Application of Crypto-Blockchain Technology for Securing Electronic Voting Systems

Lukman Adewale Ajao, Buhari Ugbede Umar, Daniel Oluwaseun Olajide, and Sanjay Misra

1 Introduction

The irregularities and malpractices in democratic positions (election) are becoming normal practices among African countries. This is due to low technology of voting system materials, poor governance, and oligarchy tendencies. For instance, Nigeria is a case study where election malpractices are domicile during the democratic process of voting, resulting in wrong selection of leadership, chaotic, unfortunate free, fair, and credible election processes and many other challenges. Voting is a democratic process by which a democratic society or citizens approved to determine their choice of leadership selection [1]. E-Voting is an acronym for electronic voting system that encompasses the integration of electronics and information technology to support the counting of electorate votes [2]. This e-voting system has been improved with recent technology in the design architecture but is still found susceptible to voters' privacy, tampering, manipulation, and frauds by the individual electoral parties' agent or authority [3]. Some of the misconduct includes ballot snatching, multiple voting, failure of smart card readers' (SCR) performance, and biometric authentication mischief. However, electronic voting systems' poor performance results from system error performance, network security challenges, and data insecurity [4].

Biometric authentication is an identification technique and control of access based on physiological or behavioral characteristics [5]. Biometrics authentication

L. A. Ajao (✉) · B. U. Umar · D. O. Olajide
Department of Computer Engineering, Federal University of Technology, Minna, Nigeria
e-mail: ajao.wale@futminna.edu.ng

S. Misra
Department of Computer Science and Communication, Østfold University College (HIOF), Halden, Norway

S. Misra, A. Kumar Tyagi (eds.), *Blockchain Applications in the Smart Era*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-89546-4_5

relies on individual authenticity, unlike password authentication, which depends on the generation of a key to which brute force attacks or man-in-the-middle attacks can compromise. Biometric authentication methods involve comparing a biometric sample (biometric template or identifier) registered or enrolled with a newly captured biometric sample.

A unimodal fingerprint biometrics electronic voting system using Advanced Encryption Standard (AES)-based wavelet and cryptographic watermarking was developed to improve the disorder in the election system. The unimodal biometrics authentication is implemented to solve the problem of voting irregularities in a situation where the voter's fingerprint cannot be authenticated by the system [6, 7]. This system ensured the integrity and credibility of votes. A system that allowed people to vote on a website using voter ID and PIN code has been developed, which builds confidence in e-voting by improving the verification process and auditing of election results voting [8]. But the central system could be exposed to denial-of-service (DoS) attacks due to the inadequacy of security countermeasure.

An e-voting system using RSA and MD5 algorithms for encryption and securing votes was developed to maintain a high level of security with the use of two encryption algorithms. Still, it is computational complexity that slows the performance of the system [9]. However, the encryption schemes required some procedure for the decryption algorithm to achieve original votes before tallying ballots, which slow the system's performance and make security authentication inefficient. Cetinkaya and Doganaksoy implemented an e-voting system using dynamic balloting and Pseudo-Voter Identity (PVID) scheme to provide adequate security. The system considered recasting of votes as a solution for coercibility problems in uncontrolled environments [10]. But it cannot prevent the manipulation of electoral results by the central authority.

The development of a smart system using cryptography and hashing methods has been a way forward to reduce the security threats in electronics or embedded system applications. But this security authentication on the electronic system is still inefficient in some application areas to prevent unauthorized third party from accessing or tampering with legitimate records, as in the financial transaction, electronic businesses, online marketing, e-health records, e-voting system, and many other areas of smart technology. Therefore, blockchain (with immutability, transparency, and decentralization advantages) has been popularly proposed as a recent security countermeasure to reduce third-party mischievous, fraudulent, stealing of legitimate information, and data privacy breaches. Therefore, this study proposed developing a bi-factor crypto-blockchain technology for securing electronic voting systems as our contribution to the existing works. The bi-factor authentication of a biometric system using fingerprint and iris identity is proposed to reduce the false acceptance rate (FAR) of the counterfeit candidates and the false rejection rate (FRR) of authentic candidates during the election voting processes. Also, private blockchain technology is proposed as a decentralized system with immutability and transparency records management system using the Paillier homomorphic encryption algorithm (PHEA) to improve the efficient performance of the chain network.

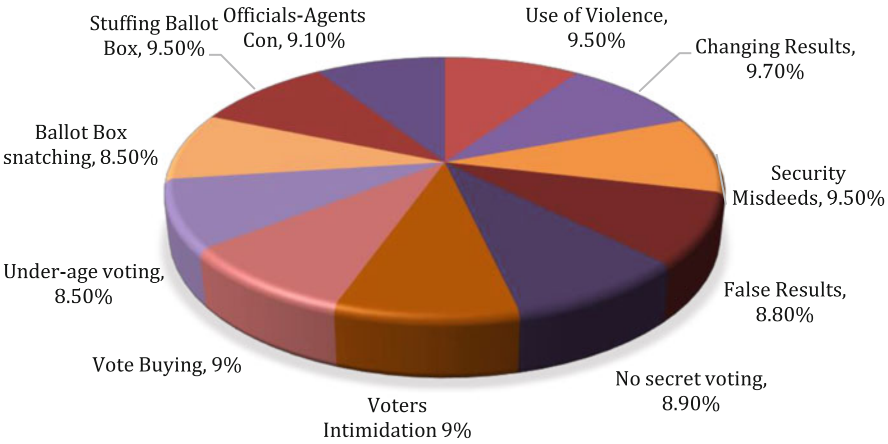


Fig. 1 Analysis of Nigeria polls' misconduct during the general election

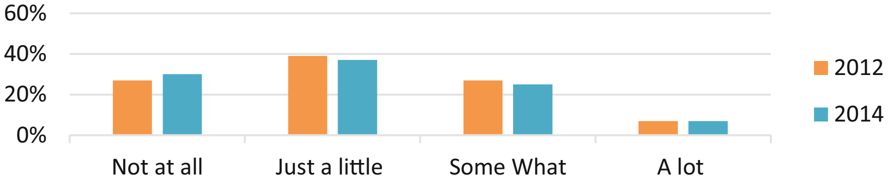


Fig. 2 Independent electoral commission evaluation

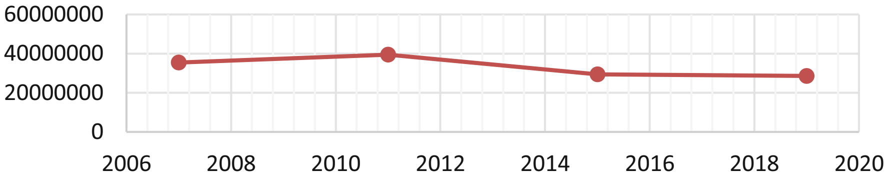


Fig. 3 Nigerian voter participation in general elections

The statistical analysis of a misconduct during a general election is presented (see Fig. 1), while the irregularities from independent electoral commission (INEC) during the 2011 and 2015 general election were analyzed (see Fig. 2). Therefore, due to the brutal experience of electorates during election processes, gross misconduct of electoral body, inefficient electronic voting system, and voters' privacy breaches have drastically reduced the citizen's participation in the democratic process. See Fig. 3 for the detailed analysis of the voters' participation in the election between 2007 and 2019.

