

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

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 we then also plan to test this website against standard tools like Burp Suite and nessus.

Introduction

Our new security design implemented here for an e-commerce website will be a new and secure way for handling the security of a website. It will prevent attacks and ensure confidentiality, integrity and availability for the website for the users.

Existing methods are often not secure enough and were built incrementally, modified to address any new threats, our model is a complete model built from scratch using the latest algorithms for encryption and hashing like RSA-3072 bit and Blake2b. These algorithms are both faster and more secure than legacy algorithms.

Security Requirements provided in our system

security requirements for a website are authorization, authentication, nonrepudiation and data protection.

Authentication

Authentication means ensuring that every party involved in using the website—the user, the server, and the ISP—is what it actually claims to be. Authentication involves getting credentials of the website (like its digital signature) and confirming them against a trusted third party.

Authorization

Authorization means the person making the request should be the person they claim to be and there should be some form of access control systems in place to confirm this. Also once identity is confirmed the person would only be allowed to make specific requests based on their predetermined access level.

Data Protection

Protection of data means that the request made to the website and response json that we get have not been altered or tampered while in transit. It is ensuring both data integrity and privacy.

Nonrepudiation

Nonrepudiation basically means accepting that you are sending the data. Once a data is sent, the sender then cannot deny that they did not send the data, there will be proofs that say the sender is in fact the sender receiver is claiming to be.

Literature survey

[1] E-Commerce refers to the exchange of goods and services over the Internet. Shopping online is getting popular among all segments of products ranging from electronic goods to groceries and even luxury goods. Rapid growth in mobile data and communication technologies has facilitated the rapid growth of e-commerce platforms. The main impediment in growth of e-commerce is cyber fraud and identity theft. Hackers are people who carry out cybercrime. Hence, poor security on e-Commerce web servers and in users computers is a core issue to be resolved for rapid growth of e-commerce. This paper provides directions for e-commerce security so as to improve customer confidence in e-commerce shopping.

[2] With the rise of the Global Economy, and with an ever-expanding level of purchasers doing their business fundamentally by means of on the web or cell phones, electronic trade, internet business, is quickly being viewed as the best approach worldwide at the bit of a catch. Subsequently, building up a successful Web based business model is getting essential for any cutting edge business. In any case, an organization must address diverse new security challenges and be sure to keep up the best expectations of web based business security, to ensure both themselves and their clients. An inability to hold fast to severe internet business security can

bring about lost information, traded off exchange data, as well as the arrival of the client's monetary information. This can lead to lawful and budgetary risk, just as a negative effect on the organization's notoriety. These new security challenges are the consequences of the utilization of the new innovation and correspondence medium, and the progression of data from big business to undertaking, from big business to purchasers, and furthermore inside the undertaking. This paper presents the distinctive innovation and calculated parts of the web based business as a rule, and recognizes and orders the various sorts of security challenges confronting online business organizations specifically.

[3] This paper deals with various security issues faced by ecommerce websites that are hosted on public networks. The main issue discussed in this paper is the security transactions on E-commerce platforms and two main aspects of it, which are the security of the information and the security of the system. The two major issues discussed are Computer network problems and The security issues of business transactions. This paper also proposes some security requirements process of E-commerce transactions. They are: The confidentiality of information transmission, validity of the information, The integrity requests when storing the data should prevent illegal destruction or change on the site, The integrity of the transaction information, Non-repudiation of information, The authenticity of the traders identity. The two traders do indeed exist, not fake, The information can not be amended. The message on the network can not be modified.

[4] This paper deals with privacy and security issues faced by modern ecommerce websites and how these issues faced by the customers are restricting them from engaging more with these websites. It also states that e-commerce applications that handle payments are at increased risk from being targeted than other websites ,there are greater consequences if there is data loss or alteration and have more compliance in issues. The paper then also goes on to discuss web security in general and how rapidly growing e-commerce is a challenge online security as a whole.

[5] Encryption and deleting data encryption: Encryption works by Byte level, so almost anything can be encrypted. As long as the key and the cipher pair are found anything can be encrypted. we cannot have a DES-initiated key and an RSA-initiated cipher. The Cipher object uses the same encryption methods as encryption, so we should first start to let them know what we want to do with the data. The result will now have an encrypted presentation of the incoming data. It is easy to remove writing with similar details. But before we can do that, we have to reboot the Cipher object and prepare it for disassembly

[6] This paper aims at speeding up RSA decryption and signature process. RSA performs directly in relation to modular exponentiation. RSA 3072 equals 128 bit symmetric and that of 2048 equals 112 bits. The paper proposes a RSA crypto variant by reducing modules. The experimental result shows that the speed of the decryption and signature has been substantially improved and the variant can be efficiently implemented in parallel.

