JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SECURE BIOMETRIC VOTING SYSTEM USING FINGERPRINT AUTHENTICATION WITH OTP VERIFICATION AND CLOUD DATA STORAGE

1. Hemanth LM Student
Department of ECE
KSIT BENGALURU,INDIA

2. Nishank BC
Student Department of ECE
KSIT BENGALURU,INDIA

3. Puneeth G Student
Department of ECE
KSIT BENGALURU,INDIA

4. Shashank. Student
Department of ECE
KSIT BENGALURU,INDIA

5. Dr. Devika B
Associate professor Department of ECE KSIT BENGALURU,INDIA

ABSTRACT- **The Secure Biometric Voting System is designed to provide a reliable, secure, and efficient method of conducting elections by integrating fingerprint authentication with cloud-based data storage. Traditional voting systems may face challenges such as impersonation, duplicate voting, unauthorized access, and inefficient management of voting records. The proposed system addresses these issues by using the unique fingerprint characteristics of each registered voter to verify their identity before allowing them to cast a vote. This biometric-based authentication helps ensure that only eligible and registered voters can participate in the election.**

Keywords – Biometric Authentication, Fingerprint Recognition, Secure Electronic Voting System, OTP Verification, Cloud Computing, Cloud Data Storage,

I. INTRODUCTION

Electronic Voting Machines (EVMs) are widely used to conduct elections in a fast and efficient manner. However, conventional voting systems may face security challenges such as identity fraud, unauthorized access, and duplicate voting. To overcome these limitations, the proposed Secure Biometric Voting System uses fingerprint authentication to provide reliable and unique voter identification. Since fingerprints are unique to each individual, biometric authentication helps ensure that only registered and eligible voters are allowed to participate in the election.

The proposed system introduces a secure multi-factor authentication mechanism that combines fingerprint verification with voter credentials to strengthen the voting process. During voter registration, the required voter information and biometric details are securely stored. At the time of voting, the voter's fingerprint is scanned and matched with the registered information. After successful authentication, the voter is permitted to cast a vote, while the system prevents unauthorized users and duplicate voting attempts.

The system also integrates cloud storage for secure and centralized management of voter and election data. Cloud technology enables efficient storage, monitoring, and retrieval of information while supporting secure access to election records. Security mechanisms such as authentication, access control, encryption, and secure data transmission can be used to protect sensitive voter information and voting records from unauthorized access or modification.

Overall, the Secure Biometric Voting System aims to provide a highly secure, transparent, reliable, and efficient approach to electronic voting. By combining fingerprint authentication, multi-factor security, and cloud-based data storage, the system reduces the risk of identity fraud and duplicate voting while improving the management of election data. The proposed solution demonstrates the potential of biometric and cloud technologies in developing a modern and trustworthy voting system.

II. LITERATURE PAPER

[1] Tarun Kancherla proposed a *Fingerprint-Based Voting System Using C#* in 2025, which focuses on improving the security and reliability of the electronic voting process through biometric authentication. The proposed system uses fingerprint authentication along with a C# application and an SQL database to uniquely identify voters and prevent voter impersonation. By verifying the fingerprint of each voter, the system ensures that only authorized individuals can participate in the election. The SQL database is used to store and manage voter information securely, while the application handles the authentication process. This approach can make the voting process more secure and reduce the possibility of fraudulent voting. However, the system requires proper database management and strong security measures to protect sensitive biometric information.

[2] Pranav Poduval, Shripad Raut, and Sayali Raut proposed an *Advanced Electronic Voting System* in 2025 that uses biometric authentication to improve the security of electronic voting. The system combines biometric verification with a digital database to authenticate voters before allowing them to cast their votes. The database is used for securely storing and managing voter information and can also support monitoring of the voting process. The use of biometric authentication helps reduce unauthorized access and voter impersonation during elections. The proposed system aims to provide a secure and efficient method for conducting electronic elections. However, the system requires strong cybersecurity measures to protect voter information and also depends on effective management of the voter database.

