International Journal of Innovative Research in Engineering
Volume 7, Issue 4 (July - August 2026), PP: 26-32.
https://www.doi.org/10.59256/ijire.20260704005
www.theijire.com
ISSN No: 2582-8746

E-Voting System Using Blockchain Technology and Facial Recognition

Yogesh Kumar[1], Dr. Shanu Kuttan Rakesh[2]
[1]*M. Tech. Scholar, Department of Computer Science and Engineering, Chouksey Engineering College, Bilaspur (C.G), India.*
[2]*Associate Professor, Department of Computer Science and Engineering, Chouksey Engineering College, Bilaspur (C.G), India.*

How to cite this paper:
Yogesh Kumar[1], Dr. Shanu Kuttan Rakesh[2], "E-Voting System Using Blockchain Technology and Facial Recognition", IJIRE-V7I4-26-32.

Abstract: *An Election is a way of selecting people to administrate the public office in democracy. Ballot is basically a piece of paper that is used to cast vote during election. To caste vote during elections, ballot is used, which is a piece of paper. In this paper-based voting method, there is a piece of paper printed with the name and symbols of the candidates called 'Ballot', and each voter uses a ballot paper and cast their votes. The EVM that is (Electronic voting machines), records the vote casted by the public. It is just like a memory recorder which records the casted votes of public. The objective of this paper is to introduces a decentralized voting framework that leverages Ethereum-based blockchain technology and biometric authentication to ensure immutable vote recording, using biometric-authentication mechanisms to preserve voter anonymity and prevent identity fraud and ensures one person one vote, while keeping their choices private and their identities secure. Along with that OTP through recognition is also one of the main advantages. The aim and objective of this paper is to implement the positive effects of security and safety in online voting system. For constructing E-voting systems, it requires great attention to Verification and Validation requirements. The system is developed using blockchain technology for immutable vote storage and facial recognition algorithms for biometric authentication. To prevent vote tampering and ensure transparency smart contracts are implemented. The experimental results had shown positive impacts against vote manipulation and unauthorized access; meanwhile efficient verification accuracy and vote processing is maintained. For hosting a secure digital election, the proposed system provides transparent framework and this framework has potential application in government and institutional voting environments. It takes care of traditional voting mechanisms challenges and provided protection against them, and keeps immutable records and preserve privacy and provide biometric authentication.*

Key Words: *Biometric-authentication, Smart Contract, Immutable, Transparent, Anonymity, Leverage, Vote Tampering.*

I.INTRODUCTION

Voting is a process used by members of a community to select a person for a particular position, whether at the national, organizational, or local level. It is commonly used in elections to choose candidates for important positions such as the President of a country.

The existing voting systems predominantly rely on traditional paper-based methods, which, while time-tested, exhibit several limitations in the contemporary technological landscape. Currently, our electoral process is carried out using EVM's (Electronic Voting Machines) and paper ballots in small villages for Panchayat elections. These existing methods have many loopholes and are used as an advantage by contestants and political parties. Traditional pen and paper voting methods suffer from vulnerabilities such as fraud, lack of traceability, and limited verifiability and requires manual verification, a process that is time-consuming and susceptible to human error. People who's having problem in mobility have to face problem in casting vote because physical voting locations are limited and there is certain time frame in which the person have to vote. This will limit the inclusivity of election process because, those people residing in remote area unable to vote in that given time frame.

The aim of this paper to digitalize the election process and enhance the security and integrity of this digital election. This paper proposes electronic voting systems that uses secure immutable Ethereum based blockchain and facial recognition technology. The system aims to increase the efficiency of the digital elections to increase the voter turnout by leveraging the decentralized nature of blockchain and biometric authentication of facial recognition. The proposed systems process starts with voter registration on the blockchain, the eligible voter gets registered by providing its biometric data of and that data is stored in hash form with other necessary information like name, age, city, etc. During voting all these details are verified and

at the time of voting face is captured and then converted into hash identifier, these hash values are matched with stored hash value, if it matches voter can caste its vote. It ensures only authentic voter can vote only. To safeguard privacy, only hashed identifiers of biometric data are stored on the blockchain, protecting sensitive information from unauthorized access.