This research is organized as follows: Section 1 introduces the general research background of the study, electronic voting system, and biometric classifications. Section 2 introduces blockchain technology and its consensus algorithm in Sect. 2.1, blockchain classification in Sect. 2.2, and the area of related blockchain applications in Sect. 2.3. The proposed system methodology with flowchart and algorithm is presented in Sect. 3. Section 4 discussed results and system performance evaluation, while Sect. 5 concludes the research investigation.

2 Blockchain Technology

Blockchain is a distributed public ledger that contains a set of blocks that are interconnected to embrace a digital signature of the preceding block with the next hash block to make it irrefutable, immune to tampering, and transparent [11]. Blockchain technology does not agree with third-party interactions in the chain participant and does not support a singular authority system [12]. A connected blockchain in the networks is known as a ledger which is shared between the chain participants in a public distributed ledger [13]. This complex cryptographic algorithm of blockchain makes it difficult for hackers or any third party to tamper, delete, and modify records [14]. So, the blockchain network participant jointly verifies the transactions and archives transaction information to ensure the integrity and reliability of records transactions. The blockchain transaction process begins with the creation of a block to store the transaction; each of the blocks is unified with a timestamp and linked to the previous blocks. The node of the blockchain participant examines the transaction before added to the hashing chain in the consensus algorithm network. Finally, some created blocks and connected chains are encrypted, and each encoding block takes a reference from the previous hashing blocks.

2.1 The Consensus of Blockchain Algorithm and its Classification

A consensus blockchain algorithm is a mechanism that issues certificate agreement to the blockchain network for mutual interrelation and verifies an agreement for the record validation. A blockchain network is a decentralized and distributed ledger in nature that exists among several nodes in the chain participant to avoid autonomous centrality, control, and validity of a transaction [15]. The consensus algorithm is the backbone of blockchain technology that can be described and classified as follows (see Fig. 4).

Proof of Work (PoW) This cryptographic technique ensures the authenticity of transactions (proof) between the parties (prover and verifier) in the chain networks using Diffie-Hellman-based puzzle, which can be subsequently verified or confirmed with little effort. For instance, PoW is popularly adopted as a prover and verifier for the consensus of Bitcoin transactions through cryptocurrencies.

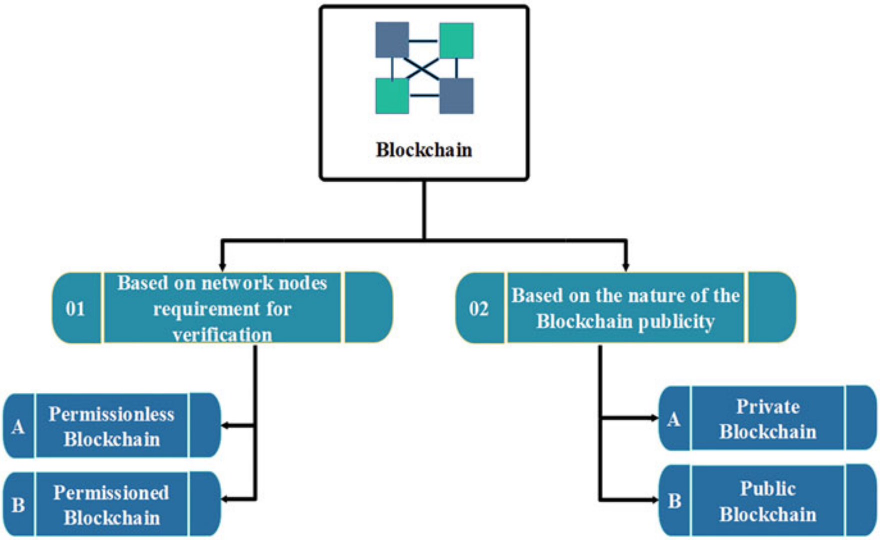

Blockchain
01
Based on network nodes requirement for verification
02
Based on the nature of the Blockchain publicity
A
Permissionless Blockchain
B
Permissioned Blockchain
A
Private Blockchain
B
Public Blockchain

Fig. 4 Classification of blockchain

The disadvantage of this POW (consensus algorithm) is high computing power requirements [16].

Proof of Stake (PoS) This protocol was adopted for securing cryptocurrency and Ethereum operation through the selection of validators, appended on the transaction which is proportional to the number of linked cryptocurrencies in the consensus mechanism. This prevents a malicious actor and groups of users in the transactions chain networks. The PoS is efficient for fast transaction of the blockchain verification with low energy consumption and minimum hardware requirements [17].

Proof of Authority (PoA) This type of consensus algorithm is automated with the use of software program to secure the transactions in the blockchain network and validated by permitted authority or accounts called validators [18].

The Blockchain-Based Network Nodes for Certificate Verification

Permissionless Blockchain Network This type of blockchain credential verification is called public blockchain, and it does not require any permission (participants' consensus) to become or join the chain network for participation and interaction [19]. This model is suitable for operating digital currencies with effective management. The permissionless approach allows individual users to create and address the issues in network for the interaction by either validating the transaction or direct the transactions to another participant on the networks. The use-cases environment are

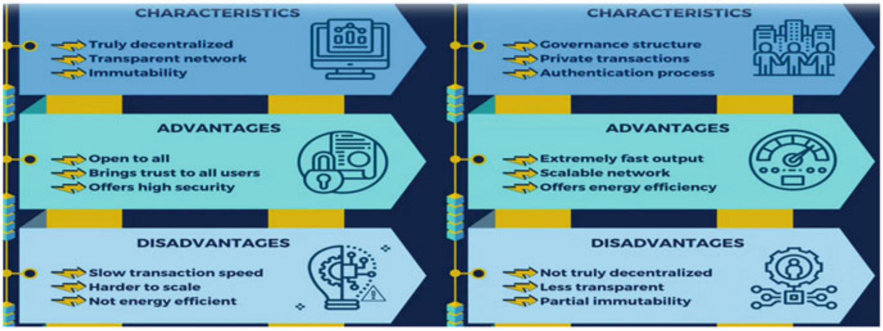


Fig. 5 Permissionless (left) and permissioned (right) blockchain characteristics

balloting systems, digital identity, and fundraising. The example includes Bitcoin and Ethereum.

Permissioned Blockchain This type of blockchain credential verification does not allow third-party participants to join the chain network for transactions without the mutual agreement of the authentic network administrator [20]. The permissioned blockchain adopts a partial decentralization technique for recording and information storage authentication. It is commonly used in the banking sectors, research, internal voting, supply chain management, and many institutions for data security and policy regulations. Ripple (XPR) is a popular example. The characteristics, advantages, and disadvantages of both permissionless and permissioned blockchain are shown in Fig. 5.

Based on the Nature of the Blockchain Publicity

Private Blockchain This type of blockchain profile-raising is a sole autonomy network and partial decentralization that allows a single organization to have permission and authority over the control of the network chain. It allows read and write for single organization access, fast transaction speed, permissioned consensus, and high efficiency and supports partial immutability [21].

Public Blockchain This type of blockchain network allows an individual participant to join the chain network without restrictions to access the ledger (decentralized records) for consensus processes. But the transaction speed is slow and supports full immutability with low efficiency [22].

