Performance Evaluation Of Cloud Based Elliptic Curve Cryptographic Digital Signature E-Voting System For The Conduct Of Election In Nigeria

Akingbesote. A.O., Babatobi, F.J. & Akinwumi, D. A.
Department of Computer Science
Adekunle Ajasin University
Akungba-Akoko, Ondo State, Nigeria.
E-mails: oluwamodimu2012@gmail.com; prudent4la@gmail.com; david.akinwumi@aaua.edu.ng

ABSTRACT

Elections in Nigeria are characterized with poor voters' turnout. One of the reasons attributed to this is the insecurity of the votes of the electorates. To resolve this, scholars have adopted various mechanisms and technologies, for example, the use of Rivest-Shamir-Adleman (RSA), Advanced Encryption StandardAES) and Elliptic Curves Cryptography (ECC). While these have added value to the body of knowledge in the conduct of elections in Nigeria, However, literature reveals that issue of insecurity of votes of electorate is still a current debate. The reason attributed to this, is due to the poor performance in terms of their key size, key strength and encryption time. This is addressed by using a Cloud based Elliptic Curve Cryptographic Digital signature (ECCDS) E-Voting system. The concept of the proposed system is to automatically encrypts, signs, decrypts votes and verifies the signed votes. The system is built on a hybridized security algorithms, these are; The ECC and Digital Signature Algorithm. This has a smart contractor that protect electorate votes against integrity modification in the cloud environment. The prototype demonstration is conducted during the students' union election in Adekunle Ajasin University where the University ICT department is used as the cloud based network Infrastructure center. Three evaluation metrics are used. These are the key size, key strength and encryption time. The evaluation metrics shows a better performance of RSA, AES and ECC systems over the ECCD when considering the encryption time. The ECC and AES also perform better using the key size. For example, we recorded 167 bits for ECCDS, while RSA, AES and ECC algorithms recorded 163, 1024 and 64 bits respectively from one of the experiments under the key size. However, the beauty and the strength of good security system is the decryption time which is the key strength. From the experiment conducted using Key strength as the metric, we observed that ECCDS key strength is higher than that of AES, ECC and RSA. It means that it will take longer time for any intruder to decrypt the system when using the ECCDS model. This satisfy both the electorates and Electoral commission request and is very reliable and produces effective results.

Keywords: E-voting, Integrity, Elliptic Curve, Cryptography, Digital Signature.

CISDI Journal Reference Format
Akingbesote. A.O., Babatobi, F.J. & Akinwumi, D. A. (2023): Performance Evaluation Of Cloud Based Elliptic Curve Cryptographic Digital Signature E-Voting System For The Conduct Of Election In Nigeria. Computing, Information Systems, Development Informatics &Allied Research Journal. Vol 14 No 3, Pp 1-.14. Availableonlineathttps://www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V14N3P1

1. INTRODUCTION

Election started in Nigeria in 1959. This was supervised by the British colonial rule that ushered in the political independence and brought in several parties, for example, National Council for Nigerian and Cameroons (NCNC), Northern People's Congress (NPC) and Action Group (AG). However, real electoral or democratic journey started in 1964 after achieving the status of a republic in 1963.

Since that time till 2013 the outcome of elections have been considered to be massively rigged, violence, murdered in cold-blood of innocent citizens and wanton pattern of killings (Awopeju, 2011). In a democracy, voting is the method by which the electorate appoints its representatives to government. In a direct democracy setting, voting is the method by which the electorates directly make decisions in order to turn bills into laws (Olaniyi *et al*., 2013). This implies that democracy must be a system of government where the people dictate the pace with the general consent of the governed. While most developed and developing countries are working hard towards perfection of their electioneering and electoral processes, it is quite unfortunate that Nigeria elections have so far thwarted the foundation upon which democracy is built (Olaniyi *et al*., 2016). The table below depicted the technologies and other details used in Nigeria election process since 1999 to 2013.

Table 1: Election Process in Nigeria 1999-2016

S/NO	YEAR	VOTER REGISTRATION	DAYS FOR REGISTRATION	DATA CAPTURE	D-BASE	ACCREDITATION/ VOTING	RESULT COLLATION
1	19991	Spread-Sheet and Type writers	14days	Basic details, no picture or finger print	Nil	Nil	Nil
2	2003	Optical Magnetic Recognition Form (OMR Form) Automated Finger Prints Identification System (AFIS)	10days	Basic details, and finger print	Yes	Nil	Nil
3	2007	Direct Data Capture Machine (DDCM)	4 Month	Basic details, Photograph and finger print	Yes	Electronic Voters' Register (EVR)	Excel Sheet / E-mail
4	2011	Direct Data Capture Machine (DDCM)	21days	Basic details, Photograph and finger print	Yes	Electronic Voters' Register (EVR)	Excel Sheet / E-mail
5	2015	Direct Data Capture Machine (DDCM) Improved AFIS Business Rule	Continuous Voter Registration (CVR)	Basic details, Photograph and finger print	Yes	EVR INEC Voters Authentication System (IVAS/Smart Card Reader SCR)	Election Transparency Administration and Collation (E-TRAC)
6	2016	DDCM Improved AFIS Business Rule	Continuous Voter Registration (CVR)	Basic details, Photograph and finger print	Yes	EVR IVAS	Electronic Collation Support (E-Collation E-TRAC)

