International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 14, No. 3, November 2025, pp. 810~820
ISSN: 2089-4864, DOI: 10.11591/ijres.v14.i3.pp810-820

Development of a blockchain-based electronic voting system utilizing national identification number

Olabode Idowu-Bismark[1,2], Oluwadamilola Oshin[1,2], Emmanuel Adetiba[1,2]
[1]Department of Electrical and Information Engineering, College of Engineering, Covenant University, Ota, Nigeria
[2]Covenant Applied Informatics and Communication Africa Centre of Excellence (CApIC-ACE), a World Bank ACE-IMPACT Centre, Covenant University, Ota, Nigeria

Article Info

Article history:

Received Jan 24, 2025
Revised Aug 14, 2025
Accepted Sep 9, 2025

Keywords:

Biometric verification
Blockchain
Electronic voting system
National identification number
Security and transparency

ABSTRACT

Traditional voting methods in Nigeria face numerous challenges, including logistic issues, security concerns, and allegations of fraud, which undermine public trust. This work develops a blockchain-based electronic voting system (EVS) that leverages the national identification number (NIN) for biometric verification to address these issues. The research identifies the limitations of current blockchain voting solutions, such as implementation complexity, scalability issues, user adoption resistance, and cybersecurity threats and provide a more secure and user-friendly alternative. The system integrates blockchain technology with biometric verification to create an immutable, transparent, and secure voting process. The methodology involves designing a system architecture that includes a blockchain network, an NIN verification module, and a user interface (UI). Users register using their NIN, authenticate themselves, and cast their votes, which are then encrypted and recorded on the blockchain. The system's functionality was tested using tools like Ganache for local blockchain development, MetaMask for Ethereum wallet integration, and Solidity for writing smart contracts. Results from the implementation indicate significant improvements in security, transparency, and user accessibility compared to traditional voting systems. The user authentication test achieved a 100% valid login success rate and 0% invalid login attempts. Meanwhile, the voting test accuracy was 100%.

Corresponding Author:

Oluwadamilola Oshin
Department of Electrical and Information Engineering, College of Engineering, Covenant University
Ota, Nigeria
Email: oluwadamilola.oshin@covenantuniversity.edu.ng

1. INTRODUCTION

The democratic process, fundamental to the governance of any nation, hinges upon the integrity and accessibility of its electoral system. In Nigeria, as in many nations worldwide, the efficiency, security, and transparency of elections have been subject to considerable scrutiny. Countries often use mechanical voting apparatuses, electronic voting methods, and traditional paper polling [1]. Nonetheless, new digital technologies are required. An e-voting system offers the potential to mitigate these challenges by leveraging technology to streamline the voting process, enhance security, and improve transparency. Blockchain, initially known for underpinning cryptocurrencies, has evolved into a powerful tool with applications across various sectors due to its immutable and decentralized nature [2], [3]. This technology offers a viable way to have transparent and safe e-voting. By using a distributed ledger, blockchain can record each vote in the chain as a block, creating a transparent and tamper-proof system [4]. In the context of Nigerian elections, this technology could potentially address concerns related to vote manipulation, double voting, and result tampering. Blockchain technology eliminates the infinite copying of digital assets. The long-standing problem of duplicate spending is resolved by ensuring that each unit of value is only transferred once [5].

Blockchain technology presents a possible way forward for revolutionizing the democratic process, ensuring greater transparency, security, privacy, and inclusivity [6]. One of the core motivations is to alleviate the logistical barriers and shortcomings of the traditional voting process. Though e-voting has a lot of obstacles to transcend, it seeks to transcend the limitations imposed by physical ballots and polling stations [7]. By utilizing blockchain technology, the suggested approach may provide an unchangeable and transparent record of election-related actions, establishing a standard for the integrity of other data-driven procedures outside of elections [8], [9]. This system's successful implementation could serve as a beacon of hope for nations globally, showcasing a model that champions fair, secure, and accessible elections. The concept of blockchain is often ascribed to Satoshi Nakamoto, who created the digital money; bitcoin. Since then, numerous new cryptocurrencies have emerged, including Ethereum, which was suggested by Vitalik Buterin in 2013 which introduced smart contracts [10]. For many years, information, assets and money has been exchanged over the internet using a trusted intermediary for the sake of accountability and security [11]. The evolution of blockchain technology can be traced through its developmental stages, marked by distinct advancements and applications. In its initial phase, often referred to as Blockchain 1.0, the technology found its primary representation in the form of cryptocurrencies, notably exemplified by Bitcoin [12]. In this stage, transactions were encrypted using the trader's private key, enabling direct completion of transactions between parties without the need for third-party management.

Bitcoin's efficiency, security, and fairness were assessed using key performance measures like as transaction throughput transactions per second (TPS), network latency, fork count, and mining reward. The technology primarily focused on transactional capabilities and lacked focus on the performance of individual blocks and tracking [12]. The introduction of programmable smart contract technology by Ethereum, a representative of Blockchain 2.0, broke the constraints of the closed loop information system previously observed. Ethereum's smart contracts allow for the passive execution of contract terms based on logical conditions, encouraging innovative methods of interacting with practical technology. The advent of Blockchain 2.0, exemplified by Ethereum, heralded in a new era of possibilities [12]. In Blockchain 2.0, agreements between many parties with electronic signatures serve as the starting point for transactions. Smart contracts that contain contractual terms and conditions are triggered and carried out by all of the blockchain network's nodes. This breakthrough, spearheaded by Ethereum, demonstrated the transformational potential of Blockchain 2.0 by expanding the use of blockchain technology beyond the realm of currency. The development of blockchain from its inception in 2009 to the present is seen in Figure 1 [12].

