International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 12 December 2025
Page No: 4339-4347
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0635

# Blockchain Based Secure Voting System

*Shwetha K R*[1], *Divya G S*[2], *Bhavan Pande*[3], *Darshan K*[4], *Gagan M S*[5], *Chiranthan B M*[6]
[1,2,3,4,5,6]*Department of CSE, AMC Engineering college, Bengaluru, India.*
**Emails:** *kr.shwetha12@gmail.com*[1], *divyags.siddaraj@gmail.com*[2], *bhavanpande18@gmail.com*[3], *darshandarsh1519@gmail.com*[4], *gagangagan55004@gmail.com*[5], *cchiranthan918@gmail.com*[6]

## Abstract

*Due to the ever-increasing demand to use safe and reliable electronic votes, a blockchain-based secure voting system has been developed to enhance transparency, trustfulness, and voter recognition. This system eliminates such issues as voting fraud, impersonation, and manipulating the results by means of biometric verification and decentralized blockchain ledger. The voters are matched to a facial-recognition database containing previously registered voters before voting. It is authenticated by a K-Nearest Neighbors (KNN) approach as it works well on classifying facial features and is not very laborious. After the vote is successfully authenticated, it is stored and signed on a blockchain network where it cannot be altered by another party. The features of smart contracts ensure the safety of voting, the correct counting of votes, and the awareness of each network node of what is happening. The cryptography of hashing and decentralized make certain that the votes are immutable, due to the decentralized structure of blockchain and consensus mechanisms. The face-matching module ensures that only the qualified individuals are allowed to vote. The system also supports mass elections and guarantees the ease of interaction among the voters. It was designed in such a way that it is scalable and user friendly. Trust, security, and efficiency are enhanced in the system through biometrical authentication, distributed ledger technology, encryption, and classification through machine-learning. It is highly dependable in how to conduct the current digital elections.*

**Keywords:** *Blockchain, Secure Voting System, Facial Recognition, K-Nearest Neighbors (KNN), Biometric Authentication, Decentralized Ledger, Cryptographic Hashing, Smart Contracts.*

## 1. Introduction

The idea of electronic voting has received much attention throughout the world because societies that adhere to democratic principles continue to shift into more modernized and technology-driven elections. Digital voting platforms, as opposed to traditional paper-based methods, have the benefits of quicker tallying, lower administration cost, and ease of accessibility. A number of states, such as Estonia, Switzerland, and Canada, have already managed to implement voting systems through the Internet during major referendums, and this proves that the digital involvement of many people is feasible. Simultaneously, blockchain technology has become a revolutionary application in different spheres of life, and it provides decentralized, immutable, and transparent data management. These distinctive features render it a compelling superstructure to protect electoral integrity and build a stronger sense of trust in digital voting system among the populace, which will also be backed up by preliminary conceptual discourses and real-world applications in distributed ledger ecosystems [1], [2]. The more recent efforts further point to the appropriateness of blockchain to safe ballot scanning and credible election administration in massive settings [3]. Also, biometric authentication, in particular face-recognition-based voter authentication has become one of the promising tools that improve access management and guarantee a legitimate partaking in the digital electoral procedure [4]. In spite of the melting ice of technological progress, there are still problems in having a complete, open, and verifiable election conditions. The conventional e-voting systems are susceptible to cyberattacks, manipulation of central servers, identity fraud, and unauthorized ballot manipulation, making them to lack confidence in the outcomes of elections. Several reports have indicated how challenging it is to maintain voter confidentiality and be able to access system transparency and at the same time be resilient to attempts of tampering and insider threats [5]. Similarly, even current frameworks that combine biometrics with e-voting are yet to overcome reliability, anonymity, and secure auditability challenges, as they restrict their use in practical implementations at the national level. Moreover, the lack of an efficient, integrated system, which would safeguard voter identity, multiple-voting at the same time, and provide unchangeable voter-vote storage, implies a serious flaw in modern digital electoral processes [6]. These weaknesses show that there is a need to have better architectures that can integrate robust authentication and tamper-resistant vote capture. To address the mentioned constraints, the present work proposes a secure voting mechanism based on blockchains and biometric authentication to provide a clear-cut participation and reliable election results. The system is set in such a way that it helps to enhance voter authenticity, ballot confidentiality, and unchangeable vote records using decentralized ledger solutions. In this strategy, focus is on preservation of privacy, integrity and valid reliable processes of validation without depending on any central authority. With the help of the principles of modern cryptography and decentralization through consensus, the framework helps to eliminate the systemic weaknesses of traditional e-voting systems and promotes the effective management of elections and related issues in diverse operational environments [7]. Also, the architecture is designed in such a way that it is flexible, scalable, and more resilient to manipulation attempts, which is consistent with all tendencies of the world to secure digital forms of governance [8]. The value of this work is that it can make electronic methods of voting far more reliable and popular. The proposed approach will help to enhance democratic institutions and enhance voter confidence by incorporating decentralized trust, transparent auditability, and secure identity verification. Its focus on privacy, integrity, and resilience makes it a solution of the future that would be a good fit in a recent electoral setting in search of greater transparency and longer-term safety.

