Dissertation on

Zero Knowledge Proof for Online Auctions

Submitted in partial fulfilment of the requirements for the award of degree of

Bachelor of Technology
in
Computer Science & Engineering

UE17CS490B – Capstone Project Phase - 2

Submitted by:

ADITYA MURALEEDHARAN NAIR	**PES1201802187**
NISHA NEMASING RATHOD	**PES1201701672**

Under the guidance of

Rajashree S
Assistant Professor
PES University

January - May 2021

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
FACULTY OF ENGINEERING
PES UNIVERSITY
(Established under Karnataka Act No. 16 of 2013)
100ft Ring Road, Bengaluru – 560 085, Karnataka, India

PES UNIVERSITY

(Established under Karnataka Act No. 16 of 2013)
100ft Ring Road, Bengaluru – 560 085, Karnataka, India

FACULTY OF ENGINEERING

CERTIFICATE

This is to certify that the dissertation entitled

Zero Knowledge Proof for Online Auctions

is a bonafide work carried out by

ADITYA MURALEEDHARAN NAIR	**PES1201802187**
NISHA NEMASING RATHOD	**PES1201701672**

in partial fulfilment for the completion of eighth semester Capstone Project Phase - 2 (UE17CS490B) in the Program of Study - Bachelor of Technology in Computer Science and Engineering under rules and regulations of PES University, Bengaluru during the period Jan. 2021 – May. 2021. It is certified that all corrections / suggestions indicated for internal assessment have been incorporated in the report. The dissertation has been approved as it satisfies the 8th semester academic requirements in respect of project work.

Signature Rajashree S **Assistant Professor**	Signature Dr. Shylaja S S **Chairperson**	Signature Dr. B K Keshavan **Dean of Faculty**

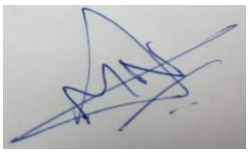
External Viva

Name of the Examiners	**Signature with Date**
1.	
2.	

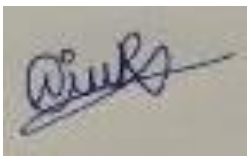
DECLARATION

We hereby declare that the Capstone Project Phase - 2 entitled **Zero Knowledge Proof for Online Auctions** has been carried out by us under the guidance of Rajashree S, Assistant Professor and submitted in partial fulfilment of the course requirements for the award of degree of **Bachelor of Technology** in **Computer Science and Engineering** of **PES University, Bengaluru** during the academic semester January – May 2021. The matter embodied in this report has not been submitted to any other university or institution for the award of any degree.

ADITYA MURALEEDHARAN NAIR **PES1201802187**



NISHA NEMASING RATHOD **PES1201701672**



ACKNOWLEDGEMENT

We would like to express our gratitude to Prof. Rajashree S, Department of Computer Science and Engineering, PES University, for her continuous guidance, assistance, and encouragement throughout the development of this UE17CS490B - Capstone Project Phase – 2.

We are grateful to the project coordinators, Prof. Silviya Nancy J and Prof. Sunitha R for organizing, managing, and helping with the entire process.

We take this opportunity to thank Dr. Shylaja S S, Chairperson, Department of Computer Science and Engineering, PES University, for all the knowledge and support we have received from the department. We would like to thank Dr. B.K. Keshavan, Dean of Faculty, PES University for his help.

We are deeply grateful to Dr. M. R. Doreswamy, Chancellor, PES University, Prof. Jawahar Doreswamy, Pro Chancellor – PES University, Dr. Suryaprasad J, Vice-Chancellor, PES University for providing us various opportunities and enlightenment every step of the way. Finally, this project could not have been completed without the continual support and encouragement we have received from our family and friends.

ABSTRACT

Cryptography is a field of security which deals with the encryption of data in order to ensure Confidentiality, Integrity and Availability (CIA) triad. Authentication and non-repudiation are other factors which are also essential for data security.

In order for the data to be securely transmitted strong cryptographic algorithms such as RSA, DSA, Diffie-Hellman etc. are used. Modern cryptographic mechanisms allow us to achieve the security, privacy and confidentiality aspects of online auctions. One such cryptographic mechanism is called Zero Knowledge Proof.

Zero Knowledge Proof is a special algorithm which ensures the data integrity by letting the truth be known to the verifier (receiver) without the prover (sender) revealing all the confidential information. Our project aims at utilizing this mechanism in order to ensure transparency and privacy in data transmission.

In an online auction, multiple buyers and sellers from across the world participate in the bidding process via the internet. However, the security feature is at risk if each of these buyers and sellers are not carefully monitored. Therefore, Zero Knowledge Proof (ZKP) Protocol provides a solution by using entity authentication and anonymity to ensure that the users participate in the bidding process without revealing their profile information.

TABLE OF CONTENTS

Chapter No.	Title	Page No.
1.	INTRODUCTION	8
2.	PROBLEM STATEMENT	9
3.	LITERATURE SURVEY	10
4.	PROJECT REQUIREMENTS SPECIFICATION	30
5.	SYSTEM REQUIREMENTS SPECIFICATION	31
6.	SYSTEM DESIGN	34
7.	IMPLEMENTATION AND PSEUDOCODE	36
8.	PROJECT DEMONSTRATION	38
9.	TEST PLAN AND STRATEGY	49
10.	RESULTS AND DISCUSSION	50
11.	CAPSTONE PROJECT TIMELINE (PHASE-1 & PHASE-2)	53
12.	CONCLUSION OF CAPSTONE PROJECT PHASE-1	54
13.	CONCLUSION OF CAPSTONE PROJECT PHASE-2	55
14.	FUTURE WORK	56
15.	REFERENCES/ BIBLIOGRAPHY	57
16.	APPENDIX A: DEFINITIONS AND ABBREVIATIONS	59

LIST OF FIGURES

Figure No.	Title	Page No.
1	Online Auction System Design	35

LIST OF TABLES

Figure No.	Title	Page No.
1	Summarization of Literature Survey	29
2	Capstone Project Testing	49
3	Capstone Project Timeline (Phase-1 & Phase-2)	53

CHAPTER 1

INTRODUCTION

Modern technologies are reshaping the world by promoting less human dependency and efficiency in terms of reduced manual work flow. However, these modern technologies challenge the three important facets of data i.e., confidentiality, integrity and security.

Traditional auctions which take place around the world involves the auctioneers and bidders to be present at a physical place. However, with the digitization aspect put in place online auctions are also becoming prominent. The concept of security, privacy and confidentiality is very essential in this domain.

Modern cryptographic mechanisms allow us to achieve the security, privacy and confidentiality aspects of online auctions. One such cryptographic mechanism is called Zero Knowledge Proof. Zero Knowledge Proof (ZKP) is a special algorithm which ensures the data integrity by letting the truth be known to the verifier (receiver) without the prover (sender) revealing all the confidential information.

The project design and implementation are inspired from eBay website. The project will focus on secure online bidding in terms of ensuring two primary factors i.e., entity authentication and anonymity. Entity authentication is the process of ensuring the identity of the two parties i.e., verifier and claimant in protocol participation. User anonymity is a feature in which the users participating in the bidding process are anonymous i.e., their profile information is hidden.

This study is motivated by the need to:
1. Implement ZKP Protocol which will ensure a fair and privacy-preserving e-auction between both the participants i.e., buyers and sellers.
2. Authenticate bidders and sellers against malicious and unauthorized adversaries.

BACK TO INDEX

CHAPTER 2

PROBLEM STATEMENT

Our project aims at utilizing Zero-Knowledge Proof mechanism in order to ensure transparency and privacy during data transmission. The purpose of our project is **authenticating bidders and sellers of auctions against unauthorized/malicious adversaries.**

The scope of the project is to create a secure online auction platform by implementing the ZKP protocol using Simple Certificate Enrollment Protocol (SCEP) curve.

BACK TO INDEX

CHAPTER 3

LITERATURE SURVEY

This chapter briefly elucidates the research papers published by different authors which provide an insight about the Zero-Knowledge Proof mechanism in online auctions.

3.1 A protocol for verification of an auction without revealing bid values

Authors: Ben Palmer, Kris Bubendorfer, Ian Welch, 2012

The role of online auctions will be significant for computational resources allocation. This can be achieved by addressing two primary issues:

1. Appropriate usage of auction model.
2. The security parameters must be addressed.

The primary focus of auction security involved privacy in terms of preserving the bidding information against multiple parties including the auctioneer.

However, the existing protocols avoids attacks pertaining to privacy-preserving combinatorial auctions such as misrepresentation of bids, removal of valid bids, unfair manipulation of auctions.

This paper focuses on addressing such attacks by implementing a privacy preserving combinatorial auction protocol while maintaining the bids secrecy. This was achieved with the help of Zero Knowledge Proof in which auction verification and result calculation took place simultaneously. In order to implement Zero Knowledge Proof homomorphic auction protocol was used.

The verification protocol was implemented with the help of two well-known ZKP's:

1. Proof of Equality of discrete logarithms and encryption is based on the proof that it can be decrypted into one of two values.
2. In order to implement non-interactive ZKP proofs for random oracle model Fiat-Shamir heuristic and SHA512 hash function was used.

Non-interactive proofs is a proof which can be published by the auctioneer with the absence of interaction with other auctioneers for result verification.

The verification protocol includes threat model, verifiable threshold El-Gamal Decryption, Verifying Shift and Randomize.

The homomorphic auction protocol has an overhead which is added by the verification protocol.

The no. of malicious auctioneers is less than a given threshold. Thus, losing of bid values are kept a secret in order to provide confidence to the participants in the auction result. The security parameter is ensured by transforming the auction protocol into a privacy preserving, verifiable and combinatorial protocol with the addition of verification protocol. This robust protocol can increase the confidence of the participants in the auction result by detecting and eliminating invalid bids or malicious auctioneers.

Limitation:

The allocation of resources for individual tasks is expensive.

3.2 Zero knowledge proofs applied to auctions

Authors: Luiz Thomaz do Nascimento, Sapna Kumari, Vedavinayagam Ganesan, 2019

This project involves ZKP application in online auctions transactions. The goal is to ensure data transparency and privacy in governmental auctions settings.

The reverse auction methods are commonly used in procurement processes by governments. The typical requirements in such public auctions are:

1. Fairness
2. Confidentiality
3. Anonymity

Zero knowledge proof properties play an important role in online public auctions. The proposed solution for the project is to design a proof system that utilizes zero knowledge proofs for demonstration of winning bid selection based on the rules defined without leaking any confidential information. The following are the main steps for the work flow solution:

1. Auction Initiation
2. Bid Commitments
3. Opening Bids
4. Proof Generation
5. Proof Verification

They have made use of Bulletproof system which allows interactive proof design to be transformed into a non-interactive proof system, NIZK, by using Fiat-Shamir heuristic. Finally, bulletproofs rely on Pedersen commitments to hide the secret inputs and provide computational integrity check.

In order to build the prototype of this project, they experimented with two Bulletproofs implementations. The first one is called **Hyrax** which is actually a doubly-efficient zk-SNARK implementation that contains code for Bulletproofs as well.

The code was developed and maintained by Riad S. Wahby. **BulletproofLib** is the other implementation developed by Benedikt Bünz.

As stated in the paper the workflow of the reverse auction setting is:

1. Setup phase
2. Bidding phase
3. Proof phase
4. Verification phase

They have implemented ZKP and designed a proof system to generate transparency alongside privacy in online auctions. This cryptographic construction is very fascinating as it enables us to put together the two contrasting objectives of privacy and transparency.

As transparency in public reverse auctions is a big concern and addressing it properly can bring several benefits to the society, there are several zero-knowledge proofs cryptographic constructions that can be used in this problem. Thus, they have made use of Bulletproof construction, which represents a good trade-off between the security assumption and performance of the proof system.

Limitation:
It assumes that every bidder knows all the bidding commitments from all other bidders. If not then it can be shown as fake even though it isn't fake.

3.3 Verifiable Sealed-Bid Auction on the Ethereum Blockchain

Authors: Hisham S. Galal and Amr M. Youssef, 2018

In this paper, they tackle the challenge which is, 'many individuals are not willing to reveal their financial transactions to the public' and present an auction smart contract that utilizes a set of cryptographic primitives to guarantee the following attributes:

1. Bid privacy
2. Posterior privacy
3. Bid binding
4. Public verifiable correctness
5. Financial fairness
6. Non-interactivity

The primitives that are utilized in this design of their proposed protocol are:

1. Addition operation supported by homomorphic commitment scheme on the underlying values.
2. Zero-knowledge proof of interval membership x 2 [0;B].

The proposed interval membership ZKP protocol runs as follows:

1. Commit
2. Challenge
3. Response

The phases included during the interaction between the bidders, the auctioneer, and the auction contract are:

Phase 1: Contract Deployment and Parameters Setup

Phase 2: Commitment of Bids

Phase 3: Opening the Commitments

Phase 4: Verification of Comparison Proofs

To achieve this, they have made use of non-interactive interval membership ZKP, where we can see these steps: Commit, Challenge and Response

Phase 5: Finalizing the Auction

A smart contract for a verifiable sealed-bid auction on the Ethereum blockchain is presented in this paper. The underlying protocol is created by using Pedersen commitment scheme along with ZKP of interval membership. The bid privacy is maintained by the auction contract so that bidders do not learn any information about the other bids when they commit.

In order to verify the proofs claimed by the auctioneer, the auction contract also exhibits the public verifiable correctness for winner determination.

There is no need for a complex interaction from the bidders other than submitting and revealing the commitments to their bids.

If the payment for winning bid is received aside from blockchain it is possible to easily modify the proposed protocol to ensure full bid privacy including the winner's bid.

3.4 Efficient Adaptively Secure Zero-knowledge from Garbled Circuits

Authors: Chaya Ganesh,Yashvanth Kondi, Arpita Patra and Pratik Sarkar, 2018

The primary contribution of this work involves efficient UC-secure constant round ZK protocols construction from garbled circuits. They are secure against adaptive corruptions due to linear communication according to the size of the statement.

They begin by showing that the practically efficient ZK protocol of Jawurek et al. The underlying Oblivious Transfer (OT) is satisfied by a mild adaptive security guarantee thus making CCS 2013 adaptively secure.

In order to obtain a three-round adaptively secure zero knowledge argument in the Non-Programmable Random Oracle Model (NPROM) conditional verification technique is used.

The contributions in this paper are as listed below:

1. Efficient Constant-round Adaptively Secure ZK Protocols.
2. Round Zero-Knowledge Proofs.

The algorithm used is ZKGC (Zero Knowledge Garbled Circuit) protocol.

Findings:

1. RE-OT Initiation (receiver equivocal oblivious transfer).
2. It uses MPC-in-the-head approach.
3. It uses CRS (common reference string) for SNARKs.
4. It uses ROM (random oracle model).

3.5 Secure Sealed-Bid Online Auctions Using Discrete Cryptographic Proofs

Authors: Jose A. Montenegro, Michael J. Fischer, Javier Lopez, Rene Peralta, 2011

The auction system design and implementation in a secure multiparty computation is described in this work.

It is a privacy-preserving protocol in which either the auctioneer or other bidders are not provided with information about losing bids due to which the winning bid is determined.

They have proposed the development of a *Proof Certificate* standard which convey sufficient information to recreate the cryptographic proofs and verify them offline.

The following algorithms are used:

1. Development of a Proof-Certificate standard.
2. Enabling secure multiparty communication (SMC).
3. It uses Public-Key cryptography.

3.6 Efficient Privacy-Preserving Protocols for Multi-unit Auctions

Authors: Felix Brandt and Tuomas Sandholm, 2005

The bidders jointly compute the auctions without the help of third parties due to the proposed privacy-preserving protocols.

In the case of marginal decreasing valuation function, the three common types of multi-unit auctions considered are uniform-price, discriminatory, and generalized Vickery auctions.

The distributed homomorphic encryption is the basis for their protocols which is executed in a small number of constant rounds in the random oracle model.

The assumption in decisional Diffie-Hellman states that security merely relies on computational intractability.

The following algorithms are used:

1. Any homomorphic encryption schemes.
2. Zero-knowledge random oracle model is obtained.

Findings:

1. It uses El-Gamal encryption.
2. Σ-protocols are used.
3. Fiat-Shamir heuristic is used to make ZK non-interactive.

Limitations:

1. The assumption is made that privacy can’t be breached (unless all bidders collude).
2. In order to compute with the price units, the bidder must continue even though he wants to quit.

