ELECTRONIC VOTING SYSTEM USING FACE RECOGNITION WITH BLOCKCHAIN TECHNOLOGY

N.KANNAN, M.Tech.,
Assistant Professor
Department of Computer Science and Engineering
E.G.S.PillayEngineering college(Autonomous),
Nagapattinam, India
kanna8890@gmail.com

M.MATHANKUMAR
Department of Computer Science and Engineering
E.G.S.Pillay Engineering college(Autonomous),
Nagapattinam,
mathankumar2k21@gmail.com

G.MULLAIVENTHAN
Department of Computer Science and Engineering
*E.G.S.Pillay Engineering College(*Autonomous),
Nagapattinam, India
suryacpm2002@gmail.com

B.NIVASHKANNA
Department of Computer Science and Engineering
E.G.S.Pillay Engineering college(Autonomous),
Nagapattinam, India
ksbnivash2000@gmail.com

ABSTRACT

The security considerations of the votes are based on blockchain technology using cryptographic hashes to secure end-to-end verification. To this end, a successful vote cast is considered as a transaction within the blockchain of the voting application. Therefore, a vote cast is added as a new block (after successful mining) in the blockchain as well as being recorded in data tables at the backend of the database. The system ensures only one-person, one-vote (democracy) property of voting systems. This is achieved by using the voter's unique face image, which is matched at the beginning of every voting attempt to prevent double voting. The Face Recognition is the study of physical or behavioural characteristics of human being used for the identification of person. So implement real time authentication system using face biometrics for authorized the person for online voting system. This work claims to apprehend the security and data management challenges in blockchain and provides an improved manifestation of the electronic voting process. A transaction is generated as soon as the vote is mined by the miners which are unique for each vote. If the vote is found malicious it is rejected by miners. After validation process, a notification is immediately sent to the voter through message or an email providing the above defined transaction id by which user can track his/her vote into the ledger. Although this functions as a notification to the voter however it does not enable any user to extract the information about how a specific voter voted thereby achieving privacy of a voter. It is important here to note that cryptographic hash for a voter is the unique hash of voter by which voter is known in the blockchain. This property facilitates achieving verifiability of the overall voting process. Furthermore, this id is hidden and no one can view it even a system operator cannot view this hash therefore achieving privacy of individual voters.

KEYWORDS: *Electronic Voting System, Face Recognition, Blockchain Technology, Voting Security,Biometric Authentication, Decentralization, Transparency, Immutable Ledger, Identity Verification, Fraud Prevention, Privacy Preservation, Voter Authentication, Consensus Mechanism, Smart Contracts, Trust and Integrity, Distributed Ledger, Data Encryption, Voter Anonymity, Auditability, Tamper Resistance.*

1. INTRODUCTION

Electronic voting is becoming increasingly popular as a solution to eliminate inefficiencies and redundancies in the paper-based voting system. In a number of countries, electronic voting systems have recently gained popularity. To compete with the traditional ballot method, an electronic vote casting system must have the same security and anonymity features as the traditional system. To ensure that it is available to voters while simultaneously protecting from outside forces changing votes or tampering with a voter's ballot, an e-Voting system must have better security. Many electronic voting systems are meant to keep the identity of voters hidden. This technique, however, does not guarantee perfect anonymity or integrity because many intelligence services across the world control different portions of the Internet and can discover or intercept ballots. The historical perspective presented in the last two decades shows that it has not been as effective due to security and privacy issues uncovered throughout time. The study of an individual's physical or behavioural attributes that are used to identify them is known as face recognition. The physical characteristics of a person include fingerprints, face, hand geometry, voice, and an iris biometric device, to name a few. Create a real-time

authentication system that leverages face biometrics to authorize people to vote online as a result of this. The goal of this study is to better understand the security and data management challenges in block chain, as well as to improve the appearance of the electronic voting process. In the e-Voting system, there should be no connections between voters' identities and ballots. The voter must remain anonymous during the voting process and after the election. The results of the vote must be correct. Every vote should be counted, and no votes should be changed, duplicated, or eliminated. The mechanism must be verified in order to ensure that all votes are counted efficiently. In addition to meeting the primary demand, our approach improves mobility, flexibility, and efficiency. The system, on the other hand, will limit the discussion in this work to the four most important needs. The capacity to reduce fraud while making the voting process traceable and verifiable can be achieved by replacing the existing pen and paper method with a new election system

