# A Secure Electronic Voting System Using Multifactor Authentication and Blockchain Technologies

O.M. Olaniyi[1*], E.M. Dogo[2], B.K. Nuhu[3], H. Treiblmaier[4], Y.S. Abdulsalam[5],

Z. Folawiyo[6]

[1,2,3,6] Department of Computer Engineering, Federal University of Technology, Minna, Nigeria.
[4]Department of International Management, Modul University, 1190 Vienna, Austria.
[5]DNA Lab, Department of Computer Science and Engineering, University Mohammed VI Polytechnic, Ben Guerir, Morocco
[*]mikail.olaniyi@futminna.edu.ng

**Abstract.** This paper presents a distributed e-voting system that solves the problems of vote-rigging, voter impersonation, and vote falsification, all of which are prevalent in traditional paper ballot systems. In general, the digitization of democratic decision-making is convenient, fast, and cost-saving but can become a gateway for electoral fraud if not properly secured. Authentication and the simultaneous achievement of confidentiality, integrity, and availability represent major challenges toward establishing e-voting as a reliable means of democratic decision-making. In this paper, a combination of multi-factor authentication (MFA) and blockchain techniques is used to secure electronic voting. MFA hampers the compromising of voters' identities and allows for easy verification, while blockchain technology protects the integrity of the votes and ensures the verifiability of the cast votes. Combining a facial recognition algorithm and RFID authenticates and authorizes voters to participate in the election process. A smart contract implemented on an Ethereum network provides the required measures of integrity and verifiability for secure e-voting. Performance evaluations of the proposed approach show that the MFA yielded a 0.1% false acceptance rate and a 0.8% false rejection rate for 100 voters, respectively. This illustrates that the proposed technique can solve issues of authentication and integrity, thereby paving the way for free, fair, and credible e-democratic decision-making in digitally-enabled voting scenarios.

**Keywords:** Biometrics, data communication, distributed system, security and privacy protection, smart cards.

# 1 Introduction

Voting is a fundamental component of a consensus-based society practicing a democratic system of governance. Citizens' voting rights must be confidential and strictly based on the "one person, one vote" principle exercised through either traditional or electronic voting systems [1]. Historically, most elections in developing countries are manipulated, and the announced results are frequently based on a non-transparent underlying electoral system [4], [5]. The electoral process is frequently characterized by problems ranging from ballot stuffing to bribery, manual counting errors, problems in the delivery of election materials from central locations to polling centers, external interference by agents handling election materials or voting database management, inconclusive ballots, high election-related costs, as well as time-consuming and non-transparent processes in general [5]-[8]. Therefore, voters are concerned whether their preferred choice in the electoral process will count and whether the votes recorded and collated truly represent the general interest of the populace [2].

In Nigeria, for instance, recent elections have adopted a semi-automated paper ballot system to address the challenges associated with the previous paper ballot system. However, despite these efforts by the electoral body in Nigeria, many of the challenges associated with conducting free and credible elections persist [3]. To provide a competitive advantage over the traditional paper ballot voting system, an electronic voting system requires security measures both during the authentication and vote casting processes [9]. In this regard, electronic voting machines have been shown to have technical and socio-technical vulnerabilities [9]. To achieve a competitive advantage, electronic voting systems must meet technical security requirements such as eligibility, coercion freeness, availability, anonymity, integrity, correctness/accuracy, robustness, fairness, receipt-freeness, voter verifiability, and universal verifiability [10]. Huge varieties of security measures are suggested in the scholarly literature to meet these requirements, including biometrics, security firewalls, cryptography, smart cards, steganography, and crystography (i.e., the combination of cryptography and steganography) [10], [11].

Existing centralized trust-based systems such as secure electronic voting in [13], [19], [33] are vulnerable to distributed denial of service (DDoS) and Sybil attacks from malicious users and provide no mechanism to track possible compromises of the electoral process by either internal or external actors [4]. Furthermore, they lack real-world deployment. To avert these possible electoral frauds, we propose a MFA mechanism in combination with a public blockchain network that ensures the required integrity of a vote in a decentralized database environment on a cloud/edge computing [14] architectural arrangement. Facial recognition and Radio Frequency Identification (RFID) techniques confirm voter identification, and verification averts possible insecurities through the authentication of invalid voters. Blockchain technology can help avert possible integrity, verification, and auditing issues, both during and after electoral processes. The proposed public blockchain contains transactions in the form of blocks, whereby each block is linked with the previous block using a cryptographic hash algorithm. The hash contained in the blocks makes use of the SHA-256 algorithm, and all blocks are distributed to each node on the network to avoid a central point of attack, which is a common weakness of existing electronic voting mechanisms.

This paper presents the development of a secure decentralized electronic voting system using MFA and blockchain techniques. MFA is a security approach that uses more than one means of authentication from independently available credentials to accredit a person's eligibility to vote [10]. It is widely recognized as the most secure method for authenticating access to data or a specific application [10], [12], [38]. The more the authentication factors exist to determine a subject's identity, the greater the authenticity trust. This paper specifically addresses security flaws of semi-automated electronic voting systems that frequently occur in developing countries [3]. Existing problems that motivated this research to secure the electronic voting systems are: (1) centralized data at a single location, (2) vulnerabilities to cyber-security attacks, (3) the problem of validating voters' identity, (4) lack of transparency, trust, and forgery during the electioneering process. Applying the proposed security mechanism will help increase the robustness in the authentication phase of future electronic voting systems and guarantee an uninfluenced, fair, and transparent election during and after the voting process.

The remainder of this paper is organized as follows: Section 2 gives a brief overview of similar works in the problem domain. Sections 3 to 5 present the materials, methods, and findings from the study. Section 6 contains the performance evaluation. Section 7 presents the security analysis, and Section 8 concludes the paper and suggests future research endeavors.

## 2 Review of Related Works

Several electronic voting systems that include various security mechanisms have been proposed in the academic literature, some of which are based on blockchain. Table 1 shows a synthesis of previous approaches. Over the years, blockchain-based electronic voting systems have emerged widely and replaced paper ballot systems for securing and providing trust to ensure transparent e-voting. Several papers have demonstrated the use of blockchain by using different consensus protocols such as Proof-of-Stake (PoS) and Proof-of-Work (PoW). Hardwick et al., [26] proposed a blockchain-based decentralized system that offers voters a dynamic way of updating and changing votes during e-voting. Their approach supports complex voting situations but does not provide auditability, consistency, and user privacy. Kshetri and Voas [27] proposed an e-voting system that allows voters to pay a certain amount to cast votes without the problem of double-spending. This scheme, however, lacks scalability due to the excessive workload on nodes during simultaneous executions.

Bartolucci *et al.* [28] proposed an Ethereum-based blockchain system that implements the circle shuffle technique for registering. Their proposed system provides a trusted environment for transparent voting processes but necessitates the use of a trusted authority. The limitation of their proposed system is that if at any point the trusted authority goes malicious, then the entire system becomes compromised. Giving the sensitivity of information during a voting process, issues of susceptible rogue parties are to be avoided at all costs. Thuy *et al.* [29] proposed the Votereum blockchain-based voting system on Ethereum, ensuring security and privacy. Their proposed solution supports requirements such as verifiability and robustness but lacks resisting coercion and receipt-freeness. Yavuz *et al.* [30] proposed a voting application that uses smart contracts on the Ethereum blockchain and is based on an android platform. However, their proposed scheme lacks robustness and receipt-freeness.