3.7 Cryptographically Secure Multiparty Computation and Distributed Auctions Using Homomorphic Encryption

Authors: Anunay Kulshrestha, Akshay Rampuria, Matthew Denton and Ashwin Sreenivas, 2017

A robust framework is introduced in order to allow secure multiparty computations cryptographically such as distributed private value auctions.

In order to guarantee security, there are certain factors considered such as two-sided authentication for all network connections, homomorphic encryption of bids, and the publication of zero-knowledge proofs for every computation.

The information broadcasted on the network by each individual bidder is used by a non-participant verifier for result verification for any such computation.

The aim of this paper involves library theory and implementation along with guidelines pertaining to the detailed usage and creation of secure special-purpose protocols.

Their framework employs four types of zero knowledge proofs. Each step in the secure fully-private protocols are verified by these proofs.

This paper presents techniques used in the design and running of large auctions such as spectrum allocation, natural resources auction, etc. that are subject to oversight by third-party verifiers. The integrity and secrecy of all losing bids are ensured in order to protect the private interests of bidding parties:

1. The Bitcoin wallet address is provided by every bidder while signing up for the auction. The wallet address is also provided by the seller while joining the auction. A simple Bitcoin script is used to ensure funds transfer from the winner to the seller after ending of the auction. The unification of the private keys used by Bitcoin and auction protocol will greatly benefit the system.

2. The proposed library which is portable to mobile devices can be implemented for the building of voting mechanisms and group decision protocols that can run as individual applications. Veto voting as described by Brandt is an example of one such group decision protocol.

3. The elimination of a random trusted third party for certificate distribution to the bidders prior to auctions is achieved using distributed hash table (or ledger).

The following algorithms are used:

1. Non-Interactive Zero Knowledge Proofs using Fiat–Shamir Heuristic. In order to flatten the proofs and eliminate the need for random challenges Fiat–Shamir Heuristic is used. The network traffic and latency are significantly cut down due to non-interactivity making the proofs non-malleable and secure against attacks.
2. Throughout the proofs, they have used a cryptographic hash function (like SHA-256) to emulate the access to a random oracle that is required by Fiat–Shamir heuristic.

Findings:

1. The framework uses El Gamal Cryptosystem, which is probabilistic and homomorphic.
2. It uses distributed El Gamal Encryption. The distribution of encryption and decryption across multiple nodes in which the decryption of no single node or group of nodes is possible without cooperation from every node is a useful property of El Gamal.

Uses:

1. Proof of Knowledge of a Discrete Logarithm.
2. Proof of Equality of Two Discrete Logarithms.
3. Proof that an encrypted value is one out of the two values.
4. Verifiable secret shuffle of ciphertexts.
5. Counting boolean disjunctions of literals.
6. Negations, disjunctions, exclusive disjunctions.
7. Count operator.

The network code makes use of Google's gRPC and protobuf implementations for establishing connections and securely and reliably distributing data.

Auction Protocols:

1. Public key generation
2. Bid encryption
3. Outcome computation
4. Joint decryption
5. Determine winner

3.8 Optimal Bidding in Online Auctions

Authors: Dimitris Bertsimas, Jeffrey Hawkins, Georgia Perakis, 2002

The objective of this paper is the determination of optimal bidding policy by constructing algorithms for a given utility function in case of a single item and multiple items for multiple simultaneous or overlapping online auctions.

In order to explain their modeling choices, they require that their build for optimal bidding for a potential buyer, called the agent, satisfies the following requirements:

1. It captures the essential characteristics of online auctions.
2. It leads to computationally feasible algorithm that is directly usable by bidders.
3. The parameters for the model can be estimated from publicly available data.

To achieve their goals, they have taken an optimization, as opposed to a game theoretic approach. The major reason is the requirement of an algorithm which is computationally feasible and directly applicable by bidders based on a given data.

Furthermore, their goal is to impose as few behavioural assumptions as possible and yet come up with bidding strategies that work well in practice.

The incorporation of other strategies is shown into the population bidding distribution thereby suggesting the approach in this paper performs better when competing against other strategies.

The following algorithms are used:

1. Dynamic Programming Framework
2. Bellman Equation
3. Integer Programming Approximation

Limitation:
The proposed method applies more generally to dynamic programming problems that are weakly coupled.

3.9 An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries

Authors: Yehuda Lindell and Benny Pinkas, 2007

They show an efficient secure two-party protocol, based on Yao's construction, which provides security against malicious adversaries.

Cut and choose techniques are applied to the original circuit and inputs in order to support their construction. The ideal/real simulation paradigm is used to prove the security which is in the standard model (with the absence of random oracle model or common reference string assumptions).

This paper provides the following contributions as listed:

1. Efficient protocol against malicious parties.
2. Simulation based proofs.
3. A black box reduction.

The algorithm used is Yao's garbled circuit construction.

Findings:

1. It uses a symmetric key encryption scheme that has indistinguishable encryptions for multiple messages and an elusive efficiently verifiable range.
2. The protocol uses both unconditionally hiding and unconditionally binding commitments.
3. The protocol needs to use an Oblivious Transfer Protocol which is secure according to the real/ideal model simulation definition.

Limitations:

1. This approach is not practical as it requires using generic zero-knowledge proofs.
2. Yao's garbled circuit construction is secure in the presence of semi-honest adversaries.

3.10 Optimizing Semi-Honest Secure Multiparty Computation for the Internet

Authors: Aner Ben-Efraim, Yehuda Lindell and Eran Omri, 2016

In this paper, they have constructed highly efficient constant-round protocols for the setting of multiparty computation for semi-honest adversaries.

As proposed in BMR, the construction of a multiparty garbled circuit is used to make the protocol work.

Oblivious transfer is used as the first protocol. In case of no honest majority it constitutes the first concretely efficient constant round multiparty protocol.

Their second protocol uses BGW, and significantly more efficient than the FairplayMP protocol (Ben-David et al., CCS 2008) that also uses BGW.

The three main contributions in this paper:

1. They present the first concretely-efficient constant-round multiparty protocol that is secure for any number of corrupted parties.
2. Following FairplayMP, they also present protocols for constructing a multiparty garbled circuit based on BGW (BenOr-Goldwasser-Wigderson), that are far more efficient than those presented in the paper.
3. They ran extensive experiments comparing the performance of their different protocols to each other and to multiparty GMW.

In the setting of secure multiparty computation over the Internet, the garbled circuit approach followed by the proposed protocol is much faster than all previous protocols.

Furthermore, the proposed protocol has an extremely fast online time, making it suitable for scenarios where pre-processing is possible and fast response time is needed.

The following algorithms are used:

1. BMR Protocol.
2. Multiparty communication using multiparty garbled circuits.
3. A new BGW-based Protocol.

Findings:

1. Double Key PRF.
2. Secure bit-bit multiplication.
3. Secure string-bit multiplication.

3.11 Line-Point Zero Knowledge and Its Applications

Authors: Samuel Dittmer, Yuval Ishai and Rafail Ostrovsky, 2020

In this paper authors introduce and study a simple kind of proof systems called line-point zero knowledge (LPZK).

LPZK is motivated by the recent practical protocols for vector oblivious linear evaluation (VOLE), which can be used to compile LPZK proof systems into lightweight designated-verifier NIZK protocols.

Motivated by the goal of minimizing prover complexity in zero-knowledge proofs, they have introduced and studied a simple kind of proof systems called line-point zero knowledge. Then they have applied this proof system towards obtaining simple, concretely efficient, and reusable protocols for non-interactive secure computation.

The following algorithms are used:

1. Zero Knowledge Proof.
2. Line-Point Zero Knowledge Proof.

Findings:

1. Vector Oblivious Linear Evaluation is used.
2. Non-Interactive Zero Knowledge Proof Protocol is used.
3. Experiments are done on Random Oracle Model.
4. Non-Interactive Secure Computation Protocol is used.

3.12 Efficient Fully Secure Computation via Distributed Zero-Knowledge Proofs

Authors: Elette Boyle, Niv Gilboa, Yuval Ishai and Ariel Nof, 2020

Secure computation protocols are used for the computation of private inputs for mutually distrusting parties by revealing nothing but the output. The protocols with full security is also known as guaranteed output delivery which provides protection against denial-of-service attacks by which a correct output is guaranteed to be received by the honest parties. The presence of an honest majority is needed to realize this feature. In order to attain full security with good asymptotic and concrete efficiency there is a significant research effort carried out for this purpose.

They have presented an efficient protocol for any constant number of parties n, with full security against $t < n/2$ corrupted parties, that makes a black-box use of a pseudorandom generator.

New methods are used for the application of sublinear-communication distributed zero knowledge proofs by the proposed protocol for Boneh et al. in order to compile semi-honest protocols into fully secure protocols during the more challenging case of $t > 1$ corrupted parties.

The proposed protocol relies on replicated secret sharing to minimize communication and simplify the mechanism for achieving full security. This results in computational cost that scales potentially with n.

The main contribution is a secure computation protocol for any constant (or logarithmic) number of parties $n = 2t + 1$ that achieves full security against up to t malicious parties, with the same amortized communication as the best known semi-honest protocol.

The following algorithms are used:

1. Zero-Knowledge Proof.
2. Distributed Zero-Knowledge proof.

Findings:

1. It makes use of Semi-Honest Protocol.
2. It uses replicated secret sharing.
3. It uses shamir secret sharing.
4. It uses DN Multiplication Protocol.
5. It uses Fiat-Shamir transform.

Limitations:

1. It works well in a small number paradigm.
2. It mainly focuses on semi-honest scenarios.

3.13 Secure Multiparty Computation [MPC]

Author: Yehuda Lindell

This paper reviews what MPC is, what problems it solves and how it is currently being used. Discusses about the aim of the secure multiparty computation that is to make it possible for the parties to securely carry out distributed computing tasks.

The paper briefly talks about the definitional paradigm of secure multiparty computation, feasibility of MPC and techniques used to realize MPC. Briefly explains the scenario of Honest-Majority MPC with secret sharing, private set intersection and threshold cryptography.

The algorithm used here is threshold cryptography.

Findings:
1. Uses oblivious pseudo random functions.
2. Uses hashing techniques.
3. Uses Shamir secret sharing.

Limitation: It is challenging to achieve security in the malicious model which makes use of oblivious pseudo random functions which is secure for semi-honest model.

3.14 Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody

Authors: Yehuda Lindell, Ariel Nof, Samuel Ranellucci

This paper presents the first truly practical full threshold ECDSA signing protocol which includes both fast signing and fast key distribution. One such use case where we can make use of this algorithm is cryptocurrency wallets and cryptocurrency custody solutions which is one of the hot topics.

This full threshold ECDSA signing protocol has practical distributed key generation and fast signing. They have achieved this breakthrough by replacing the Paillier additively homomorphic encryption with El-Gamal in-the-exponent which also brings out additive homomorphism.

The algorithm used here is threshold ECDSA.

Findings:
1. Uses El-Gamal “in-the-exponent”.
2. Checks for Deffie-Hellman Tuples.
3. Elliptic curve operations are very much efficient than Paillier operations.

3.15 Realizing Secure Multiparty Computation

Author: Trondheim

The work here is to understand the basic theory of multiparty computation. They have focused on building frameworks that inspires the implementation of the so far theoretical protocols and applications.

The main focus here is to develop the Virtual Ideal Functionality Framework (VIFF) which realizes MPC which in return can provide solutions to various voting problems.

The algorithm used here is MPC with virtual ideal functionality framework.

Findings:
1. Uses Shamir secret sharing.
2. Finite field are used called Galois Field.

Limitation: This thesis developed two applications that mainly focuses on just proof-of-concept applications.

3.16 On the Message Complexity of Secure Multiparty Computation

Authors: Yuval Ishai, Manika Mittal, Rafail Ostrovsky

This paper is based on the study of the minimal number of point-to-point messages required for general secure multiparty computation (MPC) in the setting of computational security against semi-honest, static adversaries which in return may corrupt an arbitrary number of parties.

The work done provide a tight characterization of the message complexity of computationally secure MPC in the presence of semi-honest adversaries that can corrupt any number of parties.

The algorithm used here is message complexity of MPC protocol.

Finding: It uses 2-round MPC protocol in the plain model.

Limitation: Considers its own upper and lower bound for semi-honest, static adversaries which may corrupt an arbitrary number of parties.

3.17 Fast Large-Scale Honest-Majority MPC for Malicious Adversaries

Authors: Koji Chida, Daniel Genkin, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Yehuda Lindell, Ariel Nof

This paper implies that even though the protocols for semi-honest adversaries are far more efficient there are many cases where the security guarantees are not that effective.
Thus, this paper presents new protocols where any functionality constituted by an arithmetic circuit can be securely computed.

The paper firmly supports their protocols stating they are information-theoretically secure in the appearance of a malicious adversaries assuming an honest majority. They present protocol variants for all the fields like small and large fields and exhibits how to effectively instantiate them based on replicated secret sharing and Shamir sharing.

The algorithm used here is secure multiparty computation protocol.

Findings:
1. Uses threshold secret sharing.
2. Makes use of pseudo randomness.

3.18 Performance Study of Enhanced SHA-256 Algorithm

Authors: Gowthaman A, M Sumathi

Today our modern world utilizes various electronic operations: E-mail, Internet banking, document transfer, online shopping. Cryptography has inclined a vital role for safeguard of data conversion.

Hash task which involves mapping the message of erratic length to a string of fixed length is called message hash or digest. In 2002 the national institute of science and technology (NIST) published the SHA, which specifies three new secure hash algorithms SHA224, SHA256, SHA384 and SHA512.

Hash task are mainly used to guard function of purity. They also provide the guard of authentication, when they are used in combination with digital signature and MAC algorithms. These algorithms are constant and one-way functions that input message and output message digest.

It processes the data in different stages:
Message filler (or) padding,
Message extension
Message squeezing.

SHA256 System
The optimization technique of Secure hash algorithm is designed by function of Choice, Majority and Summing operations. The input of the hash values is processed, the output of the first round hashed value is 8 numbers of 32-bit blocks. The bits are returned to the next set of iteration for processing the data with new hash values. The carry save adder (CSA) is added to the 32-bit blocks for 64 iterations. Adder saves the values in registers for further addition process. Finally, the hashed value is 8 numbers of 32-bit blocks. By merging this data, 256-bit hashed value is produced. CSA separates the sum and carry root and the carry propagation technique is applied for minimizing the delay. Another method that can also be applied for reducing the delay is implementation of Unrolling and Pipelining.

The SHA-256 algorithm compute 64 iterations over the block of 512-bit messages and hash values of 256-bits, to interpret eight numbers of 32-bit words (A, B, C, D, E, F, G, H).

In SHA-256 algorithm, there are several ways for designing the inner part of the loop, because of the number of additions needed. It is possible to rearrange the inner part for achieving high performance in the data dependencies.

The operation in the inner loop of the algorithm was performed by precomputation, and subtractions of the functions. The variables of 8 numbers of 32-bit blocks are performed by this method. The pre-computation saves the sum value during the run time iterations, for previous iteration.

Limitations:
1. This architecture requires an additional clock cycle to initialize the system for decreasing the data dependency.
2. This system needs more hardware functions to produce high throughput.

