IOT-Based Electronic Voting System with Live Web-Based Result Monitoring

Onkar Dadasaheb Sarade[1] ,Atharv Abasaheb Sutar[2] ,Ketan Kashinath Zore[3] ,Omkar Santosh Erande[4] , Mrs.Punam V. Chavan[5]
[1,2,3,4,5] *Matathwada Mitra Mandal's College Of Enginnering* Pune ,India

***Abstract*—The voting system must ensure the voters trust in fairness and transparency of the process and in the correctness and reliability of the results. In the case of customary or simple electronic voting machines (EVMs), voters may be impersonated, or ballots tampered with, counting mistakes made or results delayed. This paper presents a biometric fingerprint-based secure electronic voting system which utilizes Internet of Things (IoT) technology to enable the monitoring of the voting process as well as displaying the voting outcome in real-time based on the fingerprint recognition to identify the voter. The encrypted data of the voter selections is sent to central servers through IoT communication modules, and a web dashboard is created for displaying the voting statistics and results. Experimental results show that the proposed scheme improves accuracy and reduces the result processing time, while improving transparency. The system has been applied to elections for institutions and organizations to improve scalability and security.**

***Index Terms*—IoT, Electronic Voting Machine, Biometric Authentication, Arduino, Web Monitoring, Real-Time Voting.**

I. INTRODUCTION

Voting is a process for democratic decision-making. People were previously required to mark paper ballots, which can be misread and must then be counted. Electronic voting machines are used to make this process more efficient. However, these machines can be subject to voter impersonation, duplicate voting, and a lack of transparency [1],[2].

Due to the uniqueness and permanence of fingerprint patterns, biometric authentication offers a dependable mechanism for identifying a voter. Fingerprint-based voting systems have been proven to improve data authenticity and prevent fraudulent entry [3], [6]. Voting systems can access centralized servers to securely transmit vote data over the network using IoT technology, allowing for real-time monitoring and faster result analysis.

The researcher aims to develop the following in this research:

- To develop a biometric-based secure electronic voting system
- To enable the transmission of votes on real-time using IoT technique.
- To implement a web-based dashboard for live monitoring.
- To improve transparency and reduce human errors.

II. RELATED WORK

Electronic voting systems can be applied to improve the security and performance of elections: the first electronic voting machines were used to reduce the number of human errors in vote counting [2]. By this time, systems based on biometrics began to appear.

Anandaraj et al. proposed a secure electronic voting machine using fingerprint authentication to prevent unauthorized people from voting [1]. Ahmed et al. improved the system using biometric verification techniques [3]. Kale et al. and Satyanarayana et al. also explored biometric voting systems integrated with databases to improve the accuracy of authentication [6][9].

IoT can be used with voting machines to improve visibility and control. Arduino-based voting machines, created by Murali Prasad et al., improve the efficiency of the automated voting process [4]. Holkar and Marab proposed a real-time monitoring system based on IoT that can detect any malfunction [5]. Wibowo and Ujianto proposed an IoT-based biometric voting

system for elections in institutions [7]. Gurav et al. proposed secure vote transmission based on IoT communication modules [8].

Despite advancements, real-time result visualization is still relatively scarce. The proposed system leverages biometric authentication, IoT communication, and a web-based monitoring dashboard all within a single platform.

.

III. PROPOSED SYSTEM AND METHODOLOGY

In this system, biometric device, embedded processing to authenticate the identity and process of voting it coupled with IoT based machine to machine (devices) communication with web monitoring that maintain a secure EVM. It allows for reliable authentication of voters and secure voting and election result monitoring.

A. System Architecture

The architecture of the voting system under consideration is composed of different modules which are linked together in order to perform authentication, vote processing and data transfer.