[7] Proposed a general - purpose framework for an approach for benchmarking the security of web service frameworks. To deploy our innovative technologies and applications, we tend to use webservices. The webservices use frameworks and for communicating they use middleware. Security in the Web is a basic concern as the receptiveness to attacks is high and may achieve sad consequences for the passed on organizations. Picking the most secure framework is trying, especially considering their assortment and the unpredictability related with any security assessment. This paper is a hidden responsibility zeroing in on the significance of a security benchmark for assessing and taking a gander at the security of web organization structures. The proposed benchmark relies upon two phases: Security Qualification and Trustworthiness Assessment. In the chief stage, top tier systems are used to perceive shortcomings in the constructions. If shortcomings are found, the construction is blocked. In the resulting stage, the affirmed frameworks are inspected for affirmations of possibly unsteady viewpoints, being the seen lead used to handle a score using the Logic Score of Preferences method. Such score licenses differentiating frameworks from a dependability perspective. We applied our system for the occurrence of DoS Attacks and benchmarked ten designs. Results show that six frameworks misfire in possessing all the necessary qualities for the ensuing stage and that the overabundance ones can be situated using the figured score, allowing planners to make instructed decisions about their courses of action.

[8] Proposed a general - purpose framework for a Web Service Security Governance Approach Based on Dedicated Micro-services Architecture generally known for its agility, composability and openness called SOA or Service-oriented architecture. Such designing consolidates independent, interoperable and possibly reusable organizations, which are executed as Web Services (WS). Right when passed on in the Cloud Environment, security risks may increase at the WS level, raising some security challenges, similar to shortcoming revelation and trust or availability encroachment. Watching out for security issues require complex endeavors that should be managed freely with related concerns. To deal with this issue, we suggest here to an elective designing known as Microservices Architecture (MSA) which relies upon the norm of breaking down colossal and complex programming projects into various atomic sub-projects. In Addition, to control, chief and assurance that shortcomings are reasonably treated and the typical security objections are refined, we track down that the organization of Web Service security is certainly required. Therefore, we suggest here a Web Service security organization approach intends to diminish the security deserts and to improve trust between web organizations. This system includes in combining smaller than expected organizations by using a subset of GDPR(EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was proposed to mix data assurance laws across Europe, to guarantee and connect all EU inhabitants data insurance and to reshape the course relationship

across the locale approach data insurance.) rules and a lot of described security procedures. This procedure grants estimating the submitted smaller than usual help implying customer security requirements.

[9] Proposed a general - purpose framework for Formal methods for web security. In the past few years, researchers mainly security based have proposed to instill more robust foundations on the web based platform and allowing room for more web security issues. Given the multifaceted nature of the Web, regardless, research tries in the space are spread around a wide scope of topics and issues, and it is hard to appreciate the import of formal techniques on web security as of not long ago. In this investigation we assemble, gather and overview existing suggestions in the space of formal techniques for web security, crossing different focuses: JavaScript security, program security, web application security, and web show assessment. Considering the current composition, we talk about ideas for researchers working close by to ensure their suggestion have the right trimmings to be manageable for an immense extension gathering.

[10] Proposed a general - purpose framework for Web Application Security: An Investigation on Static Analysis with other Algorithms to Detect Cross Site Scripting. Among web application shortcomings, XSS is the most regularly occurring. Where a web application recognizes a customer input, it is functional for such shortcoming to mix malevolent substance. A large portion of the composing zeroed in on the usage of static examination to discover XSS shortcomings. The defense is its ability of achieving feasibly a 100% code incorporation and seeing every method of the program. Incidentally, the standard impediment of static examination, being the false sure rate showed up in the results, continues. Hence, researchers began to join static assessment with various computations, as genetic estimation, AI and model organizing. This is to improve the XSS disclosure results similarly as the static examination run time. This composition portrays the computations which prior improved the static assessment results concerning XSS shortcoming recognizable proof. Besides, every procedure's restriction was referred to in which the examinations keep on without a profitable revelation of XSS shortcoming in PHP web application.

[11] Proposed a general - purpose framework for Measuring web service security in the era of Internet of Things. IOT(Internet of Things) and other such technologies help small devices to instill web services and web apps on a massive scale and have open and dynamic networking. End customers or organization customers face a hard decision over which organization to pick among the available ones, as security holds a key in the powerful collaboration. In this paper a base phonetic evaluation set is arranged, taking into account which the wide scope of different feathery term sets that used for portraying security credits are officially dressed and composed for calculating an overall security worth of the organizations. This work, to the extent that we might actually know, is the principle suitable response for offering direct assessments and rankings of association organizations subject to different security credits like order, availability, insurance and obligation. We analyzed four huge cloud organization stages to address the proposed approach.

