Secure Online Auction System

A major project report submitted in partial fulfilment of the requirement for the award of degree of

Bachelor of Technology

in

Computer Science & Engineering / Information Technology

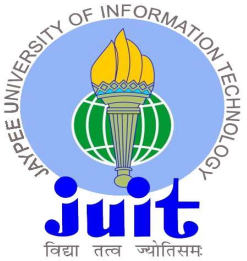
Submitted by

Satvik Tripathi (201239)

Rashik Walia (201343)

Under the guidance & supervision of

Dr. Kapil Rana



Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology,

Waknaghat, Solan - 173234 (India)

CERTIFICATE

This is to certify that the work which is being presented in the project report titled “Secure online auction system” in partial fulfilment of the requirements for the award of the degree of B.Tech in Computer Science And Engineering and submitted to the Department of Computer Science And Engineering, Jaypee University of Information Technology, Waknaghat is an authentic record of work carried out by “Satvik Tripathi, 201239” and “Rashik Walia, 201343” during the period from August 2023 to May 2024 under the supervision of Dr. Kapil Rana, Assistant Professor (SG) Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat.

Satvik Tripathi
(201239)
Rashik Walia
(201343)

The above statement made is correct to the best of my knowledge.

Dr. Kapil Rana
Assistant Professor (SG)
Computer Science & Engineering and Information Technology
Jaypee University of Information Technology, Waknaghat

CANDIDATE'S DECLARATION

We hereby declare that the work presented in this report entitled **'Secure Online Auction System'** in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science & Engineering / Information Technology** submitted in the Department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology, Waknaghat is an authentic record of our own work carried out over a period from August 2023 to May 2024 under the supervision of **Dr. Kapil Rana** (Assistant Professor (SG), Department of Computer Science & Engineering and Information Technology).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

(Student Signature with Date)	(Student Signature with Date)
Satvik Tripathi	Rashik Walia
201239	201343

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

(Supervisor Signature with Date)

Dr. Kapil Rana

Assistant Professor (SG)

Computer Science & Engineering and Information Technology

Dated:

ACKNOWLEDGEMENT

Firstly, we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the project work successfully.

We are really grateful and wish our profound indebtedness to Supervisor **Dr. Kapil Rana, Assistant Professor (SG)**, Department of CSE Jaypee University of Information Technology, Waknaghat. Deep Knowledge & keen interest of our supervisor in the field of "**Information Security**" has helped us to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism and valuable advice along with reading many inferior drafts and correcting them at all stage have made it possible for us to complete this project.

We would like to express our heartiest gratitude to **Dr. Kapil Rana,** Department of CSE, for his kind help to finish our project.

We would also generously welcome each one of those individuals who have helped us straight forwardly or in a roundabout way in making this project a win. In this unique situation, we might want to thank the various staff individuals, both educating and non-instructing, which have developed their convenient help and facilitated our undertaking.

Finally, we must acknowledge with due respect the constant support and patience of our parents.

Satvik Tripathi (201239)

Rashik Walia (201343)

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

RSA	Rivest,Shamir,Adleman
AES	Advanced Encryption Standard
DES	Data Encryption Standard
OTP	One-time Password
UML	Unified Modeling Language
XAMPP	X-operating system, Apache, MySQL, PHP, Perl
XML	Extensible Markup Language
MySQL	My Structured Query Language
GD	Graphic Draw
API	Application Program Interface
SMTP	Simple Mail Transfer Protocol
RDBMS	Relational Database Management System
REST	Representational State Transfer
TLS	Transport Layer Security

LIST OF FIGURES

ABSTRACT

An auction is a public sale where goods, services, or properties are sold to the highest bidder. Bids are placed by the participants and the item is awarded to the bidder who offers the highest amount. Auctions have a very rich history that dates back thousands of years and they have always been a prominent method for buying and selling goods and services across various cultures, in ancient Greece, soldiers' property was auctioned off in order to distribute the proceeds among the soldiers, art and other valuables were also auctioned. Whereas at the time of Roman Empire they conducted auctions for a variety of purposes, including sale of slaves, art and household items.

In today's time auctions are very widely used in various contexts, including commerce, fundraising, and asset allocation. There are several types of auctions and each of them have their own set of rules and procedures, some common types of elections are, English Auction, Dutch Auction, Sealed-Bid Auction, Vickrey Auction and Reverse Auction [13]. Nowadays, no major sports league is organized without auction, and thus due to the globalization created by internet and the advancement of technology together have forced people to look for easy solutions to problems.

All of these factors together have led to an increase in the userbase of the online auction system, such a system enables the user to buy any product of their choice without visiting any physical venue, and it also enables the seller to sell their product from any corner of the world. Given the geographical conditions and terrain of our country, this system becomes even more useful here. But there are always two sides of the coin, there is no doubt that it turns out to be very useful for the users, but it has its own demerits, the existing auction systems are focused only upon the creation of a working website or application conducting auction, they always overlook the security part of this system.

In order to enhance the security of the auction systems we aim to create a web application for online auction system where every product is offered for bidding and the interested buyers can bid on them and buy them at fair prices and to improve the overall security, we will be using various encryption and authentication methods.

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

With the advancement of technology and growth in IT sector, there is a lot of awareness of online technologies. Considering these growths and awareness, we see many problems in things around us that can be solved or improved with it. One such issue or process is our traditional offline auction system. Online auction is a good solution to conduct fair and transparent auctions without any risk of shill bidding.

The manual auctions require a lot of time and energy in order to organize materials, arrange for an auction venue, and create disruption in a team's workflow. It turns out to be time-consuming for buyers, as they are required to travel to a supplier in order to place a bid on their items. Moving the auction to an online platform helps to reduce the manual labor and effort needed for suppliers to offer their items for sale and is more convenient for buyers to review items that may meet their needs. The manual auctions also have limited participation due to the time and cost involved in the bidding process, along with this they also lack transparency as there are many opportunities to provide insider information to individual bidders or create unfair bidding situations.

The feasibility of online auction market places allows the buyers and sellers to overcome the geographical constraints and provides them the freedom to sell and buy products anytime from anywhere over the internet. It also helps the users to get products at lower prices as compared to its counterpart. However, alongside the convenience and accessibility provided by them, they also require various security measures to protect the users from various potential threats.

Some of the risks that can create problem include shill bidding, unauthorized access insider threats, etc.

In conclusion, there are several benefits to using an online auction system over a conventional manual auction, including more accessibility, convenience and quicker and accurate results. To retain the credibility of auction process, consideration must be given to security, precision, and accessibility of online auction technologies.

1.2 PROBLEM STATEMENT

The growth and advancements in the digital infrastructure has led to the conversion of various traditional systems into online processes and systems, one such traditional system that has been in practice from many years is the auction system. Now it has also been converted into a digital platform allowing the sellers and buyers the feasibility to buy and sell their products on their fingertips.

However, it also leads to an array of security concerns that can stand as a major hindrance in the integrity of the bidding process and also compromise the data of the user. Deceptive practices such as shill bidding and bid sniping pose a major problem to the transparency of the auctions, decreasing the trust of the users and leading to financial losses of authentic and genuine participants. Improper privacy protection exposes the users to various risks such as loss of personal information which includes personal information, bidding history, and payment details, it further jeopardizes the financial integrity of transactions. If there are weak user authentication mechanisms then these risks increase significantly by facilitating unauthorized account access.

A method for safeguarding the transparency and privacy of the auction system is Visual Cryptography. Visual cryptography includes dividing an image into several shares, each of which only holds a portion of the original image's information. The original image can only be recreated by combining a particular combination of shares, which can then be distributed to various parties. We may make sure that only authorized people have access to sensitive information by utilizing visual cryptography. Along with this AES-128 algorithm has also been used to deal with the problems of shill bidding, data privacy and user authentication.

At the time of registration, we will be generating an image with unique captcha and then that image will be broken into two shares, one share will be sent on the user’s email address and the other will be saved in our database The voter must combine the shares to reassemble their credentials before they may log in to the auction system. As a result, even if one or more shares are intercepted, an attacker will not be able to obtain the user's credentials without all of the shares.

Overall, an auction system that employs visual cryptography along with other encryption methods can offer a reliable approach to guarantee the accuracy and transparency of the auction process and the privacy of the participants of the auction.

1.3 OBJECTIVES

Our project aims to enhance the security and privacy of an online auction system by using various encryption and cryptographic techniques. The main objectives are as follows:

1. **User Security:** This online system helps to protect user data from unauthorized access and modifications. In order to achieve this various encryption and authentication techniques have been employed.

2. **Fraud Prevention:** In order to detect and prevent the fraudulent activities such as shill bidding, strong cryptographic algorithms such as visual cryptography have been used.

3. **Transparent Bidding Process:** Another major objective of this proposed online auction system is to make sure that transparency is maintained throughout the process, it is achieved by maintaining a clear record of all bids, user IDs and bid amounts and providing real time bidding information and clear auction results and outcomes.

4. **Fair Auction Environment:** The proposed system helps in fostering transparency and fairness in the auction process by providing clear and accessible information about items, sellers, and bidding history, in the process thus building trust among participants and enhancing the overall user experience.

5. **Compliance with Regulations:** The online auction system needs to adhere to legal and regulatory standards, thus ensuring a secure and reliable environment where the risks of legal consequences are completely minimized.

1.4 SIGNIFICANCE AND MOTIVATION OF THE PROJECT REPORT

1.4.1 SIGNIFICANCE

Some key points highlighting the importance of a secure online auction system are:

1. **Trust and Credibility:** The security measures which have been used in the auction system will instill trust among the users and it will motivate them to participate in the online auction as they will be assured that their privacy is always protected.

2. **Protection of Sensitive Data:** As being an online auction platform, it handles a lot of sensitive information such as personal details, financial details which when leaked can lead to financial losses and privacy breach. Therefore, a secure platform protects sensitive data from being hacked thereby saving the users from various kinds of thefts.

3. **Adaptation to Digital Transformation:** This auction system helps the users to switch from the traditional auction methods to this digital platform thus giving the buyers the freedom to buy the product of their choice at the comfort of their homes and along with this it also provides the sellers opportunity to let their products reach a larger market.

4. **Enhanced Security Features:** This system is equipped with multiple security features such as visual cryptography, AES-128 encryption and two factor authentication, which helps us to create a robust and secure platform.

5. **Innovation:** It also encourages innovation in cybersecurity technologies and practices. It not only drives the development of cutting-edge security solutions but also benefitting the global auction sector and contributing to advancements in cybersecurity overall.

1.4.2 MOTIVATION

As we are all aware of the rapid technological advancements that has taken place in the last decade or so and the shift it has created in the minds of the internet users which has led them to switch from the traditional and obsolete systems to the online systems, thus giving them the opportunity to explore and discover more things at the place and time of their choice, unlike the old systems where they were required to physically visit the venue.

The same thing is seen in the auction systems, where the traditional systems required the use of a lot of machinery, money, and workforce, where as its counterpart does not require any of it, instead it provides the sellers the opportunity of making their products available to a large market. In a vast country like India, such system is very important, as there are many remote parts here which are culturally very rich and they have many skilled artists and tradesmen but their talent and product remains unrecognized as they are not exposed to the other parts. But this system will give them the power to sell their products worldwide such that they are able to earn the money and respect for their talents.

This system also helps to remove the middle men who used to exploit the sellers and used to take a portion of their well-deserved money. It also stands very helpful in the situations where the sellers tend to be very cunning and used to deploy their agents or men to fluctuate the prices of their products, which is termed as shill bidding, this system will help to keep a check on such miscreants.

All of these situations have led to the increase in the use of the online auction systems, and with this the number of online frauds taking place on such sites has also increased vastly.

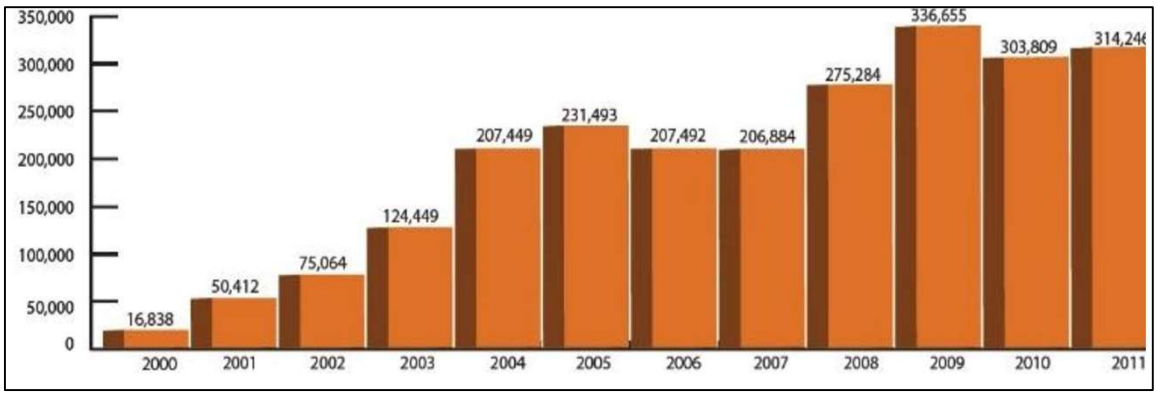


Figure 1.1: Increase in the number of online auction fraud complaints over the year

As we can see from the above statistics that the number of fraud complaints has only increased and it does not seem to be decreasing. Therefore, the development of an auction system that is equipped with multiple security features is of utmost importance.

1.5 ORGANIZATION OF PROJECT REPORT

Chapter 1: Introduction The introductory chapter aims to talk about the increase in cases of online action frauds, and the need to switch from the traditional and obsolete systems to the online version. It also emphasizes on the importance of security in such systems. The chapter describes the problem statement and objectives used in the project, which includes the implementation of various encryption algorithms.

Chapter 2: Literature Review This chapter aims to present various literature review of existing research on the need of security in the auction systems. It also talks about the most suitable algorithm to be encrypted and apart from this also addresses the key gaps present in those literature.

Chapter 3: System Development The chapter explains the various stages of the project and also describes the various security features and encryption that have been used. The chapter also describes the requirements, methodology and the problems faced in the project. The working of the visual cryptography algorithm and the AES-128 algorithm have also been described in detail.

Chapter 4: Testing This chapter presents an in-depth analysis of the testing strategy that has been used in the project, and also talks about the various checks employed at different stages of the project.

Chapter 5: Result and Evaluation This chapter presents an analysis on the result obtained in the previous chapter, it also showcases various important portions of the project, such as OTP authentication, visual cryptography and AES-128 algorithm.

