# Vote Verify: Authenticity in Electoral Process

[1]Harshita Limaye, [2]Aditi Sathe, [3]Sanika Warnekar, [4]Heeya Chawhan, [5]Yanishka Chiwhane,
[6]Pallavi Tanksale, [7]Sandeep Sonaskar
[1,2,3,4,5]UG Students, Department of Electronics and Telecommunication Engineering, MKSSS Cummins College of Engineering for Women, Nagpur, Maharashtra, India - 441110
[6]Assistant Professor, Department of Electronics and Telecommunication Engineering,
MKSSS Cummins College of Engineering for Women, Nagpur, Maharashtra(State), India – 441110
[7]Industrial Guide, Director VS Informatics Pvt. Ltd., Nagpur, Maharashtra(State), India – 440022

*Abstract*— **Maintaining electoral processes genuinely and with integrity is the greatest challenge confronting contemporary voting systems. Conventional voting processes are simple to simulate for identity theft and impersonation. Although current e-voting processes are less verifiable, which impacts the credibility of elections. Vote Verify is a sophisticated Internet of Things-based biometric authentication system that improves the security of votes through authenticating the identities of voters correctly and preventing impersonation and double voting. It relies on an ESP32 microcontroller, a biometric fingerprint sensor for identification, real-time database for monitoring the voters and automatic SMS verification for transparency in the process. Once they arrive at the polling booth the voters authenticate themselves through a fingerprint scan. When the authentication is confirmed, they get a confirmatory SMS to the registered mobile number, hence ensuring that only genuine voters can vote. This multi-step solution eradicates risks of impersonation and reduces human effort, thus guaranteeing efficient and secure election processes.**

**By incorporating biometric technology, Vote Verify ensures that each voter possesses a distinct and verifiable identity, reducing risks with traditional voting procedures. The system is programmable to provide greater transparency in the elections by creating tamper-proof proof-authentication records, real-time logs of voter authentication, and secure access control to election officials. Vote Verify is also highly scalable, hence making it applicable for local community elections, corporate voting thus promoting higher voter confidence and turnout. This intelligent, automated, and secure authentication mechanism is a quantum leap in the process of modernizing electoral systems. Using multi-factor authentication, real-time monitoring, and secure data storage in an encrypted form, Vote Verify provides a state-of-the-art solution to provide a reliable, fast, and fraud-proof electoral process, ushering the world toward a digitally secure and open democracy.**

***Keywords*—IoT, biometric authentication, fingerprint recognition, voter verification, election security, real-time monitoring, access control, ESP32, encryption, tamper-proof records, fraud prevention, database management, digital democracy, multi-factor authentication, transparent voting systems, secure electoral process**

## I. Introduction

Elections are crucial to democracy because they allow democratically and peacefully electing leaders by citizens. Voting processes, however, have undergone improvement over time from mere open displays such as raising one's hand to using vote boxes and, recently, electronic voting machines (EVMs). Along the way, claims of impersonation voters, stuff the ballot box, and generally, the usability of electronic voting systems continues to persist. Tamper-proofing of a secure, open, and tamper-evident voting system is the key to establishing public trust and obtaining democratic elections.

Vote Verify is an IoT-based biometric verification platform that secures elections through accurate verification of voters. The system uses an ESP32 microcontroller and supports a fingerprint scanner for biometric verification, LCD display, and computer-based SMS verification system. When the voter arrives at the polling station, he or she biometrically scans his or her fingerprint for verification. After matching against the pre-enrolled database, a success message SMS is sent to their enrolled mobile number to allow them to continue with the election process.

An additional verification process has been added with the inclusion of an LCD screen that displays the registered individual's name upon successful authentication. This is a second verification of identity, especially in case of a delayed confirmation message, so that election officials can validate the voter in real time. Also, information of validated voters is updated in real time on a secure webpage viewable to members of polling committees. This allows election officials to effectively trace voter authentication in a timely manner, enhancing the efficiency of operations and minimizing administrative workload. The system also contains a secure, tamper-evident database for real-time tracking, such that the election authorities can detect authenticated voters and flag fraudulent attempts like double voting. The new technology offers enhanced credibility to the elections through the removal of identity fraud and increased voter confidence, opening the door to a new, secure, and credible voting system. In the meantime, claims of voter impersonation, ballot box stuffing, and the general reliability of electronic voting systems continue.

