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

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

May, 2021

Title

A NEW MODEL METHOD TO SECURE AN E-COMMERCE WEBSITE

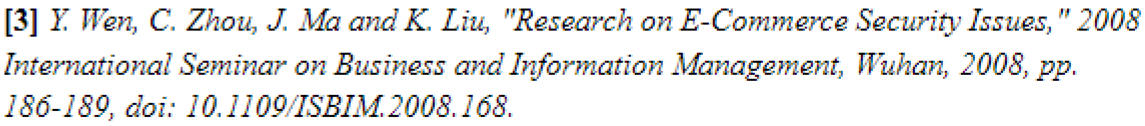
Literature survey

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

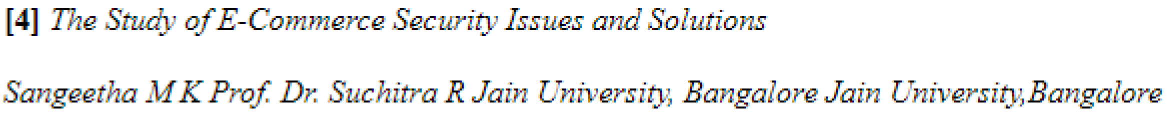
Online business refers to the trading of products and ventures over the Internet. Shopping through web based business has entered all fragments of merchandise going from food supplies to electronic products and even vehicles. Fast development in versatile registering and correspondence innovations has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

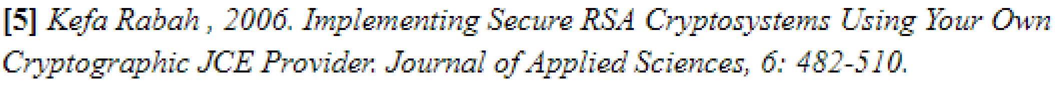

[3] *Y. Wen, C. Zhou, J. Ma and K. Liu, "Research on E-Commerce Security Issues," 2008 International Seminar on Business and Information Management, Wuhan, 2008, pp. 186-189, doi: 10.1109/ISBIM.2008.168.*

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.

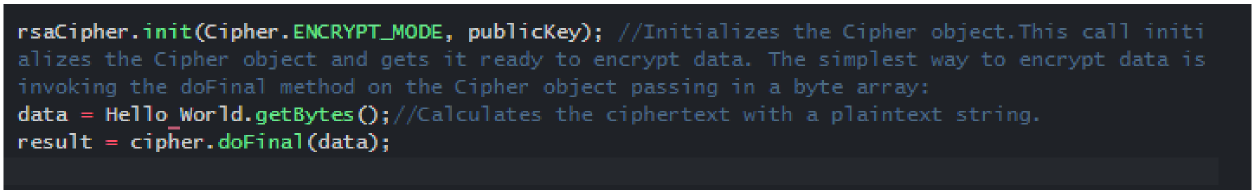

[4] *The Study of E-Commerce Security Issues and Solutions*

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.**

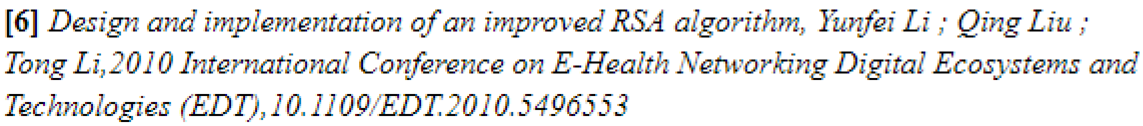

[5] *Kefa Rabah , 2006. Implementing Secure RSA Cryptosystems Using Your Own Cryptographic JCE Provider. Journal of Applied Sciences, 6: 482-510.*

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.