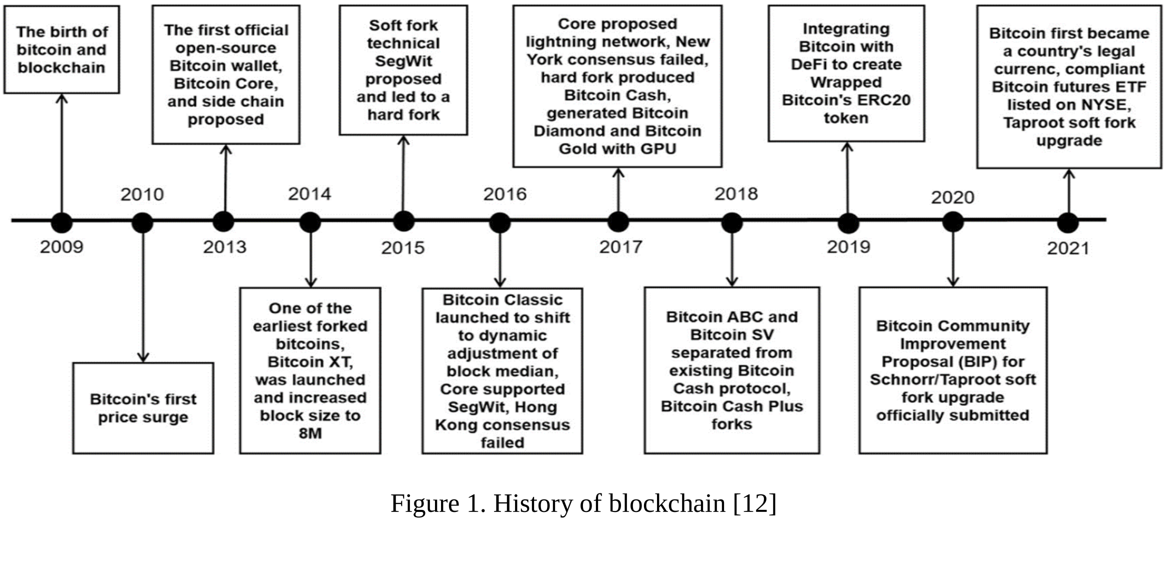

The birth of bitcoin and blockchain
2009
2010
Bitcoin's first price surge
The first official open-source Bitcoin wallet, Bitcoin Core, and side chain proposed
2013
2014
One of the earliest forked bitcoins, Bitcoin XT, was launched and increased block size to 8M
Soft fork technical SegWit proposed and led to a hard fork
2015
2016
Bitcoin Classic launched to shift to dynamic adjustment of block median, Core supported SegWit, Hong Kong consensus failed
Core proposed lightning network, New York consensus failed, hard fork produced Bitcoin Cash, generated Bitcoin Diamond and Bitcoin Gold with GPU
2017
2018
Bitcoin ABC and Bitcoin SV separated from existing Bitcoin Cash protocol, Bitcoin Cash Plus forks
Integrating Bitcoin with DeFi to create Wrapped Bitcoin's ERC20 token
2019
2020
Bitcoin Community Improvement Proposal (BIP) for Schnorr/Taproot soft fork upgrade officially submitted
Bitcoin first became a country's legal currenc, compliant Bitcoin futures ETF listed on NYSE, Taproot soft fork upgrade
2021

Figure 1. History of blockchain [12]

A blockchain is an ever-growing set of records, or blocks, that are linked together via cryptographic methods [13]. A block is a record that contains any kind of data in a blockchain [14]. Every block includes a timestamp, transaction information, and the cryptographic hash of the previous block, which may be mapped using a hashing algorithm. The timestamp influences the hash of the block by providing proof that the transaction data was there at the moment the block was added. Each additional block reinforces the integrity of the ones that came before it, forming a chain of interconnected blocks. Because of its intrinsic structure, the blockchain is impervious to changes in the data it contains since changing any one block would necessitate changing all of the blocks that come after it.

A public ledger in blockchain is a secure decentralized database shared among all network participants [11]. It records every transaction that occurs among the participants. Individuals can access and review their transactions at any time. Figure 2 highlights several other characteristics of blockchain.

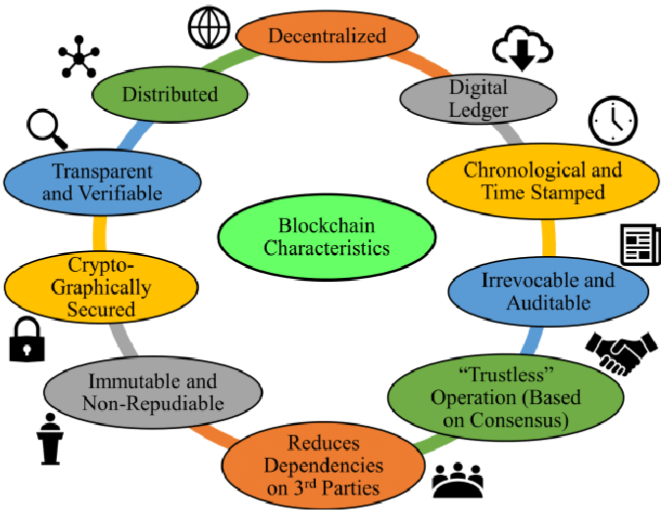

Blockchain Characteristics
Decentralized
Digital Ledger
Chronological and Time Stamped
Irrevocable and Auditable
"Trustless" Operation (Based on Consensus)
Reduces Dependencies on 3rd Parties
Immutable and Non-Repudiable
Crypto-Graphically Secured
Transparent and Verifiable
Distributed

Figure 2. Characteristics of blockchain [11]

Blockchain frameworks refer to software solutions designed to streamline the creation and implementation of blockchain applications with minimal customization [10]. These frameworks encompass both the infrastructure and libraries necessary for application development. The infrastructure, also known as the network infrastructure, comprises nodes and the corresponding software they run. In recent years, several frameworks have come into existence like Ethereum, Hyperledger, Corda, enterprise operating system (EOS), internet of things application (IOTA), Ripple (XRP), and Quorum. There are several factors to assess the effectiveness of the framework. In the case of Ethereum, it employs Merkle trees to enhance the efficiency of transactional hashing, thereby improving scalability possibilities [10].

The fundamental structure of blockchain is blocks, each of which has a list of transactions, and these blocks are connected chronologically. As seen in Figure 3, every block generally incorporates a cryptographic hash to refer to the preceding block, resulting in an unchangeable and continuous record that is stored in the chain [14], [15].

