**ISSN 1840-4855**
**e-ISSN 2233-0046**

**Original scientific article**
**http://dx.doi.org/10.70102/afts.2025.1834.1133**

# E-VOTING SYSTEM USING BLOCK CHAIN TECHNOLOGY AND CONSENSUS ALGORITHMS FOR SECURE AND FAST TRANSACTIONS OF VOTES

V. Malathi[1], R. Jaichandran[2*]

*[1]Research Scholar, Department of Computer Science and Engineering, Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation – Deemed to Be University, Chengalpattu, Tamil Nadu, India. e-mail: malathiraj0595@gmail.com, https://orcid.org/0009-0002-7715-6663*
*[2*]Professor, Department of Computer Science and Engineering, Aarupadai Veedu Institute of Technology, Vinayaka Mission's Research Foundation – Deemed to Be University, Paiyanoor, Chengalpattu, Tamil Nadu, India.*
*e-mail: rjaichandran@avit.ac.in, orcid: https://orcid.org/0000-0003-1807-2910*

***Received: October 07, 2025; Revised: November 10, 2025; Accepted: December 12, 2025; Published: December 30, 2025***

## SUMMARY

This paper introduces a new E-voting system that uses the consensus algorithms to ensure secure, efficient, and transparent voting processes on the basis of blockchain. The suggested model combines a number of cryptographic methods and consensus algorithms to overcome the current issues related to the traditional voting systems, including slow processing speed, vote manipulation, security breach, and high computation costs. Particularly, the model uses Doubling mechanism, which is based on Elliptic Curve Cryptography (DM-ECC), to generate a key, Reformed Lamport Merkle Digital Signature (RLM-ds) to authenticate voters, Hidden structure Enhanced Attribute based Searchable Encryption (HS-EASE) to encrypt votes, and Enhanced Raft Consensus Algorithms (ERCA) to secure and fast transactions of votes. All these elements combine to provide integrity in the election process which is very secure, confidential, and transparent. In the suggested E-voting model, the voters will be registered with the DM-ECC algorithm in order to create secure public and private keys. They are identified using the RLM-DS signature creation. This is followed by encrypting the votes with the HS-EASE algorithm and recording them in the blockchain that is controlled by the ERCA in order to make sure that the transactions of the votes are tamper-proof and efficient. The final tallying of the results is ensured by the use of smart contracts which ensure integrity and transparency of the election outcome. Evaluation of the system is based on a few measures of performance such as voting computation time, vote size, verification computation time, result computation time, throughput and latency. The findings prove the high efficiency of the proposed system with voting calculation time of 15 ms, 40 ms, 70 ms, 85 ms, and 100 ms as there were 1, 5, 10, 15, and 20 participants respectively. Moreover, the system is superior to other systems currently in use with respect to the size of votes, time used in verifying votes and time taken to transact the votes, and thus can be a promising option in large scale elections. Statistical comparison of the suggested model reveals a substantial increase in the processing rate, security, and scalability in comparison with the conventional voting procedures and the current blockchain-based voting systems.

Key words: *e-voting system, online voting, secure voting, blockchain technology, doubling mechanism elliptic curve cryptography, reformed lamport merkle digital signature.*

## INTRODUCTION

The integrity of the electoral will be imperative for every democratic country and also influence the public's accountability and confidence [1]. From the government's perspective, voter crowd and voter confidence will be maximized using the electronic voting systems [2]. The interest in voting for a leader will be emphasized due to the secure voting process [3]. With the development of technology, the voting system also developed as an electronic voting (E-voting) system which is conducted without paper ballots [4]. Most electronic voting systems include blockchain technology to guarantee the security of the voting process [5]. Stay at Home and PSBB adoption were two policies that the government strongly recommended during the COVID period. A potential remedy for unfettered elections is the deployment of a blockchain-based electronic voting system [6]. The designs for developing the E-voting system will differ in every research to enhance the quality. The blockchain makes use of smart contracts to boost up authentication security [7]. The smart contract-based voting system will have created with certain terms and policies that need to be obeyed by the voters during the voting process [8]. The e-voting system uses different blockchain platforms like Enterprise, Ethereum, and private blockchain. In existing models, digital signatures were used to verify user or voter authentications [9]. Moreover, the systems will be end-to-end encrypted to yields a secure voting process, even though the assaults will be occurred [10]. Regrettably, large-scale elections have not implemented such methods, either they fail to attain the same degree of freedom and justice as traditional polling site voting, or they are only viable for small-scale elections [11]. The majority of electronic voting methods are failed due to their ineffective processing. Using a consensus algorithm, several models make a secure e-voting system. Moreover, consensus like proof of stake (PoS), Proof of concept, etc., will enhance the efficiency and reliability. Those centralized approaches will resist tampering and fraud, providing a transparent and trustworthy voting system. Even though the effective use of that approach is not used in the existing approaches.[12]

The voting system's need for efficiency, security, and transparency makes a view in the decentralized network. Due to the immutable ledger blockchain provides a promising solution in developing multiple applications including an E-voting system. It ensures the voter's trust and also makes an accurate counting of voting by resisting fraud. A blockchain-based electronic voting system is currently done by many existing models that still have drawbacks of computational overhead, feasibility, and potential vulnerability. In the current scenario of conducting elections using ballet-boxes, electronic voting machines (EVMs) and E-voting systems were followed in many places.[13][14] Elections conducted using ballet boxes or EVMs require a lot of time, infrastructure, and human resources and have no mechanism to verify votes and avoid election fraud. In an E-voting system, voters can cast votes remotely using electronic devices like computers, laptops, mobile phones, EVMs, etc., connected to the server via the internet and votes can be stored in a database for verification. The disadvantages of performing elections by manually may be avoided by e-voting systems, but they are susceptible to cyberattacks and vote-rigging. A blockchain-based electronic voting method and consensus algorithms can overcome above said limitations in conducting elections. Some researchers made a blockchain and consensus algorithms-based model to enhance security during the elections. [15] The existing systems also possess some challenges like slow process, computational storage, and security issues. Hence, there is a need to develop an effective and efficient blockchain-based model is too implemented for overcoming the existing issues. The following are the primary objectives of the suggested work:

- To introduce "Doubling mechanism based Elliptic Curve Cryptography (DM-ECC)" for generating both public and private keys.
- To present using "Reformed Lamport Merkle Digital Signature (RLM-DS)" for signature creation for the authentication process.
- To provide "Hidden structure Enhanced Attribute based searchable encryption (HS-EASE)" for encryption of voting details.
- To implement the "Enhanced Raft consensus algorithm (ERCA)" for enhancing the secure storage and fast transaction.

This paper overall organized as follows: The general background of the planned research project is described in section 1, along with its structure and contribution. A few recent studies that examined safe electronic voting are discussed in Section 2. They provide the general suggested technique in section 3.

The result and discussion of the suggested approach are presented in Section 4. Section 5 concludes by outlining the study's general findings and next steps.

## RELATED WORK

A few recent studies [16] that were conducted on secure E-Voting from diverse techniques are described below. A score-voting electronic voting method that protects privacy was suggested by [17] using blockchain technology. Encrypting votes before submitting them to the Blockchain is necessary to protect voter anonymity. The election results might be manipulated in favor of a certain candidate by an unauthenticated voter that intentionally changes the score value before encryption. Furthermore, the scheme also needs voters to verify that their score falls within a given range before their vote is recorded on the Blockchain to ensure that the election is fair. Simulation experiments were conducted to evaluate the efficiency of the proposed scheme. Analysis of the experiments' outcomes indicates that the recommended scheme is very secure and capable of processing a maximum of 10,000 batches of transactions at a time. A reliable and flexible internet voting system was designed using cloud-based hybrid blockchain technology by [18]. Their recommended model consists of three separate phases: registration, voting, and counting. For the registration and voting phases, a digital signature and timestamp-based authentication system is applied to authenticate candidates and voters. Middlemen are removed by smart contracts to ensure that all transactions performed within the cloud-based blockchain are secure. Finally, a practical Byzantine Fault Tolerance (PBFT) consensus algorithm is applied to the voting system to ensure that a vote has not been altered or modified. So, in their entirety, as compared to the existing system, the proposed system performs considerably better in the future.

