Secured Electronic Voting System Using RSA Key Encapsulation Mechanism

B. O. Ahubele and Linda U. Oghenekaro

***Abstract* — A secured process whereas enumerating and casting of votes with the electronic aids with aim of improving the performance of electoral system is called E-voting (Electronic voting). Present e-voting mechanisms are faced with challenges such as confidentiality, integrity, verifiability, transparency, non-repudiation, and authenticity. In e-voting system, blockchain cryptography exists to protect voter's records. Encryption as well as decryption prevents forgery and other electoral malpractices by confirming voter's coherence and confidentiality. Rivest, Shamir, Adleman (RSA) is a crooked algorithm with trapdoor functionality which makes it difficult to factor a huge prime whole number as the product of multiplication into its component primes. RSA – Key Encapsulation Mechanism describes a hybrid encryption that makes use of unrelated keys for decryption and encryption along with a key derivation function. In this paper, a secured voting system using RSA Key Encapsulation Mechanism with two layers-Symmetric and Public key Layers was presented. RSA consist of three functions such as key generation, encryption, and decryption. In RSA-KEM, KDF3 built upon SHA-256, induction function is mainly for key generation. AES key wrap (Advanced-Encryption-Standard) provides key-wrapping functionality.**

***Key words* — Blockchain, Electronic Voting, Cryptography.**

I. INTRODUCTION

The major aim of a voting system is to enable individual vote counts therefore, in democratic societies, voting should be done with paramount effect of ensuring a transparent and a trusted election. Naturally, the probity of an election process is fundamental to the coherence of democracy. E-voting is an electronic means for vote casting and counting, unlike the conventional method that requires the usage of physical ballot papers to cast vote. Voting is carried out in a localized or distributed unit called polling booths. Before the day of election, the whole voting population is geographically splited to diverse polling booths of about 500 people capacity. Similarly, only each eligible voter within the age limit will be allowed to cast their votes under the inspection of delegated officers with party representatives. The conventional method comes with its challenges such as time wastage, ballot box snatching, lack of voter's privacy and manipulations of vote counts; are all caused by lack of proper administrator. New and more voting techniques have been created, thanks to engineers with incorruptible software and secured protocols. Similarly, technology introduced recent e-voting techniques [1], they are crucial and have caused various security threats to national sovereignty. However, the design of an electronic or paper ballot voting system must satisfy a number of criteria such as anonymity, integrity, confidentiality, transparency, non-repudiation and tamper-proof of a voter's ballot in order to guide against the activity of a fraudulent candidate. E-voting has enhanced accuracy than that of face-to-face physical polling; it has increased both integrity and sincerity [2]. E-voting is widely used due to its simplicity, cost of effectiveness and flexibility [3]. Notwithstanding, present E-voting methods like punch-cards, optical-scan, specialized v-kiosks and a Self-contained Direct-Recording-Electronic (DRE), are at risk of central authority and the unjust actions they could perform on data, voter's access, Individualized ballot processes [4], lack of fairness, privacy, anonymity, and lack of transparency and trust in the voting process. Recent procedures are controlled, measured, centralized by authority, which constitute a major challenge for a fair voting process. Alternatively, e-voting is well managed by an administrator which may give rise to an incorrect candidate selection due to the administrator's immorality [5]. The decentralized ledger network evolved as a contemporary e-voting procedure to avoid the problems it faces today. Blockchain is a distributed ledger technology that offers a decentralized node for electronic voting. Blockchain can be an appealing alternative to common e-voting mechanisms with characteristics such as decentralization, confidentiality, non-repudiation, immutability, security protection and authenticity. However, to update its data protection level and confidentiality of the E-voting, we look in the direction of cryptographic mechanisms with blockchain features to build a well-structured and well secured electronic voting system. The inclusion of blockchain technology to e-voting has introduced several security standards into the voting system. This disruptive technology marks the backbone of cyber information security. Information security entails protecting information system from unintended access, use, disclosure, modification, perusal, disruption etc. Cryptography is a field in computer information security technology that entails a secure method of transmitting personal information through open network communication channel. In an attempt to achieve a secured e-voting system, major security features to fulfill are confidentiality, non-repudiation, middleman interference, integrity, privacy and authentication.

