IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11508

Blockchain Powered Decentralized Voting System

Keerthi Prada S[1], Meghana K S[2], Nagashree M N[3], Nikhita A N[4], Ashwini M S[5]

Student, Computer Science and Engineering, GSSSIETW, Mysore, India[1-4]

Assistant Professor, Computer Science and Engineering GSSSIETW, Mysore,India[5]

Abstract: Blockchain technology is a decentralized and distributed digital ledger system that records transaction across a network of computers. It consists of chain of blocks, each containing a list of data that are linked together in a chronological and unchangeable chain. Blockchain ensures transparency, security, tamper-resistant, consensus mechanisms and immutability of data. A decentralized voting system using blockchain technology is an innovative approach to improve the integrity, security and trustworthy electoral process.

Keywords: E-polling, voting system, blockchain application, blockchain voting, E-voting, electoral system, blockchain, cryptographic hash, secure voting.

I. INTRODUCTION

The term voting, understood to be a form of choices, with varied expression performed through either ballot, or by any other electoral schemes, can be intriguing with the electronic voting. Electronic voting offers a way in which votes cast by voters can be retrieved tallied, and stored electronically.

The focus of the project at hand will be to convert the current paper-based elections system widely employed by the University of Westminster Student Union into an electronic format. The current voting system in use has seen a pessimistic voter turnout due to the inconvenient system in place. With this project, voters will now have the luxury of casting their votes for their desired candidates through an internet-enabled computer.

The project will delve into the existing voting method employed by the student union, seeking methods to integrate the internet voting system seamlessly. The system will implement various election mechanisms for casting votes.

To maintain security, the system will uphold strict security features from the very onset of voter login, throughout voting for their selected candidate, to the exit point. The system will have protective measures in place to prevent voters from multiple voting for election candidates.

The upcoming system needs to address security concerns that arise with voting online. To ensure a secure voting process, authentication, validation of users, access rights, information encryption, and vote security measures will be taken into account thoroughly. The aim is to create a safe environment for online voting.

II. LITERATURE SURVEY

"Digital Forensic Readiness Model for Internet Voting"

Digital forensic readiness it be crucial aspect to ensure security and integrity of internet vote systems. Muyambo and Baror (2023) introducing Digital Forensic Readiness Model for Internet Voting (DFRMIV) at 22nd European Conference on Cyber Warfare and Security. This model aims to enhance the readiness of internet voting systems for effectively responding to potential cyber threats and attacks. By incorporating digital forensic techniques and practices, DFRMIV provides a structured approach to proactively identify, collect, preservation, and analyze digital evidence in the event of security incidents. The DFRMIV proposed by Muyambo and Baror (2023) emphasizes importance of integrating digital forensic readiness into design and implementing internet voting systems. By doing so, organizations can better prepare self to detect and mitigate cyber threats, thereby enhancing overall security posture of their voting infrastructure. The model highlights the need for continuous monitoring, logging, and audit of system activities to facilitate timely incident response and forensic investigation. In addition to DFRMIV, Muyambo and Baror (2023) also discussing use of artificial intelligence (AI) models for digital forensic readiness in cloud. This approach leveraging AI technologies to automate and streamline forensic analysis process, enabling organizations to more efficiently identify and response to security incidents. By combining AI capabilities with traditional forensic techniques, organizations can enhance their ability to detect and mitigate cyber threats in a timely manner. Overall, work presented by Muyambo and Baror (2023) underscores importance of digital forensic readiness in internet voting systems. By adopting a proactive and systematic approach to digital forensics, organizations can better protect the integrity and confidentiality of their voting infrastructure. Moving forward, further research and development in this area are needing to address emerging cyber threats and ensure continued security of internet voting systems.[1]

“Parametric-Based Facial Recognition Technique for Improved Electronic Voting System”.