Source: Toba Ayeni, (2018)

To address this, researchers for example, Agbu *et al.,* 2015 and Esan *et al.,* 2017 agreed that the use of ICT in election process has eliminated the incidents of multiple registrations, which had been one of the main political tools for rigging elections by unscrupulous and savage elements. Despite the introduction of this technology, it is still facing some challenges. These include riggings, double voting, cancellations, and hijacked ballot boxes (Bulut *et al*., 2019). Despite the adoption of partial E-voting system coupled with the huge amount spent in Nigeria Electioneering process, the 2019 general election has been characterized with bloodshed, vote inflation, vote deflation, the issue of vote buying, vote selling, infant voting and illegal possession of ballot boxes. In addition, there were cases of insufficient and inefficient Smart Card Reader (SCR) that led to sluggish process of voters' accreditation (Johnson, 2019). The reason attributed to this is the lack of goods information storage and security infrastructure on ground. For example, the issue of inadequate cloud infrastructure with good security architecture.

That implies that a free and fair election is achievable with a suitable cloud based e-voting application with high level of data security and services in place as reported in (Arthur *et al.,* 2021). To further address this, scholars Olaniyi *et al.* (2015), Chalabi *et al.* (2015), Abdul *et al.* (2018), Khan *et al.* (2020) and Ali *et al.* (2022)" have adopted various mechanisms and technologies, for example, the use of RSA, AES and ECC. While all these authors have added value to the body of knowledge in the conduct of election, however, literature reveals that the issue of insecurity of votes of electorate is still a current debate. The reason attributed to this is due to the fact that some metrics like their key size, key strength and encryption time were not used and where they were used, poor performance were recorded. This paper addresses these challenges by evaluating the performance of our design Cloud Based Elliptic Curve Cryptography Digital Signature (ECCDS) e-voting security system for election in Nigeria. The remainder of this paper is organized as follows. Section 2 contains review of related existing research works. The design of the ECCDS E-Voting Framework is reported in section 3, while section 4 contains a vivid description of the experimental set up, results and findings of the experiment conducted. Section 5 presents performance evaluation of the system. Section 6 contains the conclusions.

2. RELATED WORKS

Researchers have put forward several algorithms to secure cloud information especially in the area of cloud based e-voting system. For example, Koluguri *et al.* (2014) developed a receipt free multi –authority e-voting scheme based on the virtual voting booth with smart card. The focus of the authors was to solve the problems of universal verifiability, coercion, bribery and fairness in the overall election process. This was achieved by distributing the voting procedure between the voter and the smart card. The voter and the smart card jointly contributed randomly for the encryption of the ballot. However, this system must assume that the briber or the coercer does not monitor voter when voting. In Olaniyi *et al.* (2015), the authors developed an enhanced stegano-cryptographic model for secure electronic voting system. This was achieved through the use of modified stegano-cryptographic model using Elliptic curve algorithm. The authors' performance metrics were based on availability, authenticity, privacy, confidentiality and accuracy. The results showed a better performance under the used metrics.

However, the issue of coercibility of voters and bribery are great challenges. The work of Chalabi *et al.* (2015 proposed a new multi-authority electronic voting scheme based on elliptic curves. The authors was motivated based on some of the existing voting schemes which were developed on discrete logarithm problem where the parameters involved in the scheme chosen are similar to those in Digital Signature Algorithm (DSA). Thus, these voting schemes require larger keys to offer higher security. According to the scheme, each voter casts their vote as a point on the elliptic curve and the final tally is computed with the assistance of multiple authorities. The proposed scheme meets the essential requirements of e-voting system.

Ultimately, the proposed voting scheme fortifies the security properties of the electronic voting procedure, since the secrecy of the particularized vote is preserved by ElGamal cryptosystem and Elliptic curve discrete logarithm. The issue of delay in the computation of final tally of the electorate votes is a great challenge of this work. This gives hacker more chances to break in to the system. This work was extended in (Olaniyi *et al*., 2016) to address the issue of coercibility of voters and bribery. However, the model has issue with time delay during voters' authentication process. The outcome of the experiment showed that voter will have to wait to receive a one-time-password (OTP) via Short Message Service (SMS), also the issue of post-election auditing was not considered. In Olayemi *et al.* (2016), the authors developed e-voting model using unimodal fingerprint biometrics with Advanced Encryption Standard and Wavelet based on Crypto-watermarking approach. The idea of the work was to eradicate the conventional voting scheme that employs paper-based ballot to verify votes.

In addition the work was to checkmate the insecurity due to issues like ballot stuffing, ballot snatching and voter's impersonation. This was achieved by solving the blundering voter's authentication and the confidentiality of vote stored in the server. The results after qualitative evaluation of the system with anti-watermarking detectors revealed that the developed secure e-voting system could serve as a platform for the delivery of credible e-election in developing countries with significant digital devices. However, how this work could be enhanced to solve other security issues like non-repudiation and data integrity is left as an open discussion. Also, how the system could be embedded with post-electoral ballot verification and aversion of vote coercion as well as vote selling prior to voting exercise were left as future work.