This paper proposed a secure blockchain-based model with cryptographic technique for an e-voting system in democratic countries where emphasis is placed on conducting transparent, trusted, and fair elections. The proposed system also aimed at a secured e-voting system with distinct features

Submitted on March 03, 2022.
Published on April 26, 2022.
B. O. Ahubele, University of Port Harcourt, Nigeria.
(e-mail:betty_ahubele@uniport.edu.ng)
L. U. Oghenekaro, University of Port Harcourt, Nigeria.
(e-mail: linda.oghenekaro@uniport.edu.ng)

such as non-repudiation and integrity in registration and transmission of electoral data during the voting process.

II. Related Works

Aruna *et al*. [6] used SHA3 and Merkle Root cryptographic mechanisms to design a blockchain enabled electronic voting system. Besides, blockchain creation and sealing, the authors further developed an effective model for generating a block for every casted vote. The sealed blocks enabled vote counting for each candidate. However, the three cryptographic algorithms such as SHA3, RSA and Merkle Root used by the authors provided higher security to the e-voting system, but the proposed design could not be implemented to an architectural model for further clarification on the discussed issue.

Yacoubi *et al*. [7] presented a fair, smooth and cost-effective election process using decentralized network called blockchain. Although, the proposed algorithm provided users anonymity and vote outcome verification in real time but was unable to implement the proposed model on a distributed platform for optimization and creditability.

Olaniyi *et al* [8] presented an improved e-voting system that guarantees voters authentication and integrity using multifactor mechanism and cryptographic hash function. The study provided solution to two key security issues in secured electronic system such as voter's authentication and integrity of vote transmitted over insecure channels. Although, the issue of insecurity was resolved by enforcing both authentication and integrity measures, but the real identity of voters could not be captured using biometric system while including other e-voting security requirements such as non-repudiation, privacy, and confidentiality.

Fraij *et al*. [9] proposed blockchain e-voting platform. The proposed system was able to resolve e-voting security debates such as integrity, privacy, and transparency. The decentralized platform deprives voters from interference in the voting records, thereby eliminating corruption either from electoral representatives or voters in the entire process. However, the blockchain-based network provided a platform where authorities and governments who are in dare need for a voting system in which no internal or external political and/or governmental interference are available, but the proposed model implementation was limited to Ethereum blockchain than other blockchain platform.

Pawlak *et al*. [10] initiated an intelligent agent and multi-agents concept for an auditable blockchain-enabled e-voting system. The study was an integration of blockchain-based e-voting process into a direct non-remote E-voting system, that provides an end-to-end verifiability and increased the voting security through the reduction of its usage in the polling stations to the middle-point linking the voter and the agents, who will then have control of all tasks that has to do with the transmission and processing of votes. To achieve anonymity of agents, they will be distributed by nodes, and this would be easy to monitor any attempt to break into the e-voting system. The proposed system can be enhanced using Blockchain-based Smart Contract, which allows the carryout of contracts automatically without the involvement of third parties.

Pawar *et al*. [11] presented a secured blockchain-based voting system. The study provided a decentralized architecture for an open, fair, and verifiable voting scheme. The proposed model implemented a fundamental protocol which offered some degrees of delegation and allows voters to renovate their vote. Moreover, the experimental result showed that the designed model will be beneficial for the existing and upcoming voting system.

A. Blockchain Overview

Technology has impacted positively on diverse aspects of our academic and industrial lives. Besides, creating a 247 global connectivity with vast access to so many services and resources, the Internet had also provided a productive area for change. Blockchain is such disordering, which form the backbone of all cryptocurrencies [13]. Many of the existing services sees blockchain distributed ledger technology as a game changer which is taking the centre stage as a factor of equalization of the equality that exist between consumers and corporate/government. Owing to these characteristics of having a decentralized architecture and immutability property, the technology is promoting effectual solution to diverse issues in various fields for maximum input and potentials. Blockchain technology consists of distributed network of multiple nodes which are linked together by their cryptographic hash function. Each node on the blockchain, has their own copy of the ledger that contains records of all transactions that has ever existed within the network. Every blockchain block has a cryptographic hash function and timestamp, added to the previous block. In Fig. 1, no single control entity can order the network. Once the majority of the nodes reaches an agreement, based on a consensus mechanism (PoW or PoS), the transaction will be generally accepted and added to the distributed ledger. This network has the capability of providing users anonymity. Blockchain technology with smart contracts implementation provides e-voting reliability and transparency with end-to-end verifiability due to its decentralized nature. Application of blockchain technology in various fields such as Health, Food Supply Chain, Finance, voting etc. has become unavoidable, as this technology provides inherent benefits despite the involvement of other technologies. Blockchain has built a democratic society where members can decide the course of policy themselves, rather than relying on trusted electoral representatives. However, the rules of a political election may have to be changed to promote a transparent system, but blockchain provides an ideal platform for informing business decisions, guiding general meetings, polling, censuses etc., [14]. Specific advantages of blockchain-based electronic voting system include:

- higher transparency based on the openness and distributed nature of the ledger;
- voters' anonymity;
- enhanced security against DoS (Denial-of-Service) attacks;
- voters' reliability;
- voting integrity due to the immutable nature of the distributed ledger.

