isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 3 ,Apr,2024 ,ISSN_NO: 2321-3337

COMBINATION OF BLOCK CHAIN AND MOBILE APPLICATION FOR EFFECTIVE VOTE FROM HOME WITH POLLING MONITORING WITH ID INTEGRATION

Arulraj A[1], Giridharan V[2], Ranjith A[3], Dr. Kamal N[4*]
[123]UG Scholar-Dept.CSE, GRT Institute of Engineering & Technology, Tiruttani, India.
[4*]Professor-Dept.CSE, GRT Institute of Engineering & Technology, Tiruttani, India.
ranjith1711r@gmail.com, acerarul1@gmail.com, girid8809@gmail.com
[*]Corresponding Author: kamal.n@grt.edu.in

Abstract

Now a day's Electronic Voting Machine (EVM) based Voting is present, but still there is no system to avoid Proxy Casting and Recasting implementation. We improvise in our project to check our own casted vote novel electronic voting system based secure application used to construct a block chain technology. We integrate Aadhaar card linked Mobile number with OTP Generation, only then the voter can cast the vote. Finally maintains database using a secure algorithm. The system also allows voters to receive a confirmation receipt, which includes anonymized but verifiable data, ensuring their vote has been counted without revealing their choices. To maintain voter confidence, the system incorporates transparent audit trails, which can be reviewed without compromising individual anonymity. Lastly, the blockchain's decentralized nature ensures that no single entity can alter recorded votes, thereby maintaining the integrity of the election process.

Keyword: *Novel Electronic Voting System, Blockchain Technology, Secure Algorithm.*

1. Introduction

In the current Electronic Voting Machine (EVM) voting system, the use of embedded integrity hardware allows for voting one at a time, ensuring security but potentially vulnerable to tampering or technical failures. Such vulnerabilities can lead to delays or disruptions in the voting process. Moreover, the setup, maintenance, and updates of the Electronic Voting Machine (EVM) system incur significant costs and resources. Single voter can vote multiple time. This issue can be overcome by this system. The main objective of the Application is to provide Effective Voting system with High secured. Maximum number of vote casting will be achieved. As Public are not required to travel from the work space to their native place. Recasting and Proxy Casting will be avoided using our application. User can verify the vote casted details to avoid any sort of hacking or manipulation. A blockchain is "a distributed database that maintains a continuously growing list of ordered records, called blocks." These blocks "are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

2. Related Works

This paper presents the evaluation of a secure stegano-cryptographic model for electronic voting. It assesses the model's performance in meeting key requirements such as authentication, integrity, confidentiality, and verifiability using a five-point psychometric analysis. Results indicate that the model effectively verifies voters' identities, maintains election integrity, ensures voter privacy and vote confidentiality, and offers fraud detection mechanisms, particularly beneficial in developing countries with significant digital disparities.[1]

The rise of the internet and technology has prompted the exploration of e-voting as an alternative to traditional elections. To ensure fairness and credibility, various information security and privacy technologies like cryptography and steganography have been devised. Standards such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA) are utilized to secure votes and maintain confidentiality and integrity. Homomorphic encryption enables vote calculation without revealing voter information. Current research emphasizes electronic voting protocols like zero knowledge authentication based on Diffie-Hellman key exchange to ensure mutual authentication between the server and voters. This thesis proposes a new protocol addressing security requirements such as authentication, privacy, integrity, anonymity, and non-repetition in the voting process.[2]

This paper proposes the implementation of online voting using Blockchain technology to address security concerns and tampering issues observed in traditional voting systems. Blockchain ensures security through encryption and hashing, treating each vote as a transaction recorded on a distributed ledger shared among peers in a peer-to-peer network. The system maintains anonymity by associating each voter with a unique Government-approved Aadhar number, allowing only one vote per voter. Votes are encrypted, hashed, and added to the blockchain, forming a chain of blocks that cannot be traced back to individual voters. The application abstracts the underlying architecture complexities for user convenience. A minimum of three peers forms the peer-to-peer network, and the scalability of the system depends on the secondary memory limit of the peers. The transition to online voting is expected to increase voter turnout.[3]

