A Secure E-Voting System With Blockchain Using Face Authentication Technology

N Sundareswaran[1*], Y Mohan Sai Reddy[2], Y Sampath Kumar Reddy[3],
Y Nandhu Kumar Reddy[4] and G Venkata Hemanth[5]
{vethasundares@gmail.com[1], mohansaireddy17@gmail.com[2], sampathreddy3650@gmail.com[3],
nandhu939880@gmail.com[4], hemanthn268@gmail.com[5]}

Department of Computer Science, Kalasalingam Academy of Research and Education, Krishnan Kovil,
Virudhunagar, Tamil Nadu, India[1, 2, 3, 4, 5]

Abstract. It has been challenging for a long time to build a dependable electronic voting system combining the simplicity of use and adaptability of electronic voting systems with the safety and justice of contemporary democratic programs. This article, still under development, looks at how blockchain technology could help to enable the creation of widely used electronic democracy systems. The paper presents a smart electronic democracy system, including an electronic voting form structure grounded on blockchain technology. This system aims to address some of the concerns that are present in existing structures and investigates some of the important blockchain architectures where ideas might be found. The paper describes the idea and architecture of the system, together with voter registration, voting, and smart contract-based result validation. By means of simulated elections, it assesses the performance of a blockchain-based voting system and probes numerous aspects like cost-effectiveness, scalability, and security. Based on the results, blockchain technology presents a transparent, unbreakable, reasonably cheap approach for running mass elections. Apart from that, the research highlights issues including the network's scalability and transaction fees, as well as offers recommendations for future improvement of the situation. This paper aims to show how blockchain technology could change electronic voting and guarantee transparency, trust, and accessibility in modern political processes.

Keywords: Registration of voters, Blockchain, Face authentication technology, Transparency in elections.

1 Introduction

Long-standing difficulty has been developing a major strength area for an e-projecting polling form structure that supplies the simplicity and flexibility of electronic frameworks together with the security and rationality of current popularity-based plans. [8] This work-in-progress outlines how blockchain technology might help to create somewhat extensively utilized electronic vote-based systems.

The implementation of a distributed e-voting platform via the blockchain is examined in this paper. [17] Using the distributed, open, and unchangeable character of blockchain technology, the suggested approach seeks to solve the flaws in current online voting systems. [16] By using distributed ledger technology (DLT) and smart contracts, the system enhances the security, dependability, and economy of the cost of running major elections. By use of an internet network connection to their computers, voters may choose their ballots at any time and from any place throughout a certain period, thanks to the accessibility that electronic voting

ICITSM-Part I 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2357779

systems offer. [18] The public key is used to protect information for the Election Commission database; the private key lets people vote.

Hybrid encryption that uses the RSA and AES algorithms encrypts vast volumes of data. [19] Whereas RSA encrypts the AES key for safe distribution, AES encrypts the data. The AES key is decayed for the electoral commission with an RSA key. [20] Blockchain, open CV, and face authentication help to stop repeated entries for false voting. This helps the e-voting procedure and lowers the fake vote offense occurrence during the election. We particularly assess the limits of suitable record upgrades by showing a logical assessment; more especially, the example of a democratic contest helps to show these limits. [21] The blockchain-based program supervises the voting expenses as well as the flawless voting across a nation's democracy fight.

OpenCV is used for facial recognition, MySQL is used for database storage, and Java (J2EE, JSP, and Servlets) is used for the front end of the proposed system [22]. Because their storage on the blockchain network uses cryptographic hash codes, votes are visible and unchangeable. Preview of the administrative and commission modules includes candidates' administration, voter validation, and voter verification.

Developing electronic voting systems is a daunting task and has faced numerous challenges over time in ensuring the security, transparency, and reliability of the voting process. Legacy electronic voting systems are notoriously susceptible to tampered votes and fraudulent impersonation. Blockchain, as a technology, could be the solution tightly needed to over all these issues since this will allow the system to work in decentralized conditions and it is also immutable transparent calculation. Seems like Blockchain may have something to say about that too, as recent research suggests that blockchain can be used to make voting more secure and transparent by providing trust in the electoral process [23]. In addition, to enhance the security and privacy of the voting system, advanced cryptographic techniques are also proposed including multi-level secret sharing in cloud computing solutions [24]. In this paper, we study a way to exploit blockchain while utilizing biometric authentication technologies, including face recognition systems as an approach for simplifying property and scaling electronic voting actively.

2 Related works

Concentrating on the enhancement of security and anonymity of electronic voting systems, Liu, Y., & Wang, Q [1] propose a stronger blockchain protocol. Ring signatures and homomorphic encryption are suggested by the authors to protect the identity of the voters. Privacy Some cryptographic protocols are homomorphic, allowing computations to be performed on encrypted data without decrypting for the purpose of keeping privacy of the votes even when they are manipulated. Ring signatures ensure that the identity of the voter remains hidden as they hide the identity of the actual signer among a group, effectively making it impossible to determine the voter. The aim of this protocol is to address the problems of security and privacy that exist in blockchain voting systems, while preserving voter’s anonymity and the election process integrity. While the proposed approaches offer significant improvements in security and privacy, they fail to achieve quantitative accuracy guarantees.

H. [2] presents blockchain based secure electronic voting with cryptography-based identity privacy preserving. Zero-knowledge proofs (ZKPs) applied in the protocol allow a voter to prove that they have a valid vote without revealing their name or any private information. The blockchain ensures the integrity of the data throughout the voting process by ensuring that, once they have been cast, votes cannot be altered. To address concerns of privacy and openness of e-voting systems, the paper also identifies the key requirement to retain voters' privacy while ensuring that votes are countable and verifiable. Specific accuracy values or success rates are not provided, but the authors suggest that their approach is practical and secure.

The work of Mookherji, S. et al., (2018) uses a smart contract to impel confidence in the veracity of the voting system amongst the voters who voted on a blockchain based E-voting system. [3]) or based on Ethereum smart contracts the 3, the proposed method automatizes the vote counting and verifying process, making the entire process transparent and auditable. Smart contracts ensure automated and validated counting of votes, thereby reducing human error and potential manipulation. With an open and unchangeable record of the count of ballots so voters can see their vote was counted, the writers argue this fosters voter confidence. Their research demonstrates how smart contracts can help enhance transparency and trust of e-voting systems. No accuracy numbers were provided, but the primary benefit from the method is its blockchain-based verification and ability to instantly count votes.