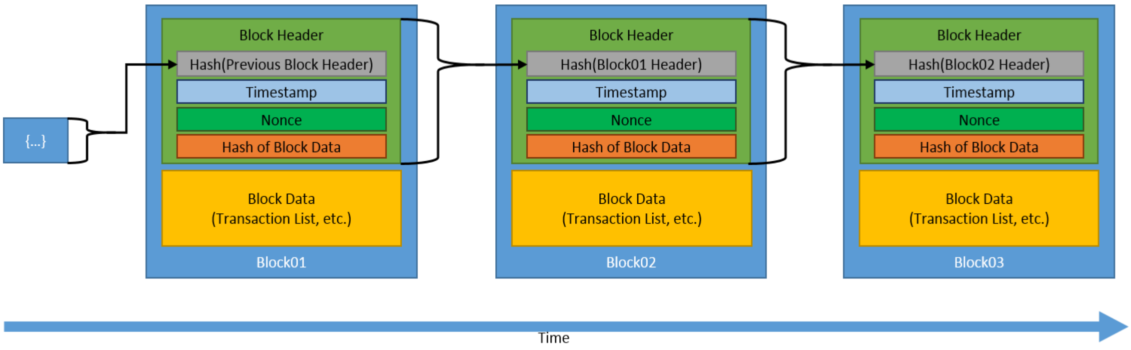


Figure 3. Structure and operation of blockchain [10]

Given the blockchain's commitment to decentralization, there is no reliance on a trusted third party for secure data storage, management, or accountability in the event of security breaches [16]. After compiling these verified transactions into a new block, all participants participate in the consensus protocol to decide whether the transaction is validated.

Blockchain technology can be classified into private, public, and consortium blockchain [17]. Decentralized networks known as public blockchains enable everyone to join, approve transactions, keep track of the blockchain ledger, and contribute to the network as they are public [18]. Participants preserve the integrity of the blockchain by validating transactions using a consensus method [19]. Public blockchains include the well-known platforms Ethereum and Bitcoin. Private blockchains are more centralized than public ones, as they are typically operated and controlled by a single organization or a group of collaborating organizations [20]. They offer a higher degree of control and privacy to participants. A hybrid concept called consortium blockchains combines elements of public and private blockchains. Consortiums provide a balance between decentralization and control [21]. In a consortium blockchain, the processes for reaching consensus are overseen by nodes that have been pre-established [20].

A pivotal aspect of blockchain infrastructure is the consensus algorithm, responsible for upholding the blockchain's security. It could be proof of work where miners compete to solve challenging mathematical puzzles or proof of stake which chooses the author of a new block based on the quantity of bitcoin that the creator is prepared to "stake" as security [6], [22]. There are also so many more consensus algorithms such as proof of elapsed time (PoET), proof of capacity (PoC), and proof of weight (PoW) [2]. The field of biometrics utilizes automated technologies to identify individuals through their distinctive physical or behavioral traits [23]. Biometric technologies were first introduced in the 2015 Nigerian elections, promising to curb widespread electoral malpractices that had long haunted the nation's democratic aspirations [24]. After the elections, the number of states which electoral malpractice occurred reduced drastically as well as the number of petitions challenging the outcome of the elections [25]. This method partially eliminated the electoral fraud for the 2015 elections. The national identification number (NIN) project began in 2003 under the Olusegun Obasanjo administration with the purpose of creating a unique identifying system for every Nigerian citizen and legal resident. Beyond its initial purpose, NIN has become a cornerstone of national infrastructure. It facilitates access to essential services like passports, bank accounts, and social programs, acting as a ubiquitous verification tool [23]. Notably, its unique identifier and biometric linkage serve as a deterrent against fraudulent activities and impersonation across various sectors. While the NIN is not yet universal for Nigerians, it's true that its enrollment has significantly increased due to its requirement for various services and activities and would continue to increase especially when it is integrated into the election process [26], [27]. The nation's elections have long been plagued by issues like multiple voting, underage voting, and the persistent presence of "ghost voters [28]." NIN's unique and verifiable nature, coupled with its biometric authentication, offers a potential solution to these systemic problems [29].

Blockchain technology is being used by voting systems because of a deep-seated need to solve flaws in conventional procedures [30]. In this context, blockchain technology emerges as a potential game-changer, offering a secure, transparent, and verifiable solution to revolutionize the way we conduct elections [31]. An unchangeable and verifiable record is created when every vote is encrypted and added to a chain of blocks [32]. Blockchain's distributed ledger makes tampering with voting data significantly more challenging, as attackers would need to compromise numerous nodes across the network, not just a single entry point [33]. The unique structure of blockchain, where the last node acts as a comprehensive repository, enables near-instantaneous result access, fostering exceptional efficiency [34]. In countries like Nigeria, where restoring faith in electoral systems is crucial, actively investigating and addressing the challenges of blockchain implementation can lay the groundwork for a brighter future of democracy [35].

The functional requirements of the system are:

- The system must accept a record of eligible voters from the electoral commission.
- The system should allow eligible voters to register and create user accounts securely. It should verify the authenticity of voter information to prevent fraudulent registrations.
- The system should provide a mechanism for candidates to register their candidacy and provide necessary information for voters to make informed decisions.
- The system should generate digital ballots that accurately represent the candidates and voting options. It should ensure that each voter receives a unique and tamper-proof ballot.
- The system should enable voters to cast their votes securely and privately. It should provide a user-friendly interface for selecting candidates and recording votes and not allow for multiple voting.
- The system should validate the integrity of each cast vote to ensure it has not been tampered with or altered. It should verify that the vote meets the necessary criteria and is valid.
- The system should count the votes accurately and transparently. It should aggregate the votes from all participants and generate the final election results.
- The system should allow voters to be able to view the election results.

Beyond the functionalities of the system, it needs to consider non-functional aspects for successful implementation such as:

- The system must be resistant to hacking, manipulation, and other security threats. This involves robust cryptography and secure communication protocols throughout the voting process.
- The system should be able to handle a large number of voters and votes efficiently, especially for large-scale elections.
- The voting platform must be highly available during elections to ensure everyone can participate without downtime.
- The system should not allow the votes to the modified after voting.
- The system should allow anyone to verify the election process and results without compromising voter privacy using blockchain's public ledger.
- The system should not link votes to individual voters.
- The voting platform should be user-friendly and accessible to voters with varying levels of technical knowledge.