A resilient electronic voting system was proposed by [19] based on the basic concept of Quantum Key Distribution and blockchain security. The main problem associated with the existing method is the security associated with the votes, along with the modifications done for authentication and data accessibility. The votes are unencrypted, and instead, the quantum cryptography feature is used in the transaction communication within the blocks. In cryptography, the most promoted technology in the quantum context is the Quantum Key Distribution system. The proposed system is divided into various phases, including registration, voting phase, data processing, and validation.

Table 1. Comparison of related work

| References | Year | Technique Used | Performance | Disadvantage |
|---|---|---|---|---|
| [16] | 2023 | Decentralized and self-tallying score voting system | Latency was 16s and 35s for the transactions | Implementing zero-knowledge proofs provides complexity and computational overhead which impact scalability in larger elections. |
| [17] | 2024 | Digital signature and timestamp-based authentication system-PBFT | Response time was 7.19ms. | Prone to vulnerability, slow vote transactions |
| [18] | 2024 | Quantum key distribution and blockchain security | Maximizing voter power over the process | Comparison of existing approaches was not done which shows the Potential vulnerability |
| [19] | 2025 | Blockchain-based, verifiable e-voting system-STAP-LINDDUN | Faced critical cyber security and data privacy requirements through testing | The main drawback was the potential complexity and resource-intensiveness for integrating STPA, LINDDUN, and blockchain |
| [20] | 2023 | Biometric-based cryptography | Provide secure and seamless voting for a population of 400 voters | Managing fingerprint-based public/private key pairs for a large-scale election was difficult. |

Cyber-security and data privacy threat modeling techniques were used by [20] to enhance the STPA analysis. The model integrated blockchain technology into the design of the mission-critical electronic voting system. The solutions of cyber security were tested for data privacy and constructed a proof of concept. According to the evaluation, the solution satisfies the essential cyber security in data privacy standards. The study brings two key contributions: first, a Blockchain-based, verifiable e-voting system; and second, an approach to enhance a system's STPA analysis through the application of cyber security and data privacy threat modeling tools. The challenges like tampering results by counterproductive votes make a high difficulty and dishonest results. On taking this issue, Adeniyi et al. [20] presented a transparent and immutable blockchain framework. A cryptography system based on biometrics was presented to maximize the transparency of the system. Each voter's biometric information was used for generating their private key, followed by the creation of a public key to function as their identification. Given that each individual's biometric trait was unique and inimitable. The anonymity of the voter is guaranteed as the public key and the private key cannot be connected.

The above Table 1 utilizes the existing model [16] [17] [18] [19] and [20] these have some significant drawbacks when it comes to the secure E-Voting mechanism employed for the final result. The limitations are implementing zero-knowledge proofs provides complexity, computational overhead with impact scalability in large elections, is prone to vulnerability, slow vote transactions, comparison of existing approaches was not done which shows the potential vulnerability, potential complexity, resource intensiveness for integrating STPA, LINDDUN, and blockchain, and managing fingerprint-based public/private key pairs for a large-scale election was difficult, in addition to the voting system's lack of flexibility, cost-effectiveness, security, response time, vote manipulation, latency, and authentication delay. To solve the issues and secure the E-voting need for nowadays new novel model is required.

## PROPOSED METHODOLOGY

In today's digital age, the security of e-voting systems is paramount to maintaining the truthfulness of the democratic process. For that reason, trustworthiness becomes an important issue since even a slight security breach may bring forth devastating consequences: it may result in tampered election outcomes, disclosed voter's privacy, and diminished public confidence in an election process as a whole. Figure 1 presents the workflow structure of the suggested model as a visual representation of the design and how it functions.

The proposed approach is designed to ensure the integrity and security of elections through a four-step process. The approach starts with a registration step, where voters create a pair of keys through the DM-ECC secure algorithm, which is then stored in a blockchain along with data from each voter. A security feature in this step comes with RLM-DS signature creation, where a high degree of authentication with respect to voter identification can be achieved in a much simpler manner. Once a voter has completed the authentication step, they are eligible to utilize their right to vote and simultaneously retain their security and privacy through encryption with the HS-EASE algorithm. Subsequent to this step comes the blockchain network that receives and stores encrypted votes through the ERCA algorithm, with a high degree of assurance that there are no discrepancies in this step with respect to manipulation and fraud among different voter nodes in the network. The final step comes with counting votes to determine the result of an election. This system allows an accurate and unaltered trail of all transactions to be produced, and ultimately, all outcomes are made public to ensure accountability and transparency within the electronic voting system. The foregoing system is further described below.

