Zero Knowledge Proof for Online Auctions

Aditya Muraleedharan Nair
Department of CSE
PES University
Bengaluru 560085, India
Email id : adikc.pes@gmail.com

Rajashree S
Assistant Professor
Department of CSE
PES University
Bengaluru 560085, India
Email id: rajashrees@pes.edu

Nisha Nemasing Rathod
Department of CSE
PES University
Bengaluru 560085, India
Email id : rathodnisha6688@gmail.com

Prasad B Honnavali
ISFCR Head
Department of CSE
PES University
Bengaluru 560085, India
Email id: prasadhb@pes.edu

***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.

Keywords*—*Zero Knowledge Proof (ZKP), Simple Certificate Enrollment Protocol (SCEP), Secure Hashing Algorithm (SHA).

I. 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.

II. 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.

III. LITERATURE SURVEY

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

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.

B. On the Message Complexity of Secure Multiparty Computation

This paper is based on the study of the minimal number of point-to-point messages required for general secure multi-party 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.

C. Fast Large-Scale Honest-Majority MPC for Malicious Adversaries

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 included 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.

D. A protocol for verification of an auction without revealing bid values

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.

E. Optimal Bidding in Online Auctions

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 behavioral 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.

F. Zero knowledge proofs applied to auctions

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:

4. Setup phase
5. Bidding phase
6. Proof phase
7. 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.

G. Verifiable Sealed-Bid Auction on the Ethereum Blockchain

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.

H. Efficient Privacy-Preserving Protocols for Multi-unit Auctions

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.

I. Cryptographically Secure Multiparty Computation and Distributed Auctions Using Homomorphic Encryption

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

J. Performance Study of Enhanced SHA-256 Algorithm

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.

IV. SYSTEM REQUIREMENTS SPECIFICATION

A. 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.

B. 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

C. 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.

D. System Features

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

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

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

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

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

E. Operating Environment

i. Operating System Platform: Windows

ii. Web Framework Platform: Django

iii. RDBMS Platform: Sqlite3

iv. Programming Language: Python

F. 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.

G. 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.

H. Non-Functional Requirements

Security Features

i. 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.

ii. 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.

I. Software Quality Features

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

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

iii. 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.

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

V. SYSTEM DESIGN

A. The website will comprise of the following webpages:
   i. Home page.
   ii. Products page.
   iii. Categories page.
   iv. Registration page.
   v. Login page.

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

C. 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.

D. 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.

E. 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.

F. 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.

G. 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.

H. 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.

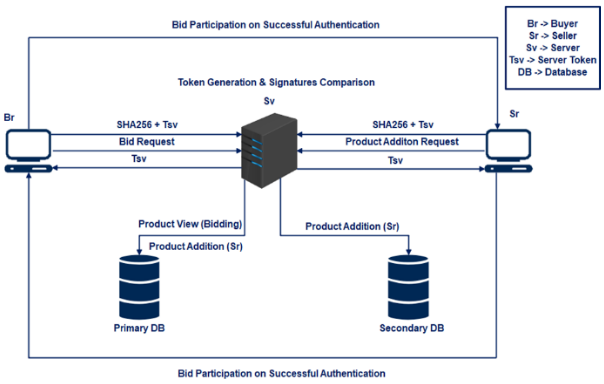


Fig 1. Online Auction System Design

VI. IMPLEMENTATION AND PSEUDOCODE

A. 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 generate a token for its seed phrase 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.

B. 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
```

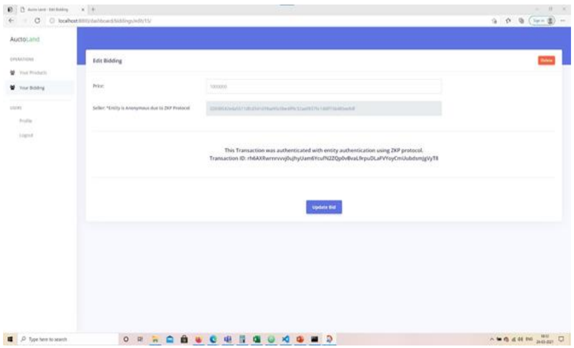
C. Pseudocode (SHA256)

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).

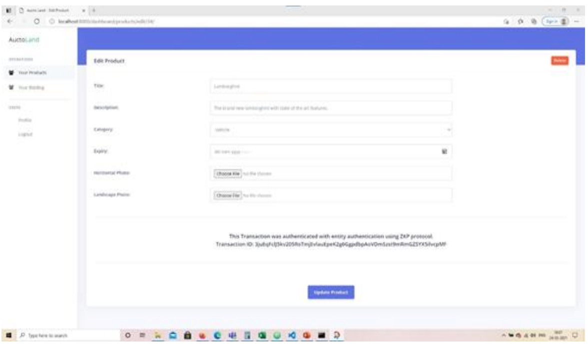
VII. PROJECT DEMONSTRATION

A. Entity Authentication

i. Buyer

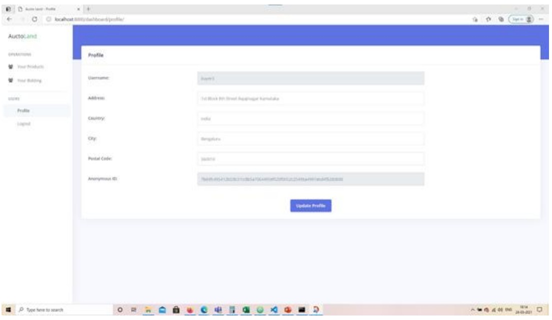


ii. Seller

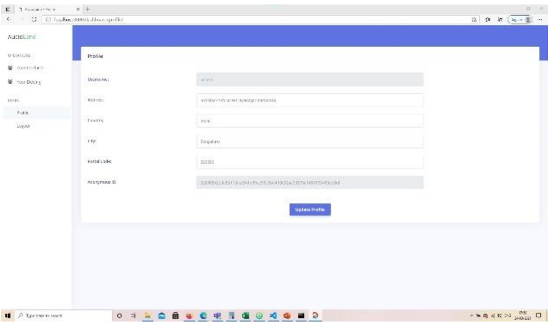


B. User Anonymity

i. Buyer



ii. Seller



VIII. 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

IX. RESULTS AND DISCUSSION

i. 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.

ii. The user generates its 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

iii. Novelty of the Project

The novelty of our project lies in Zero Knowledge Proof (ZKP) which is achieved using entity authentication and user anonymity. The random anonymous id generated using the users profile information provided during the registration process is used to ensure anonymity by which the users can engage in online auction without revealing their profile information. The entity authentication is ensured using a randomly generated transaction id which verifies the user's identity participating in online auction.

X. CONCLUSION AND FUTURE WORK

The sole purpose of our project is to ensure secure bidding in an online platform. The front end is a user-friendly and interactive website which provides the users i.e., buyers and sellers accessing the website a seamless experience. The presence of a database makes it easier to control and maintain the data by the website administrator in order to ensure data security and availability.

Zero Knowledge Proof (ZKP) protocol using SCEP curve is implemented 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 of these clients. SCEP curve is used to ensure entity authentication and anonymity.

The various types of testing such as unit, integration and system testing for both positive and negative cases help to determine the system functionality.

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 profile information in the form of a hash value, however, the user's profile is not verified for the details provided by the user.

FIGURES AND TABLES

TABLE I. LIST OF FIGURES

Figure No.	Title
1	Online Auction System Design

REFERENCES

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

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

[3] 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.

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

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

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

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

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

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

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