2. RESEARCH METHOD

The architecture of the system comprises five key components that work together to establish a secure, transparent, and efficient platform for conducting elections. These components are the user interface (UI), identity verification, blockchain network with smart contracts, voting database with consensus mechanism, and the e-voting platform. The UI serves as the front-end component, providing a user-friendly interface through which voters can interact with the system. Identity verification is an essential component that validates the identities of voters before they can participate in the voting process using a unique identification number NIN. The blockchain network with smart contracts forms the core of the system architecture. Smart Contracts, on the other hand, automate and enforce voting rules, such as eligibility criteria, vote counting, and result declaration. The voting database encrypts each vote and links it to the respective voter's identity, preserving anonymity and preventing tampering. Meanwhile, the Consensus Mechanism ensures agreement on the validity and order of transactions within the blockchain network. Lastly, the e-voting process component provides mechanisms for independent auditing and verification of the voting process. Through this architecture which is depicted in Figure 4, the system ensures transparency, security, and efficiency, revolutionizing the way elections are conducted by leveraging the benefits of blockchain technology.

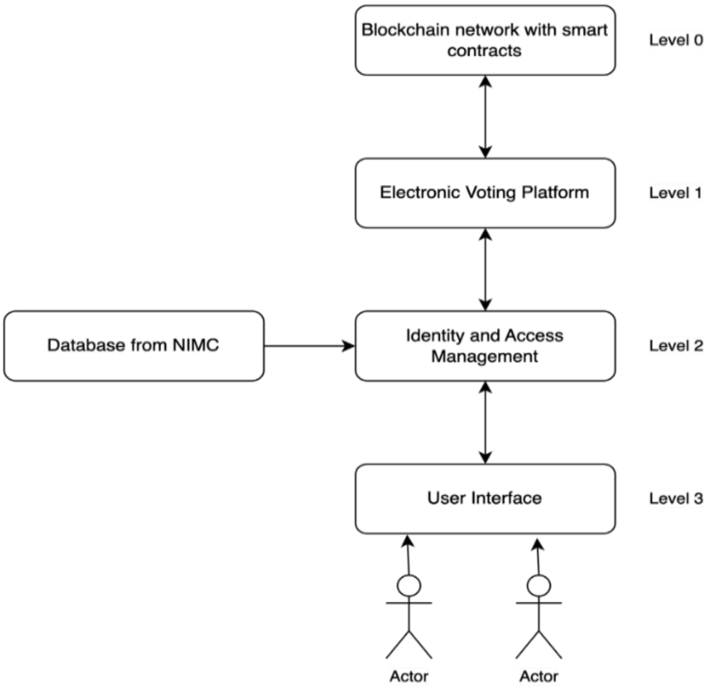

Blockchain network with smart contracts
Level 0
Electronic Voting Platform
Level 1
Database from NIMC
Identity and Access Management
Level 2
User Interface
Level 3
Actor
Actor

Figure 4. Structural layer of the system

The voting and user access layer serves as the pivotal interface within the system, orchestrating both the voting process and user authentication seamlessly. This layer encompasses two crucial components: the voting layer, responsible for the core logic governing voting operations, and the user access layer, which manages user authentication and authorization. Figure 5 shows the class diagram for the voting layer.

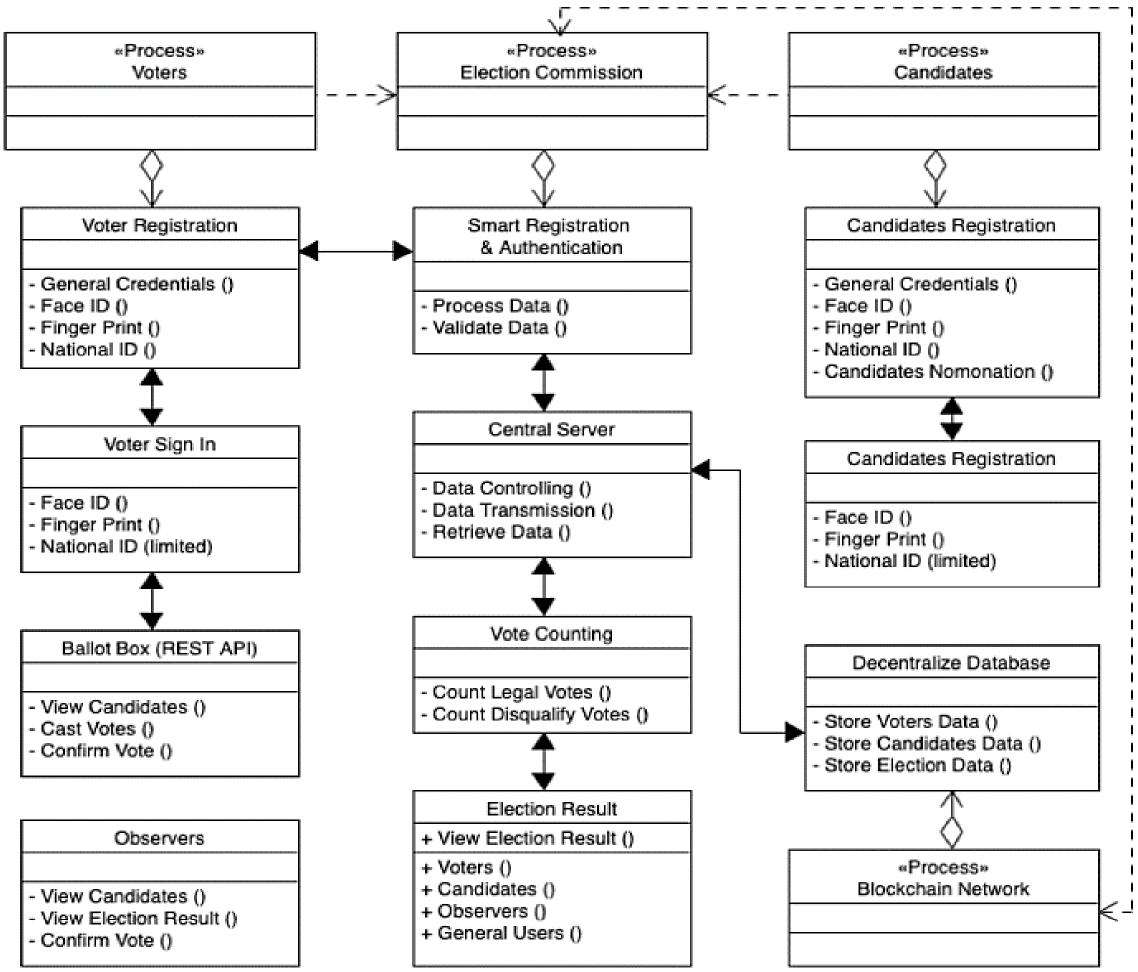


Figure 5. Class diagram for the voting layer

Moreover, the voting layer empowers administrators, or electoral officials, to manage elections effectively. This entails functionalities such as adding candidates to elections and creating new election instances, ensuring the smooth operation of the electoral process. On the other hand, the user access layer is dedicated to verifying the identity and permissions of users within the system.

