Abdul Huq, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science,
Engineering and Technology

An Open Access Journal

Secure Electronic Voting System

Abdul Huq, Ankit Pandey, Sonam Bajpai, Vinay Tiwari, Professor (Dr.) Sunil Dhore
Computer Engineering Army Institute of Technology
Pune, India

Abstract- The implementation of electronic voting systems presents the opportunity to enhance accessibility and efficiency in democracy. However, security matters such as authentication of voters, ensuring the integrity of votes cast, and protection against data tampering still pose serious problems. Voting car- ried out through paper ballots and centralized computerized voting systems suffer from voting fraud and manipulation of votes. This paper proposes a Secure Electronic Voting System which addresses these gaps and improves transparency and trust in elections. The system incorporates distributed storage, cryptographic hash functions, and multi-factor authentication. To guarantee the integrity of votes, cryptographic hash functions are incorporated to make them un-changeable. With multi-factor authentication, the authorized voters are verified. Utilization of blockchain technology for distributed storage protects the system from single point of failure. Voter information and confidentiality of vote is encrypted with AES and RSA, while tallying the votes is conducted through homomorphic encryption, enabling counting without decryption. The results of performance assessment showed that processing efficiency remains at a high level while enhancing security of the system significantly, thus creating the possibility for clear, verifiable and tamper-proof elections.

Keywords- E-voting System, Multifactor Authentication, Cryptography, Hashing, Distributed Storage, Security

I. INTRODUCTION

Civic engagement that pertains to participatory democracy revolves around citizens being informed of the electoral pro- cess and their ability to select their representatives to executive office positions, such as a president, governors, and so on. . . in a way that one person equals one vote secretively, freely, expressed without any intimidation or coercion.

Paper ballots accompanied by centralized electronic voting machines are faced with a myriad of issues ranging from voter masquerading to vote tampering. Hence, Electronic Voting Systems aim at addressing the problems arising from the traditional voting systems by streamlining and automating the multiple steps involved in casting and counting the votes. These systems offer an advancement with respect to the principles of direct, universal and unreserved, free elections.
E-Voting enables a standardized, centralized cataloguing of electoral information which can be swiftly processed digitally, thus poses an advantage with regard to time and costs. Com- puterization of these processes automatically results in easier, faster, and more accurate vote counting.

Along with the numerous advantages offered by E-Voting, E-Voting systems further present new restrictions to security. These new restrictions concerning security of e-voting range from the illegitimate sharing of privilege or accounts to the misuse of voter’s accounts wherein deceitful people can put in for votes without permission. Simply put, encryption measures have to be devised for the elector’s private information, as well as the voting information.

To address the security vulnerabilities in e-voting systems, there is a growing emphasis on employing advanced crypto- graphic techniques, multi-factor authentication, and distributed storage systems. These technologies are essential to ensure voter authentication, vote confidentiality, and data integrity.

II. RELATED WORK

[1] Satyander et al. (2019) proposed a multi-tier en- cryption model to secure data in electronic voting sys- tems. Combining Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) encryption, they sought to preserve the confidentiality and integrity of the votes and protect them from tampering. AES allows quick and effective data encryption, and RSA strengthens the security of the data by providing secure key exchange. Their studies proved that this approach is more resistant to unauthorized changes and brute-force attacks than single-layered encryption systems.

Pronika and Tyagi (2021) assessed the effectiveness of var- ious encryption algorithms such as Data Encryption Standard (DES), AES, RSA, and Blowfish on vote data and compared them. Their analysis used criteria such as the speed of en- cryption, the level of calculation required, and the strength of security. The study revealed that for voting, AES is the fastest and most efficient cipher while RSA is the most secure asymmetric encryption despite slower processing speeds.

Suwarjono et al. (2021) incorporated RSA cryptography into the security of their electronic voting system. They focused on identity masking and voter safeguarding through password hashing and asymmetric encryption to protect against online

breaches. They demonstrated the public-private key cryptog- raphy of RSA and how it ensures election confidentiality and integrity by limiting vote decryption to permitted key holders. The work of Tallapally and Manjula (2022) described the use of encryption in voting systems whereby votes can be aggregated without decrypting the individual votes. Such methods enable the election outcome to remain accurate while protecting the privacy of voters. Their research findings indicated that homomorphic encryption provides advanced security and transparency in voting systems for encrypted operations performed on private data.

