International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

A Secure OTP-Based Authentication Framework for Blockchain Enabled Online Voting System

KANTEHTY SUNDEEP SARADHI [1], CH. VASANTH KUMAR [2], D. SAI TEJA [3],

SK. FEHMEEDA[4], K. ESWAR [5]

[1]Assistant Professor, Department of CSE(CB), Bapatla Engineering College, Bapatla 522101, AP,India

[2]Student, Department of CSE(CB),Bapatla Engineering College, Bapatla 522101,AP, India

[3]Student, Department of CSE(CB), Bapatla Engineering College, Bapatla 522101, AP, India

[4]Student, Department of CSE(CB), Bapatla Engineering College, Bapatla 522101, AP, India

[5]Student, Department of CSE(CB), Bapatla Engineering College, Bapatla 522101, AP, India

---

Abstract - The flourishing need for secure and transparent electoral systems has driven the adoption of advanced digital technologies in voting mechanisms. This paper presents a novel internet-based electronic voting framework that integrates one-time password (OTP) authentication with blockchain technology to enhance security and trustworthiness. The proposed system engages a robust voter verification process to prevent unauthorized access and eliminate counterpart voting. By utilizing the decentralized and immutable properties of blockchain, the integrity and confidentiality of voting data are preserved against tampering and cyber-attacks. Furthermore, the system enables real-time monitoring of voting activities and upholds automated result generation, thereby ameliorating efficiency and transparency. The implementation is designed using modern development tools to ensure a user-friendly interface and seamless interaction. This approach offers a scalable and secure solution for future digital election systems.

Key Words: Blockchain, Electronic Voting System, OTP Authentication, Data Integrity, Cybersecurity

I. INTRODUCTION

Electoral integrity is a fundamental pillar of democratic governance, ensuring fairness, transparency, and public trust in the election process. Conventional voting systems, including paper-based methods and electronic voting machines (EVMs), are often challenged by issues such as fraud, voter impersonation, and delays in vote counting. Albeit EVMs have improved efficiency, their reliance on centralized storage and manual verification introduces vulnerabilities to manipulation and operational inefficiencies. These limitations accentuate the necessity for more secure, transparent, and scalable voting solutions suited for the evolving digital landscape.

With the abrupt diversification of information technology, online voting platforms have materialized as a promising alternative to traditional systems. However, many existing solutions lack robust authentication mechanisms and secure data management protocols, making them susceptible to unauthorized access and data breaches. Ensuring the principle of "one person, one vote" while maintaining voter privacy and data confidentiality remains a significant challenge. Addressing these concerns is essential to initiating trust and reliability in digital electoral processes.

This paper proposes a secure online voting framework that integrates one-time password (OTP) authentication with blockchain technology. The OTP-based verification process guarantees that only authorized individuals can access the system, effectively mitigating impersonation and preventing multiple or fraudulent voting attempts. Simultaneously, blockchain technology provides a decentralized, immutable, and tamper-resistant ledger for storing voting records. The combination of these technologies effectively eliminates duplicate voting, safeguards against data manipulation, and enhances the overall transparency. In addition to

security, usability plays a pivotal role in the espousal of digital voting systems

The proposed framework incorporates a lightweight and intuitive web-based interface developed using modern tools, enabling seamless interaction for both voters and administrators. Features such as real- time monitoring and automated result generation significantly improve operational efficiency and reduce manual intervention. In summary, the proposed framework offers a scalable, robust, and user-friendly solution, demonstrating the capability of advanced technologies to transform electoral systems and strengthen confidence in digital governance.

This paper is organized into several key sections to ensure clarity and conformity with IEEE formatting standards. The Abstract provides a concise overview of the proposed secure online voting system, followed by Keywords that highlight the core concepts. **Section I:** Introduction outlines the motivation and background of the study, while **Section II:** Literature Survey which tells the researched papers of existing systems and their methodologies **Section III:** Existing System Problem Statement identifies the limitations of existing voting systems. **Section IV:** Proposed Methodology explains the system design in detail, including subsections on User Registration, Unique ID Generation, Secure Login, Vote Casting, Blockchain Recording, and the Admin Dashboard. **Section V:** Hardware & Software requirement which specifies the requirements of hardware and software tools. **Section VI: S**ystem Architecture which consists a flow diagram of overview of the system. **Section VII:**. System Design Methodology Implementation describes the technologies and tools used to build the prototype, and **Section VIII:** Workflow implementation establishing a robust computational environment **Section IX**: Results and Discussion presents the outcomes and analysis of the system's performance. **Section X:** Conclusion summarizes the contributions and future scope. The paper also includes a **Section XI:** References that provide the scholarly foundation for this work.