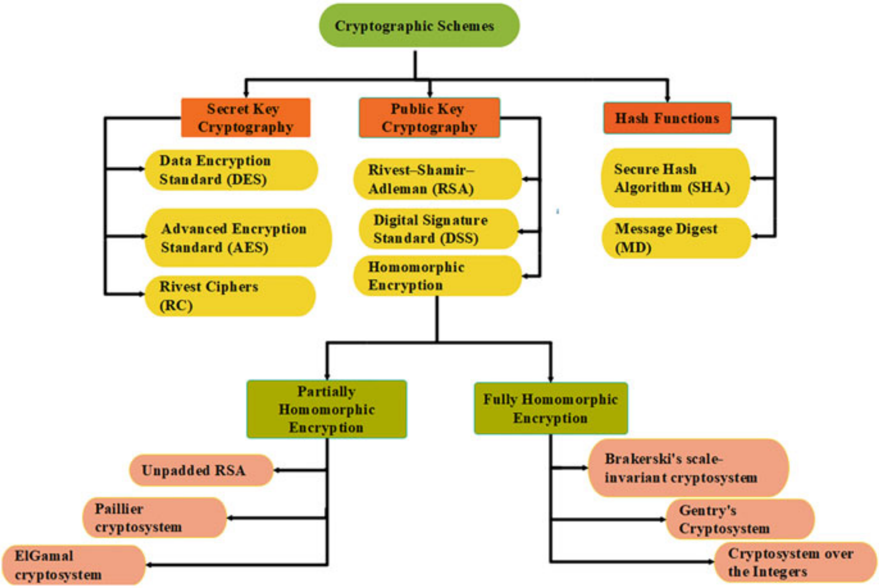

Cryptographic Schemes
Secret Key Cryptography
Public Key Cryptography
Hash Functions
Data Encryption Standard (DES)
Advanced Encryption Standard (AES)
Rivest Ciphers (RC)
Rivest–Shamir–Adleman (RSA)
Digital Signature Standard (DSS)
Homomorphic Encryption
Secure Hash Algorithm (SHA)
Message Digest (MD)
Partially Homomorphic Encryption
Fully Homomorphic Encryption
Unpadded RSA
Paillier cryptosystem
ElGamal cryptosystem
Brakerski's scale-invariant cryptosystem
Gentry's Cryptosystem
Cryptosystem over the Integers

Fig. 6 Types of cryptography schemes

2.2 The Cryptography Techniques for Securing Blockchain-Based Electronic Voting System

This technology (blockchain) is a decentralized digital ledger that helps in securing the transaction processes in the blockchain network using steganography or hashing techniques to achieve optimal security (see Fig. 6). These techniques are widely used to improve the applicability of blockchain as a security countermeasure in most systems. It provides transparent, immutable, and fraud-resistant platform and subsists the confidentiality, integrity, and user's data privacy breach [23].

The Symmetric or Secret-Key Cryptography (SKC) This type of cryptography key refers to the balanced encryption schemes that adopt a single key for the implementation of both encoding and decipherment of messages. This symmetric key approach is mainly utilized to ensure data privacies (confidentiality), integrity, and authenticity [24]. The subcategories include data encryption standards, advanced encryption standards, and the Rivest ciphers.

The Asymmetric or Public-Key Cryptography (PKC) This encryption type of cryptography scheme utilizes pairs of different and encoded keys in nature with secrecy. It includes an irregular process of encrypting data (plaintext) using a public key and a private key for lopsided ciphertext called decipher. This cryptographic method is mainly focused to achieve data authentication and non-repudiation of messages. Some of these asymmetric cryptography types include digital signature standard and Rivest-Shamir-Adleman homomorphic encryption schemes.

Hash Functions This cryptography technique uses a mathematical transformation on the ciphertext to make it irrevocable and to provide trust, privacy, confidentiality, integrity, and authenticity.

Homomorphic Encryption Algorithm (HEA) This is an encryption method that allows users to carry out computations over the encrypted message without decryption reasoning. This computation process over the encrypted message generates an identical form of result when decrypted to provide privacy and protective storage outsourced. The homomorphic encryption algorithm is suitable for securing automated systems like electronic voting systems using blockchain technology for safety services improvement and removing barriers that prevent data distribution of consolidating ballots. The homomorphic encryption algorithms can be classified into partial or full types. The partial homomorphic steganography includes unpadded RSA, Paillier, ElGamal, Goldwasser, Benaloh, Boneh-Goh-Nissim, Ishai-Parkin, and Sander-Young-Yung cryptosystem. While the fully homomorphic includes Gentry's cryptosystem, cryptosystem over the integers, and Brakerski's scale-invariant cryptosystem.

Fully Homomorphic Encryption/Cryptosystem This is a class of homomorphic encryption that supports both additive and multiplicative homomorphism operations. They are versatile but require more computational power than the partially homomorphic class.

Partially Homomorphic Encryption/Cryptosystem This is a class of homomorphic encryption that is capable of executing the additive or multiplicative homomorphism processes. They achieved high level of performance but only support one type of computation, either multiplication or addition operations [25]. Examples of partially homomorphic cryptosystems are:

(i) Unpadded RSA cryptosystem: this steganography method supports multiplicative operations and is expressed as given in Eq. 1, 2, and 3.

$$\Theta\,(s_1)\cdot\Theta\,(s_2) = s_1^e s_2^e \bmod n \tag{1}$$

$$= (s_1 s_2)^e \bmod n \tag{2}$$

$$= \Theta\,(s_1 \cdot s_2) \tag{3}$$

where.

$\Theta(s) = s^e\ mod\ n$ is the encryption of a message s and e is the encryption exponent.

(ii) The ElGamal homomorphic cryptosystem has a cyclic group P of order q, with generator p as expressed in Eq. 4, 5, and 6.

$$\Theta\ (s_1) \cdot \Theta\ (s_2) = \left(p^{r_1}, s_1 \cdot n^{r_1}\right)\ \left(p^{r_2}, s_2 \cdot n^{r_2}\right) \tag{4}$$

$$= \left(p^{r_1+r_2}, (\ s_1 \cdot s_2)\ \ p^{r_1+r_2}\right) \tag{5}$$

$$= \Theta\ (s_1 \cdot s_2) \tag{6}$$

where.

(P, q, p, n) is the public key, $n = p^s$ is the secret key, and $\Theta(s) = (p^r, s \cdot n^r)$ is the encryption of the message *s.*

(iii) The Goldwasser-Micali cryptosystem is expressed as in Eq. 7, 8, and 9.

$$\Theta\ (d_1) \cdot \Theta\ (d_2) = s^{d_1} r_1^2 s^{d_2} r_2^2 \bmod n \tag{7}$$

$$= s^{d_1+d_2} (r_1 r_2)^2 \bmod \tag{8}$$

$$= \Theta\ (d_1 \oplus d_2) \tag{9}$$

where.

$\oplus$ is the addition modulo 2 (exclusive-or), $\Theta(d) = s^d\ r^2\ mod\ n$ is the encryption of a bit *d,* and *s* is the quadratic non-residue.