Chen et al. (2022) studied the use of hash functions in the preservation of the voting integrity such as SHA-256. They explained how hashing creates a record of amounts where each vote cast possesses an identifiable digital fingerprint referred to as hash, which cannot be altered. Election security is also greatly strengthened because attempts of unauthorized changes will be readily detectable.

[2] Noor Ahmed and Pattanasetty's model makes use of distributed ledgers voting system which enables immutable storage of votes, eliminating the possibilities for centralized data breaches while also improving transparency and security. Their model focuses on the best practices of smart contracts for automation of vote validation, multiple voting prevention, and election audit accessibility in real time.

Xu and Zhao (2023) reviewed the role of blockchain and cryptographic security in voting systems. Their research high- lighted the differences between the application of distributed ledger technology (DLT) and centralised databases and con- cluded that with DLT, votes are less susceptible to tampering and cyberattacks. They suggested that hybrid models which combine blockchain with other layers of encryption technol- ogy would improve security and efficiency.

Chen et al. (2022) shed light on the use of homomorphic encryption in combination with blockchain for electronic vot- ing. Their results proved that such an implementation allows for vote counting whilst preserving voter anonymity as well

as preventing election fraud. This research highlighted the profound need for efficient scalable blockchain systems to cater for extensive elections.
Sun et al. (2023) investigated how blockchain technology can be scaled for voting systems. Although their analysis pointed out computational challenges and transaction speed concerns, security was not compromised. They suggested improvements with layer-2 scaling solutions like sharding and sidechains.

As with other traditional electronic voting systems that are maintained with a centralized database, there is a high risk of vote tampering, identity theft, and hacking. With blockchain, votes can be stored in a secure system that is virtually impossible to tamper with.

[3] Phatangare et. al added biometric verification to a multi- factor authentication (MFA) system, electing AES encryption and role-based access control (RBAC) to the administrative functions of e-voting. Their study established that MFA can mitigate the likelihood of identity theft and theft of voting rights. Also, RBAC can restrict access to records of votes, thus ensuring that only authorized users can access confidential information.

Wang and Liu (2023) devised an integrated authentication model that consists of biometric verification, one-time pass- words (OTP), and password authentication. Escalating fraud in voting is tied to people being assured that they will never be verified as voters. Their research indicated that the use of cryptographic hashing coupled with MFA systems adds more security.

Kim et al. (2022) developed a reliable voter authentica- tion method based on distributed identity verification. Their research indicated that the use of decentralized identity frame- works increases privacy and decreases centralized controlthus mitigating the chances of election fraud.

[4] While significant progress has been made in voting cryptography, implementing a secure electronic voting system still poses several unresolved issues. One of the more serious issues is resource consumption, especially with resource-heavy encryption techniques such as RSA and homomor- phic encryption. Such requirements may greatly diminish the scalability and effectiveness of the system, increasing the resources needed for real-time vote computation and delaying election processes. Another pressing issue is scalability. The low transaction throughput and high latency of traditional blockchain networks pose challenges for large scale election processes, particularly when the volume of votes reaches millions. National level elections are still difficult to manage in an effective manner without optimized blockchain scaling solutions like layer-2, sidechains or sharding techniques.

Adoption barriers pose challenges because voters do not have prior knowledge of cryptographic authentication and voting systems that are decentralized. The intricacy of these frameworks can hinder adoption, particularly among those lacking tech-savviness. Scholarship indicates that design in- terfaces that are simple and attractive, effective education materials for voters, and uncomplicated verification techniques foster smooth usability and adoption. The lack of public awareness and accessibility initiatives, no matter how secure and effective electronic voting technologies are, will work against public trust. Security and ease of use, as well as scalability, all this combined, determine the effectiveness and trustworthiness of electronic voting systems for all voters.

III. PROPOSED METHODOLOGY

Enhanced Secure Electronic Voting System

The proposed secure electronic voting system integrates several advanced security measures to establish a transparent, verifiable, and resilient electoral process. These measures are designed to address key vulnerabilities in traditional and electronic voting systems, ensuring integrity at each stage of the voting process.

Multi-Factor Authentication (MFA)

According to [3], Phatangare and their colleagues in 2024 report that MFA (Multi-Factor Authentication) is helpful in strengthening voter verification as well as preventing access by unauthorized users. MFA requires that voters must authenticate several times before they are allowed into the system. Such a system makes it almost impossible to commit identity theft and fraudulent voting.