Can the principle of secret suffrage be ensured when voters are offered the possibility to cast their votes using internet voting? With the steady introduction of different forms of remote electronic voting since 2000, it has become apparent that internet voting fails at providing the privacy guarantees offered by traditional paper-based voting systems. Against this assumption, the current proposal suggests reviewing the traditional configuration of the principle of vote secrecy. With this in mind, the proposal will: (1) assess current accepted standards on voters’ anonymity for traditional and internet-based voting systems; (2) evaluate the core elements of lawful relaxations to the principle of secret suffrage, and especially those traditionally associated to different forms of remote voting, and assess whether they can be applied to internet voting; and (3) study how current technical developments in the field of elections (and more broadly, in the field of e-governance and e-democracy) may result in further relaxations of the principle of secret suffrage in the future. Overall, the goal of the proposal is to approach the principle of secret suffrage against the specificities of internet voting and, instead of evaluating electronic voting systems using traditional standards for voters’ privacy and anonymity, evaluate how specific proposals aimed at ensuring voters' secrecy in internet voting comply with the very end that the principle of secret suffrage is aimed at protecting, namely: voters’ freedom.[4]

This paper focuses on addressing three significant challenges in cryptographic voting schemes. Firstly, it tackles the issue of secrecy and coercion resistance in the event of a compromised voting machine. A novel approach employing encapsulated design is proposed to minimize information leakage compromising ballot secrecy. Secondly, it addresses the vulnerability of receipt stealing, common in many voting schemes. A solution is presented to enhance vote protection, especially for schemes utilizing computer-generated receipts. Lastly, the paper discusses contestability in elections, emphasizing the need for detecting and proving errors or manipulations. While the solutions are discussed in the context of Bingo Voting, the insights provided extend to various cryptographic voting schemes, highlighting prerequisites for secure elections.[5]

3. Objective

The main objective of the Application is to provide Effective Voting system with High secured. Through this Application maximum number of vote casting will be achieved. As Public are not required to travel from the work space to their native place. Recasting and Proxy Casting will be avoided using our project. User can verify the vote casted details to avoid any sort of hacking or manipulation.

4. Proposed System

A novel electronic voting system based on Blockchain that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing a blockchain-based e-voting system. the development of a novel Mobile application voting system based on blockchain represents a significant advancement in electoral technology, offering a transformative solution to address the shortcomings of existing voting systems. By harnessing the power of blockchain technology and conducting exhaustive evaluations of blockchain frameworks, this system seeks to establish a more secure, transparent, and accessible electoral process for citizens around the country.

5. Architecture Diagram

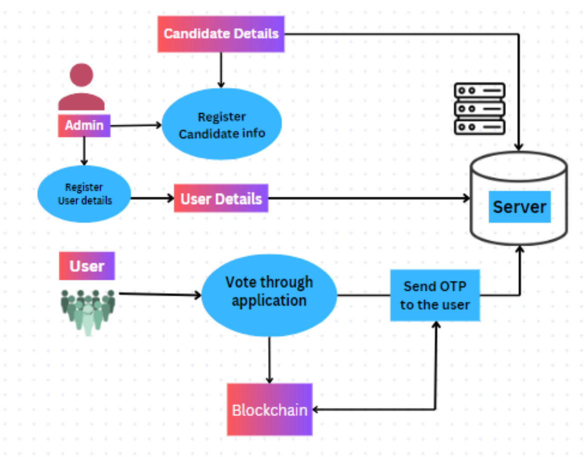


Fig:5.1Architecture diagram

6. Algorithms

6.1 Asymmetric Key Encryption - Public-Key Cryptography

Asymmetric key encryption, also known as public-key cryptography, involves the use of two keys: a public key and a private key. The public key is shared openly and is used for encryption, while the private key is kept secret and is used for decryption. Messages encrypted with the public key can only be decrypted by the corresponding private key, and vice versa. This system allows for secure communication between parties without the need to exchange secret keys beforehand.

6.2 Digital Signature

A digital signature is a cryptographic technique used to verify the authenticity and integrity of a digital message, document, or software. It works by creating a unique digital fingerprint of the content using a hashing algorithm and then encrypting that fingerprint with a private key. The recipient can then use the sender's public key to decrypt the signature and verify both the identity of the sender and that the content has not been altered since the signature was created.

