FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 4 | Pages 1381-1390 | e-ISSN: 2347-470X

Secure Routing E-voting Protocol based on Wireless Sensor Network Platform with Block chain

Mohanaprakash T A[1], Ranganayaki.V.C[2], M.S Minu[3]*, Durga Devi A[4], and Cinthuja K[5]
[1]*Department of CSE, School of Engineering and Technology, C M R University, Bangalore, Karnataka, India; tamohanaprakash@gmail.com*
[2]*Department of CSE, St. Joseph's Institute of Technology, OMR, Chennai, Tamil Nadu, India; ranganayaki.v.c@gmail.com*
[3]*Department of CSE, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India; msminu1990@gmail.com*
[4]*Department of ECE, P. B. College of Engineering Chennai, Tamil Nadu, India; durgaanbhu@gmail.com*
[5]*Department of CSE, Panimalar Engineering College, Poonamallee, Chennai, Tamil Nadu, India; cinthu16.k@gmail.com*

***Correspondence:** M.S Minu; *msminu1990@gmail.com*

ABSTRACT- Many have long aimed to create a safe electronic voting system that maintains the confidentiality and integrity of traditional voting methods while using the convenience and openness of modern technology. Ballot paper or electronic voting machines are the current voting schemes in every nation, and democratic voting is a significant event in every country. Problems with these procedures abound, including lack of openness, poor voter turnout, vote manipulation, mistrust of the election body, forgery of unique identification (voter ID card), delays in disseminating results, and, most importantly, security breaches. Prioritizing the security of digital voting is of utmost importance when contemplating implementing a digital voting system. The article assesses the objective of building a blockchain-based e-voting system [BC-E-VOT] that uses digital voting technology. Electronic voting methods that leverage the distributed ledger attract much attention because they can make digital voting more transparent, secure, and honest. As shown in this research, a successful strategy for electronic voting may be achieved by using Blockchain's cryptographic underpinnings and transparency. Due to its complete transparency, the suggested approach satisfies the essential criteria for electronic voting systems. Since Blockchain employs a decentralized mechanism for data storage rather than storing all of the data in one central place, it becomes challenging to tamper with the data when utilizing this technology to build a decentralized application. By creating a decentralized system using the WSN platform, a third party is no longer needed to oversee the election's access control. This article provides a system for electronic voting that guarantees privacy, trustworthiness, and security. The suggested approach is practical and secure, according to the findings.

Keywords: Blockchain, E-Voting, Secure Voting, Distributed Ledger, Digital Voting.

ARTICLE INFORMATION

Author(s): Mohanaprakash T A, Ranganayaki. V.C, M.S Minu, Durga Devi A, and Cinthuja K;

Received: 17/09/2024; **Accepted**: 02/11/2024; **Published**: 21/12/2024;
e-ISSN: 2347-470X;
Paper Id: IJEER 1709-16;
Citation: 10.37391/IJEER.120432
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-12/ijeer-120432.html

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Every nation's democratic voting process is essential and weighty. Most countries still use traditional paper ballots. The process of casting a vote using an electronic device, such as a voting machine or a web browser, is known as digital voting. In democracies, maintaining a fair and transparent election is crucial for gaining the trust and cooperation of the people and holding elected officials to account. Electoral systems in politics play an essential role here [1-2]. From a policy standpoint, computerized voting systems may reawaken citizens' passion for casting ballots, boost voter trust, and raise participation. One term for casting a vote via a voting machine at a polling place is "e-voting," while another is "i-voting" when done using a web browser. The primary worry when contemplating implementing a digital voting system is the security of digital voting [3-4].

A more comprehensive strategy and efficient biometric identification and cryptographic technologies for electronic voting are needed to combat the growing number of complex security challenges in the digital sphere. Security solutions based on the WSN platform have recently attracted the attention of A more comprehensive strategy. Efficient biometric identification and cryptographic technologies for electronic voting are needed to combat the growing number of complex security challenges in the digital sphere experts in many fields [5-6]. An authenticated distributed record-keeping system that operates on a P2P network and records blocks using consensus mechanisms is known as Blockchain. When applied to the many issues surrounding the security and transparency of E-voting systems, the method has tremendous potential. To achieve this goal, one can upgrade the algorithms used for voter enrolment and confirmation, integrate a blockchain for information storage, and relocate the voting procedure to the cloud. This will result in a reliable, secure voting system [7].

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 4 | Pages 1381-1390 | e-ISSN: 2347-470X

Given the gravity of the situation, the system's capacity to protect data and ward off attackers must be specific. WSN platform is one avenue that might address security concerns. WSN platform is derived from the foundational architecture of the digital currency bitcoin. In this distributed database system, each record is represented by a series of transactions called a block. A trustworthy and reliable system for online voting may be developed with the help of the WSN platform [8-9]. With the advent of E-voting systems, the traditional paper ballot voting process has the potential to be transformed into a more accessible and inclusive alternative. Voters and electoral commission officials benefit from the significant time and effort savings. Additionally, it helps the government save a tonne of money on electoral fraud. An auditable and secure digital voting system built on the Blockchain is described in this article; it does away with the need for a governing body to confirm and ratify election results [10-11].

Based on the level of access, verification, and updating rights granted to users and nodes, blockchain networks may be categorized as public, private, or hybrid. Anyone may join a public blockchain network and access all the data—view, publish, and save. Private blockchains are closed networks that enable only authorized users to see and publish data, as opposed to public blockchains that are accessible to everyone. Combining public and private blockchains creates a hybrid blockchain. Although everybody may access the data in this network, only authorized users can publish and save data using smart contracts [12-13].

This technique shows great promise in resolving many security issues while guaranteeing the possible openness of electronic voting systems. Several studies highlight Authentication and registration issues that might be improved in an electronic voting system. Considering this, the project aims to develop a trustworthy electronic voting system by implementing new security measures and using WSN platform to verify voters and their identities before storing their votes on a remote server. This study explains how a hybrid blockchain network integrated with a cloud-based electronic voting system may resolve dependability concerns, including lost votes and recovery [14-15].

Main Objective,

1. This paper builds a prototype for an electronic voting system based on the WSN platform.

2. It includes a web-based secure digital voting method that utilizes "permissioned blockchain" to facilitate liquid democracy.

3. The result shows that for digital voting to work, it is evident that privacy regulations must be updated to accommodate electronic voting as proposed by BC-E-VOT.