[3] T. Haripriya, Vidmukumar B.G., Mahesh Babu, and
G. Aswini presented a *Biometric System Based Electronic Voting Machine* in 2024. The proposed system uses a fingerprint sensor integrated with a microcontroller to authenticate voters before they are allowed to cast their votes. The fingerprint of the voter is captured and verified to ensure that the person is an authorized voter. This biometric-based approach helps prevent unauthorized voting and reduces the possibility of voter impersonation. The integration of the fingerprint sensor with the electronic voting machine provides an additional layer of security compared with conventional voting methods.

[4] M. Satyanarayana, Rajiv Pranam T., Sai Charan Reddy, and Sai Srinivas proposed a *Biometric Based Electronic Voting System* in 2023. The system uses fingerprint recognition to authenticate voters before they participate in the election. An SQLite database is used

o store voter information and manage vote-related data securely. Fingerprint verification ensures that only registered and authorized voters can access the voting system. The proposed approach aims to improve election security by reducing unauthorized voting and voter impersonation. However, the system requires secure database management and reliable biometric matching for accurate voter authentication.

[5] Kamlesh Kale, SrinwasShirure, Sushant Kachbawar proposed a *Biometric Based Electronic Voting Machine* in 2022. The system uses a fingerprint sensor connected to an Arduino microcontroller to authenticate voters before allowing them to cast their votes. The fingerprint of the voter is verified to ensure that only registered voters can participate in the election. The Arduino-based implementation provides a relatively simple approach for integrating biometric authentication with an electronic voting machine. This method can help reduce unauthorized voting and improve the security of the voting process. However, the performance of the system depends on the reliability of the hardware and the accuracy of the fingerprint sensor.

[6] Suraj H P, Skanda G, Shobith G B, and Srikanth P S proposed an *Arduino Based Smart Remote Voting System* in 2022. The system uses an IoT-based architecture with dual biometric authentication to verify voters. It combines fingerprint recognition and face recognition to provide multiple levels of voter authentication. The use of IoT technology enables the system to support remote voting and communication between different components. Dual biometric verification can help improve the identification of registered voters and reduce unauthorized access. However, the system requires continuous internet connectivity and involves a comparatively complex system setup for implementation.

[7] Madhuri Namballa, Tejasree Kaka, and Mendu Vaishnavi proposed a *Realtime Fingerprint Based Voting System* in 2020. The system uses fingerprint authentication along with an embedded controller to allow only registered voters to participate in the election. Before voting, the fingerprint of the voter is checked against the registered biometric information stored in the system. This approach helps prevent unauthorized voters from accessing the voting process and improves voter identification.

[8] B. Hyvallika and Dr. Kirupa Ganapathy presented a *Survey of Secured Voting System Using Fingerprint Scanner* in 2020. The study discusses the use of biometric fingerprint systems for preventing fraudulent voting and improving the security of elections. It explains how fingerprint authentication can be used to verify the identity of voters before they are permitted to vote.

The survey focuses on different concepts and approaches related to biometric-based voting systems. It highlights the potential of fingerprint technology to provide secure and reliable voter authentication. However, the study mainly focuses on conceptual analysis and does not provide a detailed practical implementation of the proposed system..

[9] Marwa Adeeb Al-Jawahery developed an *Arduino Based Electronic Voting Machine* in 2019. The system uses an Arduino Mega and an LCD display along with fingerprint authentication to verify voters. The fingerprint-based mechanism allows only authenticated voters to participate in the election. However, the system is mainly limited to small prototype-based implementations.

[10] Shahram Najam Syed, Aamir Zeb Shaikh, and Shabbar Naqvi proposed a *Hybrid Biometric Electronic Voting System* in 2018. The system uses both fingerprint and facial recognition algorithms for voter authentication. Combining two biometric methods provides multiple levels of identity verification during the voting process. However, it requires high computational power

and involves complex biometric processing

[11] N. K. Ratha, J. H. Connell, and R. M. Bolle presented a study on *Enhancing Security and Privacy in Biometric-Based Authentication Systems* in 2001. The work focuses on biometric authentication techniques with improved security and privacy mechanisms. It discusses methods for protecting biometric information and strengthening authentication systems.