References	Proposed	Algorithm	Findings	Limitations
(Ben Palmer, Kris Bubendorfer, Ian Welch, 2012)	A protocol for verification of an auction without revealing bid values	Existing Homomorphic Auction Protocol Verification Protocol (ZKP)	Uses El-Gamal Encryption Uses Fiat-Shamir Heuristic and SHA512 hash Function for no-interactive ZKP	Too expensive for resource allocation for individual tasks
(Luiz Thomaz do Nascimento, Sapna Kumari, Vedavinayagam Ganesan, 2019)	Zero knowledge proofs applied to auctions	Non-Interactive ZKP Follows Reverse Auction Workflow	Uses Fiat-Shamir Heuristic for converting interactive to non-interactive ZKP Implements Hyrax and BulletproofLib	Assumes that every bidder knows all the bidding commitments from all other bidders; if not then it can be shown as fake even though if it isn't.
(Hisham S. Galal and Amr M. Youssef)	Verifiable Sealed-Bid Auction on the Ethereum Blockchain	Homomorphic commitment scheme ZKP of interval membership	Uses Pedersen commitment scheme Uses ciphertext for the auction contract	

References	Proposed	Algorithm	Findings	Limitations
(Jose A. Montenegro, Michael J. Fischer, Javier Lopez, Rene Peralta, 2011)	Secure Sealed-Bid Online Auctions Using Discreet Cryptographic Proofs	Development of a proof-Certificate standard Enables secure multiparty computation(SMC)	Uses Public-Key cryptography	
(Felix Brandt and Tuomas Sandholm)	Efficient Privacy-Preserving Protocols for Multi-unit Auctions	Any Homomorphic encryption scheme Zero-knowledge random oracle model is obtained	Uses El-Gamal Encryption Σ-protocols are used Fiat-Shamir heuristic is used to make ZK non-interactive	Assumption is made that privacy can not be breached (unless all bidders collude). To compute the price units the bidder must continue even though he wants to quit.
(Chaya Ganesh, Yashvanth Kondi, Arpita Patra and Pratik Sarkar, 2018)	Efficient Adaptively Secure Zero-knowledge from Garbled Circuits	ZKGC(Zero Knowledge Garbled Circuit) protocol	Initiates RE-OT(receiver equivocal oblivious transfer) Uses MPC-in-the-head approach, CRS(common reference string) of SNARKs, ROM(random oracle model)	

References	Proposed	Algorithm	Findings	Limitations
(Anunay Kulashrestha, Akshay Rampuria, Matthew Denton and Ashwin Sreenivas,2017)	Cryptographically Secure Multiparty Computation and Distributed Auctions Using Homomorphic Encryption	Non-Interactive Zero-Knowledge Proof	Uses Fiat-Shamir Heuristic, Cryptographic hash function SHA-256, El Gamal encryption Uses Google's gPRC and protobuf implementations	
(Dimitris Bertsimas, Jeffrey Hawkins, Georgia Perakis, 2002)	Optimal Bidding in On-line Auctions	Dynamic Programming Framework	Bellman Equation Integer Programming Approximation	The proposed method applies more generally to dynamic programming problems that are weakly coupled.
(Yehuda Lindell and Benny Pinkas, 2007)	An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries	Yao's garbled circuit construction	uses a symmetric key encryption scheme protocol uses both unconditionally hiding and unconditionally binding commitments, Uses an Oblivious Transfer protocol	This approach does not seem to be very practical as it requires using generic zero-knowledge proofs. Yao's garbled circuit construction is secure in the presence of semi-honest adversaries.

References	Proposed	Algorithm	Findings	Limitations
(Aner Ben-Efraim, Yehuda Lindell and Eran Omri, 2016)	Optimizing Semi-Honest Secure Multiparty Computation for the Internet	The BMR protocol. Multiparty Communication using Multiparty Garbled Circuits. A New BGW-based Protocol.	The Double Key PRF. Secure bit-bit Multiplication. Secure string-bit multiplication.	
(Samuel Dittmer, Yuval Ishai and Rafail Ostrovsky, 2020)	Line-Point Zero Knowledge and Its Applications	Zero Knowledge Proof Line-Point Zero Knowledge Proof	uses Vector Oblivious Linear Evaluation, Non-Interactive Zero Knowledge Proof protocol, Randome Oracle Model and Non-Interactive Secure Computation protocol	
(Elette Boyle, Niv Gilboa, Yuval Ishai and Ariel Nof, 2020)	Efficient Fully Secure Computation via Distributed Zero-Knowledge Proofs	Zero-Knowledge Proof. Distributed Zero-Knowledge proof.	Makes use of Semi-Honest Protocol. Uses Replicated Secret Sharing, Shamir secret sharing, DN Multiplication Protocol, Fiat-Shamir Transform	Works well in a small number paradigm. Mainly focuses on semi-honest Scenario.

References	Proposed	Algorithm	Findings	Limitations
(Yehuda Lindell,2020)	Secure Multiparty Computation[MPC]	Threshold Cryptography	Uses oblivious pseudo random functions Uses hashing techniques Uses Shamir Secret Sharing	It is challenging to achieve security in the malicious model using the oblivious pseudorandom functions which is secure for semi-honest model.
(Yehuda Lindell,Ariel Nof, Samuel Ranellucci, 2018)	Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody	Threshold ECDSA	Uses ElGamal "in the exponent" Checks for Deffie-Hellman Tuples	
(Trondheim, 2009)	Realizing Secure Multiparty Compuatations	Virtual Ideal Functionality Framework[VIFF]	Uses Shamir Secret Sharing Finite field are used called Galois Field	The two applications developed in this thesis are mainly focused on just proof-of-concept applications.
(Yuval Ishai, Manika Mittal and Rafail Ostrovsky, 2018)	On the Message Complexity of Secure Multiparty Computation	Message complexity of MPC protocol	Uses 2-round MPC protocol in the plain model	Considers it's own upper and lower bound and focuses on semi-honest, static adversaries who may corrupt an arbitrary number of parties.
(Koji Chida, Daniel Genkin, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Yehuda Lindell and Ariel Nof, 2018)	Fast Large-Scale Honest-Majority MPC for Malicious Adversaries	Secure Multiparty Computation Protocol	Uses Threshold Secret Sharing Uses Pseudo Randomness	
(Gowthaman A, M Sumathi, 2015)	Performance Study of Enhanced SHA-256 Algorithm	SHA256		This architecture requires an additional clock cycle to initialize the system for decreasing the data dependency. This system needs more hardware functions to produce high throughput.

Fig 1. Summarization of Literature Survey

BACK TO INDEX

CHAPTER 4

PROJECT REQUIREMENTS SPECIFICATION

Our project will primarily focus on the following requirements listed below:

4.1 Hardware Interface Requirements:

SNo.	Hardware Interface	Interface Name
1	Operating System	Windows 10
2	Processor	Intel i7
3	RAM	16 GB
4	Disk Space	17 GB

4.2 Software Interface Requirements:

SNo.	Software Interface	Interface Name	Additional Packages	Versions
1	Web Framework	Django	Pillow	3.1.7
2	RDBMS	Sqlite3	-	3.8.3
3	Programming Language	Python	-	3.8.7

BACK TO INDEX

CHAPTER 5

SYSTEM REQUIREMENTS SPECIFICATION

5.1 INTRODUCTION

5.1.1 Purpose

In a traditional e-commerce environment, buyers and sellers participate in an auction where the seller publishes a price for a particular product and depending upon the highest bid offered by a buyer further negotiation of payment is carried out. Online auctions are the digital framework in which both the participants from across the world participate via the internet. However, online auctions can become vulnerable if a malicious participant unregistered on the website i.e. buyer tries to participate in the auction process. Thus, the purpose of our project is authenticating bidders and sellers of auctions against unauthorized/malicious adversaries.

5.1.2 Project Conventions

The following conventions are used for designing our proposed system (represented as a system design diagram):

Acronyms	Component Name
Br	Buyer
Sr	Seller
Sv	Server
Tsv	Server Token
DB	Database

5.1.3 Intended Audience

This project is intended towards connecting buyers and sellers from around the world for participation in auctions via the internet in a secure environment. The project is implemented under the guidance of our project mentor and coordinator.

5.2 SYSTEM DESCRIPTION

5.2.1 System Features

The following are the major features of an online auction system:

5.2.1.1 A user-friendly GUI which provides effortless service to all the users of the website.

5.2.1.2 The data flow and transaction processing are controlled and maintained by the website administrator.

5.2.1.3 Entity Authentication is used to ensure the identity between both the entities i.e., buyer and seller participating in the auction.

5.2.1.4 Zero Knowledge Proof (ZKP) Protocol using SCEP curve is used to ensure entity authentication and anonymity.

5.2.2 Operating Environment

5.2.2.1 Operating System Platform: Windows

5.2.2.2 Web Framework Platform: Django

5.2.2.3 RDBMS Platform: Sqlite3

5.2.2.4 Programming Language: Python

5.2.3 Project Limitation

Multiple clients i.e., buyers and sellers participate in online auctions. Thus, it becomes difficult to ensure trust since the identities of buyer and seller remain hidden.

5.3 REQUIREMENTS

5.3.1 Functional Requirements

Sqlite3 Database
The database storage will be controlled and maintained by the website administrator. It will include data pertaining to list of buyers and sellers, profile information of buyers and sellers, list of categories and products. The administrator has the rights to add/remove categories, products, buyers and sellers.

5.3.2 Non-Functional Requirements

5.3.2.1 Security Features

5.3.2.1.1 Entity Authentication – Since SCEP curve is used, it finds a point on the curve which ensures identity authentication and verification. This process is carried out by the server in case of both buyer and seller authentication thereby ensuring entity authentication.

5.3.2.1.2 Anonymity – The clients i.e., buyer and seller generate a new value which is computed based on the token received from the server and SHA256 encrypted data. This value will act as an id for carrying out transactions over the web interface. Thus, the identity of the clients remains hidden thereby ensuring anonymity.

5.3.2.2 Software Quality Features

5.3.2.2.1 Availability: The data pertaining to the products must be available on the website in order to provide a seamless experience to the buyers.

5.3.2.2.2 Correctness: The data about different products offered by sellers for auction must be correct such as the price of the product.

5.3.2.2.3 Maintainability: The data pertaining to the website such as user's data, product data etc. must be properly maintained by the website administrator in a database.

5.3.2.2.4 Usability: The website must be user-friendly and interactive for both buyers and sellers.

BACK TO INDEX

CHAPTER 6

SYSTEM DESIGN

The proposed system design for our capstone project is as follows:

6.1 The website will comprise of the following webpages:
- **6.1.1** Home page.
- **6.1.2** Products page.
- **6.1.3** Categories page.
- **6.1.4** Registration page.
- **6.1.5** Login page.

6.2 The home page will provide a user-friendly and interactive user interface which will enlist the top products and categories available for auction.

6.3 The products page is used to enlist the latest products offered by the sellers for auction. The product information such as category, no. of bids, highest bid, total no. of hours available for auction can be viewed.

6.4 The categories page is used to enlist the different categories available for buyers to participate in auction. The selection of a particular category will result in the display of different products. The selection of a particular product in a category will provide product information such as highest bid, product description, total no. of hours available for auction as well as the option to participate in the auction.

6.5 The registration page is used for registering the information of users i.e., buyers and sellers on the website. The details provided by the users will be used to ensure anonymity by encapsulating them to generate a random anonymous id. This anonymous id ensures entity authentication by which the users can participate in the bidding process securely without revealing their profile information.

6.6 The login page is used for logging into the user account using his credentials. Once logged in the user can view the different products/categories available on the website. Each user can also view the dashboard. In case of buyer the list of bids for different products can be viewed. In case of seller the different products which are added for auction can be viewed.

6.7 Once a user i.e., buyer or seller registers their information with the website the ZKP protocol is used to ensure entity authentication and anonymity.

6.8 User anonymity is ensured by encapsulating the users profile information to generate a random anonymous id. When the buyer bids for a particular product or when the seller adds a new product for auction a random transaction id gets generated which is secured using ZKP protocol thereby ensuring entity authentication.

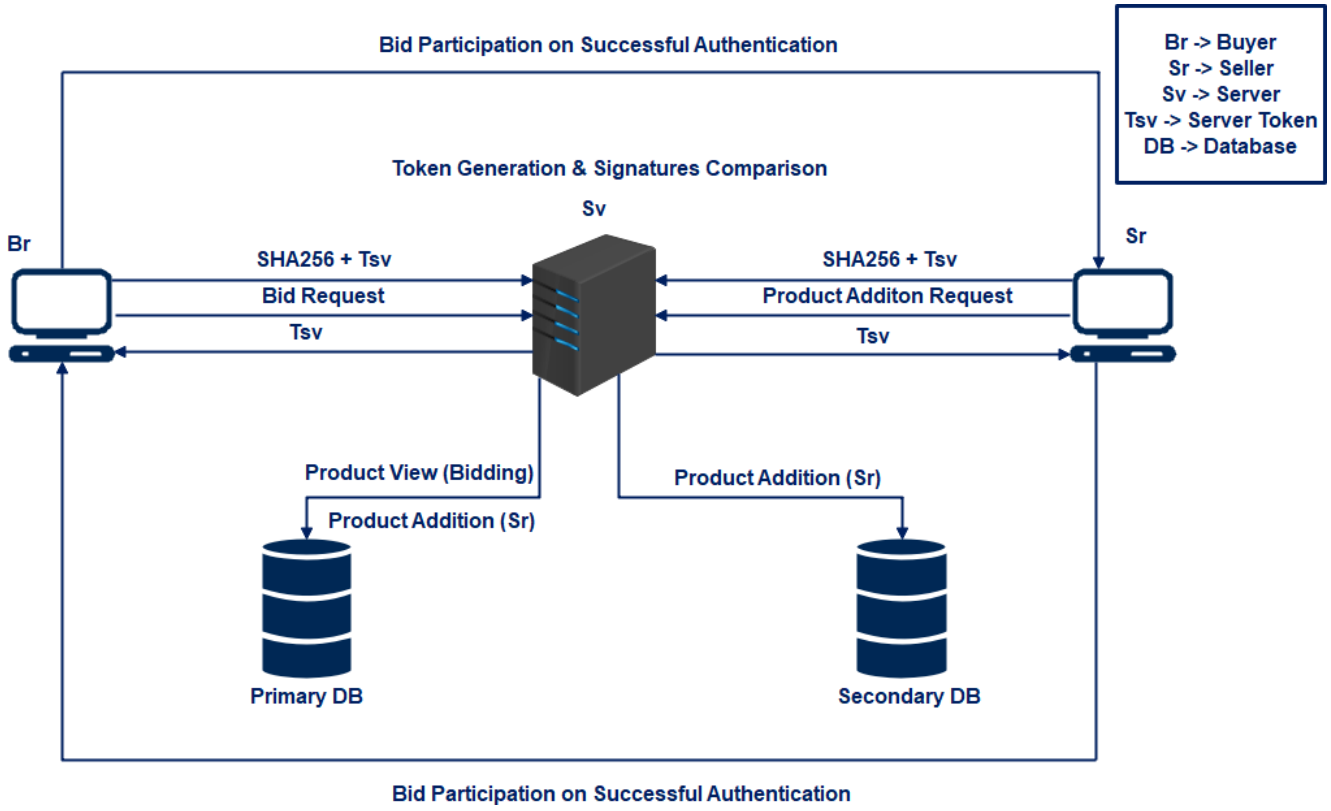


Fig 1. Online Auction System Design

BACK TO INDEX

CHAPTER 7

IMPLEMENTATION AND PSEUDOCODE

Algorithm:

Step 1: Service Request
The client sends a request to the server for participation in an online transaction. In case of an online auction, the clients i.e., buyer and seller send a request to the server. In case of the buyer, the request refers to a bid request for participation in the online auction. In case of the seller, the request refers to addition of a new product in the database.

Step 2: Server Token Generation
The server generates a SHA256 value and a token for the clients which is used for authentication. The server sends the token to its clients respectively.

Step 3: Client Token Generation
The clients i.e. buyer and seller generates a token for its seedphrase or password which is encrypted using SHA256 along with the profile of buyer and seller respectively. This newly computed value is sent to the server for authentication. This
value will act as an id for both the clients in order to carry out secure online auction.

Step 4: Client Token & Server Token Computation
The server receives the newly computed value from the clients respectively. The server has its own signature (SHA256 value and token) which is used for comparison with the newly computed value sent by the clients.

Step 5: Server Verification of Client Signature
If the server's signature and client's signature get matched thus the authentication will become successful. Therefore, the buyer can participate in the online auctions since server has ensured buyer's authentication to the seller. The seller can also participate in transaction communication since the server ensures seller's authentication to the buyer. This helps to ensure entity authentication and anonymity. It also allows the seller to add a new product to the database since he/she is an authenticated seller.