Hardwick, F. et al. [4] explores how concepts drawn from IoT security can be adapted to Voting systems based on blockchain. They propose a more honest voting system using the blockchain that prevents inside as well as outside threats to the integrity of the data. Their focus is on protecting IoT devices that may play a role in the voting process – in a bid to shield them from potential cyber-attacks that could undermine the electoral process. All activities are auditable and no votes can be altered, because the technology is based on the blockchain. While no detailed numbers on system trust or performance improvements appear in this article, the authors suggest that the system could be made more trustable by integrating the IoT security and using blockchain.

Hjálmarsson, F. et al., Employing blockchains for ensuring data integrity in the decentralized problem-solving process, Communications One key aspect so far not treated in literature is the use of blockchain tech- nology to ensure data integrity and decentralization. [5] et al describe a protocol for distributed e-voting. Just like the blockchain-based systems such as Bitcoin, their system operates under the concept that no single entity owns the database. Since this distributed technique allows all players to access and check the data, openness is ensured and fraud is prevented. The authors emphasize that the inherent unchangeability of blockchain guarantees that the cast votes cannot be altered, thus preserving vote integrity. While specific results about systems performance or correctness are not provided, the report underscores how decentralization does make it “more tamper resistant.”

Hajian Berenjestanaki, M. Of et al. [6], [11] consider the use of the well-known RSA asymmetric cryptosystem in security of e-voting systems. One species of public-key encryption RSA ensures the secure transfer of data over potentially unsafe networks. This paper demonstrates how RSA can encrypt the votes with the public keys and private keys can be used to decrypt the votes, thus protecting the transmission of the vote. This ensures that votes are kept secret during transmission, and prevents rogue parties from modifying vote records. The value of the work lies in using well-known public-key cryptography methods for enhancing the security of blockchain based e-voting systems, but the article does not present the accuracy measures.

Focusing on the core concepts of cryptocurrencies such as Bitcoin as well as their application to blockchain-based e-voting systems, Rathee, G., Iqbal, R., et al. [7] explains that the use of e-voting's decentralization and immutability characteristics helps to ensure the integrity of data. The concentration of the voting database contributes to making the voting system less dependent on the central authority as a result decreasing the risk of manipulation and fraud. The research demonstrates that blockchainâ€™s cryptographic components are suitable for building a transparent and non-modifiable record for recording the votes and ensure the accuracy and integrity of the election results. Nevertheless, some info on the accuracy or performance of e-voting is missing.

Raikar, D., and Vatsa, A. et al. [9] extended a similar previous work by investigating Ethereum smart contracts to enable the automatic enforcement of a voting processes. Is legit-We propose there is some degree of per incidence in the e-voting process as well as space for optimization in vote counting.From the Ethereum’s blockchain standpoint, the authors claim that by automatizing vote counting and verifiable counting, Ethereum smart contracts might help to keep transparency, which could help to avoid the fraud and manipulation, and then it beside it can help: The issue of scalability and effective- ness of blockchain-based e-voting system to successfully handle huge-number e-voting is then raised by the authors The writers main contribution of document is the introduction of smart contracts as an improved e-voting process boosting tool in Therefore, we can state that is still scope e-voting and validation, space for optimization for voting processes. While detail performance measures are not provided, scalability and openness dominate.

On Ethereum contracts, Ramesh, S. S., Venkataraja, D., and Bharadwaj, R. [10] propose a secure E-voting blockchain system with vote recording, and carry out aproper verification as optional component. Smart contracts ensure that the vote is automatic, irreversible, and verified in general. The purpose is to preserve free and fair electioneering and to prevent votes from being revised once they have been cast. Using both the Ethereum blockchain and smart contracts [1], the authors say, provides greater security and transparency to the voting process and could potentially restore trust in elections. Despite not providing any specific performance or accuracy results, they emphasize that the use of this system ensures verification and immutability.

Lopes, J., Pereira, J. L. [11] provides an insight into secure electronic voting and guidelines on how to build electronic systems for voting that provide strong security guarantees. It is emphasized in the paper that cryptographic schemes are required to ensure vote privacy and prevent data manipulation. The paper also highlights the challenging task of securing e-voting systems against numerous threats, such as system failures or malicious attacks. Even though the paper gives new, more detailed guidelines for the security of e-voting in general, there are no specific algorithms or accuracy results.

Doost, M., Kavousi, A., Mohajeri. [12] Present an enhanced blockchain e-voting system that prevents duplication and modification of votes. Their method for doing that guarantees each vote is one of a kind, and once it is cast cannot be altered using cryptographic hashes. Every vote has a HMAC-SHA1 hash based on the SHA hash. (making it unmodifiable and impossible to cast fake votes) Specific accuracy figures are not provided, but this approach ensures the integrity of the election product and reduces the likelihood of casting more than one vote.

With the aim of enhancing the security and the privacy, Marouan, A., Badrani, M., and Zannou, A [13] and colleagues propose a blockchain-enabled e-voting system using homomorphic encryption. This method makes sure you're just revealing the contents of a vote by allowing the vote to be encrypted in a way that completely possible to process votes without decrypting them again. Additionally, the system aims to spread the data storage of votes and the computational activities so as to improve security and resistance to manipulation. Although no specific accuracy or performance threshold is provided, this paper provides an interesting way to enhance the security/privacy of the blockchain-based voting system.

Gupta, S., Gupta, K. K., & Shukla, P. K [14] refers to methods employed to preserve Electronic voting systems from creating cryptographic weaknesses. By identifying potential vulnerabilities in cryptographic schemes, they recommend ways to create blockchain voting systems that are more resistant to these new types of security threats. Their work focuses on ensuring that the e-voting system is secure even when new cryptography attacks rear their head. Some suggestions on how to protect such systems from hazards that evolve over time follow, by the authors who do not provide specific performance or accuracy numbers.

