E-Voting Using Block-Chain

Ms. Bhoomika S Babu
Assistant Professor, Dept. of CSE (DS), SJBIT

***Abstract*—Traditional voting systems rely on either paper ballots or Electronic Voting Machines (EVMs), both of which were introduced to ensure the integrity and credibility of democratic elections. Voter verification via either electronic means and/or manual verification with a witness as to the voter's identity. that every citizen has access to vote; voter anonymity; integrity of intent behind the vote; and that voters will not be influenced or coerced into voting a particular way. However, today's elections do not provide these same protections to voters as there are vulnerabilities that can undermine the system: tampering of ballots, mistakes made by poll workers, concerns regarding fraud; and a lack of transparency. In this paper, we investigate how a blockchain-based voting system could potentially eliminate these vulnerabilities.**

Blockchain technology presents many new benefits over traditional voting methods as a result of its decentralized nature which gives rise to many opportunities for verification of a voter's identity through multiple channels.; it utilizes hashing algorithms, which make it virtually impossible to change any vote without detection; and it provides a means to restore lost data from multiple sources. Thus, a blockchain-based voting solution provides a more secure, reliable, and efficient way to conduct future elections.

***Index Terms*—E-voting, Blockchain, Homomorphic Encryption, Decentralized, Fingerprint**

I. INTRODUCTION

Electronic voting offers several clear advantages over traditional voting methods. It increases the accuracy of vote counting by minimizing human errors and safeguards the process more effectively than paper ballots. As a result, elections can be conducted more efficiently and reliably.

Around the world, interest in E-voting is steadily increasing. Estonia has been a pioneer in this field, successfully implementing nationwide Internet-based voting since 2005. Other countries, including Brazil and Switzerland, have also adopted different forms of electronic voting, demonstrating that such systems can be implemented effectively.

Electronic voting systems have the potential to make elections more accessible and convenient for eligible voters, thereby transforming how governing bodies conduct elections. However, challenges such as security, privacy, scalability, and public trust must still be addressed before large-scale adoption becomes possible. With continued technological advancements, electronic voting is likely to play an increasingly important role in future local, state, and national elections.

II. MOTIVATION

Electronic voting is driven by several important factors that support its adoption. One of the primary motivations is increased voter participation, as e-voting makes the voting process simpler and more accessible to eligible citizens. It offers greater convenience by allowing voters to cast their votes from remote locations, such as when they are residing in a different state from their registered constituency.

E-voting also helps reduce operational costs by minimizing the need for physical polling stations, staff, and transportation. In addition, it improves the accuracy of vote counting by reducing human errors that can occur in manual processes. Enhanced security is another key motivation, as electronic systems can provide controlled and monitored environments that reduce the risk of fraud and manipulation. Furthermore, e-voting enables faster vote counting, allowing election results to be announced more quickly, sometimes in real time.

Overall, e-voting is motivated by its potential to increase voter turnout and deliver accurate, efficient, cost-effective, accessible, and secure election processes.

ELECTION PROCESS IN INDIA:

Elections are a vital democratic practice in India and can be conducted through various methods, including traditional paper-based voting, electronic voting, and online voting. The outcomes of elections significantly influence the direction of the country, shaping government policies and national priorities. Therefore, it is essential that elections are conducted in a fair, transparent, and trustworthy manner.

Irrespective of the e-voting system used, ensuring fairness, transparency, and security is critical to maintaining the legitimacy of election results. This can be achieved through mechanisms such as independent audits, public verification procedures, and secure coding and system design practices.

Given India's large population and diverse electorate, managing elections presents significant challenges. While voting methods have evolved over time to improve efficiency, accuracy, and voter participation, issues such as security concerns, lack of transparency, declining public trust, and external interference continue to pose serious challenges. Although online and electronic voting systems have improved operational efficiency, addressing these drawbacks remains essential for their wider acceptance.