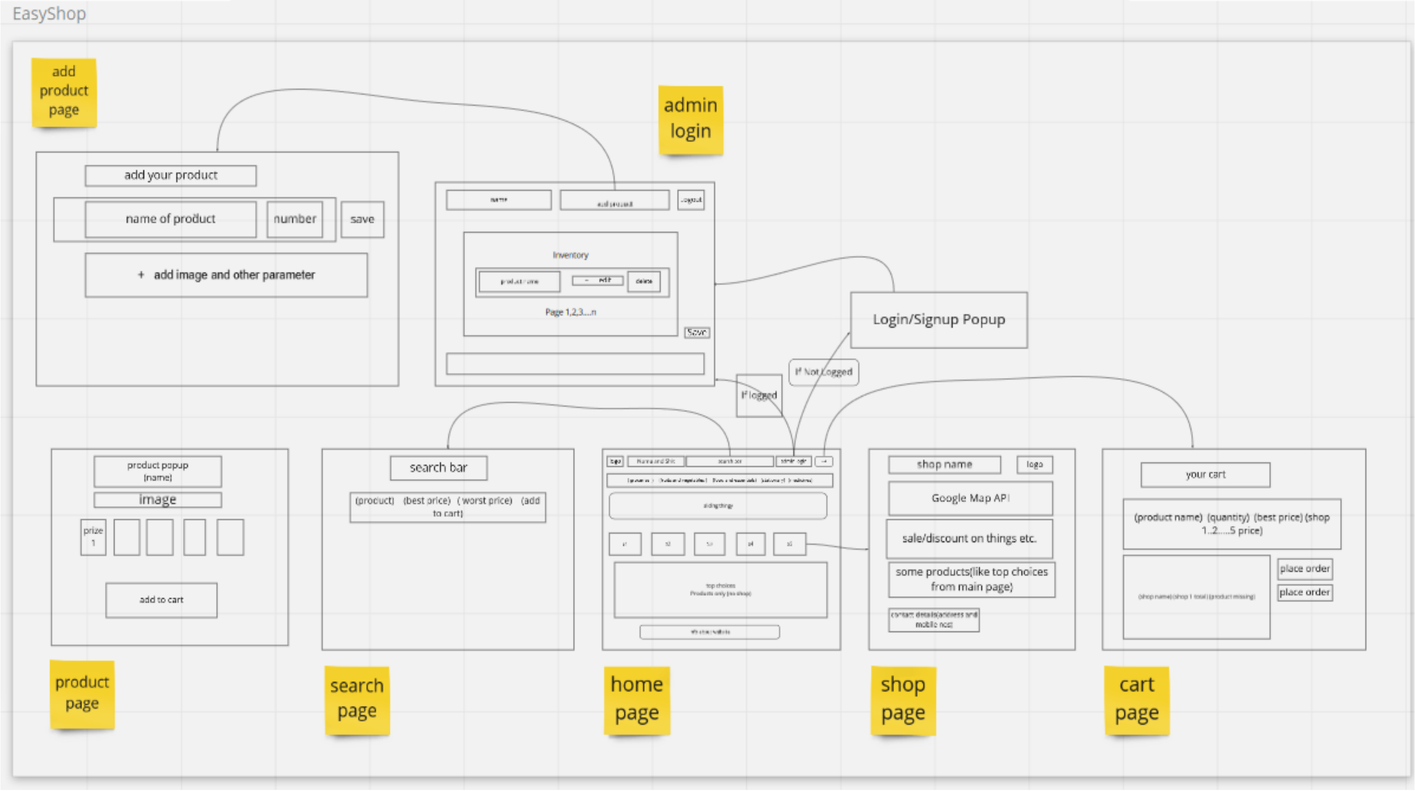


[6] *Design and implementation of an improved RSA algorithm, Yunfei Li ; Qing Liu ; Tong Li,2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT),10.1109/EDT.2010.5496553*

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.

Architecture Diagram

A functional overview of the proposed website:



Discuss proposed method with its diagram

The main aim of our project is to secure the web app as much as possible. The algorithms we are using are pretty standard, but the way we are sending the data on the server is a bit different. So, basically we are encrypting the data on the client side itself (it will be done by the browser locally) and then send the data directly. So,

```
{
   user:"Tanish"
}
```

Normally, data would be sent like this, but we encrypt it and it will be sent like this,

```
{
   payload:"Qbd3r=f" // Some base64 encoded string.
}
```

On decoding the object would be, { { user:”Tanish” } }.

Along the client side encryption, we are also deploying server side encryption with the help of a one of the newest hashing algorithms BLAKE2b which is 512 bit in length.

Steps:

Client,

Form-data -> RSA encryption with 3072 bit key -> base64 encoding -> send the form data