II. LITERATURE SURVEY

According to **MD Shadab Hussain et al. (2018)[4]**, It point out that most existing voting systems come with their own set of trade-offs, but two problems keep showing up again and again a lack of transparency and no real way to audit the process. They thought blockchain will be the answer to that problem which is occurring again and again in existing system. They introduced the Auditable Blockchain voting systems (ABVS), a system which leverages Blockchain technology with intelligent and multi-agent systems, when they combined both these technologies, they get a single supervised voting system where each and every vote can be verified end to end. By using this system, we don't need to rely on the election official or any institution to check if voters vote is counted/included or not, by using blockchain data can be checked up very easily. Any person who has casted vote can cross verify their vote using ABVS. Many countries had started adopting E-voting systems for their election process.

In this research **Nir Kshetri et al. (2018)[5],** they think that blockchain-enabled e-voting systems will help in cutting down voter fraud and will also making voting more accessible and easier for people. The idea is that eligible voters would be able to cast their ballot anonymously, using nothing more than a computer or a smartphone, with an encrypted key and tamper-proof personal IDs keeping things secure. The article walks through a few real-world BEV implementations, along with what the approach stands to gain and where it might run into trouble. Of all the public sectors blockchain could shake up, the authors suggest e-voting is one of the more promising candidates. The concept itself isn't complicated. Borrowing an analogy from digital currency, each voter is handed something like a "wallet" containing their credentials, along with a single "coin" that represents their one shot at voting. Casting a vote simply means sending that coin over to a candidate's wallet and once it's spent, that's it, it can't be used again. There is a bit of flexibility built in, though: voters are allowed to change their vote right up until a set deadline.

In the study of **BalaMurali et al. (2020)[1]** It states that; Democratic elections rely on unique voter ID numbers to track populations, but traditional PINs and passwords leave room for fraud. Switching to biometrics like fingerprints is much more secure because they are completely unique to the individual. Another issue with current Electronic Voting Machines (EVMs) is that they don't give voters any confirmation. To overcome this problem, they introduced GSM and SMS modules by using this module's voters get an instant text message verifying their vote was casted and counted. The existing system uses localized servers but they have adopted the cloud-based data storage. Rather than depending on localized servers, which often have limited processing capacity and susceptible to failure, the system uses cloud-based infrastructure to achieve efficiency and scalability. Finally, the integration of GSM technology introduces a transparency mechanism previously absent in many voting systems. Upon casting a vote, the elector receives a confirmation message indicating the candidate to whom the vote has been registered.

In this research **K.C Arun et al. (2020)[2]**, The Internet of Things (IoT) can be described as a network of physical devices, connectors, actuators, and communication tools that work together to send and receive data over the internet. It's a technology that's steadily making everyday life easier, and its influence can be seen across almost every field now. One area where this is becoming increasingly relevant is elections applying IoT to voting has the potential to improve the process in several ways. Naturally, this brings with it a range of functional and non-functional requirements that need to be carefully considered at every stage of system design, since these details tend to make or break how well the system actually works. When implemented properly, IoT-based systems can improve the precision, reliability, and efficiency of voting, while also cutting down the time it takes to declare results. Broadly speaking, there are two forms of online voting in use today. The first is used at polling stations, where the process remains under the direct supervision of electoral officers. The second is remote online voting, where voters can cast their ballots over the internet from wherever they happen to be. This second approach is particularly significant because it has the potential to boost voter turnout considerably; especially for people who live far from polling stations or simply find it difficult to travel there. using IoT systems, will make it easier to build, manage, and scale and helps to counter problems in elections like handling large populations that is spread across multiple locations. The performance of E-voting systems depends on few key things like: its user interface, the UI should be user friendly and easy to use for people, the most important thing is how secure it is. Without strong security in the system, it will suffer challenges like fraud, non-verifiability of votes, which is why robust protective measures are what ultimately separate a dependable system from a vulnerable one.