[12] A. Juels and M. Sudan proposed *A Fuzzy Vault Scheme* in 2002. The scheme uses cryptographic techniques to securely protect biometric templates such as fingerprints. It provides a method for storing biometric information while improving its security against unauthorized access. The technique can be useful for protecting sensitive biometric data in authentication systems. However, its implementation is complex and involves challenges related to cryptographic key management.

[13] D.Chaum proposed proposedA Fuzzy Vault Scheme in 2004. The scheme uses cryptographic techniques to securely protect biometric templates such as fingerprints. It provides a method for storing biometric information while improving its security against unauthorized access. The technique can be useful for protecting sensitive biometric data in authentication systems. However, its implementation is complex and involves challenges related to cryptographic key management.

[14] T. Kohno, A. Stubblefield, A. Rubin, and D. Wallach presented an *Analysis of an Electronic Voting System* in 2004. The study focuses on security analysis of electronic voting systems and identifies various potential vulnerabilities. It examines the security aspects of electronic voting technologies and highlights possible weaknesses. However, the work mainly focuses on analysis rather than providing a practical implementation.

[15] R. Mercuri presented *A Better Ballot Box?* in 2002, discussing improvements in electronic voting systems and their security aspects. The study examines different approaches for making electronic voting more reliable and secure. It emphasizes the importance of security and transparency in electronic elections. However, the work provides limited practical implementation details.

[16] S. Madan and S. Kumar proposed a *Cloud-Based Secure E-Voting System Using Encryption Techniques* in 2018. The system uses cloud storage along with encryption techniques to securely store voting-related information. Encryption helps protect sensitive election data from unauthorized access. However, the system depends on reliable network connectivity and the security of the cloud infrastructure.

[17] P. Y. A. Ryan and S. A. Schneider proposed *Prêt à Voter with Paillier Encryption* in 2008. The approach uses cryptographic encryption techniques to provide secure and anonymous electronic voting. Paillier encryption helps protect the confidentiality of votes while supporting secure election procedures. However, the system involves complex cryptographic implementation, which can make practical deployment more challenging.

[18] F. Hao, P. Y. A. Ryan, and P. Zielinski proposed Anonymous Voting by Two-Round Public Discussion in 2010. The system uses anonymous voting protocols to support secure electronic elections while protecting voter identity. The two-round communication process helps provide anonymity and security during voting. However, the approach requires multiple communication rounds and involves relatively high implementation complexity.

[19] S. Srinivasan, S. Ranganathan, and S. Venkatesan proposed *Biometric Authentication in Cloud Computing* in 2012. The study integrates biometric authentication with cloud-based systems to provide secure access to users. Biometric techniques help verify user identities before allowing access to cloud resources.

However, the security of the system depends heavily on the reliability and protection of the cloud infrastructure.

[20] A. K. Jain and K. Nandakumar presented *Biometric Authentication: System Security and User Privacy* in 2012. The study discusses biometric authentication systems with particular attention to security and user privacy. It examines the challenges involved in protecting biometric information and maintaining secure authentication. However, privacy concerns and effective protection of sensitive biometric data remain important challenges.

III . PROBLEM IDENTIFICATION

The existing voting process faces several challenges related to voter authentication and election security. One of the major concerns is the possibility of duplicate voting, where the same individual may attempt to vote more than once. Identity impersonation is another significant issue, as unauthorized individuals may attempt to vote using another person's identity. These problems can affect the accuracy and reliability of election results.

Another challenge is the lack of strong authentication methods in some existing voting systems. When voter verification depends mainly on traditional identification methods, there may be limitations in confirming the actual identity of the voter. Manual verification can also result in human errors, delays, and difficulties in handling a large number of voters efficiently. Therefore, a reliable biometric authentication method can provide an additional level of identity verification.