## II. Objective

Increased security through biometric authentication
The overall goal of the suggested biometric-based verification system for voting is to ensure greater security, efficiency, and transparency during elections. Fingerprint authentication, internet communication, and cloud storage guarantee only registered voters vote and electoral impersonation and corruption are eliminated. Ease of user interface is an ease of verification for both voters and election officials.

Efficient and time-saving process

By automating the voter verification process, vote verify significantly reduces manual effort and minimizes waiting times at polling stations. The streamlined process ensures a faster and more efficient voting experience.

Real-time verification and transparency

The system ensures secure and unintermitted voter verification using fingerprint scanning so that votes are being made by real voters. After the voter verification is successfully done, the voter's name is flashed on a lcd screen with instant feedback. Instant SMS messages are also generated and sent to the registered phone number of the voter for security with attempted verification notice and for improved transparency and awareness.

Tamper-proof data storage for election monitoring

For central management of information, the system automatically logs authentication details, i.e., voter's name and time stamp, into a secure cloud database. The system provides real-time monitoring, secure storage, as well as long-term archiving such that the election administrators can monitor and audit voter authentication records remotely. Transparency is also provided by a web portal through provision of real-time reports of voting activity to facilitate fraud detection and accountability.

Scalability for various election types

The system is flexible and scalable, and the system is applicable in various election processes ranging from organizational elections to national election systems. The system supports voters, and dynamic election needs to be added, thereby making the system a future-proof and flexible solution. With such goals, the new biometric voting system gives a highly secure, transparent, and effective voting system as regards biometric identification, real-time alert, cloud storage, and web-based monitoring for a tamper-free and technology-based election system.

## III. Literature Survey

IoT in Electoral Monitoring

A study done by Sharma et al. (2021) laid a lot of stress on the implementation of IoT for real-time monitoring of elections. This research highlighted the ability of IoT devices in monitoring voting machines, identifying any form of tampering and maintaining unimpeded communication between polling stations and central servers. This mechanism boosts transparency and curtails lags in compiling results.

Biometric Voter Authentication

Biometric systems, includes fingerprint and facial recognition, have been employed to a large degree for avoiding voter impersonation and double voting. Khan and Roy (2020) illustrated through a study how biometric authentication guarantees proper identification of voters, decreasing impersonation and double voting. System scalability and data privacy issues were identified as issues to be resolved.

Blockchain for Electoral Transparency

While IoT is the central theme of the Blockchain for Electoral Transparency project, the application of blockchain technology to electoral systems has been a subject of discussion. Gupta et al. (2022) studied how the blockchain offers an immutable record for casting votes to maintain transparency and trust. Blockchain is complemented by IoT through the availability of a secure backend to store votes and authenticate the results for the same.

Accessibility in Voting Systems

Accessibility remains even today an important issue during elections, particularly for rural or disabled voters. Studies such as Alhassan et al. (2021) indicate mobile-based voting systems with IoT-enabled devices to guarantee secure and accessible options for all voters. Such systems have been put in place to promote the voter turnout by doing away with geographical and physical hurdles.

Machine Learning in Fraud Detection

Various research explored applying machine learning to detect the voting anomalies for several reasons. Various studies examined the application of machine learning in detecting anomalies in voting patterns. The procedures mentioned by Zhou et al. (2020) illustrate the ways predictive models highlight anomalies and suspected fraud as an additional layer of protection for the various systems. The Machine Learning models also indicate how predictive models detect anomalies and suspected fraud as an extra layer of protection.

IoT Security Challenges

One of the most significant issues that have been identified in IoT-based systems is its security level. Patel et al. (2023), in their research indicated vulnerabilities in the available IoT networks, which were unauthorized entry and data breaches. These issues necessitate strong encryption and authentication mechanisms to ensure the integrity of IoT-enabled electoral systems.