III. OVERVIEW

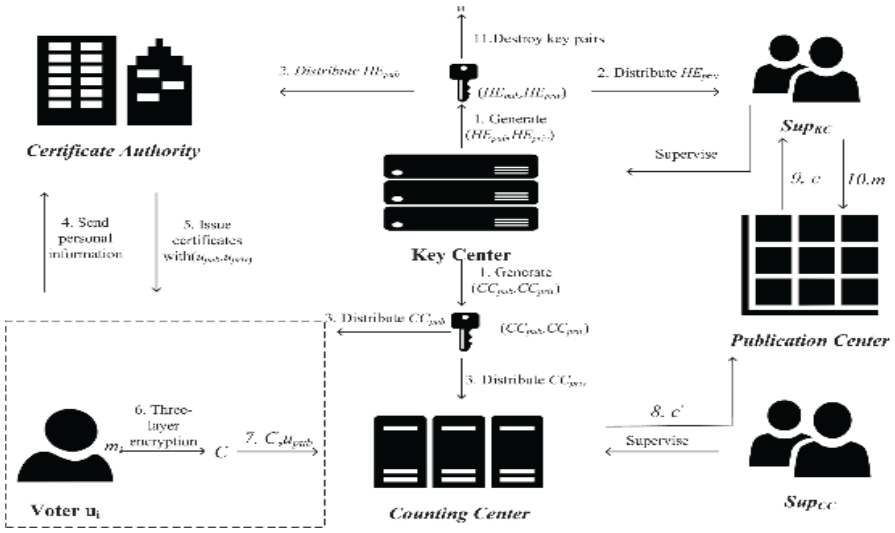
In recent years, ensuring the security, privacy, and integrity of elections has become increasingly important, especially as public trust in democratic processes faces greater scrutiny. In India, voting has traditionally been conducted using two main methods. The first is the conventional paper ballot system, which was used extensively across many states for several decades. The second is the Electronic Voting Machine (EVM), introduced by the Election Commission of India, which has now become the primary voting method in most elections due to its efficiency and reduced likelihood of manual errors.

IV. BLOCKCHAIN AND ENCRYPTION ALGORITHMS

Here, we propose a method for e-voting that is more secure than previous systems. Blockchain is a recent advanced technology used to address the aforementioned problems. It is a decentralized, secure ledger used to store and record transactions in a transparent and tamper-proof manner.

Electronic voting systems primarily offer end-to-end verification benefits. Blockchain is one of the best methods to upgrade the voting process. We use the Model-View-Controller (MVC) architecture, a popular design pattern in web development, to organize the code.

Homomorphic encryption is a cryptographic technique that allows computations on encrypted voting data without revealing the actual vote or the voter's identity. This helps maintain confidentiality during voting while enabling accurate tallying of outcomes.