## 2. Literature Review

The literature shows that significant efforts have been made so far in improving the security, transparency, and trustworthiness of a digital voting environment and also the biometric authentication mechanisms. Several forms of biometric authentication have been researched to enhance the level of security in terms of accessing the system, and face recognition has proven to be the most dependable type of biometric authentication. Liu et al. introduce the advances in the face-recognition algorithms in details and focus on the superiority to changes in lighting, pose, and occlusion, which supports their applicability to the secure verification of identity in the most sensitive cases [9]. In addition to this, alternative distributed storage systems, including the InterPlanetary File System (IPFS), have been suggested to distribute and secure big data digital information, providing a peer-to-peer architecture to make it resistant to centralized points of failure and ensure its immutability and efficient access [10]. These pillars all emphasize the value of integrating strong biometric authentication with decentralized data structures in order to have reliable digital ecosystems. The technology of secure voting based on blockchains has also been highly traced in the past. An example of how smart contracts can be used to automate the process of validating votes made Parmar and Dewangan present an Ethereum-based voting system aimed at improving transparency and auditability of the voting process and minimizing the reliance on third parties [11]. Other prior work within the wider discipline of biometrics had also highlighted the need to have robust identity-verification mechanisms. Jain et al. have described the biometric modalities in a very detailed description pointing out the inherent strengths of the modalities in ensuring proper voter authentication as well as including the possible weaknesses to spoofing and the environmental conditions [12]. Simultaneously, Chaum et al. created Scantegrity, an end-to-end voter-verifiable optical-scan system that made ballot verification stronger and did not violate voter privacy. Nonetheless, its dependence on the physical infrastructures, as well as its lack of scalability highlighted the difficulty with modifying such systems to fully digital election settings [13]. Other works are devoted to blockchain architecture and decentralized system performance considerations. Cachin analyzed Hyperledger Fabric, which offered a permissioned and modular framework of blockchain that is most appropriate with applications that demand participation on the network and great throughput [14]. Although this architecture enhances security and scalability, its complexity to deploy as well as limitations to identity-management inhibit scaling to wider public election systems. Moreover, Gupta et al. discussed the use of machine-learning algorithms to check the authenticity of the users via biometry through e-voting, providing information about the classifiers that could appropriately identify the legitimate users with high precision [15]. Despite its efficiency, most of these methods were based on a central data repository or did not provide any mechanism to guarantee the impossibility of any alterations when the votes had been cast. Although much has been made, there are still various gaps in the process of incorporating the decentralized blockchain technologies with trusted biometric authentication to provide end-to-end secure voting. Earlier efforts either concentrated on vote recording based on blockchains, and thus were solely concerned with immutability issues, or were based on biometric authentication without decentralized vote storage. Issues of voter anonymity and discouraging duplicate voting as well as safeguarding voter identities against correlation attacks are also a challenge. Furthermore, available systems have been characterized by a shortage of scalability, transparency, or adaptable implementation in a wide range of election settings.

The present work fills these gaps by integrating the decentralized ledger technology with secure biometric verification to create a fully functioning voting system to improve the transparency, immutable storing of votes and valid identity verification. With the incorporation of the decentralized trusts mechanisms, and the sophisticated authentication plans, the system is expected to address the current weaknesses and provide a secure, privacy-conscious, and reliable digital voting platform to be used in the big scale election processes.