## IV. Methodology

Legacy voting systems employ manual verification techniques, which are labor-intensive and vulnerable to human incompetence or malice in the form of impersonation. In contrast to such vulnerabilities, the Vote Verify system employs biometric authentication in combination with real-time verification to provide a safe and efficient voting process.

The system authenticates voters via a fingerprint-based biometric verification procedure. Biometric information, i.e., fingerprints, of every voter is pre-registered and saved in an ESP32 microcontroller. When the voter comes to the polling booth, he scans his fingerprint on a fingerprint reader. The system verifies the scanned fingerprint with the details present in the

database. If it matches, the system will send a successful SMS to the registered mobile number of the voter, indicating that he has been successfully authenticated. In this way, only registered voters can move ahead and cast their votes. When the SMS message is delayed, the system even has an LCD screen showing the name of the registered voter when authentication is successful. The second level of authentication introduces transparency and enables the use of voter identification in real-time by electoral officials.

The whole authentication process is fast, with minimal or no lines formed at the polling centers and the voters authenticated quicker. All authenticated voters are safely stored in a database where the electoral officials can retrieve them to trace and audit. The database makes it possible for one to trace how many have been authenticated, thus making it easy to manage elections and transparency.

The Vote Verify system has been installed through embedded C/C++ for the ESP32 microcontroller, which handles fingerprint scanning, verification database management, and SMS sending alerts. The GSM SIM 800L module is interfaced to send live messages, where instant verification would be confirmed after a voter is verified. A constant supply of power has been utilized to operate the system to prevent the disruption of voting and uninterrupted operation during the election process.

As part of its adoption of biometric authentication, the immediate verification of voters, and anti-data storage protection, Vote Verify is a fraud-proof, secure, and safe way of strengthening the electoral process's integrity.


**Fig 1: Block Diagram of Vote Verify**

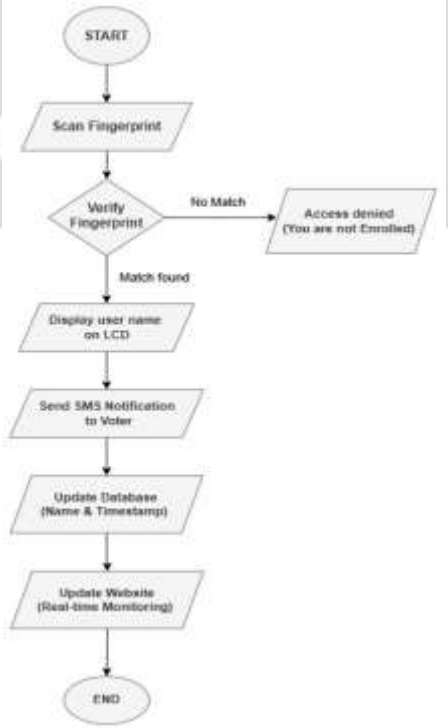


**Fig 2: Flow Chart of Vote Verify**

## V. PROPOSED SYSTEM

Vote Verify is meant to enhance the security and effectiveness of biometric-based voting and voter verification in electoral processes in real-time. Vote Verify offers fingerprint biometric system, ESP32 microcontroller, LCD display, and GSM module to facilitate secure and transparent authentication of votes.

The system is in operation with two-factor authentication: identification and verification. Identification involves comparing the fingerprint of the voter with pre-registered data kept on the ESP32 microcontroller. Verification occurs through successful fingerprint matching and transmission of an SMS authentication message to the registered phone number of the voter for validation.

The entire process of authentication is handled by the ESP32 microcontroller that detects fingerprint data in collaboration with the onboard fingerprint sensor. Once the fingerprint is read, it will be matched with records held by the system. After verification, an SMS verification message will be initiated by the GSM SIM 800L module on behalf of the voter indicating the verification status to the same effect. During network delay, a second level of authentication is provided with an LCD display that shows the name of the authenticated voter, while election officials identify themselves personally.

The information of the voters is stored in the onboard memory of the ESP32, and information of all the verified voters is securely stored in it. Information is provided to the election authority, and the election authority can know the turnout live and even make it transparent as far as the voting is concerned.