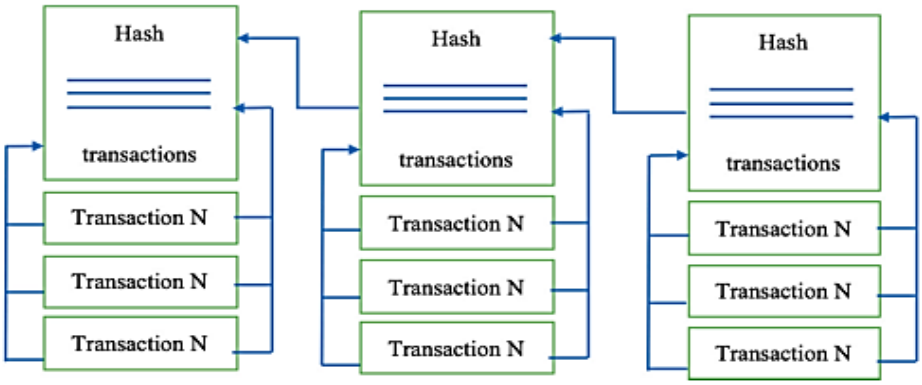

Fig. 1. The Blockchain Structure [4].

Existing works described improved electronic voting schemes with some strong guarantees based on the above listed requirements. However, this paper did not discuss Smart contract's implementation, challenges, and limitations at their current state for e-voting on blockchain platform to fully support a large-scale electronic system of voting. In this paper, we explore the possibility of using this same technology with Cryptographic mechanism to record and report votes in a bid to prevent many types of fraud possible in e-voting system.

III. Methodology

In this system, the blockchain-based distributed ledger network was used to store e-voting data in the form of blocks. Blocks in distributed platform are interconnected records which forms the chain of voting records, referred to as blockchain. In the proposed system, blockchain enhanced security in e-voting by creating different levels of trusted contracts such that if the higher authority allows voters data to get stored in blocks, then only it will be stored in the blockchain database. Stored data are immutable and cannot be tampered with by any malicious voter or electoral representative. The blocks contain information such as: voters Id, previous hash value, and timestamp. Each block consists of one transaction of blockchain, which will be broadcasted in the whole system once it has been verified by participating nodes. Whenever a new block is authenticated by the participating nodes, it is added to the chain of block, generating its hash value, which looks like a LinkedList. The Genesis block refers to the first block in the blockchain and has a hash value of zero. The next block contains the hash-value of the block before it, which makes up the chain of blocks or records called 'Blockchain'. It employs consensus protocol to prevent a third party from unauthorized access and knowledge during a communication process using cryptographic algorithms. In blockchain cryptography, we explore RSA-KEM (Rivest Shamir Adleman - Key Encapsulation Mechanism) to provide authentication and non-repudiation of electoral data/information during and after the election in order to guarantee an electoral result void of electoral malpractices and insecurity.

A. Proposed System

The proposed system is based on the ECC (Elliptic Curve Cryptography) e-voting approach identified in [11]. The system is **designed** to support a real-world implementation of an e-voting system with specific features such as voter's privacy, integrity, receipt freeness and verifiability. The designed model aimed to achieve a secured electronic voting by eliminating electoral malpractices present in the conventional system. In this paper, we used RSA-KEM (Rivest Shirma Adleman - Key Encapsulation Mechanism) to provide adequate security of voter's data and result count. RSA asymmetric algorithm is the first viable public key cryptography which is easier to implement than ECC, used in the present system. Key encapsulation mechanisms (KEMs) entail modern encryption techniques that utilizes public key algorithm to enhance security of private-key transmission over an insecure channel. The existing system [11] used ECC (Elliptic Curve Cryptography), which major limitation includes larger encrypted message size, increased complexity and tasking to carryout than RSA. This can result in errors (implementation errors), hence compromising the security of the algorithm. To control the limitation, cryptographers use hybrid coded schemes, like Integrated encrypted schemes and (KEM) Key Encapsulation Mechanism, that joins private key ciphers with asymmetric encryption to provide enhanced data security. Fig. 2 shows large file encrypted by combined symmetric crypto algorithm and public-key cryptography. A huge file such as Voter's data and vote counts can be encoded by combined symmetric crypto algorithm and public-key cryptography. The RSA-KEM provides a higher security by encoding an integer (z) with its receiver's public key and using a symmetric key wrapping scheme to encode voter's data. It has the following format:

a. Let z be an integer where z is within the range of 0 and *n*-1.
b. Using the recipient private key, encrypt z. This, $c=z^e \mod n$.
c. From the integer z, calculate KEK (encrypting key).
d. Applying KEK, get WK (i.e., warped keying data.
e. Lastly, the output c and WK is now termed the KEK (the encrypting keying data).

The RSA operation has no room for exploitations by unwanted means, hence providing a greater security assurance. The RSA input is an integer (z) between 0 and n-1, where n is regarded as the RSA modulo. However, the input is free of the voter's data, therefore the result of the RSA is unavailable to any form of adversary. The algorithm is "tight" security proof. Voters are registered in the pooling both using their various Ids; the details are encrypted and uploaded on the blockchain network. Each voter's credentials comprise a block of record that must be verified by

participating node before being added to other blocks (Voter's record) on the blockchain. Each current block is made up of the timestamp, hash of the previous block and the new hash. The generated Id with the encrypted file will be communicated with the public key to the administrator. Eligibility of voters is determined by their registration status on the blockchain. The data of the registered voters will be well managed on the blockchain network. It will be able to detect fraud voters and discards their votes. The voter generates link wallet address to send and receive the tokens generated by the system. The voter sends his vote with the generated wallet address, such that the vote will be considered not anonymous if the voter refuses to use the wallet-address for sending their votes. The wallet address guarantees that the voter receives the vote token, which is redirected to the candidate wallet in the subsequent step. The encrypted result of the election will be uploaded on the internet, which is made available to anyone to access the outcome of the electoral process.

Fig. 2. KEM Cryptography (https://cryptobook.nakov.com/).

B. *Architecture of the Proposed System*

The proposed system architecture is made up of two layers encryption algorithms: Symmetric and Public Key Encryption as shown in Fig. 3 (a, b). The RSA-KEM algorithm is a one-way forward mechanism that uses receiver's RSA asymmetric key for sending keying data to a receiver. The RSA-KEM provides an enhance security by encoding an integer with the receiver's public key, and then making use of a private key-wrapping scheme to encode the (Voting records) keying data. The RSA-Key Encapsulation Mechanism produces a different key and uniform algorithm which provides integrity protection. Layers are independent and symmetric keys are unrelated as symmetric methods avoid mathematical properties. Key encapsulation denotes an easy cryptography public-key positioning. The proposed system architecture consists of key-derivation basis, key wrapping, and length scheme.

C. *Proposed Algorithm*

The proposed system algorithm includes the following:

i. RSA for encapsulation

Encode using public key pairs (n, e):

- $r \leftarrow_R [0, n-1]$
- $C_0 \leftarrow r^e \bmod n$
- $W \leftarrow KDF(r)$

Decode using private key pairs (n, d)

- $r \leftarrow C_0^d \bmod n$
- $W \leftarrow KDF(r)$

❖ Encapsulate using KEM

1. Compute an integer value (z) such that z lies between (0 ≤ z ≤ n-1).

z = Random Integer (0, n-1)

2. Encode the integer (z), using the receiver's public key pairs (n,e).

Such that c = ze mod n.

3. Applying the key derivation function, that is, KEK = KDF (z, kekLen), obtain a KEK of length kekLen bytes.

4. Transform K with the KEK from the key-wrapping scheme (AES Key Warp) to get the result WK (i.e., WK = Wrap (KEK, K)

5. To get EK (EK = C || WK), Concatenate C (the ciphertext) and the WK.

6. Finally, the resulting output is EK (the encrypting data).

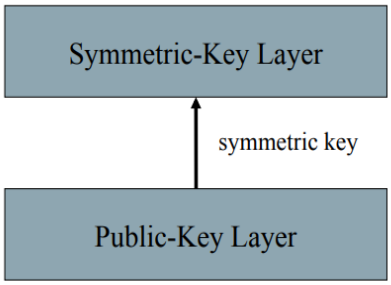

Fig. 3a. Two Layers Encryption Algorithm.