(iv) Benaloh cryptosystem and Okamoto-Uchiyama cryptosystem are expressed as in Eq. 10, 11, and 12.

$$\Theta\ (s_1) \cdot \Theta\ (s_2) = \left(p^{s_1} r_1^c\right) \left(p^{s_2} r_2^c\right)\ \bmod n \tag{10}$$

$$= p^{m_1+m_2} (r_1 r_2)^c \bmod n \tag{11}$$

$$= \Theta\ (s_1 + s_2)\ . \tag{12}$$

where.

$\Theta(s) = g^m r^c\ mod\ n$ is the public key.

2.3 Application of Blockchain Technology Survey

The blockchain has popularly gained interest in several application areas to enhance the security challenges that have become a threat to the normal operation of the smart system, online transaction, and e-business. Adopting this technology (blockchain) with the integration of cryptographic and hashing techniques has relaxed the security pressure against hackers, social network threats, malicious actors, and many others. Especially in the financial institution which gave respect to the functionality and advantage provided by this blockchain application in terms of adequate security measures against the third-party assailant in the network. Also, it is widely used in online or electronic business transactions to prevent a third-party participant or intruder from tampering, altering, or illegally modifying the records without the chain participant consolidations. Blockchain with hashing techniques has been widely adopted to secure smart devices, sensor networks, software-defined networks (SDN), and Internet of Things (IoT) infrastructures.

Several researchers have contributed with different methods and approaches to resolve the problems affecting the voting system using secure authentication Schemes [26]. However, this research area is still open for further investigation and development of an efficient security countermeasure for a smart technology like an e-voting system that may concern the security of voter privacy and protection of ballot tallying and auditing. The new trend in the blockchain application and steganography schemes for securing e-voting systems and other emergent technology of smart systems are investigated.

A hyperledger blockchain is implemented on an e-voting system to ensured immutability and record tampering as a token-free system [27]. But the system could not resist some security issues such as confidentiality and ensure voter privacy. The Ethereum private blockchain was developed and implemented on an electronic voting system to achieve a higher degree of transaction processing and to guarantee the electorate's privacy [28]. The open source-based blockchain technique was implemented on the automated voting system using cryptographic techniques based on ElGamal to ensure the privacy of the electorate. The system guarantees the immutability of the ballots and could not be interfered with by the third party in the chain network [29]. But the encoding method required the decryption of a secret ballot before it could be tallied which makes the system to be time appealing and does not guarantee privacy.

Gupta et al. developed a telesurgery scheme with multilevel user authentication to ensure a privacy-oriented and interoperable telesurgery system using a blockchain [30]. It further experiments an Ethereum blockchain system with a fifth generation-enabled tactile Internet (5GTI) to evaluate the system efficiency and privacy orientation and secure real-time delivery of health-care services through unmanned aerial vehicles (UAV). Rahman et al. developed a decentralized blockchain-based framework with mobile edge computing (MEC) to allow for the support of a large user pool with low latency. The system achieved a good level of security and user anonymity over a centralized database for the storage of actual health-care multimedia data [6]. The concept of a scalable, secured, and user-centric collection of health-care data from personal wearable devices is developed using a blockchain technology [31]. This system ensured adequate protection of personal health records but failed to consider the variety of datasets that could exist from a wide variety of wearable devices. Vora et al. proposed a blockchain framework with varying contract classification to allow for a balanced privacy-oriented and readily accessible storage of electronic health records. The proposed scheme ensured ease of use and the complete encryption of the records. It however did not put in place the consideration for the time and computational resources that would be required to decrypt the records whenever they were needed [32].

Bodkhe et al. presented a token-based blockchain with proof of collaboration and zero-knowledge proofs (ZKP) with deep learning to allow for the management and protection of tourists' data from identity theft and payment clearance cycle attacks [33]. The system however failed to put in place modalities for the security of stakeholders. A blockchain system with energy trading validation and stability was developed for the management of a smart grid system using lightweight security [34]. Wei et al. projected a scheme for a blockchain-based framework with a proxy model and Merkle hash tree for monitoring data changes and to ensure the integrity of storage data [35]. A self-sovereign identity management system based on Ethereum smart contracts was proposed for securing and managing digital assets, reputation, and personal identity. But the system did not offer privacy protection for the user recovery delegates, which could be exploited for security attacks [36].

Blockchain technology using RSA and SHA-256 cryptography algorithms was proposed to secure the process of digital banking. During testing, the system achieved high accuracy of 88% with good reliability but failed to guarantee the integrity of data in transit [37]. The bio-cryptographic systems using Gabor filter images (GFI) and lifting wavelet transforms (LWT) were proposed to safeguard an automated voting system. The results of 0.0001% and 0.1% are obtained for FAR and FRR, respectively. The system ensures security measures like authentication, confidentiality, and integrity, but computational complexity reduces the response [38, 39].

An ElGamal homomorphic encryption algorithm was developed to ensure user privacy and integrity of electorates records through the automated voting system [40]. The system encrypted votes with the matched format of the decipher to ensure privacy and verifiability of the ballots. But the tallying process of ballots was inactive due to the nature of the homomorphic encoding method used. The Paillier homomorphic cryptography was adopted to secure an electronic voting system. The system evaluation proved efficient with a high level of voter privacy but vulnerable to the manipulation of the ballot through conspiring adversaries [41]. Other security areas of blockchain technology applications are discussed with methods, strengths, and limitations (such as health care, smart home, vehicular area network (VANET), electronic voting system, financial institution, business management, and gas exploration industry. A detailed investigation of the existing works in literature is presented (see Table 1).

3 The Proposed Crypto-Blockchain Scheme and Bi-factor Authentication for Securing E-Voting Systems

An electronic voting system is proposed using a private blockchain with the Paillier homomorphic steganography and bi-factor biometrics certification of iris fingerprint systems. The biometric-based automated voting system is a reliable node with integration of a private blockchain technique for immutable and data privacy breach

Table 1 Summary of the existing research investigation

Method	Strength	Limitation
The fingerprint biometric authentication was used [39]	It solves the problems of authentication	It is not efficient enough as unimodal biometric authentication was used
The automated voting system using BEVS blockchain [42]	It enhanced security and transparency in the voting system	The system is complex to interact with and takes a longer time to operate
Electronic voting system-based blockchain using test-driven approach [43]	It ensured the ballots are safe and difficult for tampering	The confidentiality of voters can be compromised
Blockchain-based e-voting with proof-of-work consensus algorithm [44]	It ensured that ballots were safe from third-party tampering	The privacy of the electorate is not failsafe
The electronic voting system using ElGamal steganography and open source-based blockchain [45]	The ballots storage privacy is guaranteed	The decryption of ballots is essential before votes can be matched which results in excess time
A private key and digital signature-based blockchain is used [46]	It secures the ballots from third-party tampering and is openly verifiable	But it is abortive to address the privacy concerns of ballots and openly verifiable blockchain
The tokens transfer on the Ethereum blockchain network [28]	It safeguarded the openness and immutability of ballots	Not user-friendly with a high start-up cost approach
The automated voting system based on a hyperledger blockchain network [27]	It ensured the immutability of ballots	It does not adopt the cryptosystem technique to render voter privacy advantages

security. The implementation of this blockchain helps to confiscate the autonomous central authority control in the elective system by executing a decentralization system for the transactions among the participants (nodes) on the networks. The use of the Paillier homomorphic steganography is to safeguard the privacy of the voters and eliminate the requirement for decryption of the encrypting data before tallying ballots can be successfully performed. The bi-factor method of using biometrics verification of iris fingerprint (IF) helps to resolve variances that occur during voters verification. Fig. 7 shows the implementation of a crypto-blockchain-based electronic voting system model. The secure smart e-voting system architecture using crypto-blockchain technology is illustrated (see Fig. 8).

