Science Press

Contents lists available at ScienceDirect

Journal of Safety Science and Resilience

journal homepage: www.keaipublishing.com/en/journals/journal-of-safety-science-and-resilience/

E-voting system using cloud-based hybrid blockchain technology

Beulah Jayakumari [a], S Lilly Sheeba [b], Maya Eapen [c], Jani Anbarasi [d], Vinayakumar Ravi [e,*], A. Suganya [a], Malathy Jawahar [f]

[a] Department of Information Technology Tagore Engineering College Chennai, India
[b] School of Computer Science and Engineering SRM Institute of Science and Technology Ramapuram, Chennai, India
[c] Department of Information Technology Jerusalem College of Engineering, Chennai, India
[d] School of Computer Science and Engineering Vellore Institute of Technology Chennai, India
[e] Center for Artificial Intelligence, Prince Mohammad Bin Fahd University, Khobar, Saudi Arabia
[f] Leather Process Technology Division CSIR-Central Leather Research Institute, Chennai, India

ARTICLE INFO

Keywords:
E-voting
Cloud
Blockchain
Smart contract
Consensus mechanism

ABSTRACT

With the invention of Internet-enabled devices, cloud and blockchain-based technologies, an online voting system can smoothly carry out election processes. During pandemic situations, citizens tend to develop panic about mass gatherings, which may influence the decrease in the number of votes. This urges a reliable, flexible, transparent, secure, and cost-effective voting system. The proposed online voting system using cloud-based hybrid blockchain technology eradicates the flaws that persist in the existing voting system, and it is carried out in three phases: the registration phase, vote casting phase and vote counting phase. A timestamp-based authentication protocol with digital signature validates voters and candidates during the registration and vote casting phases. Using smart contracts, third-party interventions are eliminated, and the transactions are secured in the blockchain network. Finally, to provide accurate voting results, the practical Byzantine fault tolerance (PBFT) consensus mechanism is adopted to ensure that the vote has not been modified or corrupted. Hence, the overall performance of the proposed system is significantly better than that of the existing system. Further performance was analyzed based on authentication delay, vote alteration, response time, and latency.

1. Introduction

Citizens of a democratic country have the right to elect their representatives by voting for the right candidate during elections. Most citizens assume that the conventional physical voting system suffers from a lack of reliability and transparency [1,2]. Moreover, conventional voting systems demand substantial investment of money and time for the smooth execution of electoral processes [2]. Amidst the pandemic crisis, many citizens lack enthusiasm in casting their votes on an election day [3,4]. The introduction of electronic voting (E-voting) system assures the promise of revolutionizing the conventional physical voting system, making it more inclusive and accessible. Furthermore, it considerably saves time and effort for voters and election commission authorities [5]. It also saves the government an enormous expense in conducting fair elections [6]. In this paper, we propose a secure, authenticated, blockchain based E-voting system without the need for tallying authorities to verify and finalize election results [7–9].

In the conventional paper-based voting system, eligible voters must register with the country's election commission before casting their vote. The voting process takes place on election day either through in-person voting or via mail-in ballots; the latter expects submission before a specified deadline for the votes to be counted. Familiarity with in-person voting has led to broader acceptance compared to E-voting. Nonetheless, this method has faced wide criticism because the voting process is vulnerable to interruptions, such as adverse weather conditions, natural calamities as well as lengthy queues at polling stations.

Conversely, while E-voting overcomes these shortcomings, factors such as security, privacy, vote authenticity, and voter identification have inhibited its acceptance among citizens. For example, storing voter information in a database could expose it to potential hacking and unauthorized manipulation [10–12]. Moreover, the apparent absence of human intervention owing to computerized privacy measures has augmented the concerns regarding the efficiency and reliability of E-voting systems. Hence, there is a high need to implement a secure and reliable E-voting system that allows voters to vote conveniently and allows election commission authorities to announce the results

[*] Corresponding author.
E-mail address: vravi@pmu.edu.sa (V. Ravi).

https://doi.org/10.1016/j.jnlssr.2024.01.002
Received 5 October 2023; Received in revised form 23 November 2023; Accepted 8 January 2024
Available online 20 February 2024

transparently.

Hao et al. [13] introduced an E-voting system to achieve end-to-end verifiability without human intervention during registration or tallying. Nevertheless, the pre-computation phase requires access to pre-computed data during the voting phase, thereby introducing a threat to the security of the storage module and the privacy of all ballots.

To address this concern, Shahandashti et al. [14] built an enhanced privacy module, which attains fully automated end-to-end verifiability and provides a significantly stronger privacy guarantee. However, both systems mandate a secure append-only public bulletin board (PBB), as the private key of the signature might be compromised in the setup phase. Additionally, an attacker can alter or include additional ballots that can stay undetected by the tally verification algorithm [15]. A range of researchers have addressed the aforementioned vulnerability of public bulletin boards from multiple angles; for example, removing PBB as a single point of failure was extensively discussed by [16]. [17] showed that for n peers, there should be a minimum of $2n/3$ number honest item collection peers to ensure the correctness of the bulletin board.

Apart from the utilization of effective cryptography and biometric authentication methods to tackle E-voting concerns, a more holistic approach is required to address the increasingly challenging security issues in the digital realm. Recently, researchers have started focusing on blockchain based security solutions in diverse domains. Blockchain is a decentralized ledger operating on a peer-to-peer (P2P) network that utilizes consensus algorithms for block recording and encrypted ledgers [18,19]. This technology exhibits significant potential in addressing multiple security and transparency challenges inherent in E-voting systems. In the survey, [20] suggested authentication and registration as areas of improvement in an E-voting system. In this light, moving toward a reliable E-voting system, we have modified the algorithms employed during voter registration and authentication mechanisms while using blockchain and a cloud server to store the ballots.