6.3 Secure Hash Algorithm 256 - SHA-256

SHA-256 is a widely-used cryptographic hash function that belongs to the SHA-2 (Secure Hash Algorithm 2) family. It takes an input message of any length and produces a fixed-size (256-bit) hash value, which serves as a unique digital fingerprint of the original data. SHA-256 is designed to be computationally secure, meaning that it is computationally infeasible to generate the same hash value for two different inputs or to reconstruct the original message from its hash value.

6.4 Merkle Hash Tree Algorithm-Merkle Tree

A Merkle tree, named after computer scientist Ralph Merkle, is a hierarchical data structure used to efficiently verify the integrity and consistency of large datasets. It is constructed by recursively hashing pairs of data (or hashes) until a single root hash is obtained, called the Merkle root. Each leaf node of the tree represents a data block, and each non-leaf node is the hash of its child nodes. Merkle trees allow for efficient verification of data integrity by comparing just the root hash, and they are commonly used in distributed systems such as blockchain networks to ensure the consistency of large datasets across multiple nodes.

7. Implementation

7.1 User Registration

Once the User creates an account, they are allowed to login into their account to access the application. Based on the user’s request, the Server will respond to the user. All the user details will be stored in the database of the Server. User and candidate have to register their details along with Aadhaar number.

7.2 Voting Survey

The Server will store the entire voter’s information in their database and verify them if required, also the Server will store the entire voter’s information in their database, also the Server has to establish the connection to communicate with the Users. updating in its database. The Server will authenticate each voter by Aadhar before they access the Application. so that the user can access the Application.

7.3 Data Security

User information’s are encrypted using Advanced encryption standards (AES). Data is encrypted towards security apart from block chain technology. The integration of AES encryption into the E-Voting System enhances data security and confidentiality, complementing the inherent security features provided by blockchain technology. Together, these measures establish a robust and resilient framework for conducting secure and trustworthy elections in the digital age.

7.4 Candidate registration

In this module admin will register the candidate using their Aadhar number. Candidate registration will be made using Aadhar number and constituency of that candidate. If user candidate provide improper information system will discard those registration process. This module not only streamlines the candidate registration process but also reinforces trust and confidence in the electoral system by safeguarding against potential misuse or manipulation of candidate information.

7.5 Block chain formation

The Blockchain Formation module leverages blockchain technology to establish a transparent and tamper-proof ledger for recording voting transactions.

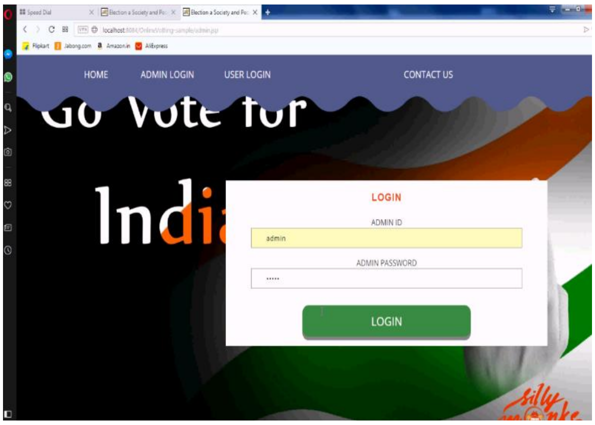
Through decentralized consensus mechanisms, the system ensures the integrity and immutability of the voting data, preventing any unauthorized alterations or manipulations. The blockchain network is designed to scale efficiently, accommodating a high volume of transactions during the voting period while maintaining optimal performance and security. Blockchain Formation module represents a significant advancement in electoral technology, providing a secure, transparent, and efficient framework for conducting elections in the digital age. By leveraging blockchain technology, this module helps safeguard the integrity of the electoral process, ensuring that every vote is accurately recorded and counted.

7.6 Verification

In this project voting system, users will receive an OTP immediately before casting their vote, which serves as confirmation. When a user polls their vote, the system generates and sends an OTP to their registered mobile number. This OTP is crucial for verifying the authentication of the vote. After receiving the OTP, users must confirm their vote by entering it into the system for verification. Once the OTP is confirmed, the system updates the vote in the database, marking it as officially cast by the verified user. This process ensures the security and integrity of the voting process by preventing proxy casting and unauthorized access. By integrating of OTP verification into the voting process, we aim to enhance transparency and accountability, providing users with a secure platform to exercise their voting rights confidently.

8. Experimental Result

This result discuss about the implementation of the Effective Vote from home with polling monitoring.