Initial Registration: Voters are required to register with identifying information, which is securely stored.

Authentication Factors:

- **Knowledge Factor:** Something the voter knows, such as a password or PIN.
- **Possession Factor:** Something the voter has, like a One-Time Password (OTP) sent to their registered mobile device, or a smart card.
- **Inherent Factor:** Something the voter is, such as biometric data like a fingerprint or facial recognition.

Process:

- The voter enters their username and password.
- The system sends an OTP to the voter's registered mobile number.
- The voter enters the OTP to gain access.
- (Optional) The system may require an additional biometric scan for higher security elections.

Cryptographic Hash Functions

According to Chen et al. (2022) Cryptographic hash func- tions are used to ensure the integrity of votes and detect any unauthorized alterations. Hash functions generate a unique, fixed-size string of characters (a hash) from an input of arbitrary size. Any change to the input data, even a single bit, will result in a drastically different hash value.

- **Vote Hashing:** Each cast vote is passed through a crypto- graphic hash function (e.g., SHA-256). The resulting hash is stored on the blockchain, instead of the vote itself, to preserve privacy.
- **Integrity Verification:** After the election, the integrity of the votes can be verified by re-hashing the votes and comparing the new hash values with those stored on the blockchain. If the hashes match, it confirms that the votes have not been tampered with.

Multi-Level Encryption

To protect the confidentiality of voter data and the votes themselves, the system employs multi-level encryption.

This involves using multiple encryption algorithms to add layers of security.

- **AES for Vote Encryption:** The Advanced Encryption Standard (AES) is used to encrypt the vote data due to its efficiency in handling large amounts of data.
- **RSA for Key Encryption:** RSA is used to encrypt the AES keys, providing a secure way to manage the symmetric keys. RSA's strength lies in its use of key pairs (public and private keys).

Process:

- Each vote is encrypted using AES with a unique session key.
- The AES session key is encrypted using the RSA public key of the election authority.
- Additionally, the encrypted AES vote and key will be preserved in new containers overweight
- Only elections authorities with the RSA private key will be able to access the AES-SK and subsequently, the vote, where they will decrypt with the key.

This approach to layered encryption enhances the speed of symmetric encryption with the secure key management of asymmetric encryption (Phatangare et al., 2024).

Distributed Storage

The methodology employs a distributed encrypted database (not blockchain) to guarantee security, secrecy, and integrity of the stored votes. This technique provides safe and reliable storage and retrieval of votes, ensuring protection against alteration, tampering, and data breach.

This approach, as explained before, adopts a systematic step to enhance the system's overall efficiency and security.

Vote Recording in Encrypted Database: After a vote is cast, it is immediately encrypted using AES-256 and placed into a distributed secure database. The database record has a timestamp, hashed voter ID, and encrypted vote which ensure correct verification. This ways safe- guards the confidentiality of votes by ensuring that only qualified agencies are able to have access to them. Control and Role-Based Authorizations: The system incorporates role-based access control (RBAC) to prevent unwanted access or modification activities. The database is ac- cessible only to election officials who have the proper credentials, and are bound to the restrictions relevant to their rank.

In order to maintain confidentiality and ensure that no linkage can be made between a vote and the associating voter, voter identities are also separated from the votes.

Vote Security and Integrity Through Cryptographic Hash- ing: SHA-256 Each vote receives its own SHA-256 cryptographic hash, further increasing vote security. This hash value functions as the vote's immutable descriptor. In attempts to alter a vote, there will always be discrepancies between the hash values.Security measures confirm that all votes stored and verified during the election process remain unchanged.

Regular Data Backups Along With Replication: System operators schedule automatic database backups to miti- gate data loss and system failure. Moreover, all votes are always preserved and retrievable due to the presence of a distributed replica database which still functions when under server failures or cyber-attacks. This redundancy increases the electronic voting system's scalability and stability.

Process:

- Vote transactions, including voter ID (hashed) and vote hash, are recorded.
- Each transaction is matched before being used in the calculation.

This distributed storage approach significantly strength- – b7x7 + b6x6 + b5x5 + b4x4 + b3x3 + b2x2 + b1x + b0 = ens the security and resilience of the voting process [2]

n
i=0
bixi

Noor Ahmed Pattanasetty, 2024.