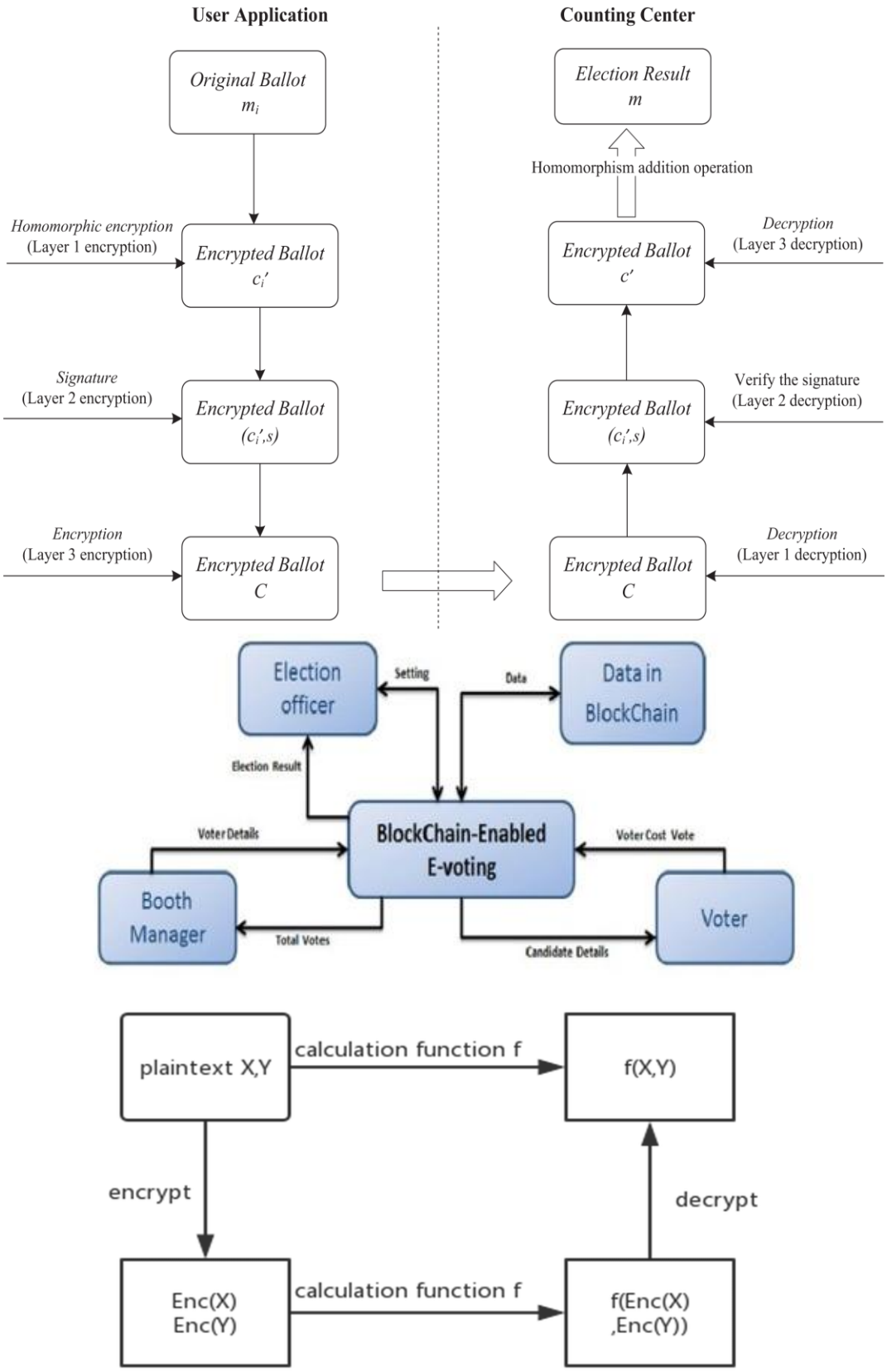


FIGURE 1: DIAGRAMS ILLUSTRATING HOMOMORPHIC ENCRYPTION IN E-VOTING PROCESS

By combining the advantages of blockchain and homomorphic encryption, e-voting systems can guarantee security and transparency while preserving voter privacy. This increases public confidence in election outcomes by ensuring results accurately reflect the will of the voters.

FINGERPRINT MODEL

In our implementation, we employ a fingerprint technique (Minutiae-Based Matching Algorithm) to authenticate voters. This is a biometric technique that identifies and verifies individuals using unique patterns and features of their fingerprints. Minutiae-based fingerprint technology in e-voting helps verify voter identity and prevent fraud, including duplicate voting. However, it can also raise privacy concerns.

Comparison with Other Fingerprint Models (Android Fingerprint):

Android fingerprint authentication is a biometric technology integrated into Android devices, using built-in sensors to capture and process fingerprint information.

For e-voting systems, minutiae-based fingerprint matching is considered more secure and accurate compared to Android fingerprint authentication.

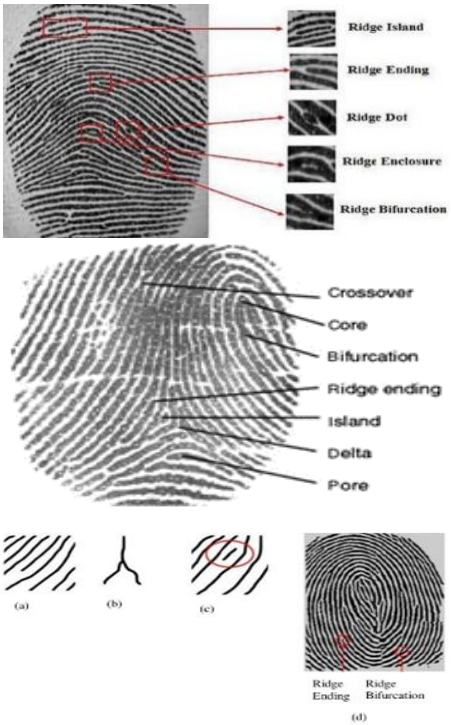


FIGURE 2: COMMON MINUTIAE PATTERNS (RIDGE ENDING AND BIFURCATION)

V. ARCHITECTURAL DESIGN OF THE SYSTEM

The system comprises two applications: a web-based application for the Election Officer and another for Booth Managers and voters. The Election Officer functions as an administrator, managing polling settings and configurations. Booth Managers are responsible for adding voter details and accessing information about cast votes and total counts. To ensure security, votes are encrypted and stored using blockchain technology.