Chapter 6: Conclusion and Future Scope The final chapter summarizes the outcomes of the project and the limitations, suggesting potential improvements and future research directions. It also talks about the future scope of the project, which needs to be taken care in the future in order to enhance the performance of the project. Some of the future scope include the use of RSA public key exchange algorithm and Aadhaar based authentication of the user.

CHAPTER 2

LITERATURE SURVEY

2.1 OVERVIEW OF RELEVANT LITERATURE

2.1.1 INTRODUCTION

Online Auctions have gained a lot of popularity in the recent years, the sole reason for this is that they offer a convenient and efficient way to buy and sell goods. However, they are also exposed to many threats such as shill bidding, illicit user authentication and data privacy. Therefore, it is very important to develop such auction systems which are capable of safeguarding the interests of both the buyers and sellers.

In recent years, various research papers have been published, which are solely focused on developing more effective techniques for enhancing the security of the auction systems. The authors of these papers come from diverse backgrounds. This chapter aims to discuss these papers and their methodologies. It will provide an overview of the latest developments in enhancing the security of the auction systems, serving as a guide for researchers and practitioners working in this field.

2.1.2 A SUMMARY OF THE RELEVANT PAPERS

M. Hasanuzzaman et al. [1] proposed an auction system wherein, the user registers himself with required credentials, once the details are filled, they can access the app where all the products will be displayed on the screen. If a buyer wants to participate in the bid, then he has to apply for virtual coins to the shop admin. After the verification, a certain number of virtual coins will be added to the user's account. A buyer cannot bid for more than the number of Virtual Coins in his account.

S.Pethe et al. [2] proposed a system made using UML to design the web application using class diagrams, sequence diagrams, data flow diagrams, etc. The UML had been developed to reduce the life cycle of system development and to easily maintain the system along with increasing model reusability. React has been used in this system which employs the use of reusable components that helps in easing the frontend development process. Functional components in React, along with hooks have been used.

S.C. Tan et al. [3] proposed a secure cryptographic auction system by using asymmetric encryption, digital signature scheme, and hash functions. The authors were aware of the fact that a symmetric encryption scheme is vulnerable to the point of failure since it relies on the existence of a third party. Hence, the authors were motivated to create a secure e-auction system with both asymmetric encryption and digital signature implementation. It was developed using Java programming language and an H2 database for storing data. It utilized the Java cryptography packages such as java.security and javax.crypto. It also used the RSA key pair consisting of a public key(pk) and private key(sk) to perform encryption, decryption, signature creation, and signature verification.

D. Anand et al. [4] proposed an auction system, where in a unique registration ID is provided to the users only when they verify and validate their email id and government issued id card. The authors mainly talked about the improvements and extra additions to the existing model, the three main things that were discussed in this research paper include trust and its significance and also how navigation support system will build security, trust and reliability and feedback and new ideas column that will let the authors know about what user thinks of their services and also the new things that users want in that system that will give them brief idea how to improve which ultimately results in betterment and growth.

AN. Ramamani et al. [5] proposed an enterprise-based system that runs on several servers in order to distribute database I/O and web transactions. The system was designed to be highly-scalable and capable of supporting large number of bidders in an active auction. This research paper proposed several techniques to solve the problem of authenticity and data privacy, in this system the administrators were provided with the responsibility of authorizing the product to auction, set auction dates and minimum auction amount for that product. In addition to this, prior to each bid, the user's bank or credit account needed to be authenticated for available balance required for the bid. It also had the option where owner could withhold rare articles on the advice of the administrator that would be further thrown open in special auctions held by the site so as to increase the bid-values.

Y. Shah et.al. [6] proposed a hybrid approach by combining the two most important algorithms i.e., AES and DES, the parameter on which these algorithms were compared was the Avalanche effect. Avalanche effect in cryptography describes the behavior where a small change in the input data results in a significantly different output or cipher text. After thorough experiments and testing the authors concluded that AES has a significantly stronger

avalanche effect compared to DES, and this was primarily due to the differences in the design and strength of these encryption algorithms. The primary reason due to which AES has a stronger avalanche effect is due to its key length and block size as it supports key lengths of 128,192, and 256 bits, while DES uses a fixed key length of only 56 bits and it operates on 128-bit blocks, while DES uses 64 bit-blocks.

2.2 KEY GAPS IN THE LITERATURE

After going through several relevant literatures on the online auction system the main problem that was common to all of them was that they ignored the importance of security in their systems their primary focus revolved around creating an online auction system to facilitate the accessibility problem but they failed to address the issue of security. None of the papers focused on the main threat to the online auction system, i.e., shill bidding which can lead to tremendous financial losses to both the seller and buyer.

In M. Hasanuzzaman et al.'s work [1], although the user registration and virtual coin mechanisms are introduced, the paper lacks a detailed exposition of the security measures implemented, leaving questions about encryption and authentication protocols unanswered. S.Pethe et al.'s research [2], while emphasizing the use of UML for system design and React for frontend development, falls short in providing an in-depth exploration of security aspects such as data transmission security, user authentication, and authorization mechanisms. S.C. Tan et al.'s cryptographic auction system [3] introduces commendable security measures but lacks a comprehensive analysis of potential attacks and countermeasures, and the choice of an H2 database raises concerns about scalability.

D. Anand et al.'s work [4] discusses trust and reliability but lacks a thorough examination of trust-building mechanisms and leaves the role of the navigation support system in enhancing security and reliability unclarified. AN. Ramamani et al.'s scalable system [5] addresses scalability but lacks details on load balancing and fault tolerance, and the authentication of user accounts is mentioned without a detailed discussion of the associated security protocols. Lastly, Y. Shah et.al.'s study [6], while contributing to the understanding of encryption algorithms, omits a discussion on the overall security architecture of the online auction system, leaving the integration of chosen encryption methods and their role in end-to-end security unexplored.

In order to address these security concerns about database protection, user authentication and data privacy we have used multiple encryption techniques for tackling the individual issue. We have implemented the RSA algorithm in case of first price sealed bid auction where the authenticity of the details of bid is of paramount importance, RSA uses public key and private key, the auction participants are provided with the public key and the private key is provided only to the admin, such that bids remain confidential and cannot be tampered with during transmission.

CHAPTER 3

SYSTEM DEVELOPMENT

3.1 REQUIREMENTS AND ANALYSIS

In order to design a Secure Auction System that is not prone to any security risks, we need to take into consideration various requirements for the same, and we also need to make sure that these requirements are met completely, apart from this we also need to perform thorough analysis to address the potential security risks. Below are some key requirements and analysis that we must need to consider.

3.1.1 FUNCTIONAL REQUIREMENTS

The following is included in the functional requirements:

1. **Seller and Buyer Registration and Authentication:** The users should be able to register with their valid credentials, and the system should be able to authenticate users safely taking into use multi-factor authentication. It will help us to ensure that only registered and verified users can take part in the bid, and thus we will be able to prevent any sort of tampering in the prices of the items available for bid.

2. **Visual Cryptography Algorithm:** The system is also equipped with an efficient and secure visual cryptography algorithm which is capable of creating unique pair of shares for each user and these shares can then be used to provide an extra layer of security at the time of auction.

3. **Item Listing:** The website is be designed in such a way that the seller is able to list the desired products for auction, and the products listed by them are visible to the buyers thus facilitating the process of auction further.

4. **Auction Monitoring:** The changes made in the prices of the articles are visible to the participants in real time, and it also notifies the users about the end date of the auction of a particular product and apart from these details of the product whose bid has been closed are also displayed.

5. **User Account Management:** The users have been given the freedom the to modify the details of their account for instance user name, password, email, phone number at their own will, at the time of login they are having the option of changing the password by clicking on the forgot password button after login they can access their profile and update the desired credentials.

6. **Winner Determination:** At the end of the auction when the end date of the auction as set by the seller has expired, then the winner of the auction is determined and the notification is sent to the buyer congratulating him for the same and also sharing details of the seller.

3.1.2 NON-FUNCTIONAL REQUIREMENTS

The following have been included in the non-functional requirements:

1. **Security:** In order to safeguard the data being entered into the database the AES-128 encryption algorithm has been used and apart from this visual cryptography, mobile otp and alphanumeric password have also been used.

2. **Performance:** The changes made in the prices of the products is updated in real time in the database and the same is also displayed without any delay, a lot of care has been taken to make sure that the performance and response time of the auction is not hindered in any way depending on the increase in number of concurrent users.

3. **Usability:** Bootstrap has been used to ensure that the website is responsive and user friendly, by doing this we have also made sure that there is no limitation on the device on which it can be used, it can be used on any device with an internet connection.

4. **Scalability:** The application has been designed in such a way that sudden increase in the user loads does not affect it and the time to fetch data from the database is also not compromised in such an untimely situation.

3.1.3 HARDWARE REQUIREMENTS

The hardware requirements are as follows:

1. **Server:** In order to scale the application XAMPP has been used as a local server, by doing this we were able to see the changes made in the code being updated in real time on the website and it also never faced any issue due to the increased traffic and load on the system.

2. **Storage:** In order to make sure that the rendering and loading time is less we have used the local storage, it also provided us with extra storage and there was no burden present for the storage level.

3. **Network:** A reliable internet connection with sufficient bandwidth is needed in order to handle the incoming and outgoing data.

3.1.4 SOFTWARE REQUIREMENTS

The software requirements needed to be taken care of in the project are as follows:

3.1.4.1 LANGUAGES USED

- **HTML:** HTML stands for Hyper Text Markup Language. It is used to design web pages using a markup language. HTML is a combination of Hypertext and Markup language. Hypertext defines the link between web pages. A markup language is used to define the text document within the tag which defines the structure of web pages. This language is used to annotate text so that a machine can understand it and manipulate text accordingly. Most markup languages are human-readable. The language uses tags to define what manipulation has to be done on the text.

- **CSS:** CSS stands for Cascading Style Sheets. It is a style sheet language which is used to describe the look and formatting of a document written in markup language. It provides an additional feature to HTML. It is generally used with HTML to change the style of web pages and user interfaces. It can also be used with any kind of XML documents including plain XML, SVG and XUL.CSS is used along with HTML and JavaScript in most websites to create user interfaces for web applications and user interfaces for many mobile applications.

- **PHP**: PHP stands for Hypertext Processor, it is a scripting language which is freely available and is very widely used for web development, it is primarily used for server-side scripting, but it can also be used for command line scripting. It is integrated with a number of popular databases, including MySQL, PostgreSQL, etc. The MySQL server after its execution is capable of handling complex queries with huge result sets in no time. It is used for developing dynamic web pages, it is executed on the server, and the result is sent to the client as plain HTML code.

- **JavaScript:** JavaScript is a versatile programming language, used for enhancing user interfaces and enabling dynamic, interactive elements within web browsers. It primarily serves as a client-side scripting language, it gets executed within the browsers of the user thus allowing for real time updates, dynamic content modifications, and improved user experiences without requiring full page reloads. It is responsive to the actions of the user such as clicks and keypresses, giving the developers freedom to created engaging and responsive web pages.

3.1.4.2 LIBRARIES USED

- **Bootstrap:** It is an open-source front-end framework widely recognized for simplifying the creation of responsive and mobile-first web pages. It was originally developed by Twitter, but now maintained by the open-source community. It offers a comprehensive toolkit which comprises of HTML, CSS and JavaScript components. Its main feature is the responsive grid system which allows the developers to create adaptable layouts across various screen sizes from desktops to mobile devices. It includes an array of pre-built UI components such as navigation bars, buttons, forms and modals, which help to provide consistency in design and in saving time and effort which is normally required for styling common elements [17].

- **GD:** It is a library in PHP which is used for the creation and manipulation of images. GD stands for Graphic Draw, it can be used for the resizing, rotation and cropping of images, it is also used to write text onto the image, this functionality of GD was utilized while applying the visual cryptography algorithm [22].

- **Twilio:** Twilio is a cloud communications platform that provides APIs and services for adding various communication features, such as SMS, voice, video, and more. In order to facilitate the integration of the Twilio services into PHP, Twilio provides an official PHP library. This library allows the developers to interact with the Twilio REST API, thus making it easier to handle and manage the communication related tasks.

- **PHPMailer:** It is very useful library in PHP which is used to send email directly from the code itself, it has an integrated SMTP support due to which it does not require any local mail server. We can send emails to multiple people and also include CC, BCC, and Reply-to addresses, it also enables us to add attachments, due to which we were able to send a share of image to the email id of the users. It validates email addresses automatically and also protects against header injection attacks [21].

3.1.4.3 TOOLS USED

- **Visual Studio Code (VS Code):** Visual Studio Code, commonly known as VS Code, is a very renowned code editor developed by Microsoft. It offers a strong code editing environment, with features such as syntax highlighting, autocompletion, and IntelliSense, thus making it adaptable to a lot of programming languages. There are various extensions available on it, which help the developers in various ways. It also has an integrated terminal within the editor which eases the process of command execution and task automation. Notably, VS Code seamlessly integrates Git, easing version control operations without leaving the editor. Live Share facility provided on it is very useful in web development.

- **XAMPP:** XAMPP is an open-source web server solution package, it is mainly used for web application testing on a local host webserver. XAMPP integrates the Apache HTTP Server with MySQL and PHP, this enables the developers to use an pre-configured environment for testing and deploying web applications on their own system. Apart from the core components mentioned above, it also includes additional tools and interpreters like OpenSSL and phpMyAdmin facilitating secure connection and database management [18].

- **MySQL:** MySQL is a relational database management system (RDBMS), it was developed by Oracle Corporation, it is widely acknowledged for its efficiency in handling structured data. It operates on basis of the relational model by organizing data into tables with rows and columns. It also supports various data types, transactions, and complex queries, which makes it suitable for variety of applications ranging from small-scale projects to enterprise-level solutions.

3.2 PROJECT DESIGN AND ARCHITECTURE

3.2.1 METHODOLOGY

In order to get themselves enrolled to the auction system; the user needs to register with the required credentials. There are two different channels for the user to register:

- **Seller:** The seller can add different products for the auction, at the time of posting a product details like product category, price, bid start date, end date and description are taken as input, seller can also delete the product that has been posted by them.

- **Buyer:** The buyer has the responsibility of bidding on the product whose bid expiry date has not arrived. The buyers can also view all the bids submitted by them, After the end of the auction the buyer with maximum bid is declared as the winner.

In order to prevent fake users from entering into the system we have also created an admin panel, where the admin can see the list of all the active sellers and buyers, and can also remove the seller and buyer whom they consider to be involved in illicit activities.

At the time of registration, the seller and buyer receive a share of image on their registered email id, which they need to use at the time of posting an item and bidding for the desired product. In order to login to the system the seller and buyer are also required to login through the OTP which is received on their registered mobile number, and entering the details of the username and password, after this stage they will be able to visit the dashboard and perform all the other activities.

