International Journal of Science and Engineering Applications
Volume 12-Issue 05, 105 - 113, 2023, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1205.1029

# Smart Voting Platform (Secured Digital Voting System) Uses Blockchain Technology and Biometric Authentication

K.Dilshi Divya
Department of Information Technology
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

W.M.M.G.B.Senarathne
Department of Information Technology
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Thirukkumaran.S
Department of Information Technology
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

P.V.D.Prathibha
Department of Information Technology
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Chethana Liyanapathirana
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Lakmal Rupasinghe
Department of Computer System Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

**Abstract**: — At present, the development of information technology has invaded all the fields of the world. Among them, blockchain technology holds a special place and it is currently used in areas that require high security. Also, the election process is an area that needs a very high level of security. When the present. there are lots of online voting applications available in the world. But developing countries like Sri Lanka did not use online platforms for the public election process until they used the paper-based voting method for the general election. Because online platforms have many issues and will be based on countries inside situations. Therefore, through this research, we are trying to find solutions to those issues and develop a new platform for the electronic voting process by using blockchain technology.

**Keywords**: E-Voting, Smart Contracts, Smart Voting Platform, Ethereum, Blockchain, Decentralized, Ballot, Biometrics.

## 1. INTRODUCTION

Voting is a major factor that Speaks about a person's citizenship. In Sri Lanka, elections are held every five years to elect the President, provincial and parliament members, as well as municipal officials and provincial council members. These elections are a fundamental aspect of a democratic society as they allow eligible citizens to choose their representatives at all levels of government. The right to vote is crucial in ensuring that the public's interests are represented. Thus, voting forms the foundation of democracy. Trust is the foundation of voting. However, people's trust has recently diminished. The outcomes of voting events in centralized settings have always been debatable and subject to differing voter perceptions. The majority of current electronic voting systems rely on centralized servers, which requires voters to trust the organizers to ensure the accuracy of results. To address this trust issue, we propose a decentralized voting platform that utilizes blockchain technology. This platform ensures data transparency and integrity, while also enforcing one vote per cell phone number for each poll, all while maintaining privacy. Organizers for each voting event will implement smart contracts on the Ethereum Virtual Machine, which provides a consistent and deterministic runtime environment. Automated biometric fingerprint identification is widely considered as the most dependable biometric technology in use today. It is proposed that this system be used to replace the conventional paper-based voting process. This electronic voting system is seen as the optimal solution in light of the current circumstances in the country. Several democratic countries have already transitioned to electronic voting systems due to the numerous issues that have arisen in the traditional paper-based voting system Blockchain technology guarantees data immutability and decentralization, without a single point of failure.

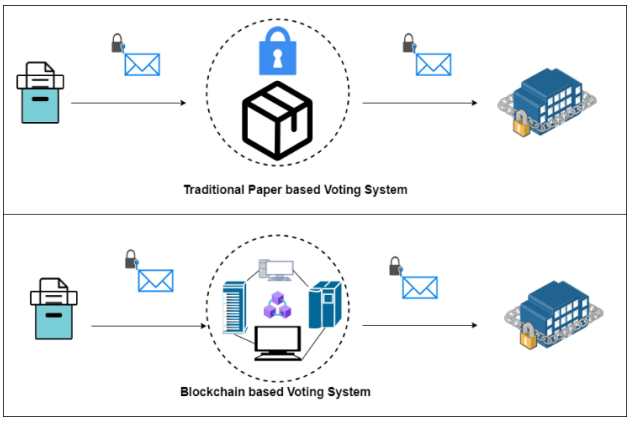


***Figure1: Blockchain base system vs Traditional voting system***

Developers can create decentralized apps (DApps) on the Ethereum Blockchain, taking advantage of its distributed computing capabilities. DApps will include features such as high data integrity, decentralized validation and control,

International Journal of Science and Engineering Applications
Volume 12-Issue 05, 99 - 104, 2023, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1205.1029

transparency, and public business rules, which will make the platform highly accessible

1. High levels of data integrity.
2. Decentralized validation and control using consensus procedures.
3. The runtime environment that is transparent.
4. Public business rules that are active in the run-time setting.
5. High accessibility and High data transparency

For our decentralized smart e-voting system, we'll utilize a similar structure to guarantee complete decentralization of the entire procedure. Decentralized voting demands that every step of the voting process, including voter identification, vote casting, vote reading, and winner announcement, be carried out independently. The voting process should be more independent of any predefined voting procedure, and it should be able to handle many voting processes using a generic voting system and smart contract concepts.