Facial recognition technology has gained, like, a lot of attention in recent years due to its potential applications in, like, various fields, including electronic voting systems. Okeaham, Otuonye, and Nwanga (2023) like, they proposed a parametric-based facial recognition technique for improving an electronic voting system. This technique aims to enhance the security and accuracy of the voting process by, like, utilizing facial recognition technology. The study by Okeahialam et al. (2023) highlights the importance of incorporating biometric authentication methods, such as facial recognition, in electronic voting systems. By, like, leveraging parametric-based facial recognition techniques, the authors suggest that the voting process can be made, like, more secure and efficient. This approach could potentially address some of the challenges associated with traditional voting systems, such as, like, identity verification and fraud prevention. Furthermore, Okeahialam, Otuonye, and Nwanga (2023) emphasize the significance of face liveness detection in, like, the context of electronic voting systems. By implementing a 3 frames architecture for, like, face liveness detection, the authors aim at, like, enhancing the reliability of the facial recognition technique proposed for the electronic voting system. This approach could help mitigate potential threats, such as spoofing attacks, and ensure the integrity of the voting process. In like, addition, the study by Okeahialam, Otuonye, and Nwanga (2023) underscores, like, the need for a robust voter authentication, like, sequence in electronic voting systems. By integrating parametric-based facial recognition technology into the authentication process, the authors suggest that the overall security and efficiency, like, of the voting system can be improved. This approach could potentially streamline the voter authentication process and, like, enhance the overall voting experience for users. Overall, the research conducted by Okeahialam, Otuonye, and Nwanga (2023) highlights the potential benefits of, like, utilizing parametric-based facial recognition techniques in electronic voting systems. By, like, leveraging advancements in facial recognition technology, such as face liveness detection and, like, robust authentication sequences, the authors propose a novel approach to enhance the security and, like, efficiency of electronic voting systems. Further research in this area could lead to, like, significant advancements in the field of electronic voting and, like, contribute to the development of, like, more secure and reliable voting systems.[2]

“Remote Electronic Voting over the Internet”.

Heinl, Golz, and Bosh (2022) talks about remote electronic voting on the internet. The authors dive into the possible

upsides and downsides connected with implementing such a system. They point out the comfort and accessibility that remote electronic voting can give, letting individuals vote from their own houses. Nevertheless, they also tackle worries about security and the likelihood of fraud in an online voting setup. The authors stress the significance of ensuring the integrity and confidentiality of votes cast electronically. They propose that tough encryption and authentication measures need to be there to shield against cyber threats and protect the democratic process. Moreover, Heinl, Golz, and Bosh (2022) admit the necessity for transparency and accountability in remote electronic voting systems to construct trust among voters and stakeholders. Generally, the authors offer a broad outline of the opportunities and challenges connected with remote electronic voting on the internet. They require more research and development in this field to address security worries and enhance the accessibility of voting processes. By analyzing these issues, Heinl, Golz, and Bosh (2022) contribute useful insights to the ongoing talk on electronic voting systems [3].

“Post-Quantum Secure Identity-Based Proxy Blind Signature Scheme on a Lattice”.

Li et al. (2023) introduces post-quantum securities-based proxy blind signature schematics on a latticework. This schematic aims to simplification key menageries and enhance resistance against quantum attacking by using a matrix cascade technique and latticework cryptosystemology. The security of the suggested schematics is proved under the random Oracle model (ROM). Zhang et al. (2003) suggested an efficient ID-based blind signatory schemer and an ID-based partial delegation proxy signature schemer based on bilinear pairs. They claimed that their blind signature schemer is more efficacious than earlier schemers. Wang et al. (2005) represented two proxy inscription schemers based on

