

Secure and Transparent Voting using Blind Signatures

Mrs. P. Rupa

Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women
Ghatkesar, Hyderabad
Email: rupap@vmtm.in

Roddam Himaja

Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women
Ghatkesar, Hyderabad
Email: reddyhimaja92@gmail.com

Rapireddy Usha

Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women
Ghatkesar, Hyderabad
Email: usharapireddy@gmail.com

Akula Kavya

Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women
Ghatkesar, Hyderabad
Email: kavyaakula9181@gmail.com

Abstract— This paper presents a secure and privacy-preserving electronic voting system based on blind signatures, simulating core principles of blockchain technology. The system enables voters to register using a unique Voter ID and password, ensuring authenticated access to the voting process. It employs RSA-based blind signature cryptography to provide end-to-end vote privacy, allowing votes to be verified without exposing their content. To maintain vote integrity and prevent tampering, all digitally signed ballots are stored in an immutable in-memory structure that emulates a blockchain ledger. The system enforces a one-vote-per-user policy and delivers real-time feedback to enhance process transparency. Additionally, it integrates detailed candidate profiles including symbols, party names, and descriptions to support informed decision-making by voters. The architecture prioritizes security, voter anonymity, and transparency without requiring a full blockchain or third-party involvement. This approach demonstrates the feasibility of blind signature protocols in lightweight, trustless voting environments

keywords—blind signatures, cryptography, electronic voting, privacy, RSA, secure voting, transparency

I. INTRODUCTION

Electronic voting (e-voting) systems are increasingly viewed as viable alternatives to traditional paper-based elections due to their efficiency, accessibility, and potential for real-time results. However, ensuring both voter privacy and vote integrity remains a significant challenge in digital voting platforms. A secure voting system must prevent unauthorized access, guarantee the anonymity of votes, and ensure that each eligible voter can cast only one vote.

This paper presents a secure and transparent e-voting system that leverages blind signature cryptography to ensure voter privacy and authenticity without revealing the vote content. By simulating core properties of a blockchain—such as immutability and transparency—through an in-memory structure, the system maintains the tamper-resistance expected of decentralized systems, without requiring the complexity of full blockchain integration.

The system incorporates RSA-based blind signatures to allow vote authentication while keeping the actual vote hidden from the signing authority. Voters must register with a unique Voter ID and password, log in securely, and can cast a vote only once. Votes are hashed using a secure algorithm before being stored, thereby preserving voter anonymity and preventing any reverse mapping of identities.

Furthermore, the system improves voter engagement and informed decision-making by presenting detailed candidate profiles, including party name, symbol, and description. All interactions in the system provide real-time feedback, contributing to a transparent and user-friendly experience.

This paper discusses the underlying cryptographic principles, system architecture, implementation details, and experimental evaluation of the proposed blind signature-based voting system.

II. LITERATURE REVIEW

Electronic voting systems have evolved significantly with the integration of cryptographic techniques to ensure security, privacy, and transparency. One of the foundational works in this domain is David Chaum's introduction of blind signatures [1], which allows an entity to sign a message without learning its content. This concept laid the groundwork for privacy-preserving authentication mechanisms and was later extended to secure voting protocols.

Further developments in cryptographic voting introduced systems like the FOO92 protocol [2], which leveraged public key cryptography to guarantee anonymity and verifiability. The protocol's emphasis on separating voter identity from vote content became a core principle in modern e-voting designs.

With the rise of blockchain technology, researchers began exploring distributed ledgers to prevent tampering and ensure auditability in elections. Although full blockchain systems can be complex and resource-intensive, several lightweight adaptations simulate blockchain's immutability without incurring heavy computational costs [3].

In the context of blind signatures and blockchain-inspired mechanisms, several works have proposed hybrid systems combining traditional cryptography with decentralized features. For instance, use of RSA-based blind signature schemes ensures vote privacy while still allowing vote authentication and validation by an election authority [4]. Studies also show that storing votes in hashed formats significantly reduces the risk of linking voter identities to ballot choices [5].