RELATED WORK

BLOCK CHAIN

Blockchain is a decentralised, immutable ledger that makes it easier to track assets and record transactions in a business network. Through the use of a decentralised network and cryptographic hashing, blockchain, also known as distributed ledger technology (DLT), makes the history of any digital asset transparent and unalterable.
It's easy to understand how blockchain technology works by making the comparison to a Google

Docs document. A Google Doc is not copied or transferred when it is shared with a group of people;
rather, it is simply distributed. As a result, a decentralised distribution network is established, allowing everyone to simultaneously access the base document. All modifications to the document are being recorded in real-time, making changes completely transparent, and no one is locked out while waiting for changes from another party. The fact that original content and data on the blockchain cannot be modified after being written, increasing its level of security, represents a significant gap to be aware of.
Decentralization is one of the key ideas behind blockchain technology. The chain cannot be owned by any one computer or organisation. Instead, it functions as a distributed ledger through the chain's chain of nodes. Any type of electronic device that keeps copies of the chain and keeps the network running can be a blockchain node. Every node has a unique copy of the blockchain, and for the chain to be updated, trusted, and verified, the network must algorithmically approve every newly mined block. Due to the transparency of blockchains, every transaction in the ledger can be easily verified and viewed, resulting in built-in blockchain security. An exclusive alphanumeric identification number is given to each participant, and this number displays their transactions.
The blockchain is able to maintain integrity and foster user trust by fusing public information with a system of checks and balances. Blockchains are essentially the scalability of trust through technology.

DATA SECURITY

Data structures created by blockchain technology have built-in security features. It is founded on cryptographic, decentralised, and consensus principles that uphold the integrity of transactions. The data is organised into blocks in the majority of blockchains or distributed ledger technologies (DLT), and each block contains a transaction or collection of transactions. In a cryptographic chain, each new block is connected to all the blocks that came before it in a way that makes tampering with it nearly impossible. A consensus mechanism verifies and accepts each transaction contained within the blocks, ensuring that each transaction is accurate and true. As a participant in a members-only network, you can use blockchain to ensure that the information you receive is accurate and timely and that only network participants you have explicitly granted access to will have access to your private blockchain records. All network participants must agree that the data is accurate, and since all validated transactions are permanently recorded, they cannot be changed. A transaction cannot be deleted by anyone, not even a system administrator. Time-consuming record reconciliations are eliminated by using a distributed ledger that is shared among network participants. Additionally, a set of instructions known as a smart contract can be saved on the blockchain and carried out automatically to speed up transactions. A set of instructions known as a smart contract is saved on the blockchain and automatically carried out to speed up transactions. A smart contract can specify terms for corporate bond transfers, stipulate how much must be paid for travel insurance, and much more. In response to the fulfilment of specific requirements, smart contracts are computer programmes or protocols for automated transactions that are stored on a blockchain. In other words, smart contracts automate the execution of contracts so that all parties can quickly ascertain the result without the need for a middleman or a waiting period. Self-executing contracts known as "**smart contracts**" are those in

which the terms of the buyer-seller contract are written directly into lines of code. Utilizing it makes the transactions transparent, irreversible, and traceable.

LITERATURE SURVEY

TITLE: A SECURE END-TO-END VERIFIABLE INTERNET-VOTING SYSTEM USING IDENTITY-BASED BLIND SIGNATURE AUTHOR NAME: MAHENDER KUMAR DESCRIPTION:

End-to-end (E2E) verification allows voters to confirm that their votes are recorded as they intended and the general public to confirm that the system has accurately tallied all of the recorded votes. The security of the E2E verifiability-based Internet voting systems faces numerous difficulties, with security ranking as the most significant. In order to analyse the e-voting system and formalise its security needs, a number of E2E voting systems have been discussed over the past ten years. This article introduces an E2E verifiable internet voting system that gives voters mobility and enables them to covertly cast their ballots on public computers while enjoying the advantages of early voting. The suggested technology makes use of the voter's distinctive identification and biometric characteristics to help the electoral process globally. We suggest a brand-new identity-based blind signing system that guarantees the voter's privacy. We use the Boneh-Lynn-Shacham short signature technique, which protects the confidentiality of votes while using a small ballot size. The technology gives each voter a digital witness that allows them to verify that their vote was recorded as they intended and the general public to verify that all recorded ballots were correctly counted. Under the well-known elliptic curve discrete logarithm and gap Diffie-Hellman assumptions, the proposed system achieves privacy.

