing up to online business associations explicitly.**

[3] *Y. Wen, C. Zhou, J. Ma and K. Liu, "Research on E-Commerce Security Issues," 2008 International Seminar on Business and Information Management, Wuhan, 2008, pp. 186-189, doi: 10.1109/ISBIM.2008.168.*

This paper deals with different security issues looked by internet business sites that are facilitated on open organizations. The center issue examined is security of E-trade exchanges and **two parts of it, which are the security of the framework and the security of data**. The two significant issues examined are Computer network issues and The security issues of deal. There are likewise some proposed security control necessities at the cycle of E-trade exchange. **They are: The legitimacy of the data, The secrecy of data transmission**, The honesty of the exchange data, The uprightness demands while putting away the information ought to forestall illicit annihilation or change on the site, Non-renouncement of data, The credibility of the brokers personality. The two dealers do without a doubt exist, not phony, The data can not be altered. The message on the organization can not be adjusted.

[4] *The Study of E-Commerce Security Issues and Solutions*

Sangeetha M K Prof. Dr. Suchitra R Jain University, Bangalore Jain University,Bangalore

This paper deals with protection and security issues looked at by current online business sites and how these issues looked by the clients are confining them from connecting more with these sites. It additionally expresses that Web internet business applications that handle installments have more consistency in issues, are at expanded danger from being focused than different sites and there are more prominent results if there is information misfortune or adjustment. The paper at that point **additionally proceeds to examine web security as a rule and how quickly developing internet business is a test of online security all in all.**

[5] *Kefa Rabah , 2006. Implementing Secure RSA Cryptosystems Using Your Own Cryptographic JCE Provider. Journal of Applied Sciences, 6: 482-510.*

Scrambling and unscrambling information: Encryption works at the byte level, so nearly anything can be encoded. **When you have a key and a code, you're all set. It ought to be noticed that a similar calculation should be utilized for both the key and code. You can't have a key introduced with DES and a code instated with RSA.** The Cipher object utilizes similar strategies to scramble and decode information, so you should introduce it first to tell it how you need managed the information:

```
rsaCipher.init(Cipher.ENCRYPT_MODE, publicKey); //Initializes the Cipher object.This call initi
alizes the Cipher object and gets it ready to encrypt data. The simplest way to encrypt data is
invoking the doFinal method on the Cipher object passing in a byte array:
data = Hello_World.getBytes();//Calculates the ciphertext with a plaintext string.
result = cipher.doFinal(data);
```

The outcome will currently contain **the scrambled portrayal of the passed-in information.** It's similarly simple to unscramble similar information. In any case, before we can do that, we should reinitialize the Cipher protest and prepare it for decoding.

[6] *Design and implementation of an improved RSA algorithm, Yunfei Li ; Qing Liu ; Tong Li,2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT),10.1109/EDT.2010.5496553*