The smart e-voting system process begins with the voters that cast their votes at the polling unit. The votes get encrypted using the Paillier homomorphic cryptosystem, after which a block containing the encrypted vote, the voter blockchain id, hash of the previous blocks, and hash of the current block's transaction is created and mined unto the private blockchain ledger. This process repeats itself continuously until the admin (electoral authority) decides to tally the encrypted ballots to obtain

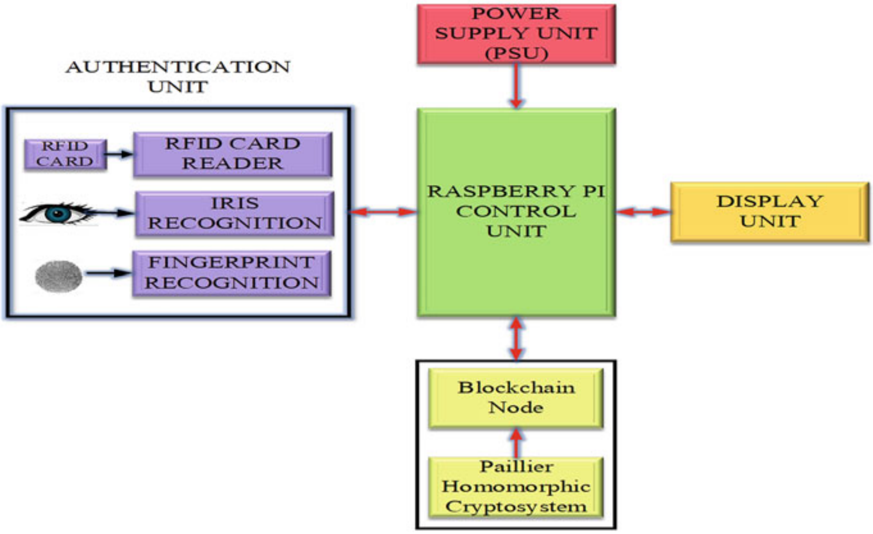


Fig. 7 Block diagram of proposed system architecture

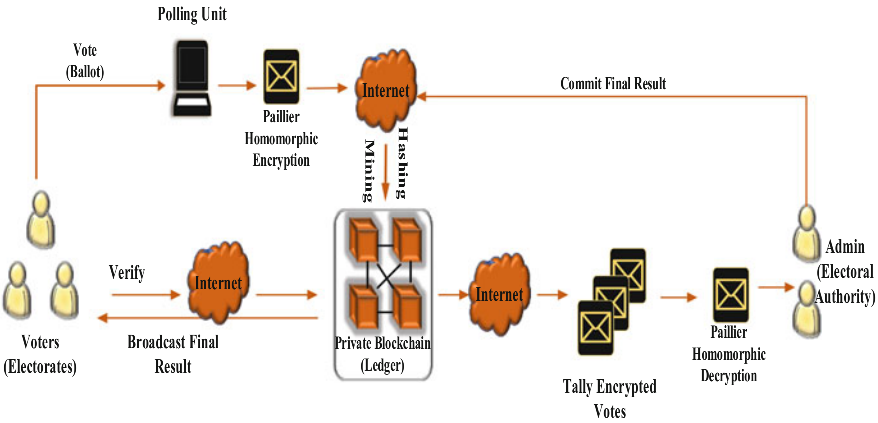


Fig. 8 The secure smart e-voting system architecture using crypto-blockchain technology

a single final encryption sum value that becomes decrypted homomorphically (see Figs. 9, 10, and 11). Therefore, the final result gets announced and broadcasted to the voters over a secure and privacy-oriented network. The Paillier homomorphic encryption algorithm-based blockchain is presented in Table 2.

The Paillier homomorphic encryption cryptosystem property is expressed in Eq. 13, 14, and 15. The Paillier encryption algorithm for the key generation, encryption, and decryption process are contained in Table I.

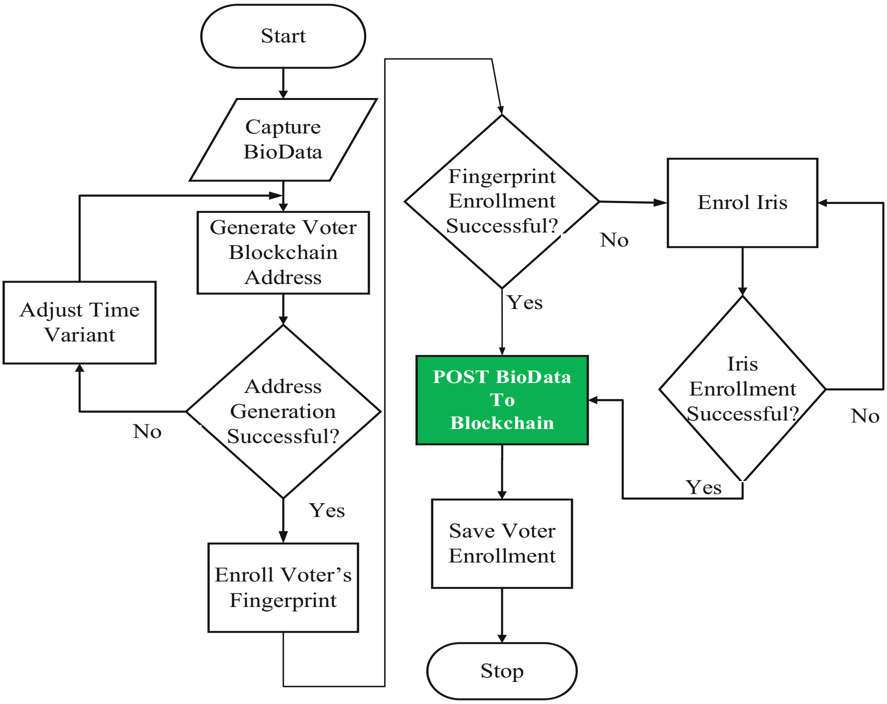

Start
Capture BioData
Generate Voter Blockchain Address
Adjust Time Variant
Address Generation Successful?
No
Yes
Enroll Voter's Fingerprint
Fingerprint Enrollment Successful?
No
Yes
Enrol Iris
Iris Enrollment Successful?
No
Yes
POST BioData To Blockchain
Save Voter Enrollment
Stop

Fig. 9 Voter enrollment process

$$\Theta\left(s_1\right) \cdot \Theta\left(s_2\right) = \left(p^{m_1} r_1^n\right)\left(p^{m_2} r_2^n\right) \bmod n^2 \tag{13}$$

$$= p^{m_1+m_2}\left(r_1 r_2\right)^n \bmod n^2 \tag{14}$$

$$= \Theta\left(s_1 + s_2\right) \tag{15}$$

where.

$\Theta(s) = p^m\ r^n\ mod\ n^2$ is the encryption of a message s.