Privacy-Preserving Vote Tallying

The process described ensures the protection of voter pri- vacy as well as the accuracy in counting votes by allowing mathematical operations to be conducted on encrypted data. This is achieved through the use of homomorphic encryption. This methodology can be divided into several parts:

- **Encrypted Vote Processing:** Transformation of encrypted votes into useable readable formats is made possible through the process of homomorphic encryption, allowing mathematical operations to be conducted without revaal- ing the contents.
- **Secure Aggregation:** The private nature of election results is maintained by aggregating and processing of votes in an encrypted form which conceals their contents.
- **Decryption by Authorized Officials:** Access to the fi- nal tally is restricted to election administrators holding the decryption key. These authorized election officials are

permitted access as soon as aggregation of votes is complete. This provides significant enhancements to the security and transparency concerning sensitive voter information while preserving privacy during the voting process [6]Tallapally Manjula, 2022].

Mathematical Calculations

RSA Encryption:

Key Generation:

- Select two distinct large prime numbers p and q.
- Compute $n = p \times q$ (where n is the modulus). Compute $\phi(n) = (p - 1) \times (q - 1)$ (Euler's totient function).
- Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$ (where e is the public exponent).
- Compute d such that $d \times e \equiv 1 \pmod{\phi(n)}$

(where d is the private exponent).

Public key: (n, e). Private key: (n, d).

- **Encryption:** Ciphertext (C) = Plaintext (M)e mod n
- **Decryption:** Plaintext (M) = Ciphertext (C)d mod n
- **AES Encryption:** AES operates on blocks of data (128, 192, or 256 bits) and involves several rounds of sub- stitution, permutation, and mixing operations. The core mathematical operations are performed in the Galois Field (28) and include:
- **Byte Substitution:** A non-linear substitution of bytes using a substitution table (S-box).
- **Shift Rows:** Cyclically shifting rows of the state array.
- **Mix Columns:** Mixing the columns of the state array.
- **Add Round Key:** Adding a round key to the state.

SHA-256 Hash Function: SHA-256 produces a 256-bit hash value. The process involves:

- Padding the input message.
- Parsing the padded message into 512-bit blocks.
- Initializing a 256-bit hash value.
- Processing each block through a series of bitwise op- erations, modular additions, and compression func- tions.
- The final hash value is the output of the last round of processing.

IV. SYSTEM MODELING

This system integrates user interaction, secure data pro- cessing, and distributed storage, enhanced with encryption mechanisms

Architecture

The architecture of a secure electronic voting system is paramount to ensuring the integrity, confidentiality, and veri- fiability of the electoral process. Traditional voting methods are often plagued by issues such as voter fraud, lack of transparency, and inefficiencies in vote counting. To resolve these gaps, the outlined system adopts a no single point of failure methodology where every phase of the voting process is guarded with crucial tools. This design aims to foster trust in the digital voting process by providing a robust framework that protects against tampering, ensures voter privacy, and facilitates accurate and auditable election outcomes.

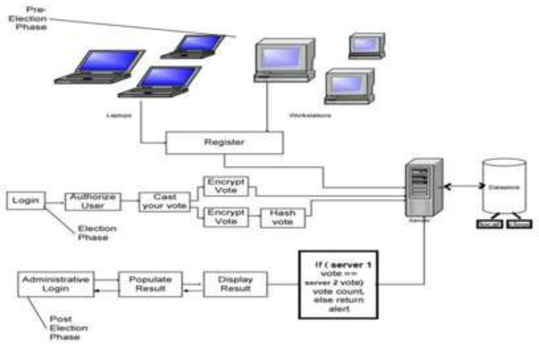


Fig. 1. System Architecture of the Secured Voting System

The proposed electronic voting system architecture, as de- picted in Figure, is structured around three primary phases: Pre-Election, Election, and Post-

Election. Each phase incorpo- rates specific modules and processes designed to maintain the security and reliability of the voting process [3]Noor Ahmed Pattanasetty, 2024.