## 3. Materials and Methods

Voter fraud, identity theft and election tampering are some of the threats of the integrity of the voting process in most parts of the world. Manual and electronic traditional voting systems are prone to numerous forms of security attacks such as impersonation, multiple voting, and post-casting vote tampering. Also, these systems may result in distrust among the voters due to lack of transparency and centralization control, which may compromise the democratic processes. In spite of the development of digital voting technologies, the issue of secure, verifiable, and transparent elections is still a serious obstacle. This leaves the effectiveness of an impeccable system to verify voters and Electronic voting systems is not popular yet due to the fact that people desire to safeguard the privacy and integrity of their votes, shown in Figure 1.

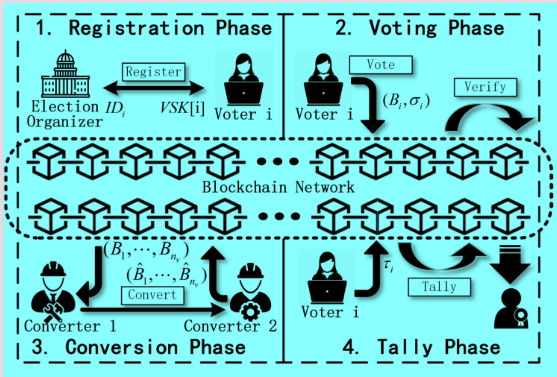


Figure 1 Proposed Architecture

### 3.1. Modules

**Initialization Phase:** The Election Organizer (ED) in the initiation phase will start with the Setup procedure to create the public parameters (PP), which is published on the blockchain and made accessible to everyone in the world. Then EKeyGen is used to create its public key EPK and secret key ESK by EO. Likewise, converters CV1 and CV2 make their own sets of secret and public keys, called (CSK1, CPK1) and (CSK2, CPK2) respectively, using CKeyGen. All the public keys, such as EPK, CPK1, CPK2 are submitted to the blockchain to ensure that nothing is not ambiguous and are also able to exchange safely during the voting process.

**Registration Phase:** At the registration stage, all registered voters Vi present a valid identification like a passport, identity card or drivers license to the EO so that the information can be verified. The EO is also conducting stringent eligibility and authenticity checks to ensure that the voter is within the stipulated requirements. Once the EO successfully performs the verification, it starts the Register protocol that produces a distinctive secret key VSKi of the voter. This secret key is used as a form of identification and gives the voter cryptographic ability to be able to safely draw and send ballots in the next round of voting.

**Voting Phase:** Vi is the confirmed voter who makes his/her ballot Bi with a signature πi and a tag τi and invokes the Vote protocol to submit his/her ballot. The two things ensure that the ballot is authentic and legitimate. After the adequate number of votes is sent, the blockchain network (BN) runs a batch verification with the Verify algorithm. This is done to confirm the authenticity of all the received ballots simultaneously to make sure that only legitimate properly formed ballots are accepted before reaching the conversion stage.

**Conversion Phase:** Conversion phase starts with the blockchain network executing deduplication to remove identical or repeated ballots to stop malicious reposts or an attempt to wrongly claim that the voter has voted more than once. Converters CV1 and CV2 then use converters CV1 and CV2 to convert the verified ballots into format that would be used in secure tallying after deduplication. This phase ensures anonymity to the voter and at the same time verifies that only valid and unique ballots are counted to the end.

**Tally Phase:** Voters Vi place their anonymous tag τi on the blockchain at the tally stage in a manner that facilitates linkage of votes in a secure but not easy manner. Once the ballots are transformed, Tally algorithm is executed to receive the final results of the poll. This stage will provide the transparency of vote counting, checking, and non-contamination, and finally deliver a reliable election result with blockchain integrity and cryptographic security.

### 3.2. Methods/Technologies

**Register:** The registration system allows new voters to generate an authenticated profile in the system. The users enter personal details and identity proof, which is verified to qualify them. After approval, the information of the voter is safely stored and a unique digital identity or credential is created. This will make sure that the voting platform is only opened to legitimate people. Registration also averts duplication of accounts as well as a very safe base on all the further actions involving voting.

**Login:** The account system provides the registered voters with an opportunity to access the platform with the help of the verified credentials. There can be multi-factor authentication or biometric verification that will guarantee that only the authorized person can log in. This measure will keep the system out of unauthorized access, impersonation, or fraudulent action. An effective login gets the voter into the voting dashboard allowing him/her to take part in the election with the integrity of the system and the privacy of the voters.