The document's following parts are structured: *Section 2* describes an in-depth research review of the study. *Section 3* explains the rationale behind the proposed paradigm. *Section 4* delves into the evaluation of the suggested model's effectiveness. *Section 5* concludes the report and offers recommendations for further research.

2. RELATED SURVEY

R. Madhusudhan et al. [16] proposed a platform for electronic voting that utilizes the Interplanetary File System (IPFS) and a consortium blockchain to address the need for modern-day technologies that are both extremely secure and efficient. Studies have developed several blockchain-based solutions to improve electronic voting; however, most of these solutions fail to scale and have significant delays. A scalable electronic voting system based on the Blockchain is difficult to develop.

The article presents the approach for a decentralized voting system that Durgesh Kumar et al. [17] suggested, which is based on Blockchain and the Internet of Things (BC-IoT). Utilizing concepts like encryption, decryption, hash functions, consensus, and Merkle trees, the WSN platform is ideal for safe and anonymous data storage and transfer. Thus, the election process in democracies is highly esteemed since the current voting method is more trustworthy and safer thanks to the qualities of Blockchain and the Internet of Things.

John Amanesi Abubakar et al. [18] proposed the waterfall method to software development for an efficient and reliable e-voting platform, which involves everything from preparing to gathering requirements to designing to implementing to verifying to deploying. Using a virtual machine guarantees the software works properly after secure cloud hosting. The Internet of Things makes electronic voting possible, promoting democracy, openness, and peace. AIoT technology boosts efficiency, security, and accuracy, making this system a great candidate for SDG 16 elections.

By comparing different authentication methods and highlighting the necessity for a multi-modal approach, Elsi Ahmadieh et al. [19] suggested integrating voice recognition and fingerprinting with the WSN platform to improve the security of electronic voting systems. The method is made more reliable by ensuring a safe, tamper-proof, and transparent system where each vote is recorded as an immutable transaction. Using the WSN platform, electronic voting eliminates the problems associated with traditional voting systems, including fraud, manipulation, and delays. Traditional voting methods also need more transparency regarding counting and seeing results.

Due to the rapid growth of the Internet, Asma Ibrahim Hussein et al. [20] suggested that electronic voting (EV) is gradually replacing traditional voting methods idea of fog computing, which aims to enhance network architecture to handle massive data loads more efficiently in processing. The research aimed to identify potential issues with implementing highly secure EV systems by conducting a comprehensive assessment of EV systems from many academic perspectives. Countries that have already implemented EV systems were also considered. Based on issues found in various works, a plan for future work on creating a secure EV system may be formulated.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 4 | Pages 1381-1390 | e-ISSN: 2347-470X

Albandari Alsumayt et al. [22] suggested the secure blockchain-based e-voting. In particular, the system suggests ways to address concerns about voters' anonymity and the results' secrecy until the formal announcement, two issues that are anticipated to arise with adopting blockchain-based voting systems. The results demonstrate that a decentralized and trustworthy voting system is within reach, benefiting all stakeholders.

Muthulakshmi and Kannammal [23] proposed the Distributed Ledger Technology (DLT) to Enhance E-Voting System Security. A directed acyclic graph is used by the Internet of Things Application (IOTA), a distributed ledger system that shows promise. The Directed Acyclic Graph architecture allows for faster transaction confirmation, great scalability, and the elimination of transaction fees. The general population may cast several votes on blockchain and IOTA tangle. An unauthorized user may generate duplicate votes in the blockchain and the IOTA tangle. This approach has the potential to concentrate on this. Using the Crowd Search Algorithm (CSA) helps fix the issue of duplicate expenditure. An enhanced solution to the issue of duplicate expenditure in electronic voting systems is generated by this optimization problem.

Sweta Gupta et al. [24] recommended End-to-end secure e-voting using blockchain and quantum key distribution. This paper discusses how the advent of quantum computers has exposed blockchain's vulnerabilities and offers broad suggestions for strengthening blockchain's defences against future technological advances. Consequently, this study uses a unique technique to demonstrate several processes of the proposed electronic voting system. The concept of electronic voting using blockchain security and quantum key distribution is included in the technique. An upgraded version of the electronic voting system that uses blockchain technology in several network contexts. This paper also addresses implementation issues, which detail the architecture, design, and design limitations of our society's potential voting system.
Fatima Zahrae Chentouf and Said Bouchkaren [25] discussed using a secure e-voting system based on blockchain to improve security and privacy in smart cities. The author examined how the four features of blockchain technology: transparency, democracy, decentralization, and security can contribute to enhancing smart city services and explored various blockchain applications in smart cities. To demonstrate the potential of blockchain technology to enhance security in smart cities, this research will be useful in developing an electronic voting model that utilizes an Ethereum blockchain-based smart contract.

Based on the survey, there are several issues with existing models in attaining high accuracy, trust, and security levels. Hence, this study proposes a blockchain-based e-voting system [BC-E-VOT] that uses digital voting technology.

3. PROPOSED METHOD

The problems above need a fresh method of voting that guarantees the confidentiality and precision of voters; these problems are not unique to BC-E-VOT but affect many nations. The overarching goal in designing the system for BC-E-VOT was to provide an alternative to the conventional voting method that did not need advanced computer skills. A thorough security analysis requires the system's sensitivity to many types of assaults, including replay attacks, denial-of-service attacks, and Sybil attacks. It needs to assess the strength of the security measures that have been established, such as authentication systems and encryption protocols. Throughput, latency, scalability, and resource consumption should all be explicitly measured as part of the performance assessment.