The absence of real-time monitoring of voting data is another limitation. Without effective monitoring mechanisms, it can be

difficult to track voting activities, identify unusual activities, and maintain updated election records. There is also a risk of data tampering or loss if voting information is not properly protected.

IV OBJECTIVES

The objective of this project is to design a secure biometric voting system that provides a safe, reliable, and efficient voting process. The system uses biometric authentication to verify the identity of voters before allowing them to cast their votes

It aims to reduce unauthorized access, duplicate voting, and identity impersonation. The system also focuses on protecting voting information and maintaining data integrity. Overall, the objective is to improve the security and reliability of the voting process through modern technology.

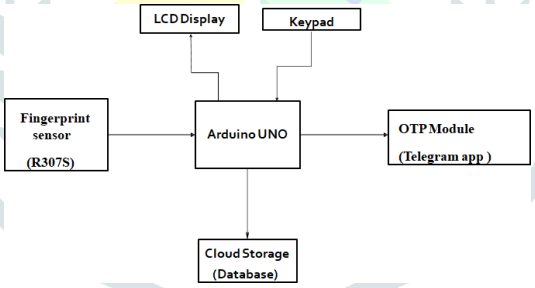
V METHODOLOGY

The raw power from the dynamo changes constantly because riding speed goes up and down. To make this energy usable, it first travels into a KBPC3510 bridge rectifier that converts the AC power into direct current (DC). Next, the power flows through a voltage booster circuit and an electrolytic capacitor. This step smooths out electrical ripples and boosts the voltage to a stable level so it does not spike and harm the electronics. The fingerprint sensor captures the voter's fingerprint and sends it to the microcontroller for verification.

The microcontroller compares the captured fingerprint with the registered fingerprint data to confirm the voter's identity. After successful fingerprint verification, an OTP is generated and sent to the registered mobile number through the GSM module. The voter then enters the received OTP using the keypad, and the system verifies the OTP.

If both fingerprint and OTP verification are successful, the voter is allowed to cast their vote. After the vote is submitted, the voting data is securely stored in local memory and cloud storage. This dual storage approach helps maintain reliable voting records and provides secure access to the stored data when require

VI BLOCK DIAGRAM



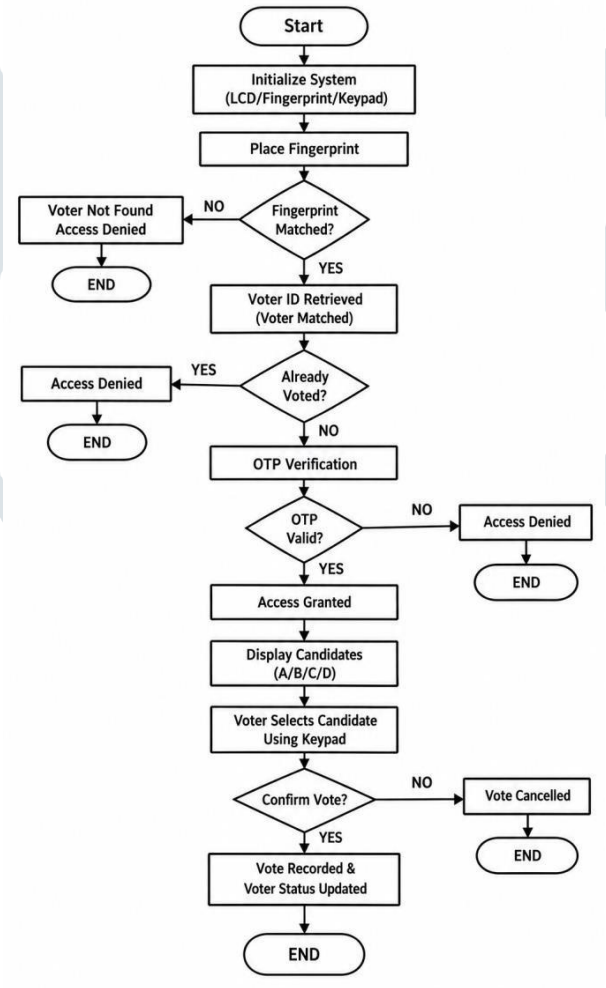
Arduino UNO (Main Controller): The Arduino UNO is the central processing unit of the system. It receives input from the fingerprint sensor and keypad, processes the information according to the programmed instructions, and controls the other modules. It verifies the user's identity and coordinates the OTP generation and verification process. It also communicates with the cloud storage database to manage relevant user information.