In the work of Olayemi *et al.* (2017), the Authors design a Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach. The system was built on the existing e-voting scheme that is insecure due to the attributed shortcomings, including ballot stuffing, ballot snatching and voter's impersonation. A secure e-voting system to ensure a free, fair and credible election, where the preference of electorate counts was developed. The system solves the possibility of blundering voter's authentication and confidentiality of vote stored in the server on e-voting scenarios using unimodal fingerprint biometrics and Advanced Encryption Standard based Wavelet based Crypto-watermarking approach. Though, the authors adjudged that the system can be enhanced to solve other security issues like non-repudiation and non-coercibilit.

This is because the fingerprint template database can be compromised by coercion and repudiation process. Abdul *et al.* (2018) designed a Novel Blind Signcryption Scheme for E-Voting System Based on Elliptic Curves (ECC) based on El-Gamal and the Rivest-Shamir-Adleman (RSA) cryptosystems which are not only expensive approache but also lack the security features like unlink ability and forward secrecy. The scheme used a low-cost elliptic curve cryptosystem with 160 bits key as compared to El-Gamal 2048 bits key and RSA 1024 bits key. In the scheme, signer signs the message blindly without knowing the original contents then the voter forward signcrypted vote to polling server. The polling server is the actual voter data verifier or validator. The polling server checks the validity/authenticity of the voter and has the right to accept or reject the vote.

The scheme offers forward secrecy, unlinkability, and non-repudiation in addition to the basic confidentiality and authenticity. However, the work did not cater for vote integrity and unforgeability. Tohari *et al.* (2019 developed Efficient Mobile Voting System Security Scheme Based on Elliptic Curve Cryptography**.** The authors presented a novel mix-type remote voting system that permits verifying the correctness of a voting process without requiring complex and costly zero-knowledge proofs. However, the authors concluded that, the system needed more security tools to withstand vulnerability to packet sniffing, key logging attacks, brute force attack and the verification process still takes longer time. Khan *et al.* (2020) developed secure digital voting system based on Blockchain Technology.

The research aimed to improve the overall resilience of e-voting systems by designed scheme conforms to the fundamental requirements for e-voting schemes. The authors described the details of the e-voting scheme along with its implementation using Multichain platform and presented in-depth evaluation of the scheme which successfully demonstrates its effectiveness to achieve an end-to-end verifiable e-voting scheme. However, the developed scheme will work upon and focus on improving the resistance of blockchain technology to 'double spending' problem which will translate as 'double voting' for e-voting systems. In Arthur *et al.* (2021), the authors presented a Cloud based e-voting system using Information Dispersal Algorithm (IDA). The goal was to improve on the existing schemes that is devoid of security breaches especially from hacking, hijacking and others malicious activities. These challenges call for noble designs into high level security infrastructure that will enhance and improved the security of e-voting system, in order to gain the full trust, acceptance and adoption of e-voting system by citizenry in a democratic setting. In the IDA approach, upon voting, the voters vote record is encrypted and split for distribution on several virtual cloud servers. At the end of the voting period, the split vote records are reassembled into their original state for counting to take place. The system represents the voters vote record in a secured manner that could not be easily accessed by hacks and exploitation while the voting process is on- going.

Transparency and trust are improved by given opportunity to the party representatives to invoke a key before and after voting process which imply the voting process only starts when all parties are satisfied with all contingencies of the software. However, the authors raised a need to improve the system to combat Intrusions breaches and Identity theft to help identify and thwart possible intrusions. Ali *et al.* (2022 proposed an efficient electronic voting system in a cloud computing environment using ECC, In this work, electronic voting system based on Homomorphic encryption to ensure privacy, confidentiality and integrity of the electorates vote in the cloud environment was presented. The system offers all the advantages of the additively homomorphic encryption cryptosystems. To further add value to body of knowledge, the use of biometric and digital signature authentication processes so as to make it harder for the malicious to compromise the system was proposed by the authors.

We appreciate these scholars for their contributions. However, the shortcomings we observed have given us the insight into making our contribution. For example, most frameworks and the developed models used confidentiality and authentication as their metrics. However, we have other metrics that are also important. Even the used metrics are still porous to various security attacks. Some of these were built using encryption algorithm, cryptography, digital signature and steganography schemes as acknowledge by in Zhao *et al.,* 2014, Mohan *et al.,* 2014 and Khan *et al.,* 2020, Not only that, the INEC chairman in person of Prof. Mahmood Yakubu as reported in the Nigeria Nation newspaper of September 10, 2022 acknowledged that the 2022 Ekiti and Osun were hijacked by hackers but they were unable to succeed. In addition, the 2023 election was not acceptable to some political parties because the results were not transmitted to the cloud as proposed by INEC, The reason attributed to this is due to the fact that some of the importance metrics like key size, key strength and encryption time were not used and where they were used, poor performance were recorded. This paper addresses these challenges by evaluating the performance of our designed Cloud Based ECCDS e-voting security system for Nigeria elections.