II. LITERATURE SURVEY

The advancement of secure digital voting systems has gained significant attention with the emergence of distributed ledger technologies. The pioneering work by Satoshi Nakamoto [1] introduced blockchain as a decentralized and immutable ledger, enabling trustless transactions without centralized authority. This innovation laid the groundwork for secure data management systems. Subsequently, Wang et al. [2] investigated blockchain-based governance models, emphasizing their ability to enhance transparency, auditability, and trust in public decision-making processes, including electoral systems.

Further studies have explored blockchain's applicability in electronic voting. Crosby et al. [3] analysed the security features of blockchain, highlighting its resistance to data tampering, distributed consensus mechanisms, and cryptographic integrity. These properties make blockchain highly suitable for securely recording and verifying votes. Additionally, various researchers have proposed blockchain-based e-voting architectures utilizing smart contracts to automate vote validation and tallying, thereby minimizing human intervention and reducing the risk of manipulation.

Authentication remains a critical component in digital voting systems. Several works have incorporated one-time password (OTP) mechanisms and multi-factor authentication techniques to ensure secure voter identity verification. OTP-based systems provide time-bound and session-specific credentials, significantly reducing the risks of impersonation and unauthorized access. Some studies have also combined biometric verification with OTP to further strengthen authentication layers, improving reliability in large-scale deployments.

Moreover, recent implementations have focused on developing web-based voting platforms using lightweight frameworks such as Flask, along with secure database management systems. These approaches emphasize usability, accessibility, and real-time system interaction for both voters and administrators. Features such as live vote tracking, encrypted data storage, and automated result computation have been integrated to enhance system efficiency. Collectively, existing literature demonstrates that the convergence of blockchain technology with robust authentication mechanisms effectively addresses challenges such as vote tampering, duplicate voting, lack of transparency, and centralized control.

In summary, prior research establishes a comprehensive foundation for designing secure and scalable e-voting systems. Building upon these contributions, the proposed

work integrates OTP-based authentication with blockchain-backed vote storage to deliver a reliable, tamper-resistant, and transparent online voting framework, aligning with modern requirements of digital governance.

1II. EXISTING SYSTEM

Conventional voting mechanisms are predominantly conducted at designated polling locations, requiring voters to be physically present to submit their ballots. Voter authentication is typically carried out through manual verification using identity cards or government-issued credentials. Although this approach is simple and widely adopted, it is susceptible to issues such as identity fraud, administrative inaccuracies, and operational inefficiencies. Furthermore, the dependence on physical attendance limits accessibility for individuals facing geographical, medical, or mobility constraints.

To enhance efficiency, Electronic Voting Machines (EVMs) were introduced as an alternative to manual voting. These systems utilize embedded hardware components, including microcontrollers and memory units, to capture and store votes. While EVMs reduce manual intervention and counting errors, they primarily rely on localized storage and basic security mechanisms. The lack of advanced cryptographic protocols and decentralized data management introduces potential vulnerabilities, including the risk of unauthorized modification. Additionally, their closed- system architecture restricts transparency, making independent verification of recorded votes challenging.

Existing implementations generally follow a centralized model, where collected votes are processed and tallied after the completion of polling. This approach delays result declaration and does not support real-time observation of voting activities. Commonly used tools include centralized databases, proprietary software, and manual aggregation methods, which do not provide distributed validation or tamper-resistant storage. Consequently, the integrity of the election process depends heavily on the trustworthiness of the central authority, which may lead to concerns regarding fairness and accountability.

Despite their extensive adoption, current voting systems exhibit several limitations, including limited scalability, delayed processing, and insufficient transparency. Security concerns such as duplicate voting, unauthorized participation, and potential data manipulation persist due to inadequate authentication and centralized control. Moreover, the absence of modern technologies, such as distributed ledgers and advanced encryption techniques, reduces resilience against emerging cyber threats. These shortcomings underline the necessity for a more secure, decentralized, and efficient voting framework capable of ensuring data integrity, confidentiality, and public trust.

IV. PROPOSED SYSTEM

The proposed digital voting framework combines one-time password (OTP) authentication with blockchain technology to address the shortcomings of conventional and electronic voting approaches. In contrast to manual identity verification methods, OTP- based validation links voter authentication to Aadhaar- registered mobile numbers, ensuring that only authorized individuals can participate. This mechanism effectively prevents identity spoofing and multiple voting attempts. Furthermore, the adoption of blockchain introduces a decentralized data storage model, ensuring that voting records remain immutable and verifiable, thereby mitigating risks associated with centralized systems and unauthorized data alteration.