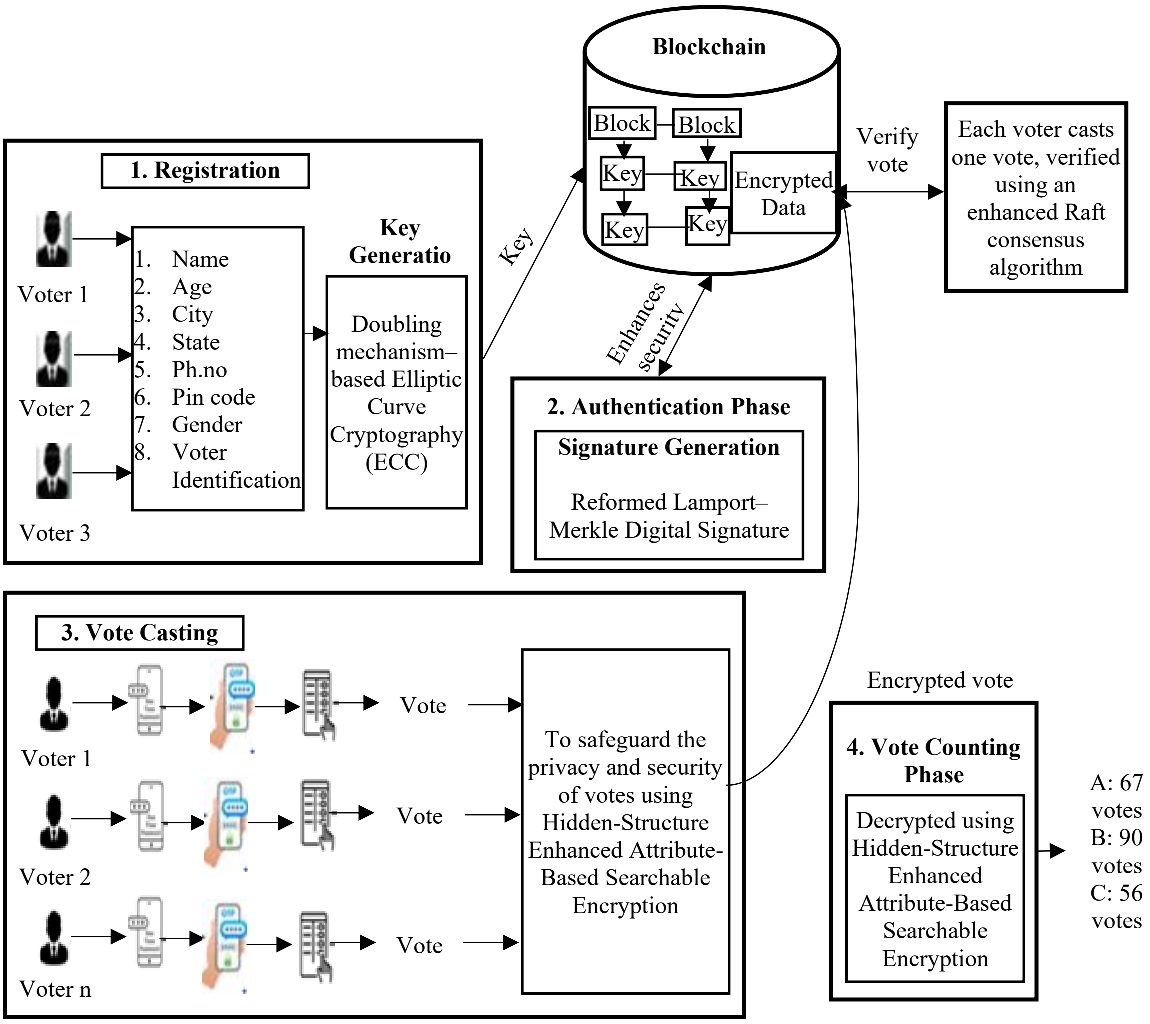

Blockchain
Block
Block
Key
Key
Key
Key
Encrypted Data
Verify vote
Each voter casts one vote, verified using an enhanced Raft consensus algorithm
1. Registration
Voter 1
Voter 2
Voter 3
1. Name
2. Age
3. City
4. State
5. Ph.no
6. Pin code
7. Gender
8. Voter Identification
Key Generatio
Doubling mechanism–based Elliptic Curve Cryptography (ECC)
Key
Enhances security
2. Authentication Phase
Signature Generation
Reformed Lamport–Merkle Digital Signature
3. Vote Casting
Voter 1
Voter 2
Voter n
Vote
Vote
Vote
To safeguard the privacy and security of votes using Hidden-Structure Enhanced Attribute-Based Searchable Encryption
Encrypted vote
4. Vote Counting Phase
Decrypted using Hidden-Structure Enhanced Attribute-Based Searchable Encryption
A: 67 votes
B: 90 votes
C: 56 votes

Figure 1: Proposed model workflow structure

## Registration Phase

In the key generation process, all candidates and voting-age citizens must register along with their data before the election occurs. This includes their name, age, city, state, phone number, postal code, gender, voter identity, and the electronic device they will use to cast their ballot. An elliptic curve cryptography–based secure procedure (DM-ECC) with a secure Doubling mechanism is used to provide each voter's secret and public keys and candidate when their registration is complete. The DM- ECC algorithm builds on the original elliptic curve cryptography (ECC) algorithm [21], which uses a doubling mechanism to enhance security by selecting the optimal point on the elliptic curve. The ECC algorithm involves a private key $R$ and the prime number $P_{nt}$. The general formula of elliptic curve cubic is in Equation (1):

$$G = m(x)^3 + s * m(x) + m \tag{1}$$

Here, $s$ and $m$ are denoted as constant values it is $s = m = 2$.The best point is selected from the elliptic curve if the conditions $U = V$ is satisfied. The values $U$ and $V$ are mathematically stated in equation (2) and equation (3).

$$U = mod(G, P_m) \tag{2}$$

$$V = mod(P_m(y))^2, P_m) \quad (3$$

Here, $P_{nt}$ state number of a prime number and states the elliptic curve points. In the ECC algorithm, the doubling mechanism is utilized for identifying the $U$ and $V$ values. The public key $nf$ and the best point are mathematically related in equation (4).

$$nf = R * n_w \tag{4}$$

In the DM-ECC algorithm, a pseudo-random key is combined with a public key $nf$ to make the electronic voting system even more secure.

### Authentication Phase

Each electronic voting system must include this component; the authentication step guarantees that the whole voting procedure is safe and sound. In this phase, the keys and information of voters are stored in the blocks of the blockchain [22], provide an open, protected record of each transaction. For voters to be authenticated, a digital signature is obtained using the Reformed Lamport Merkle Digital Signature (RLM-DS) algorithm that incorporates the usage of a pair of keys derived from the DM-ECC algorithm for voters. These are a private key and a public key. The RLM-DS algorithm can aid in improving the efficiency and security level of blockchain-based E-voting communication for voter data, which is a variation technique based on the traditional Lamport Merkle Digital Signature (LMDS) scheme proposed in [23]. Implemented in a bottom-up manner, the original LMDS scheme uses a hash tree to verify a large number of voter devices (n). The hash tree has each leaf node associated with the hash of the voter data expressed in a set.

By using the hash function and the Lamport signature, the leaves and devices are linked. Each device that gets the most connections get associated with the hash value of the previous device that was a voter or sensor. This establishes a tree structure, whereby the root of the tree represents the Voter Key Center (VKC), and the nodes of the tree are the devices that vote.

The VKC, which is also known as the root of RLM-DS generation, authenticates a set of voter devices through a comparison between the calculated root of the public key. This implies that only eligible voters have access to the election process, and their privacy is ensured. The RLM-DS method has numerous advantages, including security, efficiency, and transparency.

In general, only authorized voters are allowed to cast votes, while the identities of the voters are secured and confirmed as a result of the authentication feature of the E-voting system. The RLM-DS algorithm and blockchain technology give a secure, efficient, and transparent solution for E-voting systems.

### Vote Casting Phase

The E-voting system must provide a vote-casting phase, through which the democratic right of the voters is exercised by casting votes and sending it to the blockchain network for verification and storage in a secure manner. In this regard, on a specific day for election, each and every eligible voter gets a chance to participate in it. Therefore, to provide reliability to the election, an efficient mechanism in identifying the real identity of the voters has been adopted using a One-Time Password (OTP) authentication generated from the authorized card details of each voter. This rigorous authentication procedure ensures that only registered voters are able to cast ballots.

The proposed system encrypts the votes using the HS-EASE algorithm, for the most secure procedure, combines an attribute-based searchable encryption approach with the concealed access structure, to ensure their privacy and security:

(i) System initialization algorithm setup $T^i, K'$ . Input security parameter $i$ and global attribute set $K'$, output system public key $PU_{key}$ and master key $M_{key}$.

(ii) Private key generation algorithm $KeyGen(PU_{key,}M_{key}, A_{Net})$ Input system public key $PU_{key}$ , master key $M_{key}$ and user attribute set $A_{set}$ , output private key $PR_{key}$ .

(iii) Trapdoor generation algorithm $TokenGen(PU_{key,}Key_w, PU_{key'}$. Input system public key$PU_{key'}$, user private key $M, \rho, \tau$. Input the system public key$PU_{key'}$, the user private key $PR$ and the keyword $Key_w$ to search. Output the trapdoor $T_d$. This entrance is used to hunt translated data associated to keyword$Key_w$ .

(iv) Ciphertext search algorithm search algorithm $search\ (PR_{key}, cyber_t, T_d)$. Input the system public key $PU_{key,}$, ciphertext $cyber_t$ , and trapdoor $T_d$. If the user's attributes meet the right to use erection in the ciphertext $Cyber_t$and $Key_w = Key_{word}$. After then, it prints 1 to indicate that the search was successful. If not, it returns zero.

The HS-EASE procedure represents a significant advancement in secure voting systems by employing a dual-layer encryption strategy to protect vote data. To begin with, the process uses a symmetric key for encrypting the actual voting data, thus keeping it private. To make sure that only the concerned voter can unlock their respective votes, the symmetric key is protected by the public key of the voter. Not only is the confidentiality of the votes ensured by this dual encryption, but it also results in a foolproof system, thus increasing the authenticity of the voting process.