DOI: 10.17148/IARJSET.2024.11508

bilinear pairs. They argued that these schemers are secure in the random Oracle model without needing a securitize channel. Galindo et al. (2006) searched the generic constructing of identity-based signature schematics with additional properties without needing for bilinear pairs. Their workforce implied the existence of securitize identity-based signatures with additional properties based on general assumptions. Sahu et al. (2015) introduces an identity-based multi-proxy signature schemer and formalizes a securitize model for such schemers. They prove the securities of their schemer against choosen message and ID attacks in the random Oracle model. Zhang et al. (2015) suggest an identity-based proxy-encryption schemer from lattice assumptions in the random Oracle model. This scheme combines the functionalities of proxy signature with identity-based inscription. Zhu et al. (2018) development of an identity-based proxy blind signature schemer based on the Ring-Small Integer Solution problem over the number theorem research unit latticework. This scheme is designed to resist quantum computer attacks without relying on public key infrastructure. In conclusion, the literature reviews highlight the development of various identity-based signature schematics, including blind signatures, proxy signatures, and proxy signcryption schemers, based on different cryptographic assumptions such as bilinear pairs, latticework assumptions, and number theorem research unit latticework. The focus on post-quantum securities and efficient key menageries is evident in the suggested schematics [4].

“Online Voting System by Using Three Step Verification” .

The adoption of e-voting services has been an topic of interest for researchers, particularly in understanding the factors that influence young voters' intention to use online voting systems (Schapp et al., 2005). With an increase use of online for various purposes, including paper submissions and reviews for conferences, the security features of such systems have been an focus of analysis (Lo et al., 2007). Additionally, the growth of e-commerce and the number of Intrenet users worldwide have raised questions about the correlation between website usable and usage (Downing et al., 2009). Security challenges in critical web applications, such as online voting systems, have been highlighted, emphasizing the importance of following the latest vulnerability mitigation guidelines (Heiderich et al., 2011). To ensure robustness in verifiable voting systems, new protocols have been proposed, such as a peered bulletin board implementation for the vote system (Culnane et al., 2014). Furthermore, advancements in online signature verification systems have been made by incorporating contextual information and utilizing dynamic time warping based on vector quantization strategies (Sharma et al., 2016). Recent research has also explored e-voting systems with different verification methods, such as two-step verification using machine learning (Lakshmi et al., 2023). These advancements aim to address concerns about voter confidentiality and electoral fraud schemes associated with traditional paper ballots (Lakshmi et al., 2023). Overall, the literature review highlights the ongoing efforts to enhance the security, usability, and robustness of online voting systems, emphasizing the importance of incorporating advanced verification methods to ensure the integrity of the voting process[5].

“Smart voting through face recognition”.

Smart vote through face recognition are an emerging technology that has potential to revolutionize vote process. Vashisht, Mohan, and Prakash (2022) discussing concept of smart vote through face recognition, highlighting benefits and implications. This technology could streamline vote process, enhance security, and improve accessibility for voters. While use of face recognition technology in vote systems are a novel idea, its implementation raises concerns about privacy and data. Vashis, Mohan, and Prakash (2022) emphasizing importance of addressing these issues to ensure integrity of vote process. Additionally, authors suggest further research is needed to explore full potential of smart voting through face recognition. In related study, Vashisht, Mohan, and Prakash (2022) highlighting need for robust authentication mechanisms in vote systems to prevent fraud and ensure accuracy of election results. They propose use of face recognition technology as secure and efficient way to verify voters' identities. Overall, research by Vashisht, Mohan, and Prakash (2022) underscores potential of smart voting through face recognition to transform electoral process. However, it also emphasizes importance of addressing privacy and security concerns to ensure trustworthiness of such systems. Further research in this area is needed to fully explore implications and applications of this technology in vote systems[6].

“Secure Electronic Voting Machine using Multi-Modal Biometric Authentication System, Data Encryption, and Firewall”.

The technology has developmental security concerning in the present voting system, including issue's like EVM tampering and fraudulent activities! Address this challenging, researchers has proposed various secure electronic voting system's. Rannels et al. (2017) develops an Aadhar-based electronic voting system used biometric authentications to prevent election riggings. Chakrabarti et al. (2018) suggest an secure voting system used UIDAI data and IoT to authenticating voters and save voting statistics via VMAC encryptions. Babenko et al. (2018) introducing a distribute e-voting system with blinds intermediaries and homomorphic encryptions to ensure user authentications and

DOI: 10.17148/IARJSET.2024.11508

Anonymouses. Umar et al. (2019) proposes a fingerprint biometric authentication systems for secure electronic voting machining to combat present challenges. Jasdev Bhatti (2019) presents a secure electronic voting machining used multi-modal biometric authentication, data encryption's, and firewall to withstand malicious attacking and fraudulent behaviors. Chakraborty et al. (2021) designing a biometric fingerprint scanner-based secure electronic voting machining to ensure a secure election process. These study's highlights the importance of implementing robusticity security measures, such as biometric authentications, data encryption's, and firewall, to enhance the trustworthy of citizens in the election process and prevent tamper's and fake voting[7].