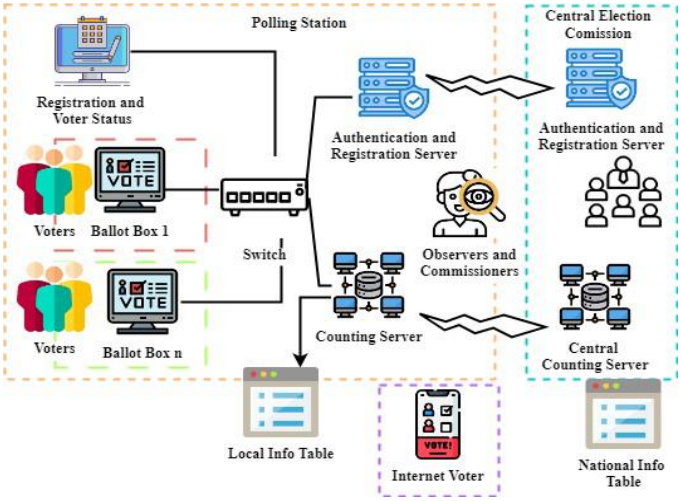


Figure 1. Architecture of e-Voting system

The electronic voting system's overall design is shown in *figure 1*. Ballot boxes, voter registration and status computers, and an authentication and registration server (ARS) make up the polling station. The counting server (CS) is also a part of it. A government public critical infrastructure was established to issue digital X. 509 certificates to individuals, servers, and other devices; this was done to guarantee the privacy of voters, as suggested. Fingerprint information is one of several pieces of personal data the BC-E-VOT keeps. When issuing a national ID card, the issuing process includes recording fingerprint data. For citizen authentication, the suggested approach makes use of this fingerprint data. Central Election Commission (CEC) sends voting lists, including fingerprint data, to each polling location. A smart card contains the private key created and used to decrypt the CS's X.509 digital certificate. Both the public and private keys for CS are 2048 bits in size. A PIN is required to access this private key, which is never stored outside the smart card. The system uses public critical infrastructure (PKI) to prevent Sybil attacks, in which an insecure node tries to create numerous identities to manipulate the voting system. An independent and trustworthy Certificate Authority (CA) provides digital certificates to each node. Since the system checks each certificate before allowing nodes to vote, this prevents them from impersonating others or creating pretend identities. Neighbour verification algorithms cross-reference identities and traffic patterns from nearby nodes to identify questionable activity. To avoid essential nodes from overloading by excessive traffic, the protocol uses rate-limiting and energy-efficient message forwarding to counter denial-of-

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 4 | Pages 1381-1390 | e-ISSN: 2347-470X

service (DoS) assaults. Using lightweight cryptographic procedures and restricting the number of requests handled by any one node decreases the possibility of resource depletion. Using timestamps and nonces, the protocol protects against replay attacks involving the malicious repetition of previously sent accurate information. A distinct reference and timestamp are appended to every vote, guaranteeing that any effort to resend or modify previous messages is promptly identified using the comparison of timestamps and sequence numbers.

Following CEC administrative requirements, the local info table displays the vote results and provides basic information on the local election process. Also kept in the Central Authentication and Registration Server (CARS) system storage is a digital X.509 certificate with its assigned private key. With this digital certificate, voters casting ballots from the comfort of their own homes may now use SSL encryption on their ballots. All polling places transmit their results to the Central Counting Server (CCS).

1. Voter Registration and Status Verification: At the polling place, voters use a system to check their voting status and the information they entered when they registered. This is crucial to restricting voting to those who can legally do so. The voter's identification is checked against the Central Election Commission's database using an authentication and registration server linked to the system.

2. Ballot Boxes: After authentication, voters use an electronic voting interface linked to Ballot Box 1 (or other ballot boxes as required) to cast their ballots. A switch securely sends the information to the next layer from these linked vote boxes.

3. Counting Server: The vote results are compiled by sending them to a counting server after they have been cast. Observers and commissioners oversee this server to ensure the integrity and openness of the counting process. The server communicates with the Central Counting Server and the Local Info Table at the Central Election Commission to keep local and national databases in sync.

4. Internet Voting: The method also allows voters to cast votes safely from faraway areas using the Internet. All the votes go via the same safe methods and are then added to the National Info Table for final tally and confirmation.

5. Authentication and Registration: This component ensures that the electoral commission's central systems authenticate all voter data to avoid fraudulent activity and keep the election process safe. The architecture design emphasizes safeguarding voter data, ensuring precise tallying, and facilitating real-time communication between regional voting locations and the election authority. To sum up, this system is built to provide a transparent, secure, and all-encompassing voting process, with digital protections included at every step to guarantee that elections are honest.

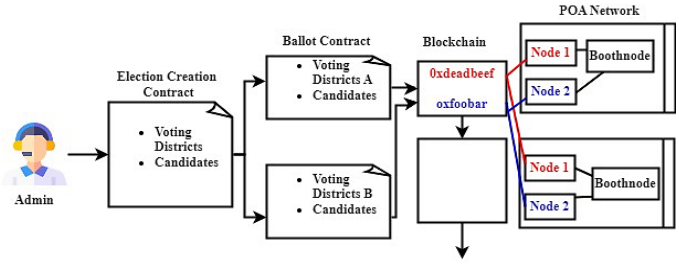


Figure 2. Election as a smart contract

3.1 Blockchain setup

To ensure the anonymity and safety of digital voting and exclude the potential of coerced voting inside the election system, voters must cast their votes under strict monitoring. This article outlined our efforts to achieve these goals by implementing a Go-Ethereum permissioned Proof-of-Authority (POA) blockchain. Quick transactions are made possible by POA's algorithm, which uses a consensus technique that uses identity as a stake. Two main types of nodes make up a blockchain, as shown in *figure 2*. PoA's exceptional efficiency and security with limited resource usage make it a proper fit for this application. In PoA, the credibility of trusted authorities (such as government agencies or election officials) is used to verify transactions, as opposed to PoS, which requires validators to invest much more bitcoin to take part. This makes it a good option for an election situation where a few pre-approved nodes are needed to ensure the process is genuine. Considering PoA's consensus mechanism is less complex, it offers greater scalability than PBFT, which is used in secure systems. As the number of participants grows, PBFT may become slower and more resource-intensive because of the considerable communication required between nodes to obtain agreement. On the other hand, PoA is perfect for time-sensitive applications like elections since it can efficiently process more transactions with less computational costs. More so than Proof of Stake (PoS) and other consensus procedures, Proof of Work (PoW) is less susceptible to the energy consumption difficulties that PoA appears.