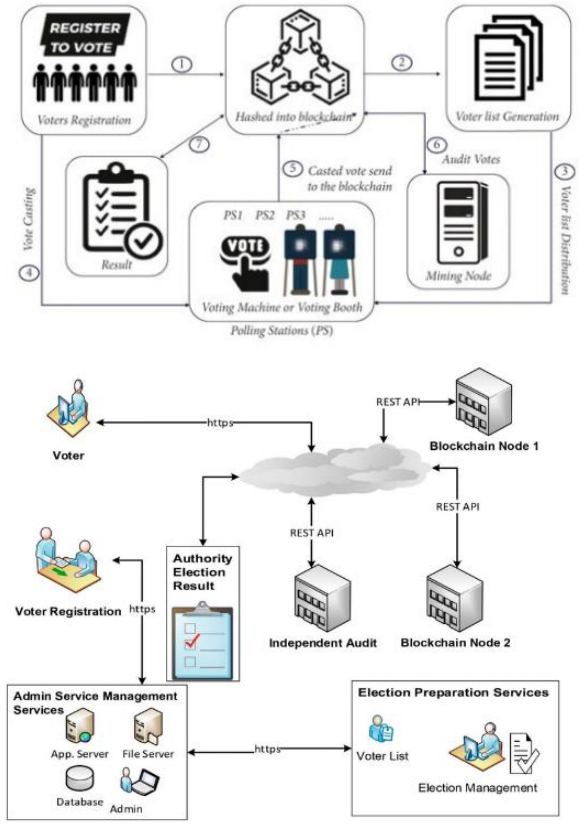
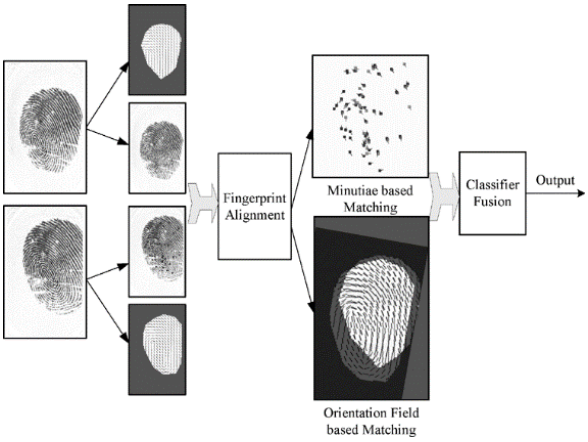
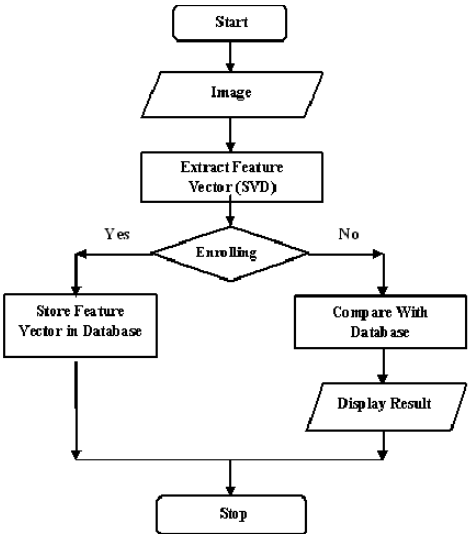