On the home page the details of all the products whose auction is live and who have not been bought by any user yet are displayed, the details of the item whose auction is over are detailed under the section of the sold items.

Now in order to submit the bid for the auction, the user needs to upload the share of image that was sent on the email id, after this, the uploaded image is merged with the one that was stored in the database and a captcha text is displayed, and the user is prompted to enter the text being displayed on the screen, if the entered text matches the original text that was encrypted then only the user can submit the bid. Similarly in order to post a product the seller needs to first upload the share of image received on the email, and then authenticate it only then the product will be listed.

The captcha text being generated at the time of registration is first encrypted with AES-128 algorithm and then uploaded on the database.

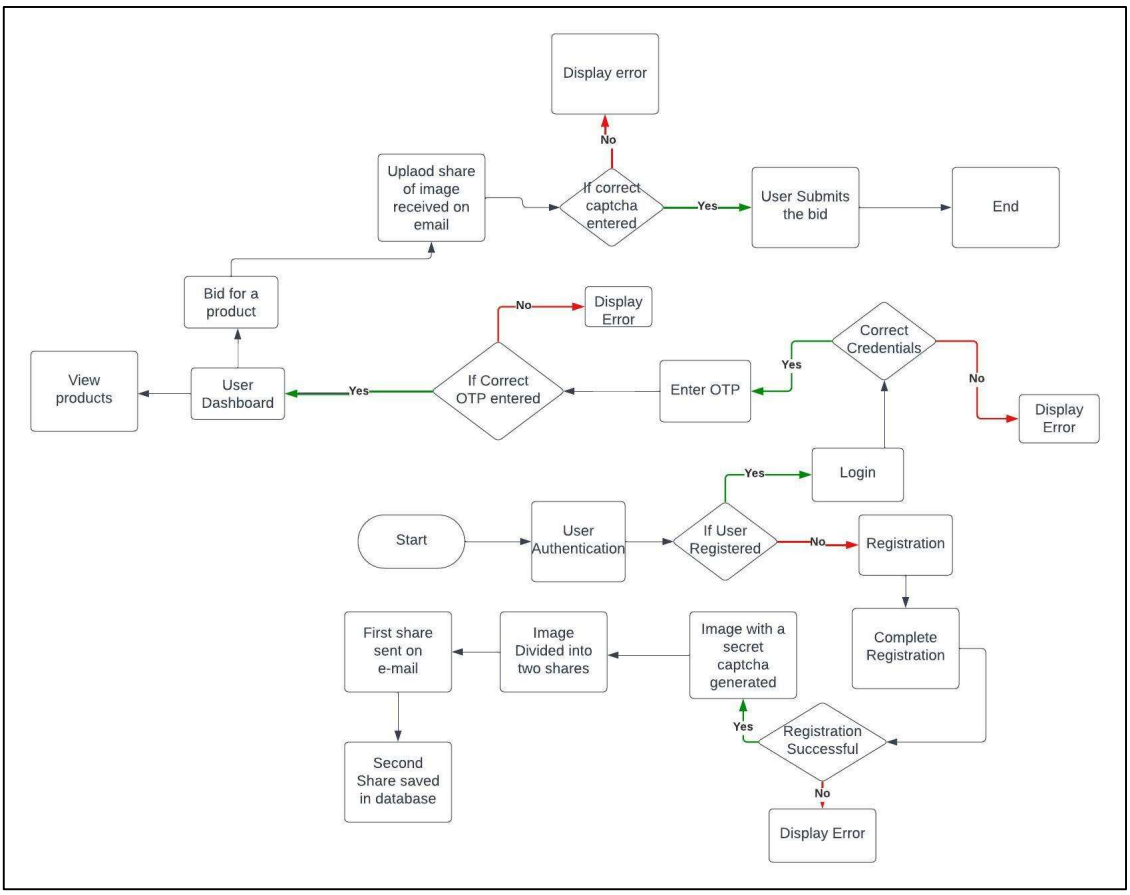


Figure 3.1: Flow Graph of the Project [16]

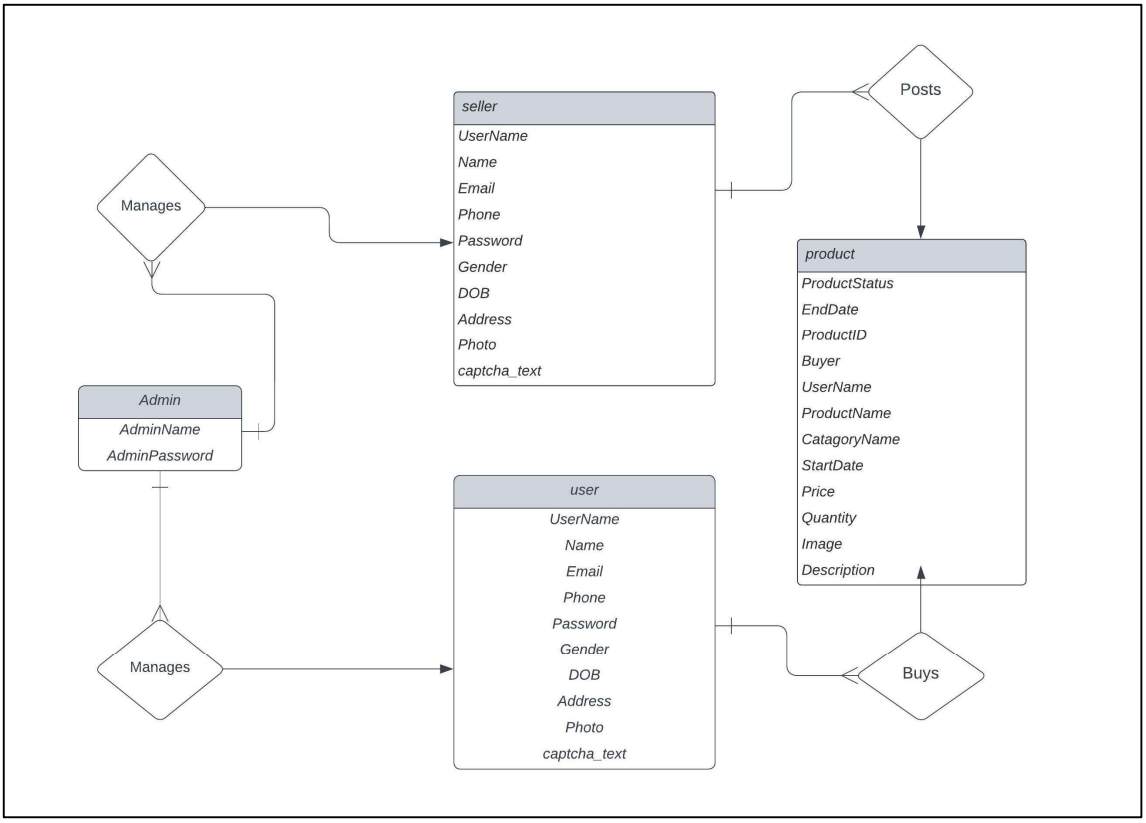


Figure 3.2: Class Diagram

3.3 IMPLEMENTATION

The following is the detailed plan in which the auction system is implemented:

3.3.1 SETTING UP THE ENVIRONMENT

The first step in the development of the auction system was to set up the required environment, i.e., all the tools that will be further used in the process. At first, we installed the XAMPP software which is a web server used to host the website locally on the system. After this we set up the database on the MySQL software which is a relational database management system. We created all the necessary tables in the database that will be required in our application.

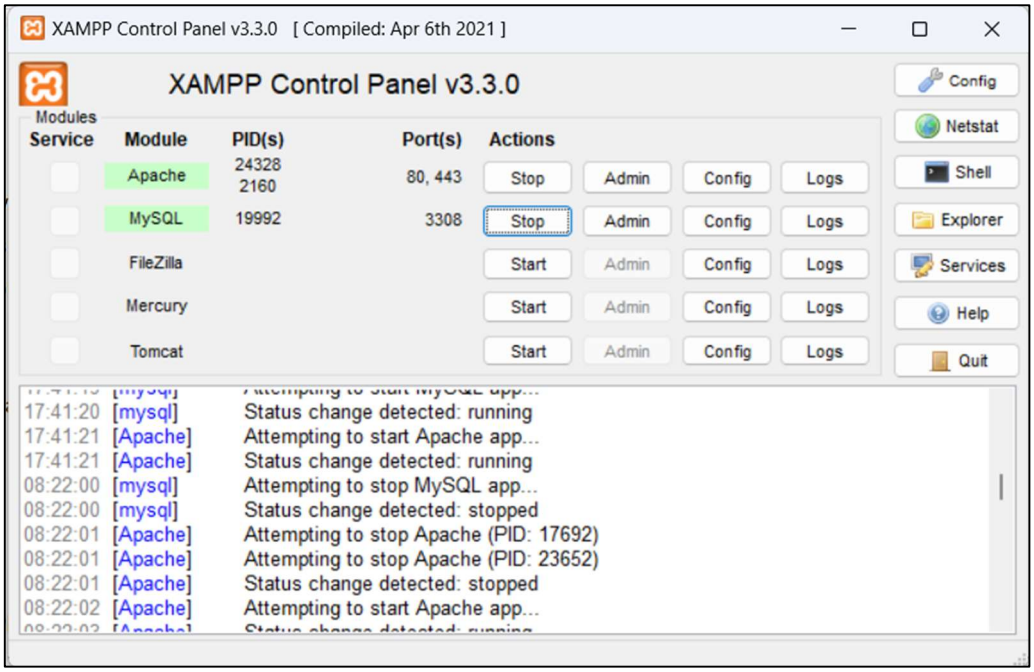


Figure 3.3: Home Page of the XAMPP control panel

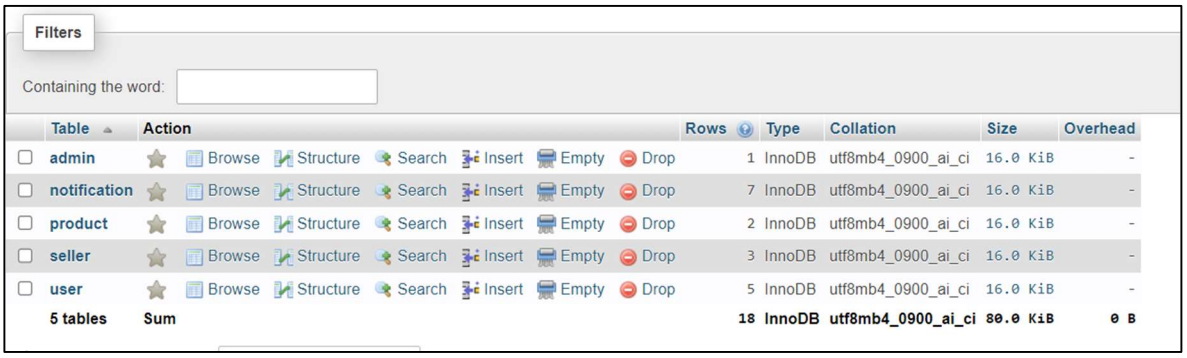


Figure 3.4: Different columns in the bidding table

3.3.2 TWILIO OTP AUTHENTICATION

Twilio is a cloud communications platform that provides APIs and services for adding various communication features, such as SMS, voice, video, and more. In order to ease the integration of the Twilio services into PHP, Twilio provides an official PHP library. This library allows the developers to interact with the Twilio REST API, thus making it easier to handle and manage the communication related tasks.

In order to integrate Twilio to our website we first of all obtained API credentials from Twilio by signing up for a free account, then we imported the Twilio PHP library in our own program.

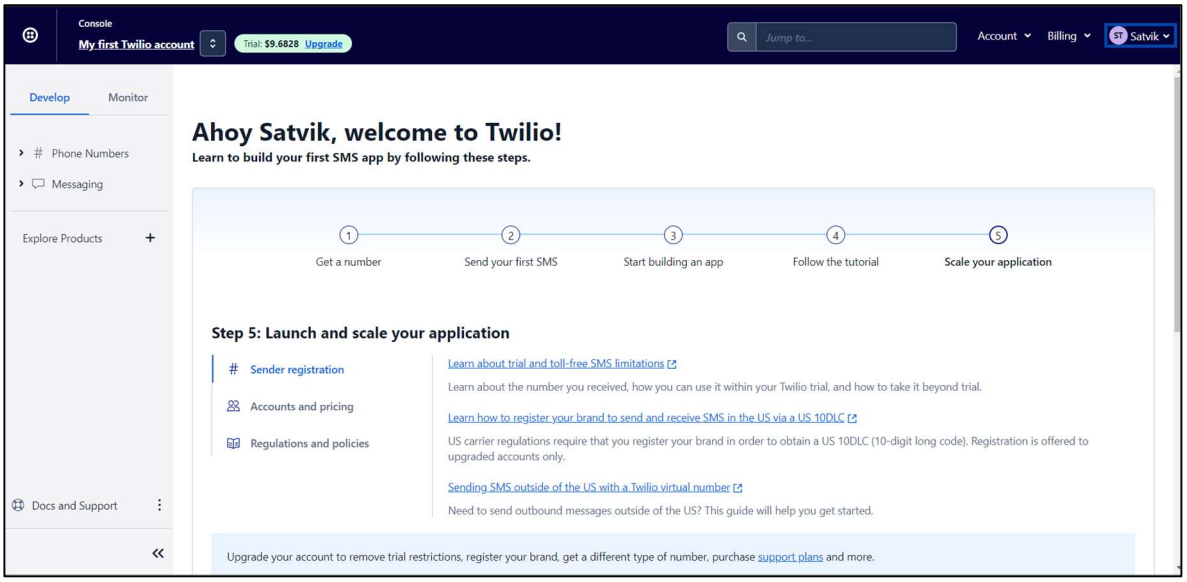


Figure 3.5: Dashboard of the Twilio API [20]

After this we extracted the mobile number of the user from the database and then generated a random number between 1 and 1000 that will be sent as an OTP on the mobile of the user.

```
        if (($username == $user) && ($password == $pass)) {
            $otp_code = rand(1000, 9999);
            $_SESSION['otp_code'] = $otp_code;

            $to = '+91' . $pass;

            $sid = "ACcf35b617cbe3cc34de807c560c02e2c5";
            $token = "4ca3a1a69551a2fb9b45aac02b53ea8c";
            $client = new Twilio\Rest\Client($sid, $token);

            $client->messages->create(

                $to,
                array(

                    'body' => 'Your OTP code is: ' . $otp_code,

                    'from' => '+14147518834'
                )
            );

            echo "OTP has been sent";
        } else {
            echo "<script>alert('Invalid credentials')</script>";
        }
    } else {
        echo "<script>alert('User not found')</script>";
    }
}
```

Figure 3.6: Code snippet for sending OTP using Twilio

3.3.3 VISUAL CRYPTOGRAPHY

Visual Cryptography is a method of secure communication that uses images to encrypt secret messages. The phenomenon of visual cryptography is that, an image is divided into multiple shares and the original message that was present behind the image is also broken into that many shares, now in order to decrypt the message all the shares in which the original image was broken into need to be superimposed.