Blockchain networks can be classified as public, private, and hybrid blockchain based on the permissions provided to the users and the nodes to access, verify or update the blockchain [21–23]. In a public blockchain, anyone can join the network and view, publish, and store information. Well-known examples of public blockchains include Ethereum and Bitcoin [24–26]. In contrast to public blockchains, private blockchains operate as closed networks, allowing only specific users to access and publish information [27,28]. A hybrid blockchain is a combination of public and private blockchains [29]. In this network, the data can be viewed by anyone, but only authorized users are allowed to publish and store data via smart contracts.

This technology exhibits significant potential in addressing multiple security challenges amidst ensuring the potential transparency inherent in E-voting systems. Many studies insist that authentication and registration are areas of improvement in an E-voting system. With this motivation, the proposed work aims to move toward a reliable E-voting system, employing profound modifications in voter registration algorithms and authentication mechanisms using blockchain and a cloud server to store the ballots [30–33]. In a few cases, information may have various levels of abstraction, where only essential information is revealed to the public and other vital vote count information is secured by hash functions. In this paper, reliability issues such as vote loss and recovery can be fixed using a cloud-based E-voting system with a hybrid blockchain network. Additionally, since a hybrid blockchain is incorporated in the proposed work, it provides more transparency to users while casting their votes and viewing election outcomes than a blockchain implemented on a private blockchain such as Etherium[34].

The motivation of the proposed protocol is to provide end-to-end enhanced security in the voting process and avoid misappropriation of voting result announcements. The contributions of the proposed modules are as follows:

(a) Timestamp-based authentication with a digital signature protocol for validating voters and candidates during registration is proposed, which goes beyond using fingerprints alone to authenticate users and offers an additional layer of protection.
(b) A smart contract for vote casting is employed to verify the authenticity of the voter's vote and eliminate the need for third-party intervention under vote casting. Smart contracts that are tamper-resistant and self-executing result in less chance of fraud or manipulation during the voting process.
(c) The practical Byzantine Fault Tolerance (PBFT) consensus mechanism ensures that the vote has not been modified or corrupted to ensure integrity and secure counting.

This paper is structured as follows. In Section 2, we examine the existing voting system and derive inferences to show the drawbacks that blockchain can rectify. Section 3 describes how this proposed system is advanced when compared to the existing system from various perspectives. Finally, Section 4 concludes the work with the future scope.

2. Related work

Currently, there are many existing E-voting systems that have different benefits and issues. The most significant issues to be identified are lack of security, transparency, and authentication. The recently developed hybrid blockchain technology could be a solution to these issues.

Rathee et al. [6] introduced an IoT-based secure and transparent E-voting system using blockchain technology. This system is implemented in advanced countries. Initially, this system assumes that all the entities involved are trustworthy. It detects threats caused by intruders to rig the vote. The performances are evaluated against various security parameters, such as message alteration, denial of service (DoS), distributed denial of service (DDoS) attacks, and authentication delay.

Pawlak et al. [7] have proposed a non-remote, Internet-based auditable blockchain voting system (ABVS) which is an end-to-end verifiable system. This approach lacks security regarding the voter's identity and involves complex computations. Hence, ABVS is applicable only for small-scale systems.

Panja and Roy [30] introduced an end-to-end verifiable voting system. The user enters the system through unique code to verify whether their vote was recorded and integrated during vote casting and counting phase, respectively. This increases the voter's trust about the system, increasing performance metrics such as robustness and fairness.

Mccorry et al. [33] suggested an Internet-based voting system that provides good results with a flexible consensus algorithm and smart contracts. This system is implemented with no polling station. However, it is difficult to achieve robustness, latency, and privacy in a considerable way.

Kumar et al. [34]. proposed a technique that combines the features of a blind signature scheme with the Boneh–Lynn–Shacham short signature scheme for authentication. In addition, the elliptical curve discrete algorithm (ECD) and Diffie-Hellman assumptions are used to securely transfer the data in the blockchain. Distributed ledger technology (DLT) provides transparency and eliminates the tampering of votes. Voter authentication and repudiation are achieved for every vote by encrypting through elliptic curve cryptography (ECC), which is much faster than the Rivest-Shamir-Adleman encryption (RSA) algorithms. ECC is best suited for key management and signature generation.

Yi [35] suggested that a modified E-voting system ensures the validity of voting that has been polled, which prevents ballot-stuffing attacks. The Non-Interactive Zero-Knowledge (NIZK) proof could be used to enhance the efficiency of the E-voting system.

Panja et al. [36] proposed the first end-to-end verifiable direct recording electronic DRE-based e-voting system using blockchain. This E-voting system uses the Paillier homomorphic encryption algorithm, which reads encrypted messages without decrypting them. This enables the system to verify voters by requiring their ID without revealing their choices.

To provide security to voters, Faber et al. [37] exploited cryptographic techniques that have been implemented along with Ethereum. A proof of concept using blockchain is shown to provide maximum trust among voters. Frooq et al. [38] proposed a framework that supports an ascendible blockchain by employing a flexible consensus algorithm. The chain security algorithm in the voting system ensures the voting transaction is successful. The inscription of transactions using a cryptographic hash and the prevention of attack of 51 % on the blockchain have also been applied. The appraisal of this framework shows that the system can be implemented in a large-scale population.

Divya and Usha [39] proposed a system that provided a firm and demonstrable voter registration and authentication framework, thus stopping a ballot stuffing attack. In this vein, they modified direct-recording electronics with a rectitude and enhanced seclusion (DRE-ip) system so that no adversary could be created. The author also elaborated on the final tally using NIZK proof and dependable multi-party computation.

A BC-based voting system (BBVS) was established by Malkawi et al. [40] in the absence of Jordan for the legislative election system. Here, the authors provided a novel yet secure BC-based E-voting system in which a voter votes on two measures: the first degree is for a group, and the second degree is for distinct group members. This framework implements a recently developed algorithm to nurture acceptable performance both when developing and casting votes for voters.