FIGURE 3: PROPOSED SYSTEM ARCHITECTURE FOR BLOCKCHAIN-BASED E-VOTING

VI. ALGORITHM USED FOR MINUTIAE FINGERPRINT MATCHING PATTERN

STEP 1: Initialize colors
STEP 2: Create a buffer image and generate a binary picture of the fingerprint
STEP 3: After generating a gray map, display a binary local result that removes noise (unwanted electromagnetic or electrical energy that decreases signal and data quality)
STEP 4: Finally, generate the skeletonization form of the image a) Binarization b) Skeletonization
STEP 5: Direction (convert the direction matrix to direction buffer image)
STEP 6: Minutiae (intersections - Extract intersection points from the binary image, a type of minutiae)
STEP 7: Minutiae (endpoints - Extract end points from the binary image, a type of minutiae)
a) Ridge ending
b) Bifurcation





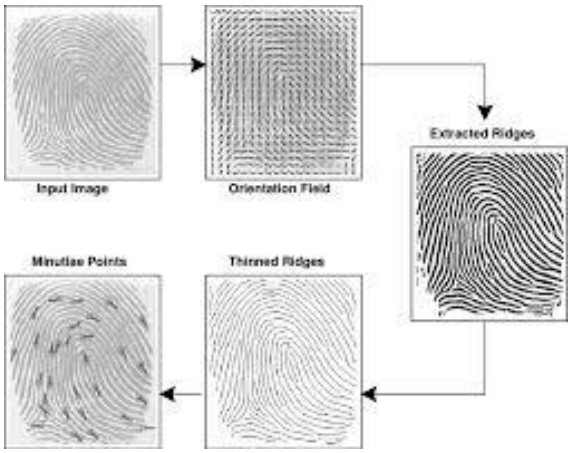
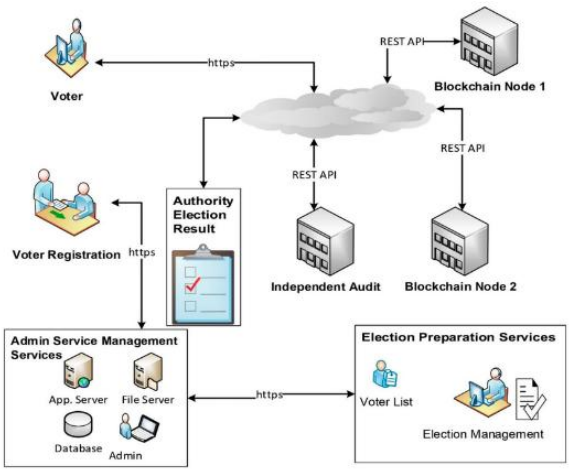


FIGURE 4: STEPS IN MINUTIAE-BASED FINGERPRINT MATCHING ALGORITHM (FLOWCHARTS)

OVERALL SYSTEM WORKFLOW:



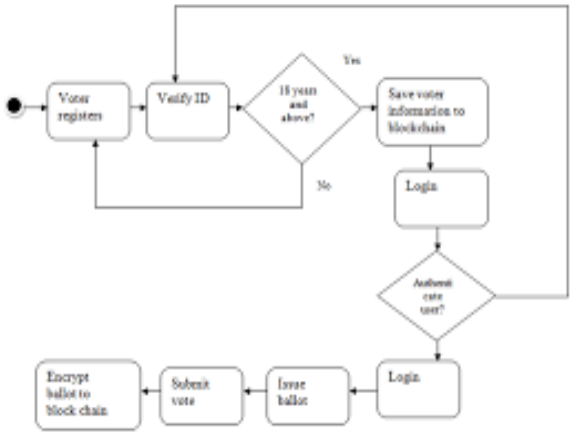


FIGURE 5: OVERALL WORKFLOW OF BLOCKCHAIN E-VOTING SYSTEM

VII. OBJECTIVE

Our main objective is to build a blockchain-based tamper-proof e-voting system. Eligible voters can cast ballots using a computer from any state, saving time by avoiding travel to home towns or designated voting centers. This addresses related issues and increases voter turnout.

VIII. LITERATURE SURVEY

Various algorithm approaches and blockchain configurations were found in the reviewed papers. Each paper has its own advantages and disadvantages. The following summarizes research from various studies:

In PAPER-01, presents a detailed analysis of existing e-voting schemes and examines the potential of homomorphic encryption for secure, anonymous, and efficient e-voting. It discusses how homomorphic encryption (an asymmetric algorithm) addresses issues like fraud and lack of privacy. The proposed online system uses voter ID for verification, keeps votes encrypted on the server, and allows only the admin to access decrypted results. However, it relies only on ID and password, lacking additional authentication.