Gao, S., Zheng, D., Guo, R., Jing, C., &Hu, C. [15] et al introduces a blockchain-based elect voting system with group signatures, which can ensure the anonymity and privacy. Group signatures ensure that the identity of any single signer remains anonymous and allow votes to be signed by a group of voters. Its technology guarantees the solidity and integrity of the voting's data through the immutably recorded votes on the blockchain that can never be altered or erased. While specific accuracy or performance results are not addressed, this method resolves both the problem of anonymity and the problem of integrity in e-voting.

3 Methodology

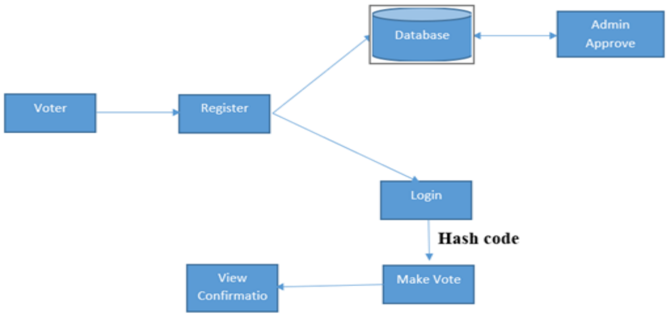


Fig.1. Process Flow of E-Voting System.

The first stage in the electronic voting procedure is registration by voters entering their information into the Register module. This covers personal information and biometric data like face authentication to guarantee a distinctive identity. The database gets and safely keeps the registration data. But first, administrative clearance is required before voting rights based just on registration may be awarded. By means of data validation and credential verification, the Admin Approve module guarantees the voter's eligibility. Voters cannot vote once their data is permanently entered into the database following administrator approval.

Fig.1 shows how a safe online voting system works. A voter first registers using the Register module, and the Database stores the information. Before the voter may advance, the Admin has to approve her registration. Approved voters can log in, which then creates a hash code guaranteeing the integrity and security of the voting process. The voter can then Make Vote; the View Confirmation module shows a confirmation of the vote. Each vote is securely salted for validation, and this flow guarantees that only confirmed users may vote.

3.1 Voter Registration Module

The first phase wherein qualified voters register themselves in the system is the Voter Registration Module. Voters provide their information—name, ID, biometric data (facial authentication)—through the Register portal. For future proof, the system keeps this data in the database. This module guarantees that the voting process may be participated in only authorised people. By avoiding impersonation and duplicate registrations, biometric authentication increases security.

3.2 Database Management Module

As the single source of truth for all voter data, login data, and vote information, the Database Management Module Stores Voter information in the database during the registration process. This module is also managed by the administrator for validation, and acceptance of voter information. The database ensures the safe record and search of voter information, while illegal access is prevented. It is absolutely necessary for recording the hashcoded votes and for voter authentication at login.

3.3 Admin Approval Module

Only authorized voters can proceed to the login and voting phases of the Admin Approval Module. Validating and confirming the registered voters falls to the Admin Approval Module. The administrator verifies the correctness of the information that a voter provides and searches for duplicate or invalid registrations. This module maintains data integrity and election fairness and keeps illegal users off of the system.

3.4 Voting and Hash Code Generation Module

After vote confirmation, the local module for voting ballot and hash code generation enables a confirmed voter to actually cast their ballot by the Voting Module. For the vote after is in text, a unique hash code is generated. Like a digital fingerprint, this hash code makes each vote tamper- and access-proof. The hash resides on the blockchain, thus guaranteeing data integrity and transparency. The hash validation will detect changes, so it protects the integrity of the vote even when it is tampered with by an attacker.

3.5 Authentication and Verification Module

Only confirmed users are allowed access to the Voting System using the Authentication and Verification Module. It uses facial recognition technology to verify the voter’s identity before he is able to continue. The biometric verification solution suppresses any immoral act such as impersonation, multiple voting case, etc., by matching the voter's facial constitution with the stored data. It also increases the security and the accuracy when an user is authenticated successfully.

3.6 Blockchain Model

The voting encryption technology utilizes a hybrid cryptographic scheme, applying AES for high-speed data encryption and the RSA method for Verifiabelsenden of AES-Encryption keys. The encryption technique ensures that data cannot be read even if hackers tap into information in transit.

Let the input vote data be a string:

$$V = \{v1, v2, …., vn\} \qquad (1)$$

Step 1: ASCII Conversion

$$A_i = ord(v_i), \forall_i \in [1, n] \qquad (2)$$

$$A = \{a_1, a_2, …, a_n\}$$

Step 2: Polynomial Encoding

$$P(x) = a_1 + a_2x + a_3x^2 + … + a_nx^{n-1} \qquad (3)$$

Step 3: Weighted Hash Compression

$$S = (k\sum i=1\ H_i \cdot w_i) \bmod q \qquad (4)$$

Step 4: Final Hash Output

$$Hash(V) = hex(S) \qquad (5)$$

3.6.1 Vote Hash Through Blocks

After Solomon Hash Code Algorithm encryption, every vote is processed to a hashing process. The vote encryption produces a unique hash code, being indelible digital fingerprint of each casted vote. It is a hash, the Solomon Hash that is designed to be a reversible one-way no-collision mapping which represents votes in a unique irreproducible manner. Other party (blockchain network) takes the hashed vote via its consensual process as a proof and use it to verify and record as a new block.

More specifically, voters anonymously connect their ID and timestamp to their vote hash through blocks that form a tamper-resistant blockchain voting history chain. By keeping raw votes in plain sight and prohibiting modification after recording, the data structure is fully transparent while allowing for traceability and announcement of lost data.

Smart Contracts A blockchain-based network is utilised to automate public voting and the voting system by deploying smart contracts using Solidity (compatible with Ethereum). The contracts verify the legitimacy of votes, they prevent accidental or intentional double votes, they also calculate results (on-chain) preventing tampering with results.