Other blockchain platforms such as Hyperledger Fabric have also been used to ensure transparency during e-voting. Hyperledger Fabric is a private permissioned network that does not rely on the use of smart contracts or cryptocurrency. Previous research illustrated the use of Hyperledger Fabric for ensuring end-to-end privacy during e-voting, providing correctability and detectability, but also exhibits a lack of coercion resistance [31, 32]. Oke *et al.* [10] developed an MFA technique (i.e., a biometric fingerprint combined with a cryptographically secured smart card) to secure the e-voting system's authentication. An enhanced Feistel block cipher is used to secure confidential data on voters' smart cards, and a first-moment feature extraction technique secures the voter's fingerprint template. This system deals with issues encountered during authentication but fails to secure the integrity of the cast votes once stored in the database.

Ashok *et al.* [2] applied RFID and fingerprint technologies for authentication in an

electronic voting system. Each voter has an ID in the form of an RFID tag and has his/her fingerprints scanned for comparison with the ones stored in the user's profiles. While overcoming voter authentication issues, this system also fails to protect the integrity of the vote once cast. In Fusco *et al.* [6], the authors propose methods to improve the traceability and auditing of voting operations using blockchain technology. Their system, however, does not present any means for authenticating the user for the election.

The security mechanisms presented in academic literature such as [4], [6], [7], [9], [15]-[18] solve either authentication or confidentiality issues surrounding e-voting, and some even manage to solve both problems, but none meets the multiple security requirements of authentication, confidentiality, integrity, and verifiability, all of which are crucial to delivering credible electronic democracy through e-voting. This research solves these critical security requirements by proposing MFA using facial recognition and RFID cards combined with a public blockchain. Table 1 shows the synthesis of related works in this domain.

**Table 1**: Synthesis of recent related works.

| Reference | Work Description | Limitations |
|---|---|---|
| [12] | Mechanism for securing an e-voting system using MFA and cryptographic hash functions. | The authentication mechanism proposed is a single factor that can easily be compromised |
| [2] | This voting system applies RFID and fingerprint technologies for voters' authentication. | No extra layer of protection is added to the RFID technique, thus posing an open door for masquerading voters. |
| [18] | Enhanced stegano-cryptographic model for a secure electronic voting system in the voting station. | Neglects key requirements of an electronic voting system, such as checking the identity of the voters. |
| [19] | Unimodal fingerprint biometrics and Advanced Encryption Standard-based Wavelet-based crypto-watermarking approach. | The system stores the vote cast in a centralized server that a malicious third party can compromise. |
| [7] | Applies an RFID reader module which senses the RFID tags with unique identity that is serially controlled by an embedded system. | Similar to the limitation of Ref [2] |

| | | |
|---|---|---|
| [10] | MFA technique via biometric fingerprint and cryptographically secured smart card to secure an e-voting authentication process. | Fails to secure the integrity of the cast votes stored in the database. |
| [16] | A secure private blockchain-based electronic voting system for a university election. | The system fails to address the issue of authentication to verify the voter's identity |
| [3] | Proposes blockchain technology to replace an existing manual or semi-digitized e-voting system. | Neglects several key requirements of an electronic voting system, such as repudiation, confidentiality, and privacy. |
| [8] | Multilayers security scheme based on a hybrid RSA algorithm and AES algorithm with a Least Significant Bit Steganographic algorithm | The scheme lacks design consideration for averting possible impersonation of ineligible erring voters through proper identification and verification measures. |
| [9] | Addresses the voter eligibility problem through the development of a fingerprint biometric authentication system for secure electronic voting machines. | The scheme design consideration fails to observe the integrity and verifiability of the vote. |
| [17] | Explores the use of biometric smart cards for voter verification and identification. Adopting this method will enhance the electoral process by ensuring that only registered voters can cast votes. | This approach does not address the issue of confidentiality of the vote cast by the user. |
| [33] | Presentation of a Secure and Verifiable Polling System (SeVEP) scheme that implements MFA and well-known cryptographic techniques to achieve privacy, verifiability, authorized multiple voting and prevents double voting. | The proposed system lacks scalability and usability in a real-world deployment. |

# 3 Preliminaries

## 3.1 Blockchain in E-voting

Blockchain has emerged as a trustless system used in several domains to ensure data integrity. It has been implemented in e-voting systems and has become an important option in overcoming various security challenges [34]. Blockchain-based e-voting systems have been predicted to be the next generation of modern e-voting due to their decentralized and distributed nature. A blockchain network is suitable for e-voting because transactions are time-stamped when recorded and cannot be modified after being validated. Also, certain blockchains offer programmability via smart contracts and are secure through encryption. Most importantly, blockchain is a distributed ledger technology, where all participating full nodes in the network maintain a copy of the ledger to ensure transparency.

A blockchain is a linear combination of blocks representing different data elements. These blocks are linked using a cryptographic collision-resistant hash function to form a chain of connected blocks (see Fig. 1). To concatenate each block or transaction data in a blockchain, a hash pointer links a block to a previous block. This pointer also creates an integrity check, allowing only verified blocks to be included in the blockchain [37].

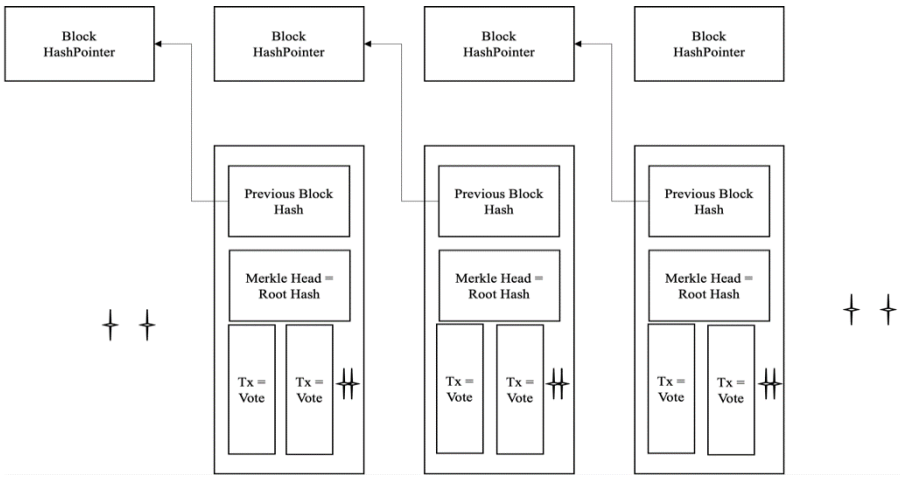



Fig 1: Representation of a blockchain.