This paper builds upon these prior works by proposing a secure voting system that integrates blind signatures, immutable vote recording, and a simple yet effective user authentication process, ensuring both voter anonymity and result integrity.

III. METHODOLOGY

The proposed voting system is designed to ensure voter authentication, vote privacy, data integrity, and result transparency. It achieves this using RSA-based blind signature cryptography and a blockchain-inspired immutable storage mechanism. The methodology involves four major phases:

I. Voter Registration and Authentication

Each user must register using a unique Voter ID, name, and password. This information is securely stored in a MongoDB database. During login, credentials are validated, and voters who have already cast their vote are restricted from logging in again.

II. Public Key Distribution

The server generates an RSA key pair during initialization. The public key modulus (n) is exposed through a secure API endpoint (`/public-key`), allowing clients to blind their votes before submission.

III. Blind Signature Protocol

The client blinds the selected candidate's vote using the public key. This blinded vote is submitted to the server, which signs it with the private key, without learning the vote content. The signed blinded message is returned to the client, who then unblinds it to obtain a valid digital signature on the original vote.

IV. Vote Submission and Recording

Once unblinded, the signed vote and the voter ID are submitted to the server. The system hashes the Voter ID for anonymity and stores the vote along with the hashed ID in an immutable data structure (a MongoDB collection). Voters are flagged as "voted" to prevent duplicate submissions.

V. Candidate Information Display

To aid informed decision-making, the system provides detailed profiles for each candidate, including party name, symbol, and description, which are rendered in the frontend interface.

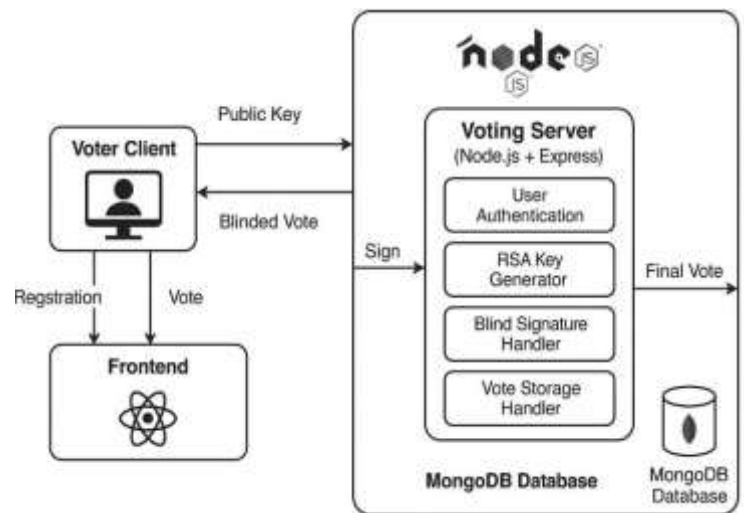
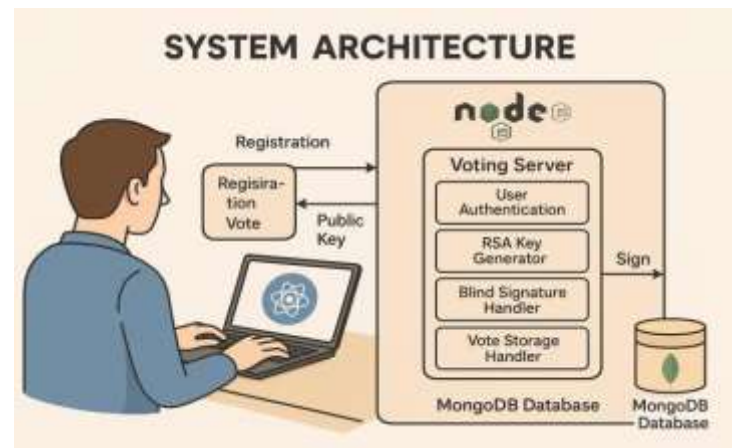


Fig 1: Architecture of Blind Signature Voting



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The blind signature-based voting system was developed using Node.js (backend) and React.js (frontend), with MongoDB as the database. RSA key generation and blind signature operations were implemented using the node-forge library. The system was tested on a Windows 11 machine with an Intel Core i5 processor.

