INTERNATIONAL JOURNAL OF NATURAL AND APPLIED SCIENCES (IJNAS), VOL. 12, Special Edition (2019); P. 132 – 140, 0 TABLES, 9 FIGS.

Development of Atomic Operation e-Voting System with Biometric Security Authentication

P.T. Bukie[1], C. Ituma[2], and A. E. Ibor[2]

ABSTRACT

Nigeria got her independence on October 1, 1960, and since then, Nigeria have been using manual voting process in conducting elections into public offices. However, this system is replete with several challenges. Prominent among these challenges is that it can only handle electronic accreditation process using the Smart Card Reader Machine, which is still deficient in authenticating voters. To proffer solution to the various challenges encountered in conventional voting system such as voter verification and authentication, ballot theft, spoiling of ballot, disenfranchisement of eligible voters, and delay in the collation, computation and release of election results, this paper presents an atomic operation e-Voting system with biometric security (verification and authentication). The system also possess a distributed relational database that can allow voters to cast votes from anywhere in the world using an open source technology called mySQL. The system also possesses the capabilities for cancelling compromised fingerprint biometrics after the enrollment, verification and authentication of voters. The research adopts the Rapid Application Development (RAD), instantiating each facet of the election structure as objects. Results from the implementation of the proposed system show that e-Voting System is capable of capturing voters' personal data and fingerprint during enrollment and link them for verification and authentication in a manner that allows duly registered voters to cast their votes and their votes devoid of any form of discrepancies. The implementation of the system shows a fingerprint capture rate of 98% in terms of accuracy, thus, representing a high operational efficiency for the proposed system.

INTRODUCTION

For good governance to be sustained in any democracy, the processes that constitute governments at all levels must be very credible. Also, for government to function well in this 21st Century, government operations must be automated. So, for any government to perform creditably the processes that constituted such a government must be very credible; i.e. political leaders must be chosen by the people they represent through credible and transparent elections.

In many democracies where government operations have been automated, the processes that constituted such governments were not automated, as such those in government were forced on the people through high-tech election malpractices. Though they have quickly, upon assumption of office automated the processes through which they function such as payments of salaries, document transfers, etc., they themselves cannot function well because the processes that brought them into power were not credible so they are not fully accepted by the people they govern and represent.

Before we continue, let us take a break to demystify three concepts that will be used frequently throughout this research. These concepts are: voting, e-voting and e-voting system.

Voting is the process which electorates present their candid judgments about the credibility and moral content of people who wish to represent them in positions of authority. Voting has been used to set up democratic governments in democratic scenery all over the world. E-voting predominantly employ IT-based technologies and devices as a replacement to the traditional use of ballot papers at polling centers for conducting election. E-voting makes use of special software called e-Voting platform.

The Swedish Government (2002) and Lambrinoudakis, Kokolakis, Karyda, Tsoumas, Gritzalis and Katsikas (2002) posited that in e-Voting Systems, pool records are documented, refined and preserved principally as digital instruction, using mobile devices such as laptops, palmtops, desktops, voting machines and phones. It wreathes a variety of poll technologies such as punch cards, kiosks, telephones, optical scan as well as Internet. E-voting has shown an accurate and speedy performance in conducting credible elections in some parts of the countries (Mohammed, Mohammed and Omar 2009). This type of voting system has greatly reduced the mind-numbing processes involved in the traditional manual voting system while adding flexibility to the electoral process.

Manual voting system has generated a lot of litigations in African states. Many of such disputes have degenerated into

*[1]Corresponding author. Email: writepaultu@gmail.com, bukiepaultawo@unical.edu.ng
[1]Department of Computer Science, University of Calabar, Calabar, Nigeria
[2]Department of Computer Science, Ebonyi State University, Abakaliki

assassinations and inter and intra tribal wars. These issues have led many nations to find alternatives, and more credible methods of voting because voters all over the world desire a medium that would easily solve the hitches presented by the conventional system. This is the reason why modern societies have now come to rely on information systems for business, governance, leisure, and even, for decision making. Countries all over the world have been examining how to leverage on the power of IT for citizens to exercise their rights.