## 2. BACKGROUND

The immutable nature of blockchain allows for secure record-keeping. Smart contracts, which are blockchain-based applications, receive and process incoming data. The validation nodes reach a consensus on the accuracy of the ledger's version. The use of blockchain technology ensures that the integrity of transactions is reliably certified. An example of this is the creation of the first blockchain-based application with Bitcoin by Satoshi Nakamoto. [6].The Ethereum Blockchain is a distributed, decentralized, and open-source computing infrastructure that facilitates the execution of smart contract software. This technology allows for decentralization not just for digital currency but for applications as well. The Ethereum Virtual Machine (EVM) executes a scripting language that can perform tasks similar to a general-purpose computer, which is capable of simulating what a Turing machine can do. This is unlike Bitcoin, which only evaluates spending conditions using a Boolean. To modify a contract's state on the blockchain, ether is used to pay the transaction fees. Ether powers the distributed application platform.

### 2.1 Voting system architecture

The proposed system's overall structure is depicted in Figure 2, which demonstrates how different entities such as Voters, VMS, AA, and IA work together to execute various voting tasks. The dAPP acts as a medium of communication for instant connection between voters and VMS. It can be accessed via a mobile app or a web portal. The Identity Authority is responsible for checking the validity of registered voters. Only the eligible voters verified by the Identity Authority can take part in the application. The system guarantees every user equal and unrestricted access to the voting process, with the added feature of traceability post-voting. To register, voters utilize their credentials, and VMS cross-checks the information provided against IA's online database. Upon verification, a unique OTP is sent to the voter, granting them access to the system. Every time the voter logs in, a new OTP is generated. VMS stores the voter's complete information. Upon registration, each voter is granted one Voting Coin (VC), which serves as an anti-duplication measure to prevent double voting.

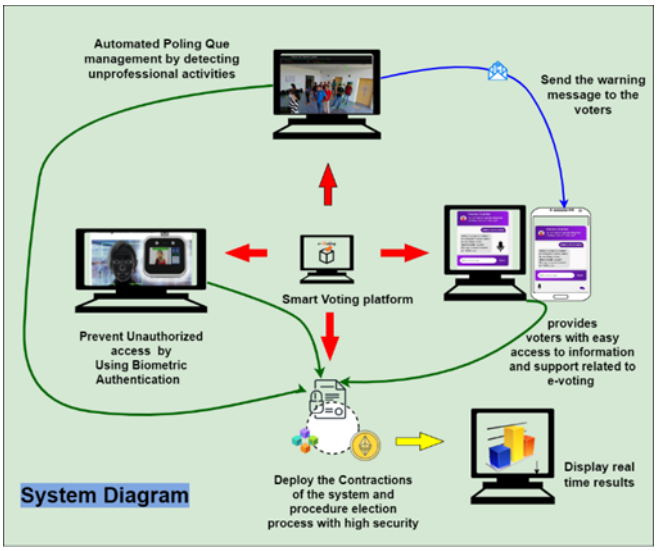


*Figure 2: System Architecture*

### 2.2 Ethereum Blockchain Account Types

The Ethereum Blockchain network has two types of accounts: externally owned accounts (EOAs) and contract accounts. EOAs are user accounts that are controlled by a private key and identified by a unique wallet address. The private key is owned by the user and is used to sign and transfer Ether, the cryptocurrency used in the Ethereum network, from the EOA. Each EOA is associated with a pair of cryptographic keys, with the private key used to sign transactions and verify their authenticity before they are executed on the network. The public key serves as the EOA address that identifies the account, and the EOA balance is measured in Ether[9].

### 2.3 Smart Contracts

A smart contract is an account on the Ethereum network that operates autonomously using its own code and is viewed as an independent agent that runs on the Ethereum Virtual Machine (EVM). All Decentralized Applications (DApps) rely on smart contracts, which are executed by the EVM if specific criteria are met. Smart contracts are publicly visible through their address, and anyone with enough Ether to carry out their functions and access to their address can execute actions on them. The transparency of smart contract code offers a significant advantage over traditional server-based systems where the code is kept confidential. The public nature of smart contract code makes it easy to verify the governing logic, which enhances their trustworthiness.

### 2.4 Private Blockchain Technology

Alongside the public version of Blockchain, a private or permissioned Blockchain also exists, and the decision on which type to choose depends on the application's specific requirements. In a public Blockchain, all EOAs can send transactions and explore the network using online network

explorers. However, in a permissioned Blockchain, a central authority is necessary to oversee and manage the ledger. For instance, in a country's electoral process, a permissioned Blockchain may be preferable as the government can regulate and supervise the election process.

## 2.5 Characteristics of blockchain technology

The three fundamental characteristics of a blockchain are as follows:

01). Immutability: One of the key features of blockchain is immutability, which guarantees that once transactions are added to the blockchain, they cannot be changed easily. The implementation of a secure hash function makes it very difficult to modify the transaction, as it would require a significant amount of processing and alteration of the entire blockchain.