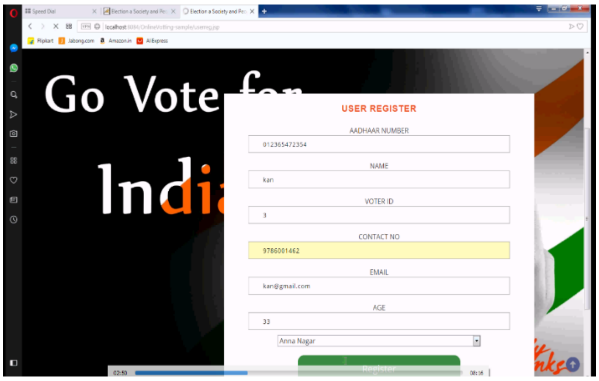
LOGIN

ADMIN ID: admin

ADMIN PASSWORD: •••••

LOGIN

Fig:8.1 User Login



USER REGISTER

AADHAAR NUMBER: 012365472354

NAME: kan

VOTER ID: 3

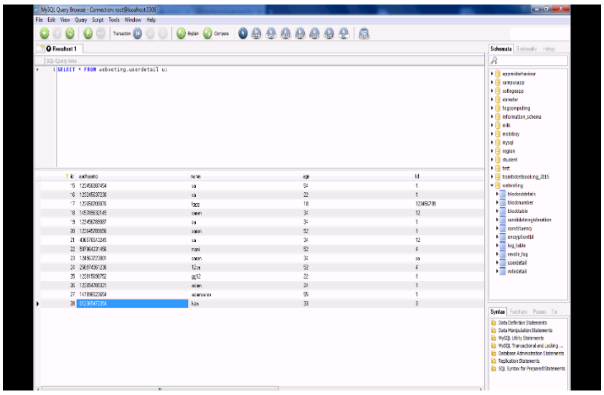
CONTACT NO: 9786001462

EMAIL: kan@gmail.com

AGE: 33

Anna Nagar

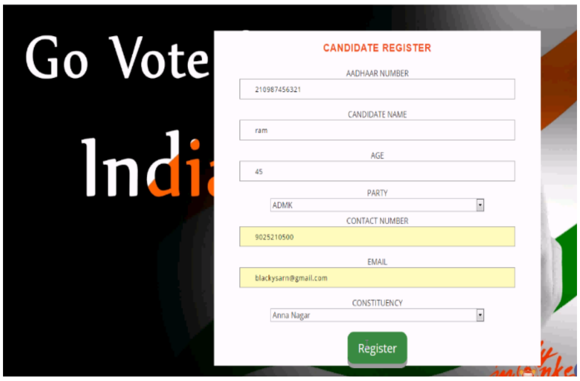
Fig:8.2 User Registration



```
SELECT * FROM webvoting.userdetail u;
```

id	aadhaarno	name	age	vid
15	123456987454	sa	54	1
16	123456987236	sa	22	1
17	123056708076	fggg	18	123456789
18	145789632145	saan	34	12
19	123456789087	sa	34	1
20	123645789656	saan	52	1
21	436578943245	sa	34	12
22	597964231456	mani	52	4
23	124963723801	saan	34	sa
24	258974561236	12sa	52	4
25	123015890752	gg12	22	1
26	123054789321	adam	24	1
27	147896523654	adamsmin	55	1
28	012365472354	kan	33	3

Fig:8.3 Voting survey



CANDIDATE REGISTER

AADHAAR NUMBER: 210987456321

CANDIDATE NAME: ram

AGE: 45

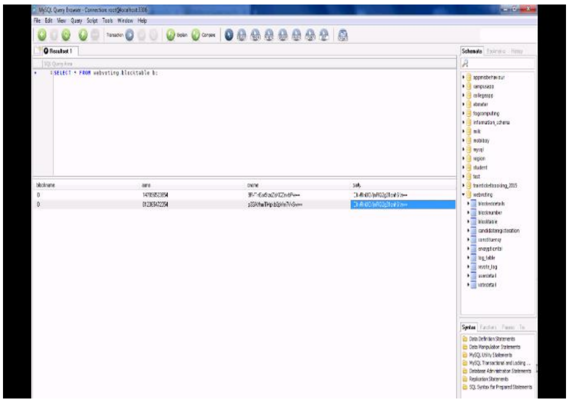
PARTY: ADMK

CONTACT NUMBER: 9025210500

EMAIL: blackysarn@gmail.com

CONSTITUENCY: Anna Nagar

Fig:8.4 Candidate registration



```
SELECT * FROM webvoting.blocktable b;
```

[illegible]	[illegible]	[illegible]	[illegible]
0	[illegible]	[illegible]	[illegible]
0	[illegible]	[illegible]	[illegible]