**Add Candidate:** Authorized administrators or election organizers key in candidate information in the system using the add candidate method. This consists of the name of the candidate, party information and any other identification information. These entries are authenticated and stored in the system in a secure manner that they cannot be changed or deleted without the necessary authorization. This approach will ensure that the list of candidates is correct, immutable, and easily visible to all voters who would be taking part in the election.

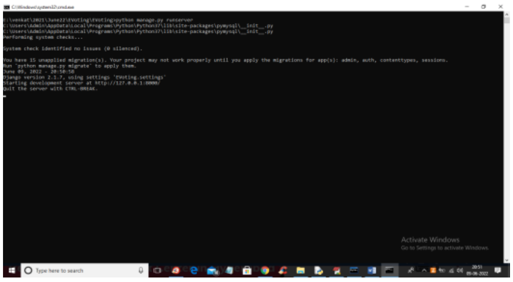
**Cast Vote:** The cast vote method is a voting method where the authenticated voters can choose their candidate of choice amongst those approved. After a vote is cast it is encrypted such that it is private and stored in a secure form. This is a way of getting a vote and not informing the voter of his identity. The system eliminates duplication of votes and lone tallying of the votes, which creates fairness and transparency in the election process.

**Check:** The check method allows the voter or the administrator to check the status of the submitted votes or the operating of the system. This might involve checking to see that a vote has been logged in, checking to see that a voter has been registered or checking to see that the system is working. The system improves transparency, as there is real time verification and confidentiality of data. It serves as a protection to make sure that the process of election is reliable and right at all levels.

**Store in Blockchain:** The store in blockchain approach stores every verified vote on a distributed registry, which is unalterable and impeccable. The data is not able to be deleted or modified once it is stored and thus the integrity of the election results is saved. This is because blockchain is distributed hence there is transparency and security, where no single entity can control the outcome. Such an approach will ensure that all the voting records are long-term reliable, authentic, and traceable.

**View Results:** The view results method enables the authorized users or voters to get the final tally of the votes after the election is over. The outcome of blockchain verified records is obtained, making the whole process of verification and results accurate and transparent. The system brings all the votes of each candidate and displays them without interfering with the anonymity of the voter. This process develops confidence owing to the availability of verifiable and tamperproof election results which represent the actual electoral choice.