02). Distribution: The distribution of Blockchain ensures that all nodes on the network possess identical copies of the ledger, which prevents the data from being stored in a single centralized location.

03). Decentralization: This implies that the Blockchain operates without the intervention of a third party, with all nodes sharing and updating the same data on the digital ledger.

## 3. LITERATURE REVIEW

This section presents some approaches that aim to merge Blockchain technology with electronic voting for the purpose of creating a decentralized voting system. Subsequently, we highlight the advantages of our proposed solution over these existing approaches.

a). The outdated paper ballot system has long been problematic for many countries, as it raises concerns about privacy, integrity, and security, as well as costing a significant amount of money and being centralized. However, transitioning to online voting platforms did not resolve many of these issues. To address these challenges, the authors propose using Ethereum and smart contracts to create a new framework for electronic voting. They utilized the Truffle framework and Meta-mask Chrome Extension to test and validate smart contracts, with the goal of simplifying the process for the 2021 International Conference on Information Technology (ICIT) at the University of Jordan. However, there are certain limitations to using this approach, as a platform is needed regardless of whether it is a private or public network. This article was downloaded from IEEE Xplore on August 3, 2021, at 07:27:59 UTC.

b). In their study, P. Mccorry and colleagues [12] discussed the possibility of conducting elections without the need for physical polling stations. If done properly, the use of blockchain technology for online voting could offer significant advantages, according to their analysis. The writers pointed out technical obstacles related to electronic voting systems, such as inadequate control over system durability and confidentiality problems with voting systems that have low latency. To tackle these challenges, they suggested utilizing blockchain technology in a voting system that incorporates smart contracts and a flexible consensus mechanism, which would enhance the system's speed while maintaining the protection and privacy of the voting process.

. c). Ali Kaan Ko and co-authors suggest a decentralized e-voting system based on Ethereum Blockchain in their paper titled "Towards Secure E-Voting Using Ethereum Blockchain" [14]. To ensure security, the system must be fully transparent and prevent duplicate votes. The authors propose implementing the e-voting application as a smart contract, which would permit only users with active EOAs to vote on the contract. However, since the Centralized Authority grants voting rights to EOAs, the system lacks an automated address verification process. The key advantages of this system are the transparency of business standards and the restriction of a single vote per EOA.

d). M. Pawlak and colleagues [11] suggested a voting system that did not rely on any operating entities, but it faced challenges in maintaining voter identity security and encountered latency issues when the user rate increased due to complex computations. The system also struggled to handle a large volume of data, making it difficult to implement on a large scale. On the other hand, our proposed voting system addresses latency concerns by utilizing consensus techniques that can be adjusted as needed, while the use of cryptographic hashes in blockchain technology ensures that voter identity is protected.

e). Fernando Lobato Meeser's article, "Decentralized, Transparent, Trustless Voting on the Ethereum Blockchain," highlights two primary issues with current e-voting systems. First, the outcomes of smart contracts can be calculated by anyone before all votes have been cast, and second, recorded votes can be linked to public keys, leading to a lack of anonymity. To address these concerns, the article proposes a new voting system that utilizes threshold keys and linkable ring signatures through an Ethereum smart contract. However, this system requires a registration process, and voters must rely on a Centralized Authority to register their public key before they can cast a ballot.

f). Tarasov and his colleagues researched the potential of blockchain technology for electronic voting and proposed a registration phase to guarantee transparency, privacy, and security in their article titled "The Future of E-Voting" [13]. They stressed the importance of the registration process for auditing and voter tracking purposes. The verification process includes a Challenge-Response handshake protocol, but it still relies on a Centralized Authority to handle and store user data (email addresses). Nevertheless, it's worth noting that email addresses can be easily falsified. The comparison presented in Table 1 shows the differences between our proposed Voting

International Journal of Science and Engineering Applications
Volume 12-Issue 05, 99 - 104, 2023, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1205.1029

Management System (VMS) and other blockchain-based voting systems. The main advantage of our system is that it uses a variable consensus method to manage voting performance, which is different from other systems that rely on a rule-based consensus algorithm to prevent harmful activity during voting, we have proposed measures to prevent 90% attacks and ensure chain authenticity using the Chain Use chain security consensus Algorithm. Furthermore, our system employs Smart Contracts to detect and prevent fraudulent or incomplete transactions in real-time.

| Problems | [04] | [11] | [16] | [18] | Proposed system |
|---|---|---|---|---|---|
| Low risk of data damage and hacking | ✗ | ✓ | ✓ | ✗ | ✓ |
| Flexible consensus algorithms | ✗ | ✗ | ✗ | ✓ | ✓ |
| Backup safe | ✗ | ✗ | ✗ | ✗ | ✓ |
| Chain Security | ✗ | ✗ | ✗ | ✓ | ✓ |
| Smart Contract | ✗ | ✓ | ✗ | ✗ | ✓ |