4 Results and Discussions

The smart electronic voting system was implemented using Raspberry Pi 3B+ as a control system with the integration of a fingerprint sensor (ZFM-60) and camera to accept the voter's registration and enrollment during voting. The data interface touchscreen with a resolution of 800x480px was used as both input and output systems. This smart system was programmed using a python programming

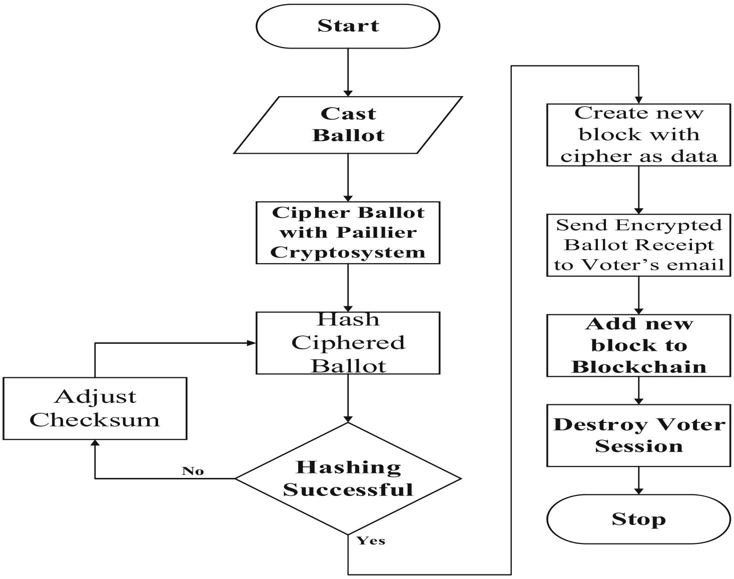

Start
Cast Ballot
Cipher Ballot with Paillier Cryptosystem
Hash Ciphered Ballot
Adjust Checksum
Hashing Successful
No
Yes
Create new block with cipher as data
Send Encrypted Ballot Receipt to Voter's email
Add new block to Blockchain
Destroy Voter Session
Stop

Fig. 10 Blockchain ballot casting process

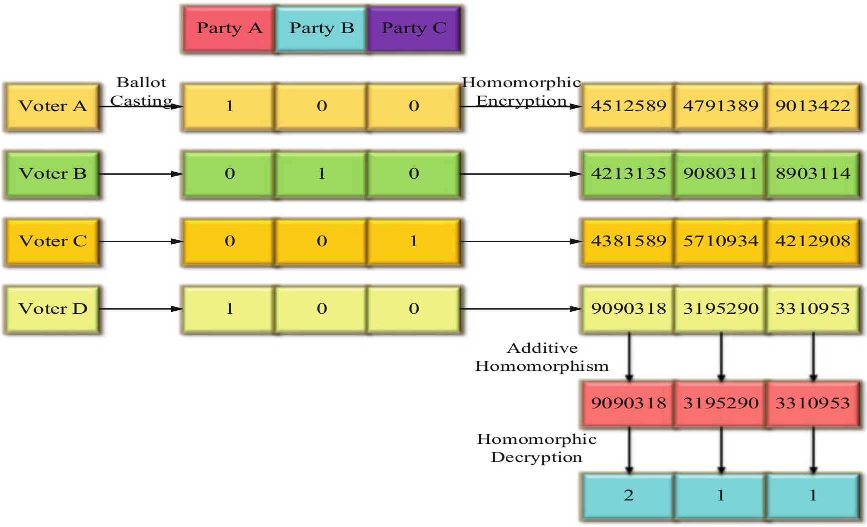
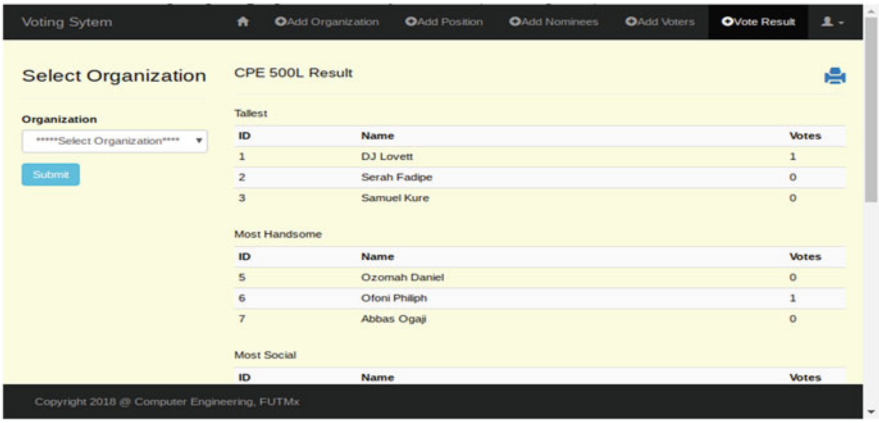


Fig. 11 Homomorphic encryption and decryption of ballots

language as a console that eases the interaction, control, and coordination of the system response and performance. The graphic user interface (GUI) was designed using MySQL, PHP, CSS, HTML, and JavaScript to sectionalize the web view page and manage the flows of data that includes admin log in page, polling unit name,

Table 2 Paillier encryption cryptosystem algorithm

1. Key generation algorithm	
Step 1	Select large, random prime numbers m and p, which is independent of each other. *Gcd(mp, (m − 1)(p - 1)) = 1*
Step 2	Calculate the value of n and λ using, $n = mp$ as well as $\lambda = lcm(m - 1, p - 1)$, where; *lcm is the least common multiple*
Step 3	Choose an integer, k at random, Where $k \in Z^*_{n^2}$
Step 4	Confirm, by using the function *J, to* check for the modular multiplicative inverse $\mu = (J(k^{\lambda} \ \ mod\, n^2\ ))^{-1} \ \ mod\, n,$ to make sure that n can divide the order of k $J(s) = \frac{s-1}{n}$
Step 5	The public key, therefore, is *(n,g)* while the private key is (λ, μ)
2. Encryption algorithm	
Step 1	Given message, s to be encrypted, Where $0 \le s \le n$
Step 2	Choose a number, y at random, Such that $0 \le y \le n$ and $y \in Z^*_n$
Step 3	Calculate the ciphertext of the message as: $c = k^m \cdot y^n \ \ mod\, n^2$
3. Decryption algorithm	
Step 1	A ciphertext, c to be decrypted, such that $c \in Z^*_{n^2}$
Step 2	Obtain the plaintext, s as $s = L(c^{\lambda} \ \ mod\, n^2) \cdot \mu \ \ mod\, n$



CPE 500L Result

Tallest

ID	Name	Votes
1	DJ Lovett	1
2	Serah Fadipe	0
3	Samuel Kure	0

Most Handsome

ID	Name	Votes
5	Ozomah Daniel	0
6	Ofoni Philiph	1
7	Abbas Ogaji	0

Most Social

ID	Name	Votes

Fig. 12 Secure e-voting system log in page

positions, voters' log in, and votes casting log in page and many others (see Fig. 12).