After the voting has been encrypted, it is cast into a blockchain system for validation and storage purposes, through the use of the Enhanced Raft Consensus Algorithm (ERCA). This is because the traditional Raft Consensus Algorithm has a strong log replication method but has a challenge that is addressed by the ERCA. The major approach or concept used by the ERCA is that of apportionment. This approach adjusts the way log replication is carried out to synchronize only one set of notes for a period. Therefore, new concepts are required to fit into the new approach that have a vital impact.

In the ERCA, the log segment indexing operation is a key component. Log segments are used to index each round of data, and these segments function with more than one purpose, such as tracking the log information capacity, ordering the log sets, and determining the owners of the follower nodes corresponding to the log information.

Allocation is the key to the log replication technique of the ERCA algorithm. The leader node checks its buffer for a predetermined number of log records before the start of every sync process, ensuring that it does not exceed the number of followers present in the region. Different requests are employed for dividing and copying those identified records to other follower nodes. As soon as the log replication message is received, every follower node stores the message in a local cache queue and sends an acknowledgment to the leader node for receiving it, which is imperative since the status of log replication can thus be verified by the leader node on the network.

When the messages of log are being sent to active follower nodes which haven't replied yet, the leader node uses a random resending in a consensus round. The leader waits for the confirmation of most nodes in order to end the log replication for that round; otherwise, the operation continues by falling into tight time limits. This is quite a systematic process that ensures that all nodes in the network attain consensus with no way to commit fraud or manipulate it.

**Vote Counting Phase**

In the vote-counting phase, verified votes are tallied to determine the election outcome through an automated process using a smart contract, ensuring transparency, accuracy, and immutability of the results. Once the voting period ends, the blockchain network collects all verified votes from nodes, each encrypted using the HS-EASE algorithm and stored on the blockchain. The HS-EASE algorithm decrypts the votes using corresponding private keys, and to ascertain the result of the election, the decrypted votes are tallied and tabulated.

(i) Decryption algorithm $decryption\ (PR_{key}, PU_{key}, Cyber_t)$. The system receives the input as ciphertext, a private key $PR_{key}$, and $PU_{key}$, by which the blockchain will decrypt it.

(ii) The election result is then ascertained by counting and adding the decrypted votes. Accurate and reliable results are guaranteed by the transparent and automated counting procedure.

Because the results are made public, recorded on the blockchain, and made available to the public, voters may verify the results and guarantee that the election process is fair.

## RESULTS AND DISCUSSION

### Software and Hardware Description

Table 2. Hardware description

| **Category** | **Description** |
|---|---|
| Hardware | |
| Processor | Intel(R) Core (TM) i5-9500 CPU @ 3.00GHz, 3.00 GHz |
| RAM | 16.0 GB (15.8 GB usable) |
| System Type | 64-bit Operating System, x64-based processor |
| Storage | Minimum 256GB SSD (recommended for faster data storage and retrieval) |
| Input Devices | Standard keyboard and mouse, touchscreen (optional) |
| Display | Minimum 1080p resolution monitor |
| Network | Ethernet or Wi-Fi (For communication and data transfer during voting process) |
| Security Features | Biometric authentication system (optional), smart card for voter identity validation |

To derive above Table 2 explains how the proposed E-voting system will run with the Intel(R) Core (TM) i5-9500 CPU at 3.00 GHz with 16 GB of RAM (15.8 GB usable) and 64-bit operating system with x64-based processor. The system will need 256GB SSD at least to store and retrieve data quickly and thus optimally perform in case of voting. The system can be operated by the users with regular keyboard and mouse, but can also have a touchscreen to give the user a more interactive experience. The display of the voting interface would require at least a 1080p resolution monitor to be clear and provide a precise display of the voting interface. The system will have the ability to connect either Ethernet or Wi-Fi with the system which will ensure a reliable network communication throughout the voting process. To provide extra security, biometric identification can be introduced so that only the authorized voters can take part and a system with smart cards can be adopted to verify the identity of the voters. This hardware setup makes the system secure, efficient as well as user friendly to provide a perfect platform to carry out secure and fast electronic voting.

Table 3. Software configuration

| **Software** | |
|---|---|
| **Operating System** | Windows 10 or Linux (Ubuntu preferred for server-side operations) |
| Blockchain Platform | Ethereum or Hyperledger Fabric (for private blockchain network) |
| Consensus Algorithm | Enhanced Raft Consensus Algorithm (ERCA) |
| Cryptography | DM-ECC (Doubling mechanism Elliptic Curve Cryptography) |
| Digital Signature | Reformed Lamport Merkle Digital Signature (RLM-DS) |
| Encryption | Hidden Structure Enhanced Attribute Searchable Encryption (HS-EASE) |
| Database | PostgreSQL (for storing encrypted vote data in the backend) |
| Web Server | Apache HTTP Server or Nginx (for serving the frontend application) |
| Web Technologies | HTML, CSS, JavaScript, React.js (for frontend development) |
| Backend | Node.js, Express.js (for backend services and API management) |
| Smart Contract | Solidity (for writing smart contracts on the Ethereum blockchain platform) |
| Development Tools | Visual Studio Code, Git, Docker (for containerization), Truffle (for blockchain testing) |

To decipher the above-table 3 explains that, the proposed E-voting system is based on a strong software configuration that is considered to be secured, efficient, and scaled. It is capable of running on both windows 10 and Linux (Ubuntu), the latter being preferred when running on the server side. The system is based on Ethereum or Hyperledger Fabric to implement the blockchain and uses Enhanced Raft Consensus Algorithm (ERCA) to provide transactions with high speed and security. The process of secure key generation is performed with the help of Doubling mechanism Elliptic Curve Cryptography (DM-ECC), as well as voter authentication is provided by Reformed Lamport Merkle Digital Signature (RLM-ds), and the confidentiality of voting information is guaranteed by Hidden Structure Enhanced Attribute Searchable Encryption (HS-EASE). The votes are encrypted and stored in a PostgreSQL database, with the interface being created in HTML, CSS, JavaScript, and React.js, offering an interactive interface to a user. The backend is based on the application logic and API management of the application through the Node.js and Express as well as the writing of smart contracts on the Ethereum platform with Solidity. The development, version control, and testing process are assisted with such development tools as Visual Studio Code, Git, Docker, and Truffle. This all-important software system guarantees development of a safe, effective, and transparent electronic voting system.

**Performance Analysis**

The efficacy of the suggested technique is thoroughly evaluated based on six key performance metrics: voting calculation time, vote size, voting verification time, voting result calculation time, throughput, and latency. By considering these factors, the suggested methodologies and present methods may be fairly and accurately compared; the findings are shown.

*Voting Calculation Time* $(T_{vc})$

This metric measures the time taken to calculate the votes, including the time required for encryption, decryption, and verification.

$$T_{vc} = \frac{(T_{enc} + T_{dec} + T_{ver})}{N} \tag{5}$$

In equation (5) Where $T_{enc}$is the time taken for encryption, $T_{dec}$ is the time taken for decryption, $T_{ver}$ is the time taken for verification, and $N$ is the number of votes. The comparison of $T_{vc}$ is presented in Figure 2.