Fingerprint Sensor (R307S): The fingerprint sensor is used to identify and authenticate users through their fingerprints. When a user places a finger on the sensor, it captures the fingerprint and compares it with the registered fingerprint data. The sensor sends the result to the Arduino UNO for processing. If the fingerprint is valid, the system proceeds to the next authentication step, improving security by ensuring that only authorized users can continue.

Keypad and LCD Display: The keypad allows users to enter information, such as an OTP (One-Time Password), while the LCD display provides instructions and feedback. The Arduino UNO receives the keypad input and checks whether the entered information is correct. The LCD displays messages such as prompts to scan a fingerprint, enter an OTP, or indicate whether authentication was successful or unsuccessful. Together, these components provide a simple and user-friendly interface.

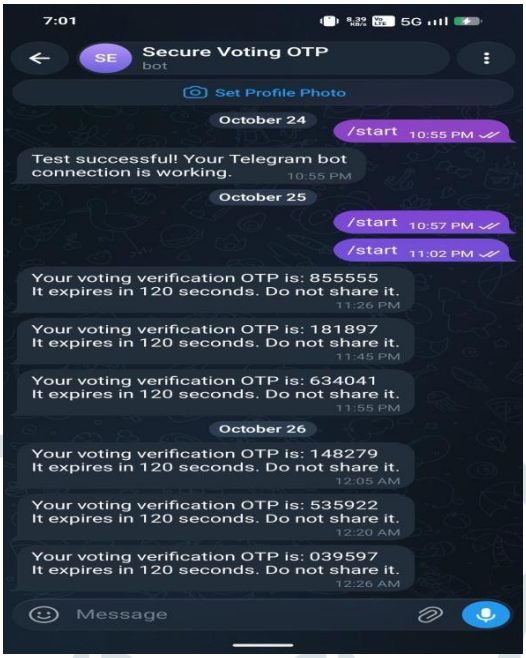
OTP Module (Telegram App): The OTP module provides an additional layer of security through a One-Time Password sent using a Telegram application. After successful fingerprint authentication, the system can generate or request an OTP and send it to the authorized user through Telegram. The user then enters the OTP using the keypad.

VII . FLOWCHART



• The flowchart begins with the start of the voting system. The system initializes the LCD display, fingerprint sensor, and keypad so that all the required components are ready for operation. The voter is then asked to place their finger on the fingerprint sensor for identity verification. This initial step ensures that the voting process begins only after the system is properly initialized.

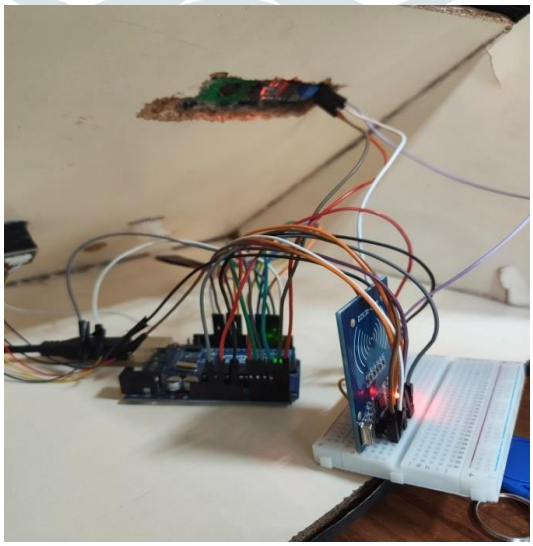
• After the fingerprint is scanned, the system checks whether it matches a registered fingerprint. If the fingerprint does not match, the voter is identified as not registered, access is denied, and the process ends. If the fingerprint matches, the corresponding voter ID is retrieved, confirming the voter's identity. The system then checks whether the voter has already cast their vote. If the voter has already voted, access is denied to prevent duplicate voting, and the process ends. Otherwise, the system proceeds to OTP verification.