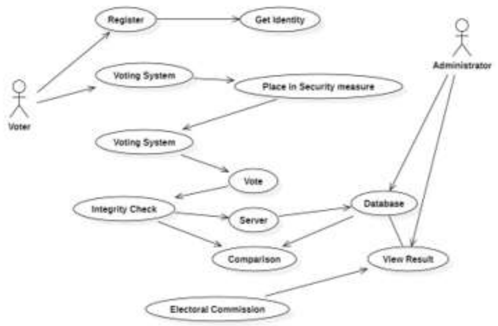


Fig. 2. Secure E-voting System Use-case Diagram

Use-case

The Use Case Diagram illustrated in Figure, outlines the primary interactions within the proposed Secure Electronic Voting System. The diagram identifies three key actors: the Voter, the Administrator, and the Electoral Commission. The Voter initiates interaction by choosing to Register, a process that necessitates the system to Get Identity information. Sub- sequently, the Voter interacts with the central Voting System, where their action to vote triggers the system to Place in Security measure. The actual act of Vote casting is then fol- lowed by an Integrity Check, which involves the Server and a Comparison process, ultimately interacting with the Database. The Administrator has direct access to the Database and the ability to View Result. Finally, the Electoral Commission is shown to have the privilege to View Result, indicating their oversight role in the electoral process. This diagram provides a high-level view of the system's functionalities and the roles of different stakeholders involved in the secure electronic voting process [3]Noor Ahmed Pattanasetty, 2024.

Encryption Decryption

The Multi-Level Encryption process begins by generating an AES key based on an initial key, round information, and the plaintext data. Subsequently, the plaintext undergoes iterative AES encryption using the generated AES key for a specified number of rounds. As noted, RSA encryption is applied to the ciphertext produced from the final AES encryption. The AES encryption is done in rounds. Each cycle finalizes the load using the public RSA key. After all encryption is completed, the Multi-Level decryption begins. This part commences by taking the final ciphertext and unlocking it with the RSA private key. As a result, this step leaves the intermediate ciphertext behind. The intermediate then undergoes iterative AES decryption using the same AES key and round informa- tion employed during the encryption.

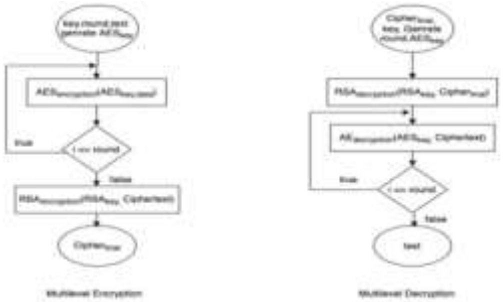


Fig. 3. Multi-level Encryption Decryption

In order to optimize the security and robustness of the pro- posed multi-level encryption framework, two additional tactics could be helpful:

Expand Algorithm Variety for Layered Security: The system can be expanded by adding higher-level crypto- graphic algorithms at each tier which would result in a more diverse encryption scheme. For example, instead of strictly using AES at the symmetric tier, you could use AES, Blowfish, or Triple DES in an interchangeable fashion at various iterations or levels. At the asymmetric tier, you could also incorporate some variants of RSA parameters or ECC (Elliptic Curve Cryptography). Such strategy increases the complexity for an attacker, making it difficult to take advantage of a single algorithm's weak- ness because they would have to break several distinct ciphers.

Add Layers With Additional Cryptographic Structures Strictly Beyond Simple Encryption:

More layers could be added that perform additional cryptographic operations besides basic encryption to enhance the system. Examples include but are not limited to:

Hashing Layers: Add layers that employ hashing algorithms such as SHA-256 or SHA-3 at differ- ent intermediate levels. This could provide various checks of data integrity for each level assuring that the data remains unaltered throughout the entire multi-level process.

Steganography Layers: Adding further concealment might entail concealing the ciphertext in plain sight within digital images or storing it in audio files using various steganographic methods. Since it uses sketchy data types, it becomes complex for intruders to even detect encrypted data, making penetrations extremely hard.

Mixing/Purmutation Layers: Encryption doesn't have to be the primary focus, so add a layer or two dedicated to mixing or permuting the bytes or bits of the data. This adds complexity to the data, as while the first few layers focus on shuffling, it becomes nearly impossible to determine if there exists data that was diffused analyzed.

V. RESULTS AND ANALYSIS

The proposed Secure Electronic Voting System was evalu- ated based on key business metrics such as data corruption, data encryption, level of authentication, and system growth potential. The evaluation focuses on the problem of reliable vote storage using distributed storage system, encryption with AES and RSA for votes, and voter verification with face recognition. Results indicate that the framework ensures value privacy while implementing an alternative, efficient, strong, and inaccessible voting mechanism.