3. ARCHITECTURAL DESIGN OF THE ECCDS SYSTEM

The Architecture comprises of three components. The first is the Elliptic Curves Cryptography (ECC), the second is the security of DSA and the third component is the Smart contractor. The Elliptic curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory. It is used to create faster, smaller, and more efficient cryptographic keys. In addition, ECC is among the most commonly used implementation techniques for digital signatures in crypto-currencies. It generate keys through the properties of the elliptic curve equation as shown in Figure 2. This is given as:

$$ax^2 + bxy + cy + dx + ey + f = 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. (1)$$

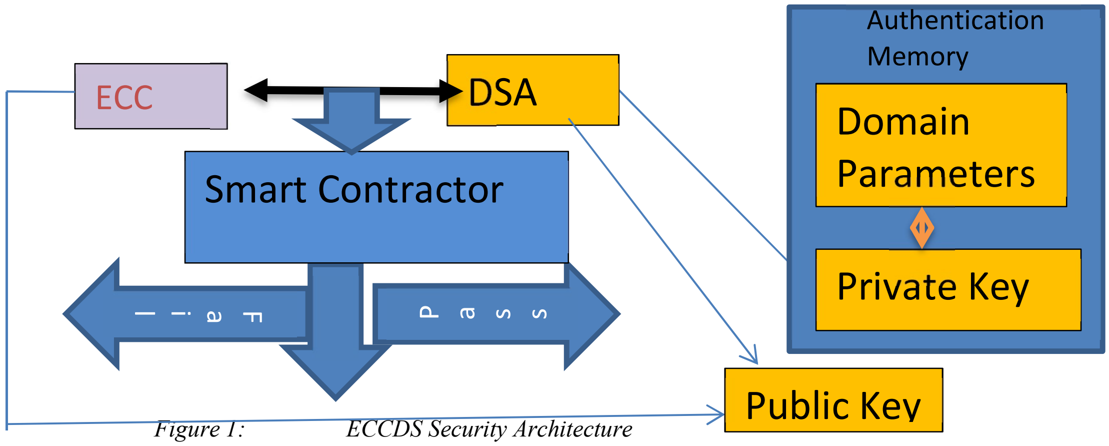

Figure 1: ECCDS Security Architecture

Where a,b,c,d,e and f are coefficients

This is a special case of the general second-degree equation. The resulting graph (see Figure 2) is a function of the parameter settings. This could be a circle, hyperbola, or parabola. This is done by computing the point, *Q*, in the graph of Figure 2. Where *Q* = *dP*. *d* is a large integer and P represent the points on an elliptic curve.

Operation of the Hybridized Model

The hybridized model uses the ECC and the DSA. When message m is send from sender A, it passes through the ECC and the DSA to get to sender B. The ECC uses the elliptic curve points while the DSA uses hash function, private and public keys for encryption and decryption. Under the ECC, we have the global elements represented by E_q (a,b) which is the curve with parameters a,b and q where q is prime number or integer in the form of 2^m. The second global

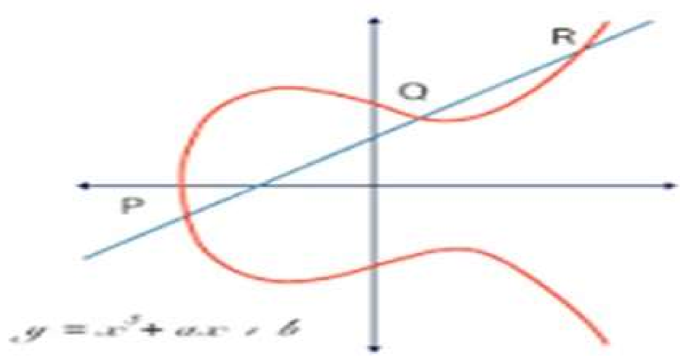

Figure 2: Elliptic Curve Graph (Olaniyi *et al.*, 2016)

element is G which is the point on the elliptic curve. The next is to generate the sender and receiver's public and private keys as depicted in Figure 3.

To generate sender keys say P_A, then we select a private key say n_A where $n_A < n$ and $n \rightarrow \infty$. The public key is therefore

$$P_A = n_A * G \quad \text{.....(2)}$$

To generate receiver's keys say P_B, then we select a private key say n_B where $n_B < n$ The public key is therefore

$$P_B = n_B * G \quad \text{.....(3)}$$

The next is to calculate the secrete keys of the sender and the receiver. The secrete key of sender is given as

$$k = n_A * P_B \quad \text{.....(4).}$$

That of the receiver is

$$k = n_B * P_A \quad \text{.....(5)}$$

After getting these secrete keys, then the encryption start as depicted in Figure 3. The message is first encoded into elliptic curve as plain text and is represented as P_m as depicted in Figure 3 for proper encryption a random positive number k is chosen which will allow us to calculate the cipher point c_m as

$$c_m = \{kG, P_m + k\,P_B\} \quad \text{.....(6)}$$

This point is sent to the receiver as depicted in Figure 3 under the ECC section.

