

---

## E-VOTING SYSTEM USING FINGERPRINT AUTHENTICATION

**Akanksha Hatale<sup>\*1</sup>, Shweta Nawale<sup>\*2</sup>, Monika Rane<sup>\*3</sup>, Kaivalya Dhaigude<sup>\*4</sup>,  
Prathmesh Kolekar<sup>\*5</sup>, Prof. Sanjeevani Shinde<sup>\*6</sup>**

<sup>\*1,2,3,4,5</sup>Student, Department Of Computer Engineering, Bhivrabai Sawant Polytechnic,  
Pune, Maharashtra, India.

<sup>\*6</sup>Prof., Department Of Computer Engineering, Bhivrabai Sawant Polytechnic,  
Pune, Maharashtra, India.

---

### ABSTRACT

Expanding advanced innovation has revolutionized the life of individuals. In contrast to the appointive framework, there are numerous customary employments of paper in its execution. The part of security and straightforwardness is a danger from the still across the board race with the customary framework. General races still utilize an incorporated framework, wherein one association oversees it. A portion of the issues that can happen in customary discretionary frameworks is with the association that has full command over the database and framework. It is feasible to mess with the information of critical chances. Blockchain innovation is one in everything about, on the grounds that it grasps a decentralized framework and the whole database are claimed by numerous clients. Blockchain itself has been utilized in the Bitcoin framework alluded to as the redistributed Bank framework. By embracing blockchain in the circulation of databases on e-casting a ballot frameworks one can decrease the duping wellsprings of database control. This venture intends to execute casting a ballot result utilizing blockchain calculation from each place of decision. Here in security and data integrity is mainly achieved by making use of Fingerprint authentication concept. This authentication technique comes in when user casts vote on an E-voting portal.

**Keywords:** Security And Protection, Fingerprint, Internet Voting System, Voter Password, Visual Secret Sharing.

---

### I. INTRODUCTION

Electronic choice frameworks have started getting utilized in a few nations. Estonia was the essential inside the world to receive relate degree electronic appointive framework for its national races [1]. Before long, electronic determination was embraced by Schweiz for its state-wide races [2], and by Norway for its gathering decision [3]. For partner degree electronic appointive framework to fight with the standard ticket framework, it needs to help similar criteria the conventional framework bolsters, for example, security and secrecy. An E-voting framework ought to have increased security so as confirm it's offered to voters anyway shielded against outside impacts dynamical votes from being produced, or shield a voter's tally from being altered. Numerous electronic choice frameworks have confidence in Tor to cover the personality of voters. In any case, this framework doesn't give absolute lack of clarity or honesty since a few insight organizations round the world administration totally extraordinary parts of the net which may empower them to spot or on the other hand capture cast a ballot.

Fingerprint Based Voting Project is a application where the user is recognized by his finger pattern. Since the finger pattern of each human being is different, the voter can be easily authenticated. The system allows the voter to vote through his fingerprint. Finger print is used to uniquely identify the user. The finger print minutiae features are different for each human being. Finger print is used as a authentication of the voters. Voter can vote the candidate only once; the system will not allow the candidate to vote for the second time. The system will allow admin to add the candidate's name and candidate photo who are nominated for the election. Admin only has the right to add candidate name and photo who are nominated. Admin will register the voters name by verifying voter. Admin will authenticate the user by verifying the user's identity proof and then admin will register the voter. The number of candidates added to the system by the admin will be automatically deleted after the completion of the election. Admin has to add the date when the election going to end. Once the user has got the user id and password from the admin the user can login and vote for the candidate who are nominated. The system will allow the user to vote for only one candidate. The system will allow the user to vote

for one time for a particular election. Admin can add any number of candidates when the new election will be announced. Admin can view the election result by using the election id. Even user can view the election result.

## II. METHODOLOGY

### Working:

Whenever any transaction will occur in the system , the record of that transaction is maintained in the form of hash value in a block. Each next block will get attached to the previous block and in this way a virtual block chain will occur. The hash value of a current block is generated using the data of a current block and the hash of the previous block. In this way if any of the block is tempered the subsequent all the block's hash must be changed. Such multiple copies are maintained at different servers , which will assure the data security and confidentiality. As everything is through application interface, it will maintain the transparency in the voting system.

This method aims to maintain data integrity, which is protected from manipulations that should not happen in the election process. This process begins when the voting process at each node has been completed. Before the election process begins, each node generates a private key and a public key. Public key of each node sent to all nodes listed in the election process, so each node has a public key list of all nodes. When the election occurs, each node gathers the election results from each voter. When the selection process is completed, the nodes will wait their turn to create the block. Upon arrival of the block on each node, then verification done to determine whether the block is valid. Once valid, then the database added with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not.