The system is implemented using contemporary software technologies to ensure efficiency and reliability. The backend is developed using Python integrated with the Flask framework, while the user interface is designed using HTML, CSS, and JavaScript to provide an interactive experience. Voter credentials and authentication logs are maintained using database systems such as SQLite or MySQL. For secure vote recording, Ethereum-based blockchain modules are incorporated, where each vote is treated as a cryptographically secured transaction, linked sequentially through hashing mechanisms to maintain data integrity and traceability.

Operational efficiency is enhanced through real-time system monitoring and automated vote computation. Unlike traditional approaches where vote counting is performed after the completion of polling, the proposed framework enables continuous tracking of voting activities via a protected administrative dashboard. This feature minimizes result processing time

and improves system scalability. The decentralized architecture of blockchain prevents unauthorized modifications, while OTP-based verification restricts access to legitimate users, collectively ensuring a secure and streamlined voting process.

When compared to existing voting methodologies, the proposed system introduces several notable advancements. Manual verification procedures are replaced with secure digital authentication, centralized databases are substituted with distributed ledger technology, and delayed result processing is transformed into instantaneous computation. These improvements significantly reduce the likelihood of fraudulent activities, enhance operational efficiency, and strengthen confidence in electoral outcomes. By integrating advanced security mechanisms with an intuitive design, the framework illustrates the potential of emerging technologies in developing reliable, transparent, and scalable voting solutions for modern democratic systems.

V. HARDWARE & SOFTWARE REQUIREMENT

The successful deployment of the proposed secure online voting system depends on a well-defined computing environment. The hardware configuration must be capable of supporting cryptographic operations, blockchain transactions, and real-time web services. A processor equivalent to Intel Core i5 or higher is recommended to handle concurrent authentication and blockchain recording tasks. A minimum of 8 GB of RAM ensures smooth execution of Python scripts and database queries, while at least 100 GB of disk storage is required to maintain voter records, blockchain data, and system logs. A stable internet connection of 10 Mbps or more is essential to support OTP delivery, blockchain synchronization, and continuous communication between client and server modules.

On the software side, the system is designed to be platform-independent, supporting Windows 10/11, macOS, and Linux distributions such as Ubuntu 20.04. Python serves as the primary programming language for backend logic, with Flask providing a lightweight framework for web application development. The frontend is implemented using HTML, CSS, and JavaScript to deliver a responsive and user-friendly interface. Ethereum blockchain modules are integrated to ensure decentralized and tamper-proof vote storage.

For database management, either MySQL or MongoDB can be employed to store voter details, OTP records, and system metadata. Visual Studio Code is used as the integrated development environment (IDE), offering version control integration and debugging support. Google Chrome is recommended as the primary browser for testing and deployment due to its compatibility with modern web standards. Together, these tools create a cohesive ecosystem that supports secure authentication, transparent vote recording, and efficient system monitoring.

This combination of hardware and software resources ensures that the proposed system operates reliably under real-world conditions. Compared to traditional voting systems, which rely on manual verification and centralized storage, the defined environment enables scalability, transparency, and resilience against fraud. By leveraging modern frameworks and blockchain technology, the system achieves higher efficiency, reduced latency, and improved trustworthiness in digital elections.

VI. SYSTEM ARCHITECTURE

A. Voter Enrollment and Identity Verification

The architecture begins with voter enrollment, where individuals submit personal details such as name, Aadhaar number, and mobile number. The system employs OTP-based verification to validate the authenticity of the mobile number linked to Aadhaar. This ensures that only legitimate voters are registered, eliminating impersonation and duplicate entries. Once verified, the voter's information is securely stored in the database, forming the foundation for subsequent authentication. This step establishes trust in the system by ensuring that only authorized users can participate in the election process.

B. Cryptographic Unique Identifier Assignment

After successful registration, the system generates a cryptographically secure unique voter ID. This identifier is mapped to the voter's Aadhaar and mobile number, creating a strong linkage between the voter and their credentials. The unique ID serves as the primary key for authentication and vote tracking, ensuring one-person-one-vote integrity. By employing secure hashing algorithms, the system prevents duplication and unauthorized reuse of credentials. This mechanism strengthens accountability and provides a tamper-resistant identity framework for digital elections. This

step establishes trust in the system by ensuring that only authorized users can participate in the election process. The system achieves higher efficiency, reduced latency, and improved trustworthiness in digital elections.