Server,

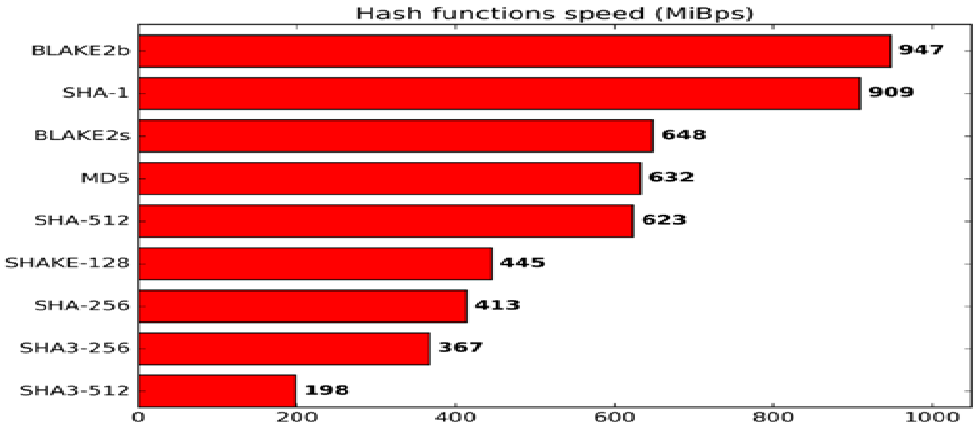
Received base 64 form data -> decoding base64 to uint8 buffer -> RSA decryption -> received the form data in the backend controller (can do operations on it)

We will also use RSA 3072 bit encryption which is better than standard encryption algorithms. The public and private keys used in the RSA algorithm are created with “ssh-keygen” which is industry standard for cloud computing. Sowe can ensure the robustness of private keys that will be used in our application.

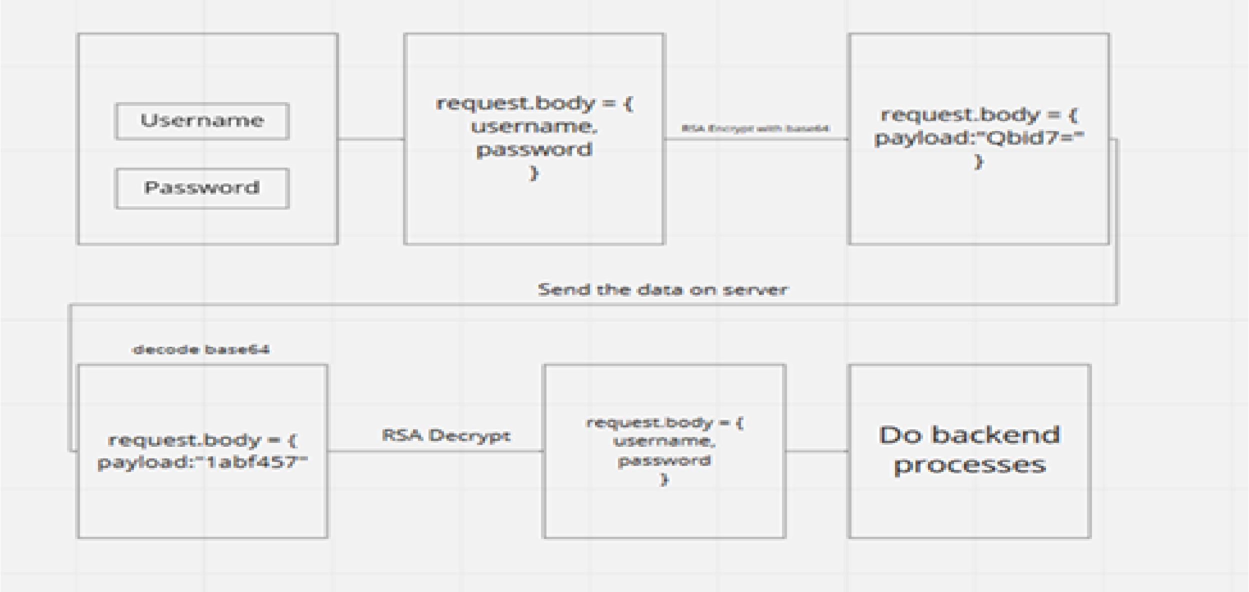
The site will be hosted on HTTPS which is more secure than HTTP. HTTPS is not stateless protocol, so it can be used to store user sessions across the complete web application

The site will be immune to most common attacks like Cross-Site Scripting (XSS), SQL injection, path traversal, local file injection and distributed attacks like DOS and DDOS.

We use new hashing algorithms like blake2b instead of SHA as they are faster and more secure. We updated our hashing algorithm from sha256 to a faster and secure blake2b hashing algorithm. While both have the same algorithmic time complexity, runtime complexity of blake2b is far more better than sha256. You can see that in picture below,



Security overview of our model


Username
Password
request.body = {
username,
password
}
RSA Encrypt with base64
request.body = {
payload:"Qbid7="
}
Send the data on server
decode base64
request.body = {
payload:"1abf457"
RSA Decrypt
request.body = {
username,
password
}
Do backend processes