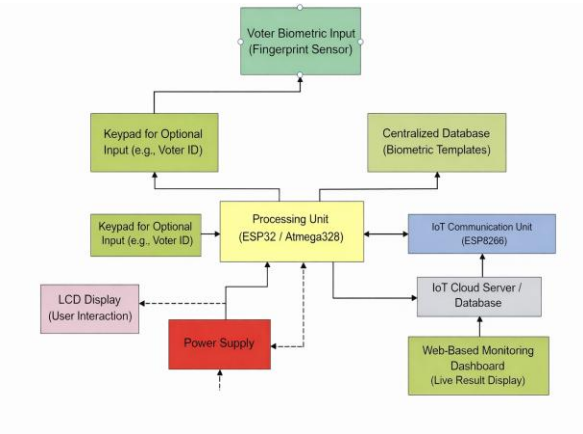

Fig. 1. Hardware block diagram of the proposed voting system.

1. Power Supply Unit: The power supply module provides stable and regulated voltage to all hardware components. It includes a step-down transformer, rectifier circuit, filtering capacitor, and voltage regulator. This module ensures uninterrupted operation of the voting machine and protects electronic components from voltage fluctuations.
2. Biometric Unit (Fingerprint Sensor): It includes providing a fingerprint authentication using a sensor like R305 module or sensor. Deregistration and Registration process Fingerprint templates are then securely saved in the systems database during voter registration. During the enrollment phase, fingerprint image is captured by the sensor and during the voting phase, user places his finger on the sensor and then compares it with already stored templates using pattern matching algorithm.

   This module also authenticates voters and blocks non-authorized users from entering the voting interface. It also does away with physical Voter Identification Cards and thus minimises the reliance on manual verification.
3. Processing Unit (E-Voting Control): It is the processing unit of the system, which is made up of an ATmega328 microcontroller. It handles authentication, result manipulation, can display candidate lists to voters, stores vote selection and is responsible for communication between the various components. The microcontroller is chosen for its low power consumption, high performance and high compatibility with IoT communication module.
4. IoT and Communication Unit: The wireless Communication using IoT section includes the ESP8266 Wi-Fi module performing a communication between the voting machine and central server wirelessly. Once a vote is submitted, an encrypted vote data portion is securely communicated to the server. The server updates the database on-the-fly, and web dashboard auto-refreshes to show you real-time voting results and system up time status.
5. Monitoring System: A central server and local device,

e.g. an Android phone, control the system in real-time. The Android app communicates with the server (which is typically set up on a device such as a Raspberry Pi) over the internet using a secure authorization code, thereby enabling centralized and remote monitoring of all EVM-related activities.

A web-based monitoring interface is also coupled with the central server, in addition to tangential hardware modules. The server automatically refreshes voting results once a vote is sent and the

web page features live statistics updates with graphical percentage results. It allows the authorized user to observe election processes from a remote location without making direct contact with voting hardware.

B. Operational Flow

The voting process is executed sequentially to ensure maximum control and prevent fraud.

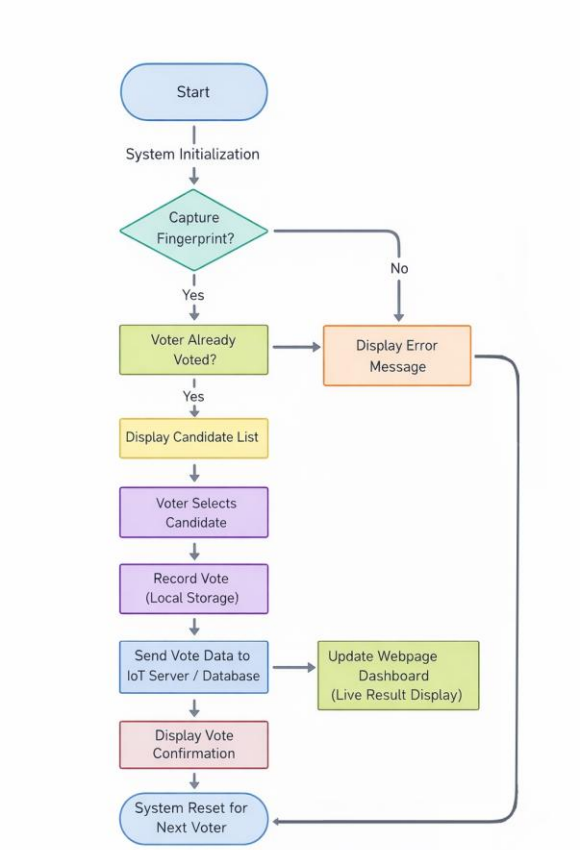

Fig. 2. Operational flow of the biometric IoT voting system.

