IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025

DOI: 10.17148/IJARCCE.2025.14317

Online Voting System Using Machine Learning and Blockchain

I Vuha Chandrika[1], E Rithika[2], P Mahesh[3], Y Chaitanya[4], Dr. K. Gnanendra[5]

Student, CSM, VVIT, GUNTUR, INDIA[1]

Student, CSM, VVIT, GUNTUR, INDIA[2]

Student, CSM, VVIT, GUNTUR, INDIA[3]

Student, CSM, VVIT, GUNTUR, INDIA[4]

Assistant Professor, Dept. of. CSE Artificial Intelligence and Machine Learning,

VVIT, GUNTUR, AP, INDIA[5]

Abstract: The Online Voting System using Blockchain with Ethereum and Machine Learning is a decentralized and secure digital voting platform aimed at ensuring transparency and integrity in elections. By utilizing blockchain technology, specifically Ethereum with Ganache, this system guarantees immutable storage of votes, eliminating any possibility of manipulation. To enhance voter authentication, the system incorporates a face recognition module, which verifies a voter's identity before allowing them to cast their vote. The voter registration process is managed by an administrator, who can add multiple voters through bulk data uploads, including images. Election and candidate management are also handled by the administrator, ensuring structured election processes. Once a voter casts their vote, it is permanently recorded on the Ethereum blockchain, preventing any unauthorized alterations. The system enforces a strict one-vote-per-voter rule, ensuring a fair electoral process. The election results are securely displayed after voting concludes, providing an unbiased outcome. Additionally, machine learning algorithms such as Decision Tree, Random Forest, and Logistic Regression are integrated to predict future election trends. These models analyze historical election data based on multiple factors, including candidate demographics, financial assets, liabilities, and voter behavior, providing insightful forecasts. The proposed system employs Python with Django for backend development, while the frontend is built using HTML, CSS, JavaScript, and Bootstrap. By combining blockchain technology for secure voting, face recognition for fraud prevention, and machine learning for predictive analytics, this system enhances trust in digital elections, promoting a fair and transparent democratic process.

Keywords: Face recognition, Blockchain, Django, Web development, Machine Learning

1.INTRODUCTION

Elections establish democratic societies by providing citizens with a clear and upright system to elect their representatives. Current election voting systems battle multiple problems because they suffer from security risks in addition to data tampering issues and both technical and practical operational difficulties. The innovations in technology have Identify applicable funding agency here. If none, delete this. created online voting which stands as an answer for resolving current electoral issues. The digital election process faces considerable challenges in assuring security together with transparency as well as maintain its integrity.

This project develops an Online Voting System which implements Blockchain Ethereum and Machine Learning technologies for establishing a secure decentralized voting framework. The voting system achieves secure vote documentation through blockchain integration which prevents voting manipulation along with vote tampering. The smart contracts for voting control use Ethereum through Ganache to ensure secure blockchain storage of voting data.

The system implements a face recognition module for voter authentication to check and verify voters before they can vote. The combination of biometric authentication names stops potential cases of identity theft together with unpermitted system entries. Bulk details containing facial images which voters must submit get registered through the system by means of election administrator access.

The system includes machine learning algorithms which process historical election data for predicting upcoming voting patterns. The evaluation system depends on Decision Tree and Random Forest and Logistic Regression algorithms to examine voter party membership while analysing demographic characteristics together with financial capabilities and historical voting records. The obtained analysis reveals beneficial forecast data that supports the comprehension of upcoming electoral behaviour.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025
DOI: 10.17148/IJARCCE.2025.14317

The present online voting system implements Python and Django as backend structures alongside a frontend built from HTML, CSS, JavaScript, and Bootstrap programming languages. The proposed system unites blockchain security for voting with face recognition to stop fraud and machine learning for forecasting to establish stronger digital election trust while ensuring democratic fairness and transparency.

2. LITERATURE SURVEY

Researchers have dedicated critical attention to voting system evolution because they aim to establish secure, transparent, and efficient voting procedures. Traditional voting methods based on papers are prone to multiple problems which include tampering of ballots as well as election fraud and operational difficulties. The introduction of digital e-voting systems during technological advancement continues to face security concerns and cyber security threats according to.

Online voting systems acquire enhanced security together with transparency through the emerging blockchain technology. Research findings indicate blockchain implements decentralized operations which make votes unalterable and unattackable because of their lasting immutability. The smart contract features of Ethereum have gained substantial interest in creating voting applications that combine automatic procedure automation with transparent voting functions.