In the proposed system we solve existing following problems solve. We need transparency, authentication and provability in the voting platform. We need to assure that the people who attend the elections are real people and use correct login credentials that we know in electronic environments, and we should be able to prove that any time, also we need our elections are 100% transparent as desired. So, we need to gather and check signed and time stamped data of the elections. Because, nobody should be able to change the votes after they are casted. Also, we need individuality in elections, so that nobody can vote for someone else.

### Software and Hardware Requirements and specification:

GPS equipment must have a rechargeable battery

- GPS equipment must have the possibility to save up 64000 records offline
- GPS equipment must support GPRS class 10 and GSM
- GPS equipment must have 4 digital and analog I/O
- GPS equipment must have RS232 connection port

GPS equipment must have a rechargeable battery

- GPS equipment must have the possibility to save up 64000 records offline
- GPS equipment must support GPRS class 10 and GSM
- GPS equipment must have 4 digital and analog I/O
- GPS equipment must have RS232 connection port

### a) Database Requirements:

MySQL is an open-source database which is mainly a RDBMS i.e. relational database management system. As a database server, primary function of this software is to storing and retrieving data as requested by other from end software applications like java which may or may not run either on the same computer or on different computer. This can be across the network either in internet or intranet.

### b) Software Requirements:

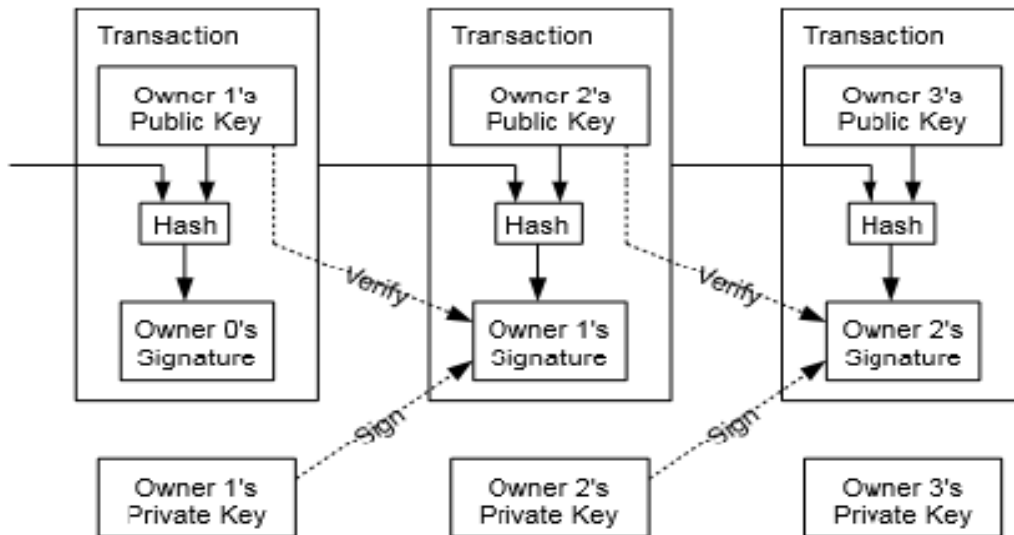
1. Operating System: Microsoft Windows 7 and Above
2. Programming Language: Java
3. IDE: Netbeans, Android Studio