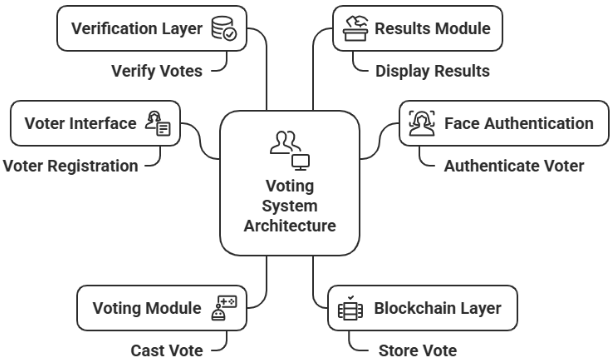


Fig. 2. Model Architecture

The process Fig 2 that determines the fundamental framework of the e-voting uses the Solomon Hash code technique; the data is secure. A small amount of data can be saved in a computer disk and fog server. It contains voter to candidate registration.

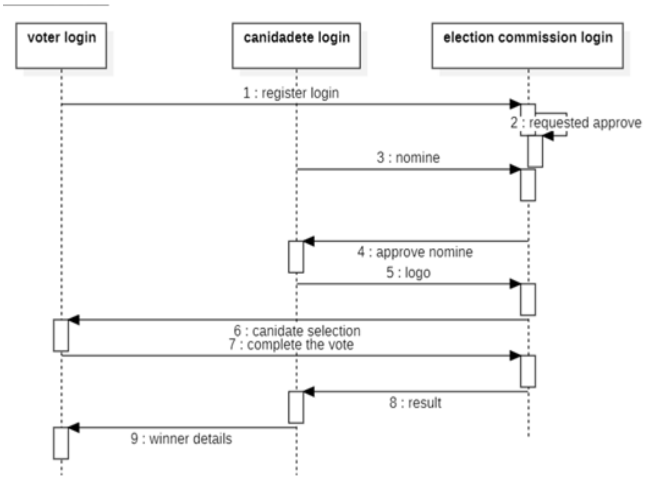


Fig. 3. Sequence Diagram Representation

Our sequence diagram Fig 3 illustrates how processes work together and in a specific order. To encrypt the data in this suggested fashion, we use the Hash-Solomon Code Algorithm, which we first proposed in our component diagram.

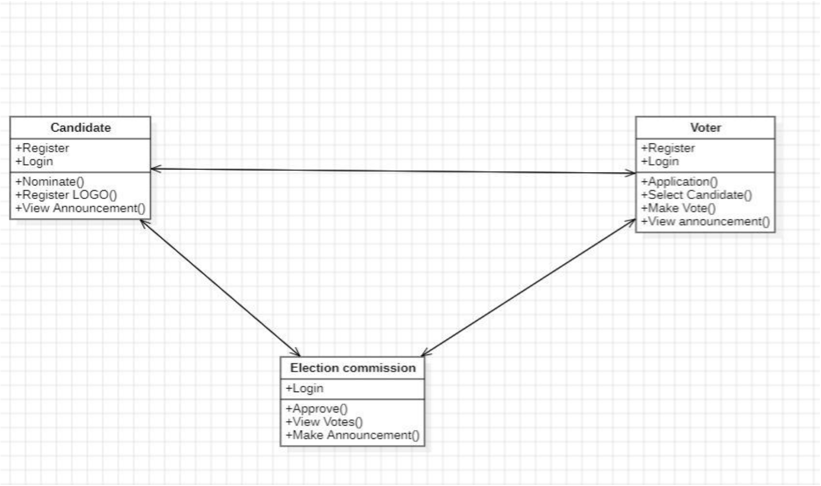


Fig. 4. Class Diagram Representation

The data acquired in a state diagram Fig 4 is proposed as the first. The algorithm of the Hash Solomon programming code is used to encrypt the given proposed data. In some cases, this is a reasonable abstraction, while in others, it is not.

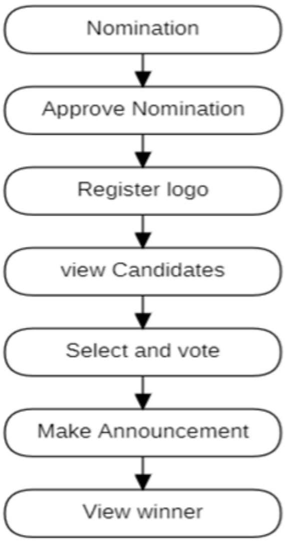


Fig. 5. State Diagram Representation

There are various types of state diagrams, each with its slight variations and semantics. In this diagram, Fig 5 the data is given first. The Hash-Solomon code Algorithm is used in this component diagram to encrypt the data. State diagrams necessitate that the system being depicted consist of a limited number of states; in certain cases, this is accurate, and in other cases, it is a suitable abstraction.

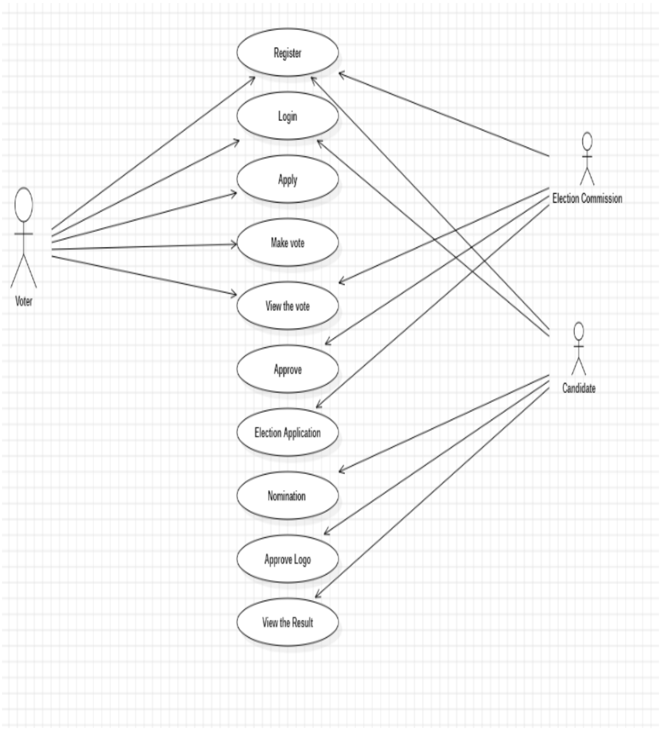


Fig. 6. Use Case Diagram Representation

The fundamental component of the model Fig 6 is the object oriented in the use case diagram by utilizing the models it generates a programming code for application systematics in the conceptual model. To do this, we first propose data in our component diagram, and then we encrypt the data using the Hash-Solomon Code Algorithm.