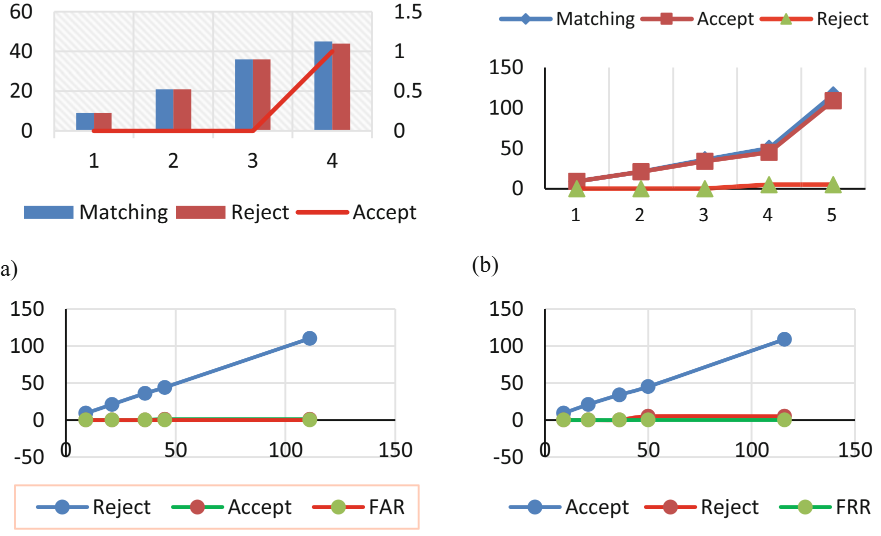
Performance Evaluation The secure smart electronic voting system is subjected to testing, and it was evaluated using false acceptance rate (FAR) and false rejection rate (FRR). The metrics were selected for the performance evaluation to cross-check and validate the correct voters' enrolment and nonregistered candidates (see Tables

Table 3 The result of FAR during testing

Matching trials	Rejected	Accepted	FAR
9	9	0	0%
21	21	0	0%
36	36	0	0%
45	44	1	2%
111	110	1	0.02

Table 4 False rejection rate FRR

Matching trial	Accept	Reject	FRR
9	9	0	0%
21	21	0	0%
36	34	0	0%
50	45	5	10%
116	109	5	0.1



(a)

(b)

(c)

(d)

Fig. 13 The system evaluation performance during testing was presented, (**a**) the number of trials for rejection to acceptance, (**b**) the number of trials of acceptance to rejection, (**c**) the rejection to the accepted rate FAR, and (**d**) the acceptance to the rejection rate (FRR)

3 and 4). The FRR is used to evaluate and benchmark the correctly authenticated registered voters and enrolment in the system. The electronic voting system was evaluated based on the number of FAR, FRR, and latency (see Figs. 13 and 14). The blockchain certification performance using the Paillier homomorphic method was evaluated based on the retrieval time (latency), certificate size, and execution (see Fig. 15).

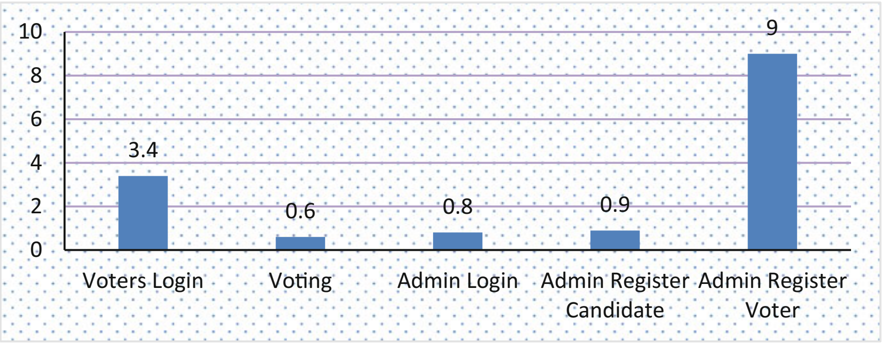


Fig. 14 System response time during testing

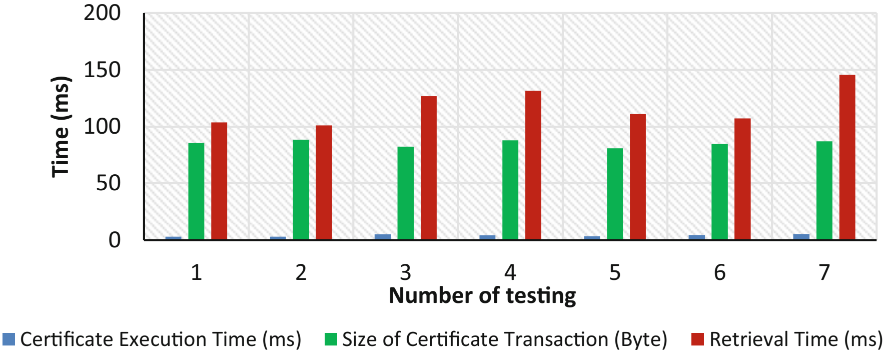


Fig. 15 Crypto-blockchain performance testing

5 Conclusions

This research study investigates the areas of an application using blockchain technology with cryptography algorithm as a recent efficient security countermeasure to avert the data privacy, confidentiality, and trust breaches. It further proposed efficient security measures against vulnerability to data tampering, fraud, and hacking of electronic voting systems. A private blockchain technology for securing decentralized ledger or database was adopted to prevent the central authority from fraud and data tampering. A Paillier homomorphic encryption algorithm was implemented with blockchain to make the system immutable, transparent in the chain transaction, and secured. Also, a bi-factor authentication technique (iris and fingerprint) was used for the voter's registration, verification, and genuine authenticity, which performs efficiently with 0.02% FAR and 0.1% FRR. The system response time was measured, and it was relatively fast as it takes less than 1 min to accept registered candidates during the verification process. The credential execution time, retrieval time, and size of the certificate transaction were measured in milliseconds and give better performance response time.