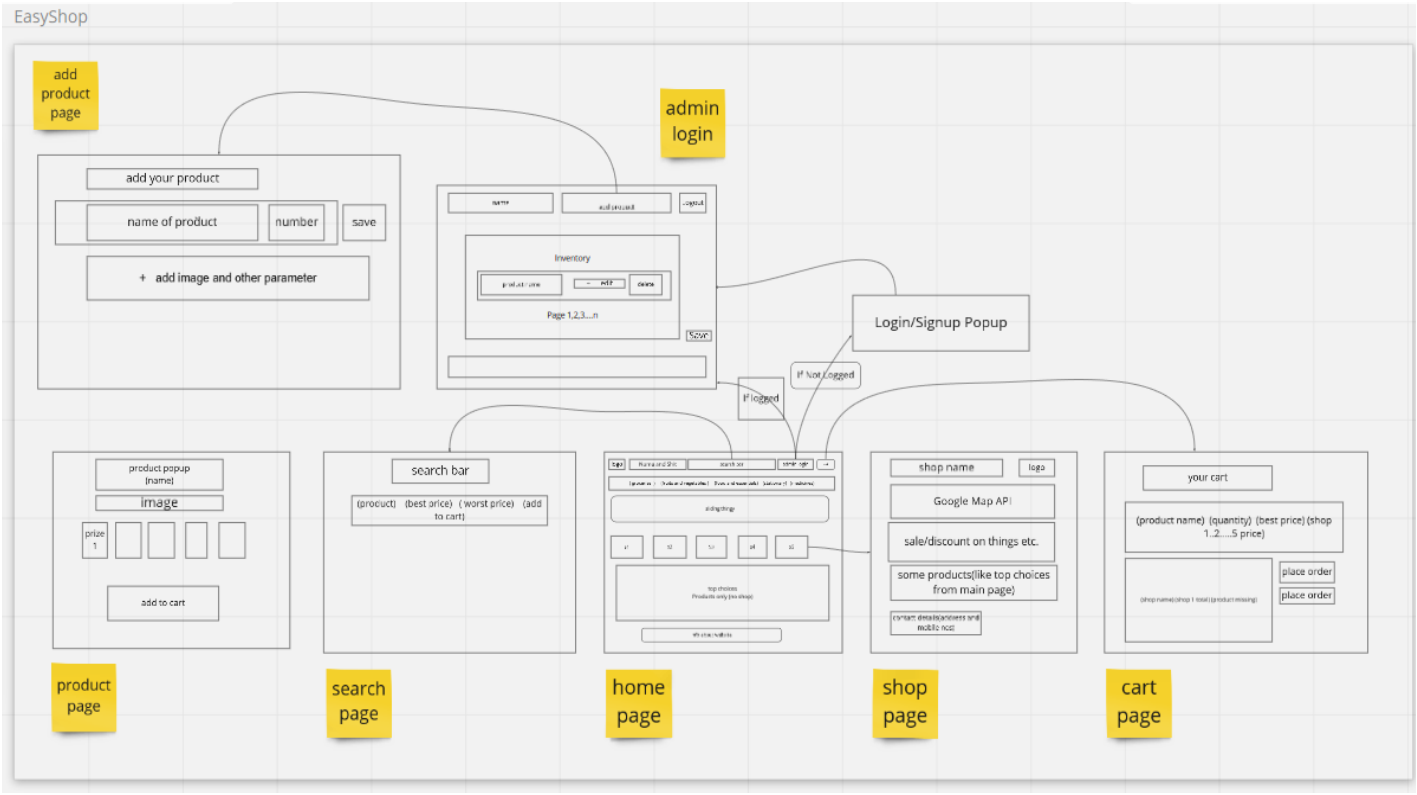
This paper targets accelerating **RSA unscrambling and signature**. The presentation of RSA decoding and mark has an immediate relationship with the productivity of measured exponentiation usage. **RSA 3072 is equivalent to 128 digit symmetric and 2048 is equivalent to 112 piece symmetric then 128-112= 16 and 2^16= 65,536.** This paper proposes a variation of RSA crypto frameworks by lessening modules and private examples in secluded exponentiation. The exploratory outcome shows that the speed of the decoding and mark has been considerably improved and the variation can be proficiently executed in equal.