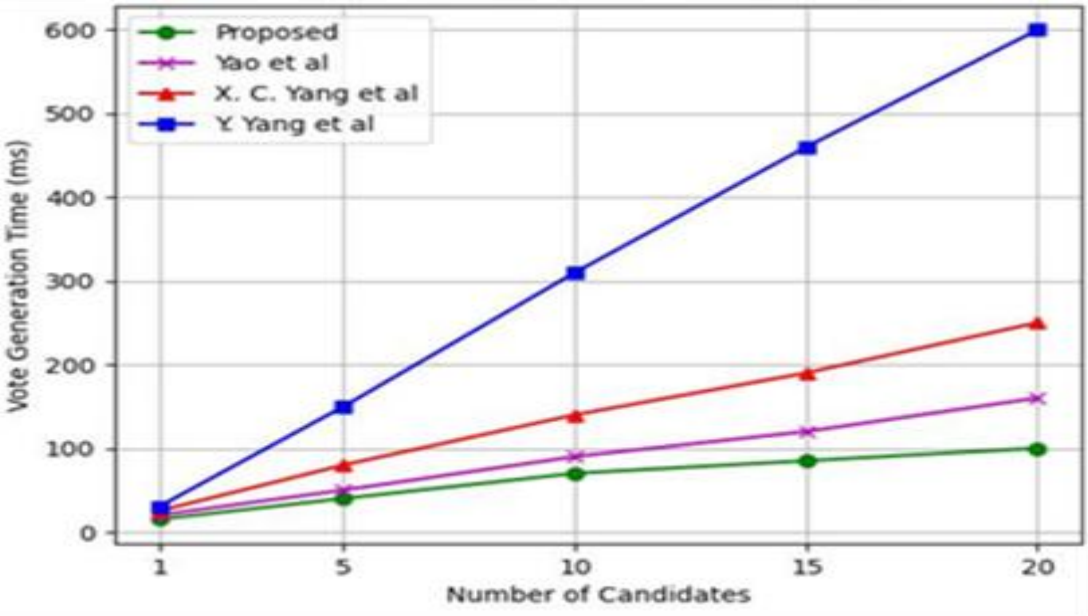


Figure 2. Analysis of the time taken by each voter to cast their vote

The efficiency of the proposed method concerning vote generation time seems much better compared to existing schemes like Yao et al., X. C. Yang et al., and Y. Yang et al. As illustrated by Figure 1, the vote generation time for the Proposed method resulted in significantly low values, with times of 15 ms, 40 ms, 70 ms, 85 ms, and 100 ms for 1, 5, 10, 15, and 20 candidates, respectively. The reason for such efficiency is the incorporation of the HS-EASE algorithm, which makes a fast symmetric key encryption of vote data along with secure public key encryption of the symmetric key, allowing access to only those voters who have been approved to access the vote data so that confidentiality and integrity can be maintained. Thus, the suggested technique offers a more efficient and accessible approach to voting systems, making it suitable for large-scale elections and other voting applications.

*Vote size ($S_v$):*

This metric measures the size of the votes, including the size of the encrypted data and the metadata required for verification.

$$S_v = (S_{enc} + S_{meta})/_N \tag{6}$$

The above equation (6) describe , $S_{enx}$ is the dimension of the encrypted data, $S_{meta}$ is the dimension of the metadata required for verification, and $N$ is the number of votes. The comparison of $S_v$ is presented in Figure 2.

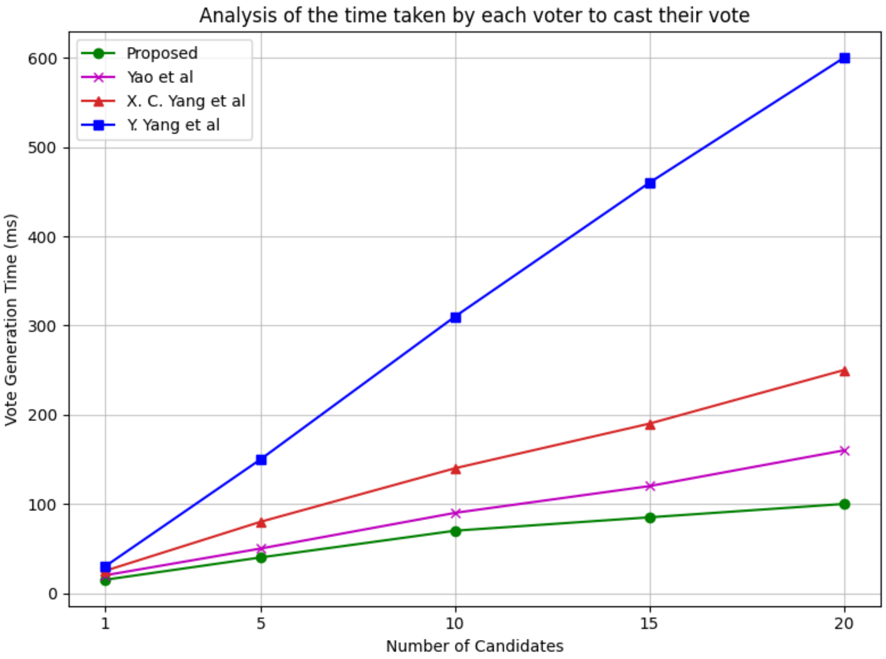


Figure 3. Analysis of the vote size of each voter

In Figure 3, the proposed scheme's vote size is compared with other schemes for different numbers of candidates. The proposed scheme shows a vote size of 15, with the shortest time achieved with 1 candidate; for a vote size of 40, the shortest time is attained with 5 candidates; for a vote size of 100, the shortest time is reached with 10 candidates; for a vote size of 170, the shortest time is obtained with 15 candidates; and for a vote size of 200, the shortest time is achieved with 20 candidates. It's important to note that each voter's vote size in the proposed method is equivalent to the vote size in the schemes presented by Yao et al, X. C. Yang et al, and Y. Yang et al.

*Voting Verification Time* **(**$V_{vt}$**):**

The $V_{vt}$ to denote the time required to verify each voter's votes. According to ERCA $V_{vt}$ calculated as:

$$V_{vt} = (2mS + 4m + 6)t_e + (2mS + 5m + 2)t \quad (7)$$

In equation (7) $S$ is denoted as the maximum score, $m$ is the number of candidates, and $t_e$ is denotes the computation time of one exponentiation, where $t_e \approx 2.325\, ms$ , $t\times$ to denote the computation time of multiplication operation, where $t\times \approx 0.012\, ms$ . The comparison of $V_{vt}$ is presented in Figures 4 (a) and (b).

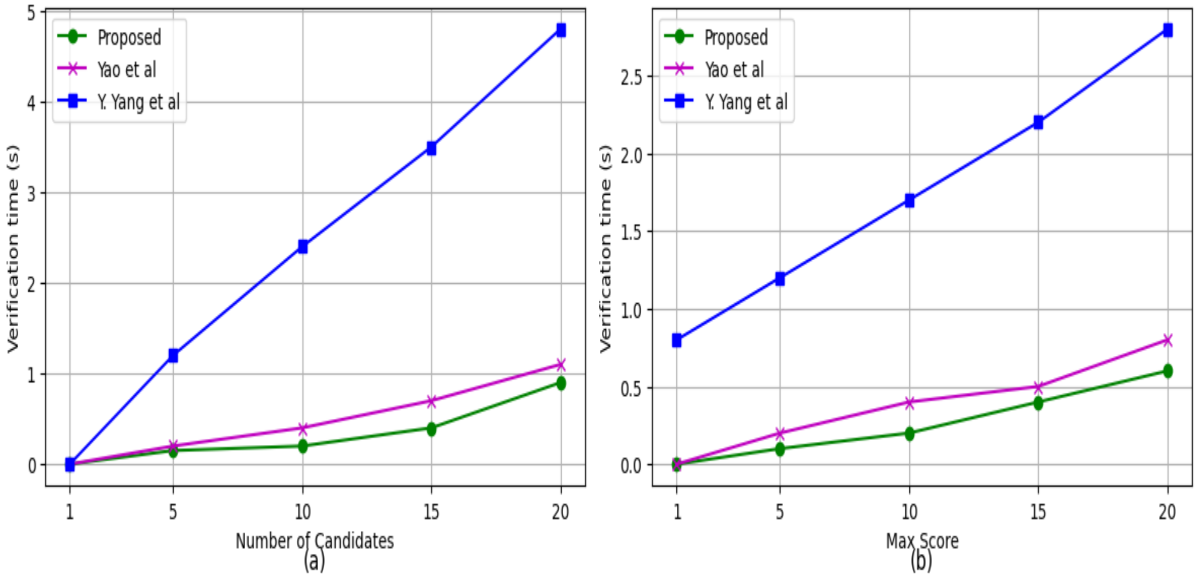


Figure 4. Comparison of verification time based on the (a) number of candidates and (b) max score