**Table 01: Present e-voting system VS proposed system**

The comparison presented in Table 1 shows the differences between our proposed Voting Management System (VMS) and other blockchain-based voting systems. The main advantage of our system is that it uses a variable consensus method to manage voting performance, which is different from other systems that rely on a rule-based consensus algorithm To prevent harmful activity during voting, we have proposed measures to prevent 90% attacks and ensure chain authenticity using the Chain Use chain security consensus Algorithm. Furthermore, our system employs Smart Contracts to detect and prevent fraudulent or incomplete transactions in real-time.

## 4. METHODOLOGY

This section outlines our proposed smart voting platform, which can be divided into four main sections.

### 4.1 Build a smart Contract For The El

**a).** Performance of e-Voting Smart Contract

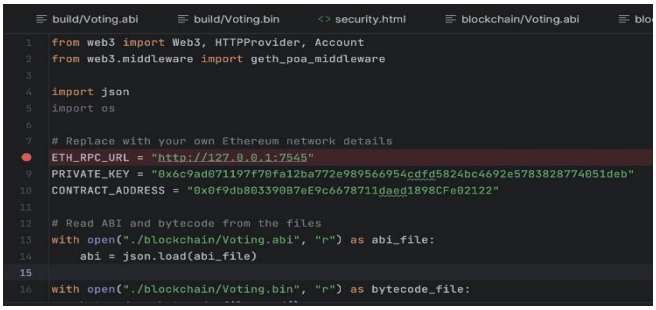


**Figure 4: Smart contract Connection with the blockchain**


**Figure 4: Smart contract Connection with the System**

To ensure secure transactions on the blockchain, smart contracts establish a secure link between the user and the network. These contracts dictate the regulations that govern the blockchain and cannot be disregarded. For the vote to be successfully stored in the system, all nodes must comply with the smart contracts.


**Figure 5: Face detection by using Rule-Based algorithm**

"Rule-based algorithm" can be used in an electronic voting system smart contract to ensure that the voting process follows a specific set of rules or guidelines This smart contract defines a simple voting system with the following rules:

1. Only registered voters can cast a vote

2. Each voter can only vote once

3. Voting is only allowed while the voting period is active

4. The winner is the candidate with the most votes

The contract contains functions to register voters, cast votes, and determine the winner. The `isRegisteredVoter`, `hasNotVoted`, and `isVotingActive` modifiers enforce the rules of the voting system. The `VoteCast` event is emitted each time a vote is cast.

This contract uses Tendermint for consensus, which means that each validator node in the network independently verifies the validity of each vote and the order in which they were submitted. The currentBlockHash and currentBlockNumber variables are used to keep track of the current block in the Tendermint consensus algorithm. The face-detection function is used to check if the voter's face can be detected. This is an example of an external service that can be integrated with the voting system to enhance its security. When a vote is submitted, the current block hash and currentBlockNumber variables are updated, and an event is emitted to notify any interested parties.

International Journal of Science and Engineering Applications
Volume 12-Issue 05, 99 - 104, 2023, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1205.1029

```
    function isValidator(address _address) public view returns (bool) {
        for (uint256 i = 0; i < validators.length; i++) {
            if (validators[i] == _address) {
                return true;
            }
        }

        return false;
    }

    function faceDetection(address _address) internal view returns (bool) {
        // Perform face detection here and return true if successful, false
    }

    event VoteSubmitted(address indexed voter, uint256 candidate);
}
```

**Figure 6: Use tendermint consensus algorithm**

```
pragma solidity ^0.8.0;

contract Voting {
  address[] public validators;

  struct Vote {
    address voter;
    uint256 candidate;
    bool isCounted;
  }

  mapping(uint256 => uint256) public voteCounts;
  mapping(uint256 => mapping(address => Vote)) public votes;

  constructor(address[] memory _validators) {
    validators = _validators;
  }

  function vote(uint256 _candidate) public {
    require(isValidator(msg.sender), "You are not authorized to vote.");
    require(!votes[_candidate][msg.sender].isCounted, "You have already vote

    votes[_candidate][msg.sender] = Vote(msg.sender, _candidate, true);
    voteCounts[_candidate]++;
  }

  function isValidator(address _address) public view returns (bool) {
    for (uint256 i = 0; i < validators.length; i++) {
      if (validators[i] == _address) {
        return true;
      }
    }

    return false;
  }
}
```

**Figure 7: Registering process by using PoA consensus algorithm**

This contract uses Tendermint for consensus, which means that each validator node in the network independently verifies the validity of each vote and the order in which they were submitted. The currentBlockHash and currentBlockNumber variables are used to keep track of the current block in the Tendermint consensus algorithm. The faceDetection function is used to check if the voter's face can be detected. This is an example of an external service that can be integrated with the voting system to enhance its security. When a vote is submitted, the currentBlockHash and currentBlockNumber variables are updated, and an event is emitted to notify any interested parties.