Tadayoshi, Adam, Aviel, and Dan (2003) maintain that an election system should be amply tough to bear up a multiplicity of counterfeit behaviour; it must be satisfactorily crystal clear, translucent, intelligible and understandable so that electorates and aspirants can agree to poll results without necessarily engaging in litigations. Surprisingly, history is beleaguered and besieged with election manipulated for the purpose of influencing results to favour a particular aspirant. Fascinatingly, the prelude of electronic voting brought a big transformation in the electoral process, even to most industrial world power nations such as US, China Russia, Britain, Ireland, Japan, etc.

The precision, correctness, vigor and robustness of e-voting system against election malpractice; its rationality, evenness, safety, and lucidity are distinguished requirements and attributes that can be delivered by an e-polling system with lofty heights of integrity. Re-engineering a polling process by using state-of-the-art ICT infrastructures can significantly mitigate many of the factors that would hamper the progress of a given election process. E-voting could also help to generate data and ease reference of materials when the need arises.

Review of Related Literature

Okediran et al. (2011) modeled a three-tier architecture of an e-Voting system: client tier, server tier and database tier. In their three tier architecture, the first tier which they called the client tier has three parts to wit: (i). portable voting unit and potable network operator: (ii) remote clients' computer and (iii) enrollment unit and voting devices. The second tier which they called Application server tier is made up of three components too: (i). The SMS sever, (ii) the web server and (iii) the poll site server. Finally the third tier which they called the database server tier which performs the core service is responsible for saving, manipulating and protecting data. The database server grants access to clients (voter and Election Management Body) who have appropriate login credentials in real-time transaction manner. It also houses the voters' records, candidates' records as well as the election results.

Peralta (2002) presented a simple e-Voting model with a generic description: (1) the voter constructs an "anonymous electronic ballot", (2) the voter shows adequate proof of identity to the election authority (3) the authority "stamps" the ballot after verifying that no other ballot has been stamped for this voter, (4) the voter anonymously inserts the ballot into an electronic mail box. He went further to explain that after the voting deadline passes, votes are counted and a database containing all ballots is made public. Anybody can verify that his/her vote is contained in the database.

Gerck (2002) presented a model of an architecture of ballot design. His design has a long Identification Number which identifies a specific election. The Voter's Nonce is a "long number", which is kept secret and is different for each voter. The Vote Field is a "short number", which denotes the confidential voter's selection(s). The Signature of Election Authority is a cryptographic signature of the other three fields.

Okwong (2012) presented an e-Voting system with two databases: server side and client side. The server side houses the central database for the voting as well as the total number of registered voters and their registration particulars, while the client side houses votes from the voting station, where voters cast their votes. Votes are synchronised between the local and central databases at the end of voting for proper counting. To avoid synchronisation conflict errors between the two servers, he proposed the use of status flags in the voter record. This flag is initialized to FALSE. If the voter is yet to vote the flag is set to FALSE. When the voter votes, the status is turned to TRUE. His architecture targeted basically network infrastructure and security. On network infrastructure, the goal was reduction of bandwidth consumption. This, he achieved by storing the scanned finger print as encoded text instead of images, while on the security, he achieved the goal by capturing the finger print many times and at different instances, so that the fingerprint can always match, even if there is it is affected by environmental hazard.

Matej (2014) presented an e-Voting system which he called OVIS. In a registrant register in a registration center and obtains a VIN. During voter registration, the registrant provides a secret PIN. On Election Day, the voter log onto the system with the secret PIN.

If the PIN does not match, the voter is denied access. A voter who forgets his/her password can retrieve it from the Administrator of the election portal. The system has the capabilities of showing the voter the candidate he/she has voted for. Once a voter cast his/her vote, such a voter will not be granted access to the system a second time. So, a voter can vote only once. Figure 3 displays a synopsis of the workability of OVIS.