PoA’s computing requirements make it secure, but its slower transaction rates and significant energy consumption make it inappropriate for instantaneous outcomes needed in electronic voting. In contrast, proof-of-stake (PoS) transactions are quicker and use less energy, which may also lead to centralization, whereby influential users control the network unfairly, raising questions about transparency and cooperation. Limiting the number of pre-approved validators, PoA improves accountability, decreases the possibility of fraudulent transactions, and speeds up transaction processing while lowering energy usage. Implementing stringent selection and supervision procedures might limit the centralization concerns introduced by PoA, which result from its dependence on a small collection of authorities. Finally, PoA offers a well-rounded answer by integrating governance, efficiency, and security, making it the best option for a credible e-voting system.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 4 | Pages 1381-1390 | e-ISSN: 2347-470X

- **District node**

Stand up for every voting district. An autonomous software agent runs each district node's smart contract life cycle and communicates with the "boot node" independently. The election administrator's responsibility (refer to the section on smart contracts) is to design elections and distribute and install ballot smart contracts onto the nodes in each district. Each district's nodes are granted access to their smart contract during the creation of the ballot smart contracts. The Blockchain will include electors' votes after the largest networks in each district have been confirmed. This occurs when each voter uses their smart contract to cast their ballot.

- **Boot node**

Any institution with permission to access the network may host a boot node. The district nodes can find and interact with one another with a boot node, a service for discovery and coordination. To help district nodes identify peers faster, the boot node operates on a static IP address and doesn't save any blockchain data. Building a private and trustworthy blockchain is the first step in developing a smart contract to power the blockchain-based electronic voting process.

3.2 Election as a smart contract

First, the people involved (in this case, the candidates, and the voting agreements); second, the procedure that led to the conclusion of the agreement (the election itself); and third, the actions taken to complete the deal (the voting transaction) are all necessary components of a smart contract definition.

1. **Election roles:** All parties involved in a smart contract must fulfil specific responsibilities for the agreement to be valid. Here are the functions performed by the election process:

   The role of the election operator is to guide the process from start to finish. Several respectable companies and groups might be involved in this capacity. The administrators of the election are responsible for its creation, voter registration, duration, and assignment of permissioned nodes.

2. **Voter:** A person with voting rights. After an election is finished, voters have the option to validate their vote, cast their ballot, and authenticate themselves.

3. **Election process:** According to the findings in *figure 2*, election administrators implement a collection of smart contracts on the Blockchain to represent each election process. There is a specified smart contract for every voting district. The most essential steps in casting a ballot are as follows:

4. **Election creation:** A decentralized app (dApp) is used by election administrators to generate ballots. This decentralized app communicates with a ballot construction digital contract where the administrator defines a set of voting areas and a list of nominees. The electronic agreement takes an argument for every voting district and returns a set of ballot electronic ballots with a list of nominees in each constituency. The next step is to add these smart contracts to the Blockchain. While the election is set up, every node in the district is allowed to talk to its corresponding smart contract for the ballot (*figure 2*).

5. **Voter registration:** This task is carried out by election authorities. When an election is set up, the administrator must specify a deterministic list of eligible voters. A federal authentication service must include an aspect that securely authenticates and authorizes qualified individuals. All eligible voters must have their voting district details, an electronic ID and a PIN to use these verification services. Each eligible voter would have a matching wallet. The voter's wallet should be made unique for each election in which they are eligible to vote.

To prevent the system from knowing which wallet corresponds to which voter, an NIZKP might be used to construct these wallets.

Voter IDs, biometric data, and Internet of Things (IoT) devices used by candidates and eligible voters must be registered in KGC before the election. Upon registration, the private keys QS_{Key_wj} *and* QS_{Key_dj} are given to each candidate and voter, respectively. When sending a list, the essential generation centre tracks registered participants and transmits them to the ECA.

Step1: To calculate the Internet of Things device's Virtual ID $WUje$, the ECA uses the numbers Wje_j, Eje_j, QS_{Key}, and NL_{FDB}, as indicated in *equation (1)*:

$$WUje_k = I(Wje_j||Eje_j||Tj||NL_{FDB}) \quad (1)$$

Step 2: *Equation 2* creates the credentials for every Internet of Things device.

$$DE_k = I(WUje_k||Tj||NL_{FDB}||UT_S) \quad (2)$$

Step 3: The ECA generates a public key by utilizing *equation (3)* after randomly selecting the private keyQS_{Key}:

$$QV_{Key} = QS_{Key}.H \quad (3)$$

For which the ECC algorithm selects H.

Step 4: The ECA in the IoT device stores the following data, including $WUje_k, QS_{Key}QV_{Key}, I(.)$.

This procedure is associated with the candidates' and voters' respective gadgets. Integrating IoT smart devices, ECAs, and edge servers is necessary as part of the deployment process.

To ensure dependability, the ECA registers the cloud server offline. To do this, the ECA selects the first cloud server identity, D_{je}, and generates temporary identities, DT_{je}. The ECA selects secret d_1 at random and determines their temporary using the formula in *eq. (4):*

$$DT_{je\_U} = I(D_{je}||d_1||UTds) \quad (4)$$

This corresponds to the cloud server registration timestamp, denoted as $UTdt$. The ECA has already pre-configured cloud

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 4 | Pages 1381-1390 | e-ISSN: 2347-470X

server CS with the credentials D_{je}, DT_{je}. Cloud servers generate their private keys at random QS_{Key} and then use those keys $QV_{Key}QS_{Key}$ and their secure memory databases H to develop their public keys$\{D_{je}, DT_{je}, QV_{Key}QS_{Key}, I(.); Hh\}$. They are broadcasting itsQV_{Key}.

1. Vote transaction: Each voter interacts with a smart ballot contract associated with their specific voting district at each voting district. If most of the relevant district nodes agree, the ballot will be added to the Blockchain using this smart contract's interaction with the Blockchain.

The Blockchain records each vote as a transaction, and each voter gets a unique transaction ID that they may use to authenticate their vote (for more on this, see the "Verifying Vote" section). The location of the vote and the voter's identity are details recorded in every blockchain transaction. Ballot smart contracts add each vote to the Blockchain only when all nodes in the related district agree to verify the vote data. To prevent voters from casting more than one ballot every election, each ballot cast reduces the weight of their wallet by one. According to *table 1*, the details as follows are included in every transaction on the public Ethereum blockchain: the transaction ID, the block where the operations are included, the age of the exchange, the wallet that sent and received the transaction, the total amount transmitted, and the price of the transaction. It is recommended that not all this data be required for each transaction in the Protocol system. For instance, in an N1SC transaction, the following information would be included: the transaction ID, the block where the transaction is placed, and the smart contract that received the transaction. The final tally represents the worth of the transaction, and because *D* stands for the voting party in this deal, this article may conclude that *D* is the voting party. As a result, see Table II for details on how our system handles transactions that do not reveal the voter's identity. By not including the age of a single transaction, individual votes are protected against timing assaults.