It is made for round-the-clock running with continuous power supply for perpetual service within the voting period. Vote Verify also removes the need for manual voter verification, avoiding human errors and the fraudulent election processes like double voting or voter impersonation.

By using biometric authentication with real-time authentication, Vote Verify provides an affordable, automated, and scalable election system. The system enhances the integrity of elections because only registered and verified voters can vote, thus ensuring citizens' trust in the democratic process.

## VI. System Explanation

Vote Verify is a sophisticated biometric authentication system used to ensure that electoral voting is secure and authentic. The ESP32 microcontroller is used as a processing board. This device has an embedded fingerprint reader for voter authentication, a GSM module for real-time authentication through SMS, and an LCD display to inform the user, guarantees safety through easy and automatic voter authentication. With the help of its easy and automatic biometric authentication, the technology makes sure there is security against voting fraud, and high operational efficiency to complement a secure voting procedure.

The authentication process starts once a voter approaches the polling booth and swipes his or her fingerprint on the biometric sensor. The ESP32 microcontroller takes the fingerprints and compares them against the fingerprints of registered voters stored in a database. On successful verification, it instructs your GSM SIM800L module to send an SMS notification to the registered voter's mobile number names. This notification informs you that a particular voter has been successfully authenticated to go and vote at this time. If, by chance, the SMS transmission is delayed due to network congestion, this system is also equipped with a display supporting LCD technology whereby the name of the authenticated voter is shown. The polling officers can thus perform manual authentication of the voter on the strength of this information.

This feature prevents a person from entering unauthorizedly. Other electrical supply features of the system can guarantee a fault-tolerant supply for long periods of time during election operations. Such features will enable continuous verification systems that allow further database procedures through Vote Verify tracking of each successful authentication. Real-time monitoring of voter turnout will become possible for managers of elections alongside the assurance of integrity and accountability of the counting of votes. The proposed design limits human supervision to the minimum level to prevent mistakes, efficiencies are optimized in general. Adding biometric authentication to this system makes its validity through real-time confirmation an open-ended, kind of fraud-proof, secured voting system that affords automatability and thus is scalable-a great system.

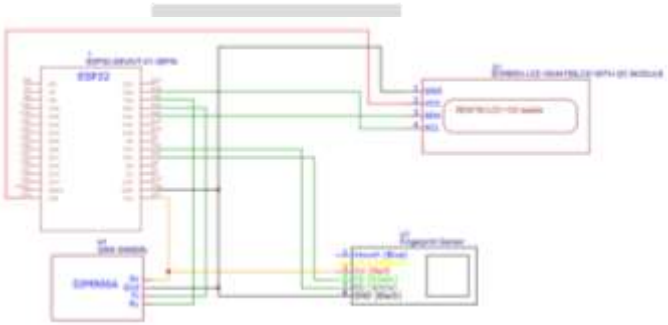

**Fig 3: Circuit Diagramof Vote Verify**

## VII. Performance Analysis

Vote Verify system is highly secure and very efficient in verifying voters during the voting process. The system makes use of biometric fingerprint verification as well as real SMS-based authentication of voters in real-time to keep the fraudulent attempts to vote low while allowing registered voters to vote.

The fingerprint identification module works with great accuracy at low false acceptance and rejection rates, providing sound voter authentication. The ESP32 microcontroller immediately carries out the authentications so that there is minimum lag between scanning and verifying the fingerprints. With the inclusion of an LCD screen, user interaction would be better as feedback would be live like for example, the name of the voter, in cases where the SMS might delay coming for manual verification if required. The GSM SIM800L module is an important second level of security as it ensures that SMS confirmations are sent live to the registered mobile numbers to add to the openness of the authentication process.

The system can also run efficiently with the use of UPS to ensure that there is no interruption of voter authentication during power cuts. Vote Verify has proven to be efficient in ushering in the verification of voters with low danger of impersonation that is other forms of attachment. Additions could be possible which could add to its ability of multiple level verification, high-level encryption for information protection and interface with facial recognition technology to solidify the reliability of authentication. Where this work would assist in scaling it with sufficient capability to enable it to serve larger scales of elections and incorporation with blockchain-based voter registry management will make it additional secure and transparent. With these improvements, Vote Verify would stand tall as a strongly robust scalable solution for contemporary electoral verification that absolutely assures equitable and transparent democratic exercises.