There are primarily two types of visual cryptography schemes:

- **(2,2) Visual Cryptography Scheme:** In this cryptography scheme, the original image is divided into two shares, these shares appear as random patterns or noise when these two shares are overlaid then only the original message is revealed.
- **(2, n) Visual Cryptography Scheme:** In this scheme the original image is divided into more than two shares and any two shares among the n shares can be stacked to reveal the original message inside the image.

The technique which we have used in our system is the basic visual cryptography in which the original image is divided into two shares.

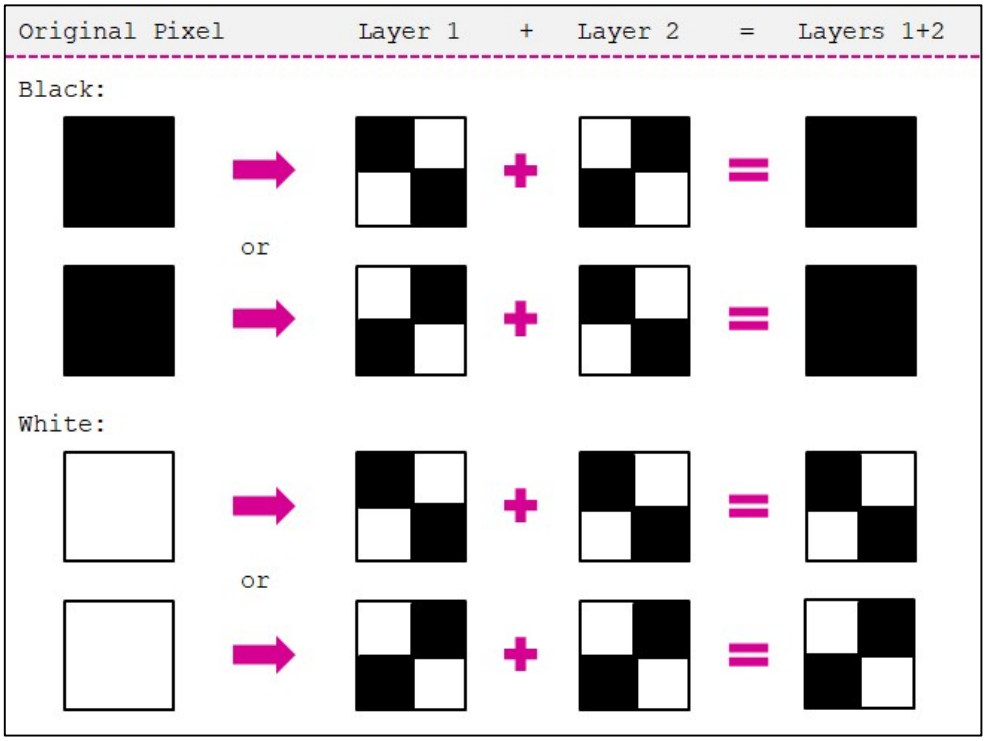


Figure 3.7: Visual Cryptography technique [12]

Figure 3.8: Initial Captcha Image

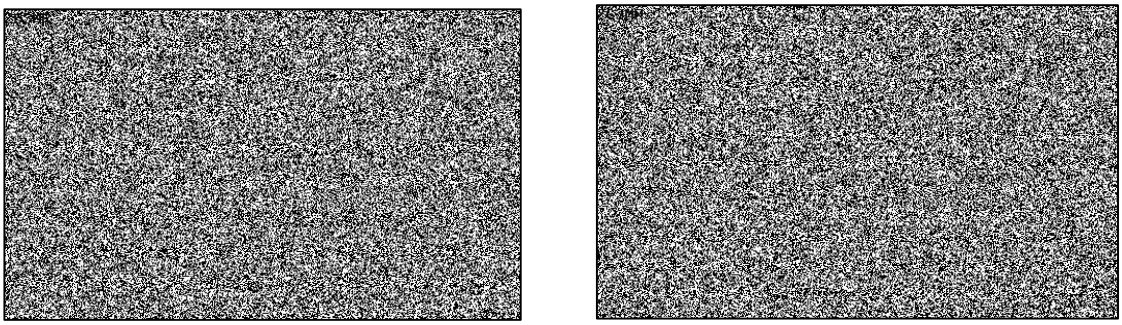


Figure 3.9: Two shares in which the original captcha Image is divided

Figure 3.10: The reconstructed captcha Image displayed on the page.

In order to implement the Visual Cryptography algorithm, we have used the GD library of PHP, which is used for image generation and manipulation. First of all, we have generated a random captcha text and then used the GD library to enshrine it on the image.

```
$captchatext="";
$captchatext = substr(str_shuffle('ABCDEFGHJKLMNPQRSTUVWXYZ123456789'), 0, 5);

$img = imagecreate(500, 300);
$white = imagecolorallocate($img, 255, 255, 255);
$blue = imagecolorallocate($img, 0, 0, 255);
imagefilledrectangle($img, 0, 0, 500, 300, $white);
imagestring($img, 5, 0, 0,$captchatext, $blue);
imagejpeg($img, "IMAGE.jpg");
imagedestroy($img);
$original_image = imagecreatefromjpeg('IMAGE.jpg');
```

Figure 3.11: Code snippet for generating the captcha image which is to be encrypted

After this we have broken the generated image into two shares, by iterating over each pixel position in the original image and then extracting the color present at that particular pixel position, then we have broken the color into their RGB components, and then we have taken a random value between 0 and 255 if this value is less than or equal to 128 then the color which was present at current pixel position is set at the same position in the first share of image, similarly if the value of the random integer is greater than 128 then the current pixel's color is filled in second share of the image at the same position.

```
    $share1 = imagecreatetruecolor(imagesx($original_image), imagesy($original_image));
    $share2 = imagecreatetruecolor(imagesx($original_image), imagesy($original_image));
    for ($x = 0; $x < imagesx($original_image); $x++) {
  for ($y = 0; $y < imagesy($original_image); $y++) {
    $color = imagecolorat($original_image, $x, $y);
    $r = ($color >> 16) & 0xFF;
    $g = ($color >> 8) & 0xFF;
    $b = $color & 0xFF;
    $rand = rand(0, 255);
    if ($rand >= 128) {
      imagesetpixel($share1, $x, $y, imagecolorallocate($share1, $r, $g, $b));
      imagesetpixel($share2, $x, $y, imagecolorallocate($share2, 0, 0, 0));
    } else {
      imagesetpixel($share1, $x, $y, imagecolorallocate($share1, 0, 0, 0));
      imagesetpixel($share2, $x, $y, imagecolorallocate($share2, $r, $g, $b));
    }
  }
}
imagejpeg($share1, "share1.jpg");
$filename = "shares/" . $uname . "_share2.jpg";
imagejpeg($share2, $filename);
```

Figure 3.12: Code snippet for breaking the original image into two shares

Now comes the decryption part of the algorithm where we will be combining both the shares of image that were generated at the time of encryption, in order to do this, we will first create a reconstructed image and then fill colors in each pixel of this image, we will iterate through each pixel of the two shares of the image and then break the corresponding color in that pixel

into their RGB components and then add these components of both the share and then put the corresponding color value into the reconstructed image.

```
$width = imagesx($share1);
$height = imagesy($share1);
$reconstructed_image = imagecreatetruecolor($width, $height);

if (!$reconstructed_image) {
    die('Failed to create new image');
}

for ($x = 0; $x < $width; $x++) {
    for ($y = 0; $y < $height; $y++) {
        $color1 = imagecolorat($share1, $x, $y);
        $color2 = imagecolorat($share2, $x, $y);
        $r1 = ($color1 >> 16) & 0xFF;
        $g1 = ($color1 >> 8) & 0xFF;
        $b1 = $color1 & 0xFF;
        $r2 = ($color2 >> 16) & 0xFF;
        $g2 = ($color2 >> 8) & 0xFF;
        $b2 = $color2 & 0xFF;
        if ($r1 == 0 && $g1 == 0 && $b1 == 0 && $r2 == 0 && $g2 == 0 && $b2 == 0) {
            imagesetpixel($reconstructed_image, $x, $y, imagecolorallocate($reconstructed_image, 0, 0, 0));
        } else {
            $r=$r1 + $r2;
            $g=$g1 + $g2;
            $b=$b1 + $b2;
            if($r > 255) { $r = 255; }
            if($g > 255) { $g = 255; }
            if($b > 255) { $b = 255; }
            if($r < 0) { $r = 0; }
            if($g < 0) { $g = 0; }
            if($b < 0) { $b = 0; }
            imagesetpixel($reconstructed_image, $x, $y, imagecolorallocate($reconstructed_image, $r, $g, $b));
        }
    }
}
```

Figure 3.13: Code snippet for rejoining the two shares to decrypt the message

3.3.4 AES-128 ALGORITHM

In order to encrypt the captcha text that is being stored in the database we have used the AES-128 algorithm, AES stand for Advanced Encryption Standard, and the 128 here signifies the key size. It is capable of encrypting and decrypting the data with the same secret key. The block size is also of 128 bits in this encryption algorithm, there are two more variants of this algorithm where the key size is 192 and 256 bits respectively. The number of rounds also vary depending on the key size for 128,192 and 256 it is 10,12 and 14 rounds respectively [14].

Each round consists of four basic operations:

- **SubBytes:** In this round each byte in the block is substituted with a corresponding value from a lookup table.

- **ShiftRows:** The rows of the blocks are shifted by a certain number of bytes in this operation.

- **MixColumns:** The mixcolumn operation mixes the columns of the block by multiplying them with a fixed polynomial.

- **AddRoundKey:** This operation is used to XOR the block with a portion of the secret key.

All of these operations occur in each round, except the MixColumn which does not occur in the final round. After the last round, the ciphertext block is obtained, which can be decrypted using the same secret key. The decryption process is the reverse of the encryption process, consisting of the same operations in reverse order.

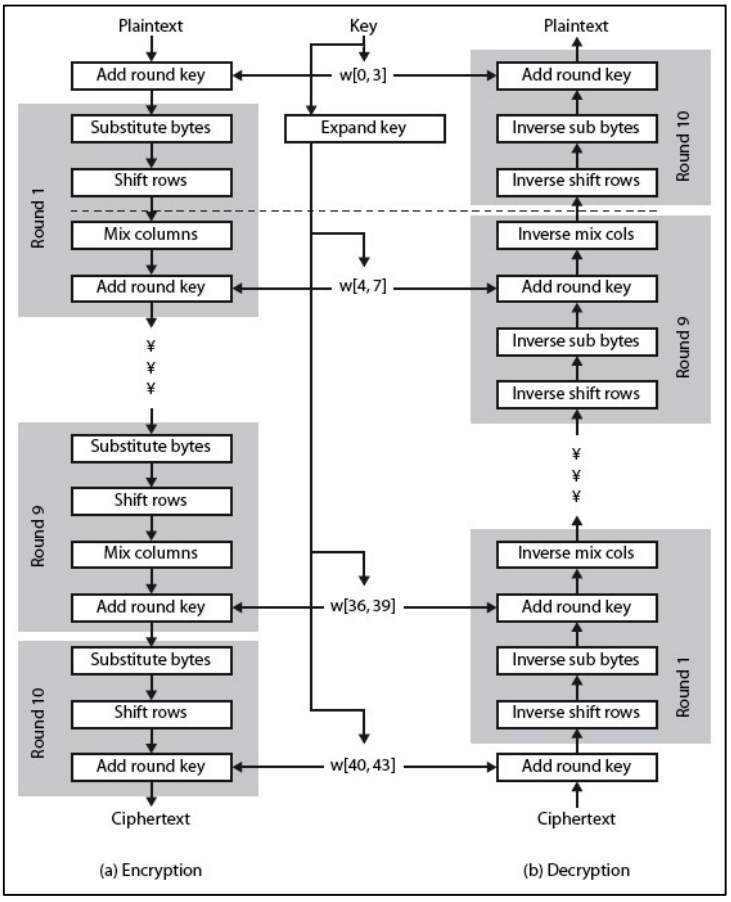


Figure 3.14: AES Architecture [15]

```
$original_string = $captchatext;
$cipher_algo = "AES-128-CTR";
$iv_length = openssl_cipher_iv_length($cipher_algo);
$option = 0;
$encrypt_iv = $phone;
$encrypt_iv = str_pad($encrypt_iv, 16, "\0");
$encrypt_key = $name;
$encrypted_string = openssl_encrypt($original_string, $cipher_algo,$encrypt_key, $option, $encrypt_iv);
$captchatext = $encrypted_string;
```

Figure 3.15: Code snippet for AES-128 encryption

```
$cap_t = $row['captcha_text'];
$encrypted_string = $cap_t;
$cipher_algo = "AES-128-CTR";
$iv_length = openssl_cipher_iv_length($cipher_algo);
$option = 0;
$decrypt_iv = $row['phone'];
$encrypt_iv = str_pad($decrypt_iv, 16, "\0");
$decrypt_key = $row['key'];
$decrypted_string=openssl_decrypt ($encrypted_string, $cipher_algo,$decrypt_key, $option, $decrypt_iv);
$cap_t=$decrypted_string;
```

Figure 3.16: Code snippet for AES-128 decryption

3.3.5 CRYPTOGRAPHIC HASHING

A hash function H accepts a variable-length block of data M as input and produces a fixed-size hash value h = H(M). A "good" hash function has the property that the results of applying the function to a large set of inputs will produce outputs that are evenly distributed and apparently random. In general terms, the principal object of a hash function is data integrity. A change to any bit or bits in M results, with high probability, in a change to the hash value.

The kind of hash function needed for security applications is referred to as a cryptographic hash function. A cryptographic hash function is an algorithm for which it is computationally infeasible (because no attack is significantly more efficient than brute force) to find either (a) a data object that maps to a pre-specified hash result (the one-way property) or (b) two data objects that map to the same hash result (the collision-free property). Because of these characteristics, hash functions are often used to determine whether or not data has changed.