To ensure the legitimacy and accuracy of the votes, a consensus algorithm is necessary to achieve agreement among all nodes in the network. One popular consensus algorithm for blockchain-based e-voting systems is Proof-of-Authority (PoA), which is specifically intended for private and semi-private networks. Utilizing PoA in an e-voting system requires assigning trusted authority nodes to validate votes and count ballots, deploying a smart contract that interacts with the PoA consensus algorithm, registering voters on the blockchain network, and conducting the election using the smart contract.

01. Designate Authority Nodes: The Proof-of-Authority (PoA) consensus algorithm requires a group of authority nodes to validate transactions and uphold the blockchain's integrity. In an electronic voting system, trusted organizations or individuals can serve as authority nodes responsible for verifying votes and tallying ballots.

02. Setup the Network: The authority nodes must be configured on the network, and the blockchain must be deployed

03. Create the Smart Contract: The creation of a smart contract is necessary to establish the voting system.The smart contract should include the rules and guidelines of the voting process and should be designed to interact with the PoA consensus algorithm.

04. Deploy the Smart Contract: Once the smart contract is created, it needs to be deployed to the blockchain network.

05. Register Voters: Voters need to be registered on the blockchain network to participate in the voting process. The authority nodes can validate voter identities and eligibility criteria before registering them.

06. Conduct the Election: During the election, voters can cast their votes using the smart contract. The PoA consensus algorithm is utilized by the authority nodes to validate the votes and accurately count the ballots.

07. Declaration of the Results: After the election, the authority nodes can declare the results and make them publicly available on the blockchain network.

**b).** Public Key and Private Key Concept

Public-key cryptography utilizes a set of keys, including a public key and a private key, to ensure the security of data. To ensure secure data delivery over public networks like the internet, the sender encrypts the data using the recipient's public key [11]. Hash functions and digital signatures can be applied to use public-key cryptography to secure historical data in a transparent and unalterable way [23].

**c).** Hash Function

A cryptographic hash function [21, 22] is utilized to authenticate data. This function takes any input size and

generates a fixed, random string of values known as a hash value or digest [9]. Bitcoin's blockchain technology uses the well-known hash function SHA-256 [9]. A cryptographic hash stores the hash value of the previous block in the current block, which is an important aspect of blockchain technology. This forms links between blocks all the way back to the genesis block [7, 23].

**d).** Digital signature

A digital signature is a method of associating a person's identity with a message or data, similar to signing an electronic document [9, 20]. By using digital signatures, it is possible to identify the origin of data received on a blockchain [10, 21].

**e).** Peer-To-Peer Network (P2P)

The P2P network is a critical component of blockchain technology, consisting of a group of nodes with equal access rights in the network. These nodes or peers provide computational resources, such as disk storage, processing power, and bandwidth, to each other without relying on a central host.

## 4.2 Poling Line Management with social distance, Crowded Area Management and unauthorized things detection

Efficient poling line management is essential in polling stations to prevent time wastage for voters. To address this issue, an app has been developed to provide users with information about polling lineups. This app utilizes the priority line system, previously used in vaccination programs, allowing voters to estimate wait times for each individual in line. If the queue is too long, voters are notified and offered suggestions for the best-preferred line. Additionally, this smart platform includes features like social distance detection and facemask detection, making it suitable for use during pandemics or in countries facing problems like a shortage of currency and political instability, as in the case of Sri Lanka.