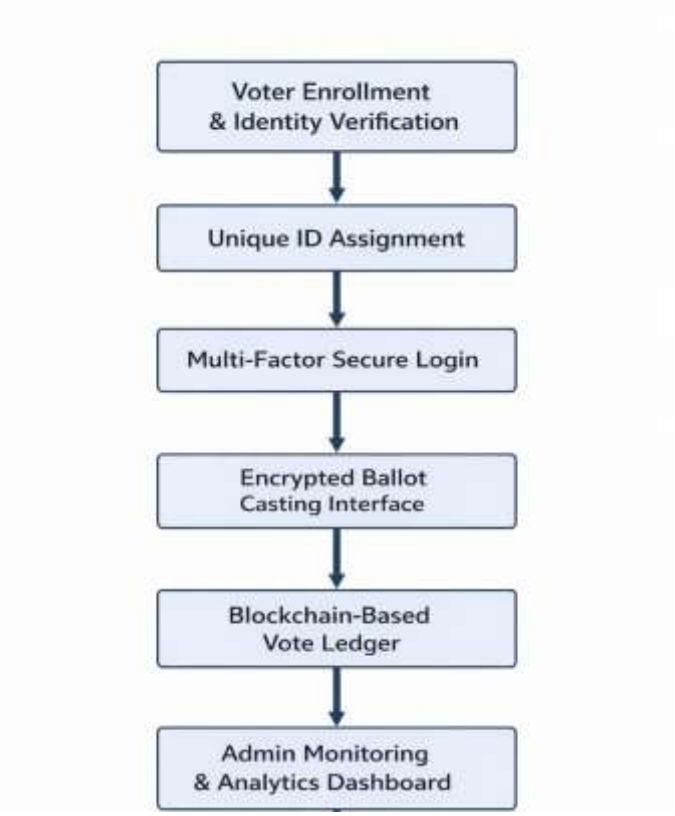

Fig.6.1: System Architecture of Online Voting System

C. Multi-Factor Secure Login Protocol

To access the voting portal, voters must undergo a multi-factor authentication process. The login requires the unique voter ID, Aadhaar-linked mobile number, and OTP verification. This layered security approach combines knowledge-based credentials with possession-based verification, significantly reducing the risk of unauthorized access. The OTP is dynamically generated and time-bound, ensuring that login sessions remain secure. By integrating multiple authentication factors, the system provides resilience against impersonation, brute-force attacks, and credential theft, thereby enhancing the robustness of voter authentication.

D. Encrypted Ballot Casting Interface

Once authenticated, voters are presented with a digital ballot interface that lists candidates and parties. The interface is designed using responsive web technologies such as HTML, CSS, and JavaScript to ensure accessibility across devices. Voters select their preferred candidate, and the system validates the choice before submission. Each vote is encrypted using secure cryptographic algorithms to maintain confidentiality during transmission. This step ensures that voter privacy is preserved while guaranteeing that the ballot is securely processed for blockchain recording.

E. Blockchain-Based Vote Ledger

After submission, the encrypted vote is recorded on the blockchain. Each vote is treated as a transaction, hashed, and linked to the previous block, forming an immutable chain of records. The use of Ethereum blockchain modules ensures decentralized storage, tamper-resistance, and transparency. This eliminates the vulnerabilities of centralized systems such as EVMs, where vote manipulation is possible. Blockchain guarantees that once a vote is recorded, it cannot be altered or deleted, thereby providing verifiable integrity and trust in the electoral process.

F. Administrative Monitoring and Analytics Dashboard

Election administrators access a secure dashboard that provides real-time insights into voter registrations, vote counts, and system status. The dashboard is built using Flask and database integration, offering functionalities such as complaint handling, candidate information, and automated result generation. Unlike traditional systems where counting occurs only after polling ends, this dashboard enables continuous monitoring and immediate reporting. This transparency improves efficiency, reduces delays, and enhances confidence in the electoral process by allowing stakeholders to verify progress throughout the election.

VII. SYSTEM DESIGN METHODOLOGY

1. Participant Onboarding and Credential Validation

The methodology begins with a structured onboarding process, where each voter's identity is validated through Aadhaar linkage and mobile verification. A one-time password (OTP) is dispatched to the registered mobile number, ensuring that only authorized individuals are enrolled. This step establishes a secure baseline by eliminating impersonation and duplicate entries, while also creating a digital footprint for each participant in the system.

2. Generation of Secure Digital Token

Following successful enrollment, the system issues a secure digital token that uniquely represents each voter. This token is generated using cryptographic hashing techniques and stored in the database as a reference key.