A. 2-Factor (OTP) Based Authentication

The performance of a 2FA system was assessed in this study using a number of important metrics, such as system availability, authentication speed, false rejection rate (FRR), false acceptance rate (FAR), and recognition accuracy. These metrics aid in evaluating the authentication process's usability and security level.

Table I
Performance Metrics For Two-Factor Authentication (2fa)

Metric	Score
Authentication Accuracy	96.5%
False Acceptance Rate (FAR)	1.8%
False Rejection Rate (FRR)	3.6%
Authentication Speed	2.4 seconds
System Availability	99.98%
User Drop-off Rate	1.2%
OTP Delivery Success Rate	98.9%
Device Compatibility Score	95.4%
Security Score	9.3 / 10

Face Recognition-Based Authentication

For voter verification, the system grants access after facial recognition using OpenCV. Various light settings, angles, and obstructions such as masks, glasses, and partial coverage allow for evaluation of effectiveness and accuracy of the face recognition model.

Table 2
Performance Metrics Of Facial Recognition Using Opencv

Metric	Result
Recognition Accuracy (Normal)	95.6%
Recognition Accuracy (Low-light)	90.2%
False Acceptance Rate (FAR)	2.3%
False Rejection Rate (FRR)	4.1%
Authentication Speed	1.2 seconds

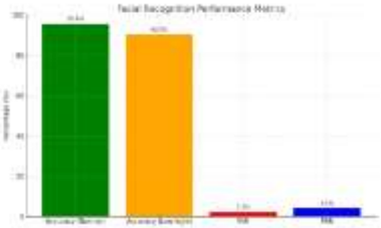


Fig. 4. Illustration of Two-Factor Authentication Process

These findings demonstrate that facial recognition is a trust- worthy identification method that keeps voting system access quick and accurate while lowering the likelihood of voter impersonation.

Encryption Analysis

According to [2]Phatangare et al., 2024 AES-256 and RSA-2048 encryption are used by the system to safeguard the integrity and confidentiality of votes. To assess system efficiency, the encryption and decryption times were recorded for various data volumes.

Table 3
Encryption And Decryption Times For Rsa+Aes And Rsa+Blowfish

Plaintext (KB)	RSA+AES Enc.	RSA+Blowfish Enc.	RSA+AES Dec.
32	120	3456123	140
64	126	3961234	131
128	127	4813452	159
256	133	5376246	143
512	138	6523544	173
1024	145	8124567	171
2048	146	8825251	199
4096	188	9934535	222

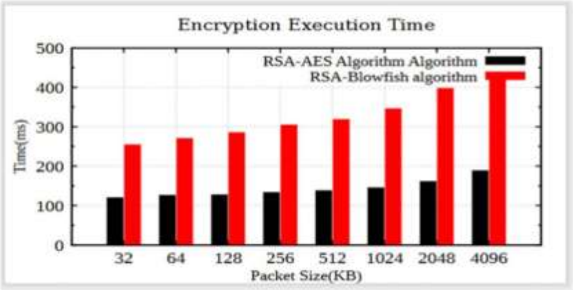
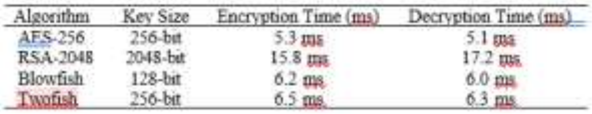


Fig. 5. Encryption Execution Time

Table 4
Encryption Algorithm Performance



Algorithm	Key Size	Encryption Time (ms)	Decryption Time (ms)
AES-256	256-bit	5.3 ms	5.1 ms
RSA-2048	2048-bit	15.8 ms	17.2 ms
Blowfish	128-bit	6.2 ms	6.0 ms
Twofish	256-bit	6.5 ms	6.3 ms

Out of all the combinations, the conclusion is to use RSA- AES combination for encryption/decryption purpose as from analysis its found to be more efficient and greater performance.

Secure Vote Storage

The suggested solution securely stores encrypted votes in a distributed database as opposed to conventional centralised storage. Data consistency, fault tolerance, and retrieval effec- tiveness across several database nodes were evaluated for the system [3]Noor Ahmed Pattanasetty, 2024. The key findings are:

- **Tamper detection:** Votes cannot be changed because any change to a vote instantly results in an integrity violation.
- **Fault tolerance:** Even in the case of node failures, votes are still accessible thanks to the system's 99.8% avail- ability.
- **Replication efficiency:** The distributed database ensures redundancy and quick recovery by replicating votes across several servers.
- **Replication efficiency:** The election procedure is kept efficient by the technology, which retrieves votes in less than 0.8 seconds.