[12] Proposed a general - purpose framework for Enhancing the security of patients' portals and websites by detecting malicious web crawlers using machine learning techniques. There has been a boom in

demand for the patient's info and their medical portals' medical information. Regardless, one of the challenges towards endless use of such assistance is keeping up the security of those passages. Continuous reports show an upsetting development in computerized attacks using crawlers. These item programs crawl pages and are prepared for executing various orders, for instance, attacking web laborers, breaking passwords, procuring customers' own personal information, and testing the shortcoming of laborers. The place of this assessment is to develop another fruitful model for distinguishing vindictive crawlers subject to their navigational direct using AI techniques.

[13] Proposed a general - purpose framework for The Web Security Password Authentication based on the Single-block Hash Function. The paper is based on protecting authentication of password and web security and uses a single-block hash function. The arrangement can deal with the issue effectively that exists in the standard mystery word affirmation or automated mark in the Web approval of the customer's character to comprehend the defect. It can go against replay attacks, snooping, change of messages and typical attacks, and insignificant exertion, high capability, satisfying security and capable necessities of hidden features for conspicuous approval in the association organization. All around, MD5 or SHA1 is used. In any case, these computations are unreasonably awkward for the Web approval of the customer's character, and the proportion of estimation is moreover exorbitantly gigantic. The test outcomes show that the arrangement guarantees prosperity by then, and grows the efficiency of the security approval.

[14] Proposed a general - purpose framework for a Survey on JavaScript security policies and their enforcement mechanisms in a web browser. We notice a quick improvement of electronic applications reliably. These applications are executed in the web program, where they interface with a combination of information having a spot with the customer. The dynamism of web applications is given by the use of web scripts, and explicitly JavaScript, that gets to this information through a program given a set of APIs. Lamentably, a segment of the substance use the given value threateningly. All through the last decade, a critical number of online attacks that ignore user's assurance and security have been recognized. Consequently, web script security has been a functioning space of exploration. Both PC security analysts and web engineers have proposed various methods to implement distinctive security and protection arrangements in the internet browser. Among every one of the deals with internet browser security, we study dynamic procedures dependent on runtime observing just as secure data stream methods. We at that point consolidate and think about the security and protection approaches they implement, and the manner in which the requirement is finished. We target two gatherings of perusers: 1) for PC security specialists we propose an outline of safety important segments of the internet browser and the security approaches dependent on these segments, we additionally show how notable authorization methods are applied in an internet browser setting; 2) for web engineers we propose a characterization of safety arrangements, correlation of existing implementation components proposed in the writing and clarification of formal assurances

[15] Proposed a general - purpose framework for Web Services Security Problem in Service-oriented Architecture. With the unforeseen development and far reaching utilization of SOA advancement, security

issues of Web organizations subject to heterogeneous stage have gotten continuously observable. This article at first presents two security different game plans of Microsoft Net, Apache Axis stage. All the while for the security issues between heterogeneous stages. A Web organizations security mode reliant upon the .NET stage and the Axis2 stage is proposed in the papers. We in like manner pointed out the direction of things to come.

[16] Proposed a general - purpose framework for Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security. In view of its passed on and open nature, Web Services lead to new security challenges. This development is defenseless to Cross-site Scripting (XSS) attack, which adventures existing shortcomings. The proposed approach uses two Security Testing procedures, to be explicit Penetration Testing and Fault Injection, to emulate XSS attack against Web Services. This development, gotten together with WS-Security (WSS) and Security Tokens, can recognize the sender and affirmation the genuine access control to the SOAP messages exchanged. We use the shortcoming scanner soapUI that is potentially the most seen mechanical assemblies of Penetration Testing. Then again, WSInject is another deficiency implantation instrument, which presents issues or slip-ups on Web Services to explore the direct in an environment not enthusiastic. The results show that the usage of WSInject, conversely with soapUI, improves the area of shortcoming grants to mimic XSS attack and delivers new sorts of them.

[17] Proposed a general - purpose framework for A Kerberos security architecture for web services based instrumentation grids. Instrumentation Grids target controlling and regulating heterogeneous resources and instruments securely, reliably and in near consistent. Inside this particular condition, we present a Web Services based Security Architecture that objectives improving security execution keeping up all the while interoperability with legacy Grid Security Infrastructure (GSI). Our design uses GSI X.509 Certificates or Proxy Certificates (RFC3820) for the fundamental confirmation of a customer. Regardless, it thus maps this character to a Kerberos one and utilizes WS Security Kerberos Token Profile for embedding customer accreditations inside WS exchange instruments. It by then gives customer endorsement, in this way understanding an all out AAI (Authentication and Authorization Infrastructure). To show and assess the show improvement achieved by our technique over a message exchange using X.509 Certificate Token Profile, we present relative assessments on executions of the two other options. Our results show that the Kerberos message exchange arrangement shows up to half message throughput improvement, under high CPU load on the laborer.