## VIII. RESULT

Vote Verify successful implementation and testing to honestly ensure voter authentication and prevent electoral fraud. The system only accepted registered voters, and their biometric fingerprint authentications could not allow any other voting. The success thereof boosted transparency and accountability through the automatic SMS confirmation sent to the voter's registered mobile number. The system was able to logically prevent unauthorized voting because unregistered fingerprints were denied entry into the system; thus, only genuine voters could have been allowed to cast votes. The inclusion of an LCD display gave real-time feedback to notify the system operator of the voter's name in the event of SMS delays and thereby enhanced any verification. The Vote Verify system, with the integration of an ESP32 microcontroller and GSM SIM800L module, enabled its efficient data processing, real-time authentication, and easy voter tracking. The system was reliable, scalable, and user-friendly, making it a very realizable solution for electoral authentication. Being able to conduct a secure and transparent electoral process, Vote Verify has bright prospects of supporting large-scale elections, hence reinforcing trust and efficiency in the electoral process.

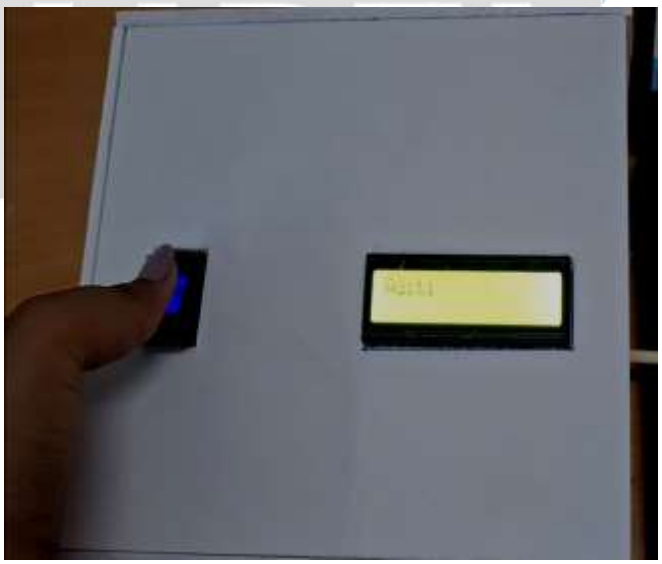

**Fig 4: Final Output**

## IX. CONCLUSION

Our system, called Vote Verify, integrates biometric fingerprint verification and real-time SMS authentication, presenting a modern and efficient means of assuring electoral integrity. Most conventional manual voting identification methods suffer from various risks and vulnerabilities; Vote Verify significantly lessens the opportunities for most varieties of electoral fraud and vote impersonation. The LCD panel system further trumps Transparency Legislation through the real-time view of candidates in case of SMS delays, with absolute checks-and-balances given attention to our process. Simplicity, yet expansion to Vote Verify, adds a secure and convenient forward mechanism to guard the credibility of an election that could keep updating until the announced results. Such features as AI-backed detection of fraudulent activities ignited in the future in association with the use of high-level encryption algorithms and coupled with advanced database management tools could transform Vote Verify into one of the very crucial integrant for modern elections. Vote Verify has direct attendance and foresight that serves to make certain the credibility of democratic workings to answer the ever-pressing need for safe and fair voting.

## X. Future Scope

Vote Verify is presumed to provide additional security against impersonation threats through the inclusion of fingerprint and facial recognition scans. Blockchain technologies have very much to contribute within the transparency framework to provide an immutable digital register of all accredited voters that can never be altered without authorization, this ensures the establishment of public trust in the election outcome.

Nevertheless, there is constant monitoring of voters' actions by AI to identify irregularities and to alert the appropriate electoral authority to security fallout. Development of a cloud-based voter authentication system can empower continuous supervision and control from the election officer's side over voters' files with remote real-time access. This equally contributes to better access for rural or remote voters and turns out to be a greater run-out. VanEvery's scalability would be the step to follow, not only for mega contests at the national level, but also for corporate boards and local elections. This system can further include voice recognition, and a behavioral pattern analysis of citizens based on their voices and previous voting records.