Pseudocode (Modified SCEP):

```
customer_hash = get_customer_details()                  # Customer Hash Value
seed_value = generate_random_seed()                     # Any Random Number
final_server_value = sha(customer_hash + seed_value)
if(final_server_value == received_value)
        transaction is authentic
else
        transaction is a failure
```

Pseudocode (SHA256):

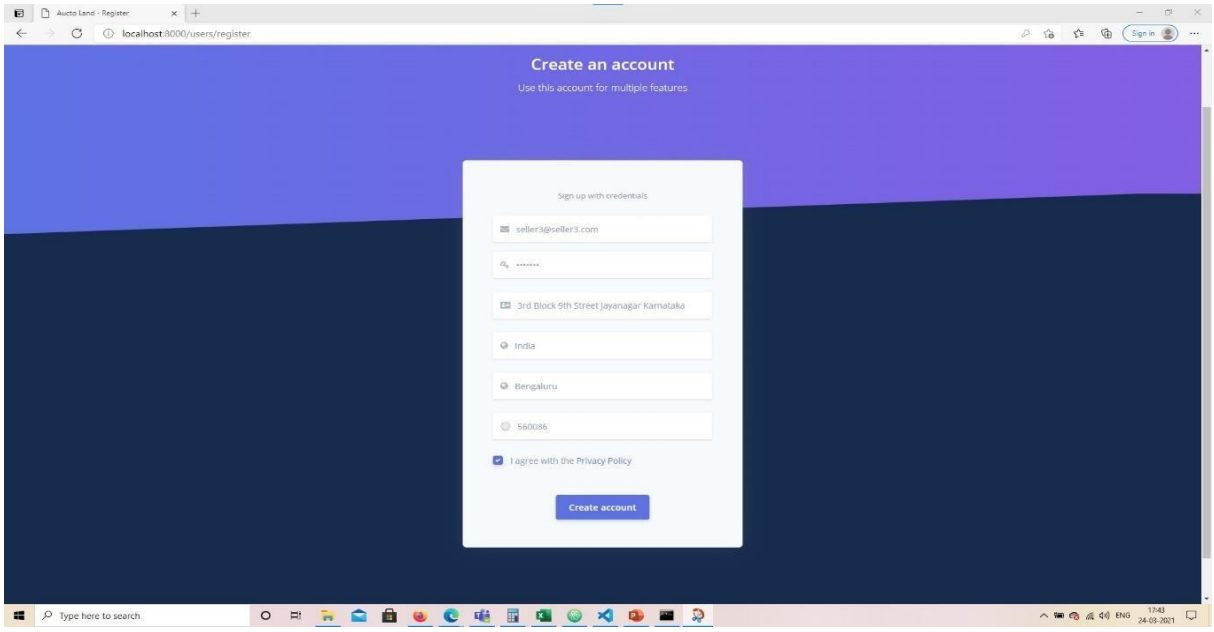
1. Initialize hash values (first 32 bits of the fractional parts of the square roots of the first 8 primes 2..19).
2. Initialize array of round constants (first 32 bits of the fractional parts of the cube roots of the first 64 primes 2..311).
3. begin with the original message of length L bits.
4. append a single '1' bit.
5. append K '0' bits, where K is the minimum number >= 0 such that L + 1 + K + 64 is a multiple of 512.
6. append L as a 64-bit big-endian integer, making the total post processed length a multiple of 512 bits such that the bits in the message are L 1 00..<K 0's>..00 <L as 64 bit integer> = k*512 total bits.
7. break message into 512-bit chunks.
8. for each chunk create a 64-entry message schedule array w[0..63] of 32-bit words.
9. Compress the chunks.
10. Add the compressed chunk to the current hash value.
11. Produce the final hash value (big-endian).

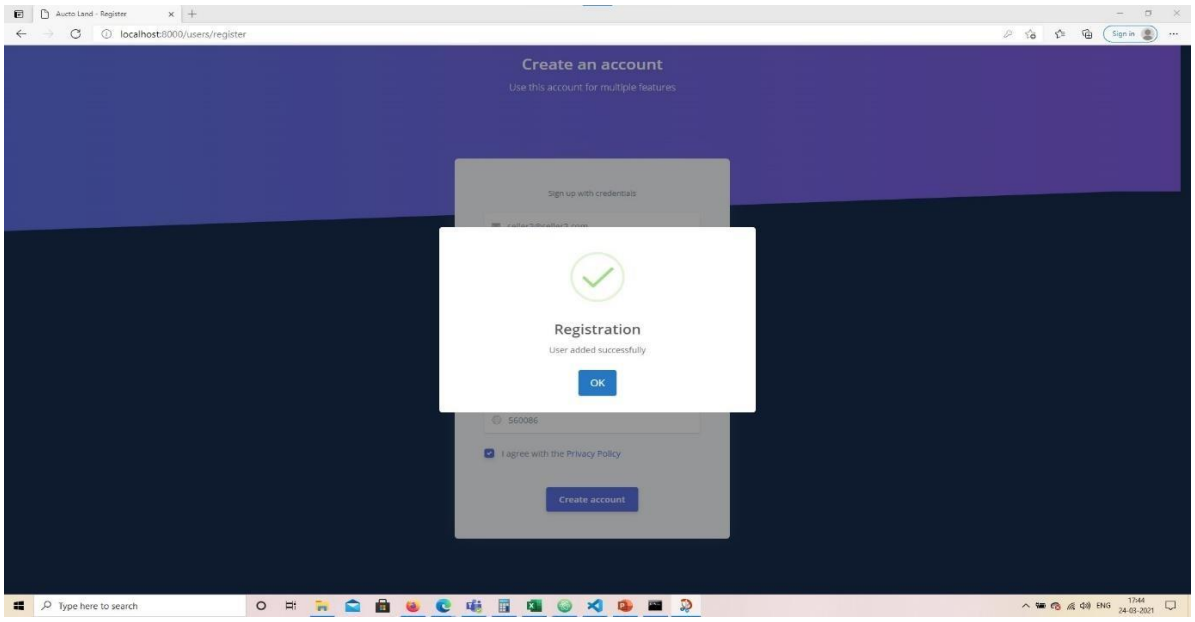
BACK TO INDEX

CHAPTER 8

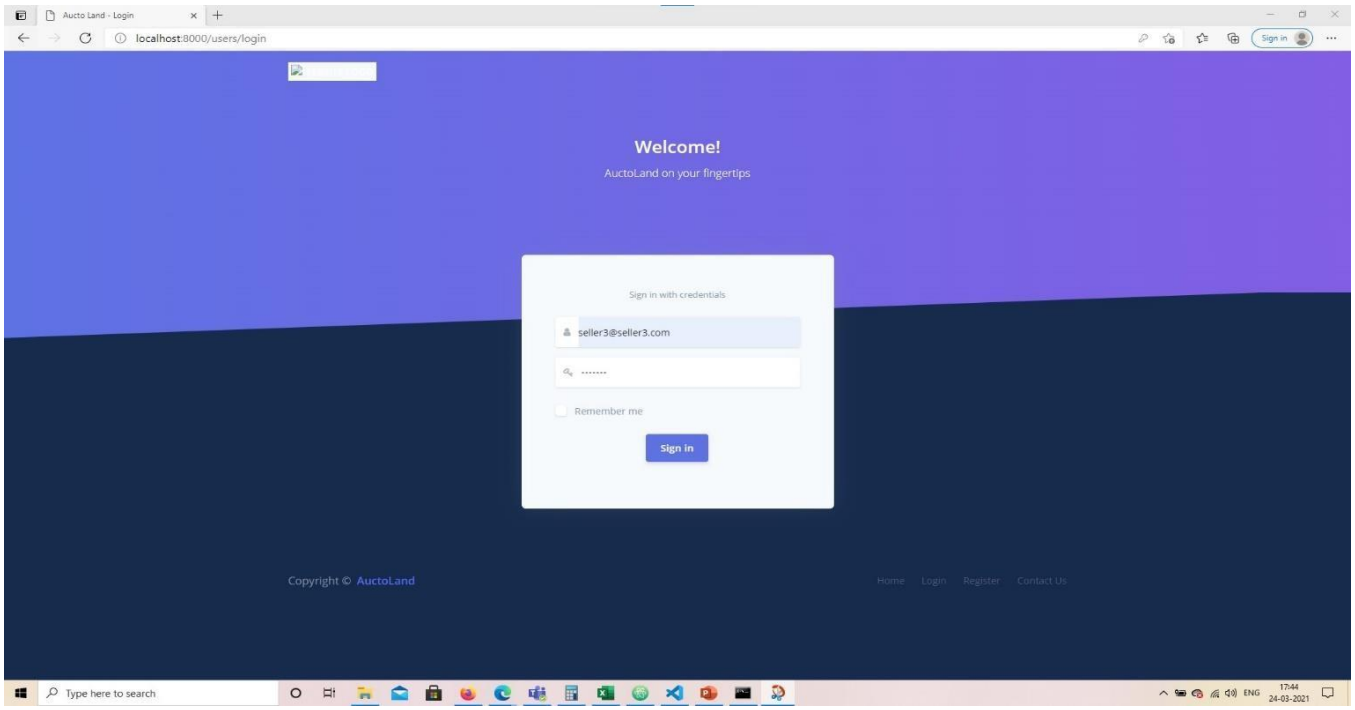
PROJECT DEMONSTRATION

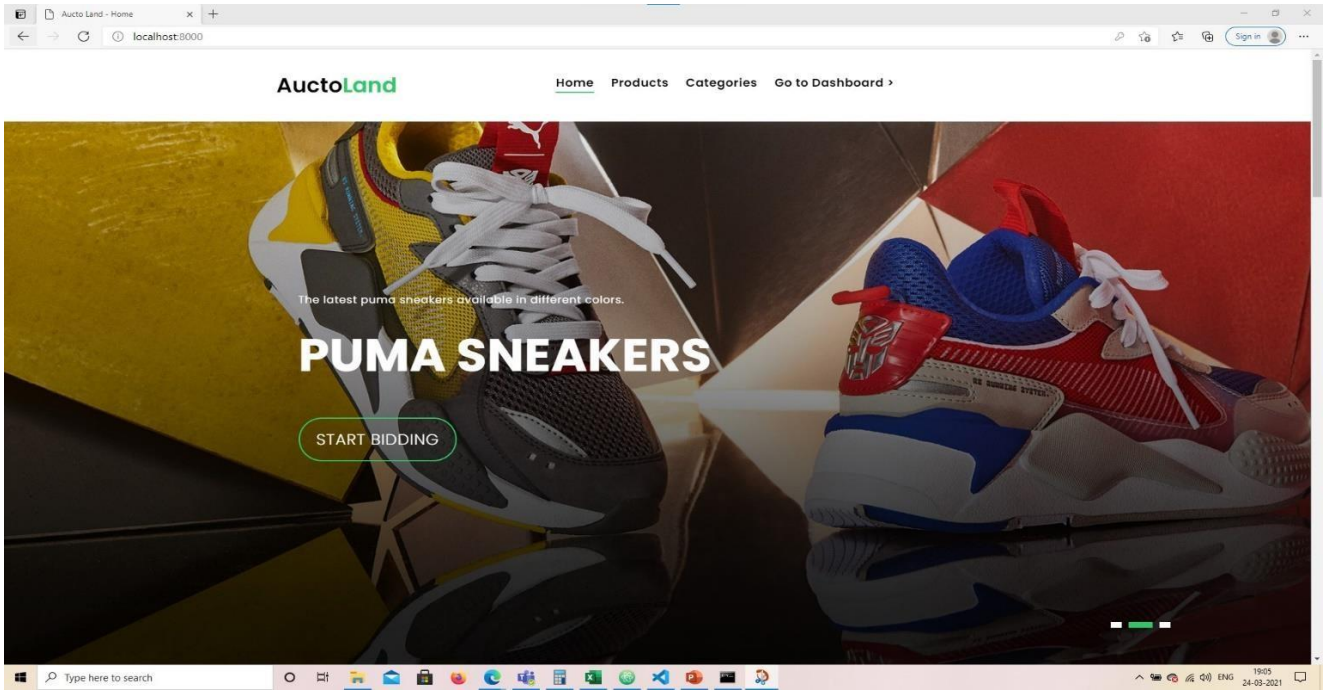
1. User Registration (Seller)



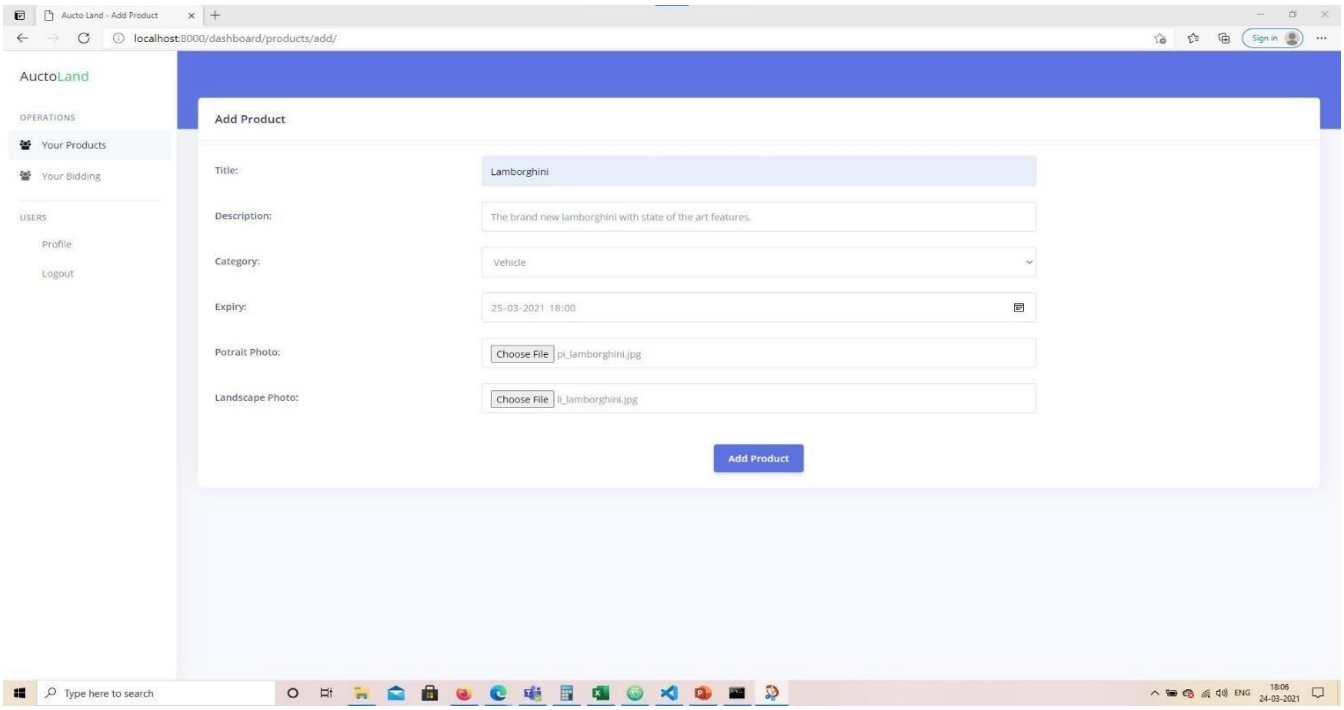


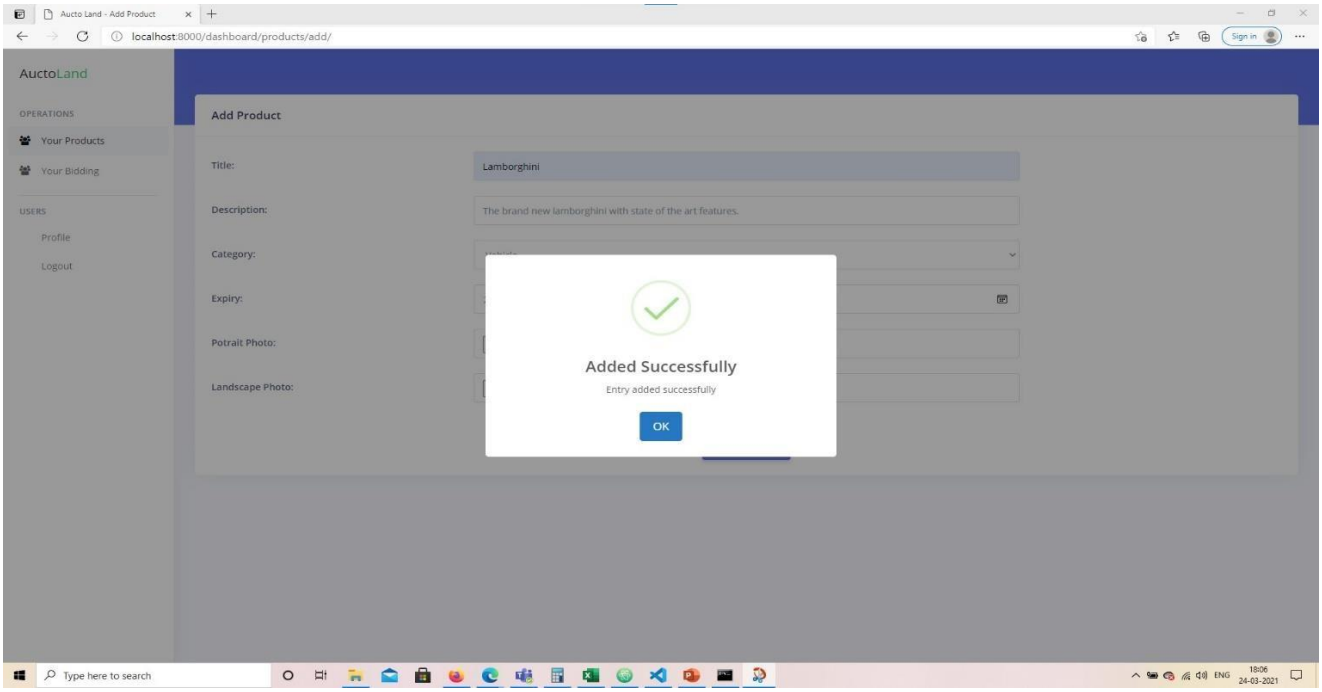
2. User Login (Seller)