[18] Proposed a general - purpose framework for Assessing the security of web service frameworks against Denial of Service attacks. Web benefits routinely give business-essential handiness over the Internet, being extensively revealed and thus tending to an engaging target for security attacks. In particular, Denial of Service (DoS) attacks may correct limit damage to web expert associations, including money related and reputation disasters. Thus, it is pivotal that the item supporting organizations sending (i.e., the web organization structure) can give a protected environment, so the organizations can be passed on regardless, when standing up to attacks. In this paper, we present a test approach that licenses

perceiving how well a given web organization framework is set up to manage DoS attacks. The approach relies upon a lot of stages that join the execution of a gigantic number of outstanding DoS attacks against a target framework and the portrayal of the saw direct. Results show that four out of the six frameworks attempted are frail against in any occasion one kind of DoS attack, and exhibit that even incredibly well known stages require squeezing security updates.

[19] Proposed a general - purpose framework for Tracing known security vulnerabilities in software repositories – A Semantic Web enabled modeling approach. The show of the Internet has disturbed our overall population just as changed the item business, with data and information sharing transforming into a central piece of programming progression measures. The resulting globalization of the item business has extended programming reuse, yet also introduced new challenges. Among the troubles, rising up out of the data sharing is Information Security, which has emerged to transform into a critical peril to the item progression neighborhood, source code just as its shortcomings are shared across project limits. Designers are ignorant of such security shortcomings in their exercises, routinely until a shortcoming is either manhandled by aggressors or made uninhibitedly available via self-ruling security cautioning databases. In this investigation, we present a showing approach, which misuses Semantic Web developments, to develop conspicuous joins between security notice stores and other programming documents. Even more expressly, we set up a bound together ontological depiction, which maintains bi-directional perceptibility joins between data trapped in programming manufacture stores and thought shortcoming informational collection. These vaults can be seen as trusted in information storage facilities that are consistently not directly associated with various resources, for instance, source code chronicles containing the uncovered events of these issues. The interest of our approach is that it licenses us to overcome a segment of these ordinary information storage facilities and change them into server farms, which advance sharing of data across vault limits. We drove a couple of tests to diagram the fittingness of our strategy by following existing shortcomings to projects which may clearly or by suggestion be impacted by shortcomings procured from various undertakings and libraries.

[20] Proposed a general - purpose framework for Semantic security against web application attacks. In this paper, we propose a technique for perceiving and describing web application attacks. Rather than current imprint based security techniques, our answer is a mysticism based strategy. It decides web application attacks by using semantic rules, the setting of result and the points of interest of utilization shows. The system is good for recognizing current attacks effectively and gainfully by exploring the foreordained section of a customer request where attacks are possible. Semantic guidelines help to get the setting of the application, expected attacks and the show that was used. These principles also license enlistment to run over the ontological models to perceive the habitually astounding polymorphic assortments of web application attacks. The ontological model was made using Description Logic that relied upon the Web Ontology Language (OWL). The inferring rules are Horn Logic decrees and are executed using the Apache JENA structure. The system is in this manner stage and development free.

[21] Proposed a general - purpose framework for A lightweight web-based vulnerability scanner for small-scale computer network security assessment. There radiates an impression of being an average acumen among typical PC customers pointing towards an overall shortfall of trust while using the Internet. The objective of this shortfall of trust relating to the use of the Internet, particularly orientated towards its business use and electronic purchasing, requires for the most part from webpage architects to make and keep up web applications that are incredible and give a particular degree of adaptability to attack from outside risks. This endeavor intends to add to this particular perspective by giving page fashioners and system analyzers, similarly as fundamental site customers, with an instrument for perception, shortcoming checking and far off association arranging that is visible, accessible and useful due to its electronic and visual, event driven interface. It is normal that the inconvenient task of sorting out some way to use different request line gadgets and their exact convenience and limits can be avoided through this and relative new developments, and consequently that this will possibly extend the permission to security testing, particularly to little and medium associations.

[22] Proposed a general - purpose framework for Security Busters: Web browser security vs. rogue sites. URL blacklists are used by a large portion of current web programs as an approach to safeguard customers from dissident destinations, for instance those serving malware and moreover working with phishing stunts. There are a lot of URL blacklists/reputation organizations, out of which Google's Safe Browsing and Microsoft's SmartScreen stand separated as the two most consistently used ones. Regularly, such records are the solitary safeguard web programs do against such risks. In this paper, we review the level of affirmation that is offered by standard web programs on iOS, Android and work region (Windows) stages, against a colossal game plan of phishing and malicious URL. The results reveal that most projects – especially those for phones – offer confined protection from such threats. In like manner, we propose and evaluate a countermeasure, which can be used to inside and out improve the level of confirmation offered to the customers, paying little psyche to the web program or stage they are using.