References

1. Banerjee, S. P., & Woodard, D. L. (2012). Biometric authentication and identification using keystroke dynamics: A survey. *Journal of Pattern Recognition Research, 7*(1), 116–139.
2. Aluaigba, M. T. (2016). Democracy deferred: The effects of electoral malpractice on Nigeria's path to democratic consolidation. *Journal of African Elections, 15*(2), 136–158.
3. Ayinde, A. F., & Idowu, A. O. (2016). Nigeria's 2015 elections: Permanent voter's cards, smart card readers and security challenges. *Journal of African Elections, 15*(2), 50–68.
4. Udu, L. E. (2015). INEC and 2015 general elections in Nigeria: Matter arising. *Democracy, 5*(12), 96–108.
5. Inalegwu, O. C., Dogo, E. M., Kolo, J. G., Bima, M. E., Ajao, L. A., & Inechioma, J. (2018). Development of a biometric-based car park access control and billing system. In *The second international Engineering Conference (IEC)* (pp. 421–425). Nigeria.
6. Okokpujie, K., Etinosa, N. O., John, S., & Joy, E. (2018). Comparative analysis of fingerprint preprocessing algorithms for electronic voting processes. In *IT Convergence and Security 2017* (pp. 212–219). Springer.
7. Abo-Rizka, M., & Ghounam, H. R. (2007). A novel e-voting in Egypt. *International Journal of Computer Science and Network Security, 7*(11), 226–234.
8. Rahman, M. A., Hossain, M. S., Loukas, G., Hassanain, E., Rahman, S. S., Alhamid, M. F., & Guizani, M. (2018). Blockchain-based mobile edge computing framework for secure therapy applications. *IEEE Access, 6*, 72469–72478.
9. Aditya, S. N., Kishore, M. V., & Suresh, C. (2018). A secure e-voting system using RSA and md5 algorithms using random number generators. *International Journal of Applied Engineering Research, 18*(11), 9468–9473.
10. Abayomi-Zannu, T. P., Odun-Ayo, I., Tatama, B. F., & Misra, S. (2019). 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).
11. Ajao, L. A., Agajo, J., Olaniyi, O. M., Jibril, I. Z., & Sebiotimo, A. E. (2019). A secure tracking automobile system for oil and gas distribution using telematics and blockchain techniques. *Journal of Electrical and Computer Engineering, 7*(3), 257–268.
12. Hjálmarsson, F. P., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018). Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)* (pp. 983–986).
13. Ajao, L. A., Agajo, J., Adedokun, E. A., & Kargong, L. (2019). Crypto-hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry. *International Journal of Molecular Sciences, 2*(3), 300–325.
14. Awotunde, J. B., Ogundokun, R. O., Jimoh, R. G., & Misra, S. (2021). Machine learning algorithm for cryptocurrencies price prediction. In S. Mistra & T. A. Kumar (Eds.), *Artificial intelligence for cybersecurity: Methods, issues, and possible horizons or opportunities* (Studies in computational intelligence) (Vol. 972). Springer.
15. Velmurugadass, P., Dhanasekaran, S., Anand, S. S., & Vasudevan, V. (2021). Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings, 37*, 2653–2659.
16. Shanaev, S., Shuraeva, A., Vasenin, M., & Kuznetsov, M. (2019). Cryptocurrency value and 51% attacks: Evidence from event studies. *Journal of Alternative Investments, 22*(3), 65–77.
17. Saleh, F. (2021). Blockchain without waste: Proof-of-stake. *The Review of Financial Studies, 34*(3), 1156–1190.
18. Zhang, R., & Chan, W.-K. (2020). Evaluation of energy consumption in block-chains with proof of work and proof of stake. *Journal of Physics: Conference Series, 1584*(1), 12–23.
19. Shaikh, M. Z. (2021). A review on cryptocurrency with distributed ledger technology for blockchain technology. *Turkish Journal of Computer and Mathematics Education, 12*(9), 143–151.

20. Singhal, B., Dhameja, G., & Panda, P. S. (2018). *Introduction to the blockchain. In beginning blockchain* (pp. 1–29). Apress.
21. Li, X., Wang, Y., Vijayakumar, P., He, D., Kumar, N., & Ma, J. (2019). Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network. *IEEE Transactions on Vehicular Technology, 68*(11), 11309–11322.
22. Jindal, A., Aujla, G. S., & Kumar, N. (2019). SURVIVOR: A blockchain-based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment. *Computer Networks, 153*, 36–48.
23. Aziz, N., Ridiah, R., & Susanto, H. (2021). Encryption of digital banking transaction records: A blockchain cryptography security approach. *International Journal of Computers and Applications, 975*, 8887.
24. Belej, O., Staniec, K., & Wieckowski, T. (2020). The need to use a hash function to build a crypto algorithm for blockchain. In *International conference on dependability of computer systems* (pp. 51–60). Springer.
25. Mondal, A. H., Ranjan, M., & Saikia, M. (2015). A brief overview of homomorphic cryptosystem and their applications. *International Journal of Computers and Applications, 975*, 8887.
26. Mistra, S. (2021). *A step by step guide for choosing project topics and writing research papers in ICT related disciplines, communications in computer and information science* (Vol. 1350, pp. 727–744). Springer.
27. Sadia, K., Masuduzzuaman, M., Paul, R. K., & Islam, A. (2020). Blockchain-based secure e-voting with the assistance of smart contract. In *IC-BCT 2019* (pp. 161–176). Springer.
28. Dhulavvagol, P. M., Bhajantri, V. H., & Totad, S. G. (2020). Blockchain ethereum clients performance analysis considering e-voting application. *Procedia Computer Science, 167*, 2506–2515.
29. Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Softwares, 35*(4), 95–99.
30. Ch, R., Srivastava, G., Gadekallu, T. R., Maddikunta, P. K. R., & Bhattacharya, S. (2020). Security and privacy of UAV data using blockchain technology. *Journal of Information Security and Applications, 55*, 102670.
31. Hobil, M., Kompara, M., Kamisalic, A., & Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry, 10*(10), 470.
32. McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications, 135*, 62–75.
33. Sharma, M., Sehrawat, R., Daim, T., & Shaygan, A. (2021). Technology assessment enabling blockchain in hospitality and tourism sectors. *Technological Forecasting and Social Change, 169*, 120810.
34. Jindal, A., Aujla, G. S., Kumar, N., & Villari, M. (2020). GUARDIAN: Blockchain-based secure demand response management in smart grid system. *IEEE Transactions on Services Computing, 13*(4), 613–624.
35. Wei, P. C., Wang, D., Zhao, Y., Tyagi, S. K. S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems, 102*, 902–911.
36. Houtan, B., Hafid, A. S., & Makraksi, D. (2020). A survey on blockchain-based self-sovereign patient identity in healthcare. *IEEE Access, 8*, 90478–90494.
37. Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure digital voting system based on blockchain technology. *International Journal of Electronic Government Research, 14*(1), 53–62.
38. Yi, H. (2019). Securing e-voting based on blockchain in a P2P network. *EURASIP Journal on Wireless Communications and Networking, 2019*(1), 1–9.
39. Umar, B. U., Olaniyi, O. M., Ajao, L. A., Maliki, D., & Okeke, I. C. (2019). Development of a fingerprint biometric authentication system for secure electronic voting machines. *KINETIK Journal, 4*(2), 115–126.

40. Jabbar, I., & Alsaad, S. N. (2017). Design and implementation of secure remote e-voting system using homomorphic encryption. *International Journal of Network Security, 19*(5), 694–703.
41. Al-Anie, H. K., Alia, M. A., & Hnaif, A. A. (2011). E-voting protocol based on public-key cryptography. *International Journal of Network Security & Its Applications, 3*(4), 87–98.
42. Lalam, N., Nithinn, M. S., & Jebakumar, D. R. (2020). BEVS-blockchain based e-voting system. *International Journal of Advanced Science and Technology, 29*, 6241–6249.
43. Hsiaso, J., Tso, R., Chen, C. M., & Wu, M. E. (2017). Decentralized e-voting systems based on the blockchain technology. In *Advances in computer science and ubiquitous computing* (pp. 305–309). Springer.
44. Panja, S., & Roy, B. (2021). A secure end-end verifiable e-voting system using blockchain and cloud server. *Journal of Information Security and Applications, 59*, 102815.
45. Bulut, R., Kantarci, A., Kesskin, S., & Bahtiyar, S. (2019). Blockchain-based electronic voting system for election in Turkey. In *2019 4th international conference on computer science and application engineering* (pp. 183–188). IEEE.
46. Yellamma, P., Anupama, P., Lakshmibhavani, K., Priya, U. J. S., & Ch, K. (2020). Implementation of e-voting system using Blockchain technology. *Journal of Critical Reviews, 7*(6), 865–870.