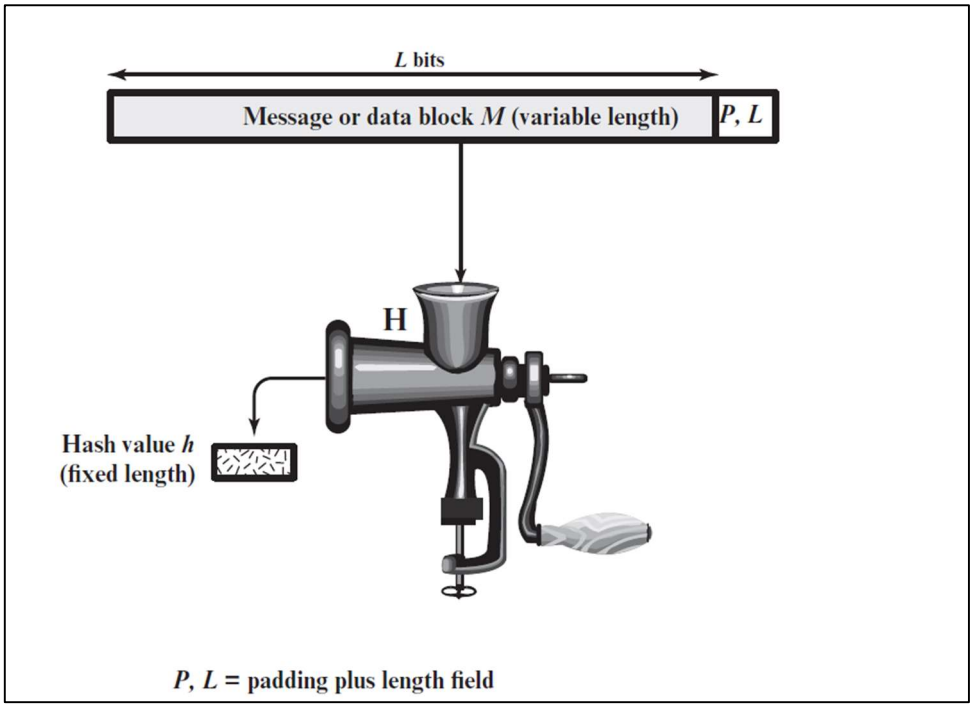


Figure 3.17: Cryptographic Hash Function; h= H(M)

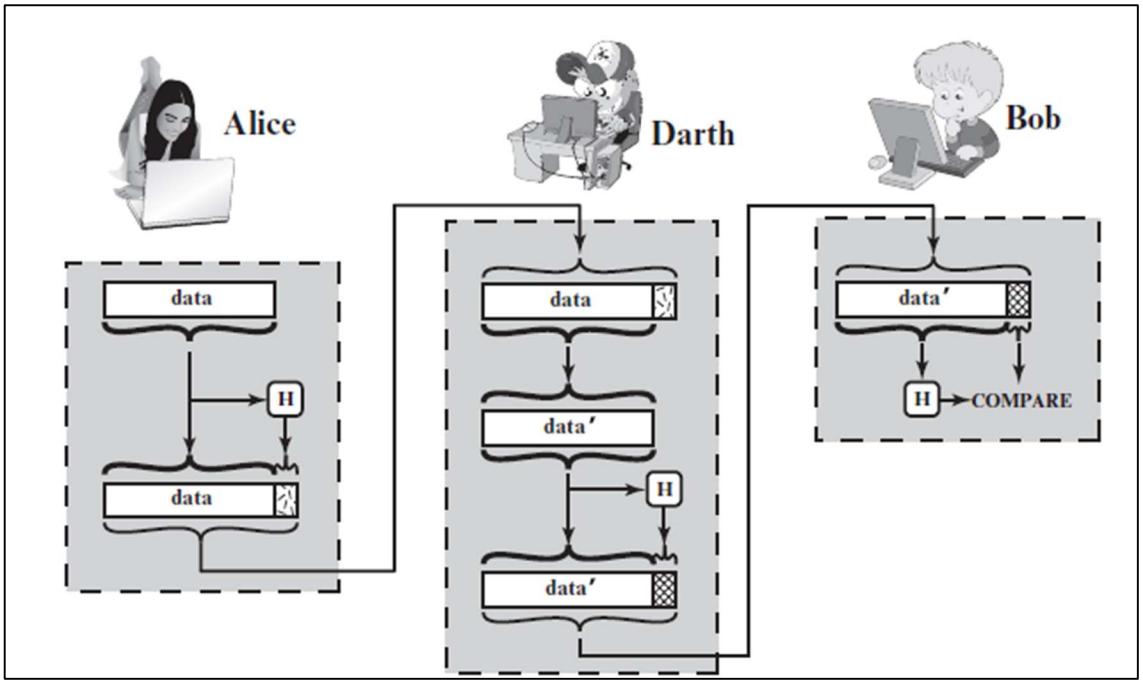


Figure 3.18: Attack against Hash Function

In order to enhance the security, we have used bcrypt hashing algorithm to store the password of buyer and seller in form of a cryptographic hash in the database. Bcrypt is a cryptographic hash function which is designed for password hashing and safe storing in the backend of

applications in a way that is less susceptible to dictionary-based cyberattacks. Bcrypt is better than SHA 256 algorithm as it contains a salt element which is not present in SHA due to which it becomes more susceptible to dictionary-based cyberattacks, therefore bcrypt is a better solution for safely storing passwords.

Bcrypt runs a complex hashing process, during which a user's password is transformed into a fixed-length thread of characters. It uses a one-way hash function, meaning that once the password is hashed, it cannot be reversed to its original form. Every time the user logs into their account, bcrypt hashes their password anew and compares the new hash value to the version stored in the system's memory to check if the passwords match [24].

Instead of simply hashing the given password, bcrypt adds a random piece of data, called salt, to create a unique hash that is almost impossible to break with automated guesses during hash dictionary and brute force attacks.

Bcrypt also stands out among other hashing algorithms because it uses a cost factor. With the help of this, we can determine the number of password iterations and hashing rounds to be performed, increasing the amount of time, effort, and computational resources needed to calculate the final hash value. The cost factor makes bcrypt a slow algorithm that takes significantly more time to produce a hash key, turning it into a safe password-storing tool.

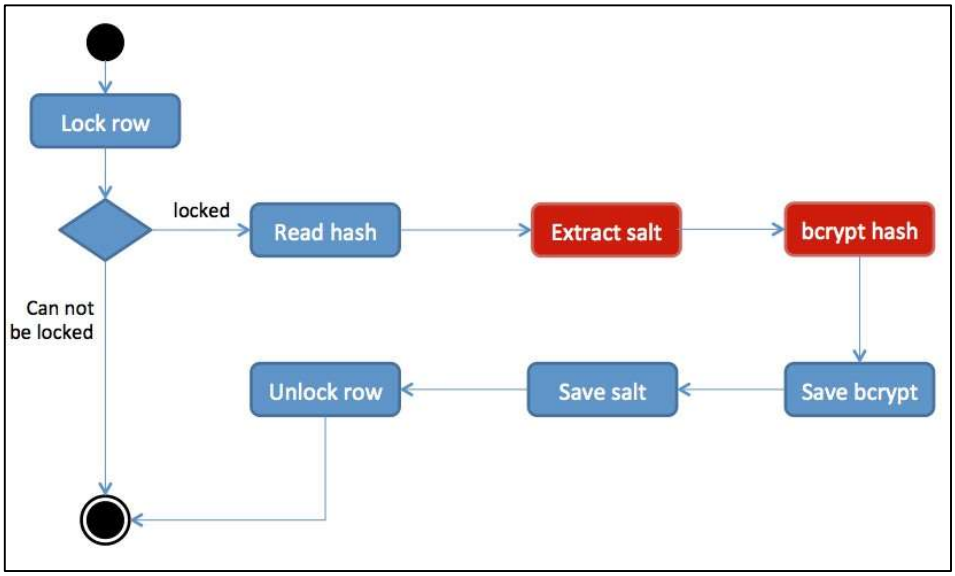


Figure 3.19: Bcrypt Hashing flow diagram

```
$name     =$_POST['name'];
$uname    =$_POST['uname'];
$Password =$_POST['password'];
$Passwordc = $Password;
$Password = password_hash($Passwordc, PASSWORD_BCRYPT);
$email    =$_POST['email'];
$phone    =$_POST['phone'];
$dob      =$_POST['dob'];
$gender   =$_POST['gender'];
$address  =$_POST['address'];
```

Figure 3.20: Code snippet for Bcrypt Hashing algorithm

3.3.6 RSA ENCRYPTION

RSA is an asymmetric cryptographic algorithm, which uses two different but mathematically linked keys in which one is public and the other one is private. In RSA cryptography, both the public and the private keys can encrypt a message. The opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm, it provides a method to assure the confidentiality, integrity, authenticity, and non-repudiation of electronic communications and data storage [25].

We have used this algorithm for sealed bid auctions where the bids submitted by the user are encrypted through the public key and the final winner of the auction is decided with the help of private key which is used to decrypt the bids.

RSA derives its security from the difficulty of factoring large integers that are the product of two large prime numbers. Multiplying these two numbers is easy, but determining the original prime numbers from the total or factoring is considered infeasible due to the time it would take using even today's supercomputers.

The public and private key generation algorithm is the most complex part of RSA cryptography. Two large prime numbers, p and q, are generated using the Rabin-Miller primality test algorithm. A modulus, n, is calculated by multiplying p and q. This number is used by both the public and private keys and provides the link between them. Its length, usually expressed in bits, is called the key length.

The public key consists of the modulus n and a public exponent, e, which is normally set at 65537, as it's a prime number that is not too large. The e figure doesn't have to be a secretly selected prime number, as the public key is shared with everyone. The private key consists of the modulus n and the private exponent d, which is calculated using the Extended Euclidean algorithm to find the multiplicative inverse with respect to the totient of n.

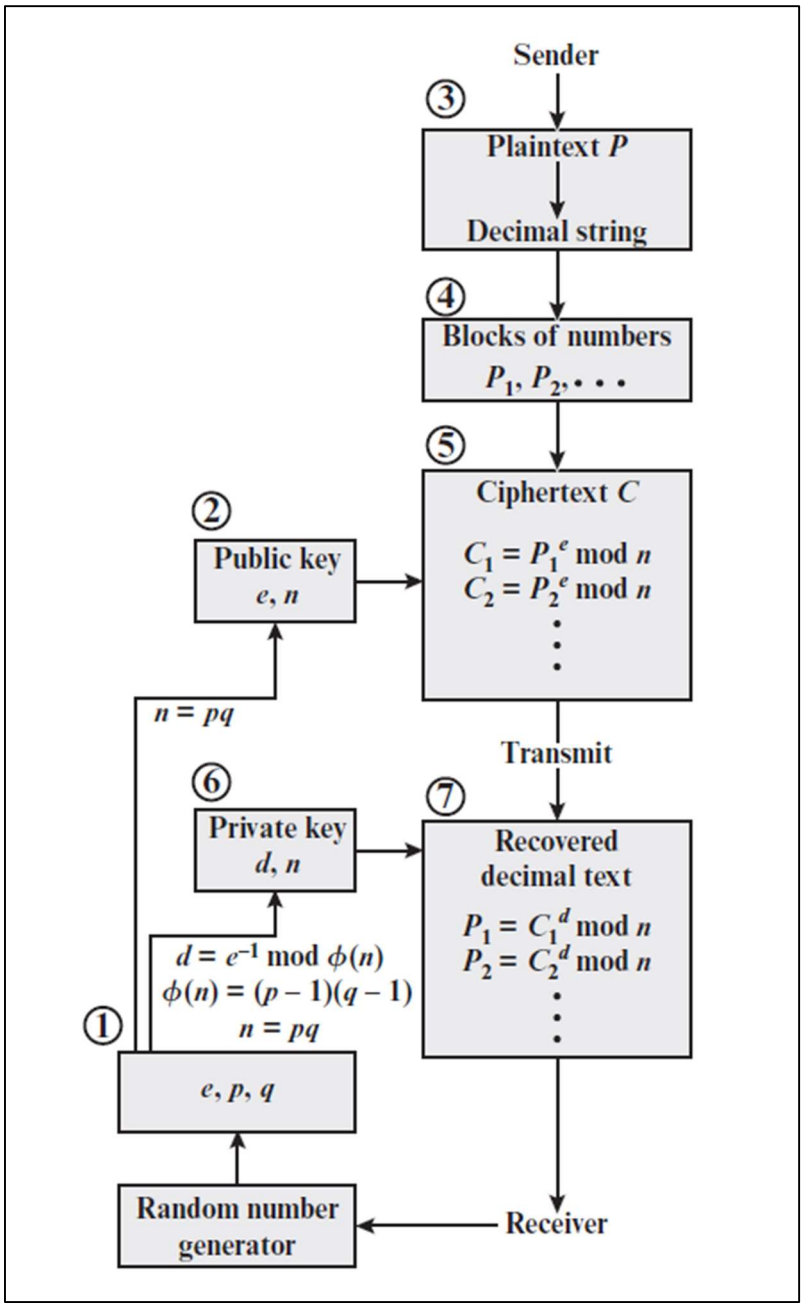


Figure 3.21: RSA processing of multiple blocks

RSA algorithm helped us to hide the current price from the user and only display the starting price of the product, sealed bid auctions only allow the users to submit a single bid for a particular product and for this purpose we created a separate table in the database which was used to store the details of the bid submitted by user for every product.

3.3.7 GOOGLE RECAPTCHA

Google reCAPTCHA has been used in our system, in order to protect it from the automated bots and spam. It is a technology that is developed by Google, which presents users with challenges, such as identifying objects in images or solving puzzles, to verify if they are human. It helps to make sure that the information submitted is coming from real users rather than automated scripts or bots. We have used this feature for the login of both the seller and buyer [19].