1. Initialization and Connection: It starts with the initialization of Wi-Fi module (e.g., ESP266) then connects to central IoT server.
2. Biometric Authentication: The voter puts his finger on sensor. The system will initialize the fingerprint sensor and try detecting the Fingerprint ID, then match it against storage. If the ID matches and the voter hasn't voted (from central record) - authentication was successful.
3. Voter Detail Retrieval: After the person is identified that individual by fingerprint then the system will retrieve area-based user detail. The names of candidates for that particular constituency would then be shown on the monitor.
4. Vote Casting: The voter participates in a voting session by clicking an option, often with a mouse or via button press on the display instance.
5. Real-Time Transmission and Storage: Upon the vote's insertion, data is stored locally and sent to central server at same time. The database then is updated by the server and the live web page updates in real time to reflect voting result stats.
6. Confirmation and Display: After the vote is taken successfully and sent to the central server, confirmation information is displayed on the voting interface for voter that their vote has been securely recevied. The transparent display has a "kleenex factor" for the voter in understanding that indeed their vote was successfully cast.

IV. RESULTS AND DISCUSSION

To evaluate system performance, reliability and real-time monitoring, the proposed IoT-based biometric electronic voting system was implemented in the laboratory and tested. The system was observed to provide accurate voter authentication via fingerprint recognition and denial of unauthorized or double voting. The authentication process was reported to be stable, and fingerprint matching was found to be fast.

This processing unit correctly recorded the votes and allowed each authenticated voter to vote once and only once, and the vote data was sent to the central computing server through an IoT communication module, with a very small packet loss and communication failures. The average time taken for a transmission was well within what was acceptable for monitoring.

One of the system's design features was the web-based monitoring dashboard which showed real time vote totals after they were transmitted to the server. The dashboard continuously updated and did not require a manual refresh to display the latest totals. This allowed election authorities to monitor the number of ballots cast at any time, and to increase transparency.

It was also faster, removing the requirement to manually count the votes and deliver results much earlier with automatic vote total entries, and was easier to read/analyse on page as well.

To summarize, the experiments in this paper demonstrate that our proposed system is applicable to secure authentication, voting and counting. Biometric verification coupled with IoT communication and live web display, makes it ideal for institutional as well as small-scale election settings.

V. SYSTEM PERFORMANCE AND BIOMETRIC METRICS

The performance of the proposed biometric e-voting system using IoT was analysed in terms of authentication accuracy, communication delay, processing efficiency and the real time-monitoring. The assessment was conducted in a laboratory environment to examine the dependability of biometric authentication and stability of IoT based data transmission while continuously operating voting.

The performance of the fingerprint acquisition system on voter authentication was stable with low error rates. The average fingerprint search time was about 1.8sec at 1:N-matching in a database of 1,000 voters (registered people) for smooth voter flow without any delay. The adopted authentication deployment successfully avoided unauthorized access and duplicate voting.

The communication performance of the IoT was evaluated in terms of latency, which is calculated for data transmission time from the processing unit to the main cloud server. The average transmission delay was 350ms (acceptable for real-time synchronization between voting unit and monitoring system). As soon as the successful voting had been transmitted, newsroom reporters were instantly able to see live vote standings and trends directly on a web-based dashboard that updated in real time without requiring any manual refresh. This highlights the robustness of webpage-based live monitoring done in the proposed system.

The system throughput was measured by counting voters processed per hour including authentication and voting duration. The resulting system was able to process around 28 voters per hour, in optimal conditions. The automated process of authentication, voting and result posting on the web-based system significantly saved manual labour required in printing ballots, stuffing ballot boxes, counting votes manually and increased the overall efficiency as compared with traditional voting methods.

.