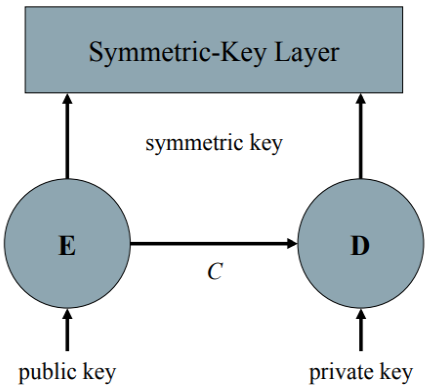

Fig. 3b. Two Layers with KEM.

D. *KEM Algorithm in Secured Voting System*

KEM is a triple of algorithms with input and output security parameters such as 1λ and a public/private key-pair (pk, sk) respectively.

KEM cryptographic 4-tuple algorithms (KEM.Setup, KEM.Gen, KEM.Enc, KEM.Dec) are formally defined below:

• KEM.Setup(1^n): takes as input and output the security parameter, n ∈ N and the public parameter pp respectively.

However, pp is generally assumed to be taken by all other algorithms as input except for KEM.Gen algorithm where it is explicitly given.

• KEM.Gen(pp): takes pp as input parameters and gives the key pair (pk, sk) as output.

• KEM.Enc(pk): the public key pair becomes the input, giving outputs as (K, ψ) such that:

- K = session key and
- ψ = ciphertext.

• KEM.Dec(sk, ψ): takes the secret key (sk) and ciphertext (ψ) as inputs, generating the session key K or ⊥ as outputs.

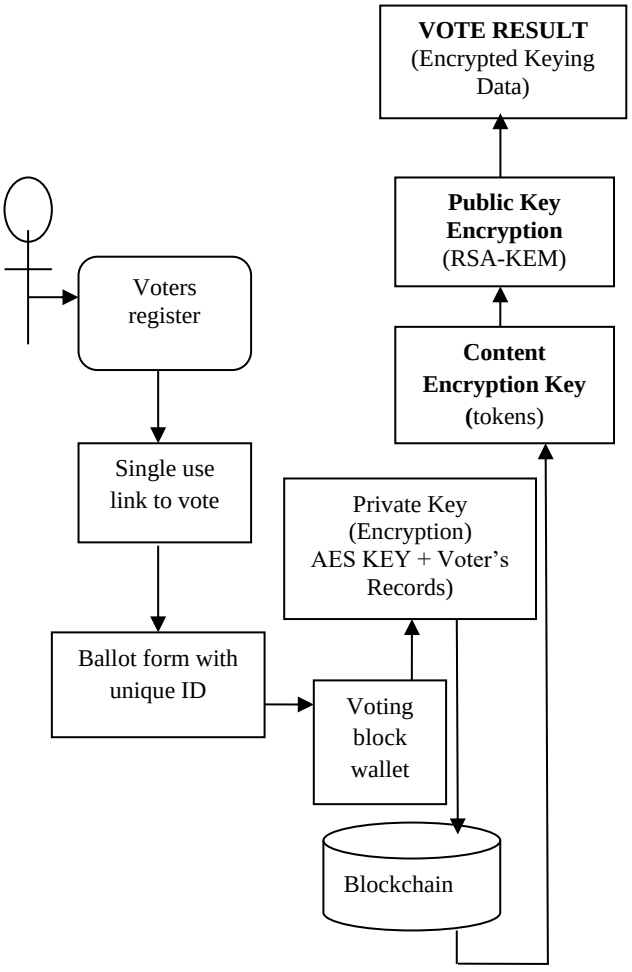

Fig. 3c. Architecture of the proposed system.

functionecdh_encapsulate (recipient Public Key):
variable (Ephemeral Secret, Ephemeral Public) = Generate Key Pair (Receiver's Public Key.curve);
varshared Secret = ecdh(ephemeralSecret, recipient Public Key);
varies Key = sha256(shared Secret || ephemeral Public); // NB "||" is concatenation
return (aes Key, ephemeral Public);
functionecdh_decapsulate (ephemeral Public, recipient Private Key):
varshared Secret = ecdh(recipient Private Key, ephemeral Public);
return sha256(shared Secret || ephemeral Public);
Decrypt (sk, σ):
(E, C) ← σ.
K ← Decapsul(sk, E, C).
m ← DecK(C).
Return (m).
Keys(1k):
(sk, pk) R← Key(1k).
Return key pairs(sk, pk).