Table 1. An Ethereum-based public transaction

TxH	Frame	Age	From	To	Value	[TxFee]
0xdead….	1338	34sec ago	0xbeef….	Token	12 Ethere	0.0870
0xface…	1338	34sec ago	0x4343	0x12345	2 Ethere	0.0560

Table 2. System transaction

TxH	Frame	To	Value
0xdeadbeef….	1338	N1SC	E
0xG1345edf….	1331	N2SC	Q

2. Summarizing outcomes: The smart contracts handle the election tallying in real-time. In their respective storage locations, smart contracts for each vote do their count. At the end of an election, the results for all smart contracts are made public.

3. Verifying vote: As previously stated, each voter gets a unique transaction ID for their vote. Any voter using their electronic ID and PIN to prove their identification may now visit an elected official in the area and show them their transaction ID. Using the municipality's node's network connection, an elected official utilizes the blockchain explorer to locate the blockchain transaction corresponding to the linked transaction ID. To verify that their votes were correctly counted, voters can access their records on the Blockchain.

Electronic ID authentication, a service provider for identity verification based in Iceland, is the backbone of our proposed system's security measures. It uses RFID scanners in conjunction with Nexus software. When individuals sign up for it, they select a 6-digit PIN corresponding to their electronic ID. To verify their identity, voters must scan their IDs and enter their PINs at the polling booth.

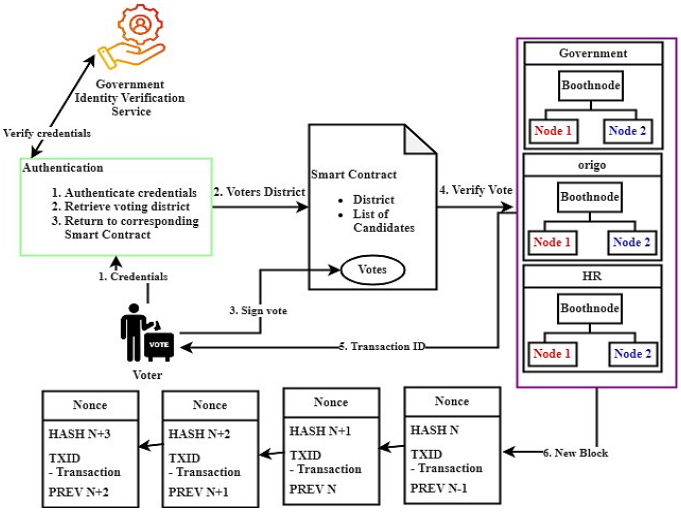


Figure 3. The E-Voting process using Blockchain

This procedure is shown graphically in *figure 3*. (I) The transaction ID; (II) the region where the trade is located; (III) The digital contract that received the data; this signifies the electoral region; and (IV) The value of the transaction; this is the vote; it signifies the organization (party) wherein the voter has given the votes.

Thus, with the system, a vote does not expose any information on the specific voter's identity.

Any qualified voter may cast their ballot from any computer in any voting district because each voter's wallet contains

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 4 | Pages 1381-1390 | e-ISSN: 2347-470X

information about their assigned voting district. Users must produce a valid ID and PIN to authenticate at a voting district using the Nexus software.

Enquiring the linked smart contract requires adequate identification to participate in the current election. A smart contract containing a list of candidates is used as the ballot for the election above.

Following the selection of a candidate and the casting of a ballot, the voter must "sign" his vote by reinputting the corresponding PIN for his e-ID.

The voter's identity and vote data are validated by the appropriate district node, which is also the point of interaction between the voter and the intelligent contract. The majority-related district node must concur with the vote data before the district above node can accept it.

Vote data is considered consensus-based if most area nodes concur with it. The next step for the user is to get the vote-related transactional ID, which may be printed or saved as a QR code. A smart contract function gives the winning party an extra vote after the vote has been cast and validated. This feature of the smart contract Protocol determines the election outcome in each voting district. This paper has merely extended the procedures visually in *figure 3.*

When a block time reaches its limit, the Blockchain updates all the received and validated transactions within that period. All of the nodes in the district sync their copies of the ledger whenever a new block is added to the Blockchain.

3.3 Assessing blockchain deployments

The work is building its WSN platform and deploying intelligent agreements via a private, permissioned network. This prevents manipulated voting and guarantees that online voting is secure, transparent, and meets privacy standards. To develop and release our election smart contracts, this section examines three different blockchain architectures: Geth, Quorum, and Exonum.

1. Exonum: Fully integrated with Rust, the Exonum blockchain ensures end-to-end resilience. Exonum is only compatible with private blockchains. It uses a modified Byzantine method to reach network consensus. The transaction speed with Exonum is five thousand per second. One limitation of the Protocol is that developers are limited to Rust structures. Unfortunately, this version only supports Rust as a programming language. Soon, Exonum will include platform-independent interface definitions and Java bindings to make it more developer-friendly.

2. Quorum: A Quorum is a distributed ledger technology built on Ethereum that introduces additional consensus methods and protects the privacy of transactions and contracts. It follows the release schedule of Geth and is thus considered a Geth branch. Quorum's new consensus method focuses on algorithms that rely on consortium chains. Incorporating this consensus mechanism enables it to sustain several transactions simultaneously.

3. Geth: A trio of early implementations of the Ethereum protocol were known as Go-Ethereum and Geth. It executes smart contract applications precisely as intended, unaffected by censorship, fraud, or third-party intervention. This Protocol is the most developer-friendly out of the ones we looked at, and it also permits development outside the Geth protocol. How fast transactions happen on a blockchain depends on whether it's a public or private network. For these reasons, this paper chose to build our project using the Geth Protocol; however, any comparable blockchain Protocol with the earlier features might be considered for usage in such systems. Following the election's conclusion, these functions are auxiliary for calculating the final tally.

The division of WSN nodes across voting sites allows for data collection on voter credentials, vote submissions, and system status. With their unique architecture, these nodes may effectively send this information to other nodes in the network that serve as validators. The validator nodes go between the WSN and the blockchain to ensure only valid information is reached. The validator nodes establish the link between the WSN and the blockchain. Some examples of these nodes include checking the voter's identification and the accuracy of their vote count using data acquired by WSN sensors. When everything is in order, the data is transformed into transactions and sent to the blockchain to be recorded. The blockchain is a decentralized, immutable ledger that keeps all the votes honest and transparent. Validators are critical in the Proof of Authority (PoA) consensus method by ensuring that only trustworthy nodes can submit data. This strengthens security by preventing hostile attacks or inauthentic data from entering the system.