Table I. System Performance and Biometric Metrics

Parameter	Value	Unit	Significance
Fingerprint Matching Time	1.8	s	Verification time
IoT Data Transmission Latency	350	ms	Network delay
False Acceptance Rate (FAR)	0.001	%	Unauthorized acceptance probability
False Rejection Rate (FRR)	1.2	%	Valid voter rejection probability
Throughput	28	voters/hour	Processing efficiency
Memory per Vote	128	bytes	Storage requirement
Dashboard Refresh Time	1.5	s	Update delay

A. Graph 1: System Throughput Comparison (Bar Chart)

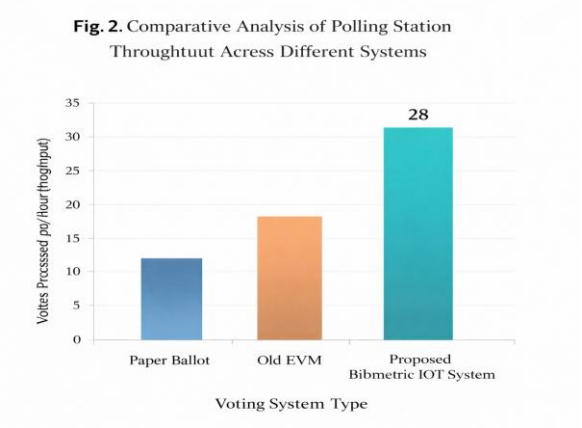

Fig. 3. Comparative analysis of voter throughput across different voting systems

The throughput evaluation for the traditional voting and for the Secured IoT-based biometric voting is plotted in Fig. 3. The number of voters being processed in an hour time each for paper ballot system, e-voting machine and proposed scheme has been compared using Fig. The results show

enhancement in the efficiency of the system with automated authentication, and live result on browser (IoT communication) & webpage based monitoring.

B. Graph 2: Biometric Performance (ROC Curve or FAR vs. FRR Plot)

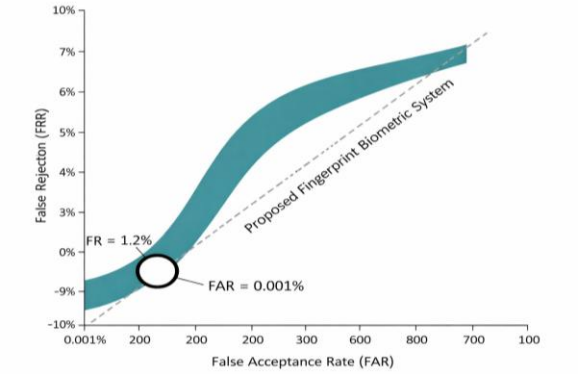

Fig. 4. ROC curve of fingerprint authentication performance.

Biometric performance of the fingerprint authentication module is plotted using a Receiver Operating Characteristic (ROC) curve in Fig. 4, the graph represents false acceptance rate (FAR) against false rejection rate (FRR), showing the trade-off between system security and ease of use. The working point (0.001% FAR and 1.2% FRR) shows a robust authentication performance which is adequate for secure voting applications.

C. Graph 3: IoT Latency Distribution

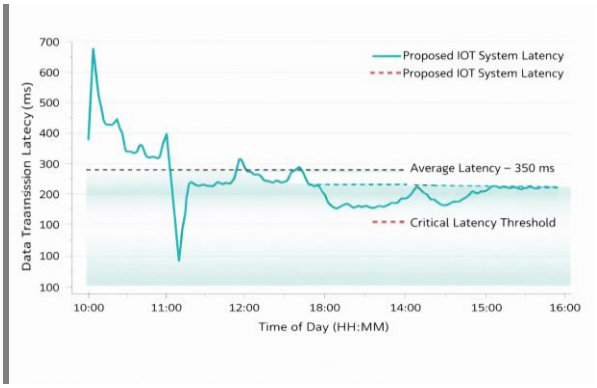

Fig. 5. IoT data transmission latency analysis.

The robustness of the IoT communication is shown in Fig. 5 through latency distribution analysis. The figure shows the delay of communication for three moments in time during the system s tests. The data show average latencies of nearly 350ms, which shows that the communication between the voting unit and cloud server is reliable. This stability allows for continuous live updates on the web-based dashboard and enables reliable real-time election monitoring."]