Blockchain networks can be classified into private and public networks and hybrid solutions that combine both types. A permissioned setting allows only designated peers to participate in the consensus agreement protocol [34], and only authorized users can contribute and modify block information. A public and permissionless blockchain does not limit the number of peers who can participate in the consensus protocol. All participants can record block information. The most common public blockchains type available include the bitcoin network [35] and Ethereum [36]. In this type of blockchain, its decentralized public nature serves as a distributed ledger to immutably record transactions between participants.

A distributed ledger is inherently resistant to modification and verifiable by authorized users. In our proposed scheme, we deploy the Ethereum blockchain to build a secure e-voting system. The Ethereum blockchain is easily accessible due to its popularity and makes use of a state transition system. The different states make it possible for new blocks to be easily verified when they are added to the blockchain. When a vote has been cast and verified in our proposed scheme, a transaction is hashed and added to the blockchain. We made use of the SHA-256 hash function, which is a collision resistance one-way function.

### 3.2 Multi-factor Authentication

MFA is a way of authenticating end-users (voters) in two or more different ways that establishes access control and identity. MFA includes three different ways of authentication: something you have (e.g., a smart card), something you know (e.g., passwords in the forms of tokens), and something you are (e.g., biometric or face recognition). In our proposed scheme, two-factor authentication is used to verify the entire e-voting process. The first level of authentication is microcontroller data verification. The microcontroller compares the data newly supplied by the RFID module with that stored in the database during authentication. Suppose the microcontroller confirms that the data matches its counterpart in the database. In that case, it sends a string of data to the software application to grant the user access to navigate to the second phase of the authentication. Facial recognition is implemented during the second phase of the authentication. The software application contains a facial recognition web interface that takes a picture of the user's face and compares it with one already stored in the database. In case of a match, the user is granted access to the voting page.

# 4 System and Threat Model

The system model of our proposed design consists of three main participants described as follows:

1. Voters: These are all eligible voters denoted as: $V = \{v_1, v_2, v_3 \ldots, v_n\}$ , where n is the total number of eligible voters.

2. Voting Authority: This contains a set of all Election Administrators (EA) = 1, responsible for the management and verification of voters' identity during the election.

3. Auditors: Agents responsible for inspecting EA compliance to election norms and monitoring the power of the EA.

The framework of the proposed blockchain voting system contains the participants = {Voters}, EAs = {Poll sites under the districts}, Auditors = {EA representative}, Hash algorithm = {SHA-256} and voting server.

## 4.1 Threat Model

In an e-voting system, a malicious user can exploit different attack scenarios, as summarized in Table 2. When using blockchain for e-voting, issues such as double voting can arise in which an authenticated malicious voter can attempt to cast multiple votes without being detected. Voter coercion can occur by persuading a voter to vote for a particular option. This can be accomplished only when a voter provides the coercer with his/her voting credentials, such as the private key. Voting modification or interruption by a malicious voter or device can also occur as a result of an infected malware or by being controlled by an attacker.

In all these cases, the option selected by the voter can be inadvertently modified before submission, which can result in falsely counting polling votes. In terms of coalition attacks, voters can collude with the voting authority to affect the transparency of the voting experience, and they can also form a coalition to affect the polling option or even modify ballot options. When using biometrics for authentication, the security of the biometric templates can be undermined through attacks using keystrokes and voice patterns stored in the database. Storing biometric templates in a plain format without encryption can result in gaining access by an unauthorized attacker. Also, records stored in the database can be modified or stolen by any malicious individual, granting them access to enrolling a voter.

**Table 2**: Threat model scenario in an e-voting system

| Threat Scenario | Forged private key | Malicious Auditor with access to storage | Unauthorized network provider | Rogue voting device | Malware infected operating system |
|---|---|---|---|---|---|
| Double voting | • | • | • | • | |
| Unauthorized administrative access | • | • | • | | |
| System modification | • | • | • | • | • |
| Vote coercion | • | • | | • | • |
| Audit log tampering | • | • | • | | |
| Transparency | • | • | • | • | • |
| Biometric attacks | | • | • | | |

## 5 Proposed E-voting System

In this section, we present the mechanisms and procedures, as well as the selected hardware subsystems and the software design considerations used in the realization of the proposed secure electronic voting system. The block diagram of the system is shown in Fig. 2 and the proposed system architecture in Fig. 3. They outline the structure of a decentralized database to store the encrypted votes, in essence making it more difficult to modify or alter a vote once cast. The architecture is robust with two-way authentication, which helps prevent unauthorized users from accessing the system or casting a vote.

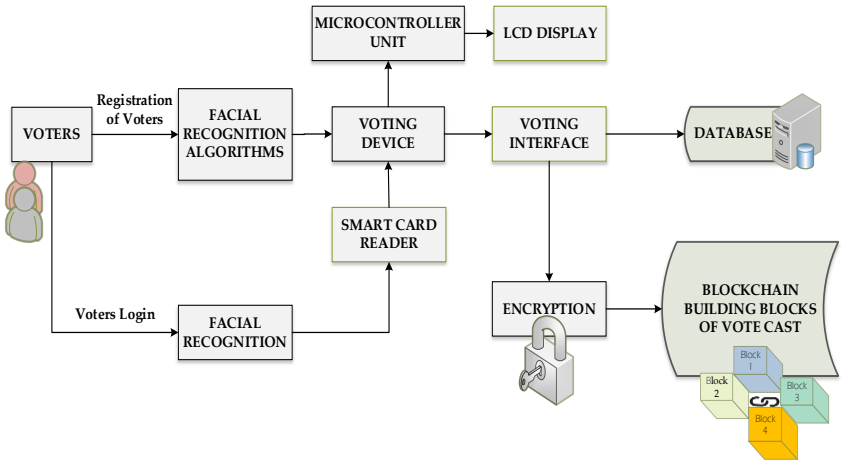



**Fig. 2**: Block diagram of the secured e-voting system.

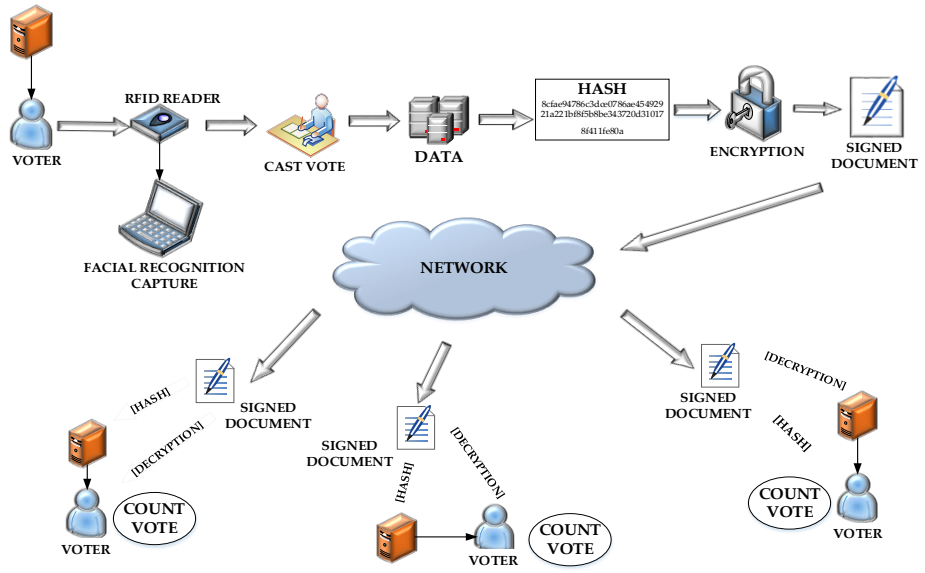



**Fig. 3**: Proposed secured e-voting architecture.

### 5.1 System Hardware Design Consideration

This section presents the integration and design process of the system hardware components. More specifically, it describes the authentication module, the microcontroller unit as a whole, and the interaction of the various components in the process of authenticating valid eligible voters. The components include an Arduino ATMEGA, an LCD, a personal computer, an RFID reader, and an RFID card reader, as depicted in Fig. 4.