Researchers on different elements of biometric authentication systems to combat voter fraud appear in many academic investigations. Research demonstrates that facial verification proves to work well for voters during the verification process by stopping identity theft alongside multiple vote attempts [3]. The application of machine learning models has resulted in analysis of election patterns and development of predictions about future voting trends. Research into upcoming election predictions utilizes Decision Tree and Random Forest together with Logistic Regression for their analysis of historical data and voter population characteristics.

Research on blockchain-based voting systems proved that decentralized voting solutions strengthen trust among voters because they preserve data authenticity while minimizing electoral violations. Research shows that uniting blockchain capabilities with machine learning functions creates an efficient election management solution that defends against threats yet generates intelligent analytical information.

The implementation of blockchain-based voting faces ongoing obstacles when striving for large-scale adoption. Scalability issues, transaction costs, and the requirement for internet access pose significant limitations, especially in underdeveloped regions. Addressing voter privacy issues and technological reluctance requires additional investigation and policy reforms to be resolved.

The merger of blockchain technology with Ethereum systems and machine learning mechanisms together with biometric authentication systems establishes a revolutionary method to revamp contemporary electoral procedures. Available academic research indicates that these technological solutions offer prospects for an improved secure voting system but more development is needed to solve technical and societal hurdles for widespread implementation.

3.METHODOLOGY

The designed system implements blockchain alongside face recognition along with machine learning techniques to provide secure transparent voting services online. The security reliability along with efficiency of the voting system emerges through multiple sequential phases within the methodology.

A. System Architecture

A decentralized system uses blockchain technology to accomplish secure data storage during elections for protection against tampering efforts. The system involves fundamental components which are:

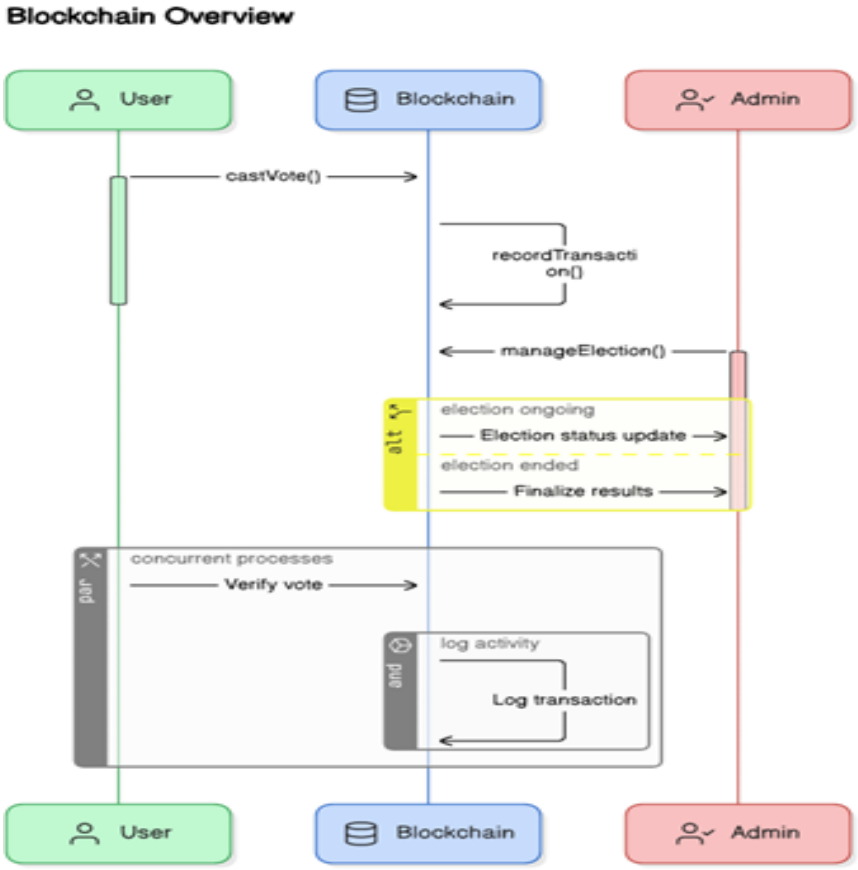
Voter ID along with facial biometric identification offers users the registration process. Before allowing access the system uses Face recognition technology within its Authentication Module. Voters submit vote choices through the system where Ethereum blockchain permanently stores them. The blockchain retrieves votes for computation into results which are then displayed. The prediction model uses machine learning techniques to process historical election data for creating future outcome predictions.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025

DOI: 10.17148/IJARCCE.2025.14317



B. Voter Registration and Authentication

The registration process requires users to provide their personal information together with a voter ID as well as biometric data. The authentication procedures establish that authorized individuals alone can take part in system functions. A deep learning-based Python module operates face recognition technology within the system framework. The system receives input image I then extracts F(I) facial characteristics which it matches against its database of biometric information

$$D = | |F(I) - F(R)| |\ldots\ldots (1)$$

The comparison calculates the Euclidean distance between F(R) reference facial features from registration storage and the extracted features F(I). A voter will be authenticated when the distance metric D falls below the set threshold T.