2.1. Sequence diagram for the user interaction with the e-voting system

The sequence diagram illustrates the flow of events during the e-voting process. The system involves several key components such as the user, UI, electronic voting system (EVS), database and the blockchain. Users begin by logging in through the UI, inputting their username and password. The UI acts as the bridge between users and the EVS. Upon receiving login details, the EVS checks for available elections by querying the database to determine which elections are currently open and The UI displays the available elections to the user. Users select their preferred candidates and after confirming their choice they cast their votes. The EVS records these votes in both the database and the blockchain and sends a confirmation request to the user. Once confirmed, the vote is officially recorded. Users can later check election results through the UI. The UI retrieves data from both the Database and the Blockchain, ensuring accurate and reliable results. Finally, users can log out from the system. This is represented in the sequence diagram in Figure 6.

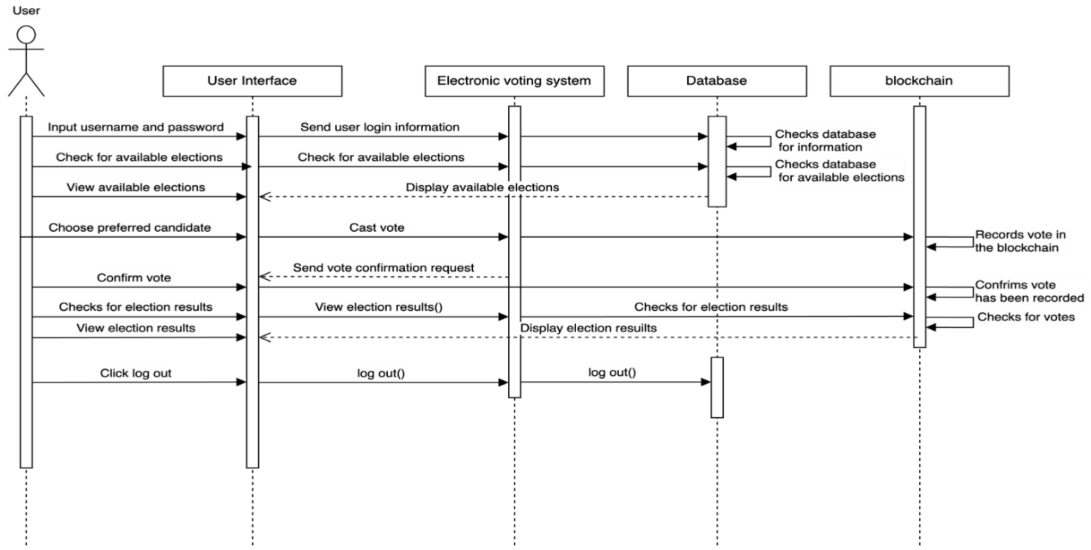

User
User Interface
Electronic voting system
Database
blockchain
Input username and password
Send user login information
Checks database for information
Check for available elections
Check for available elections
Checks database for available elections
View available elections
Display available elections
Choose preferred candidate
Cast vote
Records vote in the blockchain
Send vote confirmation request
Confirm vote
Confrims vote has been recorded
Checks for election results
View election results()
Checks for election results
Checks for votes
View election results
Display election resuilts
Click log out
log out()
log out()

Figure 6. Sequence diagram for the user interaction with the system

2.2. Sequence diagram for the admin interaction with the e-voting system

The admin system involves several critical components such as the admin, the admin interface, the EVS, the database and the blockchain. The process begins with the admin logging in through the admin interface using their username and password to gain access. Upon receiving the login details, the EVS checks for available elections by querying the database to determine which elections are currently open. The admin interface displays the available elections to the admin. If the admin decides to create a new election, they proceed by adding their preferred candidates through the same interface. This action triggers a response in the EVS, where a new election is created, and the candidates are added accordingly. The database plays a crucial role in storing and retrieving information throughout this process. It checks for information related to available elections and election results when prompted by either the admin interface or the EVS. The blockchain ensures that all data related to votes and election details is securely stored and immutable. As voting progresses, both admins and voters can check election results through their respective interfaces. The results are retrieved in real-time from data stored in the database and the Blockchain. Finally, after completing their tasks or reviewing results, admins can log out from the system. This logout action is mirrored across all components, ensuring the security and integrity of user data at all times. This is represented in the sequence diagram in Figure 7.

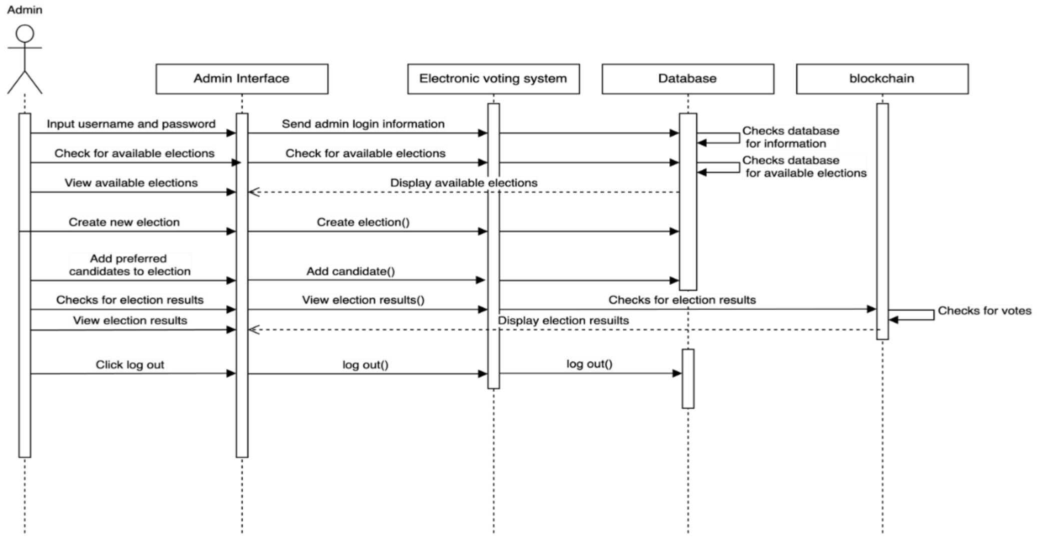

Admin
Admin Interface
Electronic voting system
Database
blockchain
Input username and password
Send admin login information
Checks database for information
Check for available elections
Check for available elections
Checks database for available elections
View available elections
Display available elections
Create new election
Create election()
Add preferred candidates to election
Add candidate()
Checks for election results
View election results()
Checks for election results
Checks for votes
View election results
Display election resuilts
Click log out
log out()
log out()