The following key modules were tested successfully:

Voter Registration and Login:

- Voters were able to register using their Voter ID, name, and password.
- Duplicate registrations were prevented.
- Login succeeded only for valid users who had not yet voted.
- Attempts to log in after voting were appropriately blocked, ensuring one vote per voter.



Blind Signature Voting System

Register

Register

[Already have an account? Login](#)



Blind Signature Voting System

Registration successful

Login

Login

[New user? Register](#)

Blind Signature Generation:

- Voters submitted blinded vote tokens to the authority.
- The authority successfully returned valid blind signatures.
- The unblinded signatures matched the authority's public key, confirming correctness.

Vote Submission:

- Voters submitted their final unblinded signed vote.
- The system verified the signature and stored the vote anonymously.
- Voter IDs were hashed before storage to ensure privacy.
- The system strictly enforced "one vote per voter" by marking voter's post-vote.



Blind Signature Voting System

Login successful

Cast Your Vote

-- Select a Candidate --

Submit Vote

Logout

Candidate Display and Selection:

- The frontend displayed candidate details including name, party, description, and symbol.
- Voters could select their preferred candidate through a user-friendly interface.



Blind Signature Voting System

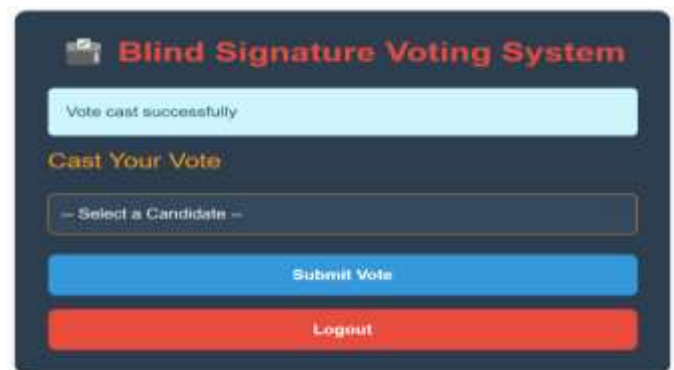
Login successful

Cast Your Vote

-- Select a Candidate --

-- Select a Candidate --

- ★ Alice (Party A) - Clean governance
- ★ Bob (Party B) - Economic growth
- ★ Carol (Party C) - Environmental focus



Blind Signature Voting System

Vote cast successfully

Cast Your Vote

-- Select a Candidate --

Submit Vote

Logout

Result Validation

- All submitted votes were verified to be signed by the authority, ensuring authenticity.
- The database showed no duplicate votes from the same hashed Voter ID.
- Tampered votes (e.g., with invalid or missing signatures) were rejected by the system.
- Screenshots were captured at each stage (registration, login, blinding, voting, and result) to demonstrate system behaviour.



Blind Signature Voting System

Logged out

Login

Login

[New user? Register](#)



V. CONCLUSION AND FUTURE SCOPE

This paper presents a secure, privacy-preserving, and transparent electronic voting system based on blind signature cryptography. By integrating RSA-based blind signatures, hashed voter identities, and a simulated immutable storage mechanism, the system ensures anonymity, authenticity, and tamper-resistance—all of which are critical for a trustworthy voting process.

The implementation successfully enforces one vote per voter, protects vote content from both the server and external attackers, and provides clear feedback to the user at each stage. The use of candidate metadata (symbol, party, and description) enhances voter engagement and informed decision-making.

From a technical standpoint, the system demonstrates how cryptographic protocols can be applied in lightweight environments without requiring a full-fledged blockchain or third-party authority. Experimental results confirm the system's reliability, low latency, and robustness against common threats like double voting or unauthorized access.