Meraoumia, Bendjenna, Amroune & Dris (2018) presented a safe crypto-biometric system dedicated to online e-voting system. The fuzzy commitment concept associated with the palmprint (PLP) and palm-vein (PLV) is the core of their system. To enhance the selective proficiency of the PLP and/or PLV feature vectors, they made use of *Gabor filter* with thresh-holding technique. The data exchanged is encrypted using a random key which is then implanted in a biometric feature vector using a fuzzy commitment scheme. The system is designed in a manner that, in the central election server, the embedded encryption key is extracted using a new retrieval scheme, which is then used to decrypt the transmitted information before being processed. Their experimental results of their system showed that online e-voting based crypto-biometric system has higher performances in terms of accuracies and key retrieval.

Babenko, Pisarev & Makarevich (2017) proposed a model of e-Voting system based on the principle of blind intermediaries using symmetric cipher GOST R 34.12-2015 (Kuznyechik) and hash function GOST R 34.11-2012 (Stribog) cryptographic algorithms. Their system is characterized by a comprehensive approach to electronic voting, namely detailing decisions at all stages of voting. They described the basic techniques for correct and safe conduct of electronic voting, such as the security of transmitted confidential data, the distribution of secret keys, the authentication of the parties, the verification of the transmitted data for integrity, the time control of the transmitted data. Their system shows how these techniques are implemented. Their model was implemented in .NET framework using C# programming language.

Naidu, Kharat, Tekade, Mendhe & Magade (2016) developed a secure e-Voting system using visual cryptography and secure multiparty computation. Secure multi-party computation allows multiple parties to participate in a computation. Security, accuracy reliability and transparency are the major concern in these systems. In their system, the captured fingerprint image is split into two. One share (part) of the fingerprint biometric is stored at administrator side and the other share (part) is stored in voter identification card (VIC) so that no one can access the full fingerprint image. Their system has four phases: enrollment, verification and authentication, vote casting and recording, as well as vote counting and election result publication.

Illakiya, Karthikeyan, Velayutham & Devan (2017) proposed a mobile e-Voting system that combines the concepts of cloud storage, biometric verification, and security to ensure trustworthy voting using Arduino boards for accessing the cloud and processing the data which combines WiFi shield and the functionality of the appliance. In their system, casted votes from polling units are sent to a cloud storage in an encrypted format. The EMB is responsible for decrypting the votes. For voting, they employed Aadhar card and a biometric sensor that assures the ballotters trust and confidence. They also employed a biometric device for verifying and recognizing the identity of voters.

Gallegos & Shin (2015) proposed the concept and design of a novel system that will allow secure e-voting. Their device was equipped with both hardware and software protection measures that prevent various attacks such as physical tampering and modification. They describe how voting and tallying can be done with the device, along with a security analysis of the proposed device. Their system eliminates public lines at voting polls, simplifies voting and may significantly increase voter participation.
Petcu, & Stoichescu (2015) proposed a mobile biometric-based e-Voting system which uses SSL encryption, certificate keys, SMS and 30 to 60 seconds token for security. Their system was able to achieve transparency, privacy and anonymity.

Gunjal & Mali (2012) presented a user friendly multilayer secured internet based voting system using biometric and wavelet based image watermarking. Their system adopts a strongly secured watermarking technique for voter's color picture in YCgCb color space, processed by embedding voter's fingerprint as watermark. The watermark embedding is processed securely through a number of levels. Their technique yields Peak Signal to Noise Ratio (PSNR) up to 54.26 and Normalised Correlation (NC) equals to 1, indicating exact recovery of fingerprint.