**c) Hardware Requirements:**

1. Processor: Intel Core I3 or Higher
2. RAM: 4 GB or Higher
3. Hard Disk: 100 GB (min)

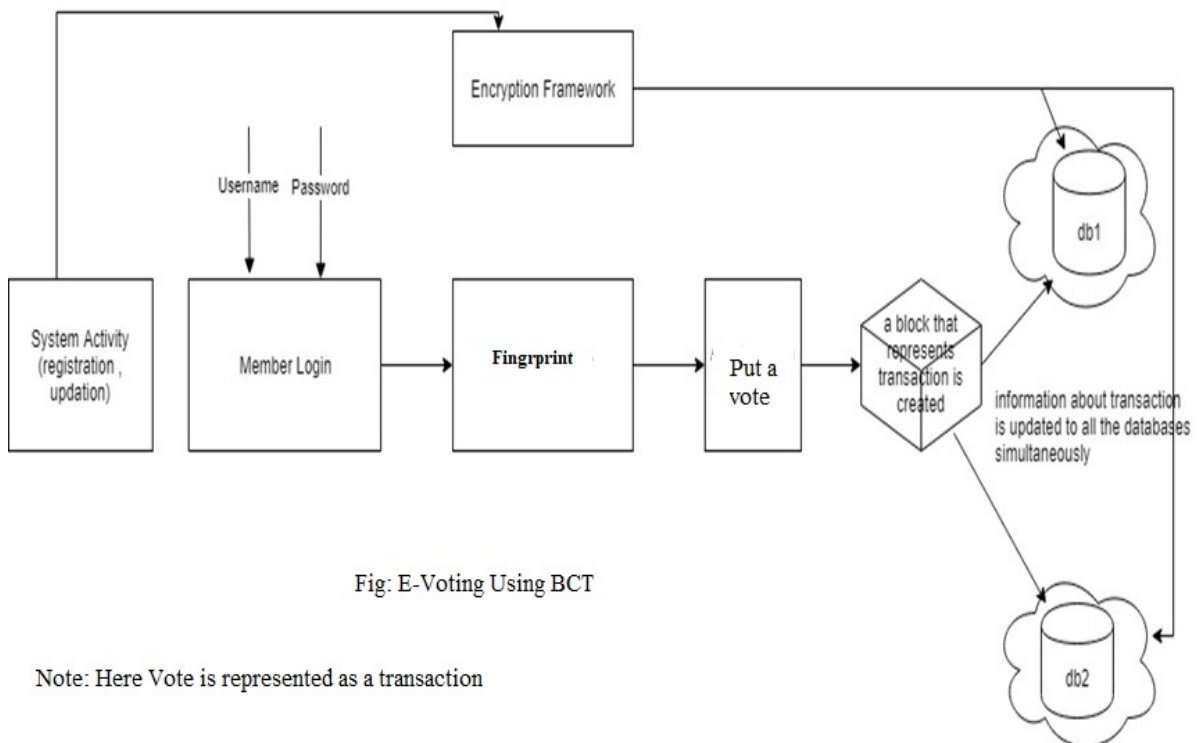
**III. MODELING AND ANALYSIS**

**Transaction Record:-**



**Figure 1: Peer To Peer Network with Transaction Record**

**Purposed System Workflow:-**



**Fig: E-Voting Using BCT**

Note: Here Vote is represented as a transaction

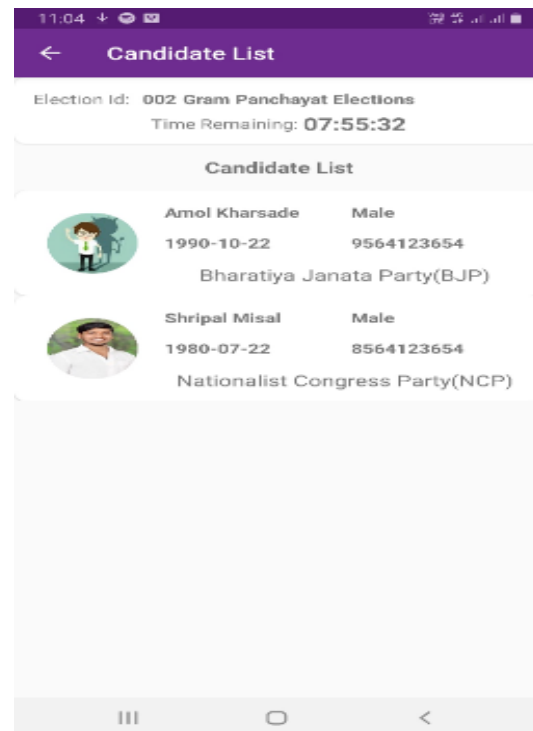
**Figure 2: Proposed System Workflow**

**IV. RESULTS AND DISCUSSION**

This page will show the user first as for authentication of candidate and to vote after authentication. By Touching the screen to sign in and to get access to vote.



This page will show if you are regular user or candidate with there names and if we want to check details about our history then also we can by clicking on your name in this list.



## V. CONCLUSION

In Proposed system internet-based voting offers many benefits including less cost and more voter participation. E-Voting systems must consider security and human factors carefully, and It should make sure that they provide voters with reliable and intuitive indications of the validity of the voting process. This system mainly uses Fingerprint Authentication to provide mutual authentication for voters and election servers.

## VI. REFERENCES

- [1] Ahmed Ben Ayed, "A Conceptual Secure Block Chain-Based Electronic Voting System",2017 IEEE International Journal of network &Its Applications(IJNSA),03 May 2017.[1]