Goyal et al. [27]. proposed using the tool Ethereum remix and proposed an E-voting system that the Indian government can use to organize the entire election procedure on a digital platform. The proposed system advocated organizing an election process in India through the decentralized application (dApp). This proposed work prompted the combination of data with machine learning.

The proposed framework by Panja [41] employed a handed-down tool called IPFS Ethereum. This framework proposed a cryptographic technique for secret ballot election with an improved false rejection rate design biometric encryption algorithm. The constraint of this framework is less efficient.

Khan et al. [42] explored the BC-based E-voting system to identify the settings for transaction pliability attacks within the system on a BC test bed organizing an E-voting application. The corresponding framework identifies the importance of the block generation rate and net-work delay and highlights directions for future research. The limitations of this proposed work are less certain. The authors tried to highlight the conditions that cause an attack on the system.

Killer et al. [43], the authors introduced a firm, adaptable, and practical BC-based voting system that achieved the properties expected from large-scale elections without needing much from the voters. Receipt-freeness and enforcement resistance were ensured by using a randomizer token for constructing the ballot that acts as a black box for the user. The mechanism adopted ensured an increase in terms of both security and efficiency.

Abuidris et al. [44] suggested a hybrid consensus model that comprises proof of credibility (PoC) and proof of stake (PoS). The MATLAB Amazon EC2 Ethereum tool was used in this study. Smart contracts were deployed to provide a dependable and firm computing environment to ensure the accuracy and safety of the ballot customs. The framework combines the PSC-B chain with the sharding mechanism to ensure the scalable performance of the E-voting system based on BC. Disagreements about the execution of attacks on the proposed hybrid BC and classical BC were performed to analyze the security efficiency and, in addition, to ensure coercion resistance and receipt freeness.

Suralkar et al. [45]. developed a secure E-voting system by using BC technology, fingerprint authentication and ring signature and worked with the Ethereum tool. The proposed framework does not require too many individuals at every degree; thus, the system is more verifiable and secure, but this work is less scalable.

AboSamra et al. [46]. proposed a secure and auditable cryptographic E-voting system to replace the conventional voting methods of the Middle East and North America (MENA) regions to build desirability among people and voters upon the voting system. The proposed E-voting system, predicated on paper ballot mix-nets, requires complex protocols for maintaining shared mix keys. In addition, mix-nets are susceptible to corruption and would be convoluted for large-scale implementation. The proposed scheme provides ballot secrecy, security, and verifiability. Threat and firm analyses were also conducted to prove that the systems resisted known attacks.

Moura and Gomes [47] explored different solicitations that did not receive BC attention. This was done to determine the potential of the application among customers, but there has always been a risk to security and privacy.

Desai et al. [9] suggested that the attainability of pellucid and fair voting systems increased only due to BC-based E-voting services. They also suggested that this approach can be implemented to promote the casting and counting of votes for singing competitions on national television.

Less focused BC application was explored by Zeadally et al. [48]. The authors evaluated the quantitative perspective of BC's suitability and its influence on different applications that did not receive BC attention. BC has gained professional expertise in digital services' legal and technical aspects.

Ahn [26] implemented an early adoption of an Ethereum-based electronic voting system that prevents fraudulent voting by enhancing the safety and reliability of the electronic voting system. González et al. [49] proposed a theoretical based two-phase verification system for privacy preservation in E-voting based on the Ethereum blockchain.

The most significant issues identified in the existing E-voting system are authentication delay, vote alteration, response time, and latency, in addition to lacking reliability, flexibility, transparency, security, and cost-effectiveness in the voting system. The proposed cloud-based E-voting system exploits hybrid blockchain technology to address these issues. It promotes reliability and transparency, as only legitimate registered voters can cast their votes. Moreover, any attempt to alter votes can be significantly captured, and such votes can be nullified. The deployment of blockchain technology with adequate consensus algorithms for block recording and encrypted ledgers, along with smart contracts, ensures security within the E-voting system. In addition, it aims at authentication delay or latency compared to conventional systems and other private blockchain based voting systems. In brief, this approach enhances the response time of the entire electoral process from casting votes to counting votes and declaring electoral results.

3. Proposed system

The proposed system comprises Key Generation Center (KGC), Election Commission Authority (ECA), IoT devices, Edge Server, Cloud Server, and Hybrid Blockchain Network. During the Initialization Phase, the registration of voter, candidate, and their IoT devices, ECA, and the edge server is performed with KGC. KGC checks for the validity of the nodes requesting registration and responds with registration credentials. It generates private keys separately for the voters and candidates. It also maintains both a list of voters and a list of electoral candidates. Once registered, a device authentication request is sent from an IoT device to the ECA, after which the device is sent. The ECA collects and forwards the transaction to the edge server for partial block creation. Then, the edge server decides which transaction should be encrypted and unencrypted for the hybrid blockchain. Partial blocks are also sent to the cloud server where the smart contract validates them. The cloud server then advances to create a full block by executing a consensus algorithm. These full blocks are ultimately added to the blockchain network. The various states of the proposed system are depicted in Fig. 1 as follows:

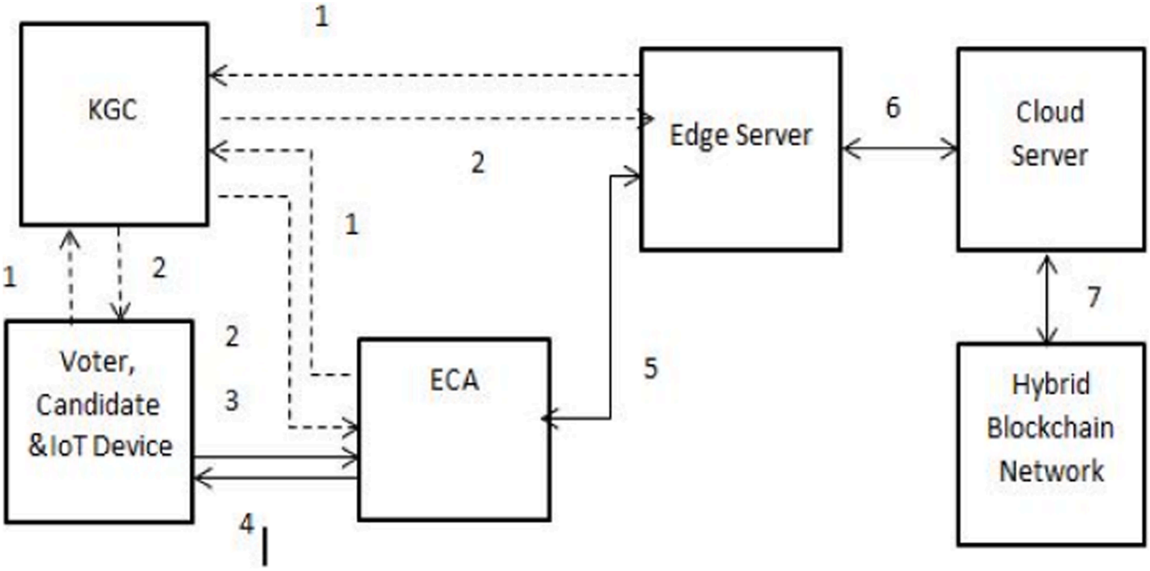

Fig. 1. Proposed System.

1. Registration Request
2. Registration Response
3. Device Authentication Request
4. Device Authentication Response
5. Data relay to the edge server
6. Data relay to the cloud server

Data block addition into the hybrid blockchain network. The notations and abbreviations for the proposed system are listed in Table 1.

The various phases in the proposed E-voting system using Cloud-based Hybrid Blockchain technology are detailed as follows:

3.1. Registration phase

Before the election, all eligible voters and candidates must register their voter identification, biometric information, and IoT devices used during the election process in KGC. Once registered, each voter and candidate are issued the private keys $^{PR}Key\_vi$ and $^{PR}Key\_ci$, respectively. The key generation center maintains a list of registered participants and sends it to the ECA. The following steps must be taken to register voters and their IoT devices before the election process, as shown in Table 2.

Step 1: The ECA chooses the Vid_i, Did_j, PR_{Key}, and MK_{ECA} to compute a Virtual ID $VTid$ of the IoT device, which is shown in Eq. (1):

$$VTid_j = H(Vid_i \parallel Did_i||Si||MK_{ECA}) \tag{1}$$

Step 2: The credentials for each IoT device are generated as in Eq. (2):

$$\mathrm{CD}_j = \mathrm{H}(VTid_j \parallel Si \parallel MK_{ECA} \parallel TS_R) \tag{2}$$

Table 1
Notations and abbreviations.

Notation	Description
KGC	Key Generation Center
ECA	Election Commission Authorities
V	Voter
I	Polled vote
^{TS}Rv	Timestamp of registered voter
Vid	Voter Identification
Did	Device Identification
VTid	Virtual Device Identification
^{PR}Key	Private Key
^{PU}Key	Public Key
H	One way cryptographic hash function
||	Concatenation operation
^{MK} *ECA*	Master key of ECA

Table 2
Steps Involved in the Registration Phase.

Election Commission Authority (ECA)	IoT Smart Device
1)Pick Vid_i, Did_i, Si, MK_{ECA} 2)Compute $VTid{=}H(Vid_i \mid\mid Did_j \mid\mid Si \mid\mid MK_{ECA})$ 3)$CD = H\ (VTid\ \mid\mid Si \mid\mid MK_{ECA}\ ^{\mid\mid}\ TS^{)}_{Rv}$ 4)Pick PR_{Key} randomly 5)Compute $PU_{Key}{=}PR_{Key}\ .G,$ 6)Preload $VTid$, PR_{Key}, PU_{Key}, $H(.)$	
	7) Store VTi, PR_{Key}, PU_{Key}, $H(.)$ in the memory

Step 3: The ECA chooses the private key PR_{Key} randomly and calculates the public key using (3):

$$PU_{Key} = PR_{Key}.G \tag{3}$$

where G is chosen by the ECC algorithm.

Step 4: The ECA stores the following information in the IoT device, which includes $VTid_j$, PR_{Key}, PU_{Key}, $H(.)$.

With this process, the candidate and voter are linked to their corresponding devices. The integration of IoT smart devices, ECAs, and edge servers is needed during deployment.

The cloud server is registered by the ECA offline for reliability. To achieve this, the ECA chooses the original identity of the cloud server as C_{id} and creates temporary identities as CS_{id}. The ECA chooses the random secret c_1 and calculates their temporary as in (4):

$$CS_{id\_T} = \mathrm{H}(C_{id}||c_1 \parallel MK_{ECA} \parallel \mathrm{TScr}) \tag{4}$$

where TScs is the timestamp for registration of the cloud server.

The ECA preloads the cloud server CS with the credentials { C_{id}, CS_{id}}. The cloud server randomly picks its own private key PR_{Key} and calculates the public key using $\mathrm{PU}_{\mathrm{Key}} = PR_{Key}$.G to its secure memory database as { C_{id}, CS_{id}, $\mathrm{PU}_{\mathrm{Key}}$, PR_{Key}, H(.), Eq(a; b); Gg}. It also broadcasts its $\mathrm{PU}_{\mathrm{Key}}$.