**Fig. 4**: Mifare 13.56Mhz RC522 RFID card reader.

RFID is a contactless auto-identification system similar to smart cards. It enables the electronic labeling and wireless identification of an object using frequency-shift keying (FSK) modulation [20]. Information exchange in an RFID system is done via radio waves where no contact or line of sight is needed for the identification process. This makes RFID relatively secure since readers can be designed to locate tags at a distance of several meters [21]. As a contactless auto-ID system, reading and writing of data in the RFID system are done through an RFID tag's non-volatile memory using an RF signal by the reader. The reader emits an RF signal, and data is exchanged when the tag comes in proximity to the reader signal. Tags can be categorized as follows: a) active tags in which a battery supplies power and which are therefore costly; b) semi-passive tags that use batteries to power the tag IC but not for communication; and c) passive tags that have a battery. The absence of a power supply makes passive tags cheaper and more reliable than active tags.

Due to cost considerations, our e-voting authentication system is designed using a passive RFID reader (i.e., MF-522ED) that can only detect a passive RFID tag at a few centimeters away from the reader. The reader operates with contactless communication and uses MIFARE transfer speeds up to 10Mbit/s in both directions [22]. The specific RFID reader used in the system is a low-cost reader for reading passive RFID tags, as shown in Fig. 3. It operates at temperatures between 20° C and 80° C, humidity levels between 5% and 95%, at a frequency of 13.56MHz, a working current of 13-26mA/3.3V DC, and a standby current of 10-13mA/3.3V DC power supply [22]. The effective detection range of the MF-522ED reader is around 5-8cm. Each RFID tag has a unique serial number or ID. In this design, each voter is identified through the passive RFID card/tag. Fig. 5 illustrates how data transmission is performed between an MF-522ED RFID reader and a voter's card/tag.

The design of the second factor, namely facial recognition, implements a face API library. Face API is a JavaScript module built with the TensorFlow open-source software library, which implements several Convolutional Neural Networks (CNNs) to solve face detection, face recognition, and face landmark detection, optimized for the web and mobile devices [23]. This system implements three face API models for facial recognition authentication: Tiny Face Detector Model, Face Recognition Model and Face Expression Recognition Model [23]. The Tiny Face Detector is a real-time face detector, which is fast and consumes few resources. The Face Recognition Model is an architecture implemented to compute a face descriptor for any given image. The Face Expression Recognition is a lightweight, fast, and reasonably accurate approach to match the facial expressions of a given image. The face API at the point of registration detects the human face and draws a canvas around it. The library gets the image of the detected face in the canvas and converts it to a float array, which is then saved to the blockchain.

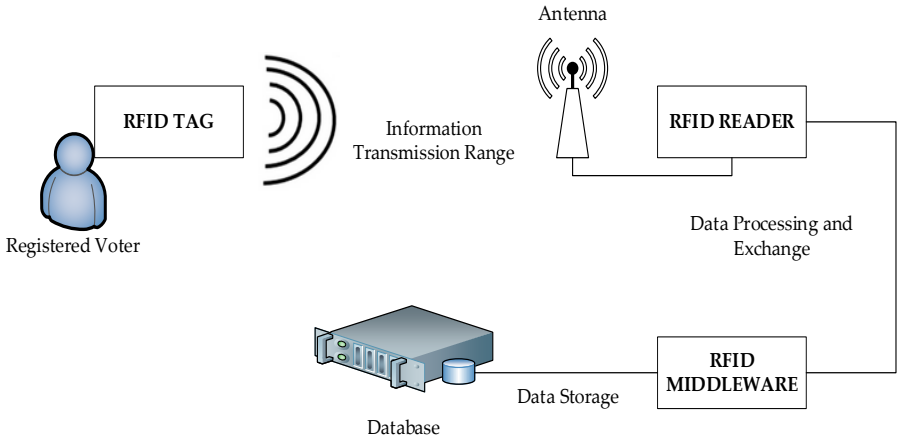



**Fig 5**: Data transmission process between an RFID reader and an RFID tag.

During authentication, a new image of the detected face is taken and is then converted to a float array by the face API. The library verifies the similarity between the image taken at the point of registration and the image taken during authentication by computing the mean distance between the float arrays. The distance threshold is 0.6 meters, and if the mean distance between the arrays is greater than 0.6 meters, then the face does not match. But if the mean distance between the arrays is less than 0.6 and the face matching is successful, then the users are granted access to vote. The facial recognition implemented in this system has a very high capacity and works efficiently on a Windows 10 HP, 6$^{th}$ generation Intel Core i5 (2.3- 2.8GHz) processor, 8GB RAM, and 500GB Hybrid Hard drive. The system might not work efficiently on systems with less capacity.

### 5.2 System Software Design Consideration

The system software structure comprises the client web application and the Facial Recognition Application (FaceAPI). The client web application provides an interface for the user to interact with the hardware components and connects to both the private blockchain and FaceAPI to ensure vote security and authentication, respectively. It allows the voters to gain access to the voting interface after comparing the password and username, unique facial recognition ID of the voter and verified RFID ID of the voter. The voting interface allows voters to cast votes for their preferred candidate. In this proposed design, the blockchain provides the required integrity, verifiability, and post-electoral auditing of ballots based on a tamper-resistant public ledger for assurance of security and reliability of the distributed stored data.

The proposed system implements a permissioned private blockchain in which only those who have permission can join the Ethereum blockchain network. The blockchain is based on hashing, encryption, and decentralization. A private key is issued to each voter during registration. The private key is used to generate signatures on the vote during the election. The encrypted data are shared across the nodes in the blockchain, which makes it a decentralized system. The design considerations of blockchain technology in our proposed secure and robust voting mechanism extend work from Singh and Chatterjee [16] and integrates MFA of voters.

***Pre-election steps:***

1. The voters need to register with the voting system. In the first step, the voters are required to:
   a) Obtain a unique ID through the RFID tag/card.
   b) Pre-enroll the facial image of the voter and obtain a Unique Facial ID (computed mean distance between the floating array stored image and real-time captured image).
   c) Choose a unique password for login.
2. After successful registration with the system, the voter receives a voter ID.