Figures 4 (a) and 4 (b) compare verification times based on the quantity of contestants and the maximum score. Both figures indicate that the proposed method generally yields faster verification times, especially as the quantity of contestants or maximum score upsurges. In Figure 4 (a), the verification time of the proposed method increases steadily with the number of candidates (1, 5, 10, 15, and 20), showing times of 0ms, 0.18ms, 0.2ms, 0.4ms, and 0.9ms, respectively. However, it increases at a slower rate compared to the methods by Yao et al. and Yang et al., consistently demonstrating the lowest verification time for all numbers of candidates. In Figure 4 (b), the proposed method also exhibits lower verification times across all maximum score values (1, 5, 10, 15, and 20), with times of 0ms, 0.1ms, 0.2ms, 0.4ms, and 0.6ms, respectively. Additionally, its verification time increases more slowly as the maximum score rises compared to the other two methods.

*Voting Result Calculation Time$T_{cr}$*:

$T_{cr}$ is denotes the time one takes to calculate the voting result and $n$to denote the number of voters. $T_{cr}$Calculated as in equation (8):

$$T_{cr} = 2mt_e + 2mnt \quad (8)$$

With, $n = 50{,}500{,}1000{,}10000{,}100000$ in this study $T_{cr}$ and the outcome is presented in Figure 5.

When the number of voters reaches 50, 500, 1000, 10000, and 100000 the calculation time is 10.815 s, 11879 s, 1719810s, 1910393 s, and 171993 s as compared to other models obtained high time.

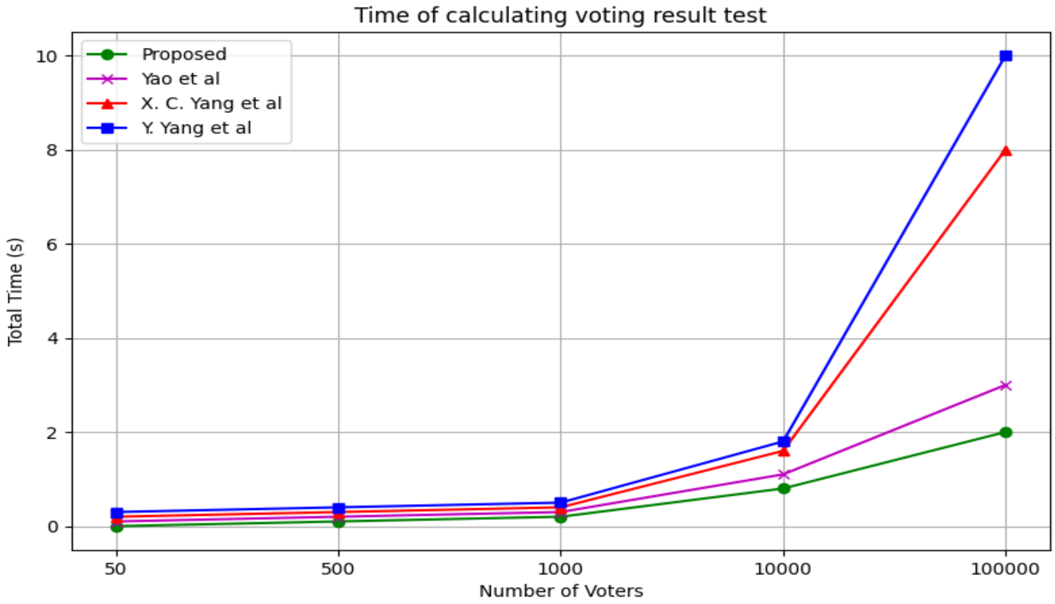


Figure 5. Time of calculating voting result test

*Throughput and average latency:*

Throughput denotes the velocity with which legitimate transactions are incorporated into the blockchain. It is quantified in transactions per second (tps). Average latency, or transaction latency, is ascertained by monitoring the duration required for a transaction to be confirmed and included into the blockchain (in seconds). This assessment accurately represents the actual latency that a user of the suggested approach can anticipate. Figures 6 (a) and 6 (b) illustrate the throughput and average delay at varying transaction send rates for the evaluation of the suggested technique.

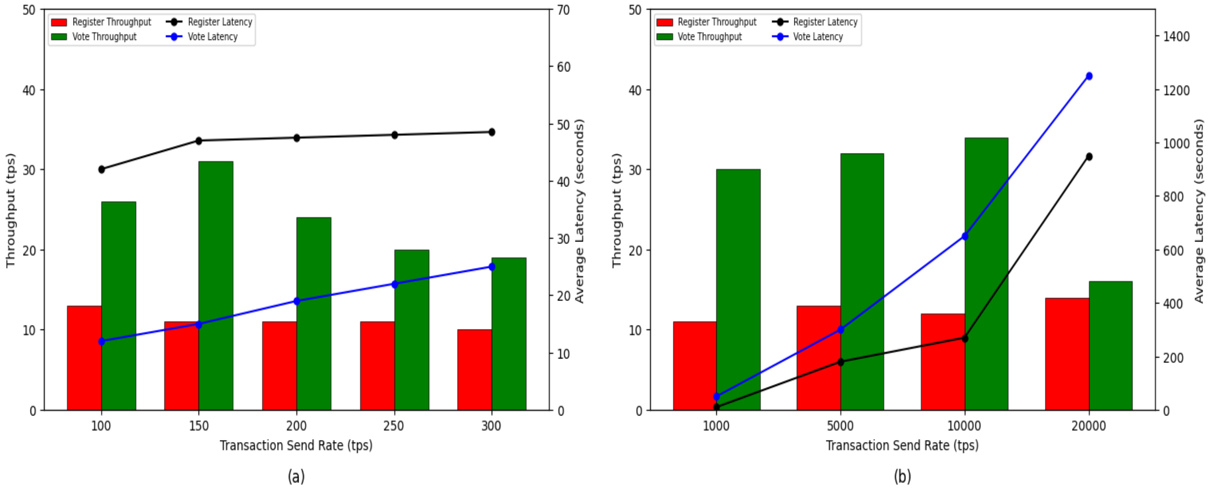
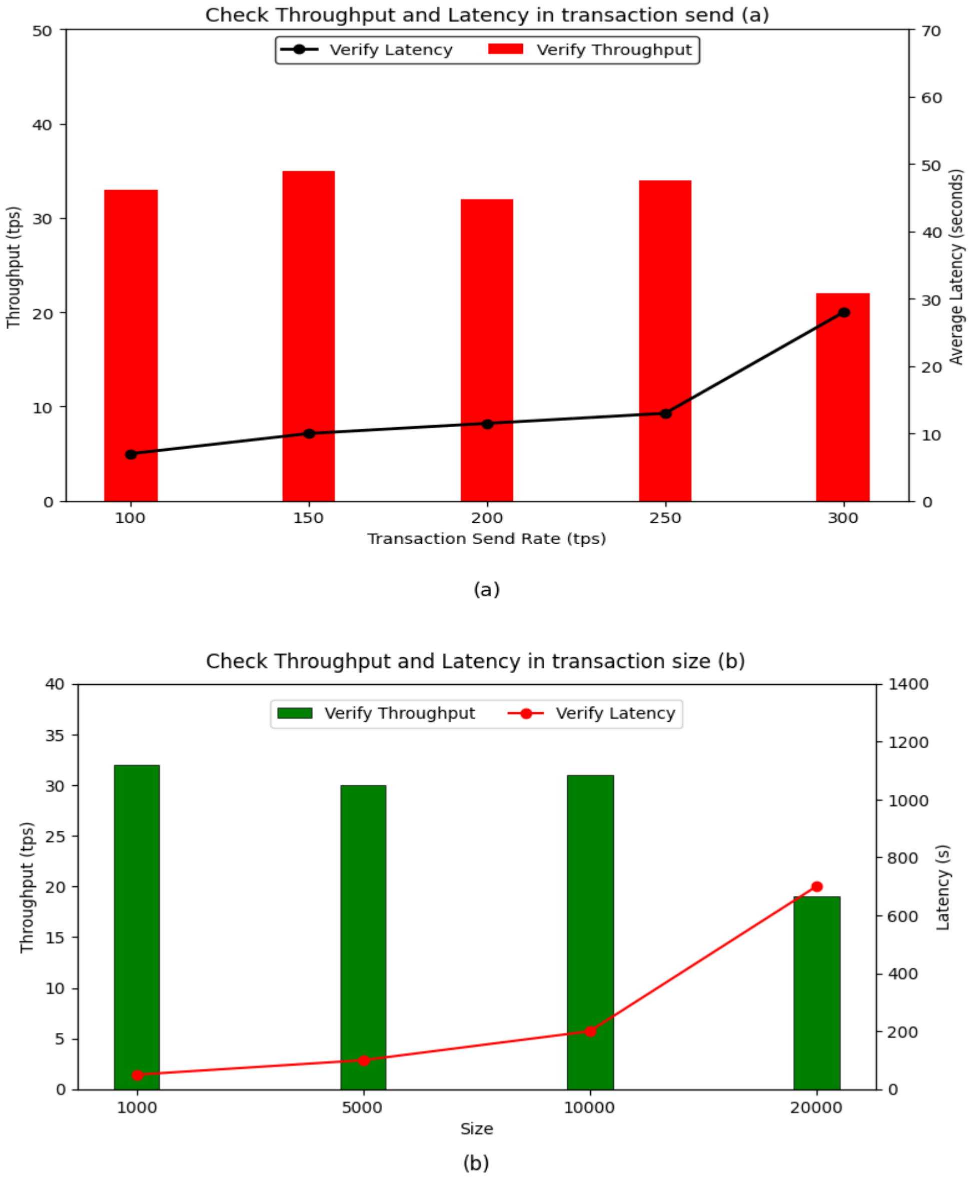