3.2. Vote casting phase

Once the registration phase has been completed, all the eligible voters are allowed to cast their vote on the day of the election. After voting, the vote becomes a transaction and needs to be securely stored in the blockchain network. Hence, an authentication protocol must be developed for an E-voting system. Authentication is a major requirement for achieving reliability in an election process. This helps to eliminate duplicate votes and achieves mutual authentication between IoT devices and election commission authorities in the blockchain network. A timestamp-based reliable authentication system establishes the validity of both the voter and the device. The IoT device sends transactions along with both current timestamps and calculates the signature by the hash of its private key, Did, with the current timestamp in the decentralized network. The ECA verifies the validity of the signature and timestamp. If the timestamp is valid, the ECA sends the response message with the transaction ID to the IoT device and adds the corresponding valid block to the blockchain network. Once the vote is cast, it cannot be modified due to the immutable characteristic of blockchain.

Implementing Transparency using Hybrid Blockchain

The proposed online voting system using blockchain eliminates the need for third-party interventions through smart contracts. Smart contracts are pieces of code that may be executed on the blockchain after each transaction. The term “code is law” refers to smart contracts. Since smart contracts are decentralized in blockchain, once executed, they cannot be modified, which significantly improves the efficiency of the voting process.

As we experience in every election involving allegations and accusations between candidates, implementing transparency through the use of a hybrid blockchain has become inevitable, which in turn increases citizens’ trust in the voting system. Hybrid blockchain is a technology that combines parts of public and private blockchains. Transactions in hybrid blockchain can be secured by enabling the required user through the smart contract. Each casted vote is treated as a transaction and is stored with encryption on the blockchain. The blocks generated by the ECA after each transaction include the number of candidates, the number of votes polled to each party, and the total number of votes polled in the particular constituency. The voting-based consensus algorithm has been applied with the help of smart contracts to validate votes and add blocks to the blockchain network.

To create blocks, the following steps are chosen by an ECA:

Step 1: Once votes have been received from voters, the ECA uses the “elliptic curve digital signature algorithm” (ECDSA) to create a signature on a transaction using the following Eq. (5):

$$\mathrm{Txi} = (\mathrm{VIDI};\ \mathrm{TS};\mathrm{I}) \tag{5}$$

using the private key PR_{Key} of the ECA as in (6)

$$\mathrm{SignTxi} = \mathrm{Sig}PR_{Key}(\mathrm{H}(\mathrm{Txi} = (\mathrm{VIDI};\ \mathrm{TS};\mathrm{I})) \tag{6}$$

where Sig(_) is the ECDSA signature generation algorithm.

The ECA then publicly sends (Txi; SignTxi) to all nodes in the blockchain network. Other confidential information, such as to whom the voter casts their vote, must be encrypted using the public key of the ECA before generating signatures on encrypted transactions to preserve the data and maintain transparency. Therefore, a hybrid blockchain has been developed to make some transactions private and other transactions public in a block.

Step 2: The ECA checks every transaction received (Txi; SignTxi) or (EPubG(Txi); ESignTxi) by validating SignTxi or ESignTxi using the public key $\mathrm{Pub}_{\mathrm{Key}}$ of the ECA. The ECA selects the (unencrypted) transaction Txi or encrypted transaction EPubG(Txi) if the signature has not been modified and is valid.

Step 3: If the validation succeeds, the ECA adds the previous block hash (Prev_Block_Hash) and computes the current block hash Cur_Block_Hash on the entire block. The algorithm used for creating blocks in the blockchain network is shown in Table 3.

3.3. Vote counting phase

Once the voting period has ended, the smart contract automatically counts the votes, declaring the results and the percentage of votes polled based on the rules specified in the contract. The election results are then recorded on the blockchain in a transparent and immutable way, making it easy for anyone to verify the authenticity of the results. To achieve consensus, the decisions of most nodes in the network are considered based on the PBFT. The transparency and immutability of the blockchain make it easy for the election to be conducted in a fair and transparent manner and the results to be accurate and valid.

3.4. Dynamic smart node addition phase

In the case of a registered IoT device malfunction, several options can be preferred. The alternative methods are

i. Users can use another registered IoT device.
ii. Suppose in case additional IoT device is unavailable, in this scenario. In that case, the ECA allows the registered voters to cast their vote offline at the voting center already deployed by the ECA.

4. Performance analysis

The software requirements:

Node.js, NPM (Node Package Manager) Meta mask browser, Truffle framework, and Ganache.

Hardware requirements:

Processor: IntelCorei5, Xeon processors or AMD Ryzen.

Memory: ITB.

Diskspace: 100 GB.

The performance of the proposed E-voting system is analyzed based on the authentication delay, vote alteration, response time, and latency as follows:

(i) **Authentication delay**: It is defined as the average time required to validate the voter after scanning their voter card. The delay incurred between the requisition and the authentication time. This delay tends to increase as the number of new voters in the blockchain network increases because checking for every voter in the database before a citizen is authorized to cast his votes is mandatory. As shown in Fig. 2, the authentication delay with ten thousand voters is 2.5 msec with the existing system; however, with the proposed system, the authentication delay is reduced to 1.5 msec. Additionally, when the number of voters increases, the proposed system tends to outperform the existing system. The experimental results show that the proposed system reduces the authentication delay by more than 50 % compared with the existing system, as shown in Fig. 2.

(ii) **Vote alteration**: Vote alteration is defined as a modification in votes due to malicious activities in the blockchain network. It is essential to have the vote unaltered, as it produces erroneous results. The prime way to retain the rate of vote alteration is by providing more secure features in the E-voting system. As depicted in Fig 3, the rate of vote alteration using the existing systems is 2.9 % per ten thousand voters. However, with the proposed system, the rate of vote alteration declined considerably to 1.9 %. On average, the rate of vote alteration has declined by 55%. The experimental results prove that the proposed system is more secure than the existing system by 55 %, as depicted in Fig. 3.