***Main voting steps:***

1. During the election period, the voter approaches the kiosk at the poll site, is then authenticated using the RFID tag ID and the generated Face ID and can log in with their assigned password.
2. After the successful login, the voter is verified by the EA and Auditors.
3. If the voter is eligible for voting through the successful verification in step 1, the client web application allows the voter to vote for his/her preferred candidate from the list of contestants.
4. The preferred vote/ballot is hashed with SHA-256 to assert vote integrity by the client Web Application.
5. The hashed vote is signed for each voter by the voter's private key.
6. The signed, fingerprinted, and encrypted vote is then stored in the voting server. This is the first block of the blockchain.
7. Steps 1 to 6 are repeated for each legitimate voter, with each vote forming a new block that is added to the existing chain for the duration of the election period.

***Post-election steps:***

1. After the election is over at each poll site level, the individual blockchains of each poll site within the districts are joined together for the preparation of the zone-level blockchain.
2. The zone-level blockchains are joined together for the preparation of the state-

level blockchain.

3. Finally, the EA and Auditors check all the votes from the blockchain and declare the final result of the election.

The pseudo-code of this procedure is detailed in Algorithm 1, and the system flowchart is shown in Fig. 6.

**Algorithm 1:** Voting Procedure

**Input:** voter unique id tag, voter face id
**Output:** Complete vote in the form of blockchain
**Begin**

1. The voter registered with the voting system.
2. Get the Voter Unique Tag Id and Voter Face ID and generate a private key.
3. If (Voter Unique Tag Id == registered voter Id) and (voter is eligible) and (Voter Facial Image == registered face ID), then go to step 4 else go to step 11.
4. Enter your password.
5. If Voter Unique Tag Id is not registered or he/she is not eligible or unregistered Face ID then deny voting and go to step 11, else go to step 6.
6. If (Password is correct) then go to step 7, else go to step 8.
7. Open the candidate choosing page, choose the candidate to vote, and go to step 9.
8. Enter the correct password and go to step 6.
9. Signing the encrypted data - SIGNV pricey (ENCRYPT(vote))
10. Generation of the block BLOCK (block header+ block data).
11. **End**

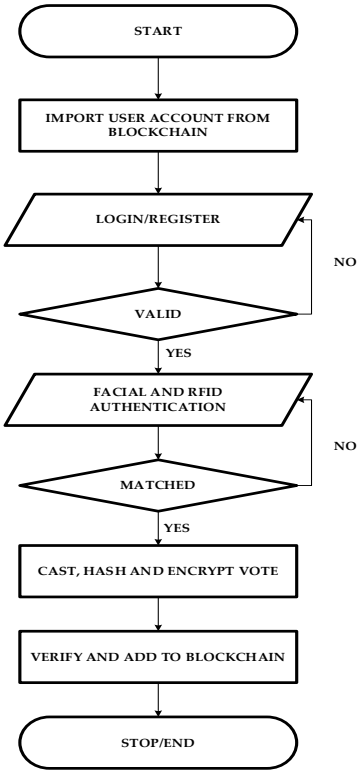



**Fig. 6**: System flowchart diagram

## 6 Performance Evaluation

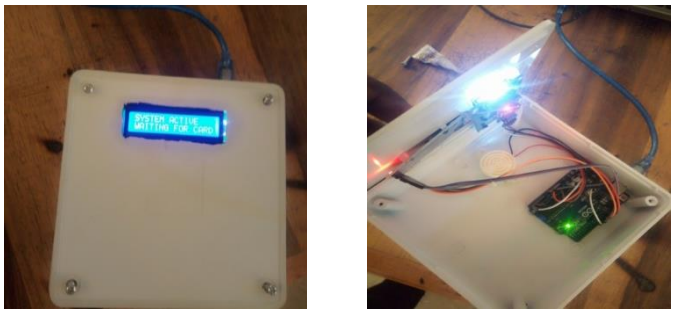
The hardware component comprises the RFID module, Liquid Crystal Display, and an Arduino Uno microcontroller development board. The software component consists of the facial recognition program and blockchain solution, which implements SHA 256 to encrypt votes. The RFID module validates the authentication in the electronic voting system. The Arduino Uno microcontroller receives a direct 5V current through its USB connector, from which both the RFID module and the LCD are powered. When the RFID reader module is powered ON, it automatically detects and reads the data from an RFID tag/card data placed in the immediate vicinity of the module and transmits a signal to the microcontroller unit to decide on whether to grant access to vote or not.

The evaluation metrics used for the facial recognition process of the electronic voting system are False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR is the probability of cases where the system wrongly authorizes an unauthorized person; the equation for computing FAR is given in (1). FRR is the probability of cases where the system wrongly denies access to an authorized person; the formula for computing FRR is given in (2). The permissioned private blockchain technique was evaluated based on transaction time and transaction cost per voter. Meanwhile, the RFID auto-ID technique was evaluated based on the transmission distance between the tag and the reader. The overall system was evaluated based on the response time.

$$\text{False Acceptance Rate (FAR)} = \frac{\text{Number of False Acceptance}}{\text{Number of Identification Attempts}} \tag{1}$$

$$\text{False Rejection Rate (FRR)} = \frac{\text{Number of False Rejection}}{\text{Number of Identification Attempts}} \tag{2}$$

The prototype of the authentication system presented in the previous section is shown in Fig. 7a and 7b.



(a) (b)

**Fig. 7**: (a) System authentication module and (b) module internal hardware integration

Fig. 7b shows the hardware integration of the Arduino microcontroller, LCD, and an RFID module. The system is powered by an Arduino USB cable connected to the computer system that hosts the web application, as shown in Fig. 7a. The RFID card of the voter is placed on the system module in Fig. 7a. The RFID reads the information on the card and compares it with the data stored inside the blockchain to grant voters access to vote or register. The performance of the RFID was evaluated by examining the read rate of voters' tags against the reader, as shown in Table 3. The read rate is the degree to which an RFID module reads tags with varying distances during voter authentication. Table 3 shows that the RFID module detected all tags up to 3.5cm.

**Table 3**: The read rate of the voter's card against distance

| S/N | Distance (cm) | No of tags (N) | Read rate (R) | Read rate $\left(\frac{R}{N} * 100\right), \%$ |
|---|---|---|---|---|
| 1 | 0.5 | 15 | 15 | 100 |
| 2 | 1.0 | 15 | 15 | 100 |
| 3 | 1.5 | 15 | 15 | 100 |
| 4 | 2.0 | 15 | 15 | 100 |
| 5 | 2.5 | 15 | 15 | 100 |
| 6 | 3.0 | 15 | 15 | 100 |
| 7 | 3.5 | 15 | 15 | 100 |
| 8 | 4.0 | 15 | 0 | 0 |
| 9 | 4.5 | 15 | 0 | 0 |
| 10 | 5.0 | 15 | 0 | 0 |

The software prototype for the system includes the client web application, which contains different interfaces for registration, login and vote casting, and result viewing. During registration, the voters need to obtain a private key required to import an account from the blockchain to the web browser and to encrypt the message sent to the blockchain. This is shown in Fig. 8.