Khasawneh, Malkawi, Al-Jarrah, Barakat, Hayajneh & Ebaid (2008) proposed a multifaceted online e-Voting system. Their system has the capacity to handle electronic ballots with multiple scopes at the same time, e.g., presidential, gubernatorial, national assembly, municipal, etc. They used system flag implementation to

ensure that votes cast in favor of a particular candidate are lost, as a result of incorrect computation. They also used a combination of simple biometrics for well-secured identification and authentication. As a way of verifying the robustness and reliability of their system, a number of simulations were done in different voting environments to show voter density, voter inter-arrival times, etc.

In summary, the e-Voting Systems reviewed above have the flowing problems: Some of the e-Voting system make us of unsupervised online registration which captures voter's personal information. Such methods of registration provides have a very weak security architecture for authentication of voters. Some of the e-Voting System reviewed above used SSL as its strongest security. In recent times, SSL has proven to be vulnerable to *"man in the middle"* attacks. Other e-Voting system described in the literature review did not eliminate the traditional paper ballot voting system and postal vote, but rather, it provided the mass voting options, so that those who prefer postal vote or the traditional paper ballot can still vote using the traditional paper ballot on the Election Day, while those who prefer internet voting can use the internet voting option. Those who prefer internet voting can vote in the comfort of their homes.

The proposed e-Voting System is designed to solve the problems identified above using cutting-edge technologies and an improved security architecture. First, the proposed system will capture bio-data (fingerprint), name, polling unit, ward, local government, state constituency, federal constituency and senatorial district of the prospective voter during registration. This registration method makes it difficult for the data to be compromised as the fingerprint is encrypted and saved and then convert it to a format that is computationally difficult to circumvent. Secondly, there is end-to-end encryption of registration data using Message Digest-5 (MD5) algorithm and the content of the vote using Advance Encryption Standard (AES). These two algorithms encrypt the entire data in the system in a manner that intruders cannot access its contents. The system also has secured login console. The login credentials are encrypted using Secure Hash Algorithm – 3 (SHA-3), which has proven to be a very good cryptographic tool. Details of these hashing algorithms are discussed in section 3.4.

The Glitches of e-Voting System in Nigeria

The first glitch of e-Voting in Nigeria is the prohibition of e-Voting system that is enshrined in the Electoral Act 2010 Part V, section 52(2). The reason for this prohibition was that Nigeria has no central database and as such voter verification and authentication will be a major drawback. In 2014, the Nigerian Bar Association challenged the use of smart card readers (SCR) in the election in court and the response of INEC lawyer was that the SCR is to be used only for accreditation and not voting. This prohibition brought a setback to Nigeria's democracy. This legislation has even caught up with the research of IT experts in e-Voting to the extent that even those who had interest in the area are feeling very reluctant to explore further.

Another challenge of e-Voting in Nigeria is the issue of security, anonymity, and trust of the vote. The growing rate of cybercrime is a big threat to e-Voting. Connoisseurs in cyber security worry about hacking of election portals that have very vulnerable system security architectures. The anonymity (the relationship between the voter credentials and the real value of the vote itself) as well as the trust of the vote are important issues in e-Voting. Furthermore, while cyberneticists are preoccupied, working towards complete cybernation of the globe, the cyberspace is speedily replete with cyberpunks, whose primordial objective is to cripple high-tech physical cyber infrastructures that were put in place for public good to further the advancement of our democracy and society.

Finally, the "African monster" called corruption is the number one glitch of e-Voting in Nigeria. The politicians have sectional, ethnic, inordinate and imperial ambitions to perpetually stay in office and enjoy affluence and government apparatuses. This has hardened their minds against legislations that will build and enforce working structures and institutions that will naturally force corruption out of our country.