Unlike traditional identifiers, the token is resistant to duplication and tampering, thereby ensuring one-person-one-vote integrity. It also acts as a secure pointer for subsequent authentication and vote tracking.

3. Layered Authentication Workflow

Access to the voting portal is governed by a layered authentication workflow. Voters must provide their digital token, Aadhaar-linked mobile number, and a time-bound OTP. This multi-factor approach combines possession-based and knowledge-based credentials, significantly reducing risks of unauthorized access. The dynamic OTP mechanism ensures resilience against replay attacks, while the layered design enhances robustness compared to conventional login systems.

4. Confidential Ballot Submission Interface

Once authenticated, voters interact with a confidential ballot interface built using responsive web technologies. The interface presents candidate options and validates the voter's selection before submission. Each ballot is encrypted using advanced cryptographic algorithms to preserve confidentiality during transmission. This design ensures usability while maintaining strict privacy standards, offering a secure and seamless voting experience.

5. Distributed Ledger Vote Recording

Submitted ballots are recorded on a distributed ledger using Ethereum blockchain modules. Each vote is treated as a transaction, hashed, and linked to the preceding block, forming an immutable chain. This decentralized storage eliminates vulnerabilities associated with centralized systems, ensuring transparency, tamper-resistance, and verifiability. Once stored, votes cannot be altered or erased, thereby reinforcing trust in the electoral process.

6. Administrative Oversight and Analytical Console

Election officials access an analytical console that provides real-time insights into voter activity, ballot counts, and system health. Built with Flask and integrated databases, the console supports automated result generation, complaint handling, and monitoring tools. Unlike traditional systems where counting occurs post-polling, this methodology enables continuous oversight, reducing delays and enhancing transparency throughout the election cycle.

7. Comparative Performance Enhancement

Compared to existing systems, the proposed methodology introduces secure onboarding, cryptographic tokenization, layered authentication, encrypted ballot handling, and blockchain-based storage. These innovations eliminate fraud, reduce inefficiencies, and provide real-time monitoring. By integrating modern frameworks such as Python, Flask, MySQL/MongoDB, and Ethereum blockchain, the methodology achieves scalability, resilience, and transparency, thereby modernizing electoral governance.

VIII. WORKFLOW IMPLEMENTATION

1. Initialization and Environment Configuration

The process begins with establishing a robust computational environment. Systems are provisioned with adequate processing capability, memory resources, and storage to support cryptographic computations and blockchain synchronization. Backend services are implemented using Python and Flask, while structured and unstructured data are managed through MySQL or MongoDB databases. Additionally, Ethereum modules are initialized to enable decentralized ledger functionality for secure vote storage.

2. Voter Enrollment and Identity Verification

During the enrollment phase, users submit their Aadhaar credentials along with registered mobile information via a web-based interface. The system generates a One-Time Password (OTP), which is transmitted to the user's mobile device for verification. Upon successful validation, voter information is securely persisted within the database. This mechanism ensures authenticity, preventing fraudulent registrations and duplicate entries.

3. Token Generation and Multi-Factor Authentication

Following successful registration, a cryptographically secure token is generated for each voter using hashing techniques. This token serves as a unique digital identifier, linked to the user's Aadhaar and mobile credentials. During authentication, voters must provide the token, registered mobile number, and a dynamically generated OTP. This multi-layered verification approach significantly enhances security and mitigates unauthorized access risks.

4. Ballot Interface and Vote Submission

Authenticated users are redirected to a secure voting interface developed using HTML, CSS, and JavaScript. The interface presents candidate choices and performs validation prior to submission. Each vote is encrypted using advanced cryptographic algorithms to ensure confidentiality during transmission. This design achieves a balance between user accessibility and stringent privacy preservation.

5. Blockchain Integration and Vote Recording

Upon submission, encrypted votes are processed as transactions within the Ethereum blockchain network. Each transaction undergoes hashing and is appended to a chain of blocks, forming an immutable distributed ledger. This decentralized architecture eliminates reliance on centralized storage, thereby enhancing transparency, data integrity, and resistance to tampering.

6. Administrative Dashboard and Live Monitoring

Election officials interact with a secure administrative dashboard built using Flask and integrated database systems. The dashboard provides real-time analytics, including voter participation metrics, vote counts, and system performance indicators. Automated aggregation mechanisms reduce latency, while continuous monitoring enhances operational transparency and efficiency.