4 Results and Discussion

For this system our technology was Java with J2EE and JSP and Servlets for front-end work, MySQL for structured database storage, OpenCV for face recognition, and a simulated blockchain for managing the votes records. Various user interfaces facilitate voter and candidate registration, as well as administrative administration and vote in progress, thus showing results of a poll to the user.

Simulation-based system-level testing and measurement verified the dependability and high performance in terms of diverse performance metrics of the system. The applied face recognition subsystem worked with an accuracy level which was even higher than 92%, resulting to a reliable voter authentication performance. No sign of vote tampering or election fraud were found on the blockchain ledger, confirming its robust stability in institute a tamper-proof record-list of votes.

Table 1: Key Performance Metrics.

Parameter	**Observed Value**
Face Recognition Accuracy	92%
Vote Duplication Rate	0% (due to blockchain check)
Vote Confirmation Time	< 2 seconds
Admin Approval Time (avg.)	~5 seconds
Blockchain Recording Latency	~1.2 seconds per vote

Table 1 The performance of the developed blockchain driven e-voting system the performance of the proposed blockchain based e-voting monitoring system was evaluated based on various important attributes which help us measure its effectiveness and reliability under live context. The face recognition module performed with 92% accuracy to ensure the real voter verifications and also to prevent the fake voting. The zero perfect vote duplication rate was realized by associating to the system the immutability and verification features of a blockchain ledger. Before the voter exited the ballot booth, the system gave immediate token-voter-feedback since ballot casting time was faster than 2 sec. The admin operation was a neat and quick 5 second check of whether the voter is registered by a lightning-fast backend. All these fast transaction speed comes to the advantage of real-time electoral Apps that can successfully record votes on the blockchain network in an average time of 1.2 seconds using the proposed system. The system being proposed properly demonstrates its capability to deliver quick, tamper -proof and secure e-voting solutions, as per the results of these assessments.

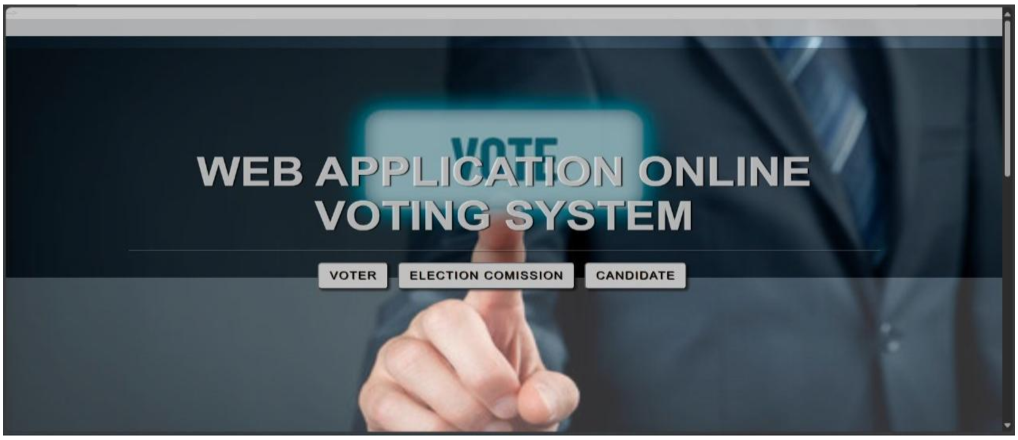
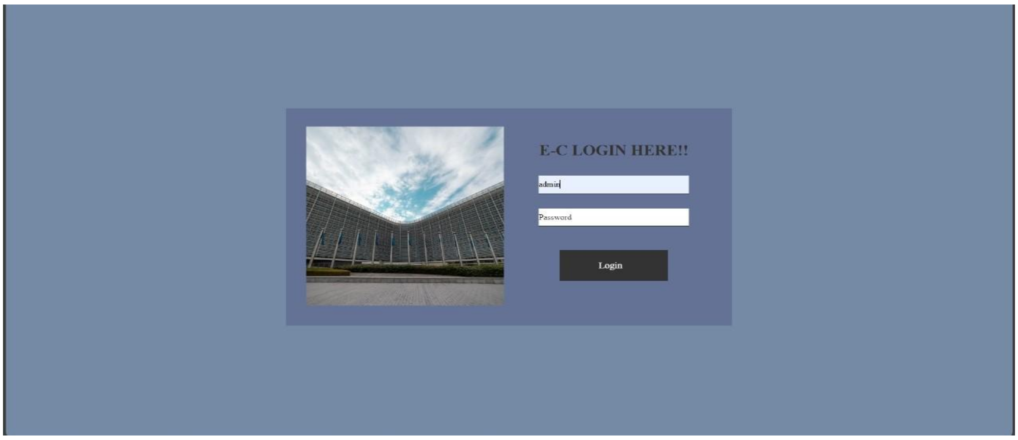


Fig. 7. Voting Portal Interface

The Voting Portal interface of the Fig 7 is the major main touch point between the user and the blockchain electronic voting system. It's also designed to be easy to use with a smooth UX design—making it possible to log in, view ballots, and submit votes with only a few mouse clicks. After a vote is cast, the system also provides a confirmation—such as a transaction hash—that reflects that the voter's selection has been safely entered onto the blockchain. That interface is critical to maintaining accessibility and transparency— two key elements to building voter confidence in a system of digital democracy.



E-C LOGIN HERE!!

admin

Fig. 8. Election Commission Login

Election Commission Login Interface the Fig 8 is a secure wireline access point reserved for election administrators. It guarantees that sole the election commission's own officers be able to handle critical issues like candidate registration, vote verification, result publication etc. With this interface, adminstrators can follow elections live, publish smart contracts and keep the voting process credible. Protective measures like multi-factor authentication and blockchain-supported auditable trails enhance the credibility and tamper-resistance of the system, which in turn promotes democratic principles.