VI. CONCLUSION AND FUTURE WORK

In this paper, we have developed an IoT based electronic voting system employing biometric fingerprint verification in order to enhance the integrity and transparency of e-voting process. The system authenticates the voter using fingerprint recognition before allowing the vote to be cast, preventing unauthorized access and multiple voting. With the IoT communication integration, votes can be sent directly to a server hosted at a central location and will reflect on the web dashboard automatically.

Stability of testing system in the process of use, it can be seen that the system is stable in both authentication time, data transmission and live result. Web-based monitoring made it possible to see the results of voting as they poured in and decrease manual counting and increase productivity. The suggested system can be successfully applied to the institutional or small-scale election conditions which requires secure and legitimate overseeing.

.In future work, the system could be enriched by other biometric methods (like face or iris recognition) for a reliable authentication. Security measures may also be improved by encryption, or storage according to the block chain for more reliable integrity of data. In the future, this may involve having support for remote voting and better scalability to accommodate more voters.

1. Inclusion of other Biometric Modalities: The security control in the current work is only based on Fingerprint, but for future enhancement other biometric techniques such as finger vein recognition, facial or iris based comparison and voice detection can be added for identification of users. This multimodal biometric system would step up security and make such voter authentication much more secure and flexible in

various situations.

2. Mobile Voting and Remote Access: With the rise of smartphone usage, officials can also consider extending the system to mobile voting applications that cater for secure voting from remote locations or even overseas. The implementation of secure mobile platforms would simplify the process to vote for people that are unable to be present in polling stations (due to geographical, health or other reasons).
3. Blockchain and Data Integrity: In order to improve transparency and security, we may incorporate blockchain with the voting system. The distributed, independent nature of a blockchain means votes could be input onto the chain and there they would stay, reducing the potential for tampering, fraud or loss.
4. AI for Voter Assistance: There is also a possibility of a future when AI-based chatbots or voice assistants might be able to help voters understand how voting works. This will increase access for our elderly, disabled and low literate eligible citizens to participate in elections.
5. GLOBAL USAGE: The existing system can be used for many forms of election process, but we also see a future application that scales the technology to global elections - accommodating integration with millions of voters as well as exceptional security and speed. This could make it suitable for international bodies, nationwide referendum, or electoral events in countries with a high population.
6. Integration with Government Systems: system can be integrated with national identity databases and other government systems, to attain voter enrollment and verification. That way the only people who would vote would be those registered to vote and you could, potentially streamline the voting by eliminating both registration and authentication steps for each person."
7. Increased Privacy: Development of more advanced privacy protocols, including cryptography and blockchain-based methods could be a useful addition in order to provide blanket protection for voters' private information, ensuring that the system is GDPR compliant and aligns with similar data protection legislation both nationally and internationally.

VII. ACKNOWLEDGMENT

The authors express their sincere gratitude to the Department of Information Technology, Marathwada Mitra Mandal's College of Engineering, Pune, for their guidance and support throughout this work.

REFERENCES

[1] S. Anandaraj, R. Anish, and P. V. Devakumar, "Secured electronic voting machine using biometric," Proc. ICIIECS, IEEE, 2015.

[2] D. Ashok Kumar and T. Ummal Sariba Begum, "Electronic voting machine," IEEE Conference, 2012.

[3] H. Ahmed et al., "Biometrically secured electronic voting machine," IEEE R10-HTC, 2017.

[4] R. Murali Prasad et al., "AADHAR based electronic voting machine using Arduino," IJCA, vol. 145, no. 12, 2016.

[5] A. L. Holkar and P. R. Marab, "IoT-Based Real-Time Security and Malfunction Detection in Electronic Voting Machines."

[6] K. Kale et al., "Biometric Based Electronic Voting Machine."

[7] Wibowo and Ujianto, "IoT-Based E-Voting System Using Fingerprint Biometrics for School Elections."

[8] S. Gurav et al., "Fingerprint Based Voting System Using IoT."

[9] M. Satyanarayana et al., "Biometric-Based Electronic Voting System."

[10] IEEE, Proceedings of ICIIECS, 2015