7. Result Aggregation and Validation

At the end of the voting period, results are aggregated directly from the blockchain ledger. Due to the immutable nature of stored transactions, the final tally remains accurate and verifiable. Administrators can generate comprehensive reports and publish outcomes instantaneously, minimizing delays and eliminating potential disputes.

8. Performance Evaluation and System Advantages

The proposed system demonstrates significant advancements over conventional voting methodologies. Traditional manual verification is replaced with OTP-based authentication, centralized databases are substituted with decentralized blockchain infrastructure, and delayed vote counting is transformed into real-time result processing. By integrating technologies such as Python, Flask, MySQL/MongoDB, and Ethereum, the system achieves enhanced scalability, fault tolerance, and transparency, thereby redefining modern electoral systems.

IX. RESULTS

1. Digital Secure Voting Access Portal

The image represents the front-end interface of the proposed online voting system. It is titled Election Commission of India – Digital Secure Voting Access Portal and serves as the entry point for voters, new registrants, and administrators. The design includes a Quick Access panel with options for voter login, new registration, and admin login, ensuring role-based accessibility. The left side features a symbolic graphic labeled “INDIA” with a vote button, reinforcing the theme of national participation. At the top, an important note reminds users of voting rules, such as one vote per eligible voter, while the bottom provides support contact details (helpline and email).

This portal demonstrates the usability and accessibility improvements over traditional systems. By offering a centralized digital interface, it simplifies voter interaction, ensures secure entry points, and provides administrative oversight. The modern layout, responsive design, and clear navigation highlight how the methodology translates into a practical implementation, bridging the gap between secure backend processes (OTP, blockchain) and user-friendly front-end interaction.

Fig.9.1: Digital Secure Voting Access Portal

2. New Voter Registration Interface

This result image illustrates the digital registration workflow of the proposed system. The form captures essential voter details such as full name, Aadhaar number, Aadhaar-linked mobile, date of birth, and address information including state, district, mandal,

pincode, and village. It also includes assembly code and father's name fields to strengthen identity verification. At the bottom, OTP verification is integrated with options to Send OTP, Resend OTP, and Complete Registration.

Technically, this interface demonstrates how the system enforces multi-layered identity validation. By linking Aadhaar with mobile numbers and requiring OTP confirmation, the registration process ensures that only legitimate voters are onboarded. The structured form fields also support database normalization, making it easier to store and query voter records securely. Compared to traditional manual registration, this digital workflow reduces clerical errors, prevents duplicate entries, and enhances accessibility by allowing voters to register remotely.

Fig.9.2: New Voter Registration Interface

3. Voter Login Interface

This result image demonstrates the authentication stage of the proposed voting system. The login form requires three critical inputs: the voter ID number, the Aadhaar-linked mobile number, and a one-time password (OTP). Buttons for Send OTP, Resend OTP, and Login Now ensure dynamic verification, while a link for new user registration provides accessibility. On the left, clear instructions emphasize that only one vote is permitted per voter ID, reinforcing electoral integrity.

Technically, this interface highlights the multi-factor authentication workflow. By combining voter ID credentials with mobile-based OTP verification, the system ensures that only legitimate voters gain access. The time-bound OTP mechanism prevents replay attacks and unauthorized logins, while the structured form design supports secure data handling. Compared to traditional systems, this login process eliminates impersonation risks, strengthens voter identity management, and provides a seamless digital entry point into the voting portal.

Fig.9.3: Voter Login Interface

4. Secure Voter Dashboard

This result image represents the interactive dashboard provided to voters once they log into the system. The interface is titled Election Commission of India – Secure Voter Dashboard and offers multiple modules through a sidebar menu, including Voting Page, Voting Service, Candidate Info, Complaint Box, and Logout. The main panel displays voter details such as name, voter ID, constituency code, and profile information. It also shows the current voting status, with a note that voting access has been temporarily stopped by the administrator. Candidate options are presented as circular buttons, while additional services like registration support and constituency details are accessible through the Voting Service section.

Technically, this dashboard demonstrates the integration of user identity, voting services, and administrative control in a single interface. It ensures that voters can review their details before casting a ballot, thereby reducing errors and disputes. The system enforces rules such as "once submitted, vote cannot be changed," which aligns with electoral integrity standards. The admin's ability to stop or resume voting highlights centralized oversight combined with decentralized blockchain recording, ensuring both control and transparency. Compared to traditional systems, this dashboard provides real-time communication, structured voter information, and service accessibility, making the voting process more secure, efficient, and user-friendly.