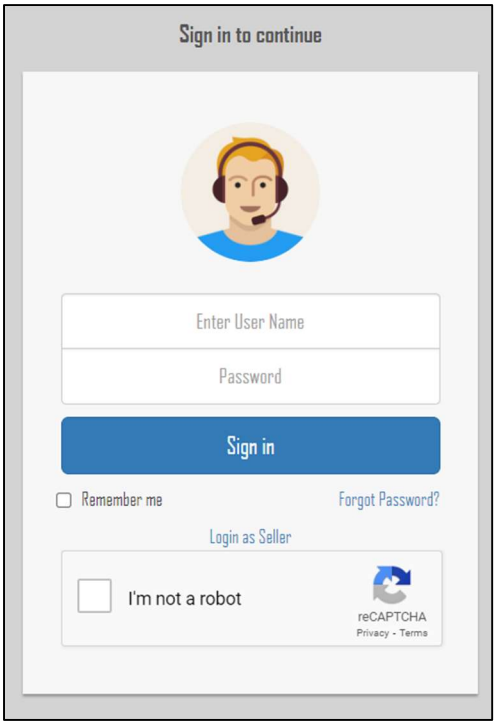


Figure 3.22: ReCAPTCHA being used in the login page

The reCAPTCHA service generates a unique token for the response of each user, which is then sent to the server for verification. The server, in turn, communicates with the reCAPTCHA's API to confirm the validity of the response of the user. If the user verification is successful, then form submission is allowed to proceed.

```php
if(isset($_POST['g-recaptcha-response']))
{
    $secretkey = "6Lc8fBglAAAAAOz5vqCJ9Sl1Y0g2KcNTlwCp0fgY";
    $ip = $_SERVER['REMOTE_ADDR'];
    $response = $_POST['g-recaptcha-response'];
    $url = "https://www.google.com/recaptcha/api/siteverify?secret=$secretkey&response=$response&remoteip=$ip";
    $fire = file_get_contents($url);
    $data = json_decode($fire);
    if($data->success==true){

      if($Rows!=Null && $Rows['UserName']==$uname &&$Rows['Password']==$Pass)
      {
          session_start();
          $_SESSION['uname'] = $uname;
          $_SESSION['Pass'] = $Pass;
          header("Location:SellerProfile.php");
          exit();

      }
      else
      {

        echo "<script>window.alert('Wrong User Name Or Password Try Again');</script>";
      }
      mysqli_close($connection);
    }

    else
    {
        echo '<script>
        alert("Please Enter Captcha!");
        </script>';
    }
}
}
```

Figure 3.23: Code snippet for the reCAPTCHA authentication

3.3.8 UPDATING USER THROUGH NOTIFICATION

We have used the PHP Mailer library, in order to send mail to the users and notify them when someone has bid for a higher amount on the product that is listed, we also notify the buyers when the auction gets over and they are the highest bidder, contact details of the seller are also attached along with the mail.

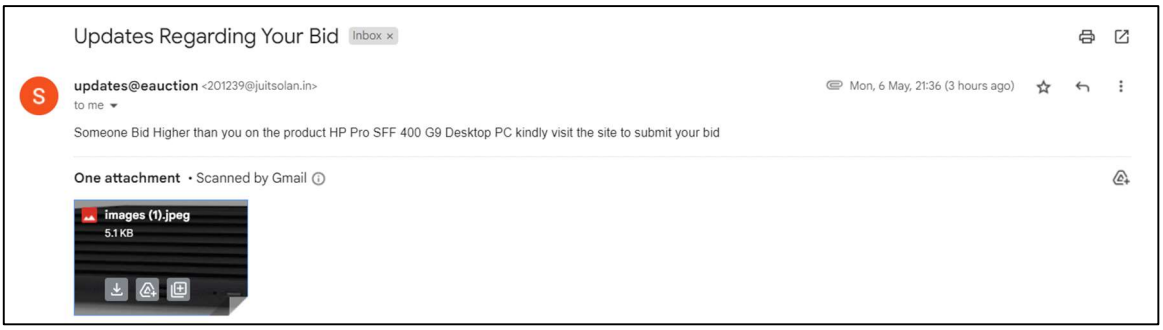


Figure 3.24: Notification received when bid submitted for higher amount

Figure 3.25: Notification received when bidding finished

3.4 KEY CHALLENGES

The key challenges faced during the development process are:

1. **Storage of the Multimedia:** The share of image that was saved locally in the database was not being able to be used at the time of decryption, the sole reason for it was that the names of all the images that were being saved for each user was same, due to which we were not being able to fetch them for the respective user. In order to solve this, we saved the image in the folder by appending it with the Aadhaar number as we had already applied the check in the database to make sure that only unique Aadhaar numbers were saved we were able to handle this issue.

2. **Separate formats of the image:** At the time of encryption, we had saved the image in form of jpeg but when we were superimposing the image then we were creating the resulted image in the form of png this resulted in format mismatch and the hidden text was not being displayed.

3. **Use of API for sending Email:** At the beginning we had used Mailgun API for sending the email to the users, but it proved to be very time consuming, therefore after doing some research we came to the conclusion of using the inbuilt PHPMailer which has the TLS encryption for security and also there is no limit in it for sending the emails.

4. **Bidding of products under sealed bid:** In sealed bid auction, the starting price of the product needed to be displayed, and along with this we were also required to prevent a buyer from submitting more than one bid on a single product, in order to

overcome this, we created a separate table bid in our database which stored the bid submitted for the products under sealed bid category.

CHAPTER 4

TESTING

4.1 TESTING STRATEGY

In order to develop a testing strategy for online auction system, our most important goal is to make sure that the system is reliable and secure. We have defined clear testing objectives that have functional aspects and security measures such as visual cryptography, OTP authentication, AES encryption and overall system performance. This strategy of ours will help us to safeguard the overall auction process and prevent shill bidding, as we have developed them keeping in mind all the possible vulnerabilities which could exploit the system.

We have conducted performance testing to evaluate the performance of our system under different loads, usability testing is also done to understand the overall user experience. We have several checks in built in the system which keep the system in check for particular set of values, we are preventing multiple entries into the database with same user name, email, and phone number. We are also keeping a check on automated bot attacks by using the reCAPTCHA, wherein a user is prompted to login only after verifying the captcha and entering correct user name and password.

4.2 TEST CASES AND OUTCOMES

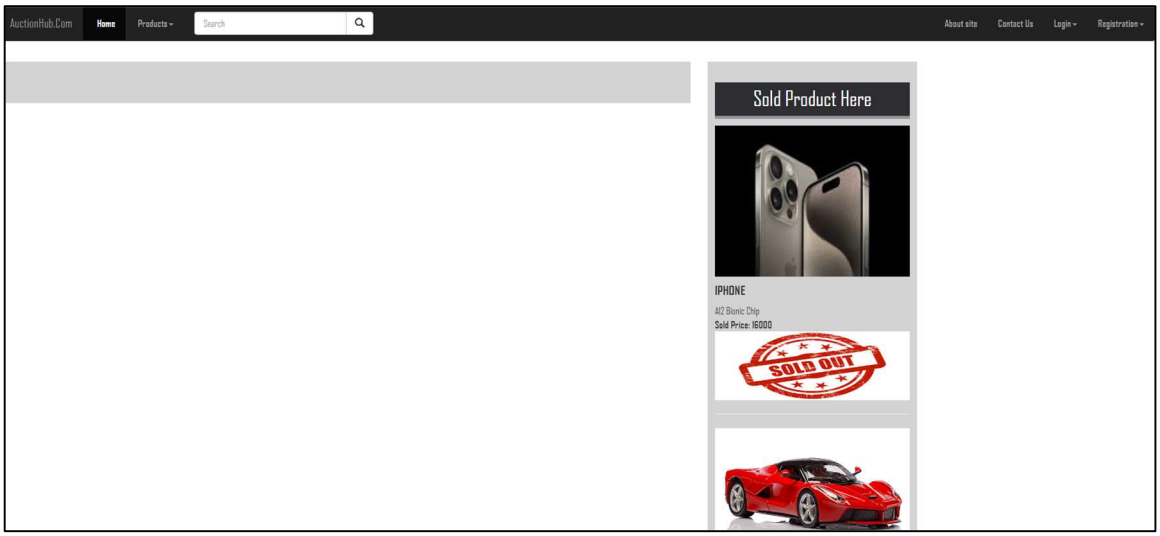


Figure 4.1: Home Page of the website

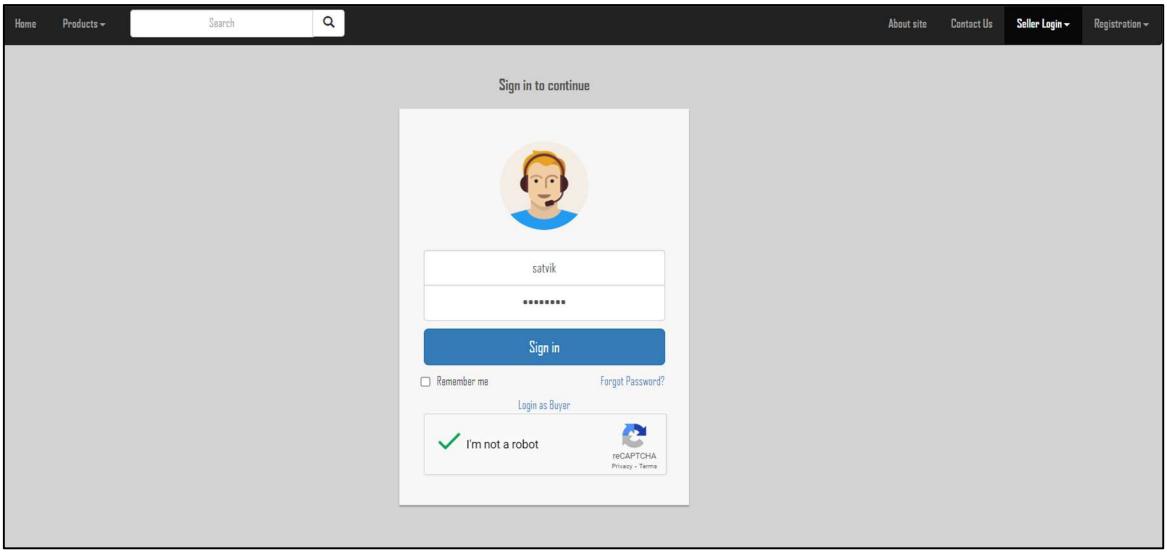


Figure 4.2: Login Page of the seller

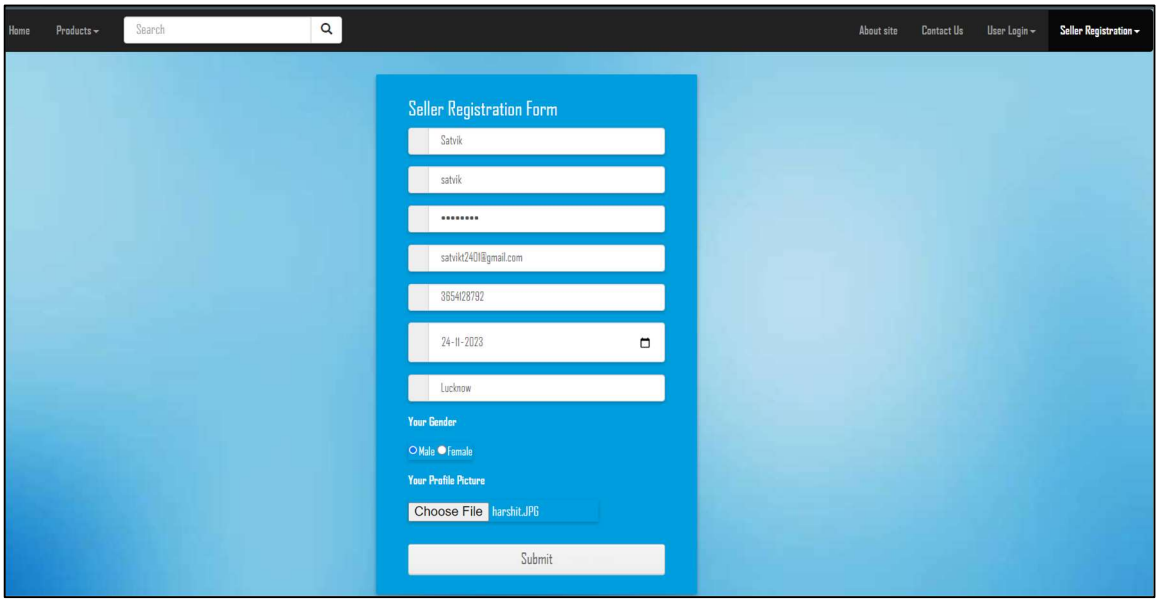
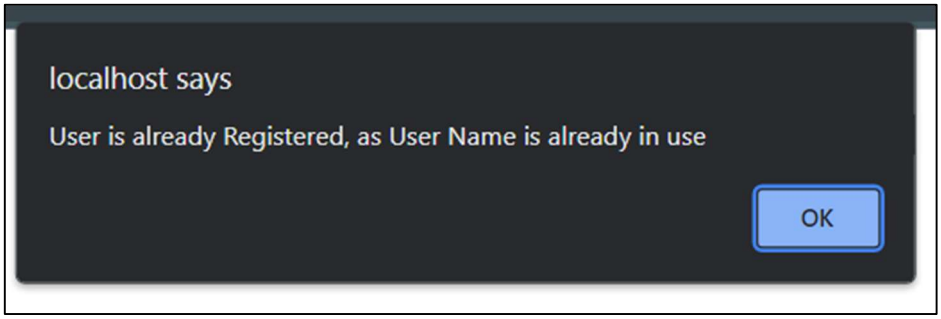


Figure 4.3: Registration Page

+ Options

	UserName	Name	Email	Phone	Password	Gender	DOB	Address	Photo	captcha_text
Edit Copy Delete	rishu02	Prianshu	201239@juitsolan.in	8181016713	$2y$10$ojXqauvTSMN7NxLTXejCOeFH/Er0AJlbabTl1cVKv5k...	Male	2002-07-19	Delhi	UserPhoto/Satvik_Image.jpg	fAx9pJQ=
Edit Copy Delete	satvik02	Satvik	tripathisid24@gmail.com	7376921711	$2y$10$E/XlwY.JS2xfhhLjNPW3aOD.xtJZ59h/IPYsX202AzU...	Male	2002-01-24	H.No 3/12 Vishnupuri Colony	UserPhoto/resize.jpg	fR1q3rY=

Figure 4.4: Details entered on the registration page added into the database



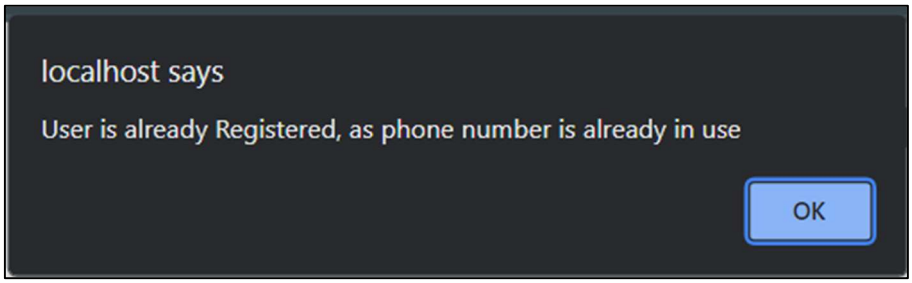


Figure 4.5: Error message displayed when registration happens with repeated credentials