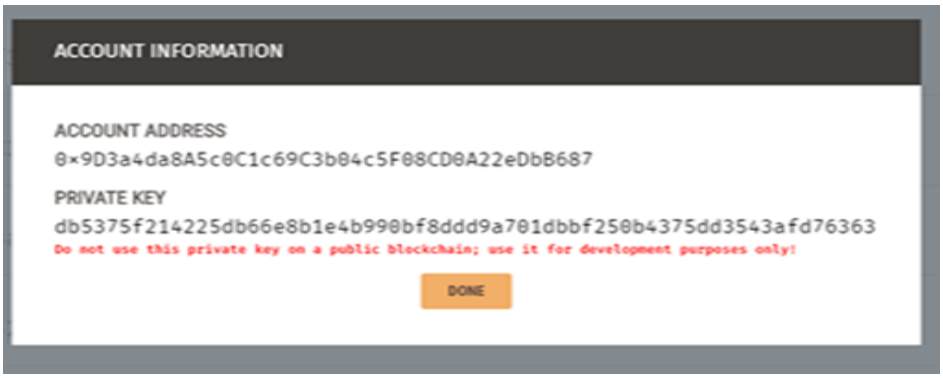



**Fig. 8**: The private key of an account

After obtaining the private key for the voters, the account address is obtained from the blockchain using the MetaMask software. The process is as shown in Fig. 9.

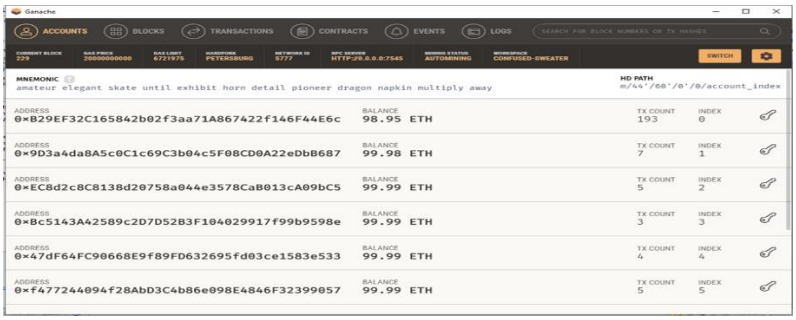



**Fig. 9**: Accounts in the blockchain

After proper prior registration, the interface in Fig. 10 provides a platform for voters to provide all means of authentication of the system before being granted access to cast a vote in the election. Fig. 11 provides the platform voters use to express their vote after being successfully authenticated.

**Fig. 10**: Authentication after a successful registration

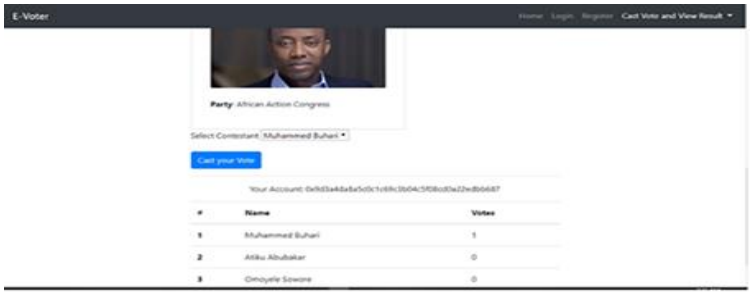



**Fig. 11**: Voting after successful MFA.

Table 4 shows the result of ten different voters' trials at facial recognition authentication to ascertain the module's efficiency. The FAR of the system was calculated using (1). It can be observed from Table 4 that out of 10 false face match attempts made, only one was granted access by the system. The false acceptance rate of 10% in the system is low, especially considering that this is just one part of the MFA system, and the single failed trial can likely be explained by the rotated and exaggerated skin distortion of the participating subject [24].

**Table 4**: FAR of the developed System

| Matching Tries | Accepted | Rejected | FAR |
|---|---|---|---|
| 10 | 1 | 9 | 10% |

The system False Rejection Rate (FRR) was subsequently investigated. From Table 5, it could be observed that in all the attempts made to match a valid voter face with the one saved in the database, the rate of voter rejection is low. Table 5 shows that, while each valid voter was rejected at least once, these rejections comprise only a small percentage of the attempts made by each voter. From this low FRR, it can be deduced that the facial recognition authentication system is sufficiently reliable for authenticating voters in an election.

**Table 5**: FRR of the developed system

| User | Number of attempts | Number of times Accepted | Number of times Rejected | FRR (%) |
|---|---|---|---|---|
| 1 | 12 | 11 | 1 | 8.3 |
| 2 | 12 | 11 | 1 | 8.3 |
| 3 | 15 | 13 | 2 | 13.3 |
| 4 | 12 | 11 | 1 | 8.3 |
| 5 | 15 | 13 | 2 | 13.3 |

Similarly, the effectiveness of blockchain was investigated by examining the transaction execution time and the transaction fees for ten nodes. Table 6 shows the transaction execution time and the required transaction fees during election registration and casting of the vote to evaluate blockchain speed when 10 nodes are connected to the blockchain network. Transaction speed is the time taken to add a new voter and add a casting vote to the blockchain. A transaction fee is a monetary cost required to register a voter and to cast a vote in the blockchain.

**Table 6**: Transaction execution time and transaction fees for ten nodes

| S/N | Transaction Execution Time (Minutes) | | | Transaction Fees (Ether) | | |
|---|---|---|---|---|---|---|
| | Slow | Avg. | Fast | Slow | Avg. | Fast |
| 1 | 11.54 | 1.12 | 0.30 | 0.0012 | 0.0029 | 0.0097 |
| 2 | 8.30 | 1.24 | 0.30 | 0.0014 | 0.0023 | 0.0096 |
| 3 | 10.12 | 1.48 | 0.36 | 0.0014 | 0.0025 | 0.0096 |
| 4 | 1.24 | 1.24 | 0.36 | 0.0035 | 0.0035 | 0.0074 |
| 5 | 24.18 | 3.24 | 0.30 | 0.0010 | 0.0030 | 0.0074 |
| 6 | 13.24 | 3.48 | 0.36 | 0.0014 | 0.0048 | 0.0096 |
| 7 | 23.48 | 3.48 | 0.30 | 0.0010 | 0.0027 | 0.0074 |
| 8 | 1.30 | 1.30 | 0.36 | 0.0018 | 0.0018 | 0.0074 |
| 9 | 1.30 | 1.30 | 0.30 | 0.0018 | 0.0018 | 0.0074 |
| 10 | 13.24 | 1.12 | 0.36 | 0.0014 | 0.0029 | 0.0074 |

The transaction execution time of slow, average, and fast with a corresponding transaction fee when ten nodes were investigated is shown in Table 6. Slow and average transaction execution times are determined by the network when an attempt is made to reduce registration and voting costs, while the fast transaction execution time is used when trying to increase the speed of adding registration and voting transactions to the blockchain network, albeit at a higher transaction cost. It can be observed from Table 6 that execution times differ greatly between slow and average, as opposed to differences in transaction fees. Thus, it can be inferred that slow and average transaction execution times should be avoided to increase the speed of the election process. Since the cost difference between the slow, average, and fast execution time is not much, the fast transaction execution time should be preferred during an election process. This also makes the system faster and more secure [39].