Figure 7. Sequence diagram for the admin interaction with the system

2.3. System implementation

The system was implemented in four stages which include the UI implementation, identity verification implementation, blockchain network with smart contracts implementation, and the implementation of the e-voting platform. This was done using HTML, CSS, JavaScript, Ganache, Truffle, Chrome browser equipped with the MetaMask extension, Visual Studio Code, Node.js, and a computer.

The UI implementation involves designing and developing the graphical and interactive elements of the system, ensuring a user-friendly and intuitive experience. This was done using HTML and CSS. The identity verification implementation involves integrating secure methods for verifying user identities against a certified database, ensuring that the system can authenticate users accurately and reliably. This was done by creating a database of registered individuals. The system checks any login credentials against the database and permits authenticated users. The format of an identity is registered in this form:

```
{
   "idNumber": "12345678901",
   "firstName": "Chinedu",
   "lastName": "Okonkwo",
   "email": "chinedu.okonkwo@gmail.com"
  }
```

The blockchain network with smart contracts implementation leverages blockchain technology to provide a decentralized and tamper-proof ledger for transactions. Smart contracts are utilized to automate processes and enforce rules within the system, enhancing transparency and reducing the risk of fraud. The voter registration process is managed by the “Vote” function within the smart contract. This function ensures that each voter can only vote once and that their vote is recorded accurately. The “addCandidate” function handles candidate registration, ensuring only the manager (administrator) can add candidates. The user registration process is managed by the “addUser” function, which stores user information securely on the blockchain. The E-voting platform implementation focuses on developing and integrating the functionalities required for electronic voting. It includes designing the voting process, ensuring the integrity and anonymity of votes, and implementing features to tally and verify results accurately.

3. RESULTS AND DISCUSSION

The system underwent three sets of comprehensive tests: blockchain tests, user authentication tests, and voting tests. The blockchain and user authentication tests were conducted on the back end, while the voting tests were performed on the front end.

3.1. User authentication test

Equations the purpose of the user authentication test was to ensure that only users with valid credentials could access the system. The test was designed to verify that users could log in only when both their username NIN and password were correct. This validation is crucial to maintaining the security and integrity of the voting system, preventing unauthorized access and ensuring that only eligible voters can participate.

Results:
Success rate for valid login attempts: 100%
Success rate for invalid login attempts: 0%

3.2. Blockchain test

For the blockchain test, Ganache was utilized to simulate the blockchain environment. Multiple blocks were created and the blockchain chains returned by each were carefully compared to verify consistency. This test confirmed two of the most significant properties of blockchain technology: immutability and decentralization. Once transactions are recorded on the blockchain, they cannot be altered or deleted, ensuring the integrity and permanence of the voting records. The blockchain operates on a decentralized network, meaning there is no single point of failure or control, which enhances the security and resilience of the system.

Results:
Consistency of blockchain chains: verified
Immutability of transactions: confirmed

3.3. Voting test

The voting test was conducted on the front end to evaluate the UI and user experience. This test ensured that the voting process was intuitive, secure, and that votes were correctly recorded on the

blockchain. It also assessed the system's ability to handle a large number of concurrent users, reflecting the conditions of a real-world election scenario.
Results:
User interface: intuitive and user-friendly
Vote recording accuracy: 100%
Concurrent user handling: efficient, with no performance degradation observed

The comprehensive results from the tests demonstrate that the blockchain-based e-voting system is secure, reliable, and user-friendly. The user authentication mechanism effectively prevents unauthorized access, ensuring that only eligible voters can participate. The blockchain test results confirm that the system maintains the integrity and immutability of voting records, which is crucial for transparency and trust in the electoral process. Based on the test results, the blockchain demonstrated persistent data storage capabilities. Even after the front end was shut down and the database was deleted, the election results remained intact. This highlights the immutability of blockchain technology, which is a key feature. Additionally, the distributed nature of the blockchain system ensures there is no single point of failure, enhancing the system's reliability. Data persistence was also evident, meaning information is distributed across the network rather than being centralized on individual computers as in traditional database systems.

4. CONCLUSION

This project demonstrated that a blockchain-based election system is both feasible and practical. The proposed system empowers the public, rather than a central authority, to validate, verify, and monitor elections. Given the crucial role voting plays in society, there is a pressing need for a secure and trustworthy voting system. The proposed e-voting system using blockchain technology is justified as it offers significant advantages over existing voting systems, including enhanced security, transparency, and resistance to tampering. These studies collectively underscore the potential of blockchain technology to revolutionize voting systems, offering enhanced security, transparency, and efficiency, and addressing many of Nigeria's electoral challenges. The decentralized and transparent nature of blockchain ensures that every vote is accurately recorded and verifiable, thereby creating greater trust in the electoral process. The implementation of smart contracts can automate and enforce election rules, further minimizing the risk of fraud and manipulation. Overall, this project highlights the promise of blockchain in creating a secure and trustworthy voting system, laying the groundwork for future developments in electoral technology. The limitations of the project include the availability of adequate technological infrastructure, internet connectivity, and accessibility, particularly in the rural areas.

ACKNOWLEDGMENTS

The authors thank the Covenant Applied Informatics and Communication Africa Centre of Excellence (CApIC-ACE), the Federated Genomic (FEDGEN) Research Cluster of Covenant University, and the Covenant University Centre for Research, Innovation and Discovery (CUCRID), Nigeria, for their support.