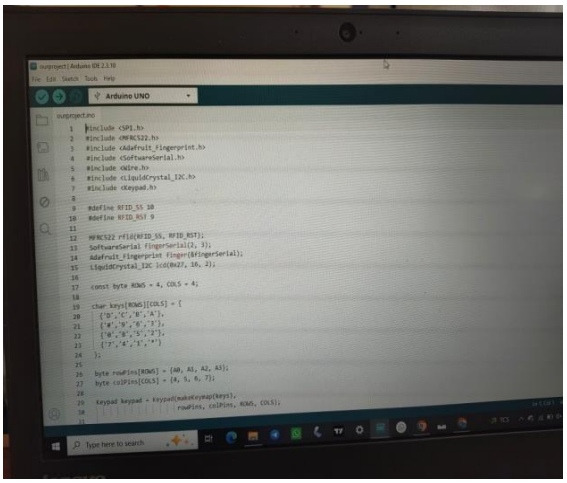


Once the voter passes fingerprint authentication and the system confirms that they have not voted previously, the OTP verification process begins. A One-Time Password (OTP) is sent to the authorized voter through the configured communication system, such as a Telegram application. The voter enters the OTP, and the system checks whether it is valid. If the OTP is incorrect or invalid, access is denied, and the process ends. If the OTP is valid, access is granted, allowing the voter to proceed to the candidate selection stage.

• After access is granted, the system displays the available candidates on the LCD, represented by options A, B, C, and D in the flowchart. The voter selects their preferred candidate using the keypad. The system then asks the voter to confirm their selection. If the voter chooses not to confirm, the vote is cancelled, and the process ends without recording the vote. If the voter confirms their selection, the system records the vote for the selected candidate and updates the voter's voting status to indicate that the vote has been cast.

VIII . RESULTS





.

VIII APPLICATIONS

1. GovernmentElections:Fingerprint-based voting systems can help verify voter identities and reduce the chances of duplicate voting. They can improve the security and efficiency of the election process.

2.College Elections:These systems can be used in college elections to authenticate students before they cast their votes. They help ensure that each eligible student votes only once.



3. Corporate Voting Systems:Corporate organizations can use secure voting systems for employee polls, internal elections, and decision-making. Biometric authentication helps verify the identity of participants.

4.Secure Digital Polling:Digital polling systems can use fingerprint authentication to verify voters before recording their votes. This helps improve access control and reduce unauthorized voting.

5.Remote Voting Systems:Remote voting systems can allow eligible voters to participate without physically visiting a polling station. Additional secure authentication and communication mechanisms are required to protect voter identity and ballot secrecy.

6.Smart Voting in Rural Areas:Smart voting systems can help simplify the voting process in rural areas. Portable devices and suitable connectivity can support voter verification and improve accessibility.

7.Online Voting Platforms (Future):Future online voting platforms may integrate biometric authentication and secure cloud technologies. These systems must also ensure ballot secrecy, data security, and election integrity.

CONCLUSION

The Secure Biometric Voting System Using Fingerprint Authentication with OTP Verification and Cloud Data Storage provides an efficient and secure approach to modernizing the traditional voting process. By integrating fingerprint authentication with One-Time Password (OTP) verification, the system adds multiple layers of security to verify voter identity and reduce the possibility of unauthorized access and duplicate voting. The use of cloud data storage enables centralized data management, easy access to voting records, and efficient storage and retrieval of election-related information. These features can help improve the accuracy, reliability, transparency, and convenience of the voting process.