## 4. Experimental Results



```
E:\venkat\2021\June22\EVoting\EVoting>python manage.py runserver
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
Performing system checks...

System check identified no issues (0 silenced).

You have 15 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin, auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
June 09, 2022 - 20:50:58
Django version 2.1.7, using settings 'EVoting.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

Figure 2 Diagram

As indicated in the above screen, the server is active. Light up a browser and enter the following address in the browser: http://127.0.0.1:8000/index.html. Hit enter key to view the results as follows.

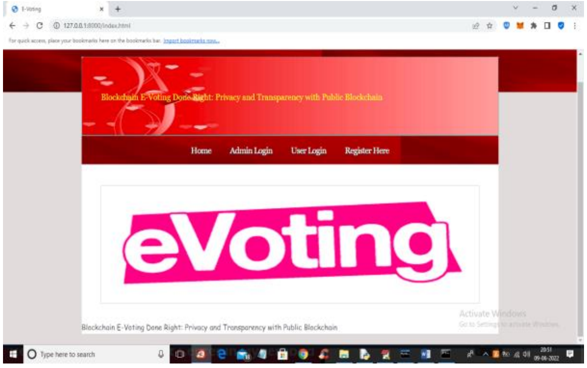
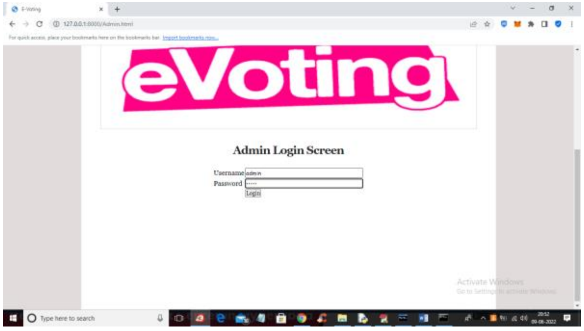

Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain
Home
Admin Login
User Login
Register Here
eVoting
Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain

Figure 3 Admin Login

Above, click "Admin Login" to log in as admin. Below, see the screen that comes up.

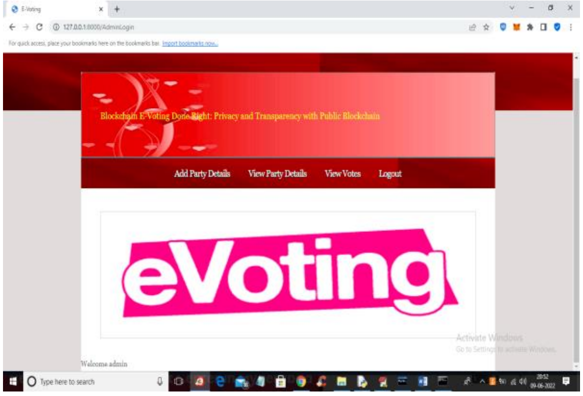


Admin Login Screen

Username admin
Password
Login

Figure 4 Admin Login

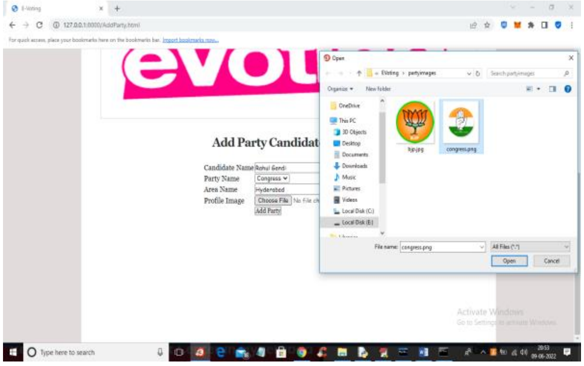
This is the screen where the manager logs in. Once they're in, they'll see this screen below.


Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain
Add Party Details
View Party Details
View Votes
Logout
eVoting

Welcome admin

Figure 5 Add Party Details

To add new party information, click "Add Party Details" on the screen above.



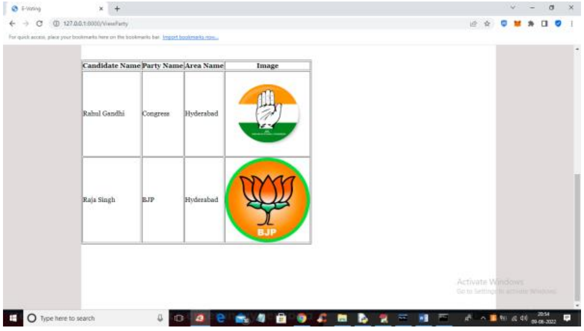
Add Party Candidate

Candidate Name Rahul Gandi
Party Name Congress
Area Name Hyderabad
Profile Image Choose File No file ch
Add Party
File name: congress.png

Figure 6 View Party Details

On the screen above, you can add candidate information and a party picture. To add a new party, click the "Add Party" button. To see a list of all the parties, click "View Party Details."

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 12 December 2025
Page No: 4339-4347
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0635

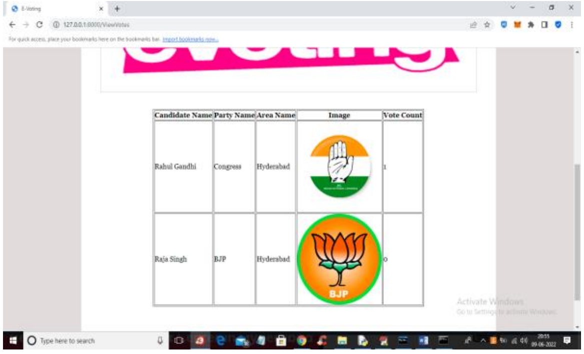


127.0.0.1:8000/ViewParty

| Candidate Name | Party Name | Area Name | Image |
|---|---|---|---|
| Rahul Gandhi | Congress | Hyderabad | |
| Raja Singh | BJP | Hyderabad | BJP |

**Figure 7** **View Votes**

All the information about each party is shown above. If we click on the "View Votes" link, we'll see what's shown below.

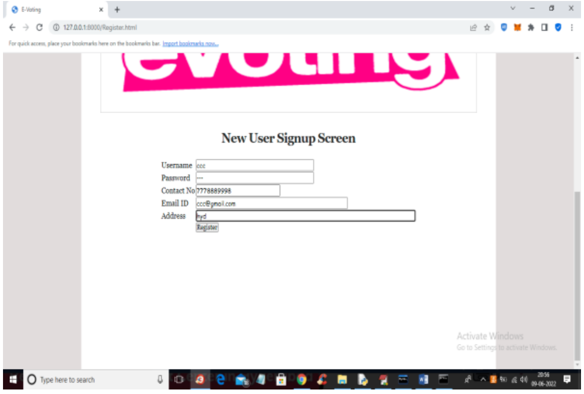


127.0.0.1:8000/ViewVotes

| Candidate Name | Party Name | Area Name | Image | Vote Count |
|---|---|---|---|---|
| Rahul Gandhi | Congress | Hyderabad | | 1 |