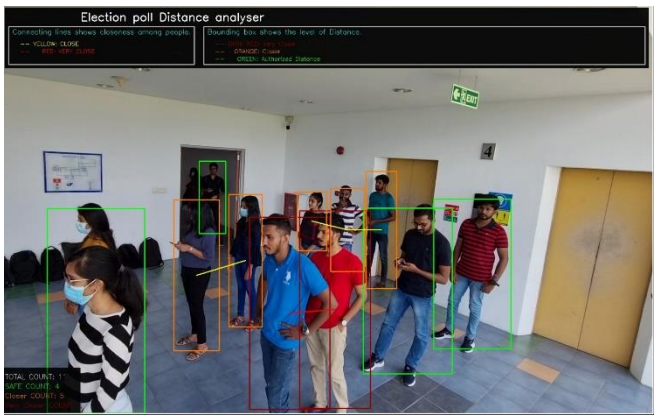


**Figure 08: Social distance and facemask detection**

## 4.3 Detecting the eligible voters through facial detection and avoid voting fraud using image processing

The act of voting is a critical component of any democratic society where citizens express their preferences and ideas through the election process. Over time, the voting process has evolved from handwritten ballots to digital technologies, including internet voting. This project proposes a smart voting system that uses facial recognition technology, allowing Sri Lankan citizens to cast their votes at their local constituency polling station. The system utilizes advanced biometric security measures and stores the voter information in a secure database on a server. Before beginning the voting process, the user must stand in front of a camera that captures their image and verifies their age to confirm their eligibility to vote. The web application software maintains a current personal database. After casting their vote, the system displays a confirmation message. If an individual under the age of 18 attempts to cast a vote using a facial sample, the system indicates their ineligibility to vote.

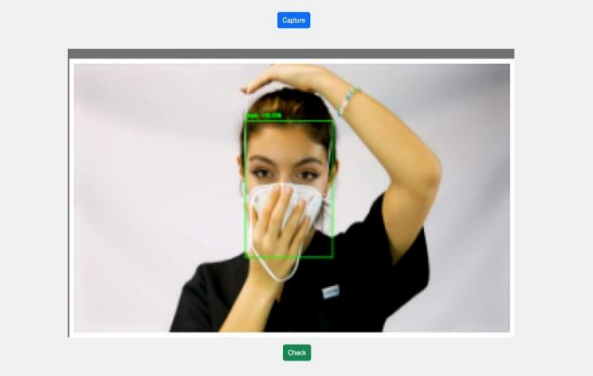


**Figure 9: Voter authenticates by face detection**

## 4.4 Chatbot for voter Guiding

This platform also offers a chatbot service to enhance the voters' experience. The chatbot enables users to initiate a conversation and obtain information on a variety of topics, including details on candidates, available polling stations, and guidance on obtaining election-related information in Sinhala, English, and Tamil languages. Furthermore, the chatbot assists voters in locating their nearest polling station. The main objective of the chatbot is to enhance the voters' experience during public elections by addressing their inquiries.

International Journal of Science and Engineering Applications
Volume 12-Issue 05, 99 - 104, 2023, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1205.1029

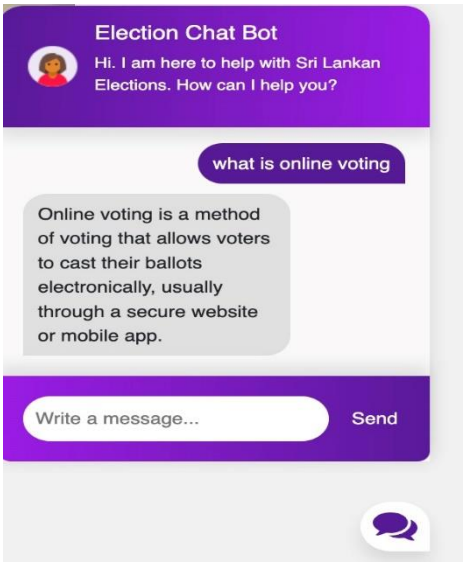


**Figure 10: Election Chatbot**

## 5. IMPLEMENTATION

We employed various technologies to implement our proposed approach and ensure the validity of the system. The Solidity programming language [23] was used to create smart contracts for voter registration and voting. NodeJS [20] was employed for server-side scripting on the Event Management Server, and Web3.js was utilized to interface with the light client [19]. Additionally, an HTML5 web application for PC devices was created using Apache Cordova [22]. We utilized the Rule-Based algorithm and the PoA consensus algorithm to develop a secure smart contract. Chain Link and Meta Mask were utilized to simulate the Blockchain network and get the private key. Twilio [24] was used for the SMS gateway API. And also, we used flutter foe develop our mobile application. For chatbot. Furthermore, we utilized algorithms for polling line management, unauthorized item detection, eligible voter detection, and voice recognition.

## 6. RESULTS AND DISCUSSION

The Biometric Electronic Voting System is considered superior to the traditional paper-based system due to its efficiency and security measures. The biometric identification process helps to prevent illegal voting, while the system records vote in a database and produces quick results. The final count is displayed on the website, and the system can be expanded for all elections in Sri Lanka, with the ballot sheet available in Sinhala, English, and Tamil languages. This automated system is more efficient than the current voting system and streamlines the registration process for voters, candidates, and political parties. With the use of face detection technology and smart contracts, the electronic voting process becomes more reliable. Initially, the system is being implemented for the presidential election.