# 7 Security Analysis

This section provides the security analysis of the proposed system and highlights solutions to the threat model analysis mentioned in Section 3.

## 7.1 Vote Consistency and Integrity

The proposed model provides vote consistency since all nodes in the network maintain the same copy of the voting results using the blockchain time stamp. Furthermore, at any time of any update, the newly generated data blocks are subsequently updated. In the case of new voting requests, old votes in the blocks have to be committed in the chain before any new blocks can be inserted. Our model groups votes into blocks, and

anytime a vote is being cast; the voting authority adds the votes with other unverified votes to be accepted by other nodes after proper verification. The block also contains the hash of the previous block. We assume that the hash function is collision-resistant.

### 7.2 Cast-as-Intended Transparency and Verifiability

Our proposed scheme provides cast-as-intended voting by first providing integrity through a consensus protocol as defined in the previous section. Also, it uses double authentication to make sure that each voter is directly cast. Each voter is assigned a private key that is used as the nonce for hashing blocks into the blockchain. In the case of a corrupted system or a malware malfunction in the operating system, the vote cast into the blockchain will eventually be dropped since the consistency of the blocks is not maintained. The final polling outcome of all tallied votes is a summation of all the individual blockchains of each poll site within the districts, combined with the zone-level blockchain and state-level blockchain.

### 7.3 Vote Coercion Resistance

Our definition of resistance in this context is defined as our proposed system being able to resist modification by an adversary or a malicious entity after votes are being cast. Let's assume an adversary *A* tries to change a voter's option or an attempt to tamper with the votes stored in the blockchain. In the first case, this is not possible in our proposed scheme since each vote is secured through a collision resistance hash function such as SHA-256, afterward sign the vote using the private key. Additionally, each vote cast is sent and distributed on the entire decentralized network for approval and verification, meaning that a change in one node will invalidate the vote since the initially generated signature will be different on the other nodes using the voter's public key.

Our proposed scheme is secure against blockchain modification in the second case because each block has a hash pointer to the next block, creating a Merkle tree. For instance, if *A* makes an attempt to modify the vote on some blocks, the adversary will encounter a mismatch problem because the modified block will have an inconsistent hash value compared to the hash of the preceding blocks contained in the blockchain. In the worst-case scenario, if the adversary successfully breaks the hash of the previous block, the adversary will eventually fail when the head of the list is reached. Besides, every node in the network has a copy of the blockchain, making it very hard for an adversary to modify all the blocks in the entire network.

### *7.4 Double Voting*

Our proposed system can thwart the instances of double voting through the blockchain's consensus protocol since each vote's authenticity is verified through time stamps and logs for each vote on the blockchain. Also, all nodes in the network can publicly verify votes in every block before committing it to the blockchain, ensuring that each voter votes for an option. Furthermore, each vote is signed by each voter using their private key, ensuring that the verifier can easily detect any falsification.

## 8 Conclusion

This paper has presented an effective approach to solving the authentication, integrity, and verifiability issues of electronic voting using MFA and a private blockchain solution. The suggested procedure uses MFA and smart contracts to enable secure and cost-efficient election processes while guaranteeing voter privacy. The proposed blockchain approach provides high speed and scalability for casting votes as intended without incurring high transaction cost during slow, average, and fast transaction execution speed times. The proposed approach incurred a cost difference of 0.0085 Ether, 0.0068 Ether and 0.0017 Ether between fast, average, and slow transaction times. The strength of the system is in its synergistic application of MFA of facial recognition and RFID authentication with blockchain-based distributed ledger data storage. The proposed mechanism has shown that decentralized distributed electronic voting through blockchain technology offers a better possibility for countries to conduct a credible election without compromising critical attributes of integrity, confidentiality, and verifiability of voter’s choice while being able to view the result of the election in real-time. Adopting the proposed technique in future electronic democratic decision-making will help make vote casting easy, secure, and fast, which may encourage more citizens' participation in the electioneering process.

In the future, the authors would like to pay detailed attention to the communication complexity of the network of distributed computers [25] and to improve the overall system’s performance, which is critical for a large-scale e-voting scenario.

## Acknowledgment

We want to thank the Federal University of Technology Minna, Nigeria, and Modul University Vienna, Vienna, Austria, for making the resources available to complete this work.

## References


1. N. Mpekoa and D. van Greunen, "m-Voting: Understanding the complexities of its implementation," *International Journal for Digital Society,* vol. 7, *(4),* 2016. DOI: 10.20533/ijds.2040.2570.2016.0149.
2. N. Ashok, B. Teja, and A. Balakrishna, "RFID and Fingerprint Recognition based Electronic Voting System for Real-Time Application," *International Journal of Engineering Development and Research,* vol. 2, *(4),* pp. 3850-3854, 2014.
3. EM Dogo, NI. Nwulu, O.M. Olaniyi, C.O. Aigbavboa, and T. Nkonyana. "Blockchain 3.0: Towards a Secure Ballotcoin Democracy through a Digitized Public Ledger in Developing Countries," *I-Manager's Journal on Digital Signal Processing,* vol. 6, *(2),* pp. 24, 2018. DOI: 10.26634/jdp.6.2.15593.
4. T. P. Abayomi-Zannu, I. A. Odun-Ayo and T. F. Barka, "A Proposed Mobile Voting Framework Utilizing Blockchain Technology and Multi-Factor Authentication," *Journal of Physics. Conference Series,* vol. 1378, pp. 32104, 2019. DOI: 10.1088/1742 6596/1378/3/032104.
5. V. C. Iwuoha, "ICT and Elections in Nigeria: Rural Dynamics of Biometric Voting Technology Adoption," *Africa Spectrum,* vol. 53, *(3),* pp. 89-113, 2018. DOI: 10.1177/000203971805300304.
6. F. Fusco, M.I. Lunesu, F.E. Pani, A. Pinna, "Crypto-voting, A Blockchain Based e-Voting System", *10th International Conference on Knowledge Management and Information Sharing (KMIS)*, Seville, Spain, pp. 221-225. 2018
7. KD. Anil, D., Rakshith, C.V. Manoj, and NU. Poornachandra, "RFID Based Voting Machine," *International Journal of Current Engineering and Scientific Research,* vol. 4, *(6),* pp. 23-25, 2017.
8. O. O. Okediran, A. A. Sijuade and W. B. Wahab, "Secure Electronic Voting Using a Hybrid Cryptosystem and Steganography," *Journal of Advances in Mathematics and Computer Science,* pp. 1-26, 2019. . DOI: 10.9734/jamcs/2019/v34i1-230201.
9. B. Umar, OM Olaniyi, L. Ajao, D. Maliki, and I. Okeke, "Development of a Fingerprint Biometric Authentication System for Secure Electronic Voting Machines," *Kinetik (Malang),* vol. 4, *(2),* pp. 115-126, 2019. DOI: 10.22219/kinetik.v4i2.734.
10. B. A. Oke, O.M. Olaniyi, A.A. Aboaba, and O.T. Arulogun," Developing Multi-factor Authentication Technique for Secure Electronic Voting Systems", *Proceedings of IEEE International Conference on Computing, Networking and Informatics (ICCNI 2017),* pp. 48-53 DOI: 10.1109/ICCNI.2017.8123773.2017.
11. A. J. Gabriel, B.K. Alese, and, A.O. Adetunmbi, O.S. Adewale, and O.A. Sarumi, "Post-Quantum Crystography System for Secure Electronic Voting," *Open Computer Science,* vol. 9, *(1),* pp. 292-298, 2019. DOI: 10.1515/comp-2019-0018.
12. O. M. Olaniyi, O.T Arulogun, E.O. Omidiora, and O. Adeoye. "Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions," *International Journal of Computer and Information Technology (IJCIT),* vol. 2, *(6),* pp. 122-1130, 2013.
13. M. Li *et al*, "CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing," *in IEEE Transactions on Parallel and Distributed Systems, vol. 30, no.6, pp. 1251-1266*, 2019. DOI: 10.1109/tpds.2018.2881735.