TITLE: WE VOTING: BLOCKCHAIN-BASED WEIGHTED E-VOTING WITH VOTER ANONYMITY AND USABILITY AUTHOR NAME: ZIKAI WANG DESCRIPTION

E-voting is essential for ensuring and advancing social justice and democracy. However, traditional e-voting systems rely on a centralised structure, which causes a crisis of confidence in the results of the vote-counting. Researchers have developed blockchain to enable decentralised e-voting in response to this issue, but doing so also raises additional problems with regard to flexibility, privacy, and usability. WeVoting, which offers weight based flexibility with strong anonymity and improves usability by inventing a voter-independent on-chain counting mechanism, is the solution we suggest in this work. To accomplish voting anonymity with weight, we specifically use distributed ElGamal homomorphic encryption and zero-knowledge proof. Additionally, WeVoting creates a counterbased counting mechanism in place of those self-tallying systems in order to improve usability. We Voting can ensure a proper counting outcome even in the presence of dishonest counters by carefully creating an honesty-and-activity-based reward system. We Voting achieves strong anonymity in weighted voting, according to our security and performance evaluations, on the assumption that it satisfies the essential security standards for electronic voting. Additionally, its counting system has reasonable overhead and is adequate for practical needs.

TITLE: AVECVOTING: ANONYMOUS AND VERIFIABLE E-VOTING WITH UNTRUSTWORTHY COUNTERS ON BLOCKCHAIN AUTHOR NAME: MEIQI LI DESCRIPTION

E-voting is essential to contemporary social life .Traditional e-voting systems, on the other hand, frequently rely on a reliable third party, making them non-verifiable and vulnerable to a single point of failure. Many researchers have attempted to use blockchain in recent years to fix the flaws in e-voting systems. Blockchain-based electronic voting, however, has a significant negative impact on performance and introduces new issues with maintaining the confidentiality of ballots and the privacy of voters. In this work, we suggest AvecVoting, a highly secure and efficient blockchainbased anonymous and verifiable e-voting mechanism. To specifically safeguard voters' privacy and the secrecy of ballots, we employ threshold encryption and one-time ring signing. Additionally, we introduce the term "counter" to count the votes in order to improve performance. The reputationbased PayOff algorithms based on smart contracts and the carefully crafted RandomSortition algorithms allow AvecVoting to achieve accurate counting regardless of whether some counters are unreliable.Our safety and efficacy analyses demonstrate that AvecVoting offers high security features like anonymity, non-repeatability, secrecy, verifiability, etc., while also resolving blockchain-related performance difficulties and offering good efficiency during the voting and counting stages.

TITLE: BIEVOTE: A BIOMETRIC IDENTIFICATION ENABLED BLOCKCHAIN-BASED SECURE AND TRANSPARENT VOTING FRAMEWORK AUTHOR NAME: MD JOBAIR HOSSAIN FARUK DESCRIPTION

In this study, we look into the current developments in voting technology, including online voting and potential applications for blockchain and biometric voting systems. We conclude from the literature assessment that the current electronic voting system poses questions about global confidence, security, and transparency. So, in order to address the issue, we propose a biometricenabled and hyperledger fabric-based architectural framework for e-Voting applications. This framework will automate identity verification. We want to implement the system in a real-world setting and give a high-level architectural framework as part of our extension effort. Traditional voting methods use paper ballots and a manual mechanism, which raises a number of security issues. In this essay, we've looked at the present state of voting technology development and security concerns. We also shared a proposed architectural model for a voting application that combined blockchain and biometrics, two cutting-edge technologies.

EXISTING SYSTEM

In existing system, if you wish to vote for someone, then you have to go to the destination where the voting procedure is going on and then only you can vote for him or her. In existing system the results will be modified easily by third parties. There is no way to protect data in server. Server can be hacked by third parties and fake results will be announced easily. So the existing approach does not provide trusted environment for online voting process. The voter has to visit Booths to vote a candidate so there is wastage of time. The voter has to manually register into the voter list. Also vote counting has to be done manually. Voter must be present in his/her constituency to give his/her vote. In current system after voting if any technical problem or damage occurs with the machines it may leads to the re election.