For decryption to occur at the receiver end, the x coordinate of the cipher point is multiply by the public key of the sender which given as

$$z = kG * n_B \quad \text{.....(7)}$$

This is then subtracted from the y coordinate of the cipher point as

$$result + k\,P_B - z = P_m + k\,P_B - (kG * n_B) \quad \text{.....(8)}$$

But from equation 3, $P_B = n_B * G$. Therefore equation 8 becomes

$$result = P_m + k\,P_B - z = P_m + k\,(n_B * G) - (kG * n_B) \quad \text{.....(9)}$$

$$result = P_m + k\,P_B - z = P_m + k\,n_B * G) - kG * n_B \quad \text{.....(10)}$$

$$result = P_m$$

This is the same plain text message sent by the sender in Figure 3. This is now pass to the smart contractor for further processing. On the DSA layer, The DSA is the second component of ECCDS architecture. A digital signature is a type of electronic signature based on cryptography and used to authenticate the identity of the sender of a message or the signer of a document and to ensure that the original content of the message or document is unchanged. Both ECC and DSA work on public key cryptography architecture. However, the basic difference between asymmetric system and digital signature is that an asymmetric key system, encrypts using a public key and decrypts with a private key. For digital signatures, however, the reverse is true. The signature is encrypted using the private key and decrypted with the public key as depicted in Figure 3. Because the keys are linked, decoding it with the public key verifies that the proper private key was used to sign the document, thereby verifying the signature's provenance. It uses hash function, private and public keys for encryption and decryption.

The Smart contractor is the third component of our model. It is the security unit that contains stored program on the cloud that run when predetermined conditions are met. Protocol was based on ECCDS. In addition, the smart contractor is used to automate the execution of ECCDS security policies. It also ensures that all participants can be certain of outcome of the election without any intermediary's involvement or time loss. Additional thing the smart contractor does in the work is to use the outcome of ECC for encryption and decryption purpose and the use the DSA for signature purpose.

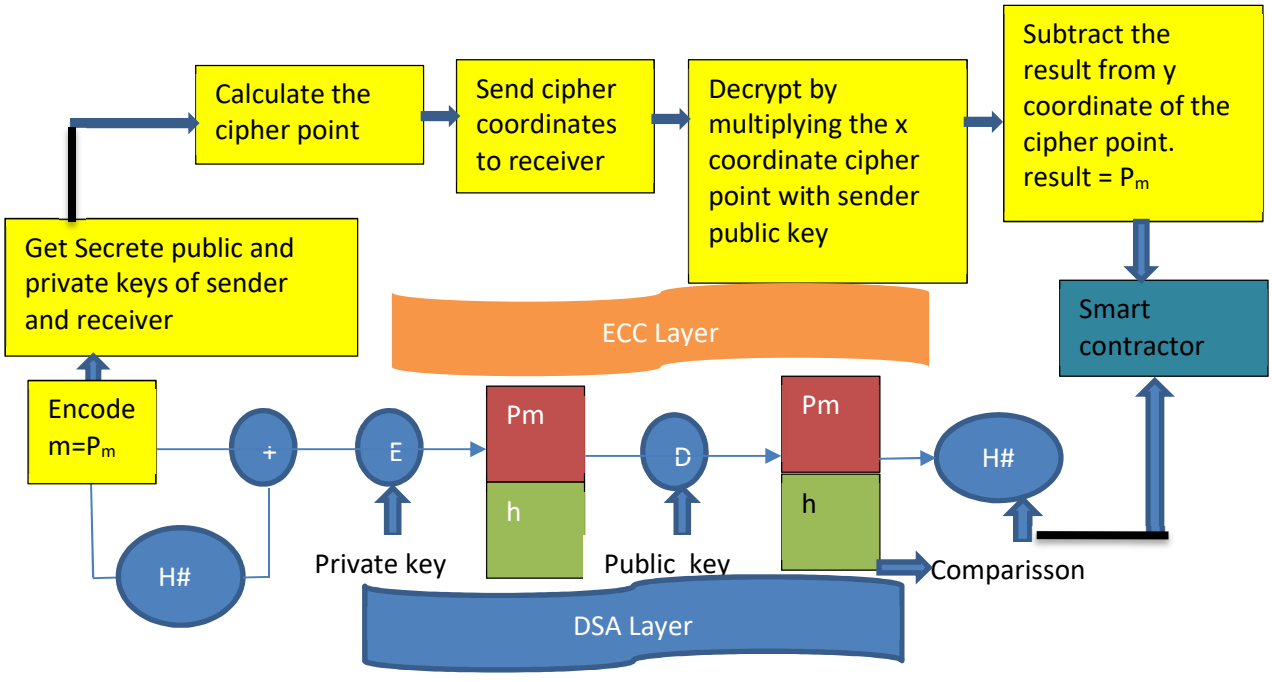

Figure 3: Operation of the Hybridized Model

4. EXPERIMENTAL SETUP, RESULTS AND DISCUSSIONS

Experimental Setup

The prototype demonstration of this work was carried out using the campus network of Adekunle Ajasin University, Akungba-Akoko, Nigeria. In the Experimental setup, 50 computers with the hardware configuration were connected on a LAN to access ECCDS portal in the cloud. The implementation was carried out during the students' Union election so as to gather our information. The computers were station at various Units, Departments and Faculties for student to vote. Each eligible student has a password that was used to login to the ECCDS portal. Once the application is launch, the user activates the system by first signing up. If the registration or sign up is successful, the user is expected to login into the system. Login information (username and password) is authenticated and error returned if failed. This is depicted in Figure 4.