| Raja Singh | BJP | Hyderabad | BJP | 0 |

**Figure 8** **Vote Count**

The vote count is shown on the screen above. Now, log out and sign up a new user, as shown on the screen below.



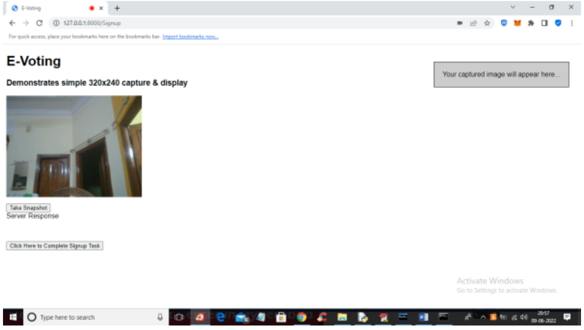
127.0.0.1:8000/Register.html

New User Signup Screen

Username: ccc
Password: ···
Contact No: 7778889998
Email ID: ccc@gmail.com
Address: hyd
Register

**Figure 9** **Register**

On the screen above, enter information about a new user. Then, press the "Register" button to see the screen below, where you can take a picture of the user.



127.0.0.1:8000/Signup

E-Voting

Demonstrates simple 320x240 capture & display

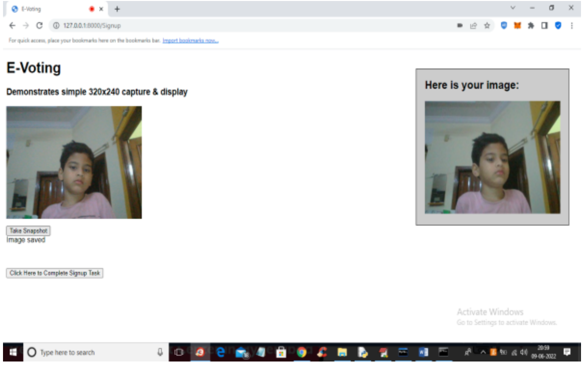
Your captured image will appear here...

Take Snapshot
Server Response

Click Here to Complete Signup Task

**Figure 10** **Take Snapshot**

Click the "Take Snapshot" button on the screen above to take a picture, and you'll see what comes up next.



127.0.0.1:8000/Signup

E-Voting

Demonstrates simple 320x240 capture & display

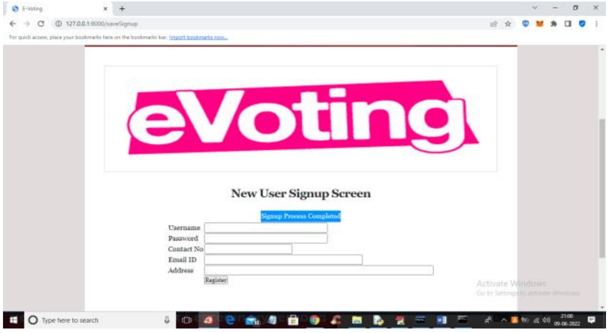
Here is your image:

Take Snapshot
Image saved

Click Here to Complete Signup Task

**Figure 11** **Complete Signup Task**

The user's picture is shown above. Click the "Click Here to Complete Signup Task" button to save the picture in the database, and you'll see what comes up next.



127.0.0.1:8000/saveSignup

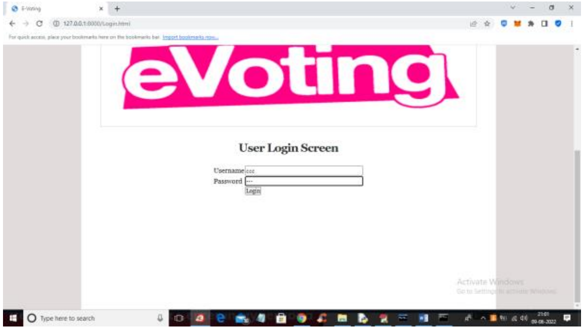
New User Signup Screen

Signup Process Completed

Username:
Password:
Contact No:
Email ID:
Address:
Register

**Figure 12** **User Login**

The above screen shows that the signup process with the user picture is complete. All user images can be found in the "static/profiles" folder. Click on the "User Login" link to go to the screen below where you log in.

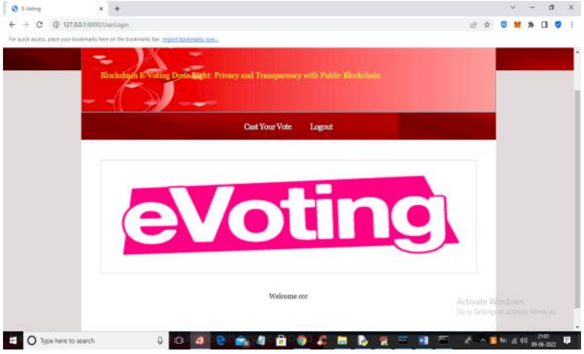


User Login Screen

Username ccc
Password ···
Login

Figure 13 Results

This is the user's screen after they log in and press the button to see the results below.



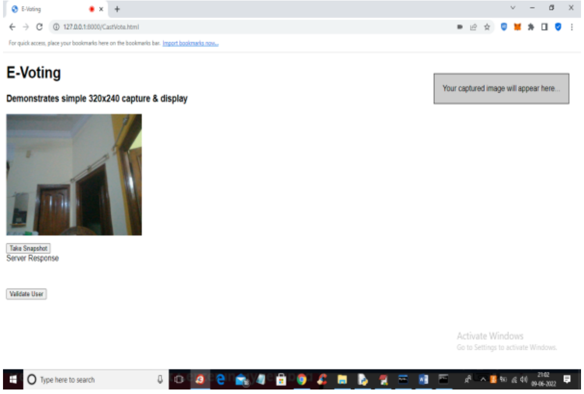
Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain

Cast Your Vote  Logout

Welcome ccc

Figure 14 Cast Your Vote

Click on the "Cast Your Vote" link in the top screen to go to the next screen.



E-Voting

Demonstrates simple 320x240 capture & display

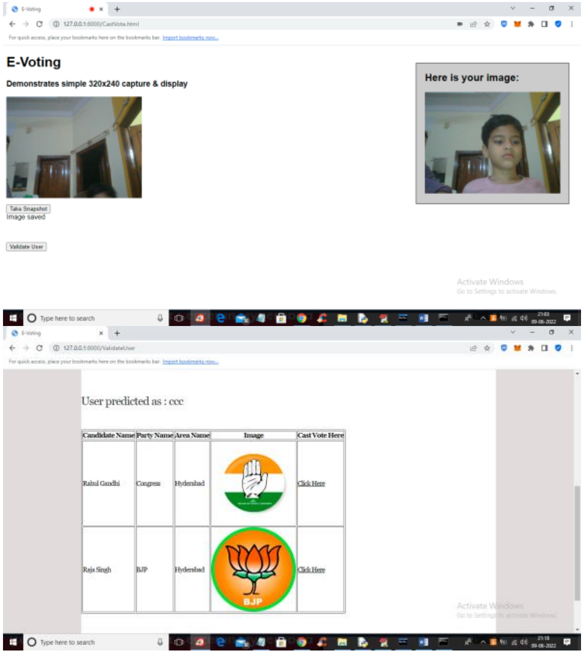
Your captured image will appear here...

Take Snapshot
Server Response

Validate User

Figure 15 Validate User

If you want to vote, click on "Take Snapshot" and then "Validate User" on the screen above. This will give you the result below. "User predicted as ccc" is shown above. If the user clicks on the "Click Here" link, he can see all the party lists and cast his vote, as shown below.