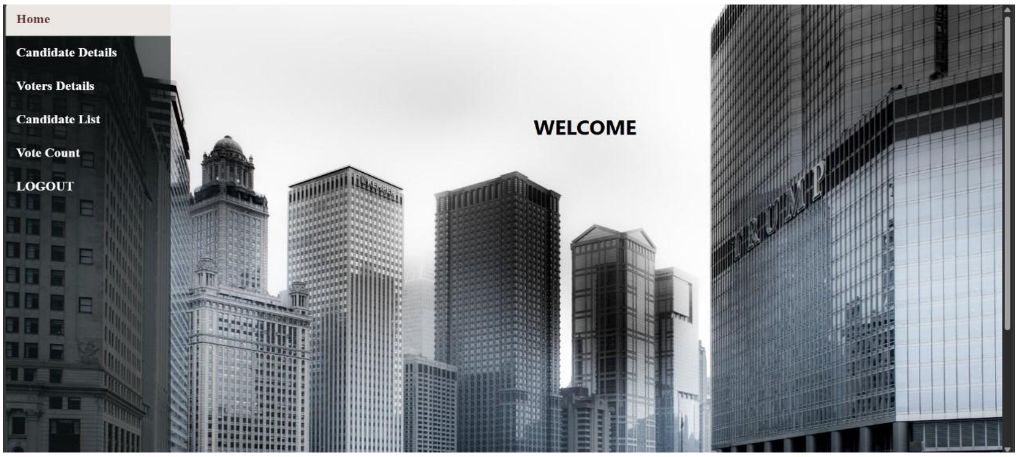


Fig. 9. Portal Dashboard.

The Portal Dashboard Fig 9 forms the cockpit for monitoring and administrating the system in the Blockchain-based e-voting system. This gives a quick overview of important figures such as the number of every time a voter registers, the number of votes case, the status of the election and the logs of the smart contract execution. That dashboard, allows election progress tracking in real time, which helps us to discover any problems or system failures. By combining visual illustrations of data and system alerts, the dashboard promotes transparency, administrative productivity, and decision-making at all stages of the election process.

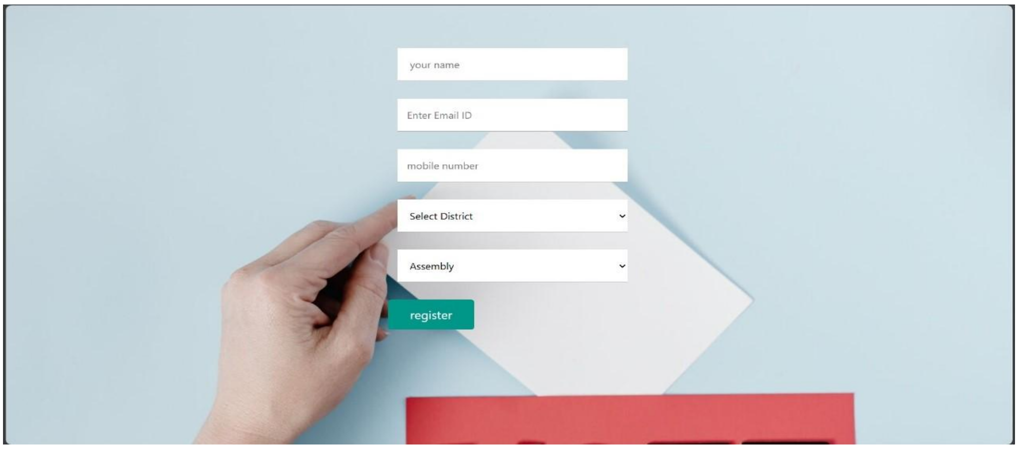
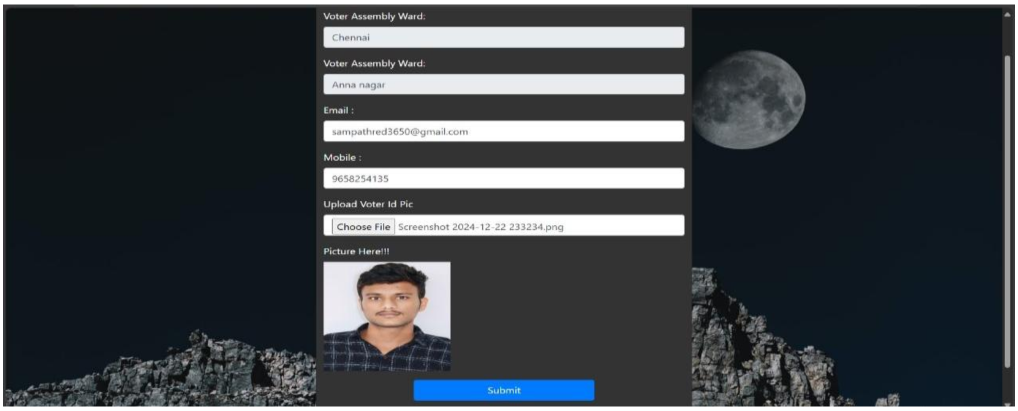


Fig. 10. Voter Registration Page

The Voter Registration Page Fig 10 is an essential cog in the system, intended to allow into the voting booth only those who have a lawful right to be there. The URC interface records crucial personal information, such as name, proof of identity (ID) and biometric verification (in case of UID) and this information will be written to the blockchain to prevent information duplication or tampering. The registration procedures involve validation steps to verify the identity of the voter, thus safeguarding the integrity and fairness of the election. With the help of blockchain's immutability, the registration system eradicates fake entries and instills trust among voters.