- [2] RifaHanifatunnisa, Budi Rahardjo, "Block-chain Based E-Voting Recording System Design", IEEE 2017.[2]
- [3] Kejjiao Li, HuiLi, HanxuHou, KedanLi, Yongle Chen, "Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Block-chain", 2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems.[3]
- [4] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Accessed: Feb. 13, 2018. [Online].[4]
- [5] Maaten, E. (2004). Towards Remote E-Voting: Estonian case. Electronic Voting in Europe.[5]
- [6] Azad, Muhammad & Bag, Samiran & Hao, Feng & Salah, Khaled. (2018). M2M-REP: Reputation System for Machines in the Internet of Things. Computers & Security. 79. 10.1016/j.cose.2018.07.014.[6]
- [7] Supriya Thakur Aras, Vrushali Kulkarni, "Block-chain and Its Applications – A Detailed Survey", International Journal of Computer Applications (0975 – 8887) Volume 180 – No.3, December 2017.[7]
- [8] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, Konstantinos Markantonakis, "E-Voting with Block-chain: An E-Voting Protocol with Decentralisation and Voter Privacy", IEEE 2018,03 July 2018.[8]
- [9] Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan," Secure Digital Voting System based on Block-chain Technology",IEEE 2017.[9]
- [10] Huaqing Wang, Kun Chen and DongmingXu. 2016. A maturity model for block-chain adoption. Financial Innovation, Springer, Open Access, DOI 10.1186/s40854-016-0031-z[10]
- [11] Buterin, Vitalik. 2015, On Public and Private Block-chains. [Online] <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>[11]
- [12] Zyskind et. al. 2015. Decentralizing Privacy: Using Block chain to Protect Personal Data, 2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, July 2015 [Online]. Available: <http://dx.doi.org/10.1109/SPW.2015> JianliangMeng, JunweiZhang, Haoquan Zhao, "Overview of the Speech Recognition Technology", 2012 Fourth International Conference on Computational and Information Sciences.[12]
- [13] Carlo Blundo, University of Salerno, Alfredo De Santis and Douglas R Stinson (1998), "On the contrast in visual cryptography scheme"pp. 1-28 [13]
- [14] Thomas Monoth, Babu Anto P (2009), "Achieving optimal Contrast in Visual Cryptography schemes without pixel expansion". International Journal of Recent Trends in Engineering, Vol 1, No 1, pp. 468-471. [14]
- [15] A B Rajendra and H S Sheshadri (2012), Study on Visual Secret Sharing Schemes Using Biometric Authentication Techniques, AJCST, Vol 1, pp.157-160. [15]
- [16] Anusha MN and Srinivas B K (2012), "Remote Voting System for Corporate Companies using Visual Cryptography," vol. 2, pp. 250–251. [16]
- [17] Pallavi V Chavan, Mohammad Atique, and Anjali R Mahajan, (2011) "An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review", ACCE Int J. on Network Security, vol. 02, No. 04.pp. 7-9 [17]
- [18] Rajendra Basavegowda, Sheshadri Seenappa(2013) "Electronic Medical Report Security Using Visual Secret Sharing Scheme", IEEE UKSim 15th International Conference on Computer Modeling and Simulation Proceedings, pp, 78-83 [18]
- [19] Hussein Khalid Abd-alrazzq1, Mohammad S. Ibrahim2 and Omar Abdurrahman Dawood (2012), "Secure Internet Voting System based on Public Key Kerberos", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, pp. 428-434. [19]
- [20] Adhikari Avishek and Bimol Roy (2007) "Applications of Partially Balanced Incomplete Block Designs in Developing (2, n) Visual Cryptographic Schemes". IEICE Trans. Fundamentals, Vol.E90–A, No.5 ,pp. 949-951 [20]

- 
- [21] Marek R. Ogiela, Urszula Ogiela(2009) "Linguistic Cryptographic Threshold Schemes", International Journal of Future Generation Communication and Networking.Vol.2, No.1,pp. 33-40 [21]
- [22] Carlo Blundo, University of Salerno, Alfredo De Santis and Douglas R Stinson (1998), "On the contrast in visual cryptography scheme".pp. 1-28 [22]
- [23] Thomas Monoth, Babu Anto P (2009), "Achieving optimal Contrast in Visual Cryptography schemes without pixel expansion". International Journal of Recent Trends in Engineering, Vol 1, No 1, pp. 468-471. [23]
- [24] A B Rajendra and H S Sheshadri (2012), Study on Visual Secret Sharing Schemes Using Biometric Authentication Techniques, AJCST, Vol 1, pp.157-160. [24]
- [25] Anusha MN and Srinivas B K (2012), "Remote Voting System for Corporate Companies using Visual Cryptography," vol. 2, pp. 250–251. [25]
- [26] Pallavi V Chavan, Mohammad Atique, and Anjali R Mahajan, (2011) "An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review", ACCE Int J. on Network Security, vol. 02, No. 04.pp. 7-9 [26]
- [27] 2014 "Electronic Medical Report Security Using Visual Secret Sharing Scheme", IEEE UKSim 15th International Conference on Computer Modeling and Simulation Proceedings, pp, 78-83 [27]