In this study **Mr. Santosh Kumar et al. (2020)[3]**, they make smart e-voting system with a simple web interface, using blockchain technology The system has mainly two modules. First the Admin module, where administrators can add candidates, manage their details, and verify whether a voter is legitimate or not. Then the second modules is Voter module, where the voter can cast their vote for a candidate. This paper focuses on electronic voting systems which uses Aadhar-card's QR code to verify voters' identity online rather than voter id card which are used for manual verification of the voter, this voters authentication process confirms voters' identity and also prevent double voting in elections. It allows auditing and stops fraudsters from vote tampering because the casted votes are securely stored on servers. when voting is done and all the votes are casted, Admin can login and declare the results.

In this research **Shubham Ghule et al. (2020)[23]**, they developed an Android based e-voting system platform to encourage the electronic voting process. Which will increase the voter turnouts, because increase in accessibility will also increase the voter's participation in the voting. They integrate facial recognition for voters' authentication by using mobile

camera and Android based platform for voting interface. For registration voter has to capture his or her face then they have to input the password. After successful registration voter can vote by again capturing their face and entering password. upon successful authentication voter can cast its vote. The proposed systems have flaws such as manipulation risks, privacy and data protection risk due to facial data capturing. The android-based e-voting application with facial recognition has scope and potential to digitalize the election process but for scalability and wider adoption of these systems their issue must be addressed properly.

In this study **Rihab H Sahib et al. (2021)[22]**, they proposed an innovative blockchain technology based, e-voting system which leverages the advantage of blockchain such as decentralization, transparency, immutability. Citizen can use digital devices to cast their vote digitally, which encourages the digitalized voting and accountability of votes, provides safe and secure voting environment. They review the existing literature on e-voting systems, while keeping focus on blockchain based solutions. Privacy, security, transparency, accuracy, and decentralization are used as an evaluation criterion for this research paper. They explore various implementations and user interactions, covering registration, authentication, and result presentation in research work. This review paper provides promising aspects of blockchain-based e-voting which overcomes the challenges of traditional voting systems by providing transparency, security and privacy but has many drawbacks like, scalability challenges, security challenges and requires technical literacy.

In this research **Uzma Jafar et al. (2023)[21]**, To analyse the current status of blockchain based voting research and online voting system they have conducted a comprehensive literature review. This paper aims to identify potential developments. To enhance the legitimacy, integrity, security and accuracy of election, they proposed a E-voting system which has blockchain technology. Which aims to address existing vulnerabilities in electronic voting. Its decentralized nodes are used for voting. Conceptual descriptions of blockchain-based electronic voting applications were explored, emphasizing the technology's structure and characteristics.

III. EXISTING SYSTEM

In another existing system they introduce Auditable Blockchain Voting System (ABVS) Elections run on trust. Take that away, and the whole machinery of democratic participation starts to wobble. To resist the problem of the Auditable blockchain voting system (ABVS) was introduced. which can eradicate the mistakes and rebuild the foundation so, that there would be no need to discard all the electronic voting devices. To resist the problem of the Auditable blockchain voting system (ABVS) was introduced. which can eradicate the mistakes and rebuild the foundation so, that there would be no need to discard all the electronic voting devices.

In the mainstay, the system is antiquated which pairs that sound in compare to blockchain buzzword: Across by paper trail it’s a digital convenience through procure online portal voters can login, through these voters can choose their ballots electronically and can get a receipt, voters-verified paper audit trail or VVPAT. it is a paper record they can get in real by which voter's check whom they have voted for and they generate later if asked. It's not like screen which disappears while closing the tab. Beside this every vote gets recorded into a blockchain ledger. Which is constant distributed and resistant to tempering that torment the databases from decennary. that's the intention of using blockchain here- unconventionally for ourselves, but the fact that, altering or misleading the records can become practically impossible without leaving obvious trace.

The significant of ABVS, it's not just the technology blueprints. It's the logging tier. The auditor can cross reference it directly against the paper records which is generated at the moment of voting. Instead of, blindly trusting the digital tally. these two lines of evidence can be checked again each other independently. if they align in same way or they point towards the same conclusion then only it would be trustworthy or credible. if there is any discrepancy it becomes the scepticism for legitimacy. By no means to say that system is a finished solution. What appears to be a genuine concern is scalability- Blockchain networks, especially once handling something high rolling and high volume as a national election tends to strain under load.