E. Block Diagram of Blockchain and Cryptograph in Voting System Mechanisms

A key encapsulation mechanism (KEM) is a cryptographic primitive used to transport a symmetric key to a designated party in a public-key infrastructure.

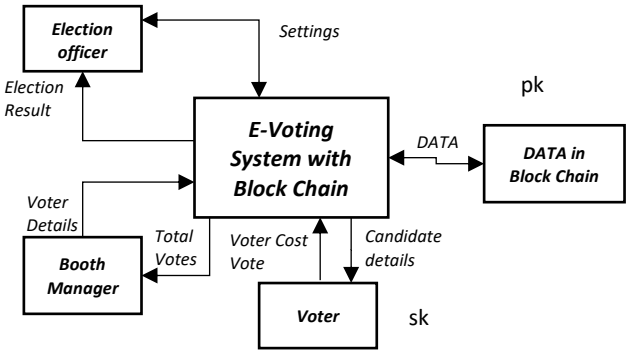

Fig. 4. Block Diagram Mechanism.

F. Flowchart of the Proposed System

The blockchain transaction consists of voter's record, electoral candidates, and the results of the election process. The voters cast their votes using their unique address (ID), a token will be generated which consists of voter's identification number, voter's information, and previous hash-value. Firstly, the user registers on the blockchain, a token is created. The participating nodes confirm the token wallet, if agreed by over 51% of the participating nodes, the voter is allowed to select the party to vote, else denied proceeding. Thereafter, the voter's private key (pk) is verified and finally vote casted. This method will ensure the uniqueness of each transaction using ken private key and KEM algorithm.

G. Advantages of the Proposed System

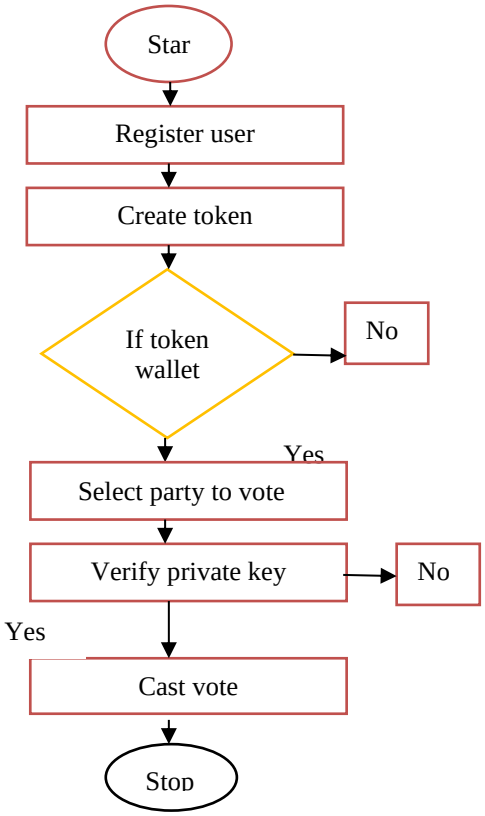

Fig. 5. Flowchart Diagram of the Proposed System.

The proposed system provides the following advantages of higher security assurance because:

(a) rather than the RSA modulus' size, the symmetric key-wrapping scheme bounds the keying data length.

(b) The public key and secret-key both have different operations on the keying data; therefore, it is an architecturally convenient approach.

(c) RSA operation input is free of the keying data and considered a random integer (0 and n-1), whereas n represents the RSA modulus which makes it impossible for exploitation by any rival.

(d) Unlike various padding schemes like PKCS #1v1.5 with less security since the input is dependent on the keying data. The RSA decryption operation output is not directly accessible by any adversary; hence the algorithm is highly secured

IV. Results and Discussion

The distributed ledger technology was used to implement an electronic voting system where user's credentials are recorded as blocks on the blockchain network. Application of cryptographic algorithm in electronic voting enables voters to distribute their voting rights to the election committee. Besides, the system will encrypt the election results using AES (Advanced Encryption Standard), a symmetric key and then converts the data and the private key with RSA algorithm where the public key pair (e,n) of the receiver (electoral committee) is sent to the sender. The message (m) must be an integer value (0,n-1). The encryption process is described as 'c', such that $c=m^d \bmod n$. Thereafter, the results of the election will be encoded, c, to the committee. To gain access to the encrypted message (decryption), the receiver uses a private key by decrypting the c, cipher text, the receiver uses his own private key (pk), d (decryption exponent) and modulo, n. Consequently, $m=c^d \bmod n$, which will give the plaintext.