Any vote cast by students goes into the server that contains the ECCDS Application. That is, the DSA, ECC and the smart contract. Six contesting positions were available. These are: The president with 6 contestants, Vice-President, having 4 contestants, General Secretary with 5 contestants, Assistant General Secretary, with 3 contestants, Treasurer and the Auditor, having 2 contestants each. The number of voters trying to log were 2040. However, 1670 eventually voted. The information gathered was run for12 weeks for proper evaluation purpose.

Figure 4: ECCDS login page

5. RESULTS AND DISCUSSIONS

From the results collated through the ECCDS administrator, we had 50 result centres uploaded to the portal with a total of 1670 accredited voters. The crux of our work is to evaluate the Key size, encryption processing time and the Key strength of our ECCDS model with other existing models. These are ECC, RSA and AES respectively. Table 2 and Figure 5 depict the results of key size obtained for 12 weeks. In the Table and Figure, ECC and AES have the best performance while our ECCDS perform better than RSA. For example, in the first experiment, ECCDS has 167 while ECC, RSA and AES had 163, 1024 and 64 respectively.

The results of the encryption processing time is depicted in Table 3 and Figure 6 respectively. The result shows that, ECCDS encryption time is higher than the encryption time of AES, ECC and RSA. These implies that ECCDS performs lesser than ECC, RSA and AES in term of encryption process time For example, the result of the first experiment in Table 3 and Figure 6 shows that ECCDS had 68bits while ECC, RSA and AES recorded 21, 5 and 15 bits respectively with RSA having the best performance.

However, the beauty and the strength of good security system is the decryption time which is the key strength. Table 4 and Figure 7 show the results of the Key strength (Decryption Time). From the result, we observed that ECCDS key strength is higher than that of AES, ECC and RSA. It means that it will take longer time for any intruder to decrypt the system when using the ECCDS model.

Table 2: Results of the System Performance Evaluation based on key size (Bits)

WEEK	AVG ECCDS KEY SIZE (Bits)	AVG ECC KEY SIZE (Bits)	AVG RSA KEY SIZE (Bits)	AVG AES KEY SIZE (Bits)
1	167	163	1024	64
2	164	159	1126	66
3	166	164	1064	64
4	168	166	1026	67
5	167	164	1106	63
6	164	163	1024	64
7	166	162	1025	66
8	168	167	1060	65
9	164	162	1028	68
10	169	164	1024	64
11	165	163	1028	68
12	166	164	1026	65

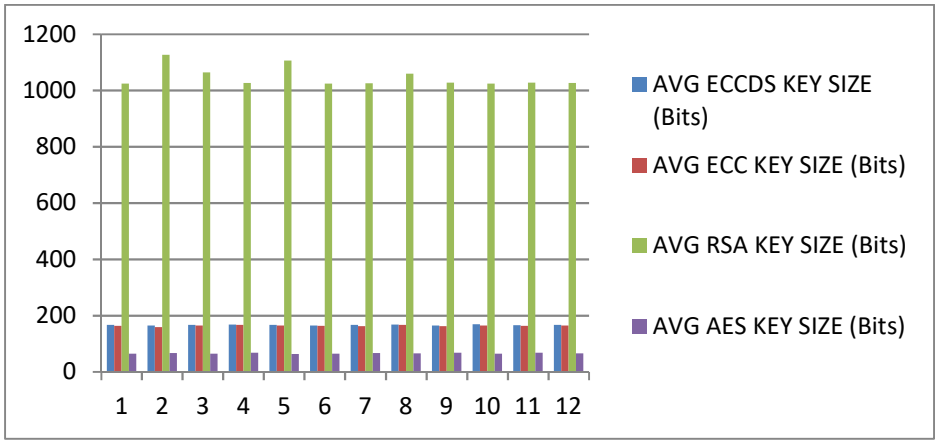

Figure 5: ECCDS Performance Evaluation Using Key Size (Bit)

Table 3: ECCDS Performance Evaluation Using Key Encryption Time

WEEK	ECCDS AVG. ENCRYPTION TIME(ms)	ECC AVG. ENCRYPTION TIME(ms)	RSA AVG. ENCRYPTION TIME(ms)	AES AVG. ENCRYPTION TIME(ms)
1	68	21	5	15
2	65	24	6	14
3	62	22	4	16
4	58	25	4	13
5	62	23	7	15
6	66	26	3	13
7	63	27	5	15
8	69	24	6	13
9	57	25	8	12
10	68	21	4	15
11	60	23	7	17
12	64	24	5	13