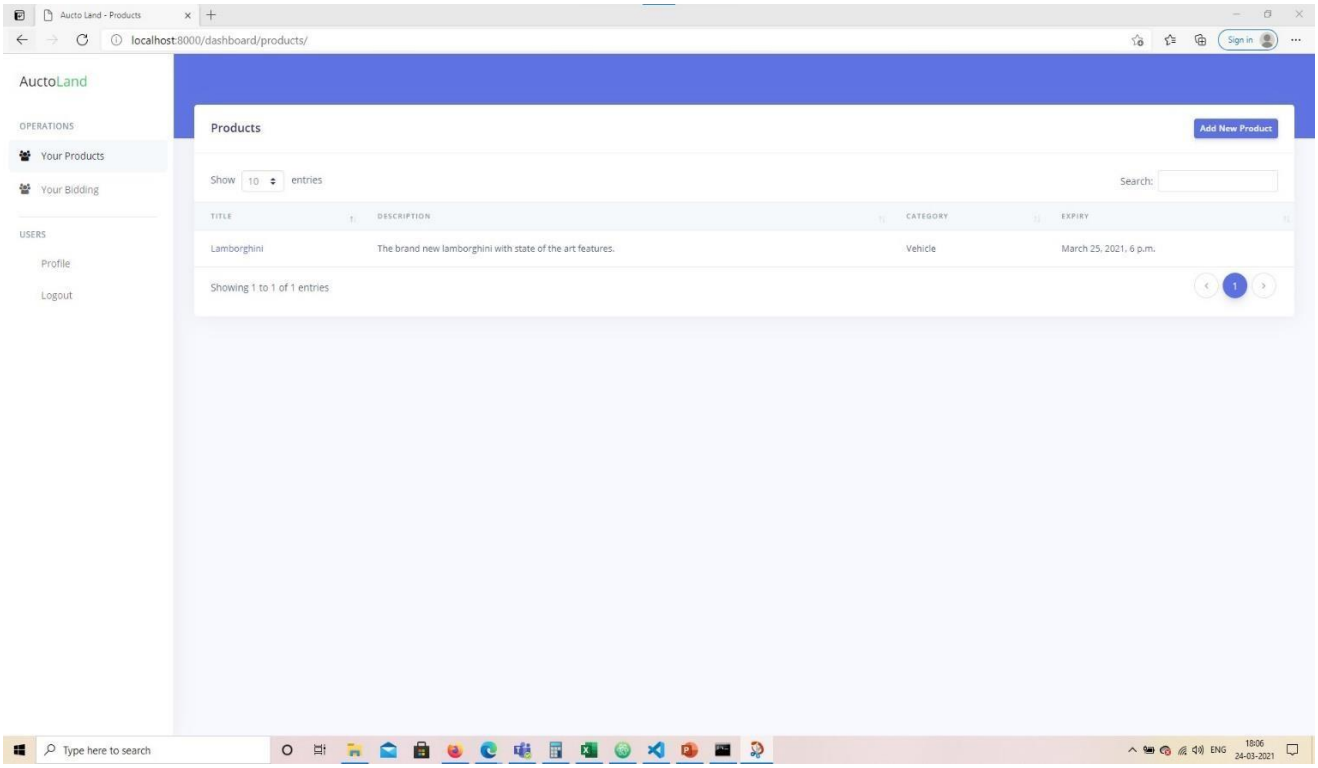


3. Product Addition (Seller)

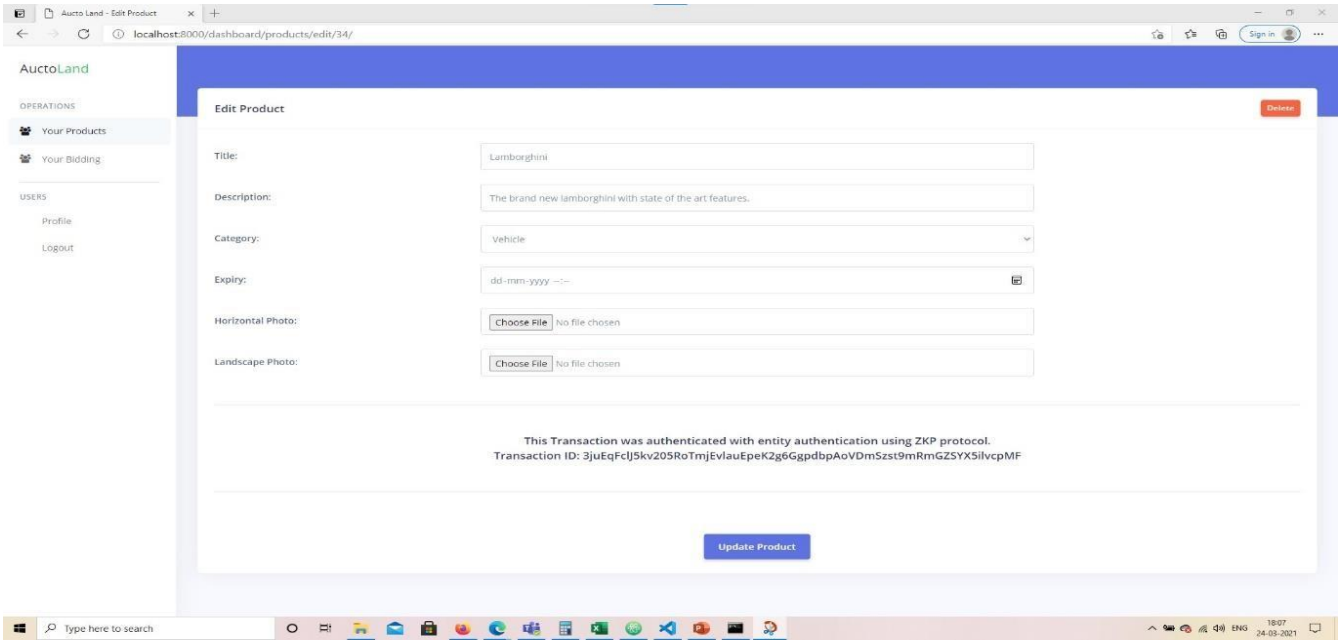




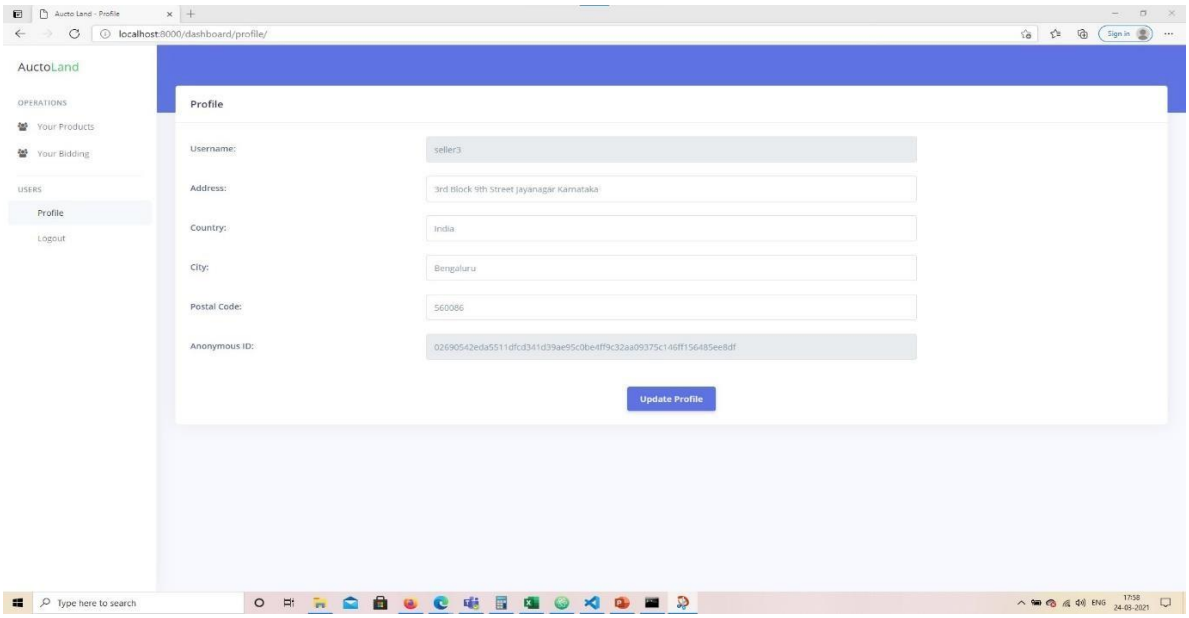
4. Product Display (Seller)



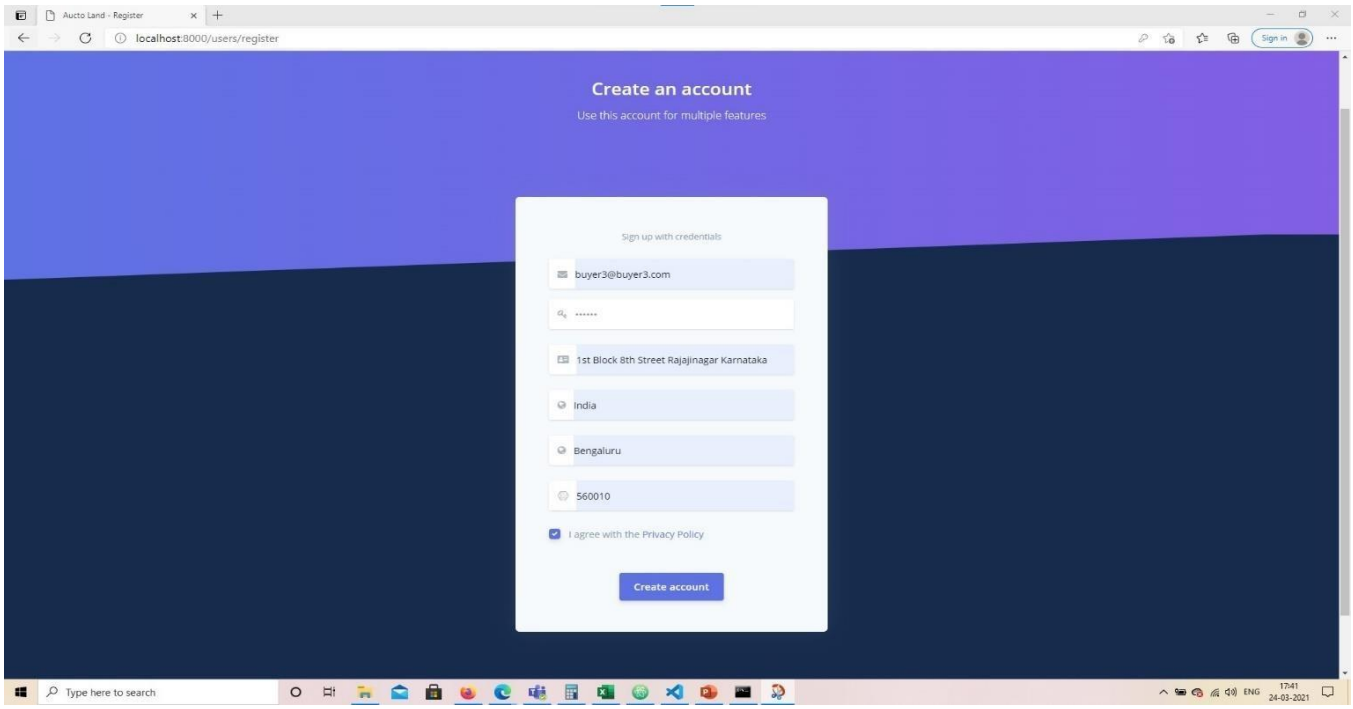
5. Entity Authentication (Seller)