Problem Definition

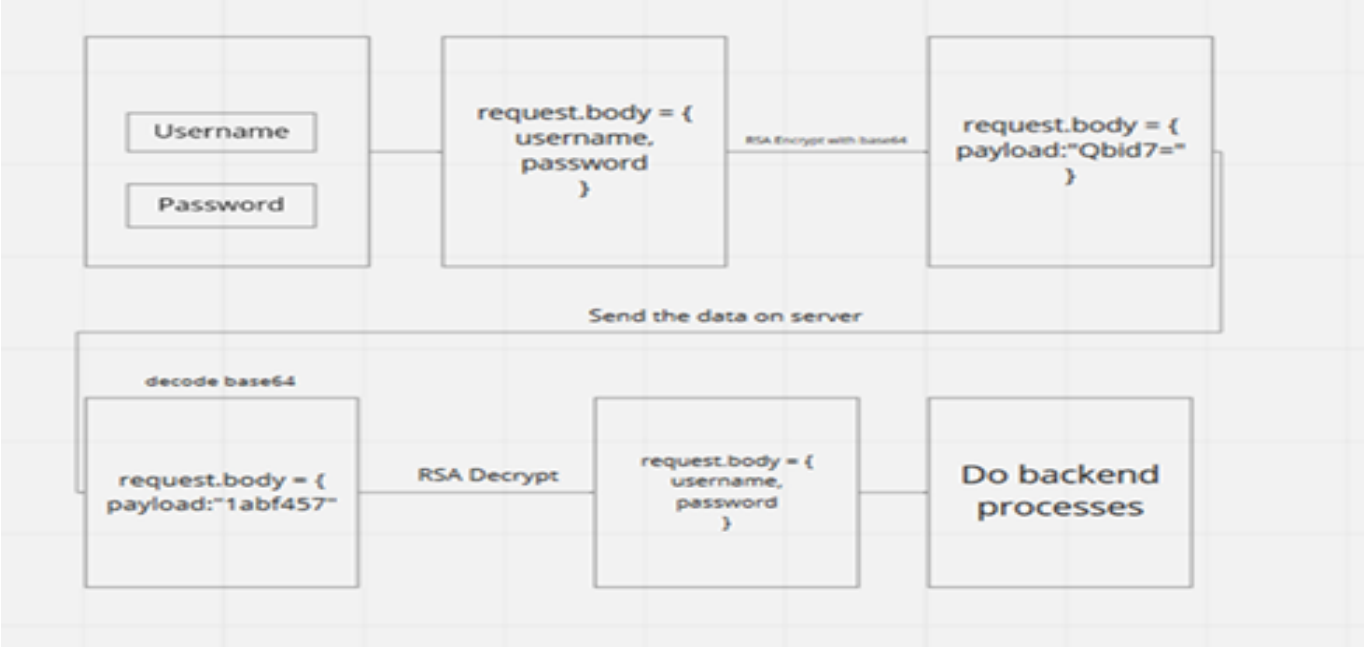
Creating a Securing e-commerce website secured from common attacks like Cross-Site Scripting (XSS), SQL injection, path traversal, local file injection and distributed attacks like DOS and DDOS and then also test it on tools like Nessus, BurpSuite and Google Lighthouse. Website also use BLAKE2b encryption to store all the user data, so in any case there is a leak of the database, the user's private information will be secure cause we can't unhash the BLAKE2b encrypted message.

Architecture Diagram

A functional overview of the proposed website:



Security overview of our model



Scheduling diagram based on week

Week-1	21-02-21 to 27-02-21	Project Idea Finalisation
Week-2	28-02-21 to 06-03-21	Website Design Finalisation
Week-3	07-03-21 to 13-03-21	Define website functional requirements & meet with stakeholders
Week-4	14-03-21 to 20-03-21	Find a suitable css framework for frontend development
Week-5	21-03-21 to 27-03-21	Choose a suitable backend framework with required libraries
Week-6	28-03-21 to 03-04-21	Create a database schema for the product to be made
Week-7	04-04-21 to 10-04-21	Meet on the security aspects of the website and frontend development
Week-8	11-04-21 to 17-04-21	frontend and backend development
Week-9	18-04-21 to 24-04-21	Continue development & start testing for backend routes
Week-10	25-04-21 to 01-05-21	Debugging week for the development done, Roll out beta release
Week-11	02-05-21 to 08-05-21	Start working on DevOps, acquire a domain name for the website

Project Outcome

We plan to come up with our own security mechanism for websites and then demonstrate it with the help of the e-commerce website we have created.
This method can be published as a research paper detailing the method and our website as a working prototype which will have a working model of our algorithm .

References

1) *Y. Wen, C. Zhou, J. Ma and K. Liu, "Research on E-Commerce Security Issues," 2008 International Seminar on Business and Information Management, Wuhan, 2008, pp. 186-189.*
2) *Kefa Rabah, "Implementing Secure RSA Cryptosystems Using Your Own Cryptographic JCE Provider ", 2006, pp.*
3) *Yunfei Li, Qing Liu, Tong Li, "Design and implementation of an improved RSA algorithm ", International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT),2010*
4) *Sangeetha M K Prof. Dr. Suchitra R," The Study of E-Commerce Security Issues and Solutions",2017*
5) *Dr. Rajesh Kumar Mahajan,"E-Commerce Security Challenges: A Taxonomy - Book", 2016 ISSN : 2349-5138*
6) *Shazim W. khan,"Cyber Security; Issue and Challenges in E-Com",2019 ISSN : 976-6375*