(iii) **Response time** is defined as the time taken for each transaction to be included in the blockchain network. As the number of voters increased, the number of inclusions also increased. It is denoted

Table 3
Addition of blocks in Blockchain.

```
# Algorithm for adding block into blockchain
  Input: $Block_i$, Total number of cloud servers in the blockchain
  Output: Valid block$VBlock_i$
  Step 1: Transmit the received $Block_i$ to all the nodes '$N'$
  Step 2: for each cloud server node $CS_j$ perform the following
  Step 3: Smart contract processing
  Step 4: Set Cons_Vote$_j$ = NO
  Step 5: Calculate hash of the block using$H(Block_i)$
  Step 5.1: if $(H(Block_i) = = H'(Block_i))$then
  Step 5.2: if (validation of Sig using PubKey is successful) then
  Step 5.3:if $(TS_i = = TS_j)$ then
  Step 5.4: Set Cons_Vote$_j$ = TRUE
  end if
  end if
  end if
  Step 6: Add Cons_Vote$_j$ to block 14:
  end for
  Step 7 Set Count= 0
  Step 8: for each vote V reply in count i do
  Step 8.1: if (V is TRUE) then
  Set Count = Count + 1 19:
  end if
  end for
  Step 9:Add block $Block_i$ into the blockchain
  Step 10: Successfully block gets added resulting $VBlock_i$
```

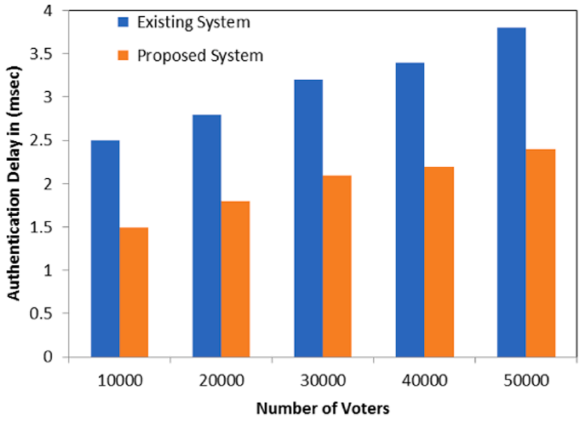

Fig. 2. Authentication delay vs. Number of Voters.

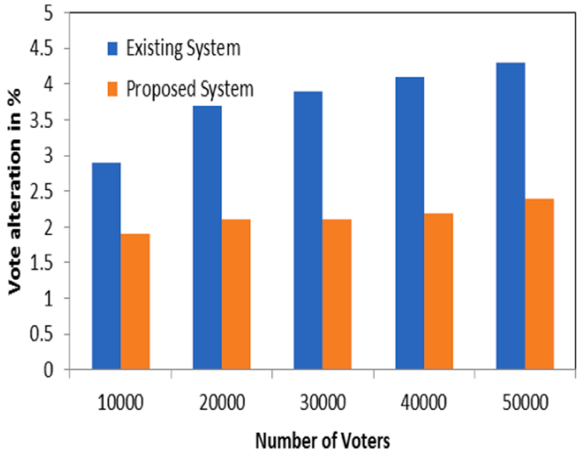

Fig. 3. Vote alteration in% vs. no. of voters.

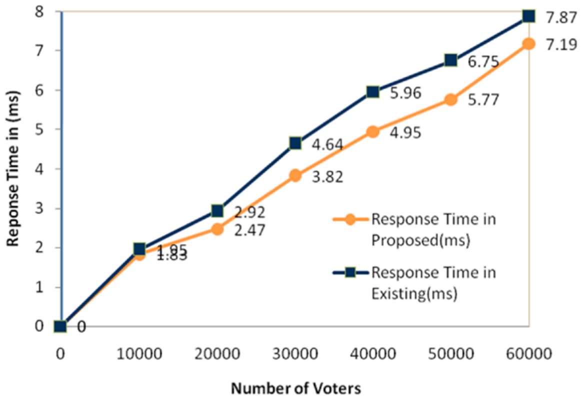

Fig. 4. Response time vs. Number of Voters.

in milliseconds (ms). A considerable reduction in response time is key when voluminous voters participate in E-voting. As shown in Fig. 4, the response time with sixty thousand voters stays at 7.87 ms in the existing system, whereas in the proposed system, the response time is 7.19 ms. The experimental results show that the response time is about 0.7 ms longer than that of the existing system shown in Fig. 4. The proposed system has contributed to significantly reducing the response time compared to the existing system.

(iv) **Latency** is defined as the time taken to delay the execution of each transaction in the blockchain network. Latency is directly proportional to the increase in the number of voters in the network. Lowering latency is also a key measure in an E-voting system. As shown in Fig 5, the latency is 7.97 ms with sixty thousand voters; however, the latency of the proposed system decreases significantly to 7.55 ms. As the number of voters increases, the latency increases significantly. However, the experimental results clearly show that the latency is lower than that of the existing system by 0.7 ms, as shown in Fig. 5.

5. Conclusion & future work

The purpose of developing E-voting system using cloud-based hybrid

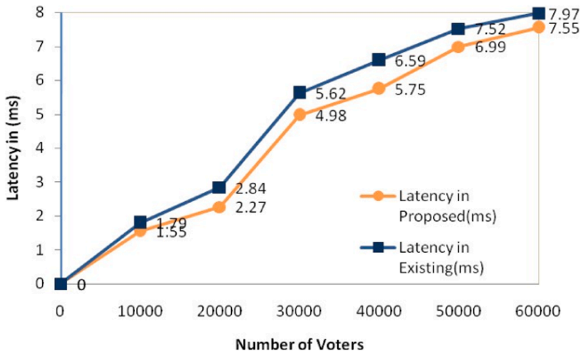

Fig. 5. Latency vs. Number of Voters.

blockchain technology is to improve the security, transparency, and reliability requirements of the existing E-voting system. This helps people in democratic countries rely more on voting processes to choose their leaders. Additionally, they can help government and voting authorities conduct time- and cost-effective elections. Modern blockchain technology completely alleviates malicious or incomplete transactions in the blockchain network without third-party interventions. Reliability and transparency were achieved during vote casting through timestamp-based authentication protocol and digital signature algorithm. A voting-based consensus for block addition was obtained using the PBFT algorithm during vote counting to publish authenticated results. Finally, it is concluded that the proposed system outperforms the other systems in terms of authentication delay, vote alteration, response time, and latency.