REFERENCES

[1] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "From conventional voting to blockchain voting: categorization of different voting mechanisms," in *2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI)*, Dhaka, Bangladesh, Dec. 2020, pp. 1–6, doi: 10.1109/STI50764.2020.9350399.

[2] R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for e-voting," *Symmetry*, vol. 12, no. 8, pp. 1–24, Aug. 2020, doi: 10.3390/sym12081328.

[3] W. Fan, H. J. Hong, X. Zhou, and S. Y. Chang, "A generic blockchain framework to secure decentralized applications," in *IEEE International Conference on Communications*, Montreal, QC, Canada, Jun. 2021, pp. 1–7, doi: 10.1109/ICC42927.2021.9500924.

[4] H. Yi, "Securing e-voting based on blockchain in P2P network," *Eurasip Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1-9, Dec. 2019, doi: 10.1186/s13638-019-1473-6.

[5] M. Ibrahim, K. Ravindran, H. Lee, O. Farooqui, and Q. H. Mahmoud, "ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication," in *Proceedings - 2021 IEEE 18th International Conference on Software Architecture Companion, ICSA-C 2021*, Stuttgart, Germany, Mar. 2021, pp. 123–129, doi: 10.1109/ICSA-C52384.2021.00033.

[6] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, "Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review," *IEEE Access*, vol. 10, pp. 70746–70759, 2022, doi: 10.1109/ACCESS.2022.3187688.

[7] E. Aljarrah, H. Elrehail, and B. Aababneh, "E-voting in Jordan: Assessing readiness and developing a system," *Computers in Human Behavior*, vol. 63, pp. 860–867, Oct. 2016, doi: 10.1016/j.chb.2016.05.076.

[8] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," in *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data,*

Blockchain, Computer and Information Technology, iThings/GreenCom/CPSCom/SmartData/Blockchain/CIT 2018, Halifax, NS, Canada, Jul. 2018, pp. 1561–1567, doi: 10.1109/Cybermatics_2018.2018.00262.

[9] U. C. Çabuk, E. Adıgüzel, and E. Karaarslan, "A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems," *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, vol. 7, no. 3, pp. 124–134, Mar. 2018, doi: 10.17148/ijarcce.2018.7324.

[10] M. T. Quasim, M. A. Khan, F. Algarni, A. Alharthy, and G. M. M. Alshmrani, "Blockchain Frameworks," in *Studies in Big Data*, vol. 71, pp. 75–89, 2020, doi: 10.1007/978-3-030-38677-1_4.

[11] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as a Decentralized Security Framework [Future Directions," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, Mar. 2018, doi: 10.1109/MCE.2017.2776459.

[12] F. Liu, S. He, Z. Li, and Z. Li, "An overview of blockchain efficient interaction technologies," *Frontiers in Blockchain*, vol. 6, Feb. 2023, doi: 10.3389/fbloc.2023.996070.

[13] A. Averin, V. Bogatyreva, and V. Degtyarev, "Review of e-voting systems based on blockchain technology," in *AIP Conference Proceedings*, vol. 2910, no. 1, p. 020032, 2023, doi: 10.1063/5.0167048.

[14] A. Gómez, C. Joubert, and J. Cabot, "Blockchain Technologies in the Design and Operation of Cyber-Physical Systems," in *Digital Transformation: Core Technologies and Emerging Topics from a Computer Science Perspective*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 223–243, 2023, doi: 10.1007/978-3-662-65004-2_9.

[15] S. Bukhari, K. Sharif, and L. Zhu, "Standardized Blockchain Structure using TLV-Encoding for Large-scale Interoperability," in *2024 6th International Conference on Blockchain Computing and Applications, BCCA 2024*, Dubai, United Arab Emirates, Nov. 2024, pp. 279–284, doi: 10.1109/BCCA62388.2024.10844490.

[16] S. Zhang, L. Wang, and H. Xiong, "Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability," *International Journal of Information Security*, vol. 19, no. 3, pp. 323–341, Jun. 2020, doi: 10.1007/s10207-019-00465-8.

[17] R. H. Sahib and E. S. A. Shamery, "A Review on Distributed Blockchain Technology for E-voting Systems," *Journal of Physics: Conference Series*, vol. 1804, no. 1, pp. 1-24, Feb. 2021, doi: 10.1088/1742-6596/1804/1/012050.

[18] A. S. Parihar, D. Prasad, A. S. Gautam, and S. K. Chakraborty, "Proposed End-to-End Automated E-Voting Through Blockchain Technology to Increase Voter's Turnout," in *Proceedings of International Conference on Machine Intelligence and Data Science Applications: MIDAS 2020*, 2021, doi: 10.1007/978-981-33-4087-9_5.

[19] S. Park, M. Specter, N. Narula, and R. L. Rivest, "Going from bad to worse: From Internet voting to blockchain voting," *Journal of Cybersecurity*, vol. 7, no. 1, Feb. 2021, doi: 10.1093/cybsec/tyaa025.

[20] R. Fatih, S. Arezki, and T. Gadi, "A Review of Blockchain-Based E-Voting Systems: Comparative Analysis and Findings," *International Journal of Interactive Mobile Technologies*, vol. 17, no. 23, pp. 49–67, Dec. 2023, doi: 10.3991/IJIM.V17I23.45257.

[21] S. S. Hossain, S. A. Arani, M. T. Rahman, T. Bhuiyan, D. Alam, and M. Zaman, "E-voting system using Blockchain technology," in *ACM International Conference Proceeding Series*, pp. 113–117, Dec. 2019, doi: 10.1145/3376044.3376062.

[22] N. El Madhoun, J. Hatin, and E. Bertin, "A decision tree for building IT applications: What to choose: blockchain or classical systems?," *Annales des Telecommunications/Annals of Telecommunications*, vol. 76, no. 3–4, pp. 131–144, Apr. 2021, doi: 10.1007/s12243-020-00814-y.

[23] O. F. Nebechi, "Biometric Information Management in Nigeria: A Case of National Identity Management Commission," *ESUT JOURNAL OF SOCIAL SCIENCES*, vol. 6, no. 2, pp. 1-17, 2021.

[24] A. S. Adewuyi, "Biometric registration, card readers and the integrity election in Nigeria," Dept. of Political Science, University of Ibadan, Apr. 2021.