Methodology

Security:

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 different. So, basically we will be encrypting the data on the client side itself (it will be done by the browser locally) and then send the data directly. So,

For request body,

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

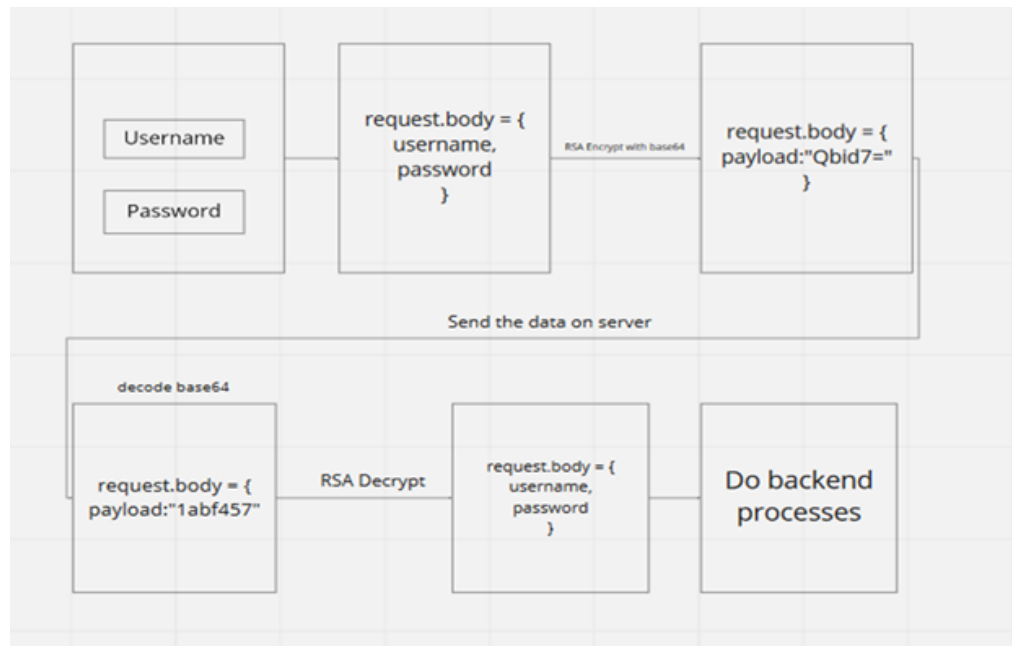
Normally, data would be sent like this, but we encrypt it and it will be sent like this,

```
{  
  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)

Performance Requirements

The website should be easily accessible via both laptop/desktops and mobile phones as most customers will prefer to order via their phones.

Also the database should be distributed, and NOSQL based so that it can be easily accessed by multiple users simultaneously.

The website should also feel quick and responsive to the user to give them a convenient shopping experience.

Safety Requirements

The password of admins i.e the shopkeepers are being stored in hashed format instead of plain text format in the database. For this, we are using the blake2b hashing algorithm.

The hashing should be done in such a way that it should be hashed in controller logic itself...not after entering in the database. For that a function is defined which needs to be called while doing CRUD operations with the database.

We need to use IP filtering for preventing DDOS attacks on the server to ensure availability from the CIA triad.

Use of SSL certificate for establishing secure links between networked computers.

Security Requirements

security requirements are authentication, authorization, data protection, and nonrepudiation.

Authentication