In the future, regular AI-enabled security audits can be conducted in collaboration with cyber security experts to identify and address vulnerabilities in the system. Educating voters, election officials, and the general public about the benefits of blockchain-based E-voting is critical for addressing misconceptions and promoting understanding to build trust in the system. It should be ensured that the system falls in tandem with election laws and regulations in different jurisdictions. Two-factor voter identity verification methods can be used in combination with blockchain technology. Moreover, E-voting system must be made more user-friendly for a diverse range of voters, including those with disabilities or limited technical expertise.

Ethics statement

Not applicable because this work does not involve the use of animal or human subjects.

CRediT authorship contribution statement

Beulah Jayakumari: Writing – original draft, Methodology, Data curation, Conceptualization. **S Lilly Sheeba:** Conceptualization, Methodology, Visualization, Validation, Resources, Investigation. **Maya Eapen:** Conceptualization, Methodology, Visualization, Validation, Resources, Investigation. **Jani Anbarasi:** Conceptualization, Methodology, Visualization, Validation, Resources, Investigation. **Vinayakumar Ravi:** Writing – review & editing, Supervision, Methodology, Conceptualization. **A. Suganya:** Methodology, Visualization, Software, Resources, Investigation. **Malathy Jawahar:** Methodology, Visualization, Resources, Data curation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] J. Huang, D. He, M.S. Obaidat, P. Vijayakumar, M. Luo, K.K.R. Choo, The application of the blockchain technology in voting systems: a review, ACM Comput. Surv.(CSUR) 54 (3) (2022) 1–28.

[2] A. Alam, S.M.ZUr Rashid, Md.A Salam, A. Islam, Towards Blockchain-Based E-voting System, in: International Conference on Innovations in Science, Engineering and Technology (ICISET), 2018. ISBN: 978-1-5386-8524-2.

[3] R. Hanifatunnisa, B. Rahardjo, Blockchain based e-voting recording system design, in: 11th International Conference on Telecommunication Systems Services and Applications (TSSA), 2017, pp. 1–6.

[4] J. Chen, J. Wu, H. Liang, S. Mumtaz, J. Li, K. Konstantin, A.K. Bashir, R. Nawaz, Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation, IEEe Trans. Ind. Appl. 56 (4) (2019) 4478–4488.

[5] Y. Dalvi, S. Jaiswal, P. Sharma, E-Voting using Blockchain, Int. J. Eng. Res. Technol. (IJERT) 10 (03) (2021).

[6] G. Rathee, R. Iqbal, O. Waqar, A.K. Bashir, On the Design and Implementation of a Blockchain Enabled E-voting application within IoT-Oriented smart cities, IEEe Access. 9 (2021) 34165–34176. Feb.

[7] M. Pawlak, A. Poniszewska-Mara«da, N. Kryvinska, Towards the intelligent agents for blockchain e-voting system, Proc. Comput. Sci. 141 (2018) 239–246. Jan.

[8] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, P. Vora, Scantegrity: end-to-End voter verifiable optical-scan voting, IEEE Secur. Privacy 6 (3) (2008) 40–46. Jun.

[9] S. Desai, M. Han, L. Li, Z. Li, J. He, X. Xu, ‘Untampered Electronic Voting in Entertainment Industry: a blockchain-based implementation, in: 20th Annual SIG Conf. Inf. Technol. Educ., New York, NY, USA, 2019, p. 166. Sep.

[10] A.A. Monrat, O. Schelén, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, IEEe Access. 7 (2019) 117134–117151. Aug.

[11] T.A Syed, A. Alzahrani, S. Jan, M.S. Siddiqui, A. Nadeem, T. Alghamdi, A comparative analysis of blockchain architecture and its applications: problems and recommendations, IEEe Access. 7 (2019) 176838–176869. Dec.

[12] W. Gao, W. Hatcher, W. Yu, ‘A survey of Blockchain: techniques, Applications, and Challenges, in: 27th International Conference on Computer Communication Networks (ICCCN), 2018, pp. 1–11. Jul.

[13] F. Hao, M.N. Kreeger, B. Randell, D. Clarke, S.F. Shahandashti, P.H.J. Lee, Every vote counts: ensuring integrity in large-scale electronic voting, USENIX J. Election Technol. Syst. 2 (3) (2014) 1–25. July.

[14] F. Shahandashti Siamak, H. Feng, DRE-ip: a verifiable e-voting scheme without tallying authorities, in: 21st European symposium on research in computer security, 2016, pp. 223–240. Sep.

[15] J. Al-Jaroodi, N. Mohamed, Blockchain in Industries: a survey, IEEe Access. 7 (2019) 36500–36515. Feb.

[16] H.N. Dai, Z. Zheng, Y. Zhang, Blockchain for Internet of Things: a survey, IEEe Internet. Things. J. 6 (5) (2019) 8076–8094. Oct.

[17] K. Wüst, A. Gervais, Do you need a blockchain? Crypto Valley Conf. Blockchain Technol. (CVCBT) (2018) 45–54. Jun.

[18] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, M. Alazab, Blockchain for Industry 4.0: a comprehensive review, IEEe Access. 8 (2020) 79764–79800. Mar.

[19] J. Liu, Z. Liu, A survey on security verification of blockchain smart contracts, IEEe Access. 7 (2019) 77894–77904. Jun.

[20] F. Rabia, A. Sara, T. Gadi, A survey on e-voting based on blockchain, in: 4th International Conference Netw., Inf. Syst. Acad. Manage. Perspect. Security, Apr. 2021, pp. 1–8.