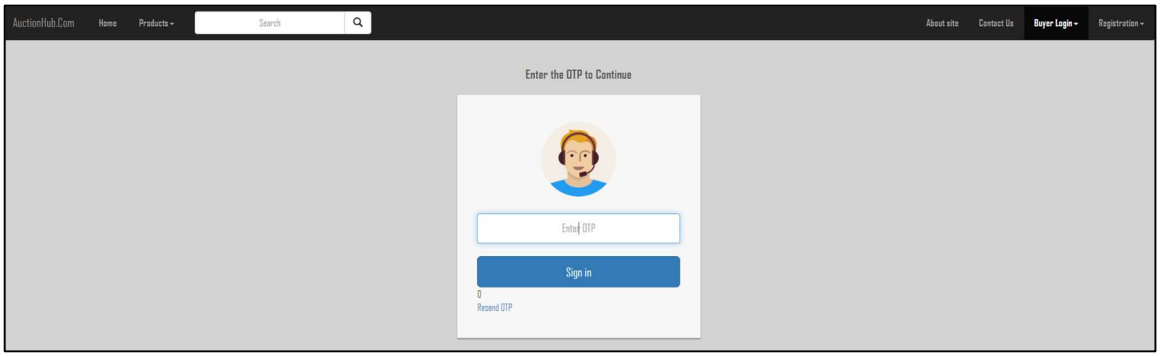


Figure 4.6: OTP Authentication Page

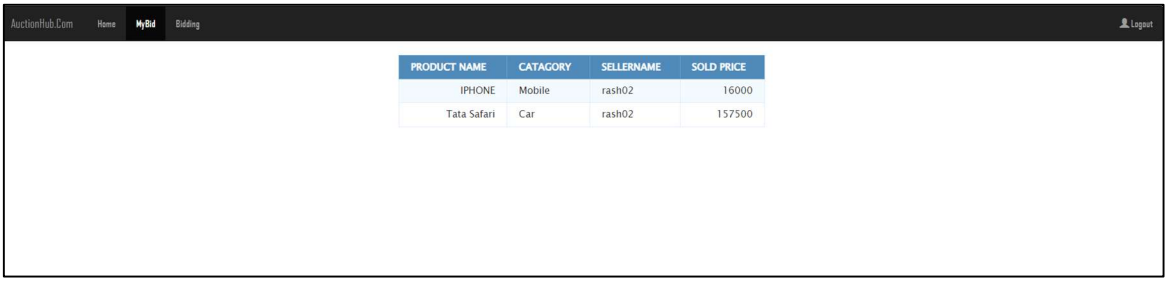


Figure 4.7: My Bid page of the buyer showing details of products won in bidding

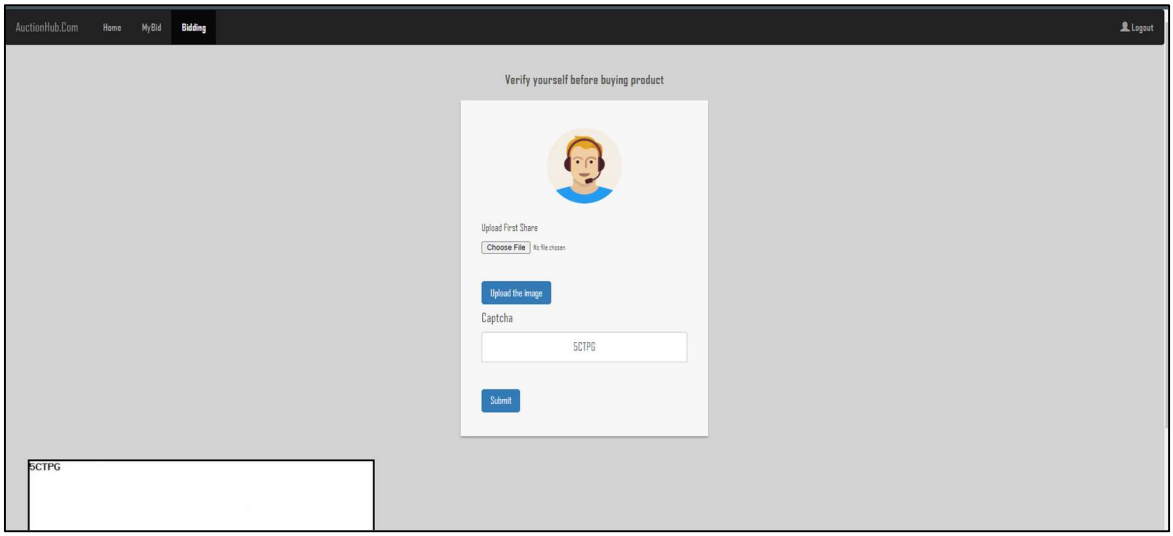


Figure 4.8: Authentication before submitting the bid

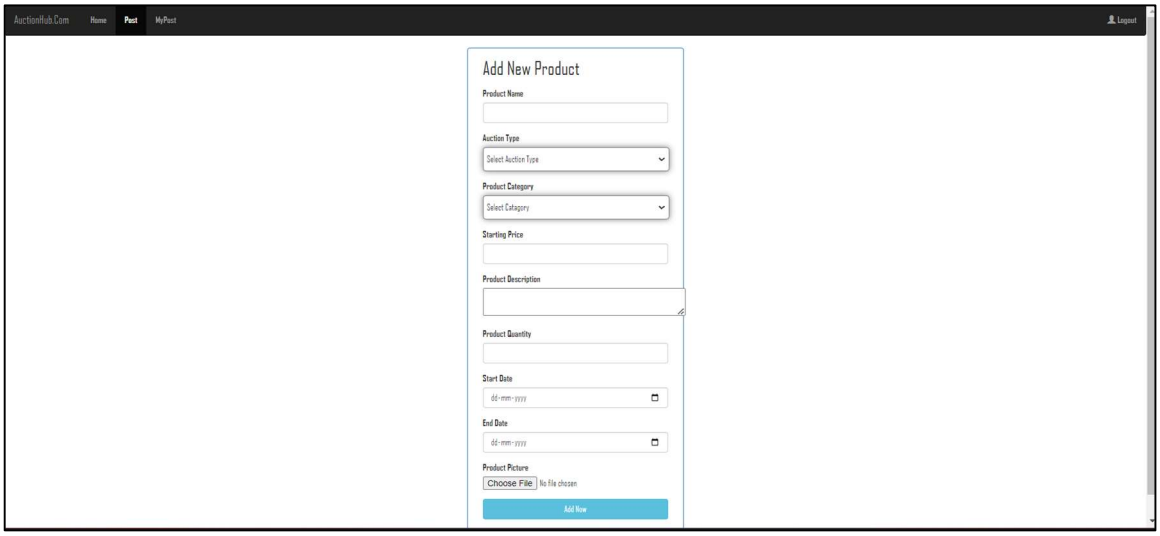


Figure 4.9: Seller's page to add a product for auction

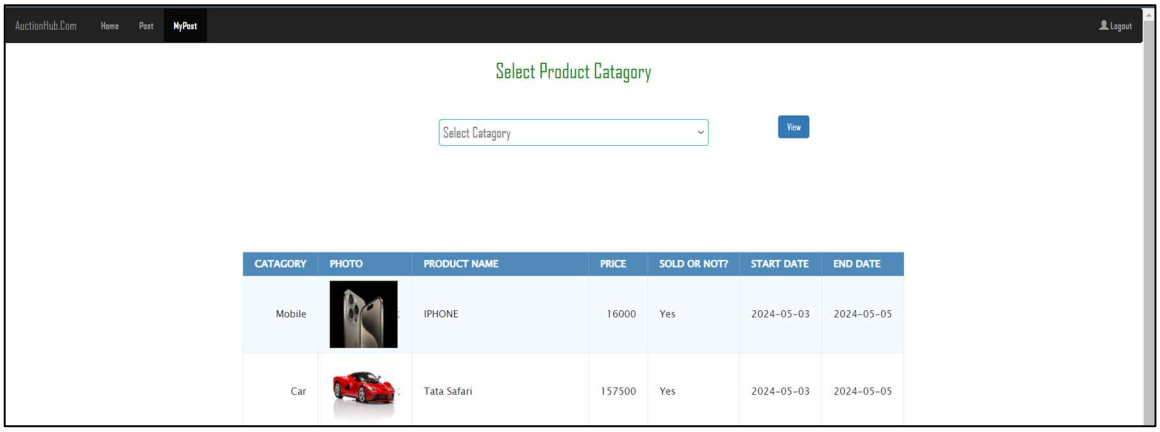


Figure 4.10: My Post page of seller showing details of products posted by them

Figure 4.11: Details of products uploaded under normal bidding

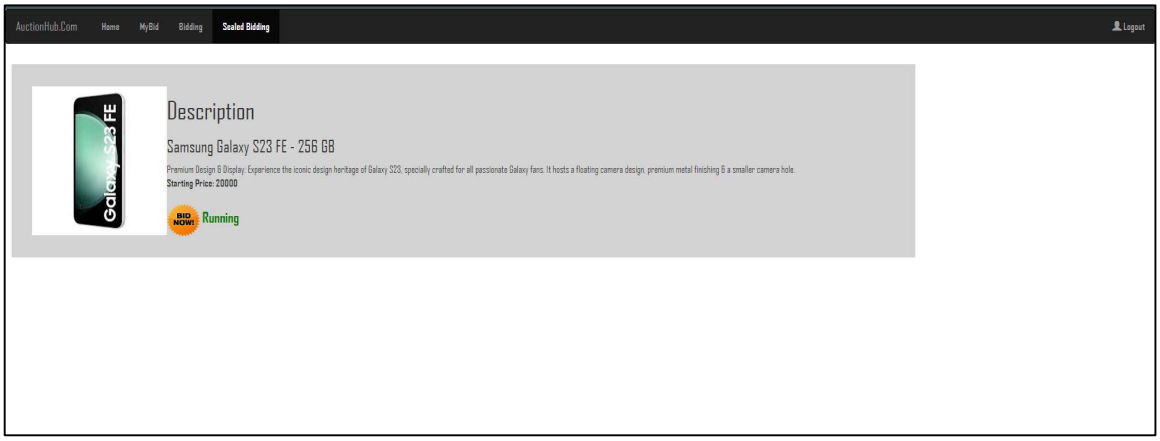


Figure 4.12: Details of products uploaded under sealed bidding

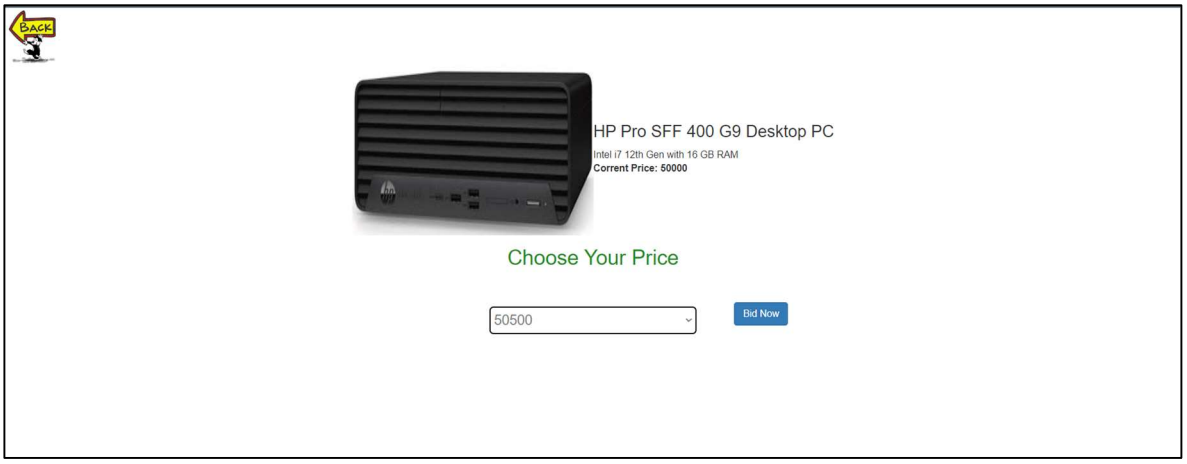


Figure 4.13: Bidding Page

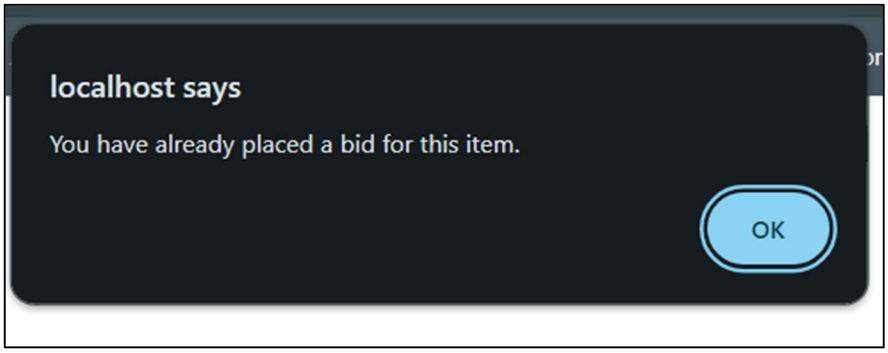
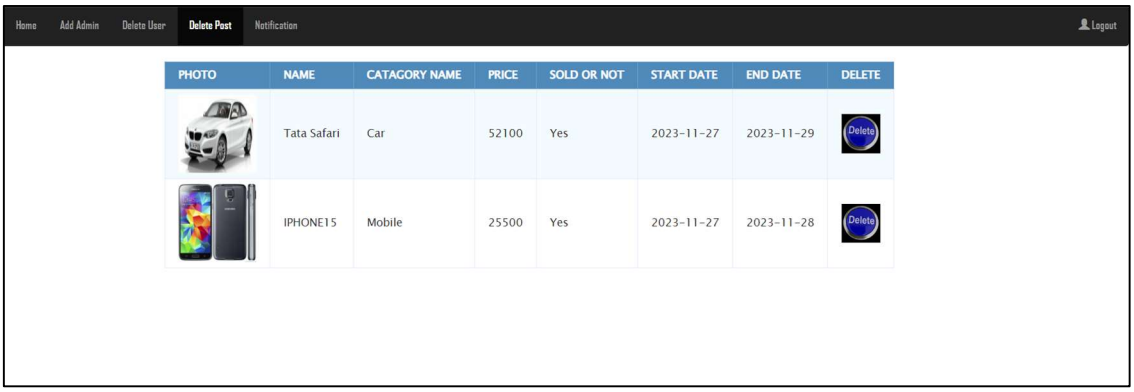


Figure 4.14: Error Message displayed when user tries to submit duplicate bid



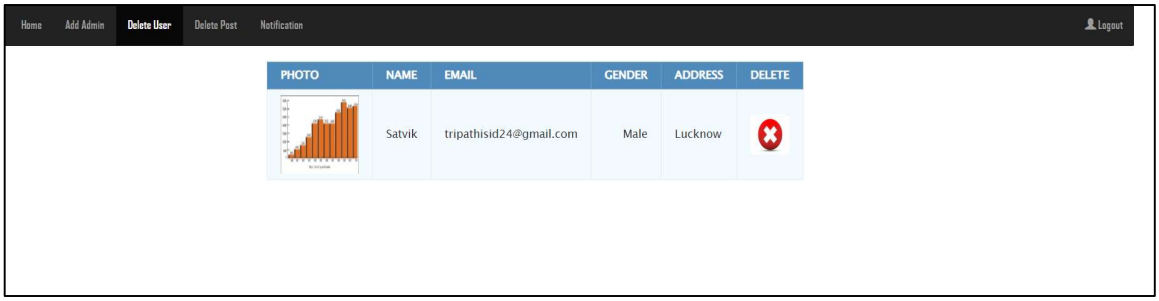


Figure 4.15: Admin Panel

CHAPTER 5

RESULTS AND EVALUATION

5.1 RESULTS

Throughout our project, there were various encryption algorithms and security measures that were used to safeguard the overall auction system and to also increase the experience of the users, these measures have been discussed below:

- **OTP Authentication:** Twilio API was used to authenticate the real users into the system and prevent the fake users from manipulating or influencing the auction in any sense.