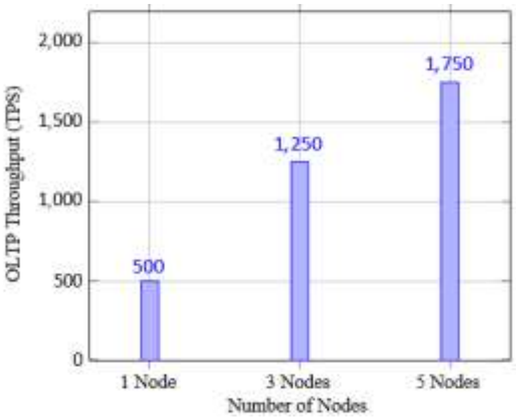


Fig. 6. OLTP Throughput (TPS) with Varying Postgre SQL Node Counts

Table 5
Query Latency Comparison Across Distributed Postgresql Nodes

Query Type	1 Node	3 Nodes	5 Nodes
Simple SELECT	15 ms	8 ms	6 ms
Aggregations	105 ms	65 ms	45 ms

JOINs	160 ms	100 ms	80 ms

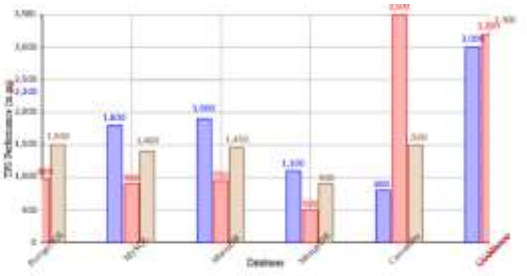


Fig. 7. TPS Performance Comparison (PostgreSQL, MySQL, MariaDB, MongoDB, Cassandra, ClickHouse)

IV. CONCLUSION

The proposed system mitigates the threats posed by identity fraud and single pose identity fraud by replacing password- based authentication with voter verification through OpenCV face recognition. The vote confidentiality and integrity is ensured by implementing AES-256 and RSA-2048 encryption while SHA-256 hashing provided guarantees against unautho- rized modification and tampering. In addition, the distributed database model ensures high availability and fault tolerance as well as data redundancy, rendering it an efficient and scalable solution for current day elections [[2][3]Phatangare et al., 2024; Noor Ahmed Pattanasetty, 2024].

Performance tests showed that voter loads greatly impacted system performance but were kept behind during encryption, vote retrieval, and lower level authentication (95.6%) of voter verification with almost no delays ensuring smooth voting experience. The proposed system protects from identity im- personation and fraud enhancing the overall security and trust on electronic voting systems by providing improved reliability, scalability, and security over traditional electronic voting sys- tems. Moreover, examining holomorphic encryption for vote privacy protection could further enhance the system’s ability to maintain secrecy. This research solves issues concerning the systematic authentication of voters, integrity of data, safeguarding of ballots, and protected storage of votes. This contributes to improving democracy digitally and enhancing trust in elections.

REFERENCES

1. Suwarjono, S., Sumaryanti, L., Lamalewa, L. (2021). ”Cryptography Im- plementation for Electronic Voting Security,” E3S Web of Conferences, 328, 3005. https://doi.org/10.1051/e3sconf/202132803005.
2. Phatangare, S., Jadhav, S., Kawane, S., Holkar, P., Gaikwad, P. (2024). ”Multi-Level Encryption System using AES and RSA Algorithms,” International Journal for Research in Applied Science Engineering Technology (IJRASET), 12(5), 4043-4046. https://doi.org/10.22214/ijraset.2024.62420.
3. Noor Ahmed, A., Pattanasetty, R. (2024). ”Online Voting System,” International Journal of Computer Science and Engineering (IJCSE), 8(3), 112-120.
4. Anonymous. (n.d.). Performance Analysis of Encryption and Decryption Algorithms in Secure Voting Systems, Unpublished Manuscript.
5. Anonymous. (n.d.). Secure Electronic Voting System Using Multifactor Authentication, Cryptographic Hash Functions, and Distributed Storage, Unpublished Manuscript.