[21] M.A. Cheema, N. Ashraf, A. Aftab, H.K. Qureshi, M. Kazim, A.T. Azar, Machine learning with blockchain for secure E-voting system, in: 1st International Conference of Smart System and Emerging Technology (SMARTTECH), 2020, pp. 177–182.

[22] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, in: IEEE International Congress on Big Data, 2017, pp. 557–564. Jun.

[23] M. Alharby, A. Aldweesh and A.V. Moorsel, “Blockchain-based smart contracts: a systematic mapping study of Academic Research" Sep. 2020.

[24] M.H. Nasir, M. Imran, J.S. Yang, Study on E-voting systems: a blockchain based approach, in: IEEE International Conference Consumer Electronics- Asia (ICCE-Asia), 2021, pp. 1–4. Nov.

[25] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, M. Badra, Analysis of blockchain solutions for E-voting: a systematic literature review, IEEe Access. 10 (2022) 70746–70759. Jan.

[26] B. Ahn, Implementation and early adoption of an Ethereum-based electronic voting system for the prevention of fraudulent voting, Sustainability. 14 (5) (2022) 2917. Mar.

[27] J. Goyal, M. Ahmed, D. Gopalani, A privacy preserving E-voting system with two-phase verification based on Ethereum blockchain, Res. Sq. (2022) 1–33. Jun.

[28] K.L. Ohammah, S. Thomas, A. Obadiah, S. Mohammed, Y.S. Lolo, ‘A survey on electronic voting on blockchain, in: Proc. IEEE Nigeria 4th Int. Conf. Disruptive Technol. Sustain. Develop. (NIGERCON), 2022, pp. 1–4. Apr.

[29] M.V. Vladucu, Z. Dong, J. Medina, R. Rojas-Cessa, E-voting meets blockchain: a survey, IEEe Access. 11 (2023) 23293–23308, https://doi.org/10.1109/ACCESS.2023.3253682.

[30] S. Panja, B. Roy, A secure end-to-end verifiable e-voting system using blockchain and cloud server, J. Inf. Secur. Appl. 59 (2021) 102815. ISSN 2214-2126Jun.

[31] S.S. Hossain, S.A. Arani, M.T. Rahman, T. Bhuiyan, D. Alam, M. Zaman, E-voting system using blockchain technology, in: Proc. 2nd Int. Conf. Blockchain Technology and Applications, 2019, pp. 113–117. Dec.

[32] F.P. Hjálmarsson, G.K. Hreiòarsson, M. Hamdaqa, and G. Hjálmtýsson,"Blockchain-based E-voting system'', in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), pp. 983986.

[33] P. McCorry, S. Shahandashti, F. Hao, A smart contract for boardroom voting with maximum voter privacy. Financial Cryptography and Data Security, Springer, Sliema, Malta, 2017, pp. 357–375.

[34] M. Kumar, S. Chand, C.P. Katti, A secure end-to-end verifiable internet-voting system using identity-based blind signature, IEEe Syst. J. 14 (2) (2020) 2032–2041.

[35] H. Yi, Securing e-voting based on blockchain in P2P network, EURASIP. J. Wirel. Commun. Netw. (137) (2019). May.

[36] S. Panja, S. Bag, F. Hao, Bi. Roy, Smart contract system for decentralized borda count voting, IEEE Trans. Eng. Manage. (2020). May.

[37] FD. Giraldo, MC. Barbosa, yCE. Gamboa, Electronic voting using blockchain and smart contracts: proof of concept, IEEE Latin America Trans. 18 (10) (2020). Oct.

[38] M.S. Farooq, U. Iftikhar, A. Khelifi, A framework to make voting system transparent using blockchain technology, IEEe Access. 10 (2022) 59959–59969.

[39] K. Divya, K. Usha, Blockvoting: an online voting system using block chain, in: Int. Conf. Innovative Trends in Information Technology (ICITIIT), 2022, pp. 1–7. Feb.

[40] M. Malkawi, M.B. Yassein, A. Bataineh, 'Blockchain based voting system for Jordan parliament elections, Int. J. Electr. Comput. Eng. 11 (2021) 4325–4335. Oct.

[41] S. Panja, Zero-knowledge proof, deniability and their applications in blockchain, E-voting and deniable secret handshake protocols, Diss. Indian Stat. Inst.-Kolkata (2021).

[42] K.M. Khan, J. Arshad, M.M. Khan, Secure digital voting system based on blockchain technology, Int. J. Electron. Gov. Res. 14 (1) (2018) 53–62. Jan.

[43] C. Killer, et al., Provotum: a blockchain-based and end-to-end verifiable remote electronic voting system, in: 2020 IEEE 45th Conference on Local Computer Networks (LCN), IEEE, 2020.

[44] Y. Abuidris, R. Kumar, T. Yang, J. Onginjo, Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding, Etri J. 43 (2) (2021) 357–370. Apr.

[45] S. Suralkar, S. Udasi, S. Gagnani, M. Tekwani, M. Bhatia, E-voting using blockchain with biometric authentication, Int. J. Res. Analyt. Rev. 6 (1) (2019) 77–81. Jan.

[46] K.M. AboSamra, A.A. AbdelHafez, G.M.R. Assassa, M.F.M. Mursi, A practical, secure, and auditable e-voting system, J. Inf. Secur. Appl. 36 (2017) 69–89. Oct.

[47] T. Moura, A. Gomes, 'Blockchain voting and its effects on election transparency and voter confidence, in: 18th Annual International Conference on Digital Government Research, New York, NY, USA, 2017, pp. 574–575. Jun.

[48] S. Zeadally, J.B. Abdo, Blockchain: trends and future opportunities, Internet Technol. Lett. 2 (6) (2019) e130. Nov.

[49] C. Denis González, D. Frias Mena, A. Massó Muñoz, O. Rojas, G. Sosa-Gómez, Electronic voting system using an enterprise blockchain, Appl. Sci. 12 (2) (2022) 531.