Prospects of e-Voting System in Nigeria

The flexibility, accessibility, convenience, trust, secrecy, anonymity and other fundamental characteristics and functionalities of existing e-Voting system have given e-Voting system an edge over the traditional manual paper ballot voting system. Many civilized nations of the World have since the last decade, adopted different types of e-Voting system. While some of these nations (Ireland 2004, Netherlands 2007, Paraguay 2008 and Germany 2009) have discontinued the use of e-Voting system for some very cogent reasons, other nations such as (Switzerland, Estonia, France, Canada, Australia, Spain, USA and UK) are improving on their pilot e-Voting schemes, making them better than ever before (Esteve, Goldsmith and Turner 2012). Kimbi and Zlotnikova

(2014) found that Tanzanians have accepted the implementation of remote e-Voting system by virtue of the level of trust they repose in National Electoral Commission of Tanzania (NEC) and also due to the high level of access to financial and pecuniary services via mobile devices over the internet. They pointed out reasons impelling citizens' enthusiasm to remote e-Voting and further subjected the factors to SWOT analysis.

Nigeria has also improved on the partially automated e-Voting system and other supported documents to reflect high-tech transparency. However, Nigeria, through the instrumentation of National Assembly and INEC can improve more in their e-Voting system by simply scraping the "incident vote" because this is one of the major loopholes left in the voting system. Consequent upon the increasing telecommunication infrastructure penetration in Nigeria, and research in network security (Secure Socket Layer, Transport Session Layer, and Cryptography, etc.), e-Voting system is expected to grow geometrically in next two decades.

METHODOLOGY

Architectural Diagram of the Proposed System

The architectural diagram in figure 1 shows a clear picture of the way the system will function and how it integrates the different component. It shows a design of the functionality of the e-Voting System proposed in this research. In the diagram, there are four locations representing four polling units. In each of the four locations, there is an Omni-directional network Antenna broadcasting at 360º. There are also two computer systems. At the center of the diagram, there is an authentication server, vote server and a 3-sectorial network antenna broadcasting 120º each. The black dotted lines with double headed arrows depicts the voter devices and the vote server exchanging information for authentication of voter while the red lines with one arrow depicts encrypted votes moving from the voter devices to the vote server. See figure 1.

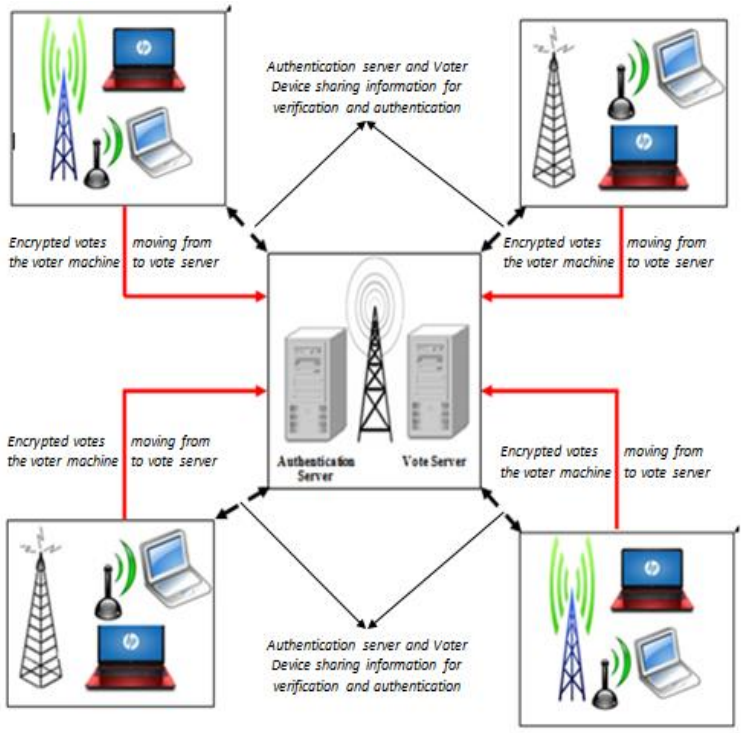

Fig. 1.Architectural diagram of the Proposed System

Data Flow Diagram of the System

Figure 2 shows how data moves from one component of the proposed system to another. It describes the complete entities of the system and how data flows into and out of each of these components. A detail explanation of the DFD of the system is given below:

(i) Registrant enroll/register and data is captured and stored in data store 1;

(ii) Check if voter has registered before (voter verification and authentication) retrieve voter's data from the data store 1;

(iii) During voting, voter particular candidate and votes is stored in data store 1;

(iv) Admin adds Election, election type is stored in data store 2; audit trail records transaction;

(v) Admin Adds Candidates, candidates name and party is stored in data store 1; audit trail records transaction;

(vi) Super Admin adds Admin User, audit trail keeps track of the changes and store records in data store 2.

(vii) Data can be retrieved from audit trail

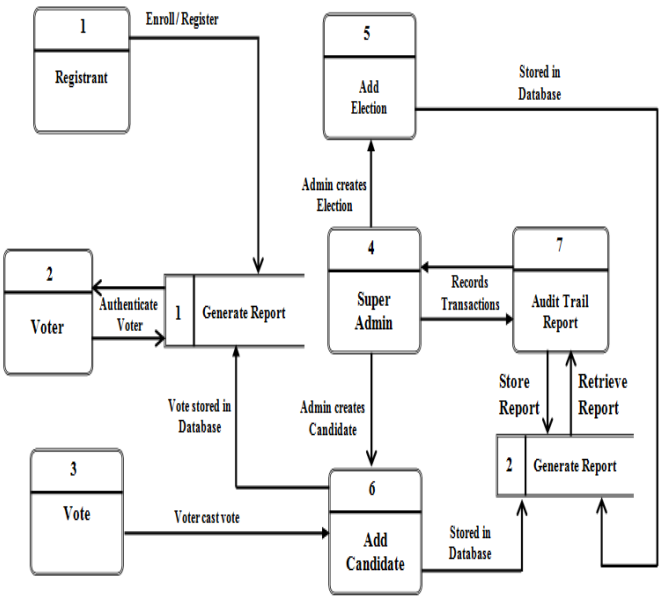

Fig. 2. Data Flow Diagram of the Proposed System

RESULTS AND DISCUSSIONS

An Appraisal of the Functionality and Structure of the System

The system will is a full e-Voting system. We have re-engineered the existing half-way automated system that is in use in Nigeria and the porous architecture and security frameworks. It is going to be process re-engineering because there exist already in Nigeria, a half-way automation of the voting system. So we intend to improve on the system architecture to a fully operated e-Voting system with 3-tier architecture: backend, frontend and database. The entire election process will have the following stages: check voter, enroll voter and cast vote.

Check Voter Operation

The check voter operation checks if the voter has registered. If the voter fingerprint matches any of the fingerprints stored in the database, the system displays a message "The fingerprint was verified". But if the voter fingerprint does not match any of the fingerprints saved in the enroll table of the database, the system prints another message, "Voter record does not exist. Please register". See figure 3.

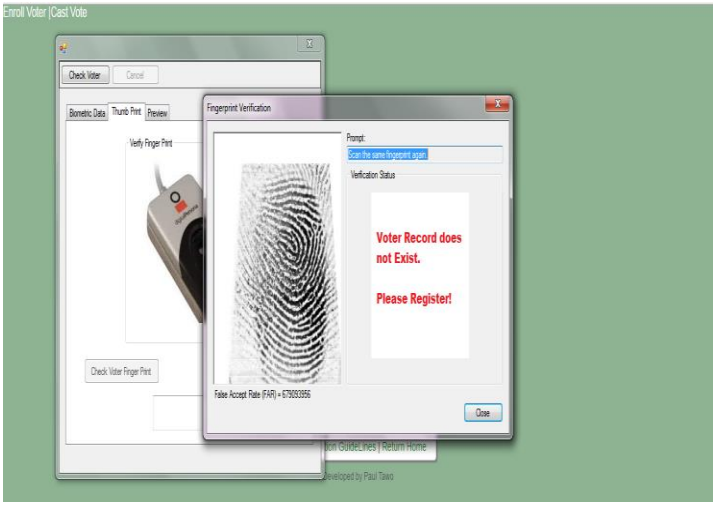

Fig. 3. Unsuccessful-Voter not registered

Enroll Voter Operation

The enroll voter operation register a prospective voter, convert the fingerprint to base 64 and post the fingerprint and bio-data into the database. See figure 4, and 5.