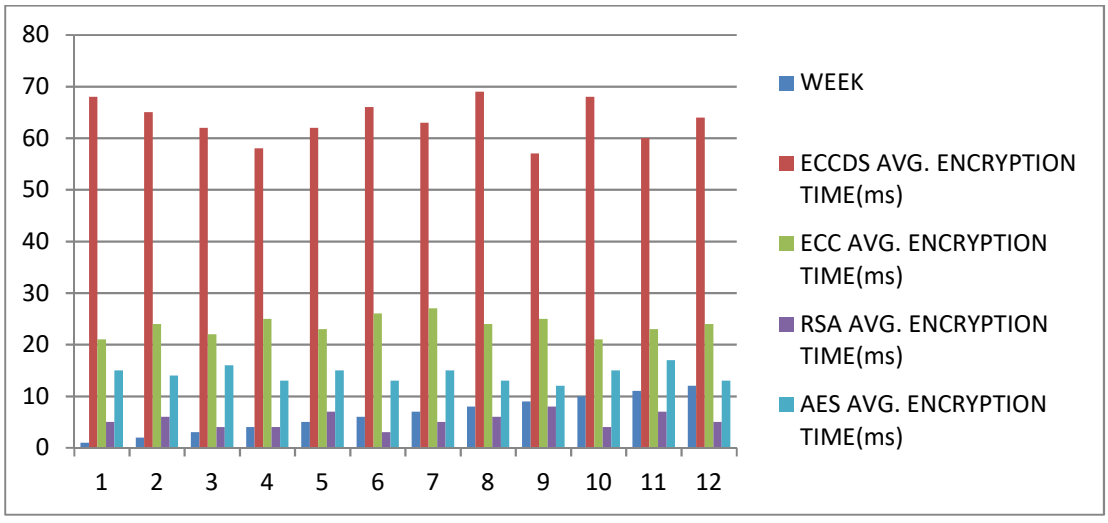

Figure 6: ECCDS Performance Evaluation Using Key Encryption Time

Table 4: ECCDS Performance Evaluation Using Key Strength

WEEK	ECCDS AVG. KEY STRENGTH (ms)	ECC AVG. STRENGTH (ms)	RSA AVG. STRENGTH (ms)	AES AVG. STRENGTH (ms)
1	70	10	3	12
2	71	12	5	11
3	82	11	4	13
4	78	10	4	13
5	74	13	6	14
6	76	12	3	13
7	72	11	5	11
8	81	10	3	13
9	77	10	5	12
10	78	12	4	10
11	70	13	4	15
12	74	11	5	12

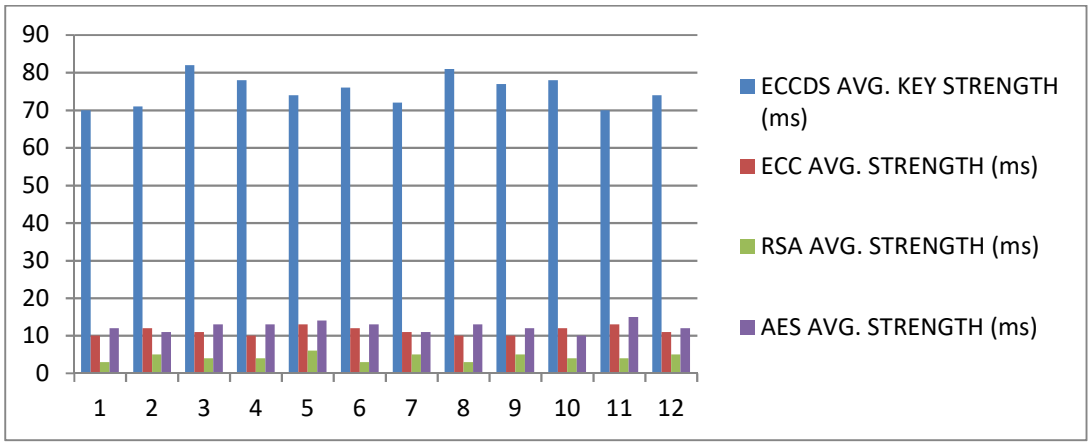

Figure 7: ECCDS Performance Evaluation Using Key Strength

6. CONCLUSION AND RECOMMENDATION

The political landscape of Nigeria elections are dominated by some issues. These include ethnicity, insecurity and the capacity of the institutions responsible for delivering the elections. Among the topmost is the insecurity of votes of electorate which invariably has effect on voters' turnout. For example, the 2023 election was not acceptable to some political parties because the results were not transmitted to the cloud as proposed by INEC. Adoption of e-voting has been of interest to stakeholders and political party leaders in Nigeria.

Academics and technocrats have delved into technical issues related to e-voting system that could foster its smooth implementation and this have encouraged it's full acceptance in Nigeria. The challenge however, is how to secure and maintain a trustworthy e-voting system devoid of security breaches especially from hacking and hijacking. Most researchers have adopted the use of some technologies like RSA, AES and ECC. However, the issues of key size, key strength and encryption time remain open areas that call for novel designs into high level security infrastructure that may enhance and improve the security of e-voting systems. We address this by using a Cloud based ECCDS e-voting system. This is a hybridized technology combining both the ECC and DSA with smart contractor to protect electorate votes against integrity modification in the cloud environment. Adekunle Ajasin University cloud based architecture is used as our network infrastructure.