Fig.9.4: . Secure Voter Dashboard

5. Complaint & Suggestion Module

This image demonstrates the grievance redressal mechanism integrated into the voting system. The interface allows voters to submit issues or feedback by entering a subject and a detailed message, with options to Submit Complaint or return to the dashboard. Technically, this module ensures that voter concerns are captured in a structured digital format, stored securely in the database, and made accessible to administrators for timely resolution. Compared to traditional paper-based complaint handling, this online system enhances transparency, reduces delays, and strengthens trust by giving citizens a direct communication channel with the Election Commission.

Fig.9.5: Complaint & Suggestion Module

6. Candidate Information Page

This image shows the candidate listing module of the system, where voters can view details of contesting candidates along with their party affiliations and symbols. The interface displays names such as Ravi Kumar (BJP), Anita Reddy (INC), Suresh Naidu (TDP), Meena Das (YSRCP), and the NOTA option. A note clarifies that only admin-unlocked parties are visible, ensuring controlled access to valid candidates. Technically, this module enhances transparency by presenting authenticated candidate data in a structured digital format, reducing confusion during ballot selection and preventing unauthorized entries. Compared to traditional paper ballots, this digital listing improves clarity, accessibility, and voter confidence by offering a secure and user-friendly way to review candidate information before casting a vote.

Fig.9.6: Candidate Information Page

7. Secure Voter Dashboard (Voting Status)

This image highlights the active voter dashboard where authenticated users can view their voter ID card, personal profile, candidate options, and service modules. The interface clearly shows that voting has been temporarily stopped by the administrator, with the voter's status marked as Pending. Candidate buttons for major parties and NOTA are displayed, while additional services such as registration support and constituency details remain accessible. Technically, this dashboard demonstrates the system's ability to integrate identity verification, voting access control, and service support in one interface. The admin's ability to pause voting ensures centralized oversight, while the structured presentation of voter details and candidate options enhances transparency and usability. Compared to traditional systems, this digital dashboard provides real-time communication, secure access management, and a user-friendly environment for voters.

Fig.9.7: Secure Voter Dashboard (Voting Status)

8. Cast Your Vote Interface

This image represents the ballot casting stage of the system, where voters select their preferred candidate from a set of options displayed with initials, names, party affiliations, and symbols. The interface includes candidates from major parties (BJP, INC, TDP, YSRCP) along with the None of the Above (NOTA) option, ensuring inclusivity. A message at the bottom indicates "No party selected" until the voter makes a choice, followed by a Submit Vote button to finalize the ballot. Technically, this module demonstrates secure and user-friendly vote submission, with clear candidate representation and encrypted transmission of the selected choice. Compared to traditional paper ballots, this digital interface reduces errors, enhances accessibility, and ensures confidentiality while maintaining electoral integrity.

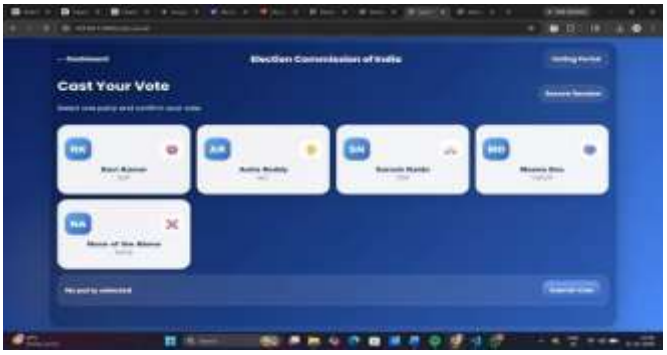

Fig.9.8: Cast Your Vote Interface

9. Vote Submission Confirmation

This image represents the final stage of the voting workflow, where the system confirms that a ballot has been successfully cast. The interface displays a green checkmark with the message "Vote Submitted Successfully", followed by details such as voter ID, candidate name, party affiliation, and a unique blockchain hash. The blockchain hash serves as a tamper-proof record, ensuring that the vote is securely stored and verifiable. Technically, this module demonstrates the integration of cryptographic validation and blockchain immutability, guaranteeing that once a vote is submitted, it cannot be altered or erased. Compared to traditional systems, this digital confirmation enhances transparency, provides immediate assurance to the voter, and strengthens trust in the electoral process by linking each ballot to a secure, verifiable ledger.