E-Voting

Demonstrates simple 320x240 capture & display

Here is your image:

Take Snapshot
Image saved

Validate User

User predicted as : ccc

| Candidate Name | Party Name | Area Name | Image | Cast Vote Here |
|---|---|---|---|---|
| Rahul Gandhi | Congress | Hyderabad | | Click Here |
| Raja Singh | BJP | Hyderabad | BJP | Click Here |

Figure 16 Vote

The vote is accepted on the screen above, and if the same person tries again, they will see the error message below. "Vote has already been cast by this user" is written in blue on the screen above. You can also sign up and cast your vote in the same way, shown in Figure 2 to 16.

## Conclusion

In the end, the face-based authentication blockchain-based secure voting method shows a highly reliable and technologically advanced framework for ensuring transparent and tamper-resistant elections. Using a pre-processed facial-recognition dataset, the system employs feature extraction and classification through the K-Nearest Neighbors (KNN) algorithm, achieving accurate and consistent voter identification while preventing impersonation and duplicate voting. The use of decentralized blockchain structure, cryptographic hashing, and immutable distributed ledger systems is guaranteed to securely store the votes and ensure real-time verification and prevent illegal alterations. Operations driven by smart contracts also automate the validation process and provide more trust among all the involved nodes. Experimental findings support high authentication rates, smooth recording of votes, low verification time, and high-performance scale, indicating the relevancy of the system in conducting elections on the national level or an organization. This solution effectively overcomes the drawbacks of conventional e-voting, and therefore, through the use of biometric authentication, machine-learning-driven classification, blockchain consensus, and encrypted data processing, it can be stated that they have solved most of the restrictions of this technology. By and large, the system is able to create a resilient and scaled up voting platform that is able to reinforce the democratic processes, enhance voter trust, and put a solid base on future developments in secure digital election systems. The future of this system is to add multi-modal biometrics like fingerprint and iris recognition to enhance authentication that is not based on face information. The use of deep learning models can also increase the accuracy and processing power. To enhance accessibility among remote users and the disabled, it would be better to expand the platform into a secure mobile voting application. Also, the possibility of interoperability between various blockchain models can greatly expand scalability, and the system can be used in large national and international elections without compromising the quality of security and transparency.