In conclusion, this system demonstrates the potential of combining biometric technology, OTP-based authentication, and cloud computing to develop a more secure and user-friendly voting platform. It can reduce manual effort, minimize human errors, and improve the overall efficiency of election management.REFERENCE

[1] A. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[2] R. Das and K. Roy, “Secure Electronic Voting System using Fingerprint Authentication,” IEEE Access, vol. 8, pp. 125678–125687, 2020.

[3] S. Kumar and P. Sharma, “Biometric Based Electronic Voting System,” Proceedings of the IEEE International Conference on Communication Systems, pp. 245–249, 2019

[4] M. Satyanarayana, R. Pranam and S. Reddy, “Biometric Based Electronic Voting System,” International Journal of Recent Technology and Engineering, vol. 9, no. 5, pp. 1120–1125, 2021.

[5] K. Kale, S. Shirure and S. Kachbawar, “Fingerprint Based Electronic Voting Machine using Arduino,” International Journal of Engineering Research and Technology, vol. 11, no. 3, pp. 450–455, 2022.

[6] S. H. P., S. G. and S. P. S., “Arduino Based Smart Remote Voting System,” International Journal for Research in Applied Science and Engineering Technology, vol. 10, no. 6, pp. 1850–1856, 2022.

[7] M. Namballa, T. Kaka and M. Vaishnavi, “Real-Time Fingerprint Based Voting System,” International Journal of Engineering Research & Technology, vol. 9, no. 7, pp. 150–154, 2020.

[8] M. A. Al-Jawaherry, “Arduino Based Electronic Voting Machine,” Tikrit Journal of Pure Science, vol. 23, no. 10, pp. 45–50, 2019.

[9] S. N. Syed, A. Z. Shaikh and S. Naqvi, “Hybrid Biometric Electronic Voting System,” arXiv preprint arXiv:1801.02430, 2018,

.

[10] T. Kancherla, “Fingerprint Based Voting System,” International Journal for Research in Applied Science and Engineering Technology, vol. 13, no. 2,
pp. 325–330, 2025.

[11] N. K. Ratha, J. H. Connell and R. M. Bolle, “Enhancing Security and Privacy in Biometrics-Based Authentication Systems,” IBM Systems Journal, vol. 40, no. 3, pp. 614–634, 2001.

[12] A. Juels and M. Sudan, “A Fuzzy Vault Scheme,” Proceedings of IEEE International Symposium on Information Theory, pp. 408–408, 2002.

[13] D. Chaum, “Secret-Ballot Receipts: True Voter-Verifiable Elections,” IEEE Security & Privacy, vol. 2, no. 1, pp. 38–47, Jan. 2004.

[14] T. Kohno, A. Stubblefield, A. D. Rubin and D. S. Wallach, “Analysis of an Electronic Voting System,” IEEE Symposium on Security and Privacy, pp. 27–40, 2004.

[15] R. Mercuri, “A Better Ballot Box?,” IEEE Spectrum, vol. 39, no. 10, pp. 46–50, Oct. 2002

[16] S. Madan and S. Kumar, "Cloud-Based Secure E-Voting System Using Encryption Techniques," International Journal of Computer Applications, vol. 179, no. 7, pp. 20–25, 2018.

[17] P. Y. A. Ryan and S. A. Schneider, "Prêt à Voter with Paillier Encryption," Mathematical and Computer Modelling, vol. 48, no. 9–10, pp. 1646–
1662, 2008.

[18] F. Hao, P. Y. A. Ryan and P. Zielinski, "Anonymous Voting by Two-Round Public Discussion," IET Information Security, vol. 4, no. 2,
pp. 62–67, 2010.

[19] S. Srinivasan, S. Ranganathan and S. Venkatesan, "Biometric Authentication in Cloud Computing," IEEE International Conference on Cloud Computing,
pp. 832–839, 2012.

[20] A. K. Jain and K. Nandakumar, "Biometric Authentication: System Security and User Privacy," IEEE Computer, vol. 45, no. 11, pp. 87–92, Nov.
2012.