14. Y. Jiao, P. Wang, D. Niyato and K. Suankaewmanee, "Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks," *in IEEE Transactions on Parallel and Distributed Systems, vol. 30, no. 9, pp. 1975-1989*, 2019. DOI: 10.1109/tpds.2019.2900238.
15. T. Habibu, K. Sharif and S. Nicholas, "Design and Implementation of Electronic Voting System," *International Journal of Computer & Organization Trends,* vol. 7, *(4),* pp. 1-6, 2017. DOI: 10.14445/22492593/IJCOT-V45P301.
16. A. Singh, and K. Chatterjee, "SecEVS : Secure Electronic Voting System Using Blockchain Technology". *International Conference on Computing, Power and Communication Technologies (GUCON),* pp. 863-867. 2018.
17. A.N. Oluwatobi, T.P. Ayeni, O.T. Arulogun, A.A., Ariyo, and K.A. Aderonke. "Exploring the Use of Biometric Smart Cards for Voters' Accreditation: A Case Study of Nigeria Electoral Process," *International Journal on Advanced Science, Engineering and Information Technology,* vol. 10, *(1),* pp. 80, 2020. DOI: 10.18517/ijaseit.10.1.8459.
18. O. M. Olaniyi, O.T. Arulogun, E.O. Omidiora, and O.O. Okediran. "Enhanced Stegano-Cryptographic Model for Secure Electronic Voting," *Journal of Information Engineering and Applications (JIEA),* vol. 5, *(4),* pp. 1-15, 2015.
19. O. M. Olaniyi, T. A. Folorunso, A. Ahmed, O. Joseph, "Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach," *International Journal of Information Engineering and Electronic Business,* vol. 8, *(5),* pp. 9, 2016.
20. A. Zaid, AA Firas and A. Hussein. "Design and implementation of RFID system, *Proceedings of 5th International Multi-Conference on Systems, Signals and Devices*, DOI: 10.1109/SSD.2008.4632787. 2008
21. M. Kassim, H. Mazlan, N. Zaini, M.K. Salleh. "Web-based Student Attendance System using RFID Technology", *Proceedings of 2012 IEEE Control and System Graduate Research Colloquium* (ICSGRC 2012), 213-218, 2012
22. Allelectronics. *RFID Read and Write Module*. Available: https://www.nxp.com/docs/en/datasheet/MFRC522. 22nd August 2020
23. ITNEXT. *face-api.js — JavaScript API for Face Recognition in the Browser with tensorflow.js*. Available: https://itnext.io/face-api-js-javascript-api-for-face-recognition-in-the-browser-with-tensorflow-js-bcc2a6c4cf07. 31st August 2020
24. Y. Faridah, Haidawati Nasir, A.K. Kushsairy, Sairul I. Safie, Sheroz Khan and Teddy S. Gunawan, "Fingerprint biometric systems". *Trends in Bioinformatics*., vol. 9, pp. 52-58, 2016. DOI: 10.3923/tb.2016.52.58.
25. L. Xu and J. Bruck, "Deterministic voting in distributed systems using error-correcting codes," *in IEEE Transactions on Parallel and Distributed Systems, vol. 9, no. 8, pp. 813-824*, 1998. DOI: 10.1109/71.706052.
26. F. S. Hardwick, A. Gioulis, R. N. Akram, K. Markantonakis. "E-voting with blockchain: An e-voting protocol with decentralization and voter privacy." In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* pp. 1561-1567. IEEE, 2018.
27. N. Kshetri, J. Voas Blockchain-enabled e-voting. IEEE Software. 2018 Jul 6;35(4):95-9.

28. S, Bartolucci, P. Bernat, D. Joseph. "SHARVOT: Secret SHARe-based VOTing on the blockchain." *In Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain-WETSEB'18,* Gothenburg, Sweden, 27 May–3 June 2018; pp. 30–34.
29. L.V.-C. Thuy, K. Cao-Minh, C. Dang-Le-Bao, T.A. Nguyen. "Votereum: An Ethereum-Based E-Voting System." *In Proceedings of the 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF),* Danang, Vietnam, 20–22 March 2019; pp. 1–6.
30. E. Yavuz, A.K. Koc, U.C. Cabuk, G. Dalkilic. "Towards secure e-voting using Ethereum blockchain." *In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS),* Antalya, Turkey, 22–25 March 2018; pp. 1–7.
31. W. Zhang, Y. Yuan, Y. Hu, S. Huang, S. Cao, A. Chopra, S. Huang. "A Privacy-Preserving Voting Protocol on Blockchain". *In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD),* San Francisco, CA, USA, 2–7 July 2018; pp. 401–408.
32. V. Sathya, A. Sarkar, A. Paul, S. Mishra. "Blockchain Based Cloud Computing Model on EVM Transactions for Secure Voting." *In Proceedings of the 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC),* Erode, India, 27–29 March 2019; pp. 1075–1079.
33. A. Qureshi, D. Megías, and H. Rifà-Pous, 2019. SeVEP: Secure and Verifiable Electronic Polling System. *IEEE Access*, *7*, pp.19266-19290.
34. R. Taş, O. O. Tanrıöver. "A systematic review of challenges and opportunities of blockchain for E-voting." *Symmetry*. 2020 Aug;12(8):1328.
35. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system." https://bitcoin.org/bitcoin.pdf.
36. G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, 2014.
37. Y. Zhang, C. Xu, X. Lin, XS, Shen. "Blockchain-based public integrity verification for cloud storage against procrastinating auditors." In *IEEE Transactions on Cloud Computing*. 2019.
38. T. P. Abayomi-Zannu, I. Odun-Ayo, B. F. Tatama, and S. Misra. "Implementing a Mobile Voting System Utilizing Blockchain Technology and Two-Factor Authentication in Nigeria". In *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)*, pp. 857-872. Springer, Singapore, 2020.
39. J. B. Awotunde, R. O. Ogundokun, R. G. Jimoh, S. Misra, T. O. Aro (2021) Machine Learning Algorithm for Cryptocurrencies Price Prediction. In: Misra S., Kumar Tyagi A. (eds) *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities. Studies in Computational Intelligence*, Vol 972. Springer, Cham. https://doi.org/10.1007/978-3-030-72236-4_17, 2020.