PROPOSED SYSTEM

To implement an e-voting scheme based on blockchain technology that meets the fundamental evoting properties whilst, at the same time, provides a degree of decentralisation and places as much control of the process in the hands of the voters as was deemed possible. The system has been designed to support a bio-metric verification based voting application in the real world environment taking into account specific requirements such as privacy, eligibility, convenience, receipt-freeness and verifiability. The proposed system aims to achieve secure digital voting without compromising its usability with the help of blockchain technology. Within this context, the system is designed using a web-based interface to facilitate user engagement with measures such as face recognition to protect against fake and double voting. With a clear need to administer the voters, constituencies and candidates for constituencies, a user-friendly administrator interface is implementing to enable ease of access

ADVANTAGES

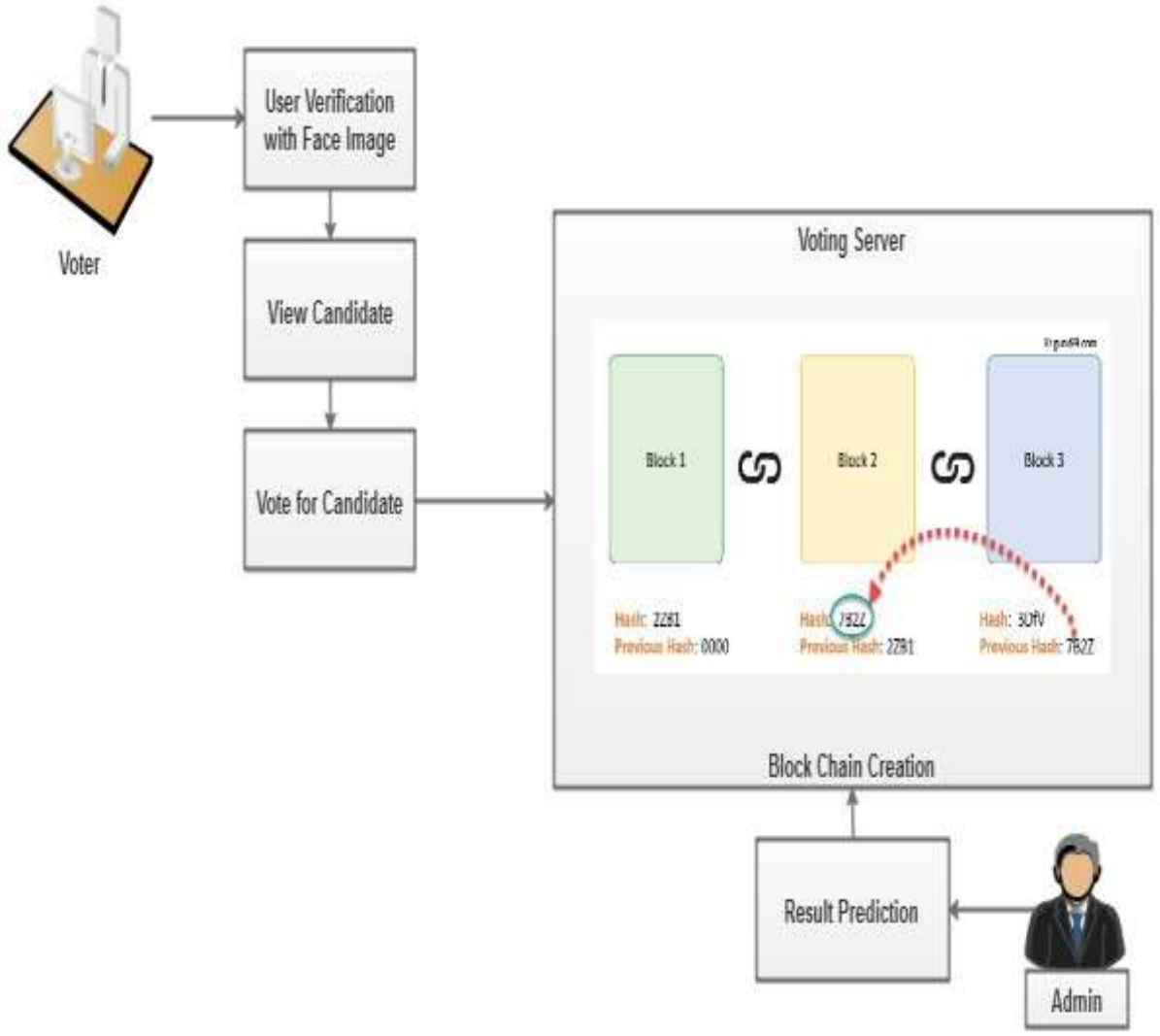
- Elimination of error handling through real-time tracking of voting result with no double spending.
- The block chain guarantees traceability and non-degradability of information.
- It decreases the success rate of attackers.
- It provides security, transparency and efficiency.