For electronic voting initiatives, the WSN platform may be the best answer. There has been a lot of research on electronic voting, and many systems have been tried and tested, with some even being in operation for some time. Unfortunately, there aren't many stable implementations that are still in use. We can't say the same for governments and corporations' online voting, even if there are many effective online polls and surveys. For the most part, it's since democratic administrations—the most popular form of government in the contemporary era and democratic elections go hand in hand.

4. RESULTS AND DISCUSSION

According to the study, the blockchain-based Secure routing E-voting architecture enhanced voters' privacy, immutability, and transparency. The distributed nature of Blockchain significantly lessens the likelihood of vote fraud and manipulation. Furthermore, the smart contract's functionality ensured the secure validation and tally of every vote, cutting out any intermediaries. Ultimately, the Protocol proved to be a reliable and efficient method for ensuring the integrity of electronic voting systems.

Dataset: By the end of 2036, the voting system market is expected to have grown to 1.2 billion USD, with a compound

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 4 | Pages 1381-1390 | e-ISSN: 2347-470X

annual growth rate (CAGR) of 7% from 2024 to 2036. Increased internet penetration and smartphone accessibility in the Asia Pacific are driving predictions that the region will have the most significant market share by 2036, at 36%. [21]

The system's user-friendly interface makes it simple for voters to vote using designated voting stations or portable devices. To simplify the voting procedure for people with varying levels of technical knowledge, everyone has simplified it with clear instructions, a few steps, and an intuitive design. Voters may rest easy knowing their votes will remain anonymous because of the system's emphasis on privacy and strong encryption. Voice aid, large letters, and interactive support are some of the accessible features included in the protocol to help those with impairments. Examining it from the standpoint of election authorities, the system streamlines vote management by providing capabilities to track voting status, guarantee secure tallying, and validate vote integrity in real-time. Scalability in the system architecture allows election authorities to manage both small and large voter populations easily.

4.1 Accuracy

To determine if our method is effective in data segmentation and classification, we put it through its paces, utilizing the challenge evaluation criteria. Here are the defined success criteria:

$$\text{Accuracy} = (\text{TP} + \text{TN})/(\text{TP} + \text{TN} + \text{FP} + \text{FN}) \quad (5)$$

Equation (5), which is the ratio of the number of assessments to the number of correctly predicted values (where TN stands for true negative, meaning that a negative observation is correctly predicted as unfavourable), can be used to *figure* out how well a model finds correlations and patterns in datasets.

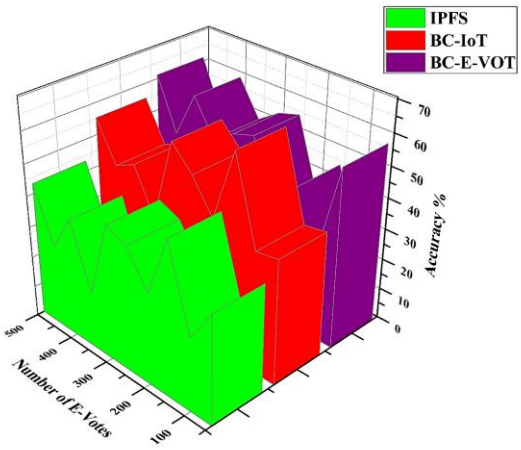


Figure 4. Accuracy

Figure 4 displays the Accuracy curves of the refined BC-E-VOT composites, as determined by *equation 5*. With e-votes ranging from 100 to 500, the 3D bar chart shows the accuracy percentages of IPFS, BC-IoT, and BC-E-VOT systems. Each system's performance is represented by a separate bar. A comparison of these systems' handling of the integrity and correctness of e-votes may be inferred from the accuracy percentages on the *y-axis*. The accuracy of IPFS (InterPlanetary File System) remains below 30% even as the number of electronic votes rises, demonstrating continual inferior performance. So, it seems like IPFS isn't designed to provide precise voting in this scenario. The accuracy of BC-IoT (Blockchain for IoT) varies from 20% to 60% based on the number of electronic votes. Its performance is generally better than IPFS, but it is unstable and experiences variations. Compared to IPFS and BC-IoT, BC-E-VOT (blockchain-based e-voting) always comes out on top regarding accuracy. Its accuracy ranges from 60% to 70%, so it seems to be a more dependable approach for managing electronic ballots. Based on these findings, the blockchain-based electronic voting system (BC-E-VOT) is a potential option for safe and precise electronic vote administration, outperforming the other two systems. High accuracy ensures that all votes are captured accurately, provided without error, and counted according to schedule, without manipulation or miscounts. If this assertion is to be assumed, the system must include strong error handling features like checksum verification and error correction codes to identify and fix transmission issues, protecting votes from corruption or loss. Further measures should be taken to ensure the authenticity of each vote by using data validation methods, such as comparing voter IDs with cryptographic signatures. In addition, there must be mechanisms in the system to deal with differences; for example, there should be a way to reconcile votes and keep track of audit trails, which include comparing logs to resolve inconsistent results and guarantee the correct counting of votes.

4.2 Trust Level

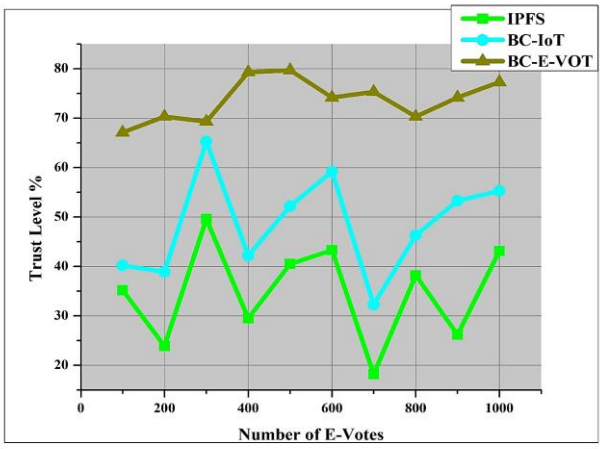


Figure 5. Trust Level

Figure 5 displays the Trust curves of the refined BC-E-VOT composites, as determined by *equation 1*. BC-E-VOT shows a consistently high trust level throughout, maintaining values around 70%–80%. This stability highlights its strong potential for being a reliable system in e-voting processes, with minimal fluctuation in trust as the number of e-votes increases. BC-IoT experiences more variation in trust levels, ranging between 30% and 60%. While it peaks at 60% when the number of e-votes is around 300–400, it tends to fluctuate more drastically compared to BC-E-VOT, indicating inconsistency in trustworthiness. IPFS generally performs the worst regarding trust, with values

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 4 | Pages 1381-1390 | e-ISSN: 2347-470X

oscillating between 20% and 40%. The trust level for IPFS is volatile, showing a tendency to drop significantly and fail to surpass 40% throughout the entire range of e-votes. In summary, BC-E-VOT is the most trusted system for handling e-votes, maintaining consistently high trust levels.