Authentication ensures that each entity involved in using a Web service—the requestor, the provider, and the broker (if there is one)—is what it actually claims to be. Authentication involves accepting credentials from the entity and validating them against an authority.

Authorization

Authorization determines whether the service provider has granted access to the Web service to the requestor. Basically, authorization confirms the service requestor's credentials. It determines if the service requestor is entitled to perform the operation, which can range from invoking the Web service to executing a certain part of its functionality.

Data Protection

Data protection ensures that the Web service request and response have not been tampered with en route. It requires securing both data integrity and privacy. It's worth mentioning that data protection does not guarantee the message sender's identity.

Nonrepudiation

Nonrepudiation guarantees that the message sender is the same as the creator of the message. Now that we have an idea of what constitutes Web service security, we'll examine the top ten security factors affecting Web service implementation.

Requires the use of RSA to encrypt the form data before sending it on the server. Passwords are protected in the database with the help of Blake2B hashing algorithm.

An SSL certificate to ensure secure links between networked nodes.

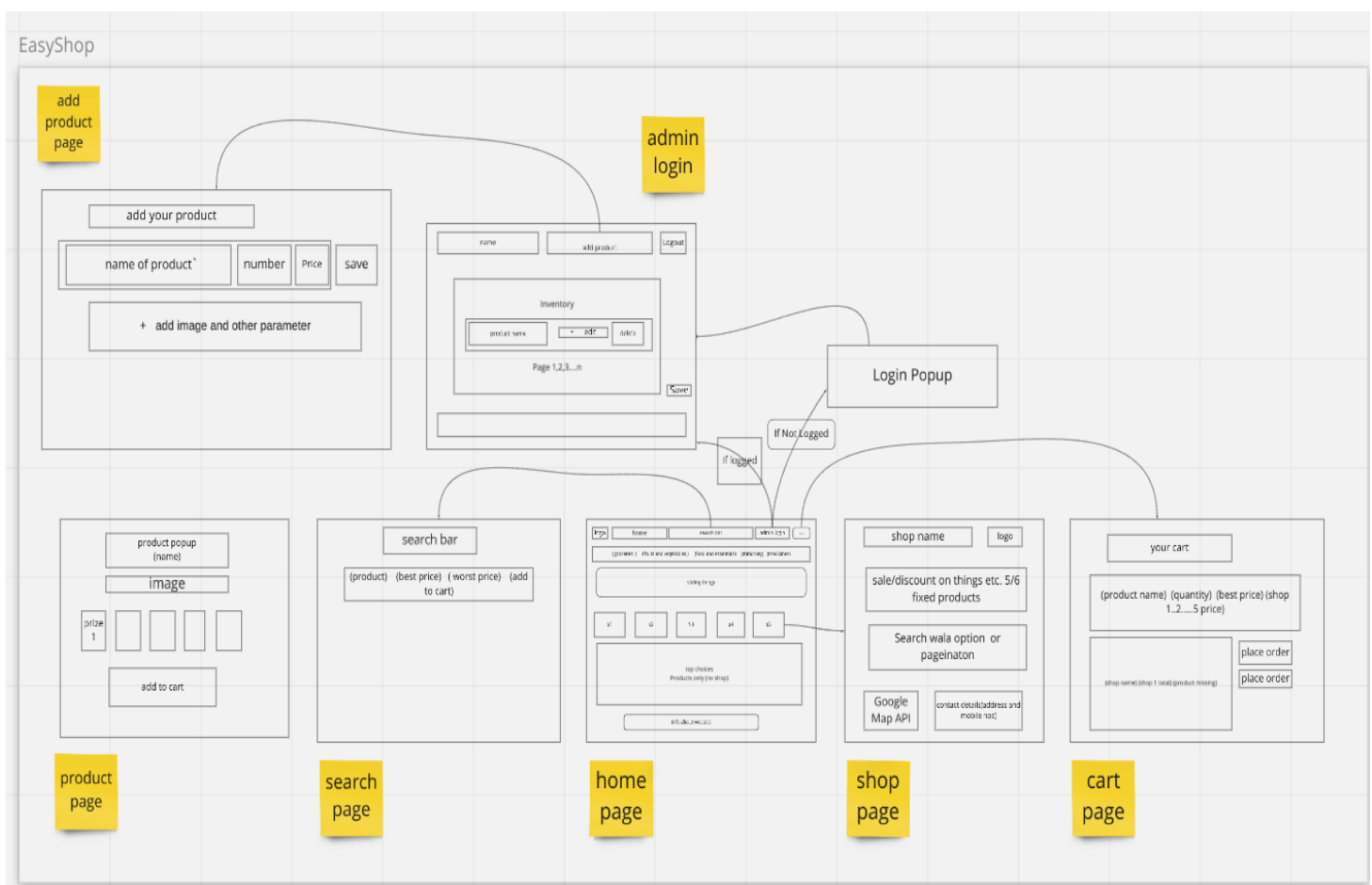
Modelling design

We have created a website and implemented our security system on it so we will discuss both the website and security structure and functionalities.

Website Functionalities

- If you are a user then there is no need to login. You can directly search your wish list.

- On the homepage, there will be a list of shops and specific items that are purchased more often and recommended by users.