## References

[1]. M. Swan, Blockchain: Blueprint for a New Economy, 1st ed. Sebastopol, CA: O'Reilly Media, 2015.

[2]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: Dec. 8, 2024].

[3]. K. Zhang, J. Li, K. Zhang, and W. Yang, "A Blockchain-Based Secure Voting System," in Proceedings of the IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, 2019, pp. 541-545.

[4]. B. Moreno, A. Pernías, and F. Garcia-Sanchez, "Face Recognition in Voting Systems," in Proceedings of the IEEE International Conference on Computational Intelligence and Security, 2020, pp. 48-54.

[5]. S. Nojoumian, A. Stinson, and T. Topaloglu, "Secure and Privacy-Aware Voting Using Blockchain Technology," IEEE Access, vol. 7, pp. 40794–40806, Apr. 2019.

[6]. K. C. Nguyen, A. K. Singh, and R. Kumar, "Blockchain-Based E-Voting System with Biometric Security," in Proceedings of the IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 2021, pp. 123–130.

[7]. P. Mittal and J. Singh, "Enhancing Voting Transparency Using Blockchain Technology," in Proceedings of the IEEE International Conference on Big Data (BigData), 2021, pp. 978–985.

[8]. T. Nguyen and J. Kim, "Reliable Blockchain Architecture for Electronic Voting System," in Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), 2020, pp. 1–5.

[9]. Y. Liu, K. Lu, and W. He, "Face Recognition Algorithms for Biometric Authentication in Secure Systems," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3628–3637, Nov. 2020.

[10]. J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," 2014. [Online]. Available: https://arxiv.org/abs/1407.3561. [Accessed: Dec. 8, 2024].

[11]. P. Parmar and A. K. Dewangan, "Design and Implementation of Blockchain-Based E-Voting System Using Ethereum," in Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, Canada, 2021, pp. 330–335.

[12]. K. Jain, P. Flynn, and A. Ross, "Handbook of Biometrics," New York, NY: Springer, 2007.

[13]. D. Chaum, R. Carback, J. Clark, and B. Essex, "Scantegrity: End-to-End Voter Verifiable Optical-Scan Voting," IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 611–627, Dec. 2009.

[14]. C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," in Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Chicago, IL, 2016, pp. 1-4.

[15]. R. K. Gupta, H. Rajpoot, and A. S.

Raghuvanshi, "Performance Analysis of Machine Learning Techniques for Biometric Authentication in Secure E-Voting," IEEE Access, vol. 8, pp. 120015–120025, Aug. 2020