[25] A. Fatai and L. I. Adisa, "The Use of Biometric Technology in the Success of the 2015 General Elections in Nigeria," *Politeia*, vol. 36, no. 2, Mar. 2018, doi: 10.25159/0256-8845/2861.

[26] I. Ayamba, "National Identity Management in Nigeria: Policy Dimensions and Implementation Okonette Ekanem," *International Journal of Humanities & Social Science Studies (IJHSSS) A Peer-Reviewed Bi-monthly Bi-lingual Research Journal*, vol. 3, no. 1, pp. 279–287, 2016.

[27] O. Enwe, "Understanding the Mandatory Use of National Identification Number in Nigeria", pp. 1-5, 2023. [Online]. Available: https://www.researchgate.net/publication/375963871.

[28] A. Fatai, T. O. Shittu, and M. Y. Zuberu, "E-Voting System and Biometric Technology: An Instrument of True Democracy in Nigeria," *Bilingual Journal of Multidisciplinary Studies (BJMS)*, vol. 3, pp. 91-102, 2017.

[29] R. Agbeyeke and A. Babalola, "Positive and Negative Aspects of Implementing Blockchain-based E-Voting Systems in Nigeria," *Reaserchgate*, pp. 1-9, 2023, doi: 10.13140/RG.2.2.13482.80325.

[30] M. Malkawi, M. B. Yassein, and A. Bataineh, "Blockchain based voting system for Jordan parliament elections," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 5, pp. 4325–4335, Oct. 2021, doi: 10.11591/ijece.v11i5.pp4325-4335.

[31] S. Singh and A. Sharma, "Blockchain-Based Elections: A Comprehensive Analysis," *Computer Science, Computing in Social Sciences, Arts and Humanities, Professions, Cyber Security, Blockchain Technologies*, 2023.

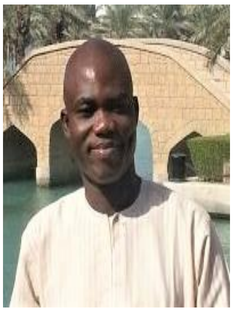
[32] A. R.-Pérez, P. V.-Montfort, and J. Cucurull, "Bringing transparency and trust to elections: Using blockchains for the transmission and tabulation of results," in *ACM International Conference Proceeding Series*, Apr. 2019, vol. Part F148155, pp. 46–55. doi: 10.1145/3326365.3326372.

[33] A. Mani, S. Patil, S. Sheth, and L. S. Kondaka, "College Election System using Blockchain," *ITM Web of Conferences*, vol. 44, p. 03005, May 2022, doi: 10.1051/itmconf/20224403005.

[34] R. Bulut, A. Kantarci, S. Keskin, and S. Bahtiyar, "Blockchain-Based Electronic Voting System for Elections in Turkey," in *UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering*, 2019, pp. 183–188, doi: 10.1109/UBMK.2019.8907102.

[35] F. Ikuero, V. Germanos, L. Brooks, and W. Zeng, "Is E-voting Systems based on Blockchain Technology Efficient in Nigeria General Elections?," *ICST Transactions on Security and Safety*, vol. 7, no. 25, pp. 1-12, Jun. 2021, doi: 10.4108/eai.10-3-2021.168964.

BIOGRAPHIES OF AUTHORS



Olabode Idowu-Bismark is a Senior Lecturer at the Department of Electrical and Information Engineering, Covenant University, Ota, Nigeria. He holds a B.Eng. degree in Electrical and Electronics Engineering from the University of Benin, Nigeria and a M.Sc. in Telecommunications Engineering from Birmingham University UK. He obtained his Ph.D. in Information and Communication Engineering from Covenant University. He has worked in various companies as an engineer, senior engineer, and technical manager. He is a Faculty Member of the Covenant Applied Informatics and Communication Africa Centre of Excellence (CApIC-ACE), and FEDGEN Cloud Computing Research Project (World Bank and AFD funded). He is a member of the Nigerian Society of Engineers, member, MIEEE, and a COREN Registered Engineer. His research interest is in the area of machine learning for mobile communication, mmwave communication, MIMO system, and OTFS for MIMO Communication. He has published many scientific papers in international peer-reviewed journals and conferences. He can be contacted at email: olabode.idowu-bismark@covenantuniversity.edu.ng and idowubismarkolabode@gmail.com.

Oluwadamilola Oshin received the Ph.D. degree in information and communication engineering (with a focus on nano-electronic biosensing) from Covenant University, Nigeria, in 2020. She is a Senior Lecturer of information and communication engineering with the Department of Electrical and Information Engineering, Covenant University. She is also a Faculty Member of the Covenant Applied Informatics and Communication Africa Centre of Excellence (CApIC-ACE), a World Bank ACE-IMPACT Centre, Covenant University. She has broad research experiences and interests including mobile communications, data analytics, artificial intelligence, and MEMS-based biosensing. She is professionally registered with the Council for the Regulation of Engineering in Nigeria (COREN) and is also a member of the Institute of Electrical and Electronics Engineers (IEEE). She enjoys teaching, research and solving health-related issues using engineering and technology. She can be contacted at email: damilola.adu@covenantuniversity.edu.ng.

Emmanuel Adetiba a member of IEEE received the Ph.D. degree in information and communication engineering from Covenant University, Ota, Nigeria. He was the Director of the Center for Systems and Information Services (aka ICT Center), Covenant University, from 2017 to 2019. He is the incumbent Deputy Director of the Covenant Applied Informatics and Communication Africa Centre of Excellence (CApIC-ACE) and a Co-PI of the FEDGEN Cloud Computing Research Project at the center (World Bank and AFD funded). He is the Founder and a Principal Investigator of the Advanced Signal Processing and Machine Intelligence Research (ASPMIR) Group. He is a full Professor and the former Head of the Department of Electrical and Information Engineering, Covenant University, from 2021 to 2023. His research interests and experiences include machine intelligence, software defined radio, cognitive radio, biomedical signal processing, and cloud and high performance computing (C&HPC). He is a registered engineer (R.Engr) with the Council for the Regulation of Engineering in Nigeria (COREN) and a member of the Institute of Information Technology Professional (IITP), South Africa. He can be contacted at email: emmanuel.adetiba@covenantuniversity.edu.ng.