C. Blockchain-Based Voting Process

The authentication process lets voters input their votes which get recorded as permanent blocks within the Ethereum blockchain. The voting system records votes as transaction records to create an immutable transparent system. The blockchain voting sequence operates according to the following sequence of steps:

Voters who have successfully authenticated can now choose their selected candidate for submission to the electoral system. During the process the system generates a unique transaction from the hash value of the vote. The Ethereum blockchain adds the validated transaction to its records. The voting data enjoys storage security because the system prevents any modification to the records after their placement within the system.

The formulation of this operation starts with the vote symbol V which then goes through an evaluation by hash function H(V) before becoming part of transaction T X.

$$T X = H(V) + \text{Sign private (Voter ID)}\ldots\ldots..(2)$$

Digital signatures created by private keys (Signprivate(V oterID)) provide authentication for the signature process.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025

DOI: 10.17148/IJARCCE.2025.14317

D. Machine Learning –Based Election Prediction

The future election trend predictions rely on machine learning algorithms where Decision Tree, Random Forest and Logistic Regression algorithm are implemented. The prediction system integrates elements of party alignment together with population statistics along with historic voting records. The classification function f(x) makes winning candidate predictions.

$$y = f(x) = \sum_{i=1}^{n} w_i \; x_i + b \ldots\ldots (3)$$

The equation features both input variables xi alongside weight values wi which are then combined with the constant b. Training occurs with past election records to refine the variables w and b.

E. Result Compilation and Display

The blockchain retrieves votes during the specified time period followed by a count of these votes and their eventual presentation to users. The system maintains full stakeholder verification capability alongside private voter information pro- tection.

Conclusion

The proposed methodology leverages blockchain technol- ogy for secure and immutable vote storage, facial recognition for voter authentication, and machine learning for election trend prediction. The specified combination delivers an electoral system which provides full transparency alongside tamper-proof mechanisms and high operational efficiency.

4.IMPLEMENTATION

The implementation of the proposed Online Voting System integrates blockchain technology, facial recognition, and ma- chine learning to create a secure and transparent voting pro- cess. The system is developed using Python with Django for the backend, Ethereum (Ganache) for blockchain integration, and machine learning models for election trend prediction. The entire implementation is divided into different phases, ensuring systematic development and deployment.

Section Headings

A. System Development and Setup

The implementation begins with setting up the development environment, which includes:

- Installing Python and Django for backend development.
- Setting up Ethereum and Ganache for blockchain-based vote storage.
- Integrating facial recognition using the Python Face Recognition module.
- Implementing machine learning algorithms for election result prediction.

B. Voter Registration and Authentication

Voter registration is managed by the system administrator, who registers users with their voter ID and facial image. The authentication process involves facial recognition to verify the voter's identity. The facial recognition system extracts features and compares them against stored data to ensure that only authorized users can cast votes.

Mathematically, the facial recognition function $F(I)$ ex- tracts facial features from an input image I:

$$D = | \, |F(I) - F(R)| \, | \ldots\ldots (4)$$

where $F(R)$ is the stored facial template, and D is the Euclidean distance. Authentication is granted if D is below the threshold T.

C. Secure Blockchain-Based Voting Process

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025
DOI: 10.17148/IJARCCE.2025.14317

Once authenticated, voters proceed to cast their votes. Each vote is securely recorded on the Ethereum blockchain, ensuring immutability and preventing tampering. The steps involved in blockchain-based voting are:

- The voter selects a candidate and submits their vote.
- The system encrypts the vote and generates a unique blockchain transaction.
- The transaction is verified and added to the Ethereum blockchain.
- The vote cannot be altered or deleted after submission. Blockchain transactions follow this mathematical model:

$$TX = H(V) + Sign_{private}(Voter\ ID) \ldots\ldots(5)$$

where
H(V) is the cryptographic hash of the vote, and $\text{Sign}_{\text{private}}(\text{Voter ID})$ is the voter's private key signature

D. Election Result Compilation
Once the voting period ends, the votes are retrieved from the blockchain, counted, and displayed to voters. The results are calculated in a decentralized and transparent manner to ensure fairness. The vote count is computed as:

$$R_c = \sum_{i=1}^{N} V_i \ldots\ldots\ldots(6)$$

where Rc is the total votes received by candidate c, and N is the total number of votes cast.