"Post-Quantum Crystography System for Secure Electronic Voting 2019".

Arone Junior Gabriel (2019) discussion the implements of a Post-Quantum Cryptography System for Secures Electronic Voting. The author highlight the importance of utilized post-quantum computing techniques to enhances the securities of electronic voting systems.The usage of post-quantum cryptography in electronic voting systems are crucial in safeguarded sensitives voter information and preventing unauthorized access to voting data's. By incorporates advanced cryptographic techniques, such as quantum-resistant algorithmics, electronic voting systems can better protecting against potential cyber threats and attacking! Overall, Gabriel (2019) emphasis the significancy of implements a robust Post-Quantum Cryptography System for Secure Electronic Voting to ensure the trustworthiness and reliabilities off the electoral processes. This research contribute to the ongoing effort to enhances the securities of electronic voting systems and mitigate potential vulnerabilities associated with traditional cryptographic methods[8].

III. METHODOLOGY

Research and Need Gatherment start at fully researching existing vote systems, blockchain technology, and relevant regulations.

Design: Develop the system infrastructure based on the needed gatherments. This includes selectivizing an appropriate blockchain platform (e.g., Ethereum, Hyperish), designating the voting method, determinating the agreement mechanism (e.g., Proof of Working, Proof of Staking), and outlinizing the general system workflow.

Develop: Coding the smart contracts, user interfaces, and backend structure according to the designed framework. Assure that the system can securely manage voter authenticating, ballot creatation, vote casking, and tallyation.

Deploying: Deploy the blockchain webs, containing setting up knots and deployment smart contracts. Assure that the webs are decentralized to avoid singular points of failure and intensify resistantness against assaults.

Teaching and Edification: Provide training and edifying materials to stakeholders, including election squads, voters, and technical crew, to make them acquaint with the voting system's characteristics and operation.

Collaboration and Pliance: Work closely with relevant stakeholders, including government tenebrations and election squads, to secure compliance with regulative demands and address any worries or challenges that may occur.

Monitoring and Reparations: Implement mechanisms for continuous monitoring, maintenance, and updates to the voting method. Regularly audit the method for security frailties and make needed improvements to secure its long-term efficiency and security.

IV. ALGORITHMS USED

SHA512 Algorithm

Cryptography is a fascinating technique used to secure communication across networks. One of the prominent cryptographic hash functions is SHA-512, which creates a unique 512-bit hash value. This hashing algorithm plays a crucial role in data security, providing a robust method for protecting sensitive information.

Using SHA-512 involves taking an input message and processing through a series of complex mathematical operations. The resulting hash is a fixed-length string that represents the original data.

Even the slightest change in the input message will produce a vastly different hash value, making it practically impossible to reverse-engineer the original information. The hexadecimal representation of the SHA-512 hash is typically 128 characters long, providing a high degree of cryptographic security. This makes SHA-512 an ideal choice for verifying

DOI: 10.17148/IARJSET.2024.11508

data integrity and ensuring that information has not been tampered with.

In conclusion, SHA-512 is a powerful tool in the field of cryptography, offering a robust and reliable method for securing data. Whether you are transmitting sensitive information over the internet or storing confidential files, SHA-512 can provide the protection you need to keep your data safe and secure.