Another major challenge is - Accessibility, for those who are not acquainted with the digital interface they won’t be able to feel comfortable, they won't be able to trust in unfamiliar technology or a system, not even every voter's has reliable internet access. Still takes as a whole ABVS represents a meaningful way- legitimately more credible attempts yet towards electronic voting and people that can be verifiable rather than simply hoping for the correct way of voting.

Disadvantages:

1. **Security vulnerabilities:** An entire elections outcome comes into impugn- and often by the time anyone notices, the damage is already done. The reason behind this can be the existing system which is exposed to hacking easily, tempering and cyber-attacks.
2. **Lack of transparency:** Voters cast their votes and then, have faith on the conventional system, that they had counted their ballot correctly. Auditor also face the same issue, without a clear verifiable mechanism to check outcomes against original intent.
3. **Unreliable post-election audits**: Conducting audits in these systems is certainly complicated-complex procedures, incomplete records, no dependable way to reconcile what auditors have counted and what voters have voted for. The real assurance isn’t trusted on audit.

These three failure points towards the conclusion: Electronic voting need a structural fix, not a far cry from patch. That’s the gap ABVS is attempting to close.

Research gap:

In the existing system if a voter wants to vote for a particular party or candidate, then he has to visit the polling booth where voting is taking place. He must visit the designated polling booth assigned to his permanent address in order to cast his vote. Then manual verification is done by the booth agents and officers by verifying person's identity using voter id. Then vote is casted and recorded. For results votes are counted manually by counting each vote in EVM.

So, the existing approach doesn't provide the safe and secure environment and counting of votes is done manually which is suspectable to human error.

IV. PROPOSED SYSTEM

This system is designed to completely rethink how we vote by replacing paper ballots with a digital platform that anyone can use on their regular computer. At its core is blockchain technology, which locks each vote into a secure digital ledger that can't be changed or erased without everyone noticing. To make sure only the right person votes, the system uses two layers of identity checks: facial recognition and a one-time password sent by email, making it much harder for someone to pretend to be someone else. The interface, built with Django, is reliable and can handle lots of users at the same time without slowing down. Most importantly, it's simple and easy to use, so it works for everyone—not just tech experts. Altogether, this creates a voting system that's not just digital, but also more trustworthy, secure, and accessible to all.