The proposed electronic voting system offers many benefits such as reducing the time required for counting and publishing accurate and reliable results. It also prevents illegal access and voting, and automatically stops voting after the designated time period. The electronic voting system makes it easy to analyze data from the output, and all data is automatically stored in the database. This allows for easy filtering of data at any time and in any way. The system can also identify voting patterns easily, and the comparison of previous election results can be obtained automatically. Results of elections can be compared quickly and the system ensures an efficient and secure output.

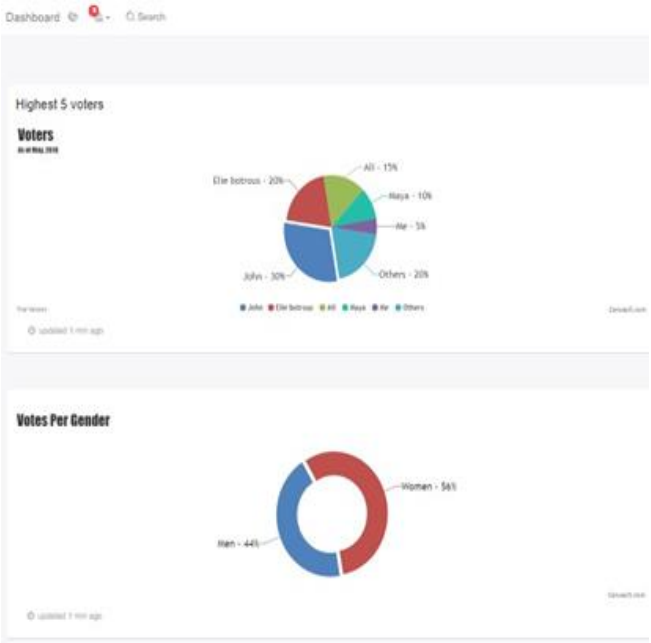


**Fig 11: Real Time Result**

This system is advantageous because it allows for easy analysis of stored data and filtering of data to identify voting patterns. Furthermore, it offers a quick comparison of results from previous elections, making it an efficient and secure solution for the voting process. The e-Voting system has been designed to produce efficient and secure results, making it a suitable alternative to the traditional voting method used in Sri Lanka. However, several critical factors need to be considered, such as ensuring proper security standards, conducting usability testing, and manufacturing the system appropriately. Additionally, given the computer literacy rate in Sri Lanka, both methods should be implemented for a period until people become familiar with the new system.

## 7. CONCLUSION

This article proposes a Smart voting platform for Sri Lanka that incorporates automatic poling line management and face authentication techniques, using the Ethereum Blockchain to prevent multiple votes and to solve a present dollar shortage, paper shortages, reduce officers' contribution and get the

election result in real time. So according to our proposed system government will be able to save public money. So they can used it for another development purposes in Sri Lanka. And also, voters can save their time and government can easily use this system in a pandemic situation. Like COVID-19. The success of an election system can be measured by its security and usability. The e-Voting system has standard security features to prevent unauthorized access and third-party software to detect malicious attacks. Therefore, it is considered a secure voting system. Usability is also crucial as the system will be used by citizens of all backgrounds, including those with disabilities, the elderly, and non-technical individuals. Designing a ballot that is accessible to all is important, and it should not show any bias towards any candidate. The list of candidates should be created using a standard mechanism. Hardware maintenance is also crucial for an e-Voting system to function properly and prevent voter discomfort.

## 8. FUTURE WORK

The proposed platform can be further improved for government elections by adding fingerprint identification or special devices at voting centers. Additionally, the user interface and result visualization can be customized to meet the specific needs of clients. This platform has the potential to replace the centralized SMS polling systems and can be used for government elections, competitions, and expositions, creating a new business model for voting service providers. Event organizers can use the services of the voting service provider to deploy an event voting smart contract with fixed costs paid by the organizers for smart contract deployment, and voters paying fees for registration and voting. This proposed platform offers a novel business model for voting service providers, voting event organizers, and voters. The current centralized SMS polling systems supporting various voting events can be substituted with this platform. The Event Management Server deploys the voting contracts in the Ethereum network according to the requirements of the voting event customer. Voting Event Organizers can pay a fixed cost for the deployment of the smart contract, while voters who register and cast their votes may pay a fee to the Voting Service Provider

## REFERENCES

[1]. S. S. Hossain, S. A. Arani, M. T. Rahman, T. Bhuiyan, D. Alam, and M. Zaman, ‘‘E-voting system using blockchain technology,’’ in Proc.2nd Int. Conf. Blockchain Technol. Appl., Dec. 2019, pp. 113–117, doi:10.1145/3376044.3376062.

[2]. L. S. o. H. &. T. Medicine, "The use of epidemiological tools in conflict-affected populations: open-access educational resources for policy-makers," London School of Hygiene & Tropical Medicine, 2009. [Online]. Available: http://conflict.lshtm.ac.uk/page_70.htm. [Accessed 25 January 2022].