In this paper we implemented a secure online voting system with RSA Key Encapsulation Mechanism for encryption and decryption employed in voter's registration phase and also for securing voter's vote. The proposed algorithm is more secured than the existing RSA algorithm. The RSA cryptosystem is the world's most commonly used public key cryptography algorithm. It can be used to encode a message which doesn't require the exchanging of a nondescript key separately While KEM key transport algorithm encodes different numbers using the receiver's public (general) key, and then the keying data is encrypted by a symmetric key wrapping scheme. KEMs are a hybrid of encryption algorithms proven to be most effective than other algorithm in data encryption and decryption. With the rigid architecture of blockchain, properly applied in the electronic voting platform, the debate surrounding the voting process could be reduced remarkably. However, the addition of blockchain which is the core architecture of cryptography protects the necessary information of both the candidates results and its voters.

A. Evaluation of the Proposed System

Several cryptographic algorithms have been utilized in securing electronic voting, however, the challenge of confidentiality, non-repudiation and highly secured voting process still persists. Consequently, the present electronic voting system employed only the public key cryptography which uses the ECC (Elliptic Curve Cryptography). Challenges with the existing Systems are Lack of an architectural model: Present system lack an architectural model for e-voting implementation using Blockchain. Message length (M) could be limited; Encryption cannot guarantee message integrity and mathematical properties. Message encryption may be related. However, message padding was employed to tackle these limitations, but new innovations for RSA are less than idea. PKCS#1 v1. 5 padding is ad hoc, and still does not guarantee e-voting data integrity. The proposed system handles the above limitation of the existing system by modeling RSA, and other PKC, no message length limitation, providing voters integrity protection and unrelated properties of Symmetric keys. Key Encapsulation Mechanism emerges to eliminate cryptography padding which could be clumsy using public key cryptography (ECC). The message is encrypted, and the AES Cryptographic key is generated, the Key is encrypted with RSA (Rivest Shamir Adleman), yielding the Data Encryption Mechanism (encrypted content with the symmetric key) RSA Key Encapsulation Mechanism (KEM) algorithm is used for vigorous security in transmitting the data or information over an unsecured channel. In electoral voting process, voter's credentials are encrypted and also the voters result encrypted using this technique.

V. Conclusion

Blockchain is an evolving technology that has been applied as smart contracts in various fields such as insurance, supply chain, land mortgage, education, air ticket reservation, virtual banking, hospital records etc., due to its end-to-end verifiability. Blockchain technology has the capacity to improve electronic voting and tackle the two major prevalent problems in voting such as voter's access and voter's fraud. In addition to the benefits derivable from conducting electoral process using blockchain technology, cryptographic techniques are employed to encrypt votes, digital ballot boxes, verify voter's identity, protect the secrecy of stored votes and assist in electoral process result auditing and tallying.

Several cryptographic algorithms exist to provide secure e-voting system using a blockchain platform [12]. No votes are tampered in the system; else, it will detect the tampered votes and resolve it. We developed a blockchain model using cryptographic technique for secure voting system that portrays voter's confidentiality and voting authenticity so that the populace benefits democratically from an effective election process. The proposed RSA-KEM algorithm encrypts voter's credentials using a symmetric key and also encrypts both the key and the ballot form with a public key, to ensure that no votes are tempered with during communication until the broadcast of the result of the election on the blockchain nodes. A non-blockhain user can access the election result once uploaded on the website by the electoral officers, all the information about the e-voting system is highly secured on the blockchain through the Proof-of-Work

(PoW) or Proof-of-Stake (PoS) consensus mechanisms. Although, RSA Key Encapsulation Mechanism, is a highly efficient and secure cryptographic technique but limited to protection against quantum computer attacks. Therefore, blockchain with counter measures to computer attacks should be future researched.