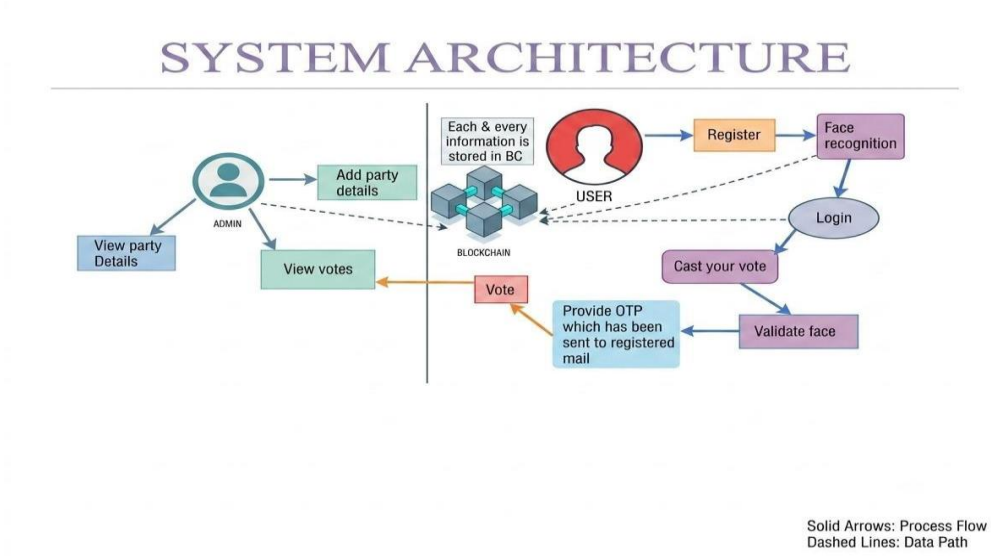

Figure 1: Architecture Diagram

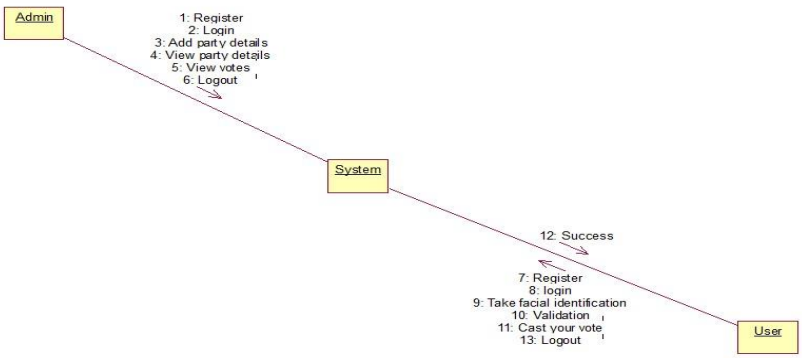

Figure 2: Collaboration Diagram

Working:

Working of the Proposed Blockchain-Based E-Voting System

The proposed e-voting system makes elections secure and transparent by combining blockchain technology with facial recognition and email-based one-time passwords (OTPs). It all starts with voter registration, where eligible voters provide their personal details like name, email, address, ID info, and a facial photo. The system checks this information and safely stores it.

Election administrators log in through a special admin module where they can manage the election by adding details about political parties, candidates, party logos, and other important info. This data is stored securely and is available for voters to see during the election.

When it's time to vote, registered users log in and go through a two-step verification process to confirm their identity. First, facial recognition matches their live image with the one on file. Then, an OTP is sent to their registered email, which they must enter to proceed. This double-check makes sure only authorized voters can participate.

Once verified, voters can see the list of parties and candidates and cast their vote by choosing their preferred option. The system makes sure each voter only votes once and confirms the vote with a message.

Behind the scenes, blockchain technology securely stores all voter info, party and candidate details, and voting records. Each piece of data is linked to the previous one with a special cryptographic code (using SHA-256), which keeps everything tamper-proof and transparent. If anyone tries to change the data, it's immediately obvious because the code won't match.

Blockchain also prevents people from voting more than once by permanently recording each vote and marking that voter as having voted. Since the blockchain data is stored across many computers (nodes), it stays safe and reliable.

At the end, the system automatically counts all the votes and shows the results. Administrators can track the vote counts and election progress through a dashboard, all while being confident that the blockchain keeps the votes accurate, transparent, and secure throughout the entire election.

Advantages:

1. Security is maintained through 2 factor authentication process, first it required a facial recognition and then an email OTP and using this 2-factor authentication process it covers the gap which was there in the existing system adding blockchain technology, that is a distributed tamperproof ledger that helps in locking the votes once they are casted by the voters.
2. Django powers the interface, it provides the framework and interactive interface for voting, that anyone can use irrespective of how uncomfortable they are with technology and can use it easily without any confusion or problem. These little things matter in wider adoption of technology because there is certain section or group in society that might struggle in this step. so, using Django framework narrows down that gap.
3. Blockchain helps to prevent the alteration and deletion of vote, once the vote is casted it cannot be changed or deleted later on. This fact builds trust and confidence in election process and it gives the results weight, something people can actually trust, rather than take on faith