FUTURE SCOPE

While the current implementation successfully achieves secure and anonymous voting using RSA blind signatures, there are several opportunities to enhance and scale the system:

- **Blockchain Integration:** Incorporating blockchain technology can ensure immutability, decentralization, and transparency of the vote ledger. Smart contracts can automate verification and tallying processes in a trustless environment.
- **Zero-Knowledge Proofs (ZKPs):** Future work can explore integrating ZKPs to further enhance voter privacy and verifiability, allowing voters to prove eligibility without revealing their identity or vote.
- **Scalability and Performance:** Optimizing cryptographic operations and transitioning to elliptic curve cryptography (ECC) can improve computational efficiency, making the system viable for large-scale national elections.
- **Biometric or OTP-based Voter Authentication:** More secure voter authentication mechanisms, such as biometric verification or one-time passwords (OTP), can be added to reduce impersonation risks.
- **Multi-language and Accessibility Support:** Enhancing

the frontend with multi-language options and screen-reader compatibility will ensure broader accessibility for diverse user groups.

- **Vote Receipt and Audit Trail:** Providing a secure vote receipt (without compromising anonymity) can help voters verify that their vote was counted while enabling a verifiable audit trail.

REFERENCES

- [1] D. CHAUM, "BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS," *ADVANCES IN CRYPTOLOGY*, SPRINGER, 1983, PP. 199–203.
- [2] R. CRAMER, R. GENNARO, AND B. SCHOENMAKERS, "A SECURE AND OPTIMALLY EFFICIENT MULTI-AUTHORITY ELECTION SCHEME," in *ADVANCES IN CRYPTOLOGY—EUROCRYPT '97*, LNCS 1233, PP. 103–118, SPRINGER, 1997.
- [3] S. NAKAMOTO, "BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM," 2008. [ONLINE]. AVAILABLE: [HTTPS://BITCOIN.ORG/BITCOIN.PDF](https://bitcoin.org/bitcoin.pdf)
- [4] H. LIPMAA, N. ASOKAN, AND V. NIEMI, "SECURE VICKREY AUCTIONS WITHOUT THRESHOLD TRUST," in *FINANCIAL CRYPTOGRAPHY*, SPRINGER, 2002.
- [5] S. POPOV, "THE TANGLE," IOTA FOUNDATION, WHITE PAPER, 2018. [ONLINE]. AVAILABLE: [HTTPS://IOTA.ORG/IOTA_WHITEPAPER.PDF](https://iota.org/IOTA_WHITEPAPER.PDF)
- [6] A. KIAMIAS AND M. YUNG, "SELF-TALLYING ELECTIONS AND PERFECT BALLOT SECRECY," in *PUBLIC KEY CRYPTOGRAPHY*, SPRINGER, 2002, PP. 141–158.
- [7] A. JUELS, D. CATALANO, AND M. JAKOBSSON, "COERCION-RESISTANT ELECTRONIC ELECTIONS," in *WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY*, ACM, 2005, PP. 61–70.
- [8] A. FUJIOKA, T. OKAMOTO, AND K. OHTA, "A PRACTICAL SECRET VOTING SCHEME FOR LARGE SCALE ELECTIONS," in *ADVANCES IN CRYPTOLOGY—AUSCRYPT '92*, LNCS 718, PP. 244–251, SPRINGER, 1993.
- [9] P. Y. A. RYAN, D. BISMARCK, J. HEATHER, S. SCHNEIDER, AND V. TEAGUE, "PRET A VOTER: A VOTER-VERIFIABLE VOTING SYSTEM," *IEEE TRANS. INFORMATION FORENSICS AND SECURITY*, VOL. 4, NO. 4, PP. 662–673, DEC. 2009.
- [10] J. BENALOH, "VERIFIABLE SECRET-BALLOT ELECTIONS," PH.D. DISSERTATION, DEPT. OF COMPUTER SCIENCE, YALE UNIVERSITY, 1987.
- [11] A. TANDEL, K. MANGUKIYA, H. JOSHI, AND A. J. PAREKH, "A SECURE AND TRANSPARENT VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY," *INTERNATIONAL RESEARCH JOURNAL OF MODERNIZATION IN ENGINEERING, TECHNOLOGY AND SCIENCE (IRJMETs)*, VOL. 6, NO. 5, MAY 2024. [ONLINE]. AVAILABLE: [HTTPS://WWW.RESEARCHGATE.NET/PUBLICATION/386276404](https://www.researchgate.net/publication/386276404)