Evaluation of this work is done with the three other technologies. That is ECC, RSA and AES . The results show that ECCDS key size is higher than that of AES, ECC and RSA. On the issue of encryption time, ECCDS encryption time is higher than the encryption time of AES, ECC and RSA. These implies that ECCDS performs better than ECC, RSA and AES in term of encryption process time.. On the third evaluation, which is the key strength, the ECCDS performs better than both ECC, RSA and AES at the decryption end. This research has added value in the context of security in the conduct of election in Nigeria. . The system is therefore recommended for efficient deployment in any election not only in Nigeria but in other part of the world. One major area which has not been discussed in the work is the issue of votes' integrity during transmission which is left as a future work.

REFERENCES

1. Abdul, W., Nisamud, D., Arif, T. U. and Riaz, U. (2018). "Novel Blind Signcryption Scheme for E-Voting System Based on Elliptic Curves" Mehran University Research Journal of Engineering and Technology 40 (2): 314-322.
2. Ali, A., Zaid, K., Mustapha H., Mostafa, B., Mostafa B. and Mohamed, M. (2022). "An Efficient electronic voting system in a cloud computing environment using Elliptic curve cryptography (ECC)" International Review on Computers and Software (I.RE.CO.S.), Vol. 10, N. 11.
3. Arthur, J. K., Kofi, S. A. and Charlse A. (2021). "A Secured Cloud-based E-voting System using Information Dispersal Algorithm" International Journal of Computer Applications 175(20):975-8887.
4. Awopeju, A. (2011). Election rigging and the problems of electoral act in Nigeria. Afro Asian Journal of Social Sciences,2(24), 1-17
5. Bulut, R.; Kantarci, A., Keskin, S. and Bahtiyar, S. (2019). Blockchain Based Electronic Voting System for Elections in Turkey. In Proceedings of the 2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, 11–15 September 2019; pp. 183–188.
6. Chalabi, M., Mukhtar, M. and Yahya, Y. (2014). E-Voting Systems to Facilitate Elections in Iraq, International Journal on Information Technology (IREIT), 2 (4), pp. 108-113.
7. Chaieb, M., Koscina, M., Yousfi, S., Lafourcade, P., Robbana, and Dabsters, R. (2019). Distributed Authorities using Blind Signature to Effect Robust Security in e-Voting. In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, Prague, Czech Republic, 26–28 July 2019; pp. 228–235.
8. Chalabi, M., Mukhtar, M. and Yahya, Y. (2014). E-Voting Systems to Facilitate Elections in Iraq, International Journal on Information Technology (IREIT), 2 (4), pp. 108-113.
9. Chan, C., Zheng, W., Chuah Chai, W. (2018). "Blockchain-Based Electronic Voting Protocol", International Journal on Informatics Visualization, Vol 2(2018), No 4-2.
10. Fan, X., Li, P., Zeng, Y. and Zhou, X. (2020). "Implement Liquid Democracy on Ethereum: A Fast Algorithm for Real time Self-tally Voting System. arXiv 2020, arXiv:191108774.

11. Johnson, D. (2019). Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values? Eur. J. Risk Regul. 10, 330–358.
12. Jussi A. (2015). "Electronic voting case law in Finland". In Ardita Driza / Jordi Barrat, editor, E-Voting Case Law. A Comparative Analysis, pages 173–181. Farnham: Ashgate, 2015.
13. https://www.thecable.ng/nigerian-elections-a-history-and-a-loss-of-memory
14. Khan, K. M., Junaid A. and Muhammad M. K. (2020). "Secure Digital Voting System based on BlockchainTechnology"NED University Research Journal of Engineering and Technology. Volume 456 (13).
15. Koluguri, A., Gouse, S. and Reddy P. B. (2014). Text steganography methods and its tools. International Journal of Advanced Scientific and Technical Research, 2(4), 888-902.
16. Tohari, A., Jianku, H. and Song, H. (2019). "An Efficient Mobile Voting System Security Scheme Based on Elliptic Curve Cryptography" Third International Conference on Network and System Security, NSS 2019, Gold Coast,Queensland, Australia, October 19-21, 2019.
17. Olaniyi, O., Arulogun, O., Omidiora, E. and Okediran, O. (2015). "Enhanced stegano-cryptographic model for secure electronic voting". Journal of Information Engineering and Applications,5(4).
18. Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O. and Oludotun, A. (2013). "Design of secure electronic voting system using multifactor authentication and cryptographic Hash Functions".
19. Olaniyi, O. M., Folorunso, T. A., Aliyu, A. and Olugbenga, J. (2016). "Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach". International Journal of Information Engineering and Electronic Business, 8(5), 9.
20. Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O. and Okediran O. O. (2016). "Performance assessment of an
21. imperceptible and robust secured E-Voting model", International Journal Of Scientific and Technology Research Volume 3, Issue 64.
22. Olaniyi, O. M., Taliha A. F., Aliyu A.and Olugbenga J. (2017). "Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach"International Journal of Information Engineering and Electronic Business Research Volume 4, Issue 72.