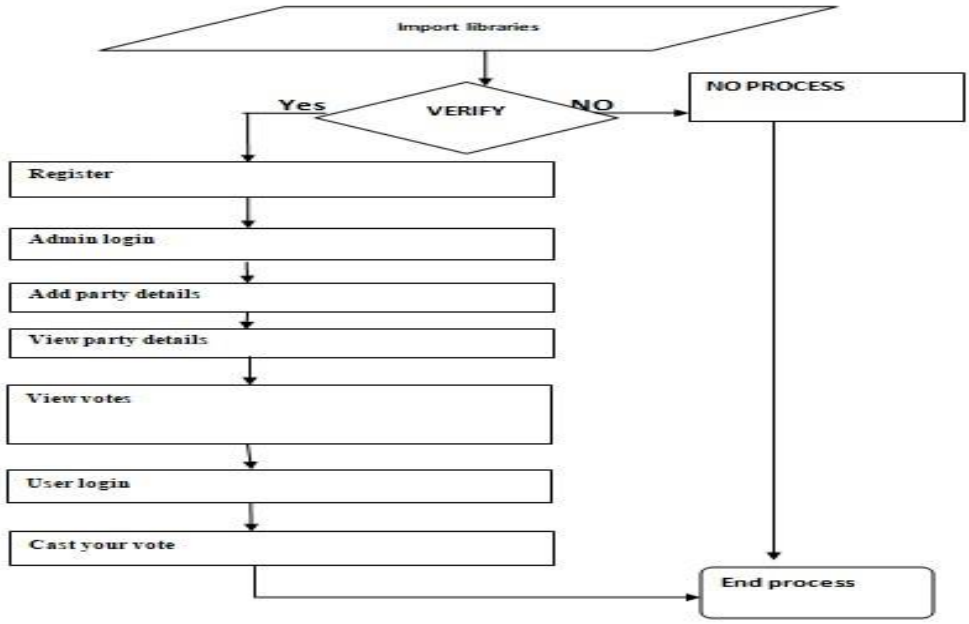

Figure 3: Data flow Diagram

Modules:

These are the seven modules which broadly explaining the whole process:

Register: In this module voter register itself for the system by giving his relevant personal details like email id, name, address, etc. After that systems checks the given credentials and confirm that he/she is eligible for voting or not. If they are eligible then their face is captured and then this facial data along with the relevant personal information are converted into hash templates and stored in the blockchain.

Admin Login: Admin module is used by administrators only. It means that whole election administrator is running the

system in the backend. Admin login with the given credentials. Once they login to system they can add, delete and update the details of the candidate also watching the whole voting progress and pull reports when needed.

Add Party Details: In This module, administrators add the party party's name, symbol, as well as the candidate list according to their respective party.

View Party Details: Party detail modules design for both voters as well as for voting officers. Voters can see the candidate and then the party who they vote for. There is also correction window in this module by which voting officer edit or update the details of party and their candidate when needed.

View Votes: This module shows the current summary of the voting; It means which party or candidate get's how much vote. Also, this can be accessible for people so that they can follow the voting pattern. But it is more useful for admin to know the whole voting scenario.

User Login: This module is used by the voters, who cast their vote by two step verification that is: facial recognition and email OTP confirmation after the successful authentication they entered the voting interface.

Cast Your Vote: This is the module in which voters select his/her candidates or party, by the given following steps that are shown on the screen. System allowed one vote from one login that means one person is allowed to vote only one time, therefore fraudulent and bogus voting is not possible. After that the vote is submitted in the system and voter received the confirmation message and the vote gets recorded in the blockchain.

Blockchain Integration

- Blockchain as a very secure digital storage system. It holds the important stuff for our e-voting setup — votes that have been cast, candidate details, voter details, all of it. Each piece of information sits inside its own "block," and these blocks are chained together one after another. Because of this chaining, the record ends up being pretty much unchangeable — nothing in it can quietly be altered once it's added.
- Blockchain also plays a role in making sure only the right person is voting. It does this by using 2-factor authentication process first is facial recognition, which matches the voter's face with the stored face template data, and second is an email OTP, a one-time code sent to voters registered email. using this 2-factor authentication method, it becomes really hard for someone to pretend to be another person and vote on their behalf.
- It also prevents anyone from voting twice. The moment when a vote is casted, it gets recorded on blockchain, the same identity that is login credentials or face cannot be used to submit another vote after that. This keeps final results fair and accurate.