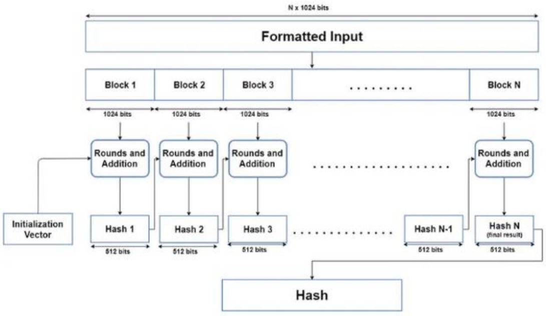


Figure: 1024 Bit blocks in SHA Algorithm

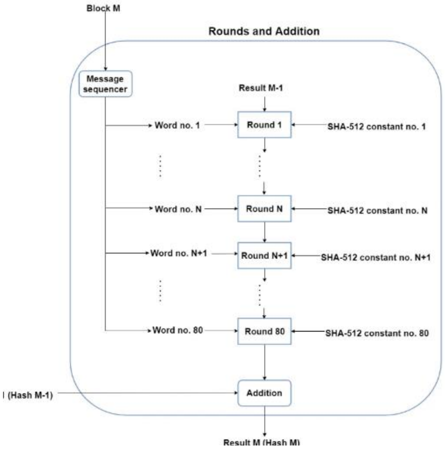


Figure: Rounds and additions in SHA Algorithm

V. SOFTWARE REQUIREMENTS

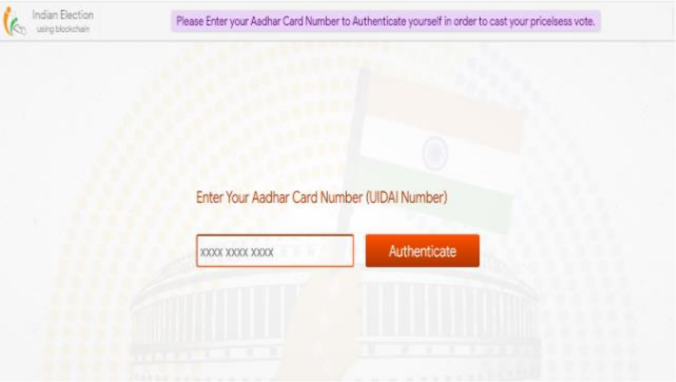
OPERATING SYSTEM	**WINDOWS**
LANGUAGE	PYTHON, SQL
DATABASE	MYSQL
IDE	VSCODE

VI. RESULTS

The point of proposing a blockchain-supported resolution for the vocation system were to construct trust within the government and voters to fictitiously pretend that their voting integrity is kept safe. The blocking chain-based voting also assembles the voting process transparent and trustworthy! The amount of money spent on voting activity in any country is very high for the traditional voting system whereas the propound solution for using the blockchain voting systems to make the voting process cheaper, faster, and trustworthy. It assists to enhance people relations with their democratic state; as they get a clear system on which they can rely and trust. The framework elaborates on the features,

DOI: 10.17148/IARJSET.2024.11508

services, and roles of aforesaid official authorities using the blockade in the voting system which is greatly in need to improve the level of the elective system and its repute, traceability, and trust. The checking of each vote makes it immutably. The use of hash reassures the privacy of voters and the concept of public and private keys enables the authorities to control the process precisely. The traceability of the voting system assists in preventing hackers from modifying or viewing the voting information! It assures that a single voter only votes one vote. The usability of this system perform well by using the more effective approach of implementing a flexible consensual algorithm to reduce extensive computing resources in the blockade. This transparent behavior of the system tends to be promising for vocation to rely and trust. The Chain Security Algorithm is also added, which automatically checks the validness of the chain each time a new block is added to it! Smart Contracts play an important role to prevent any incomplete and malicious transactions in the blockade voting system! The propound system is a secure, transparent and reliable platform for the authorities and voters. The propound framework has a promising output based on the performance evaluation of the blockade technology in VMS. The experiment shows that the system keeps processing efficiently while processing a large volume of transactions in the blockade.