In PAPER-02, the authors developed "Election Block," a revolutionary e-voting system using blockchain and fingerprint authentication for secure elections. It describes architecture, security, performance, and a user-friendly interface. Votes are stored on Ethereum with SHA-256 encryption and Android fingerprint authentication. The system claims to be non-duplicative, secure, and private.

In PAPER-03, presents an overview of blockchain's application in the election industry through the implementation of a decentralized and immutable ballot record system on the Ethereum blockchain. While significant advancements continue to be made within this area, much additional research is required concerning how to create an effective e-voting option utilizing blockchain technology.

In PAPER-04, explores various types of blockchain-based cloud systems supporting secure voting via the Ethereum virtual machine (EVM). The authors recommend the use of distributed ledgers and smart contracts to prove the legitimacy of all votes cast. Unlike traditional electronic voting machines (EVMs), which store all votes using MD5/SHA1 cryptography and provide no means of verifying voter identity, the author believes blockchain technology increases the overall trust level by adding a level of openness.

In PAPER-05, describes a permissioned blockchain that maintains a record of votes cast using smart contracts, thereby allowing voters to authenticate their vote without having to rely on a third party for verification. Votes are counted using SHA-256 cryptographic standards after voter authentication through the use of OTPs. However, further research is required on the benefits of increased security and resiliency.

In PAPER-06, proposes a distributed method for voting by allowing multiple voters on the same peer and then voting simultaneously. The paper also includes using homomorphic encryption to provide tallying of votes while keeping all results hidden from anyone, which improves results by allowing only authorized people to view the resulting counts. Paper 06 also uses cryptographic techniques to validate voter identities, utilizes zero-knowledge proofs to anonymize all votes, and discusses how these techniques may contribute to making electronic voting scalable in large elections.

In Paper 07, describes a distributed ledger that can be used to improve the security, transparency, and anonymity of electronic voting. Also, the authors create an incentive structure to minimize the risk of double voting, while creating an electronic voting system that is easy to use and understand for all voters.

IX. FUTURE WORK AND CONCLUSION

Future enhancements could integrate the system with the Aadhaar database for stronger voter verification and duplicate prevention.

This survey shows that while blockchain offers clear advantages for election integrity, ongoing improvements are needed in security, privacy, and verification mechanisms. Some existing solutions use simpler Android fingerprint authentication, which

may not be robust enough for national-scale deployment.

Moving forward, a practical implementation should combine blockchain immutability, homomorphic encryption for privacy-preserving tallying, and minutiae-based fingerprint authentication to create a truly reliable and trustworthy e-voting system.

REFFERENCE

[1] Tannishk Sharma, "E-Voting using Homomorphic Encryption Scheme", International Journal of Computer Applications 2016

[2] Mohamed Ibrahim, Omair Farooqui, "Election Block: An Electronic Voting System using Blockchain and Fingerprint Authentication", 2021 IEEE
18th International Conference on Software Architecture Companion

[3] Abhishek Subhash Yadav, Yash Vandesh Urade, Ashish Uttamrao Thombare, Abhijeet Anil Patil, "E-Voting using Blockchain Technology", International Journal of Engineering Research & Technology 2020

[4] Sathya V, Arpan Sarkar, Aritra Paul, Sanchay Mishra, "Block Chain Based Cloud Computing Model on EVM Transactions for Secure Voting", Proceedings of the Third International Conference on Computing Methodologies and Communication 2019

[5] Prof. Anita A. Lahane, Junaid Patel, Talif Pathan, Prathmesh Potdar, "Blockchain technology-based e-voting system", ITM Web of Conferences 2020

[6] Wenbin Zhang, Yuan Yuan, Sheng Huang," A Privacy-Preserving Voting Protocol on Blockchain", 2018 IEEE 11th International Conference on Cloud Computing

[7] Divya Rathore, Virender Ranga, "Secure Remote E-Voting using Blockchain", Proceedings of the Fifth International Conference on Intelligent Computing and Control Systems (ICICCS 2021)