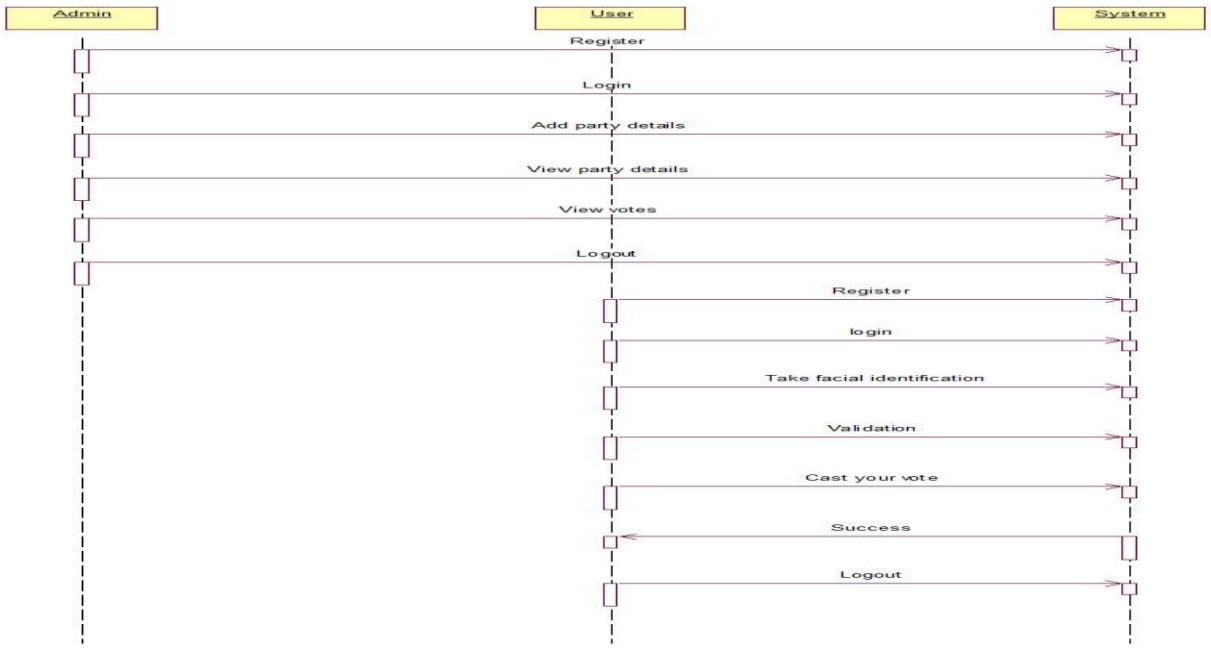

Figure 4: Sequence Diagram

V. CONCLUSION

Through blockchain voting becomes more secure and trustworthy. As every vote gets recorded, changes in votes is next to impossible. Due to tangible system it's not just a matter of faith or hope, it's crystal clear. Voters can actually check their casted vote at any moment. In this research the priority or center of attraction is its security, mainly two points: Facial recognition and email OTP, that assures that one person can cast their vote only single time. So that there would be no parody, no trespass. The system uses SHA-256 hashing to protect data from records tempering and assures that a single vote for a

single person. The system stays stable doesn't slow down or break even with a huge number of voters casting their votes on a same day and same time. The use of this system is very easy, like any other website, simple for every single person whether, they are voters, auditory, authority or admin, no special training or learning is required. In a single line -It is very convenient, tangible, secure for anyone. It is withstanding which works everything in the background very smartly. In short, it's a voting system that's secure, transparent, and simple enough for anyone to use.