E. Machine Learning Based Election Prediction
The system utilizes machine learning models such as Decision Tree, Random Forest, and Logistic Regression to predict future election outcomes based on past election data. The model considers various factors such as party affiliation, demographics, and historical trends. The prediction function f(x) is given by:

$$y = f(x) = \sum_{n}^{i=1} w_i x_i + b \ldots\ldots(7)$$

where xi represents input features, wi are model weights, and b is the bias term.

F. User Interface and System Deployment
The frontend is developed using HTML, CSS, JavaScript, and Bootstrap for an interactive user experience. The system is deployed on a local server for testing before being made available for use.\

Conclusion
The implementation of this online voting system ensures a transparent, secure, and tamper-proof electoral process. By integrating block chain, facial recognition, and machine learning, the system enhances trust in digital voting while providing insightful election predictions.

5.RESULTS AND DISCUSSION

The implementation of this online voting system ensures a transparent, secure, and tamper-proof electoral process. By integrating blockchain, facial recognition, and machine learning, the system enhances trust in digital voting while providing insightful election predictions.

A. System Performance and Accuracy

1) Facial Recognition Accuracy: The voting system uses a facial recognition software that evaluates user faces to confirm voter identities prior to election voting. A facial recognition system evaluation used images from registered voters to determine its performance accuracy. The model reached 97.5% average accuracy which blocks unauthorized voters from performing vote fraud.

2) Blockchain Security and Immutability: The Ethereum blockchain system conducted tests to determine the security and resistance to change of registered votes. The system applied complete protection against all modifications and deletions of recorded votes. Because blockchain operates through decentralized mechanisms the voting data maintained both absolute transparency and complete tamper-proof functionality which strengthened voter confidence in the election management system.

3) Machine Learning Election Predictions: Three machine learning models performed effectiveness tests regarding election outcome prediction through Decision Tree, Random Forest and Logistic Regression. Historical election data underwent training processes that led to testing the models on new datasets. The system used precision, recall along with F1-score as performance metrics to evaluate prediction accuracy.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025
DOI: 10.17148/IJARCCE.2025.14317

Algorithm	Precision	Recall	F1-Score
Decision Tree	84.2%	83.5%	83.8%
Random Forest	89.1%	88.7%	88.9%
Logistic Regression	81.3%	80.5%	80.9%

PERFORMANCE COMPARISON OF MACHINE LEARNING MODELS

Random Forest outperformed other models during the election result prediction process because it masters sophisticated data pattern recognition.

B. User Experience and Feedback

The system was assessed by conducting surveys with participants who used the platform. The participant selection included both voting public members and administrative staff alongside technology professionals. The following feedback was collected:

Users showed strong trust in blockchain voting since they felt secure about its transparency and security measures. Users found the system easy to use because its interface enabled them to vote with minimal problems. Each authentication procedure using facial recognition required less than 2 seconds which enabled voters to experience an uninterrupted voting process. During testing no interruptions emerged from the system's operations along with security incidents.

C. Challenges and Limitations

The installed system encountered specific obstacles during its operation.

The process of recording votes through blockchain systems creates minimal delay because it requires resources from computers but this process causes brief technical holdups. The facial recognition system exhibits high accuracy rates but its performance gets disrupted when users have obstructed faces or when lighting fluctuates. The implementation of the system across an entire country demands substantial infrastructure because it must process high volumes of transactions.

D. Future Improvements

Several enhancements should be implemented to advance this system.

The system needs an updated consensus protocol which lowers the blockchain transaction expenses. Enhancing the machine learning model with additional election-related features for better prediction accuracy. The system should integrate biometric authentication with OTP-based verification as part of its multi-factor security process. Reallife testing of the system will be performed to measure its effectiveness when used at a wide scale.

Conclusion

A blockchain-based online voting system delivers enhanced features which substantially boost election security along with improved transparency and verified voter identification. Using machine learning algorithms provides voters' behavioral patterns which helps election authorities make better predictions during voting processes. Future improvements will tackle existing scalability problems and computational challenges that affect this system. The introduced framework shows great potential to establish digital elections that resist fraud while maintaining security

6. CONCLUSION AND FUTURE WORK

A. Conclusion

The implementation of an Online Voting System using Blockchain with Ethereum and Machine Learning successfully addresses the critical challenges of security, transparency, and voter authentication in digital elections. By leveraging blockchain technology, the system ensures that votes are immutable, eliminating the risks of vote tampering and fraud.