[3]. I. S. Jacobs and F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, ‘‘Crypto-voting,a blockchain based e-voting system,’’ in Proc. 10th Int. Joint Conf.Knowl. Discovery, Knowl. Eng. Knowl. Manage., 2018, pp. 223–227, doi:10.5220/0006962102230227.

[4]. K. Elissa, “Title of paper if known,” unpublished. M. S. Farooq, M. Khan, and A. Abid, ‘‘A framework to make charity collection transparent and auditable using blockchain technology,’’ Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106588, doi:10.1016/j.compeleceng.2020.106588.

[5]. G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum project yellow paper, vol. 151, pp. 1–32, 2014

[6]. K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, “Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab,” in International Conference on Financial Cryptography and Data Security. Springer, 2016, pp. 79–94.

[7]. M. Pilkington, “11 blockchain technology: principles and applications,” Research handbook on digital transformations, p. 225, 2016.

[8]. Clack C. D., Bakshi V. A., Braine L. Smart contract templates: foundations, design landscape and research directions. 2017. arXiv preprint arXiv:1608.00771.

[9]. A. Ben Ayed. 2017. A conceptual secure blockchain-based electronic voting system. International Journal of Network Security & Its Applications (IJNSA) 9(3), (2017), 1–9.

[10]. D. L. Dill and A.D. Rubin. 2004. E-Voting Security. Security and Privacy Magazine, 2(1) (2004), 22–23.1–5.

[11]. J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where iscurrent research on blockchain technology? a systematic review,” PloSone, vol. 11, no. 10, p. e0163477, 2016.

[12]. Mohammad Hosam Sedky, E. M. (2015). A Secure e-Government's e-Voting System. Science and Information Conference 2015, 9.

[13]. R. C. Merkle, “Method of providing digital signatures,” Jan. 5 1982, uS Patent 4,309,569.

[14]. A. K. Koc¸ and U. C. C¸ abuk, “Towards secure e-voting using ethe F. L. Meeser, “Decentralized, transparent, trustless voting on theethereum blockchain,” 2017. reum blockchain.”

[15]. V. K. Katankar and V. Thakare, “Short message service using smsgateway,” International Journal on Computer Science and Engineering,vol. 2, no. 04, pp. 1487–1491, 2010.

[16]. “Twilio - connect the world with the leading platform for voice, sms,and video.” [Online]. Available: https://www.twilio.com.

[17]. .E. Akanksha, N. Sharma and K. Gulati, "OPNN: Optimized Probabilistic Neural Network based Automatic Detection of Maize Plant Disease Detection," 2021 6th International Conference on Inventive Computation Technologies (ICICT), 2021, pp. 1322-1328, doi: 10.1109/ICICT50816.2021.9358763.

[18]. M Qatawneh, W Almobaideen, and O AbuAlghanam (2020). Challenges of Blockchain Technology in Context Internet of Things: A Survey. In International Journal of Computer Applications. Vol.175(16).

[19]. Kriti Patidar, Dr. Swapnil Jain (2019, July). Decentralized EVoting Portal Using Blockchain. In 2019 10th International Conference on Computing Communication and Networking Technologies (ICCCN)

[20]. Cosmas Krisna Adiputra, Rikard Hjort, and Hiroyuki Sato (2018).Proposal of Blockchain-based Electronic Voting System. Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)

[21]. Alcazar, V. (2017). Data You Can Trust: Blockchain Technology. Ai& Space Power Journal, 31(2), 91–101. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&dbaph&AN=123448757&site=ehost-live

[22]. Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). Understanding the landscape of distributed ledger Technologies/Blockchain: Challenges, opportunities, and the prospects for standards. RAND Corporation. Retrieved from Social Science Premium Collection Retrieved from https://search.proquest.com/docview/1958456299?accountid=8144

[23]. Supeni Djanali, B. A. (2016). Design and Development of Voting Data Security for Electronic Voting (E-Voting). 2016 Fourth International Conference on Information and Communication Technologies (ICoICT), 4.

[24]. Rudrappa B. Gujanatti, S. N. (2015). A Finger Print based Voting System . International Journal of Engineering Research & Technology (IJERT) , 6

[25]. application platform,” white paper, 2014.[5] E. F. Kfoury and D. J. Khoury, “Secure end-to-end volte based on ethereum blockchain,” in 2018 41st International Conference onTelecommunications and Signal Processing (TSP). IEEE, 2018, pp.1–5.

[26]. J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where iscurrent research on blockchain technology? a systematic review,” PloS one, vol. 11, no. 10, p. e0163477, 2016.