References

1. BalaMurali, Potru Sarada Sravanthi, B. Rupa." Smart and Secure Voting Machine using Biometrics",2020 Proceedings of the Fourth International Conference on Inventive Systems and Control (ICISC), September 2020.
2. K.C Arun1, Shahbaz Ahmad2, Saba Noor3, Iqra Mumtaz4and Mubashir Ali5." Arduino Based Secure Electronic Voting System with IoT".4th Global Conference on Computing & Media Technology,July 2020.
3. Mr. Santosh Kuma, Dr.NitikaSinghi, Abhijit Patankar." A Survey on Smart Electronic Voting System through Block-Chain Technology",2020 Journal of Emerging technologies and Innovative Research(JETIR), April 2020.
4. MD Shadab Hussain, Dr Mohammad Sarfraz, Salim Rukhsar. " Towards The Intelligent Agents for Block Chain E-Voting System ", 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018.
5. Nir Kshetri and Jeffrey Voas." Block ChainEnabled E-Voting."2018 The Institute of Electrical and Electronics Engineers (IEEE),2018.
6. MichałPawlaka, AnetaPoniszewskaMaranda ´ a, Natalia Kryvinskab,c." Towards the intelligent agents for block chain e-voting system." 2018 The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN),2018.
7. M. Pawlak, J. Guziur and A. PoniszewskaMaranda,"Voting process with blockchain technology: Auditable Blockchain Voting System",FatosXhafa, Leonard Barolli, MichaÅGreguÅ (Eds.): Advances in Intelligent Networking and Collaborative Systems, LNDECT 23, ISBN978-3-319- 98556-5, Chapter 21, Publisher: SpringerVerlag Heidelberg, 2018.
8. S. Mello-Stark and E. A. Lamagna,"The Need for Audit-Capable E-Voting Systems", Proc. of 31st International Conference on AdvancedInformation Networking and Applications Workshops (WAINA), Taipei, Taiwan, 2017.
9. X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso and P. Rimba, "A Taxonomy of Blockchain-Based Systems for Architecture Design", Proc. of IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 2017.
10. J.Deepika, S.Kalaiselvi ,S.Mahalakshmi, S.AgnesShifani "Smart Electronic Voting System Based On Biometric IdentificationSurvey". Third International Conference on Science Technology Engineering & Management (ICONSTEM), 2017.
11. V. Kiruthika Priya, V. Vimaladevi, B. Pandimeenal, T. Dhivya, "Arduino based Smart Electronic Voting Machine", International Conference on Trends in Electronics and Informatics, ICEI 2017,
12. Dr. Z.A. Usmani , Kaif Patanwala, Mukesh Panigrahi, Ajay Nair, "MULTI PURPOSE PLATFORM INDEPENDENT ON LINE VOTING SYSTEM", International conference on innovation in Information, Embedded and Communinaction Systems, 2017
13. S. M. Anggriane, S. M. Nasution and F. Azmi," Advanced e-voting system using Paillier homomorphic encryption algorithm", Proc. ofInternational Conference on Informatics and Computing (ICIC), Mataram, Indonesia, 2016.
14. Poniszewska-Maranda, L. Gebel," Retrieval and processing of information with the use of multi- agent system", Journal of Applied Com-puter Science, Vol. 24, No 2, ISSN 1507-0360, pp. 17-37, 2016
15. Julia Pomares, Ines Levin, R. Michael Alvarez, Guillermo Lopez Mirau, Teresa Ovejero, "From Piloting to Roll-out: Voting Experience and Trust in the First Full eelection in Argentina"‖, International Conference on Electronic Voting EVOTE,2014.
16. Alex Delis, Konstantin Gavatha, AggelosKiayias, CharalamposKoutalakis, EliasNikolakopoulos, LamprosPaschos,MemaRousopoulou, Georgios Sotirellis,Panos Stathopoulos, PavlosVasilopoulos, Thomas Zacharias, Bingsheng Zhang, "Pressing the button for European elections", International Conference on Electronic Voting EVOTE2014, EVoting.CC GmbH, 2014
17. Chunlin Yang, Techshino, "Fingerprint Biometrics for ID Document Verification", IEEE 9th Conference on Industrial Electronics and Applications (ICIEA), pp.1441-1445, 2014
18. D. Ashok Kumar, T. UmmalSariba Begum, "Electronic Voting Machine – A Review", Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering, March 21-23, 2012.
19. Sravya. V, Radha Krishna Murthy,Ravindra Babu Kallam, Srujana B, "A Survey on Fingerprint Biometric System", International Journal of Advanced Research in Computer Science and Software Engineering ,pp.307- 313 Volume II, Issue 4, April 2012.
20. Nani FadzlinaNaim, Ahmad Ihsan Mohd Yassin, Wan MohdAmeerul Wan Zamri, Suzi SerojaSarnin, "MySQL Database for Storage of Fingerprint Data", UKSim 13th International Conference on Modelling and Simulation, pp. 293-298, 2011
21. Uzma Jafar,Mohd Juzaiddin Ab Aziz, and Zarina Shukur, et. al.,"Blockchain for Electronic Voting System—Review and Open Research Challenges", Published in ieee, 2023
22. Rihab H Sahib and Prof. Dr. Eman S. Al-Shamery, et. al., "A Review on Distributed Blockchain Technology for E-voting Systems" Published in iopscience, 2021
23. Shubham Ghule , Mayur Bhondave , Pournima Mishra , Vaibhav Survase , Prof.Alka Kulkarni, et. al., "Smart E-Voting System with Face Recognition by BlockChain Technology "Published in ijarcee open Access ,2020