- If the user clicks on a particular shop, then the user will be redirected to the shop page. On that page, users can see all details about that shop like location, sale, discount, contact details.
- Users also can use the search bar to add products in cart.
- There will be a page for your cart also. There will be a list of all items that you have selected.
- Then based on the algorithm we will give the best shop to buy groceries
- There will be a login for the shopkeeper to update the inventory.
- There will be an add product page for admin. Via this page admin can update their inventory



Security Functionalities

- The passwords for the users are stored in an hashed manner before being sent to the firebase database which then encrypts it before storing.
- On the homepage, there will be a list of shops and specific items that are purchased more often and recommended by users.
- We use new hashing algorithms like blake2b instead of SHA as they are

faster and more secure.

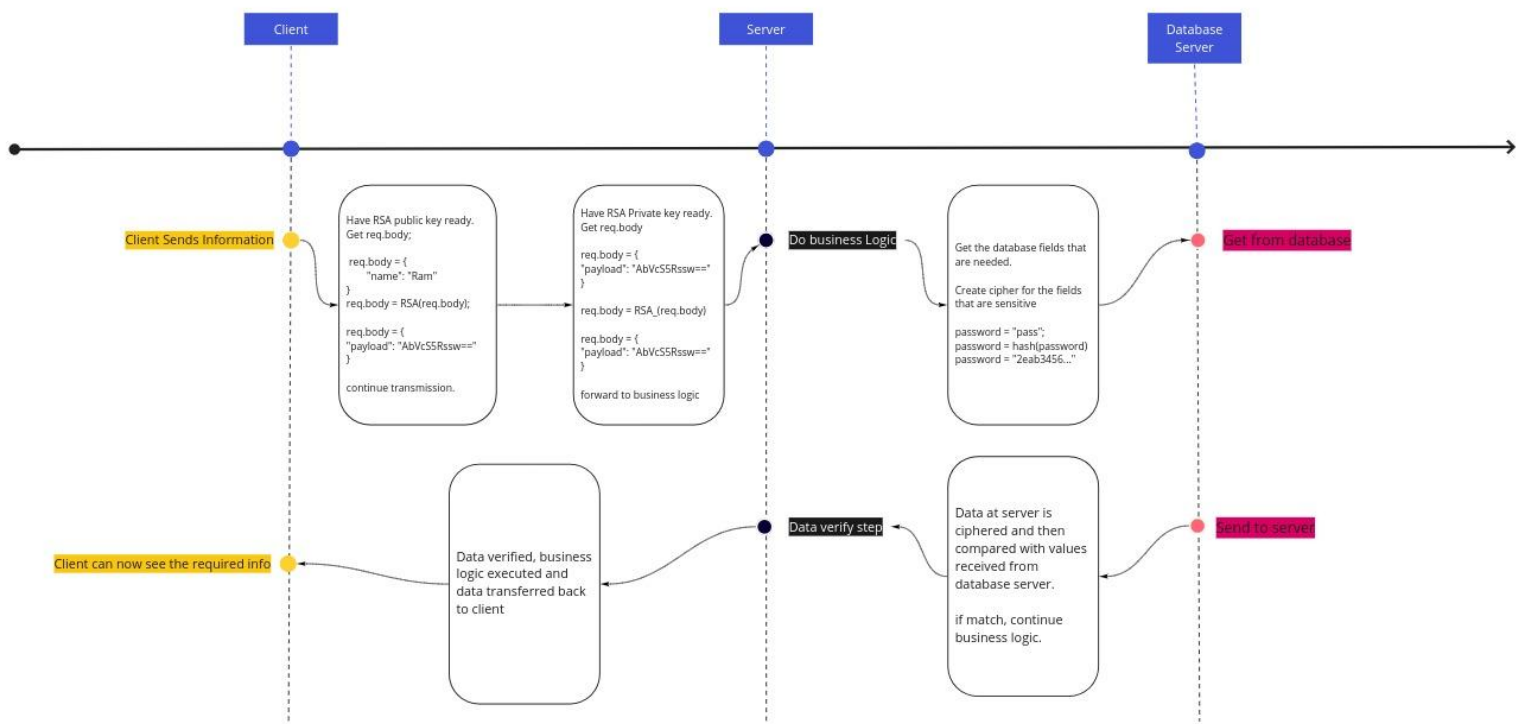
We updated our hashing algorithm from sha256 to a faster and secure blake2b hashing algorithm. While both have the same algorithmic time complexity, runtime complexity of blake2b is far more better than sha256.

- We 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 an industry standard for cloud computing. Sowe can ensure the robustness of private keys that will be used in our application.





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

The above points are visualized using the security architecture diagram between client, server and the database server given below.



Results and Experiments

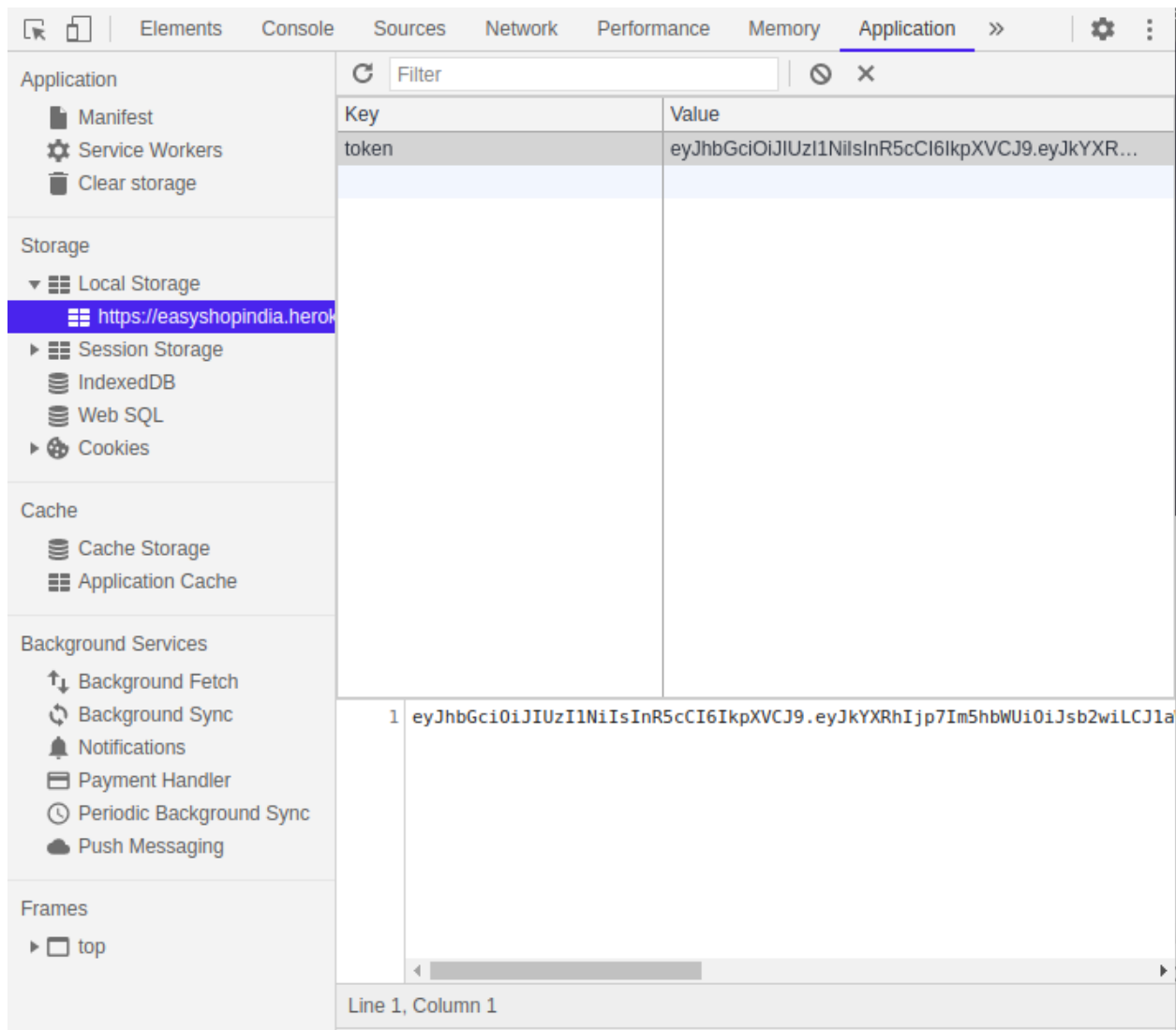