Figure 6 (a) and (b). Latency and throughput effects of increasing transaction rates

In Figure 6(a), the transaction send rate is varied from 100 to 300 tps. Register latency is relatively constant, but vote latency varies linearly. The transaction sends rates for both Register and vote transactions drop with the increase in send rate. From Figure 6(b), the transaction send rate varies from 1000 tps to 20000 tps. Register latency varies prominently, but vote latency varies exponentially. Transaction send rate for Register or vote transactions is constant but drops slightly with the upsurge in send rate. It is shown that increasing transaction rates can cause a rise in latency and a fall in transaction send rate. The perception of increased transaction rates on latency and transaction send rate depends on the type of transaction figure.



(a)

(b)

Figure 7. Check throughput and latency in transaction send (a) and size (b)

Figure 7 depicts the effect of verification throughput and latency and the two variables of transaction send rate and size. From Figure 7 (a), when the transaction send rate varies from 100 to 300 transactions per second (tps), the verification throughput remains constant; however, a slight drop in the throughput is observed when the highest transaction send rate is achieved. However, the verification latency continues to increase. This verifies that an increase in the transaction send rate causes an increase in the verification time. Figure 7 (b), when the size varies from 1,000 to 20,000 units, the verification throughput and verification latency decrease and increase significantly. This confirms that as the size of units increases, the latency and throughput will decrease. Table 3 demonstrates the overall performance comparison of the proposed scheme and the other schemes for the E-voting system.

Table 4 represents the performances of different techniques compared with the suggested system, and clearly determines the efficiency of the suggested system. The performance of the proposed technique is finer compared to other works.

Table 4. Overall performance comparison

| **Time Calculating a Voting Result** | | | | | |
|---|---|---|---|---|---|
| **Transaction Sends Rate (TPS) In the Proposed E-Voting Scheme** | | | | | |
| Category | Transaction send rate | | | | |
| | 100 | 150 | 200 | 250 | 300 |
| Register throughput | 13 | 11 | 11 | 11 | 10 |
| Vote throughput | 26 | 31 | 24 | 20 | 19 |
| Register latency | 30 | 33.8 | 34 | 34.2 | 34.5 |
| Vote latency [22] | 9 | 11 | 14 | 16 | 18 |
| Verify the tps in the proposed E-voting scheme | | | | | |
| Size | Transaction send rate | | | | |
| | 100 | 150 | 200 | 250 | 300 |
| Verify throughput | 33 | 35 | 32 | 34 | 22 |
| Verify latency | 5 | 7 | 8 | 9.2 | 20 |
| Transaction sends rate (tps) in the proposed E-voting scheme | | | | | |
| Category | Transaction send rate | | | | |
| | 1000 | 5000 | 10000 | 20000 | |
| Register throughput | 11 | 13 | 12 | 14 | |
| Vote throughput | 30 | 32 | 34 | 16 | |
| Register latency | 10 | 180 | 270 | 970 | |
| Vote latency | 50 | 300 | 650 | 1250 | |
| Verify the tps in the proposed E-voting scheme | | | | | |
| Category | Size | | | | |
| | 1000 | 5000 | 10000 | 20000 | |
| Register throughput | 32 | 30 | 31 | 19 | |
| Register latency | 50 | 100 | 200 | 700 | |

DISCUSSION

The proposed e-voting system on blockchain technique using a consensus algorithm has been assessed and compared with other similar techniques used in Table 5. Analysis of the results shows that the proposed system surpasses other techniques in voting calculation time, size of the vote, voting verification time, voting result calculation time, throughput, and latency.

Table 5. Analysis by comparison

| Reference Number | Technique used | Latency |
|---|---|---|
| [14] | Decentralized and self-tallying score voting system | 16 s |
| [15] | Digital signature and timestamp-based authentication system-PBFT | 35 s |
| [16] | Quantum key distribution and blockchain security | 13 s |
| [17] | Blockchain-based, verifiable e-voting system-STAP- LINDDUN | 9 s |
| [18] | biometric based cryptography | 4.8 s |
| [19] | A voting platform that uses blockchain and smart contracts in a Web 3.0 architecture that is secure, distant, and protects privacy | 7.5s |
| [20] | d-BAME | 3.09s |
| [21] | Using blockchain technology to decipher an electronic voting platform for more secure and efficient voting | 2.0s |
| [22] | Democracy Guard: | 1.97s |
| [23] | Bie vote | 1.4s |
| [24] | Blockchain-Powered Electronic Voting System: Effective and Transparent Implementation for Reliable Election Processes | 1.8s |
| Proposed | E-Voting System Using Block Chain Technology and Consensus Algorithms for Secure and Fast Transactions of Votes | 0.3 s |

This is made possible by the HS-EASE algorithm that makes the proposed system efficient, which uses fast symmetric key encryption of the votes and secure public key encryption of the symmetric key, which ensures that only authorized voters have the right to use the vote data while preserving its confidentiality and integrity. Another algorithm, ERCA, also ensures nodes within the network are in consensus and do not carry any possible manipulation and fraud.