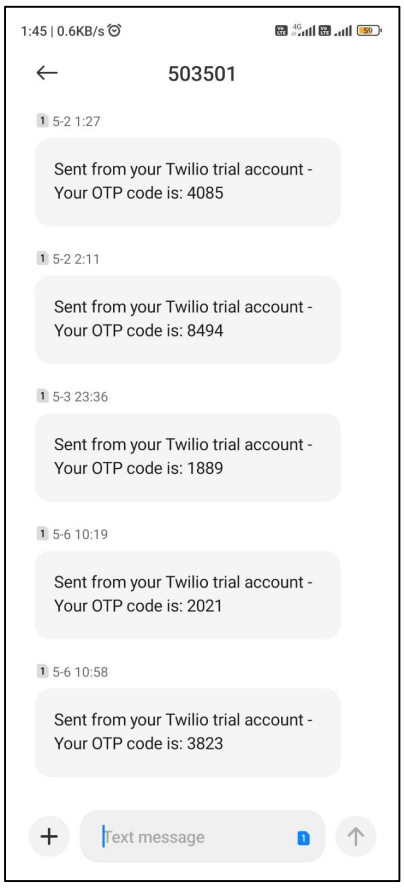


Figure 5.1: OTP received on the mobile number of the user

- **AES Encryption:** We have used the AES encryption algorithm to encrypt the captcha text value before sending it to the database, such that in any case the original text is not leaked or exposed.

+ Options

	UserName	Name	Email	Phone	Password	Gender	DOB	Address	Photo	captcha_text
Edit Copy Delete	rishu02	Prianshu	201239@juitsolan.in	8181016713	$2y$10$ojXqauvTSMN7NxLTXejCOeFH/Er0AJlbabTI1cVKv5k...	Male	2002-07-19	Delhi	UserPhoto/Satvik_Image.jpg	fAx9pJQ=
Edit Copy Delete	satvik02	Satvik	tripathisid24@gmail.com	7376921711	$2y$10$E/XlwY.JS2xfhhLjNPW3aOD.xtJZ59h/IPYsX202AzU...	Male	2002-01-24	H.No 3/12 Vishnupuri Colony	UserPhoto/resize.jpg	fR1q3rY=

Figure 5.2: Table of the user where captcha text is encrypted

- **Visual Cryptography:** The major and most integral encryption algorithm that was used was the visual cryptography, and in order to the make this successful the main part was to send the email to the user containing the first share of the image as an attachment that will further be used in the auction process.

Figure 5.3: Share 1 received on the Email of the user

- **Bcrypt Hashing:** We used this cryptographic hashing algorithm in order to convert the passwords in the form of a hash and then save them into the database, this helped us to stop any unauthorized user from entering our system and also in preventing any form of data breach. Bcrypt uses an adaptive hashing algorithm due to which it takes a larger amount of time in generating hash and thus hackers find it difficult to hack the passwords using brute force attacks.

- **RSA Encryption:** In order to successfully conduct the sealed bid auctions, we have taken the help of RSA algorithm for maintaining the secrecy of the bids, because in these types of auctions the price of the product does not change with time, but the bids allowed to be submitted for a certain time duration and in that duration the person with the highest bidding price is declared as winner.
  In order to achieve this, we have also created a separate table in our database in which the bids of each buyer are stored so that user cannot submit their bid for more than one time for a single product, and we have also made sure that the user is able to submit their bid above the starting price.

  Sealed-bid auctions are often used for government contracts; each potential contractor tries to offer the best (lowest) price to win the contract. They can also be used in real estate; in which case the highest bid is likely to be the winner. A sealed-bid auction benefits sellers because buyers are encouraged to offer their best bid immediately, rather than improving their offer slowly in response to how others bid [23].

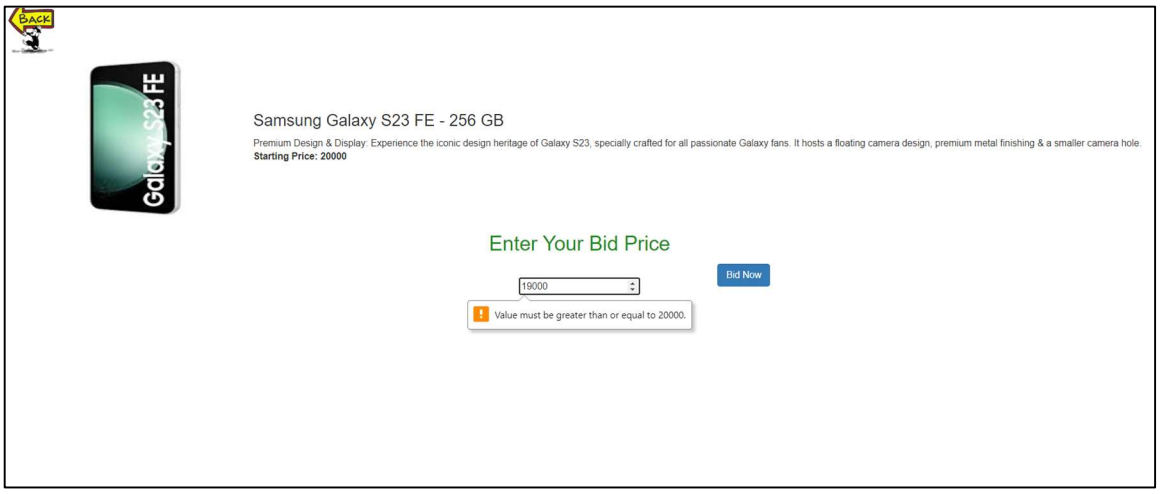


Figure 5.4: Sealed Bidding Page

- **Admin Panel:** Administrator is a professional authorized to manage the website and look after its operations and working. We have also created a separate admin panel wherein admin can delete suspicious users and fake posts listed on the website, this

helps in saving resources and time of the seller and also helps in ensuring the smooth operation, security, and growth of the website.

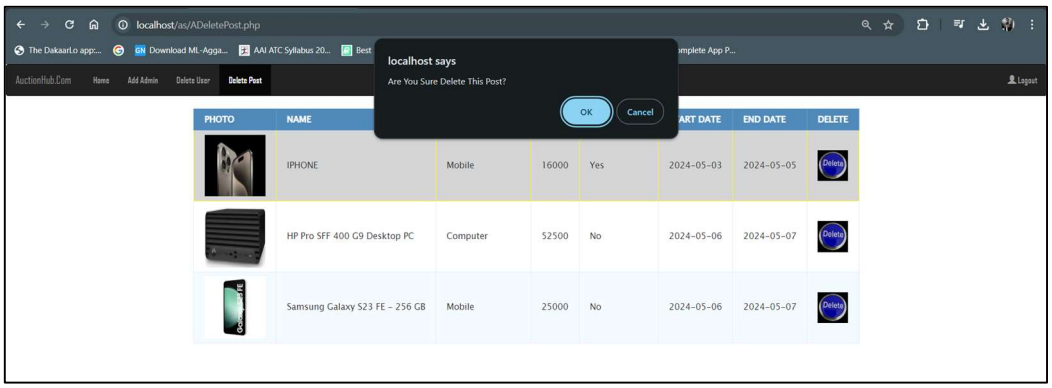


Figure 5.5: Admin page to delete a product

CHAPTER 6

CONCLUSIONS AND FUTURE SCOPE

6.1 CONCLUSION

In conclusion, the development and implementation of a secure online auction system represented a complex task, which required us to be careful to various security concerns. The use of security features such as visual cryptography, AES-128, multi factor authentication helped us to preserve the privacy of the users, thus protecting the system from the malicious activities.

By implementing the visual cryptography, we were able to encrypt the captcha text without any complexities and thus being able to separate the legit users from the illegitimate one. The integration of OTP mechanism also added an additional layer of security providing more security to the data of the user, we faced several changes in maintaining the lifecycle of the OTP but we were able to successfully overcome them.

Furthermore, by implementing the AES we were able to secure the randomly generated captcha text. While these security measures were able to foster the performance and security of the auction system, but we need to acknowledge the fact that the landscape of cybersecurity is very dynamic. In order maintain the security of our system over time, we need to stay updated on the regular updates taking place and also need to monitor it regularly.

6.2 FUTURE SCOPE

Some potential areas for future development where we need to work in future are as follows:

1. **Enhanced User Experience:** We can further use the Bootstrap to enhance the overall experience of the website thus making it more attractive and user friendly.

2. **Emphasizing on product delivery:** We can improve the accessibility for the users by directly providing the option of product delivery on the website through which sellers can send the products from their home and the buyers can receive them at the ease of their homes, without having the need to go anywhere.

3. **Regulatory Compliance:** We also need to stay updated with evolving regulations related to online auctions, especially regarding data protection and consumer rights, to ensure full compliance and build trust among users.

REFERENCES

1. M. Hasanuzzaman, A. Nabil, E. Nahid, M. Rahaman, M.Uddin, “Implementation of Online Shopping and Auction System (SPAROO)", International Research Journal of Engineering and Technology, VOL. 9, November 2022

2. S. Pethe, H. Munshi, A. Polekar, S. Sabnis, “Let’s Bid: A Web Application for Online Auctions", International Journal for Research in Applied Science & Engineering Technology, VOL. 10, April 2022

3. S. Tan, S. Heng, “Secure Cryptographic E-Auction System", International Journal of Technology, VOL. 9, August 2022

4. D. Anand, “Implementation of Online E –Auction to Overcome the Problem of Corruption with Effective and Efficient Procurement with Transparency", Turkish Journal of Computer and Mathematics Education, VOL. 12, April 2021

5. J. N. S. Lakshmi, A. N. Ramamani, “Online Bidding System", Journal of Emerging Technologies and Innovative Research, VOL. 7, May 2020

6. Y. Shah, R. Rane, S. Kharade, R. Patil, “Analysis of AES and DES algorithm”, International Journal of Trend in Research and Development, Vol. 2 April 2020.

7. R. Suhas, “An Agent based Approach to Secure Real Time Auction System using Trust Management Module with Image Encryption", International Journal of Engineering Research & Technology, VOL. 3, February 2015

8. V. Borkar, M. Dave, R. Shyamasundar, “Design and Implementation of SeTiA: Secure Multi Auction System", Journal of Intelligent Systems, VOL. 14, September 2005

9. S. Khan, Zeeshan, “Advanced and Secure Online Web-Based Auction System", International Journal of Computer, VOL. 43, May 2022

10. J. Trevathan, W. Read, “Cryptographic Online Auction Schemes", IASK International Conference E-Activity and Leading Technologies, VOL. 13, December 2008

11. Z. Guo, Y. Fu, C. Cao, “Secure first-price sealed-bid auction scheme", EURASIP Journal on Information Security, VOL. 16, November 2017

12. "Visual Cryptography," geeksforgeeks.org. https://www.geeksforgeeks.org/visual-cryptography-introduction/ (accessed Aug. 20, 2023)

13. "Different types of auctions" ClarityVentures.com. https://www.clarity-ventures.com /auction-ecommerce/types-of-auctions-in-ecommerce (accessed Aug. 22, 2023)

14. "Difference between AES and DES Ciphers" Tutorialspoint.com https://www.tutorialspoint.com/difference-between-aes-and-des-ciphers (accessed Aug. 25, 2023)

15. "What is AES Encryption and how does it work" Simplilearn.com. https://www.simplilearn.com/aes-encryption (accessed Aug. 30, 2023)

16. "Flowchart Maker," Lucidchart.com. https://www.lucidchart.com/pages/examples/flowchart-maker (accessed Sep. 10, 2023)

17. "Get started with Bootstrap" Bootstrap.com. https://getbootstrap.com/docs/5.3/getting-started/introduction/ (accessed Sep. 15, 2023)

18. "XAMPP Tutorial" javatpoint.com https://www.javatpoint.com/xampp (accessed Sep. 25, 2023)

19. "reCAPTCHA" Google.com. https://www.google.com/recaptcha/admin/site/ 62236 1660 (accessed Oct. 1, 2023)

20. "Console|Twilio" Twilio.com. https://console.twilio.com/?frameUr=%2Fconsole%3Fx-target-region%3Dus1 (accessed Oct. 10, 2023)

21. "How to send Emails in PHP Using PHPMailer Library" Cloudways.com. https://www.cloudways.com/blog/send-emails-in-php-using-phpmailer/ (accessed Oct. 26, 2023)

22. "GD - Manual" Php.net. https://www.php.net/manual/en/book.image.php (accessed Nov. 1, 2023)

23. "Sealed-Bid Auction: Definition and how it works in real life" Investopedia.com https://www.investopedia.com/sealed-bid-auction.asp (accessed Feb. 15, 2024)

24. "What is bcrypt and how does it work?" NordVPN.com https ://nord vpn.com /blog /what-is-bcrypt/ (accessed March 20,2024)

25. "What is the RSA algorithm?" Techtarget.com https://www.techtarget.com/ search security/definition/RSA

APPENDIX

Rashik_Report

ORIGINALITY REPORT

17%	16%	6%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.coursehero.com Internet Source	4%
2	nordvpn.com Internet Source	2%
3	searchsecurity.techtarget.com Internet Source	2%
4	doaj.org Internet Source	1%
5	www.ijraset.com Internet Source	1%
6	sersc.org Internet Source	1%
7	www.techtarget.com Internet Source	1%
8	dev.to Internet Source	1%
9	www.jetir.org Internet Source	1%