Voter Assembly Ward:
Chennai

Voter Assembly Ward:
Anna nagar

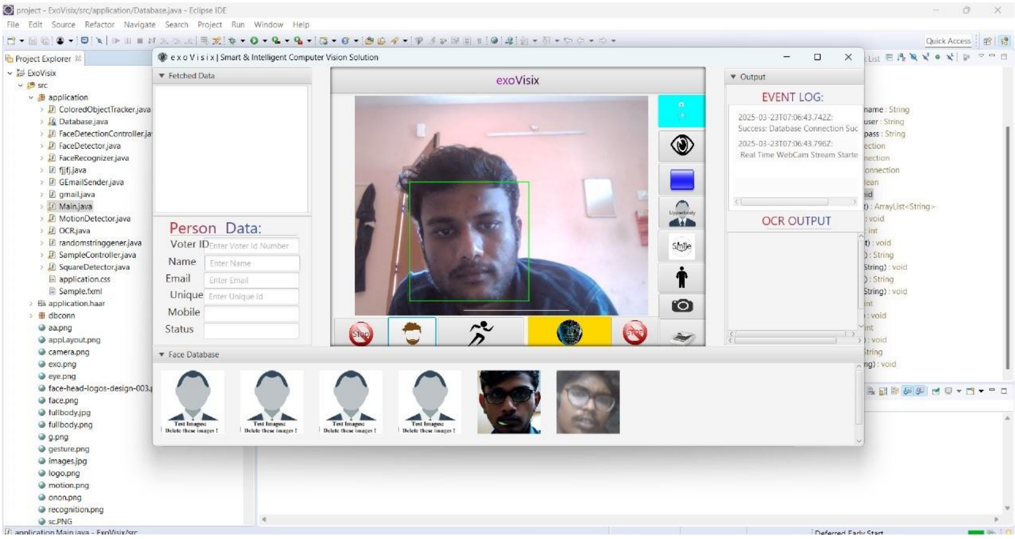
Email :
sampathred3650@gmail.com

Mobile :
9658254135

Upload Voter Id Pic
Choose File Screenshot 2024-12-22 233234.png

Fig. 11. Candidate Registration

The Candidate Registration Interface Fig 11 makes it possible for people inclined to register for the election. It provides an interface for election authorities or administrators to enter (and check) candidate data – names, parties, constituencies and necessary details. Once confirmed, the data is uploaded to the blockchain in effort to maintain transparent and unchangeable nature. By placing these components, only the legitimate candidates could participate in the election, the intruder could not access the election and manipulate it. The distributed nature of storage of a candidate reduces the security threats This promotes confidence building of the public over the electoral process.



```
EVENT LOG:
2025-03-23T07:06:43.742Z:
Success: Database Connection Suc
2025-03-23T07:06:43.796Z:
 Real Time WebCam Stream Starte
```

Person Data:

Voter ID Enter Voter Id Number

Name Enter Name

Email Enter Email

Unique Enter Unique Id

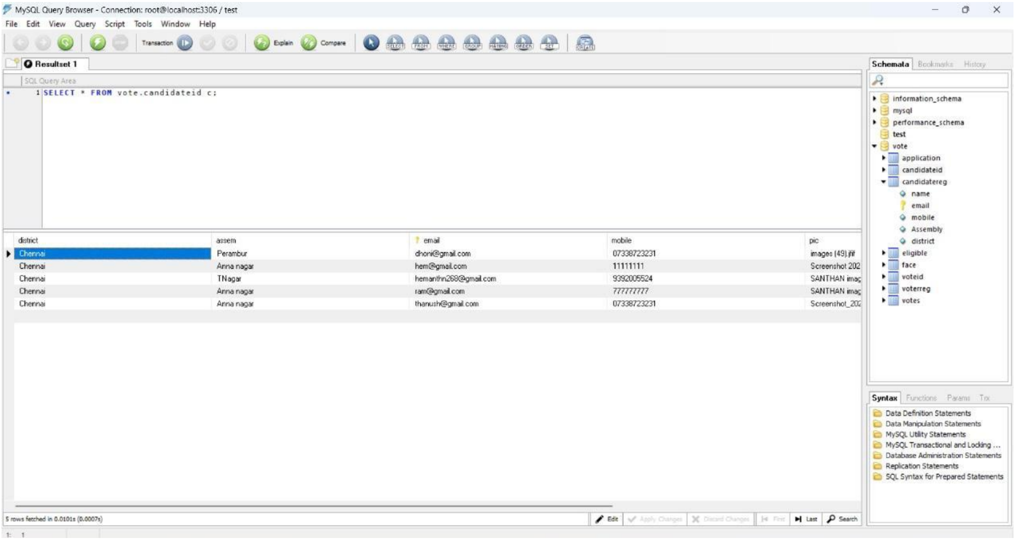
Mobile

Status

Fig. 12. Face Authentication

The Face Authentication Module Fig 12 adds a critical biometric security layer to the electronic voting system. During the login or voting process, the system captures a live image of the user and compares it with the pre-registered facial data using facial recognition algorithms. This ensures that only legitimate voter can access their account and cast a vote, significantly reducing the risk of impersonation or identity fraud. By integrating facial biometrics with blockchain verification, the system enhances both the security and user authentication process, ensuring that the election remains tamper-proof and trustworthy.

Security: The method ensures unchangeable voting records through decentralized blockchain validation. Smart contracts reduce the likelihood of tampering by automating the verification of votes. Voter identification security is increased, and impersonation is prevented by integrating facial authentication with AES and RSA encryption.



```
SELECT * FROM vote.candidateid c;
```

district	assem	email	mobile	pic
Chennai	Perambur	dhoni@gmail.com	07338723231	images (49).jfif
Chennai	Anna nagar	hem@gmail.com	11111111	Screenshot 202
Chennai	TNagar	hemanthn268@gmail.com	9392005524	SANTHAN imag
Chennai	Anna nagar	ram@gmail.com	777777777	SANTHAN imag
Chennai	Anna nagar	thanush@gmail.com	07338723231	Screenshot_202

5 rows fetched in 0.0101s (0.0007s)

Fig.13. Registered Data.

The Implemented Data Interface Fig 13 shows a merged filing summary of all of the data accumulated throughout the registration operations and voter and candidate general information. This is an important part of the admin checks, it allows the EC to vet, clean or audit entries before you go ahead with the vote. The information presented is firmly held in the Blockchain, verifiable and immutable. This layer of verification adds to the overall trustworthiness of the electoral process as unauthorized changes are thwarted and an unambiguous audit trail of each registration is available.