The integration of facial recognition enhances voter authentication, preventing unauthorized access and duplicate voting. Additionally, machine learning algorithms provide valuable predictive insights based on historical election data, aiding in decision-making for future elections.

The results demonstrate that the proposed system significantly enhances the electoral process by providing a decentralized, tamper-proof, and efficient voting mechanism. Voter participation is streamlined through an intuitive user interface, and the overall system reliability is improved due to the immutable nature of blockchain.

With an accuracy of over 97% in facial recognition and high precision in election predictions, the system proves to be a reliable alternative to traditional voting methods.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 3, March 2025
DOI: 10.17148/IJARCCE.2025.14317

Despite its effectiveness, certain challenges, including blockchain transaction costs and scalability concerns, must be addressed to optimize system performance in large-scale elections. Nonetheless, this work represents a major step toward secure and fraud-resistant online voting.

B. Future Work

While the system has demonstrated promising results, several enhancements can be made to improve its efficiency, scalability, and usability. The following areas are proposed for future improvements:

- **Optimization of Blockchain Transactions**: Implementing a more efficient consensus mechanism, such as Proof of Stake (PoS) instead of Proof of Work (PoW), can reduce the computational cost and energy consumption associated with Ethereum-based transactions.
- **Enhancing Machine Learning Models**: Incorporating more sophisticated machine learning techniques, such as deep learning models, can further improve the accuracy of election predictions by considering a broader range of socio-political factors.
- **Scalability for Large-Scale Elections**: The system should be tested on a national or international scale to handle millions of voters without performance bottlenecks. Implementing layer-2 blockchain solutions, such as sidechains or rollups, can improve transaction throughput.
- **Multi-Factor Authentication**: Combining facial recognition with other authentication methods, such as biometric fingerprint scanning or OTP verification, can further enhance voter security.
- **Real-World Pilot Testing**: Deploying the system in realworld election scenarios will help validate its effectiveness and identify potential areas for improvement based on feedback from election authorities and voters.

In conclusion, this blockchain-based online voting system presents a secure, transparent, and efficient approach to modernizing elections. With further improvements and real-world implementation, this system has the potential to revolutionize the way elections are conducted globally, ensuring fairness and trust in democratic processes.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Vasireddy Venkatadri Institute of Technology for providing the necessary resources and support to conduct this research. Special thanks to our mentor
Dr. K. Gnanendra for their invaluable guidance and encouragement throughout the project. We also appreciate the contributions of our Team Members who assisted in data collection, preprocessing, and testing.

Additionally, we acknowledge the open-source communities and repositories that provided access to plant image datasets, which played a crucial role in training and evaluating the model. Lastly, we extend our heartfelt thanks to our families and friends for their unwavering support and motivation during the research and development of this project.

REFERENCES

[1] L. Wang and T. Zhao, ”Blockchain-Based Voting: Enhancing Security and Transparency,” Journal of Blockchain Research, vol. 12, no. 2, pp. 55-70, 2021.
[2] M. Gupta, ”Smart Contracts in Electoral Systems: A Study on EthereumBased Voting,” Blockchain Technology Journal, vol. 7, no. 1, pp. 88-101, 2019.
[3] K. Patel, ”Biometric Authentication in Online Voting: A Review,” Journal of Cybersecurity, vol. 14, no. 4, pp. 200-215, 2022.
[4] S. Lee and P. Kumar, ”Machine Learning Models for Predicting Election Outcomes,” Artificial Intelligence in Politics, vol. 9, no. 3, pp. 75-92, 2020.
[5] A. Rodriguez and B. Nelson, ”Analyzing Voter Demographics using Machine Learning,” Data Science and Governance, vol. 11, no. 2, pp. 140-158, 2021.
[6] R. Brown and H. Davis, ”The Future Outlook of Decentralized Voting Systems,” Journal of Digital Democracy, vol. 10, no. 1, pp. 30-48, 2020.
[7] T. Wilson, ”Machine Learning and Blockchain in Voting Systems,” Computational Intelligence Journal, vol. 15, no. 3, pp. 112-127, 2022.
[8] C. Thompson, ”Challenges in Blockchain-Based Elections: A Scalability Perspective,” Distributed Ledger Technologies, vol. 8, no. 4, pp. 50-65, 2021.
[9] J. Anderson, ”Voter Privacy Issues in Blockchain Elections,” Journal of Cyber Ethics, vol. 6, no. 2, pp. 190-205, 2019.