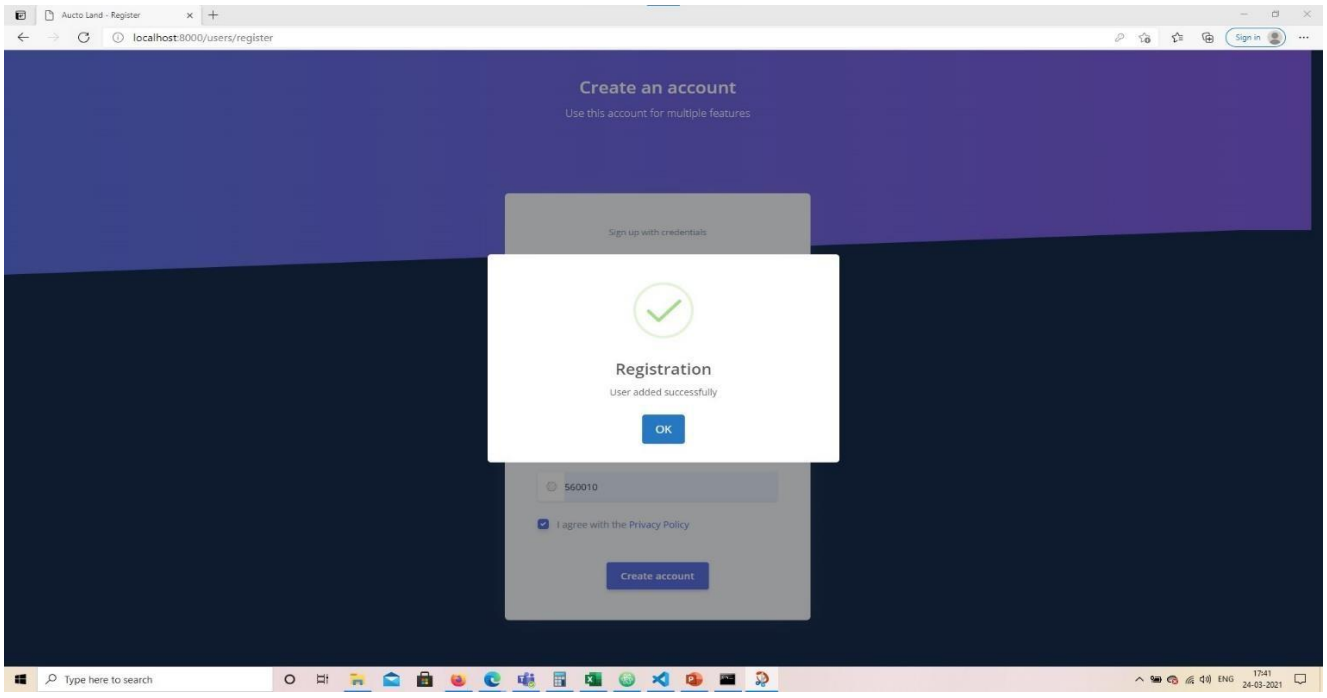


6. User Anonymity (Seller)

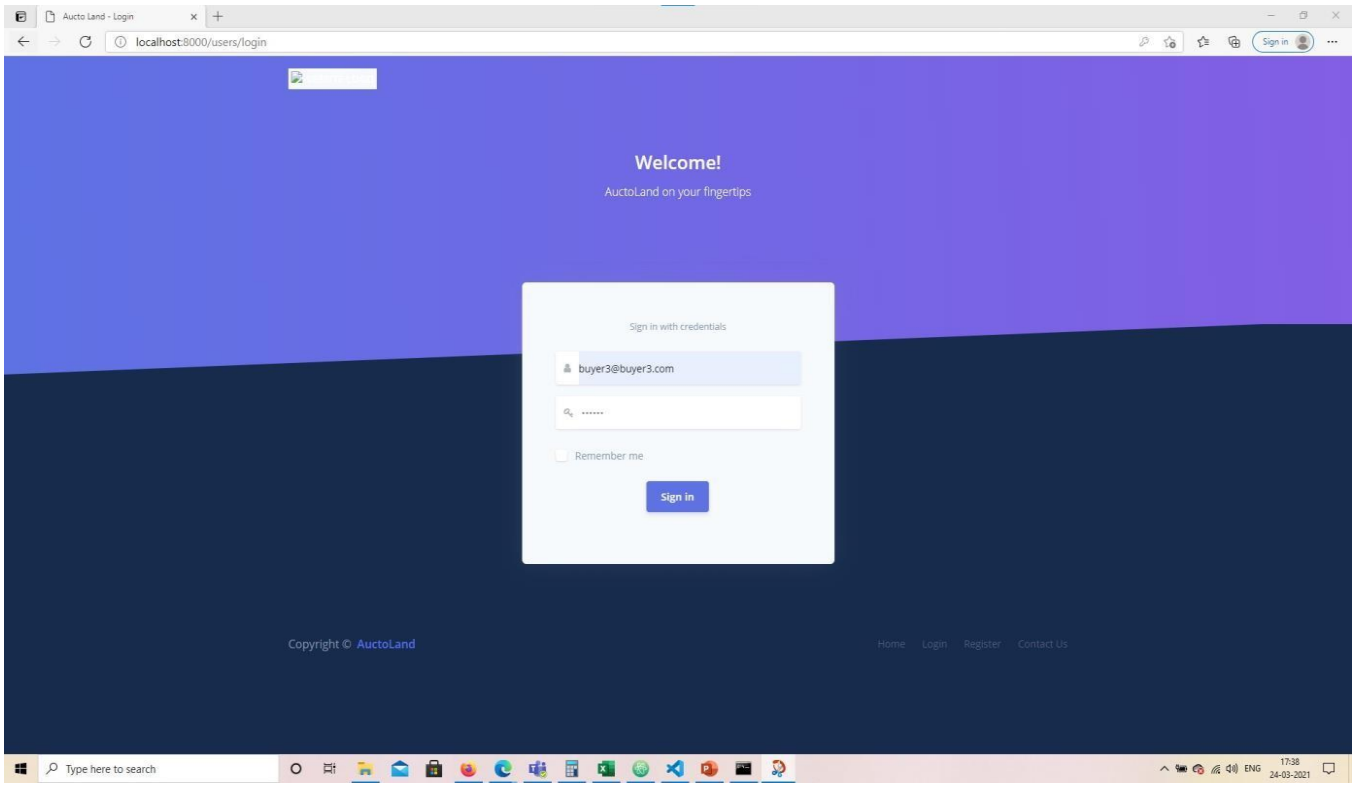


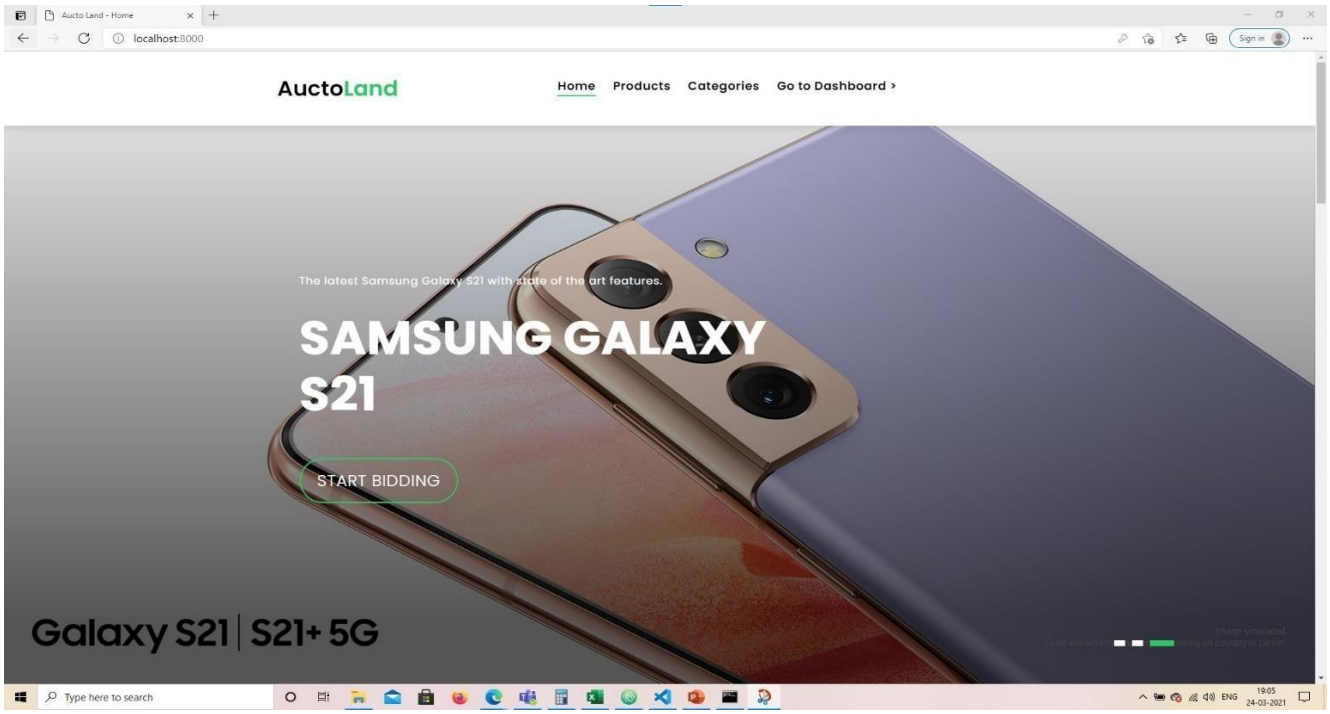
7. User Registration (Buyer)



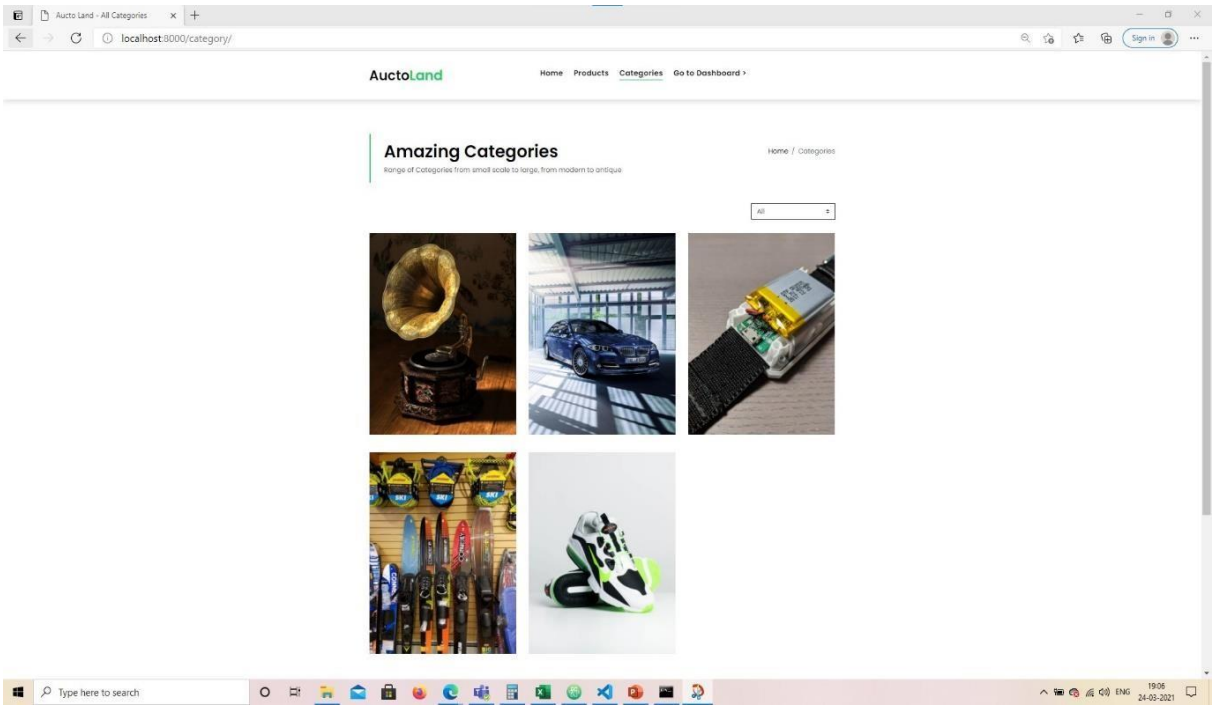


8. User Login (Buyer)

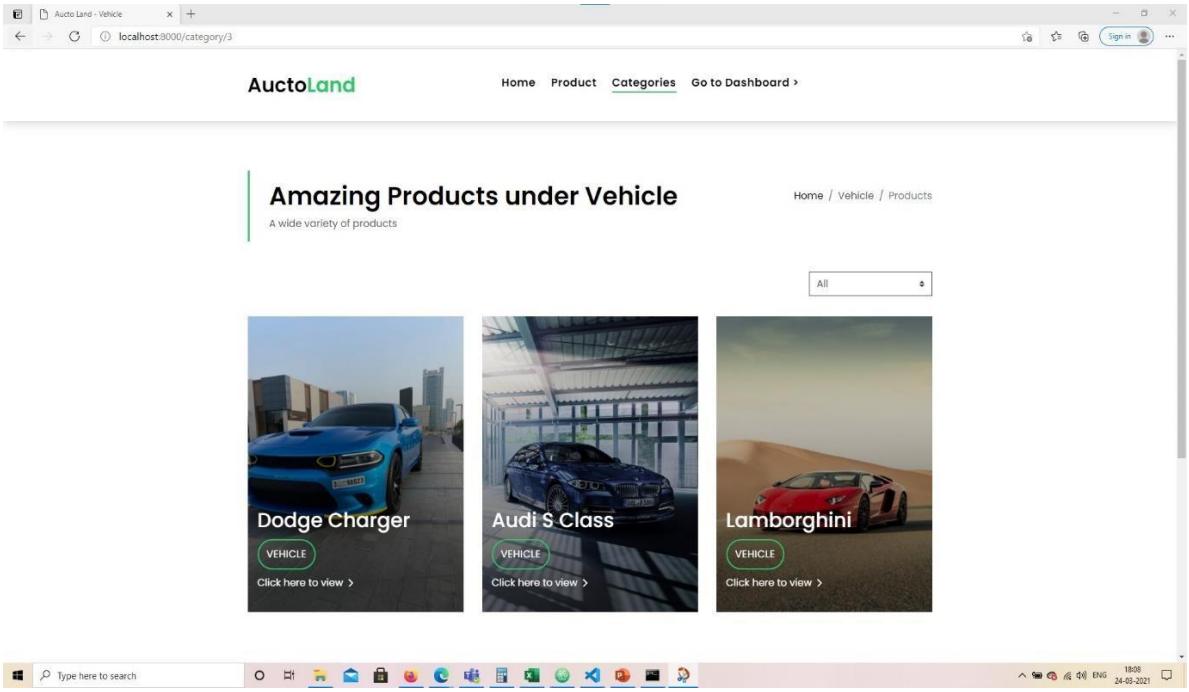




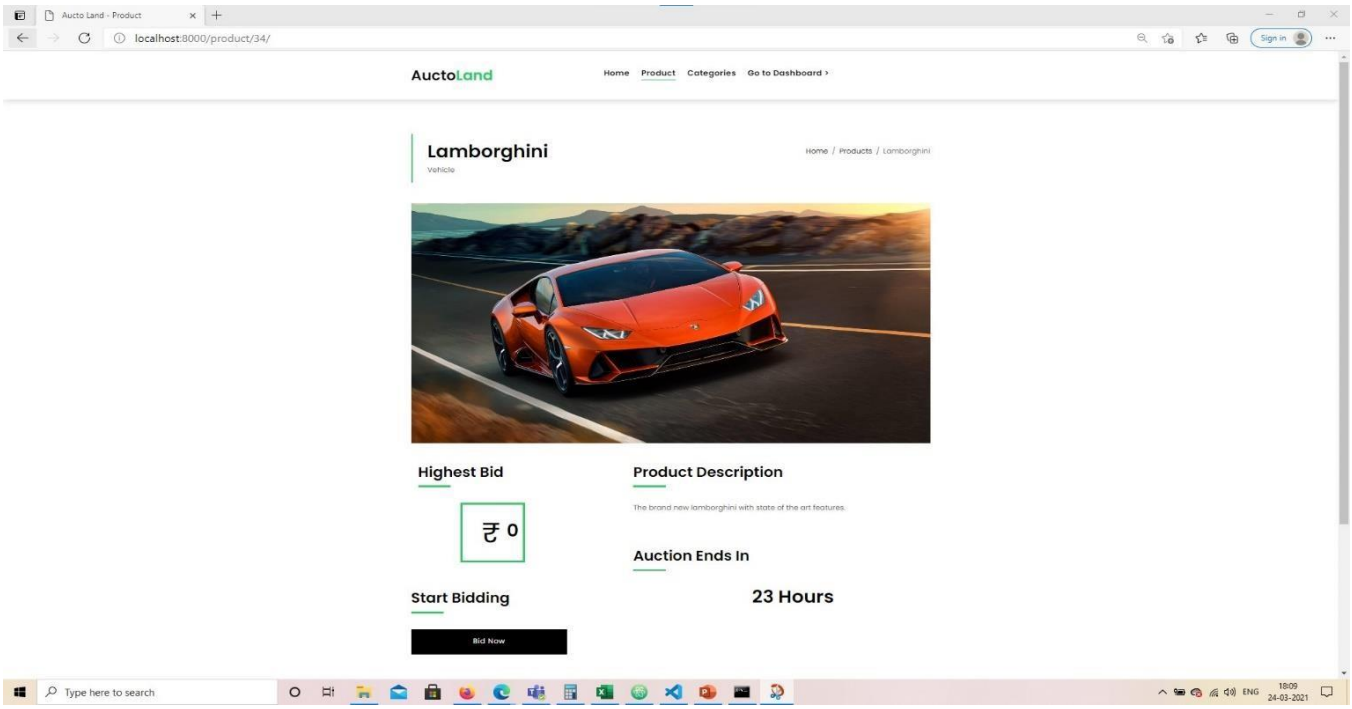
9. Categories Display (Buyer)