The main objective of our project is securing a website. To do that we have created an experimental website based on ecommerce as frauds and vulnerabilities in such websites are ample. We have designed and implemented the ecommerce website in which the frontend includes Home page, Login and Admin as of now. In the backend in terms of security we have implemented JWT token and validation.

Test	Expected Output	Observed Output
Testing secured API without auth header	"noAuthHeader"	
Testing secured API with wrong / tempered auth header	"JWTVerifyFailed"	
Test secured route with proper Auth header	Responds successfully with data	
Successful Login	Responds with JWT token signed from the backend.	

We have developed the basic structure of the website, and some basic security aspects.

easyshop-ace15	users	5ae462abbb
+ Start collection	+ Add document	+ Start collection
sample	09de02fe79	+ Add field
users	3ac5139270	<div>0</div> <div>image_link: "https://www.amul.com/files/hits/amul-hits-1251.gif"</div> <div>1 {image_link: "https://www...."</div> <div>2 {image_link: "https://encr..."</div> <div>3 {image_link: "https://lpl..."</div> <div>email: "enzo_benzo@gmail.com"</div> <div>maps_url: ""</div> <div>name: "Enzo-Benzo"</div> <div>password: "d2d548838ef2c2eed01f5a1e6ece7dd4058500a0b98652bfae97e"</div> <div>products: [{quantity: 76, image_link:...}]</div> <div>uid: "5ae462abbb"</div>
	5ae462abbb	
	d67d825418	
	e065f8a8a1	
	e341ef2961	

Hashed Password Stored in Database- We store our users' data in hashed format. So if in any case there is database breach, hacker can't see the details of our user



Encrypted JSON web Token- We also take care of the request that our website makes. Our website will all request in just one line of “payload”. So it will be very secure in case like the hacker will try to use a burp suite then the hacker can see the only “payload” that is our request to the server.