- **ALGORITHM SHA Algorithm**

- The SHA (Secure Hash Algorithm) family of cryptographic hash functions are used to generate fixed-length outputs from inputs of variable length. The most commonly used SHA algorithms are SHA-1, SHA-256, SHA-384, and SHA-512. Here are the basic steps involved in the SHA algorithm:

- **Padding**: The input message is padded with a bit sequence to make its length a multiple of 512 bits (for SHA-1 and SHA-256) or 1024 bits (for SHA-384 and SHA-512). The padding includes a length field that specifies the length of the original message.
- **Initialization**: The algorithm initializes a set of constants and variables known as the "initial hash value" or "intermediate hash value".
- **Message Processing**: The message is processed in 256-bit blocks. For each block, the algorithm performs a series of operations on the block and the intermediate hash value. These operations include bitwise operations (AND, OR, XOR), modular arithmetic, and logical functions (rotations, shifts).
- **Finalization**: After all the blocks have been processed, the final hash value is calculated by appending a few more bits to the processed message and performing one last round of operations.
- **Output**: The final hash value is output as a fixed-length string of bits. This value is unique to the input message, meaning that any change in the input message will produce a completely different hash value.

- **ARCHITECTURDIAGRAM**



Experimental Results

CONCLUSION

This online voting system using block chain technology will manage the voter's information by which voter can login and use his voting rights. The system will incorporate all features of voting system. It provides the tools for maintaining voter's vote to every party and it count total no. of votes of every party. There is a database which is maintained by the election commission of India in which all the names of voter with complete information is stored. Voting detail store in database and the result is displayed by calculation. By online voting system percentage of voting is increases. It decreases the cost and time of voting process. In proposed voting system no one can make changes without the knowledge of hash value. This will improve the performance with reduced error rate.

REFERENCES

[1] Kumar, Mahender, Satish Chand, and Chittaranjan Padmanabha Katti. "A secure end-to-end verifiable internet-voting system using identity-based blind signature." IEEE Systems Journal 14.2 (2020): 2032-2041.

[2] Wang, Zikai, et al. "WeVoting: Blockchain-based Weighted E-Voting with Voter Anonymity and Usability." GLOBECOM 2022-2022 IEEE Global Communications Conference. IEEE, 2022. [3] Li, Meiqi, et al. "AvecVoting: Anonymous and verifiable E-voting with untrustworthy counters on blockchain." ICC 2022-IEEE International Conference on Communications. IEEE, 2022.

[4] Faruk, Md Jobair Hossain, et al. "Bie Vote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework." 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA). IEEE, 2022.

[5] Ibitoye, Ayodeji Olusegun, Halleluyah O. Aworinde, and Esther T. Adekunle. "An enhanced multi-level authentication electronic voting system." International Journal of Applied Sciences and Smart Technologies 4.2 (2022): 149-158.

[6] Neeru, Pathak, et al. "BIOMETRIC BASED ELECTRONIC VOTING SYSTEM." (2020).

[7] Farooq, Muhammad Shoaib, Misbah Khan, and Adnan Abid., A framework to make charity collection transparent and auditable using blockchain technology, 2020

[8] Ajish, S., and K. S. AnilKumar. Secure mobile internet voting system using biometric authentication and wavelet based AES, 2021

[9]. Abayomi-Zannu, T. P., I. A. Odun-Ayo, and T. F. Barka. , A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication, 2019

[10]. Ajish, S., and K. S. Anil Kumar, Secure I-Voting System with Modified Voting and Verification Protocol, 2020