4.3 Security Level

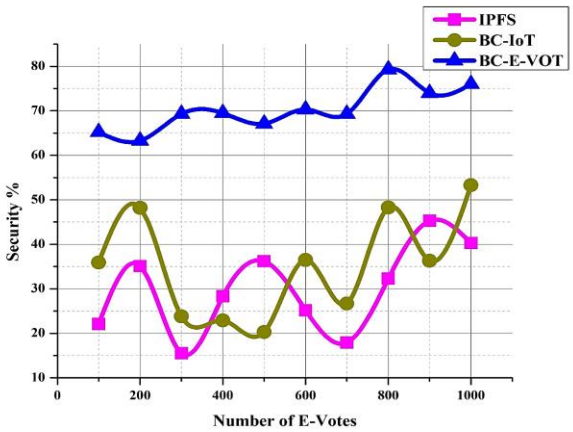
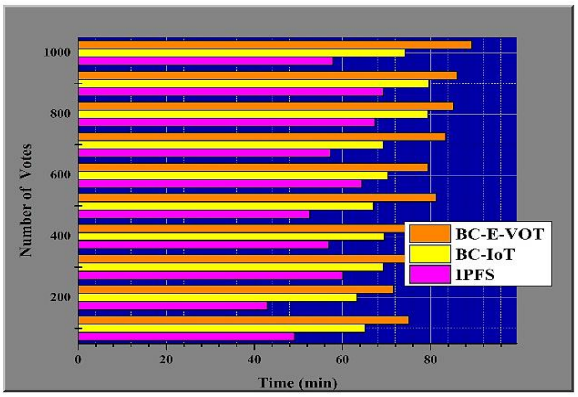


Figure 6. Security Level

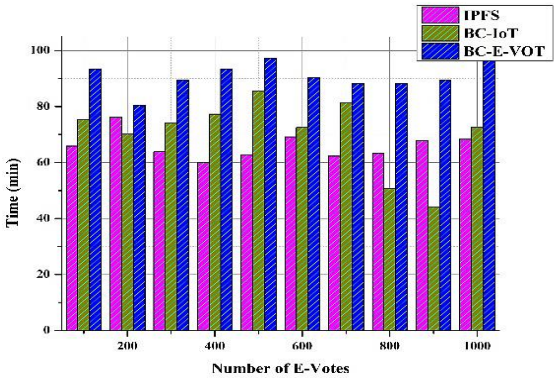
Figure 6 displays the Security curves of the refined BC-E-VOT composites, as determined by *equation 2*. By maintaining a security level of over 60% and increasing it to 75% with an increase in e-votes, BC-E-VOT displays the most significant levels of protection. Because of its consistent and robust security, BC-E-VOT is the best system for handling electronic voting. BC-IoT security has considerable volatility, ranging from 20% to 50%. The security levels are uneven, exhibiting poorer dependability compared to BC-E-VOT; however, there are times of stronger security, particularly between the 200 and 1000 e-vote marks. IPFS offers the least security, ranging from 20% to 40%. This confirms that IPFS isn't a good choice for safe e-voting apps due to its security flaws and poor performance when dealing with a high volume of votes. Finally, the safest system is BC-E-VOT, which constantly maintains high-security levels, compared to BC-IoT, which provides fluctuating intermediate security levels. When keeping electronic votes secure, IPFS performs the poorest and displays serious security flaws.

4.4 Paper Votes vs E-Votes

Figure 8(a) shows that paper voting is trusted and secure due to physical verification and recounts that reduce manipulation. Paper ballots are inconvenient, costly, time-consuming, and prone to error while counting. *Figure 8(b)* shows that electronic voting does not need human interference and gives results immediately. It is simpler and more scalable for international elections. However, public trust, voter anonymity, and cybersecurity issues remain. WSN platform might make computerized voting systems safer and more transparent, but public scepticism and security worries remain. Paper ballots are reliable, but computerized voting is more efficient. Modern elections need reliable digital solutions.



(a)



(b)

Figure 8(a) and 8(b). Paper Votes VS E-Votes

The system can implement effective identity verification protocols for validators and voters. These protocols can use biometric authentication or digital certificates to guarantee that only authorized individuals can access the system, thus reducing the risk of Sybil attacks. To secure continuous availability and avoid denial-of-service (DoS) assaults, the system might use rate-limiting mechanisms, distributed validation, and redundant server topologies. Including cryptographic nonce values or timestamped vote submissions prevents replay attacks, in which an attacker tries to disrupt the voting process by resending legal transactions. To further protect against data manipulation and man-in-the-middle attacks, robust, tamper-proof recording techniques (such as blockchain-based ledgers) and end-to-end encryption of vote data are recommended.

5. CONCLUSION

The use of digital voting technology to simplify, shorten, and lower the cost of the public political process is an enticing proposition regarding the usage of voting technologies today. In addition to standardizing the voting process in the eyes of the voters, making it inexpensive and quick reduces the power barrier between the voter and the elected official. It puts some pressure on the elected person. Other benefits include making the voting process more expensive and faster. It prepares the way for a democracy that is more participatory, in which people are allowed to have their voices heard about certain policies and activities. This research includes introducing a groundbreaking electronic voting system built on the Blockchain. This system

International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 4 | Pages 1381-1390 | e-ISSN: 2347-470X

uses smart agreements to ensure smooth and secure decisions while protecting voters' privacy. Detailed information on the system's design, architecture, and security analysis has been provided. Compared to previous studies, our results suggest that the WSN platform gives a novel possibility for democracies to convert their election systems from paper-based to digital ones. This can be accomplished while simultaneously improving the safety of the existing system and opening new possibilities for transparency. By using the smart contract to its maximum potential, an Ethereum private blockchain can process hundreds of transactions per second, dramatically minimizing the pressure placed on the network. Electoral fraud and tampering with vote results are possible vulnerabilities of conventional digital voting methods since they often depend on centralized infrastructure.