Fig:8.5 Verification

9. Conclusion & Future Work

E-Voting System represents a pivotal advancement in the realm of electoral technology, offering a transformative solution to address the inherent challenges of traditional voting methods. By leveraging cutting-edge technologies such as blockchain, biometric authentication, and Aadhaar integration, this system ensures the highest standards of security, transparency, and accessibility in the electoral process. Mobile based Voting Application is proposed as Future Enhancement, so that Maximum number of users can cast their Votes, which would increase the Vote casting Percentage. Finger Print based Mobile Interface is also integrated along with Our Application. So the user can cast their votes sitting from anywhere around the world.

10. References

[1] Olaniyi Olayemi M, Arulogun Oladiran T**,** Omidiora Elijah O, Okediran Oladotun, “Performance Assessment of An Imperceptible and Robust Secured E-Voting Model”.

[2] Monira Monir Haroon Khater, “Secure E-Voting System” 2011.

[3] Shalini Shukla, Shashank D O, Thasmiya A N, Dr. Mamatha H R, “Online voting application using Ethereum blockchain” 2018.

[4] Adrià Rodríguez-Pérez, Secret Suffrage in Remote Electronic Voting Systems.

[5] Jens-Matthias Bohli, Christian Henrich, Carmen Kempka, Jörn Müller-Quade, and Stefan Röhrich, “Enhancing Electronic Voting Machines on the Example of Bingo Voting” December 2009.

[6] Salanfe, *Setup your own private Proof-of-Authority Ethereum network with Geth*, Hacker Noon, 2018. Available at: https://tinyurl.com/ y7g362kd.

[7] Geth.ethereum.org. (2018). *Go to the Ethereum.* Available at: https://geth. ethereum.org/

[8] Vitalik Buterin. (2015). *Ethereum White Paper to the* Available at: https: //github.com/Ethereum/wiki/wiki/White-Paper.

[9] Ethdocs.org. (2018). *What is Ethereum? — Ethereum Homestead 0.1 documentation*. [online] Available at: http://ethdocs.org/en/latest/ introduction/what-is-ethereum.html

[10] Agora (2017). *Agora: Bringing our voting systems into 21st century* Available at:https://agora.Vote/Agora_Whitepaper_v 0.1.pdf.

[11] Łukasz Wiktor Olejnik, "Cycles in a cycle: investment expend Ture sand their composition during the political budget army cycle," Local GovernmentStudies,vol.0,no.0,pp.1–32,2021.[Online].

[11] Łukasz Wiktor Olejnik, "Cycles in a cycle: investment expend Ture sand their composition during the political budget recycle," Local of the Indian Government Studies, vol.0, no.0, pp.1–32,2021. [Online]. Available at the website is: HTTPs://doi.org/10.1080/03003930.2020. 1851207.

[12] M.GuinjoanandT.Rodon,title is the pro "Let'sparty! theimpactoflocalfestivities on the incumbent's electoral support," Available: https://doi.org/10.1080/03003930.2020.1771308

[13] A. Kern and P. Amri, "Political credit cycles, "Economics & Politics, vol. 33, no. 1, pp. 76–108, 2021. [Online]. Available: https://doi.org/10.1111/ecpo.12158

[14] G. Wenzel burger, C. Jensen, S. Lee, and C. Arndt, "How government strategically time welfare state reform legislation: empirical evidence from five European countries, "West European Politics, Vol. 43, no. 6, pp. 1285–1314, 2020.

[15] S. Galiani, N. Hajj, P. J. McEwan, P. Ibarrarán, and N. Krishnaswamy , "Voter response to weakhanded transfers: Evidence Oma conditional cash transfer experiment, "American Economic Journal: Economic Policy, Vol. 11, no. 3, pp. 232–60, August 2019. [Online]. Available: HTTPs://www.aeaweb.org/articles?id=10. 1257/pol.2