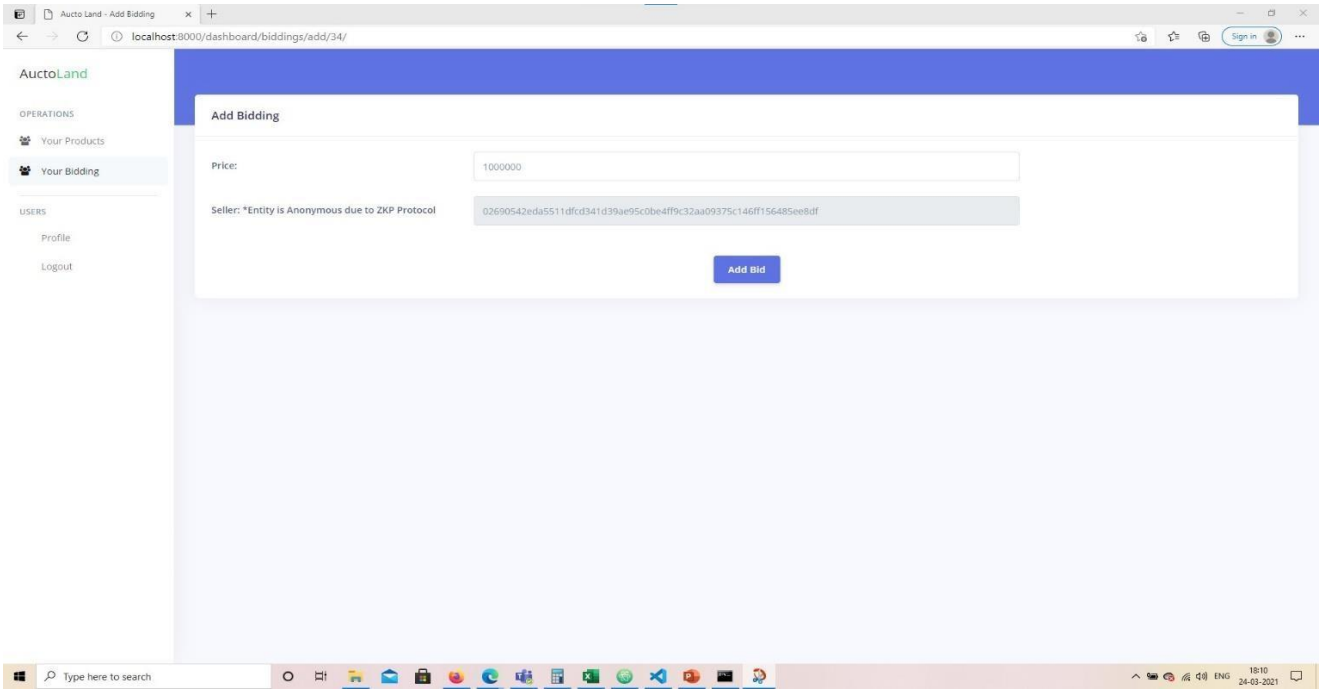


10. Products Display (Buyer)

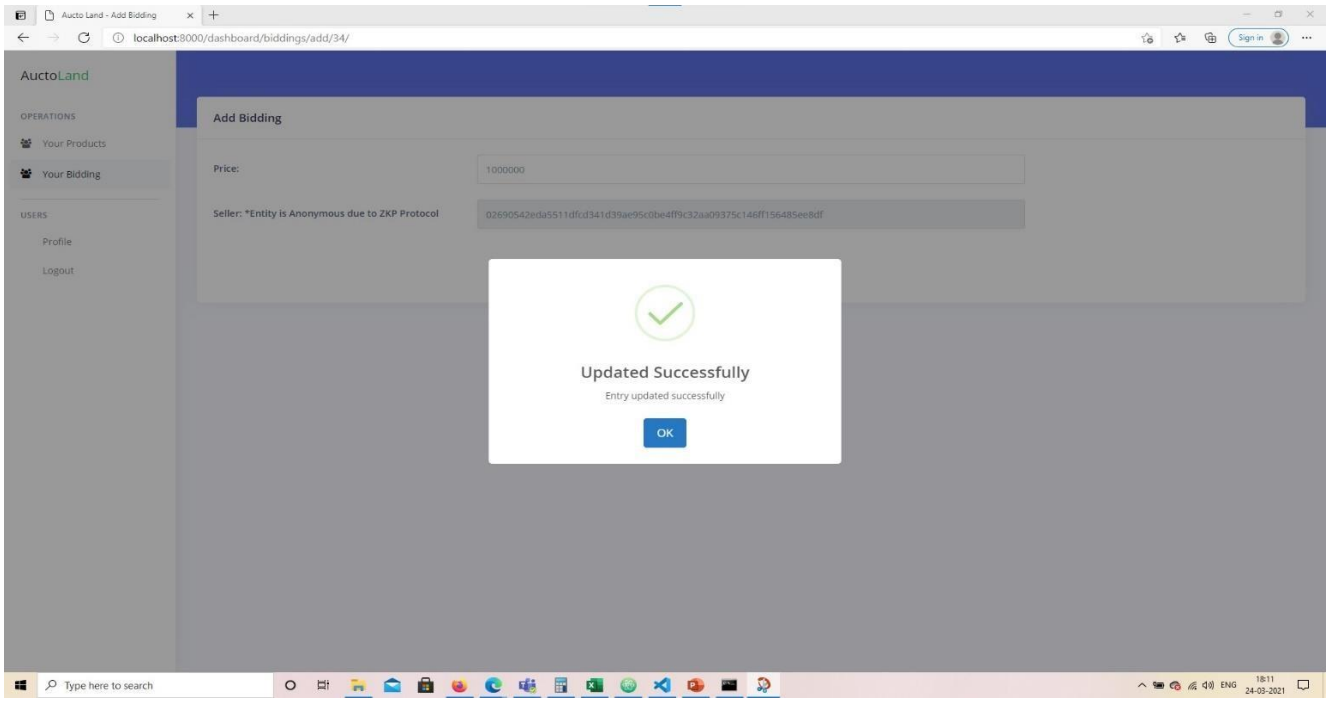


11. Products Bidding (Buyer)

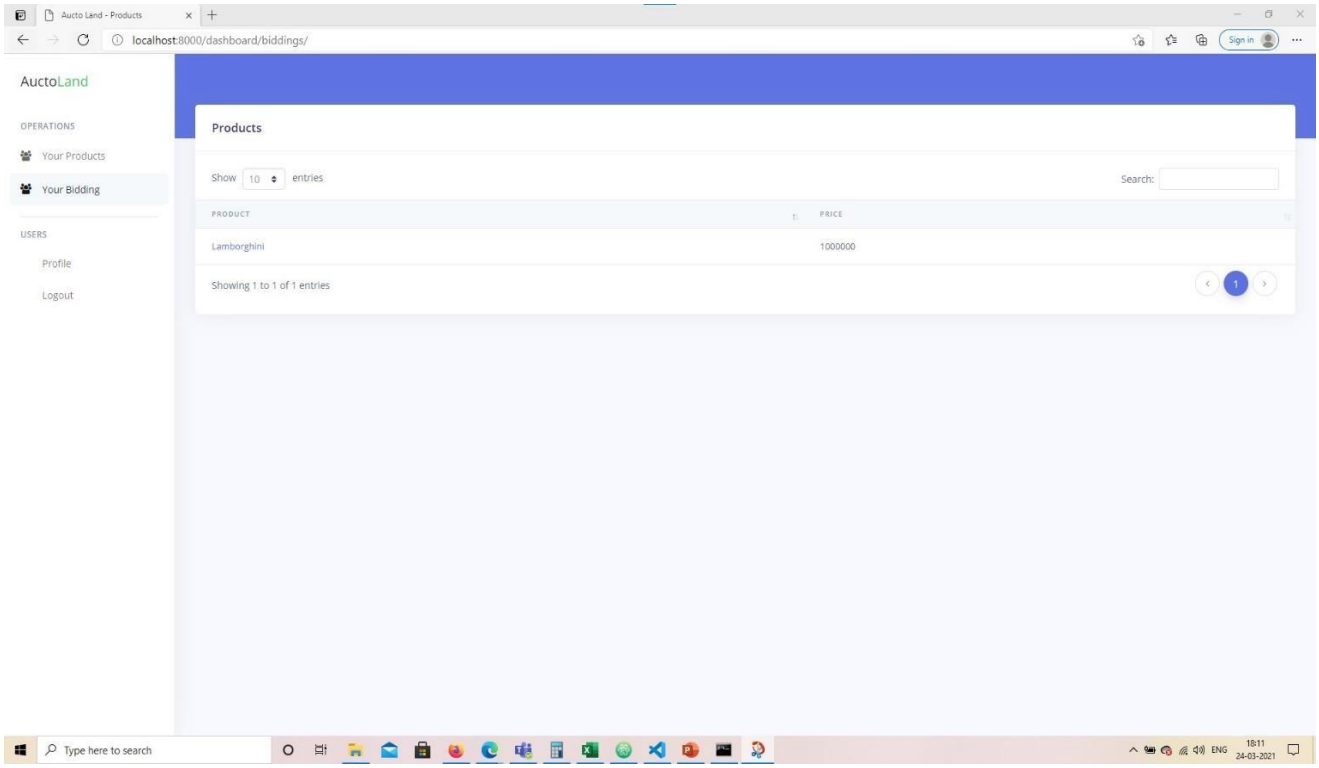




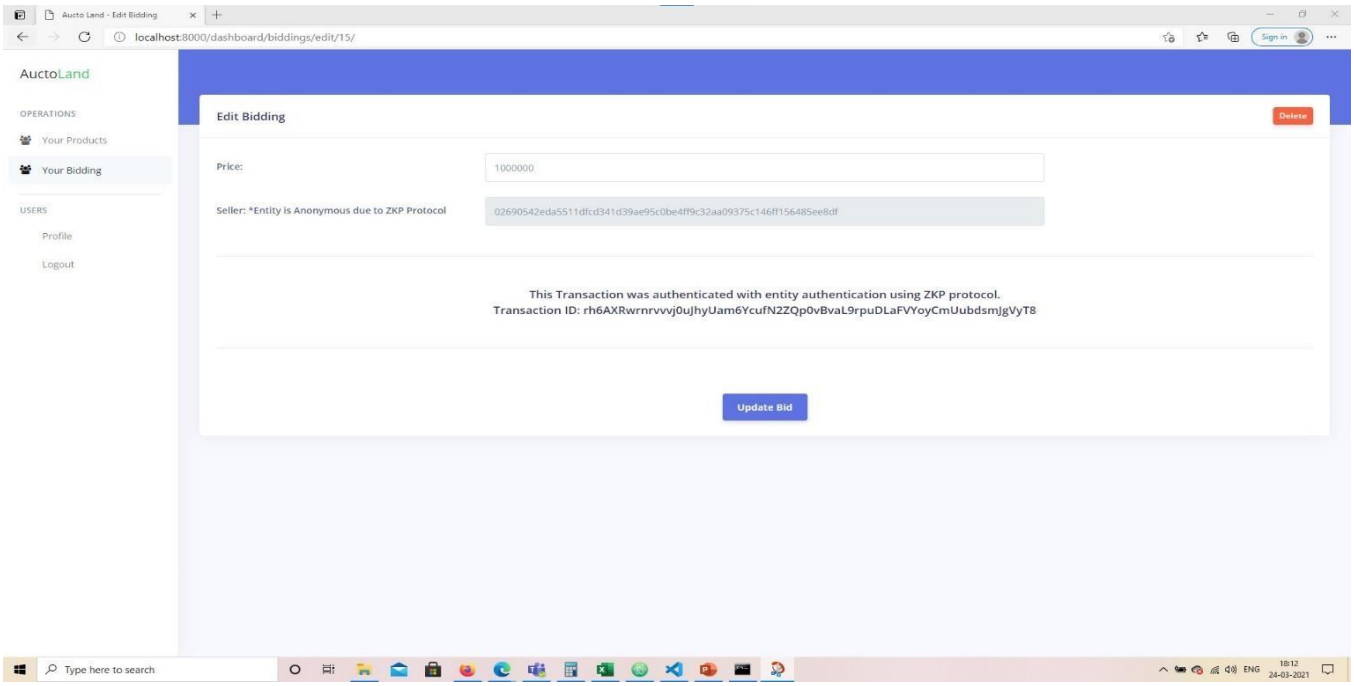
12. Product Bidding (Buyer)



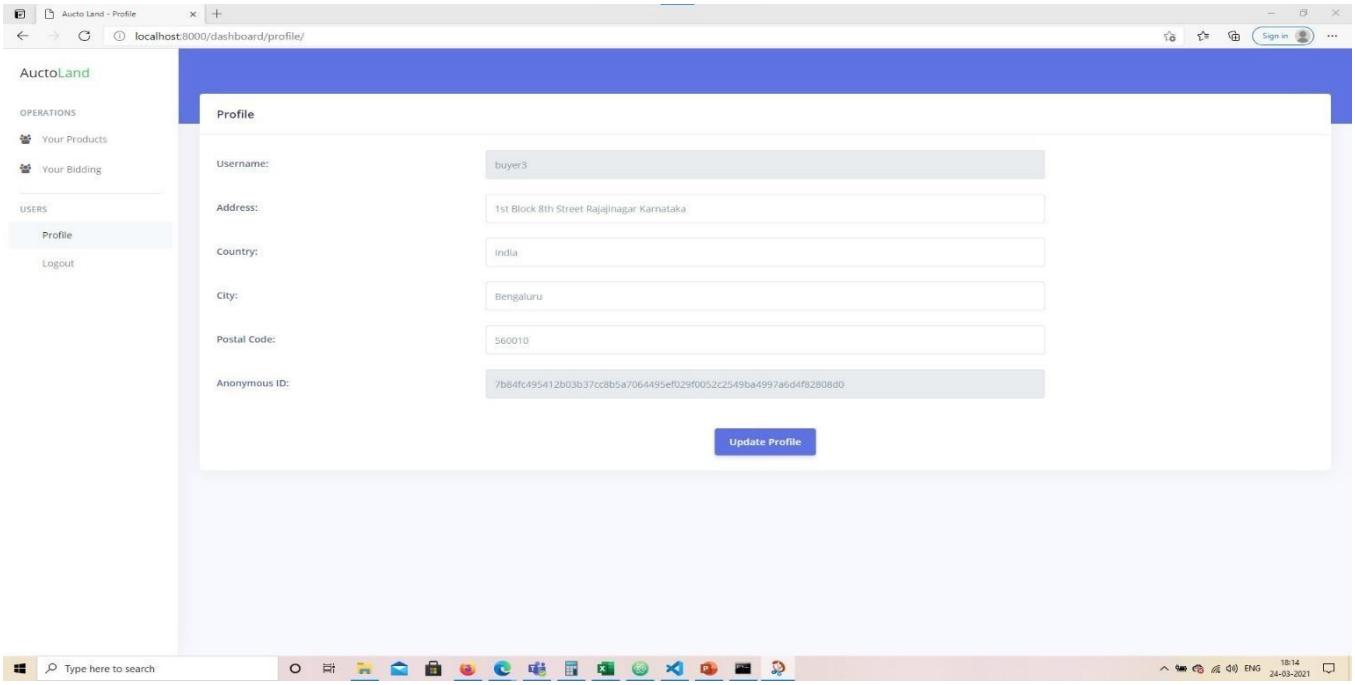
13. Product Bid Information (Buyer)



14. Entity Authentication (Buyer)



15. User Anonymity (Buyer)



BACK TO INDEX

CHAPTER 9

TEST PLAN AND STRATEGY

UI-licious Testing Tool

UI-licious software testing tool can monitor the application for defaults so that the clients using the software can rectify those defaults and launch their application faster.

UI-licious can be used on any front-end applications and supports all major browsers, such as Chrome, Firefox, Safari and Internet Explorer.