## References

[1] M. Odden, "Biometric crisis: Legal challenges to biometric identification initiatives," SearchSecurity, [Online]. Available: https://searchsecurity.techtarget.com/definition/biometrics. Accessed: Mar. 10, 2025.
[2] M. Smith and S. Miller, "The ethical application of biometric facial recognition technology," AI Soc., vol. 37, no. 1, pp. 167–175, Mar. 2022, doi: 10.1007/s00146-021-01199-9.
[3] L. H. Adamu and M. G. Taura, "Embryogenesis and applications of fingerprints: A review," Int. J. Hum. Anat., vol. 1, no. 1, pp. 1–8, Jan. 2017, doi: 10.14302/issn.2577-2279.ijha-17-1539.
[4] W. Zafar, T. Ahmad, and M. Hassan, "Minutiae-based fingerprint matching techniques," in Proc. 17th IEEE Int. Multi-Topic Conf., 2014, pp. 411–416. [Online]. Available: https://api.semanticscholar.org/CorpusID:27847944.
[5] A. C. S. Sheela and G. F. Ramya, "E-voting system using homomorphic encryption technique," J. Phys. Conf. Ser., vol. 1770, no. 1, Apr. 2021, doi: 10.1088/1742-6596/1770/1/012011.
[6] J. Liu, T. Han, M. Tan, B. Tang, W. Hu, and Y. Yu, "A publicly verifiable e-voting system based on biometrics," Cryptography, vol. 7, no. 4, 2023, doi: 10.3390/cryptography7040062.
[7] N. B. Kintu, "A secure e-voting system using biometric fingerprint and cryptwatermark methodology," [Online]. Available: https://www.researchgate.net/publication/329116213. Accessed: Mar. 10, 2025.
[8] M. Hajian Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl, "Blockchain-based e-voting systems: A technology review," Electronics (Basel), vol. 13, no. 1, p. 17, Dec. 2023, doi: 10.3390/electronics13010017.
[9] M. Nalayini, K. Vishnupriya, A. Dhivyabharathi, and H. Yuvapriya, "Biometric-based mobile voting application," J. Inf. Technol. Digit. World, vol. 5, no. 2, pp. 159–168, Jun. 2023, doi: 10.36548/jitdw.2023.2.006.
[10] Z. Acemyan, P. Kortum, and F. L. Oswald, "The trust in voting systems (TVS) measure," Int. J. Technol. Hum. Interact., vol. 18, no. 1, 2022, doi: 10.4018/IJTHI.293196.
[11] L. Miltgen, A. Popovič, and T. Oliveira, "Determinants of end-user acceptance of biometrics: Integrating the 'big 3' of technology acceptance with privacy context," Decis. Support Syst., vol. 56, no. 1, pp. 103–114, Dec. 2013, doi: 10.1016/j.dss.2013.05.010.
[12] M. Kumar, "Fingerprint recognition system: Issues and challenges," Int. J. Res. Appl. Sci. Eng. Technol., vol. 6, no. 2, pp. 556–561, Feb. 2018, doi: 10.22214/ijraset.2018.2080.
[13] S. Zhao, D. Ge, J. Zhao, and W. Xiang, "Fingerprint pre-processing and feature engineering to enhance agricultural products categorization," Future Gener. Comput. Syst., vol. 125, pp. 944–948, 2021, doi: 10.1016/j.future.2021.07.005.
[14] T. Keerthi, M. C. Chinnaiah, A. Kumari, P. Asharani, D. Harikrishna, and G. Divyavani, "Real-time implementation of biometric-based EVM system for distinct verification," Procedia Comput. Sci., vol. 230, pp. 407–416, 2023, doi: 10.1016/j.procs.2023.12.096.
[15] R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo and M. A. Rahman, "Biometrically secured electronic voting machine," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh, 2017, pp. 510-512, doi: 10.1109/R10-HTC.2017.8289010.
[16] G. Deepa et al., "Biometric Based Voting System Using Aadhar Database," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2022, pp. 1071-1075, doi: 10.1109/ICAIS53314.2022.9743138.