REFERENCES

[1] Hang L, Kim D.H. Design and implementation of an integrated Iot blockchain platform for sensing data integrity, 2019.
[2] Chang, VP, Baudier H, Zhang Q, Xu J, Zhang, Arami M. How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees. *Technol. Forecast. Soc*., 2020.
[3] Wang B, Sun J, He Y, Peng D,Lu N. Large-scale election based on blockchain. *ProcediaComput. Sci*., 2018. 129; 234–237.
[4] Jafar U, Juzaidden M, Aziz A, Shukur Z. Blockchain for Electronic Voting System: Review and OpenResearch Challenges, 2021; Retrieved 29/01/22. www.mdpi.com
[5] Lahane AA, Patel J, Pathan T. Potdar P. Blockchain technology based e-voting system. *ITM Web of Conferences 32, 03001. ICACC 2020.*
[6] Aruna S, Maheswari M, Saranya A. Highly Secured Blockchain Based Electronic voting system using SHA and Merkle Root. *IOP Conference Series: Materials Science & Technology*, 2020; 993(2020): 1-10.
[7] Yacoubi A, Erraha B, Asri H. An electronic voting system adopting Blockchain. *Interpretation characteristics and Investigation. E38 Web of Conference, 297,* ICSSRE'2021. 1-4.
[8] Olaniyi OM, Arulogun O, Omidiora EO. Design of Secure Electronic Voting System using Multifactor Authentication and Cryptographic Hash Functions. *International Journal of Computer and Information Technology*, 2013; 2(6): 1122-1130.
[9] Fraij, J, Aldabbas A, Aburumman N. Blockchain as An E-Voting tool. *International journal of Advanced Research (IJAR),* 2021; 8(12): 858-866.
[10] Pawlak M, Poniszewaska-Maranda A, Kryvinska N. Towards the Intelligent Agents for Blockchain e-voting system. 9th International Conference on Emerging Ubiuitous Systems and Pervasive Networks (EUSPN 2018). *Procedia Computer Science*, 141(2018): 239-246.
[11] Pawar D, Sarode P, Nimbalkar PP. Implementation of Secure Voting System Blockchain. *International Journal of Engineering Research & Technology (IJERT)*, 2020; 9(6): 1595-1598.
[12] Haibo Y. Securing e-voting based on Blockchain in P2P Network. *EURASIP Journal on Wireless Communications and Networking*, 2019;137.
[13] Harwick FS, Gioulis A, Akram RN, Markantonakis K. E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. ISG-SCC, Royal Holloway, University of London, Egham, United Kingdom, 2015;1-7.
[14] Liebkind J How Blockchain Technology Can Prevent Voter Fraud. Retrieved 26/01/2022). https://www.investopedia.com/news/how-blockchain-technology-can-prevent-voter-fraud/.

Betty Osamegbe Ahubele was born in Lagos State, Nigeria, on the 16th of October 1981. She received a Bachelor Degree in Computer Science from Ambrose Alli University (AAU), Edo State, Nigeria, in the year 2005 and finished as the best graduated student of the department. She obtained her M.Sc (Computer Science) from University of Port-Harcourt, Rivers State, Nigeria, in the year 2012. She also received her Ph.D degree in Computer Science from University of Port-Harcourt, Rivers State, Nigeria, in the year 2021. She is equipped with an extraordinary caliber and appreciable academic potency.

She has about 8 years of experience in teaching. Her research interest includes Cloud Computing, Cryptography and Blockchain Technology. She has published over 5 papers in various International Journals.

Dr. B.O. Ahubele is a member of Nigeria Computer Society (NCS).

Linda Uchenna Oghenekaro is a lecturer and researcher in the Department of Computer Science at the University of Port Harcourt, Nigeria. She obtained her undergraduate degree in Computer Science from the University of Port Harcourt in 2009 and finished as the best graduated female student of the Department. In 2012, she joined the UBA Group where she managed their business processes and supported their online applications. In 2014, she returned to academia, as a graduate assistant, and while working, she started her graduate program. Linda has a PhD in the Department of Computer Science. Her area of research includes Process Mining, Artificial Intelligence, Data Science and Machine Learning Algorithms. Her current area of research involves mining business processes using various machine learning tools and techniques. She has to her credit several articles published in peer-reviewed journals and conference proceedings. Presently, she is the Treasurer of the Organization for Women in Science for the Developing World (OWSD), UNIPORT Chapter where she has continually demonstrated good leadership and accountability. She is also a member of Nigeria IEEE Computer Society, Nigeria Computer Society (NCS) and Computer Professional of Nigeria (CPN).