Test No.	Test Name	Test Type	Case	Role	Expected Outcome	Final Outcome
1	User Login	Unit Test	Positive	Aditya	Displaying home page on successful login	Displaying home page on successful login
2	User Registration & Login	Integration Test	Positive	Aditya	Successful user registration & login resulting in display of home page	Successful user registration & login resulting in display of home page
3	ZKP (Product Bidding)	System Test	Positive	Aditya & Nisha	Successful buyer authentication for bidding using ZKP	Successful buyer authentication for bidding using ZKP
4	User Registration	Unit Test	Negative	Nisha	User registration failed due to existing user in the system	User registration failed due to existing user in the system
5	User Login	Unit Test	Negative	Nisha	User login failed due to incorrect credentials	User login failed due to incorrect credentials
6	User Registration & Login	Integration Test	Negative	Aditya & Nisha	User login failed due to unregistered user resulting in non-existing template	User login failed due to unregistered user resulting in non-existing template
7	ZKP (Product Bidding)	System Test	Negative	Aditya & Nisha	Product bidding failed due to incorrect amount provided	Product bidding failed due to incorrect amount provided

Fig 2. Capstone Project Testing

BACK TO INDEX

CHAPTER 10

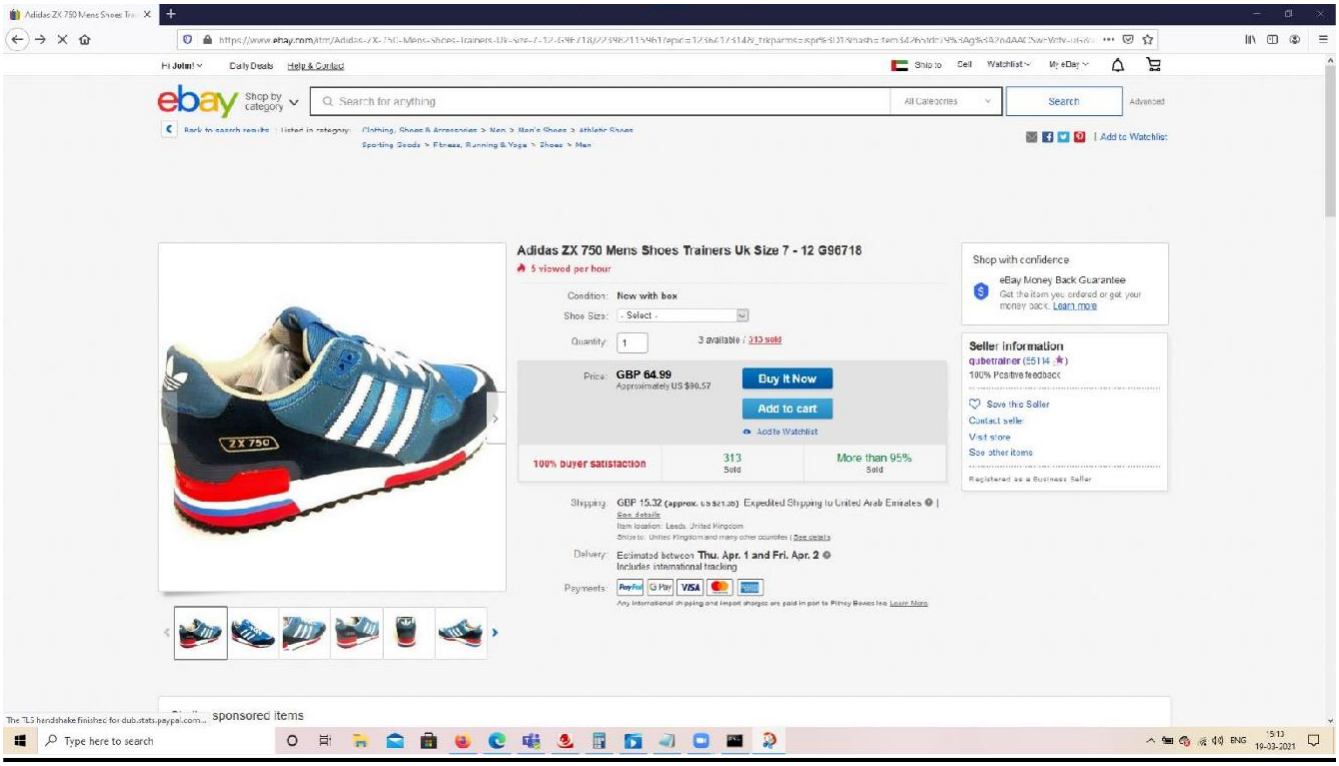
RESULTS AND DISCUSSION

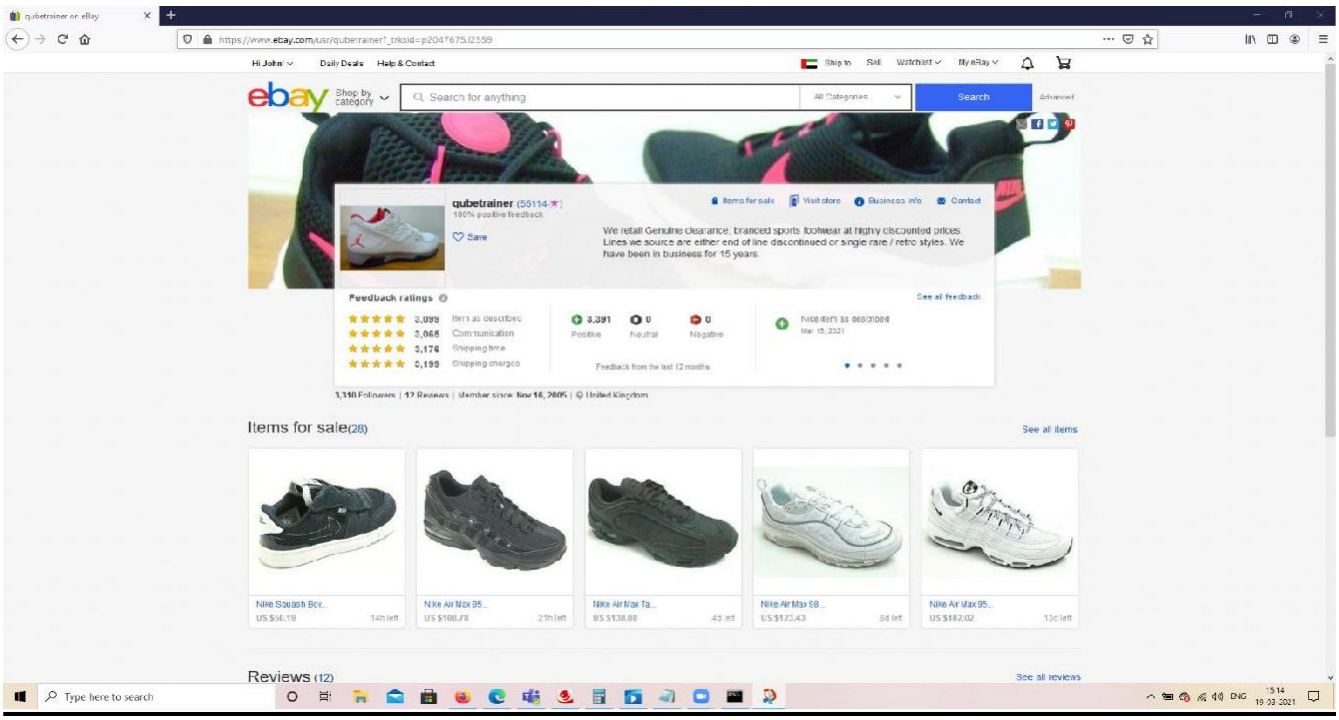
The user's details are obtained via a registration form. These details are encrypted using a hashing algorithm to generate a hash value. A random seed value (token) is generated by the server. The server's signature is obtained by generating a hash value using the server's token and the user's hash value.

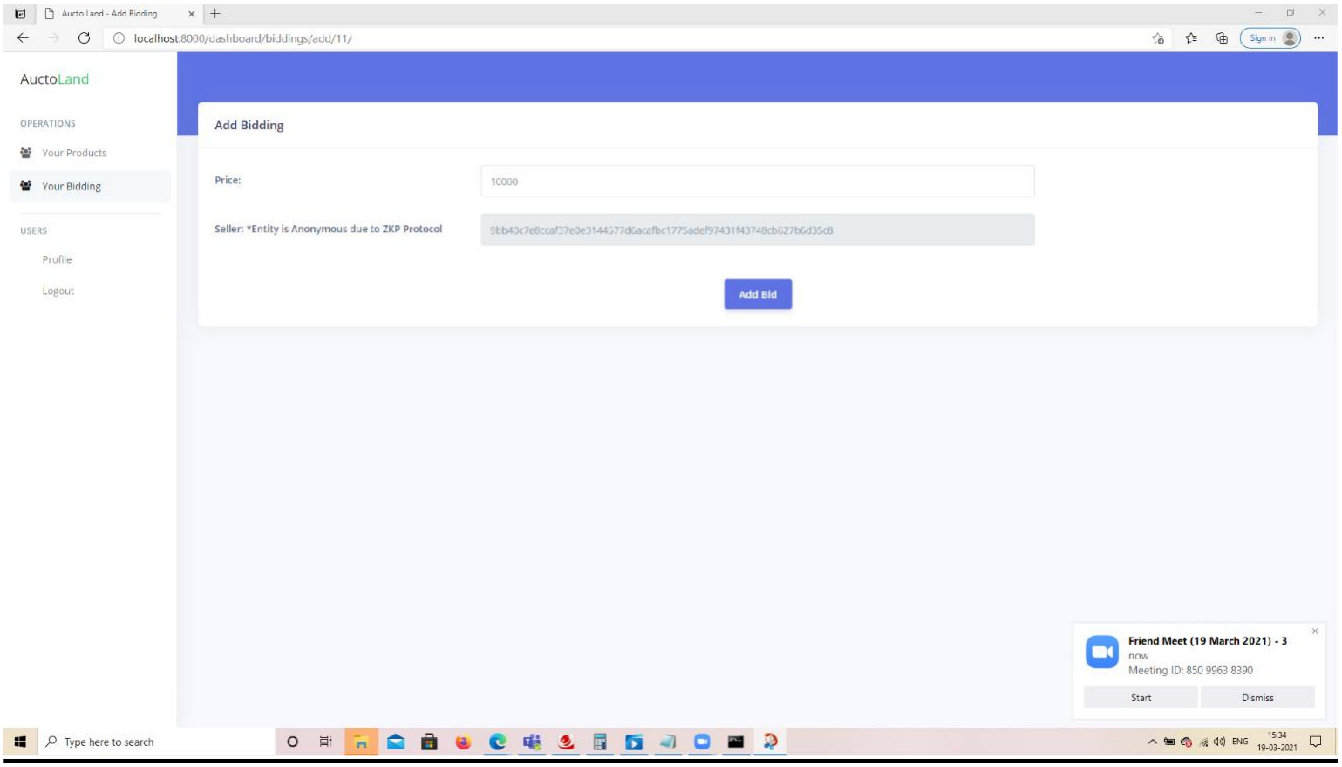
The user generates it's own signature by using the token received from the server along with the hash value of the seed phrase to generate a new hash value. The user and server signatures are compared. If the signatures match the user is allowed to participate in the bidding otherwise their request is discarded.

Expected Outcome	Final Outcome
8e2e914344e4793fc16769763c4e9192fc991bfecc9331f80e4aea40145278d2	8e2e914344e4793fc16769763c4e9192fc991bfecc9331f80e4aea40145278d2
240aa150573a4e2ca4a31055bbfd5af0299b94b2b1602ef3c656c8eda8c471af	240aa150573a4e2ca4a31055bbfd5af0299b94b2b1602ef3c656c8eda8c471af
feb51cb614f6dc71140c76806cf42bf5162e95b56d078a44229181824fd328c0	feb51cb614f6dc71140c76806cf42bf5162e95b56d078a44229181824fd328c0
f259909799cb654f05da047b07352f637bf4fe298b7c00bc96556d57eb975f8d	f259909799cb654f05da047b07352f637bf4fe298b7c00bc96556d57eb975f8d
152235943ac2fec914e378803f1291e6fe0be2e4fa6efb55358686942e582869	152235943ac2fec914e378803f1291e6fe0be2e4fa6efb55358686942e582869

Novelty of the Project







BACK TO INDEX

CHAPTER 11

CAPSTONE PROJECT TIMELINE (PHASE-1 & PHASE-2)

PHASE 1 (AUG 2020 – DEC 2020)

SL.NO	PHASE	ACTUAL HOURS	START DATE	END DATE	STATUS
1	Extensive Literature Survey	3-4 hrs / day	26-Aug-2020	24-Sep-2020	Completed
2	Problem Statement	2-3 hrs / day	25-Sep-2020	21-Oct-2020	Completed
3	Making Hypothesis	3-4 hrs / day	22-Oct-2020	17-Nov-2020	Completed
4	Research Design	3-4 hrs / day	18-Nov-2020	14-Dec-2020	Completed
5	Demo/Evaluation	2 hrs	15-Dec-2020	23-Dec-2020	Completed

PHASE 2 (JAN 2021 – MAY 2021)

SL.NO	PHASE	ACTUAL HOURS	START DATE	END DATE	STATUS
1	ZKP Implementation	7-8 hrs / day	16-Feb-2021	28-Feb-2021	Completed
2	Backend Implementation	3-4 hrs / day	1-Mar-2021	10-Mar-2021	Completed
3	Frontend and Backend Integration	2-3 hrs / day	11-Mar-2021	16-Mar-2021	Completed
4	Test Plan and Test Cases	4-5 hrs / day	17-Mar-2021	20-Mar-2021	Completed
5	Project Report Preparation	3-4 hrs / day	21-Mar-2021	26-Mar-2021	Completed
6	IEEE Paper Preparation	3-4 hrs / day	21-Mar-2021	26-Mar-2021	Completed
7	Project Evaluation	2 hrs	1-May-2021	9-May-2021	In Progress

BACK TO INDEX

CHAPTER 12

CONCLUSION OF CAPSTONE PROJECT PHASE-1

The proposed capstone project phase-1 concludes with the creation of a front end website for auctions. The sole purpose of our project is to ensure secure bidding in an online platform. This project has helped us understand zero knowledge proof and its various concepts.

The website which has been created is user-friendly and interactive in order to provide the users accessing the website i.e. buyers and sellers a seamless experience. The presence of database makes it easier to control and maintain the data by the website administrator in order to ensure data availability and security.

BACK TO INDEX

CHAPTER 13

CONCLUSION OF CAPSTONE PROJECT PHASE-2

The proposed capstone project phase-2 concludes with the implementation of Zero Knowledge Proof (ZKP) protocol using SCEP curve in order to ensure secure online auctions. Simple Certified Enrollment Protocol (SCEP) is a curve which follows a client-server model where multiple clients participate in online auctions based on the server authentication. Since, SCEP curve is used it helps to ensure entity authentication and anonymity.

The various types of testing such as unit, integration and system testing were performed for both positive and negative cases in order to determine system functionality.

BACK TO INDEX

CHAPTER 14

FUTURE WORK

Identity Verification

Identity verification is the future work that can be done on ZKP based online auctions. Currently, anonymity is maintained on the basis of user's details in the form of a hash value, however, the user's profile is not verified for the details provided by the user.

BACK TO INDEX

REFERENCES / BIBLIOGRAPHY

[1] Ben Palmer, Kris Bubendorfer, Ian Welch, “A protocol for verification of an auction without revealing bid values”, 2012.

[2] Luiz Thomaz do Nascimento, Sapna Kumari, Vedavinayagam Ganesan, “Zero knowledge proofs applied to auctions”, 2019.

[3] Hisham S. Galal and Amr M. Youssef, “Verifiable Sealed-Bid Auction on the Ethereum Blockchain”, 2018.

[4] Chaya Ganesh, Yashvanth Kondi, Arpita Patra and Pratik Sarkar, “Efficient Adaptively Secure Zero-knowledge from Garbled Circuits”, 2018.

[5] Jose A. Montenegro, Michael J. Fischer, Javier Lopez, Rene Peralta, “Secure Sealed-Bid Online Auctions Using Discreet Cryptographic Proofs”, 2011.

[6] Felix Brandt and Tuomas Sandholm, “Efficient Privacy-Preserving Protocols for Multi-unit Auctions”, 2005.

[7] Anunay Kulshrestha, Akshay Rampuria, Matthew Denton and Ashwin Sreenivas, “Cryptographically Secure Multiparty Computation and Distributed Auctions Using Homomorphic Encryption”, 2017.

[8] Dimitris Bertsimas, Jeffrey Hawkins, Georgia Perakis, “Optimal Bidding in Online Auctions”, 2002.

[9] Yehuda Lindell and Benny Pinkas, “An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries”, 2007.

[10] Aner Ben-Efraim, Yehuda Lindell and Eran Omri, “Optimizing Semi-Honest Secure Multiparty Computation for the Internet”, 2016.

[11] Samuel Dittmer, Yuval Ishai and Rafail Ostrovsky, “Line-Point Zero Knowledge and Its Applications”, 2020.

[12] Elette Boyle, Niv Gilboa, Yuval Ishai and Ariel Nof, “Efficient Fully Secure Computation via Distributed Zero-Knowledge Proofs”, 2020.

[13] Yehuda Lindell, “Secure Multiparty Computation [MPC]”, 2020.

[14] Yehuda Lindell, Ariel Nof, Samuel Ranellucci, “Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody”, 2018.

[15] Trondheim, “Realizing Secure Multiparty Computations”, 2009.

[16] Yuval Ishai, Manika Mittal and Rafail Ostrovsky, “On the Message Complexity of Secure Multiparty Computation”, 2018.

[17] Koji Chida, Daniel Genkin, Koki Hamada, Dai Ikarashi, Ryo Kikuchi, Yehuda Lindell and Ariel Nof, “Fast Large-Scale Honest-Majority MPC for Malicious Adversaries”, 2018.

[18] Gowthaman A, M Sumathi, “Performance Study of Enhanced SHA-256 Algorithm”, 2015.

BACK TO INDEX

APPENDIX A: DEFINITIONS AND ABBREVIATIONS

Abbreviations	Definitions
ZKP	It is a protocol in which one party proves authenticity of knowledge to another party without revealing the essential information.
Simple Certified Enrollment Protocol (SCEP)	Simple Certified Enrollment Protocol (SCEP) is a curve which follows a client-server model where multiple clients participate in online auctions based on the server authentication.
SHA256	SHA-256 is one of the successor hash functions to SHA-1 and is one of the strongest hash functions. It is computed with 64-bit words.

BACK TO INDEX