Regarding these problems and weaknesses, the WSN platform offers a solid alternative to conventional and other electronic voting methods. It has the potential to provide an open and secure platform where many organizations may carry out electronic voting procedures. Through the combination of conventions and encryption technologies, blockchain-based solutions provide transparent, safe, and auditable choices for the voting process. Unlike conventional voting methods, blockchain-based digital voting can optimize time and expenses.

REFERENCES

[1] Jayakumari, B., Sheeba, S. L., Eapen, M., Anbarasi, J., Ravi, V., Suganya, A., & Jawahar, M. (2024). E-Voting System Using Cloud-Based Hybrid WSN Platform. Journal Of Safety Science and Resilience, 5(1), 102-109.

[2] Lahane, A. A., Patel, J., Pathan, T., & Potdar, P. (2020). WSN Platform-Based E-Voting System. In Itm Web of Conferences (Vol. 32, P. 03001). EDP Sciences.

[3] El Kafhali, S. (2024). Blockchain-Based Electronic Voting System: Significance and Requirements. Mathematical Problems in Engineering, 2024(1), 5591147.

[4] Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2023). Blockchain-Based E-Voting Systems: A Technology Review. Electronics, 13(1), 17.

[5] Yadav, A. S., Urade, Y. V., Thombare, A. U., & Patil, A. A. (2020). E-Voting Using WSN Platform. Int. J. Eng. Res. Technol, 9(7).

[6] Indapwar, A., Chandak, M., & Jain, A. (2020). E-Voting System Using WSN Platform. Int. J. Of Advanced Trends in Computer Science and Engineering, 9(3).

[7] Chafiq, T., Azmi, R., & Mohammed, O. (2024). Blockchain-Based Electronic Voting Systems: A Case Study in Morocco. International Journal of Intelligent Networks, 5, 38-48.

[8] Ramesh, S. S., Venkataraja, D., Bharadwaj, R. N., Kumar, M. S., & Santhosh, S. (2019). E-Voting Is Based on WSN Platform. Int. J. Eng. Adv. Technol., 8(5), 107-109.

[9] Indapwar, A., Chandak, M., & Jain, A. (2020). E-Voting System Using WSN Platform. Int. J. Of Advanced Trends in Computer Science and Engineering, 9(3).

[10] Alabri, R., Shaikh, A. K., Ali, S., & Al-Badi, A. H. (2022). Designing An E-Voting Protocol Using WSN Platform: A Case Study of Oman. International Journal of Electronic Government Research (IJEGR), 18(2), 1-29.

[11] Al-Madani, A. M., Gaikwad, A. T., Mahale, V., & Ahmed, Z. A. (2020, October). Decentralized E-Voting System Based on Smart Contract by Using WSN Platform. In 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC) (Pp. 176-180). IEEE

[12] Naik, A. C., Prajapati, A. M., Pandey, S. N., & Mishra, A. C. (2023, April). Blockchain Based E-Voting System. In 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI) (Pp. 316-320). IEEE

[13] Jayakumari, B., Sheeba, S. L., Eapen, M., Anbarasi, J., Ravi, V., Suganya, A., & Jawahar, M. (2024). E-Voting System Using Cloud-Based Hybrid WSN Platform. Journal Of Safety Science and Resilience, 5(1), 102-109.

[14] Chentouf, F. Z., & Bouchkaren, S. (2023). Security And Privacy in Smart City: A Secure Routing E-Voting System Based on Blockchain. International Journal of Electrical and Computer Engineering, 13(2), 1848.

[15] Kumar, D. D., Chandini, D. V., Reddy, D., Bhattacharyya, D., & Kim, T. H. (2020). Secure Electronic Voting System Using WSN Platform. International Journal of Smart Home, 14(2), 31-38.

[16] Madhusudhan, R., & KK, V. (2024, April). A Protocol for Blockchain-Based Scalable E-Voting System Using Sharding and Time-Slot Algorithm. In International Conference on Advanced Information Networking and Applications (Pp. 432-443). Cham: Springer Nature Switzerland.

[17] Kumar, D., & Dwivedi, R. K. (2023, January). Blockchain And Internet of Things (IoT) Enabled Smart E-Voting System. In 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIOT) (Pp. 28-34). IEEE

[18] Abubakar, J. A., Oluwatobi, A., & Ademola, O. F. (2024). Advancing Democratic Governance with AIOT-Enabled E-Voting: A Case Study of Covenant University's Departmental Associations in Alignment with SDG 16. In Artificial Intelligence of Things for Achieving Sustainable Development Goals (Pp. 335-360). Cham: Springer Nature Switzerland.

[19] Ahmadieh, E., & El Madhoun, N. (2024, November). Comparative E-Voting Security Evaluation: Multi-Modal Authentication Approaches. In The Sixth International Conference on Blockchain Computing and Applications (Bcca 2024).

[20] Hussein, A. I., Maolood, A. T., & Gbash, E. K. (2023). A Review: E-Voting Security in Mobile Fog Computing. Iraqi Journal of Computers, Communications, Control and Systems Engineering, 23(1).

[21] https://datasetsearch.research.google.com/search?src=0&query=E-voting%20based%20on%20Blockchain%20technology&docid=L2cvMTF3OW12MHdkcQ%3D%3D

[22] Abed, H., Al-Zoubi, O., Alayan, H., & Alshboul, M. (2024). Towards Maintaining Confidentiality and Anonymity in Secure Blockchain-Based E-Voting. Cluster Computing, 27(4), 4635-4657.

[23] Muthulakshmi, S., & Kannammal, A. (2024). Preventing Double Spending Attacks Through Crow Search Algorithm to Enhance E-Voting System Security. Eai Endorsed Transactions on Internet of Things, 10.

[24] Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2023). End To End Secure E-Voting Using Blockchain & Quantum Key Distribution. Materials Today: Proceedings, 80, 3363-3370.

[25] Chentouf, F. Z., & Bouchkaren, S. (2023). Security And Privacy in Smart City: A Secure E-Voting System Based on Blockchain. International Journal of Electrical and Computer Engineering, 13(2), 1848.