## CONCLUSION

The E-voting system proposed, which is a blockchain-based system, incorporates advanced cryptography methods and consensus algorithms to overcome the issues of the traditional and the existing systems of e-voting so as to provide a secure, efficient and transparent process of election. The system makes use of Elliptic Curve Cryptography (DM-ECC) based on Doubling Mechanism to generate keys, Reformed Lamport Merkle Digital Signature (RLM-ds) to authenticate, Hidden Structure Enhanced Attribute-based Searchable Encryption (HS-EASE) to encrypt votes, and Enhanced Raft Consensus Algorithm (ERCA) to conduct secure and speedy transactions with vote transactions to ensure high security and reduce weaknesses. The performance analysis proves to be more efficient with a calculation time of 15ms, 40ms, 70ms, 85ms and 100ms to vote 1,5,10,15 and 20 candidates respectively as opposed to other methods. Vote size is also kept down to minimum with the proposed system getting 15, 40, 100, 170 and 200 vote sizes on the same number of candidates. The system performs well on the verification of voting time with a time of 0 ms, 0.18 ms, 0.2 ms, 0.4 ms, and 0.9 ms indicating time of 1, 5, 10, 15, and 20 candidates respectively. The calculation time of the voting results is much shorter and the time of 50, 500, 1,000, 10,000, and 100,000 votes is 0, 0.1, 0.2, 0.8, and 2 seconds respectively. Throughput and latency analyses also show that the system is in better operation and the proposed system has a higher transaction rate with less latencies as compared to other approaches. This is because of the decentralized nature of the system, which guarantees increased transparency, elimination of vote manipulation, and voter confidence. The research shows that the system is scalable, effective, and secure, and thus it will be appropriate in large scale elections. Nevertheless, enhancements in the future may be on additional scalability to large scale real-world elections, better usability to non-technical voters, biometric authentication to increase safety, hybrid consensus algorithms to optimize, and improvements in privacy preservation methods. Such developments may see blockchain-based e-voting systems become even more flexible, secure, and efficient in future election.

## REFERENCES

[1] Taş R, Tanrıöver ÖÖ. A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry. 2020 Aug 9;12(8):1328. https://doi.org/10.3390/sym12081328

[2] Mikhaylovskaya A. Enhancing deliberation with digital democratic innovations. Philosophy & Technology. 2024 Mar;37(1):3. https://doi.org/10.1007/s13347-023-00692-x

[3] Mochtak M, Lesschaeve C, Glaurdić J. Voting and winning: perceptions of electoral integrity in consolidating democracies. Democratization. 2021 Nov 17;28(8):1423-41. https://doi.org/10.1080/13510347.2021.1918111

[4] Wang KH, Mondal SK, Chan K, Xie X. A review of contemporary e-voting: Requirements, technology, systems and usability. Data Science and Pattern Recognition. 2017 Feb;1(1):31-47.

[5] Kamil M, Bist AS, Rahardja U, Santoso NP, Iqbal M. COVID-19: Implementation e-voting blockchain concept. International Journal of Artificial Intelligence Research. 2021 Jun 30;5(1):25-34. https://doi.org/10.29099/ijair.v5i1.173

[6] Averin A, Bogatyreva V, Degtyarev V. Review of e-voting systems based on blockchain technology. In AIP Conference Proceedings 2023 Oct 13 (Vol. 2910, No. 1, p. 020032). AIP Publishing LLC. https://doi.org/10.1063/5.0167048

[7] Jumaa MH, Shakir AC. Iraqi e-voting system based on smart contract using private blockchain technology. Informatica. 2022 Aug 1;46(6).

[8] Geetha SK, Sathya S, Sakthi ST. A secure digital e-voting using blockchain technology. In Journal of Physics: Conference Series 2021 May 1 (Vol. 1916, No. 1, p. 012197). IOP Publishing. https://doi.org/10.1088/1742-6596/1916/1/012197

[9] Denis González C, Frias Mena D, Massó Muñoz A, Rojas O, Sosa-Gómez G. Electronic voting system using an enterprise blockchain. Applied Sciences. 2022 Jan 6;12(2): 531.https://doi.org/10.3390/app12020531

[10] Ahn B. Implementation and early adoption of an ethereum-based electronic voting system for the prevention of fraudulent voting. Sustainability. 2022 Mar 2;14(5):2917. https://doi.org/10.3390/su14052917

[11] Jain M, Raut S, Ghadge S. E-Voting System Using Machine Learning, Blockchain, and Cryptography. IJSAT-International Journal on Science and Technology. 2025 Jun 23;16(2). https://doi.org/10.71097/IJSAT.v16.i2.6512

[12] Arnob MS, Sarker N, Haque MI, Sarwar MG. Blockchain-based secured e-voting system to remove the opacity and ensure the clarity of election of developing countries. International Research Journal of Engineering and Technology (IRJET). 2020 Jan;7(01):1826-31.

[13] Panja S, Roy B. A secure end-to-end verifiable e-voting system using blockchain and cloud server. Journal of Information Security and Applications. 2021 Jun 1;59:102815. https://doi.org/10.1016/j.jisa.2021.102815

[14] Jafar U, Aziz MJ, Shukur Z. Blockchain for electronic voting system—review and open research challenges. Sensors. 2021 Aug 31;21(17):5874. https://doi.org/10.3390/s21175874

[15] Das A. Usability of electronic voting system in India and innovatory approach. International Journal of Applied Science and Engineering Research. 2015;4(5):633-42.

[16] Alshehri A, Baza M, Srivastava G, Rajeh W, Alrowaily M, Almusali M. Privacy-preserving e-voting system supporting score voting using blockchain. Applied Sciences. 2023 Jan 13;13(2):1096. https://doi.org/10.3390/app13021096

[17] Jayakumari B, Sheeba SL, Eapen M, Anbarasi J, Ravi V, Suganya A, Jawahar M. E-voting system using cloud-based hybrid blockchain technology. Journal of Safety Science and Resilience. 2024 Mar 1;5(1):102-9. https://doi.org/10.1016/j.jnlssr.2024.01.002

[18] Singh A, Ganesh A, Patil RR, Kumar S, Rani R, Pippal SK. Secure voting website using ethereum and smart contracts. Applied System Innovation. 2023 Aug 10;6(4):70. https://doi.org/10.3390/asi6040070

[19] Wiśniewski KP, Zielińska K, Malinowski W. Energy efficient algorithms for real-time data processing in reconfigurable computing environments. SCCTS Transactions on Reconfigurable Computing. 2025;2(3):1-7.

[20] Kumar S, Sharma D. Key generation in cryptography using elliptic-curve cryptography and genetic algorithm. Engineering Proceedings. 2023 Dec 18;59(1):59. https://doi.org/10.3390/engproc2023059059

[21] Mia M, Emma A, Hannah P. Leveraging data science for predictive maintenance in industrial settings. Innovative Reviews in Engineering and Science. 2025;3(1):49-58.

[22] Huang D, Ma X, Zhang S. Performance analysis of the raft consensus algorithm for private blockchains. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2019 Mar 12;50(1):172-81. https://doi.org/10.1109/TSMC.2019.2895471

[23] Wilamowski GJ. Embedded system architectures optimization for high-performance edge computing. SCCTS Journal of Embedded Systems Design and Applications. 2025;2(2):47-55.

[24] Peelam MS, Kumar G, Shah K, Chamola V. DemocracyGuard: Blockchain-based secure voting framework for digital democracy. Expert Systems. 2025 Feb;42(2): e13694. https://doi.org/10.1111/exsy.13694