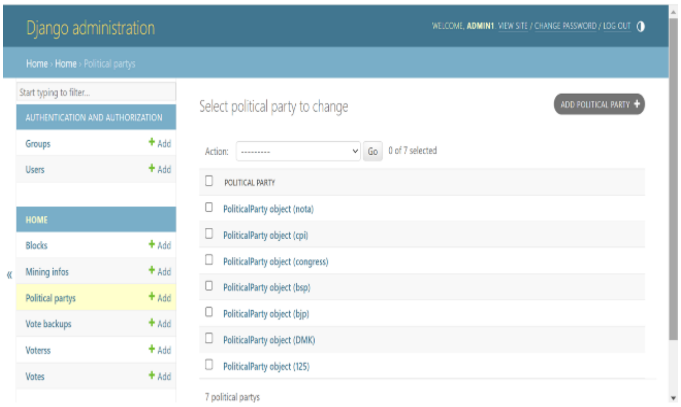


Please Enter your Aadhar Card Number to Authenticate yourself in order to cast your pricelsess vote.

Enter Your Aadhar Card Number (UIDAI Number)

XXXX XXXX XXXX

Snapshot: Login Page for Voter



Select political party to change

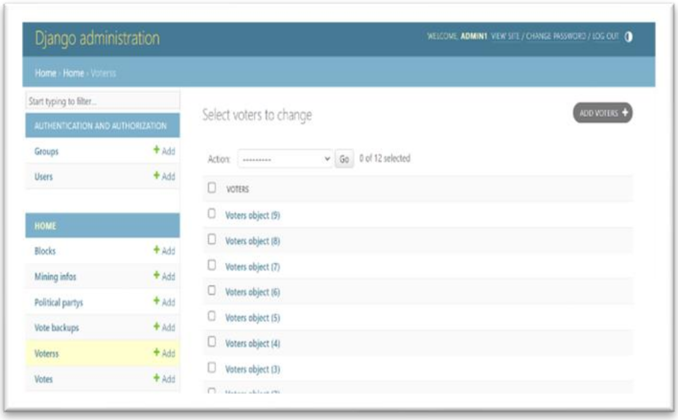
Action: ---------

0 of 7 selected

☐ POLITICAL PARTY
☐ PoliticalParty object (nota)
☐ PoliticalParty object (cpi)
☐ PoliticalParty object (congress)
☐ PoliticalParty object (bsp)
☐ PoliticalParty object (bjp)
☐ PoliticalParty object (DMK)
☐ PoliticalParty object (125)

7 political partys

Snapshot: Add and update page of political party



Snapshot: Add and update page of Voters

VII. CONCLUSION

The system will feature an intuitive and user-friendly interface accessible to administrators, doctors, and patients. Each user will have a personalized navigation tailored to their specific role and responsibilities within the healthcare ecosystem.Patients will be able to easily schedule appointments through the system, selecting their preferred doctor, date, and time slot from the available options. The system will check for conflicts in the doctor's schedule and notify patients of any conflictsThe system will maintain electronic health records for each patient, storing information such as medical history, diagnosis. Doctors can easily access and update patient records during appointments.

REFERENCES

[1] Digital Forensic Readiness Model for Internet Voting- Muyambo, Edmore, Baror, Stacy Omeleze- European Conference on Cyber Warfare and Security-2023
[2] Parametric-Based Facial Recognition Technique for Improved Electronic Voting System -Udochukwu Okeahialam, Anthony I. Otuonye, Mathew E. Nwanga-2023
[3]Remote Electronic Voting over the Internet Michael P Heinl, Simon Golz, Christoph Bosh- Dec2022
[4] Smart Voting System Through Face Recognition-2022 4th International Conference on Advances in Computing, Communication Control and Networking(ICAC3N).
[5] An Analytical View on Political Voting System using Blockchain Technology-UAE Case Study-2020.
[6] Post-Quantum Crystography System for Secure Electronic Voting-2019.
[7] Secure Electronic Voting Machine using Multi-Modal Biometric Authentication System, Data Encryption, and Firewall – Jasdev Bhatti, Satvik Chachra, Ansh Walia.