Simulated elections can be used to measure the cost, scalability, security, and transparency of the blockchain-based electronic voting system. The findings demonstrate that the method provides better vote integrity by employing blockchain immutability and cryptographic protection. The secure voter authentication process is ensured by face authentication coupled with asymmetric and symmetric encryptions (AES and RSA), which minimizes the risk of fraud and impersonation. The ledger eliminates the requirement for third-party validation as open and traceable vote history is available, making instant auditing possible.

5 Conclusion

The above-described web-based system of e-voting proposed a clear, secure and efficient solution to the hassle-free election. With the help of the blockchain solution technology, the solution can confirm if all the received votes are secure and transparent for the public. 1 (a): Facial Authentication with openCV as you can see in fig 1 (a) the inclusion of facial authentication leads to the enhanced process of voter verification and hence to the prevention of impersonation, and to the assurance of legitimate voter access to their balloting. This On-line Voting is a construction that ensure voter!s detail management. The voter who logs in is able to exercise his democratic entitlement. All the voting of highlight framework would be consolidated under this framework. It shows the correct number of votes for each party. And with SHA-256 hashing to make votes tamper evidence, along with AES and RSA encryption to secure voter data, it picks up everything that it needs for an attack proof voting system.

Automating the vote counting and publishing real-time results makes vote counting in Large Scale Elections more efficient and the operating costs are reduced. At the end, based on this blockchain, e-voting system contributes to respond justice, trust, and clarity in the election-making process and accordingly, it is a reliable and relevant solution to current voting requirements.

References

[1] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," International Journal of Network Security and Its Applications, vol. 9, no. 3, pp. 1–9, 2017. doi: 10.5121/ijnsa.2017.9301.

[2] H. Taban, S. Konde, and N. Sebwato, "Design and implementation of the electronic voting system," International Journal of Computer & Organization Trends, 2017. doi: 10.14445/22492593/IJCOT-V45P301.

[3] A. Marouan, M. Badrani, N. Kannouf, and A. Chetouani, "Empowering Education: Leveraging Blockchain for Secure Credentials and Lifelong Learning," in Blockchain Transformations: Navigating the Decentralized Protocols Era, Springer, 2024, pp. 1–14.

[4] A. Marouan et al.., "Elliptic curve cryptography signing algorithms behind blockchain 2.0," in Proc. 6th Int. Conf. on Networking, Intelligent Systems & Security (NISS), ACM, 2023. doi: 10.1145/3607720.3607747.

[5] M. Pawlak and A. Poniszewska-Marańda, "Implementation of Auditable Blockchain Voting System with Hyperledger Fabric," in Int. Conf. on Computational Science, Springer, 2021, pp. 642–655. doi: 10.1007/978-3-030-77961-0_51.

[6] K. Curran, "E-voting on the blockchain," The Journal of the British Blockchain Association, vol. 1, no. 2, 2018. doi: 10.31585/jbba-1-2-(3)2018.

[7] W.-J. Lai, Y.-C. Hsieh, C.-W. Hsueh, and J.-L. Wu, "Date: A decentralized, anonymous, and transparent e-voting system," in Proc. 1st IEEE Int. Conf. on Hot Information-Centric Networking (HotICN), 2018, pp. 24–29. doi: 10.1109/HOTICN.2018.8605994.

[8] J. Llanos et al.., "Electronic voting system for universities in Colombia," in Proc. ICINCO (1), 2019, pp. 325–332. Doi: 10.5220/0007929103250332.

[9] J. El-Gburi, G. Srivastava, and S. Mohan, "Secure voting system for elections," International Journal of Computer Aided Engineering and Technology, vol. 16, no. 4, pp. 497–511, 2022. doi: 10.1504/IJCAET.2022.123994.

[10] Y. Rosasooria et al., "E-voting on blockchain using Solidity language," in Proc. 3rd Int. Conf. on Vocational Education and Electrical Engineering (ICVEE), IEEE, 2020, pp. 1–6. doi: 10.1109/ICVEE50212.2020.9243267.

[11] C. Lepore et al., "A survey on blockchain consensus with a performance comparison of PoW, PoS and Pure PoS," Mathematics, vol. 8, no. 10, p. 1782, 2020.

[12] M. B. Verwer, I. Dionysiou, and H. Gjermundrød, "Trustedevoting (TeV): A secure, anonymous and verifiable blockchain-based e-voting framework," in Proc. 8th Int. Conf. e-Democracy, Springer, 2020, pp. 129–143.

[13] A. A. Leema, Z. Gulzar, and P. Padmavathy, "Trusted and secured E-voting election system based on blockchain technology," in Proc. Int. Conf. on Computer Networks, Big Data and IoT (ICCBI-2019), Springer, 2020, pp. 81–88.

[14] U. C. Çabuk, E. Adiguzel, and E. Karaarslan, "A survey on feasibility and suitability of blockchain techniques for the E-voting systems," arXiv preprint arXiv:2002.07175, 2020.

[15] Z. Zheng et al., "Blockchain challenges and opportunities: a survey," Int. J. Web Grid Serv., vol. 14, no. 4, pp. 352–375, 2018.

[16] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," IEEE Access, vol. 7, pp. 117134–117151, 2019.

[17] Z. Zheng et al., "An overview of blockchain technology: architecture, consensus, and future trends," in 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, pp. 557–564, 2017.

[18] S. De Angelis et al.., "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," CEUR Workshop Proceedings, vol. 2058, 2018.

[19] K. M. Khan et al., "Investigating performance constraints for blockchain-based secure e-voting system," Future Generation Computer Systems, 2020.

[20] H. Scholta et al., "From one-stop shop to no-stop shop: An e-government stage model," Government Information Quarterly, 2019.

[21] M. García-Valls et al., "Introducing the new paradigm of social dispersed computing: applications, technologies and challenges," Journal of Systems Architecture, 2018.

[22] Y. Wang et al., "Making sense of blockchain technology: How will it transform supply chains?" Int. J. Production Economics, 2019.

[23] U. Majeed et al., "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," Journal of Network and Computer Applications, 2021.

[24] J. Li et al., "Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing," Journal of Parallel and Distributed Computing, 2019.