IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025

DOI: 10.17148/IJARCCE.2025.14434

Secure Online Auction System

Pratiksha Nikalje[1], Pragati Randive[2], Shabana Machkuri[3]

Final Year Student, Department of Computer, Al Ameen College of Engineering, Pune, India[1]

Final Year Student, Department of Computer, Al Ameen College of Engineering, Pune, India[2]

Final Year Student, Department of Computer, Al Ameen College of Engineering, Pune, India[3]

Abstract: The rise of e-commerce has made online auctions increasingly popular, but existing systems often lack robust security measures. Vulnerabilities like data breaches, unauthorized bidding, and manipulation are prevalent in traditional platforms. This paper introduces a cryptographically enhanced online auction system that ensures bid confidentiality, user authentication, and overall fairness. By integrating AES encryption, SHA-256 hashing, and role-based access control, the system guarantees the integrity of auction operations. A detailed security analysis compares our model with existing solutions, showcasing its effectiveness in addressing the security concerns of digital auction environments.

Keywords: Secure Auction, Cryptography, Data Integrity, Bid Confidentiality, Online Bidding System.

I. INTRODUCTION

Online auctions provide a competitive and flexible way for buyers and sellers to engage in real-time transactions. However, many existing systems are vulnerable to security risks, including bid tampering, identity theft, and session hijacking. This paper proposes a secure auction system that integrates advanced cryptographic techniques to enhance fairness, trust, and transparency in the auction process.

II. LITERATURE REVIEW

Numerous models have been proposed to improve the security of online auctions. Kumar et al. [3] introduced a cryptographic approach focusing on bid privacy but lacked user role management and secure result evaluation. Reddy et al. [4] developed a web framework for validating auction results, though they did not incorporate bid encryption. Sharma and Patel [5] proposed a blockchain-based model for immutable bid storage, albeit with a higher computational cost. Gupta and Mehta [6] employed multi-factor authentication and biometric verification to improve access control.

While these models address certain security issues, none offer a comprehensive solution that covers bid confidentiality, data integrity, and user authentication. This paper builds upon these approaches and presents a holistic security model for online auctions.

III. SYSTEM FUNCTIONALITY

A. User Roles

The system supports three user roles:

- Admin: Manages platform operations and validates users.
- Seller: Lists items for auction and manages auction parameters.
- Buyer: Places bids during active auctions.

B. Authentication Mechanism

User credentials are secured using SHA-256 password hashing. To further protect user accounts, the system supports email verification and will integrate two-factor authentication (2FA) in future versions.

C. Auction Configuration

Sellers define auction parameters such as item description, base price, and auction timings. Auctions are automatically initiated based on the system's internal clock.

D. Encrypted Bidding Process

Each bid is encrypted using AES encryption before submission. Bids are stored securely and remain confidential until the auction ends.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 4, April 2025
DOI: 10.17148/IJARCCE.2025.14434

E. Auction Closure and Result Publication

After the auction concludes, the highest bid is determined by decrypting and sorting the submitted bids. Notifications are then securely sent to the winner and other participants.

IV. TECHNICAL SPECIFICATIONS

Module	Technology Stack
Frontend	HTML5, CSS3, JavaScript, React.js
Backend	Node.js, Express.js
Database	MongoDB
Security	JWT (JSON Web Tokens), Bcrypt, HTTPS, Helmet.js
Deployment	Vercel / Netlify (Frontend), Render / Railway / Heroku / AWS (Backend + DB)

V. COMPARATIVE ANALYSIS

Feature	Existing Systems	Proposed System
Encrypted Bidding	✗	✓
Secure Authentication	Partial	✓
Bid Confidentiality	✗	✓
Role-based User Management	✗	✓
End-to-End Data Integrity	✗	✓

VI. SECURITY REVIEW

The proposed system integrates multiple security measures to address common vulnerabilities:

- **Confidentiality**: AES encryption ensures that bid data remains private.
- **Integrity:** SHA-256 hashing and secure timestamping safeguard data integrity.
- **Authentication**: Passwords are securely hashed using SHA-256, preventing unauthorized access.
- **Authorization:** The system supports role-based access, ensuring that users only have access to the necessary functionalities.
- **Input Validation:** The system is designed to prevent SQL injection, XSS attacks, and other common exploits.

VII. FUTURE ENHANCEMENTS

Future developments include:

- Integration of blockchain technology to ensure immutable bid records.
- Support for anonymous bidding through zero-knowledge proofs.
- Biometric authentication for enhanced user verification.
- Implementation of real-time bidding analytics and fraud detection mechanisms.

VIII. CONCLUSION

This paper presents a secure online auction system that addresses the security flaws found in existing platforms. By combining cryptographic techniques such as AES encryption, SHA-256 hashing, and role-based access control, the system ensures bid confidentiality, user authentication, and data integrity. Comparative analysis demonstrates its superiority over existing systems, making it a viable solution for modern e-auction applications.

REFERENCES

[1]. B. Schneier, Applied Cryptography, Wiley, 1996.
[2]. W. Stallings, Cryptography and Network Security, Pearson, 2017.
[3]. A. Kumar, "Online Auction Security using Cryptographic Algorithms," IJCA, vol. 95, no. 12, pp. 21–26, 2022.
[4]. M. Reddy, "Secure Web-based Auction Framework," International Journal of E-Commerce, vol. 8, no. 3, pp. 40–47, 2021.
[5]. R. Sharma and D. Patel, "Blockchain-Based Bidding Systems for Transparency," Journal of Decentralized Applications, vol. 12, no. 4, pp. 33–39, 2023.
[6]. P. Gupta and S. Mehta, "Enhanced Auction Security Using Multi-Factor Authentication," Cybersecurity Transactions, vol. 10, no. 2, pp. 15–22, 2022.