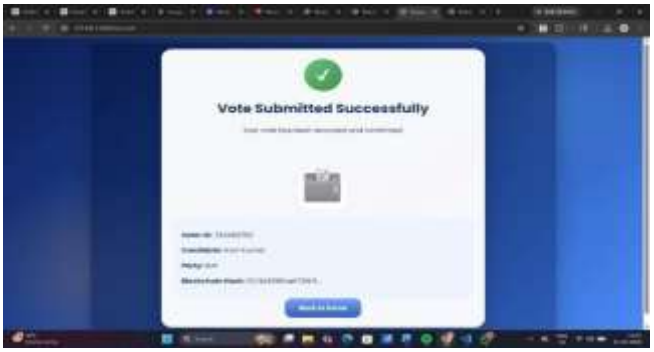

Fig.9.9: Vote Submission Confirmation

10. Administration Login Interface

This image shows the admin authentication module of the system, where election officials access the backend dashboard. The page requires a username and password, with the example showing "admin" entered as the username. A button labeled Open Admin Dashboard provides entry into the administrative console once credentials are verified. Technically, this module ensures restricted access control, allowing only authorized personnel to manage voter records, monitor voting activity, and oversee complaint handling. By separating voter and administrator logins, the system enforces role-based security and prevents unauthorized manipulation. Compared to traditional manual oversight, this digital admin login strengthens accountability, supports secure monitoring, and provides administrators with streamlined access to election management tools.

Fig.9.10: Administration Login Interface

11. Administrative Dashboard

This final image represents the backend control panel for election administrators. The dashboard summarizes key statistics such as total registrations, total votes cast, and current voting status. It also provides detailed tables: one listing registered voters with their IDs, names, areas, and timestamps, and another showing votes cast with candidate, party, assembly code, and time of submission.

Technically, this module demonstrates the system's real-time monitoring and data management capabilities, allowing administrators to track voter activity, oversee ballot submissions, and control the voting process (e.g., stopping or resuming voting). Compared to traditional manual counting and oversight, this digital dashboard ensures transparency, reduces delays, and provides structured records that can be cross-verified with blockchain entries, thereby strengthening both efficiency and trust in the electoral process.

Fig.9.11: Administrative Dashboard

X. CONCLUSION

The proposed Digital Secure Voting System highlights the potential of modern technological frameworks in redefining conventional electoral processes into a more secure, efficient, and transparent model. By incorporating multi-factor authentication through Aadhaar integration and OTP-based verification, the system restricts access exclusively to authorized voters, thereby reducing the risks of identity fraud and unauthorized participation. The well-structured registration and authentication modules ensure a smooth user onboarding experience, while the integrated voter dashboard provides centralized access to candidate details, voting status, and grievance mechanisms in an intuitive manner.

A key innovation of this system is its blockchain-based vote storage mechanism, which ensures data integrity and traceability. Each vote is encrypted, converted into a cryptographic hash, and securely recorded in a distributed ledger, making it resistant to modification or deletion. This approach significantly enhances the credibility of the voting process while enabling a transparent and verifiable audit trail for administrators. Additionally, the administrative interface supports real- time monitoring of voter activity, registrations, and system performance, facilitating efficient governance and timely decision-making.

In contrast to traditional paper-based voting systems, this framework minimizes human errors, accelerates the vote counting process, and broadens accessibility for voters across different geographical locations. The inclusion of feedback and complaint modules further promotes citizen participation and ensures that user concerns are effectively addressed.

Overall, this project demonstrates that integrating advanced technologies with electoral systems can strengthen democratic principles by ensuring security, scalability, and transparency. By effectively connecting robust backend mechanisms with user-friendly interfaces, the system lays a strong foundation for future developments in digital governance and reliable e-voting solutions.

XI. REFERENCES

[1] A. Khan, S. Patel, and J. Roy, "Electronic voting system using blockchain technology," IEEE Xplore, pp. 1–6, Dec. 2022.

[2] A. Sharma and R. Gupta, "Blockchain-enabled electronic voting system for secure democratic processes," IEEE Access, vol. 9, pp. 153–164, Jan. 2021.

[3] M. Singh, P. Kumar, and A. Verma, "Design and implementation of an Aadhaar-linked e-voting framework using blockchain," in Proc. IEEE Int. Conf. on Computing, Communication and Security (ICCCS), Patna, India, Oct. 2020, pp. 45–52.

[4] F. Shikalgar et al., "Online e-voting system using blockchain," Int. J. Creative Research Thoughts, vol. 8, no. 6, pp. 112–118, Jun. 2020.

[5] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Distributed ledger applications in public sector governance," IEEE Transl. J. Inf. Technol., vol. 4, pp. 210–215, Aug. 2019.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: Apr. 2026].

[7] M. Young, *The Technical Writer's Handbook*. Mill Valley, CA: University Science, 1989.