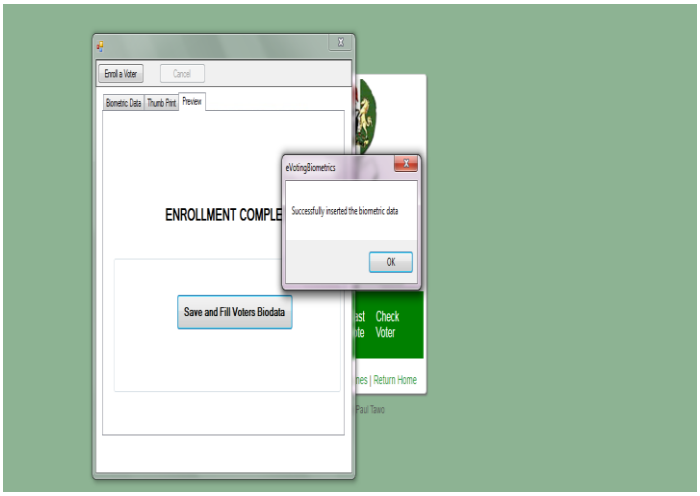

Fig. 4. Enrollment Completion Page

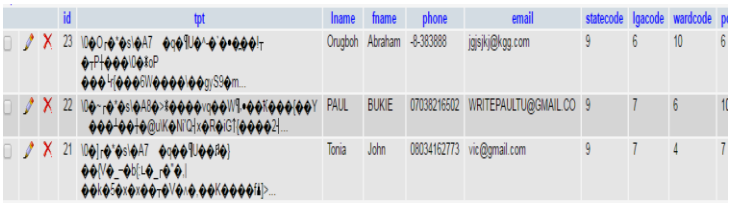

Fig. 5. Encrypted Fingerprint template in the database

Cast Vote Operation

On the day of election, the vote servers will be open to all eligible voters (i.e. those who enrolled). The voter is authenticated using fingerprint. After the voter is authenticated, and there is

evidence that his/her finger print matches the fingerprint in the database, the voter is then served with a voting page to cast vote. This task is also performed on the client-side of the application. The cast vote operation enables registered voters to verify their identity and then cast their votes. It has two phases: the verification/authentication phase and the cast vote phase. See figure 6, 7 and 8.

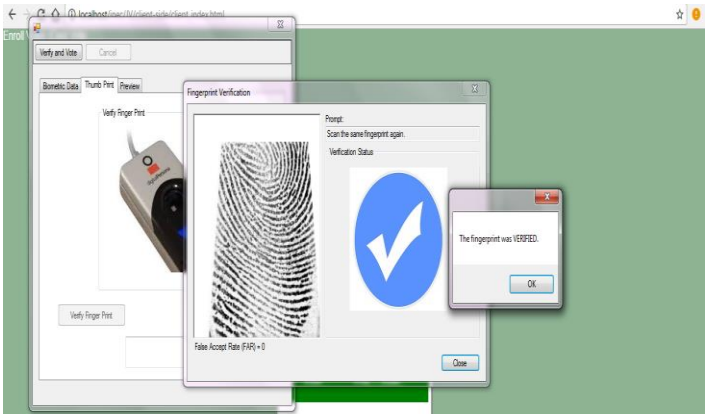

Fig. 6 Successful Fingerprint Verification Window

Fig.7. Cast Vote Window

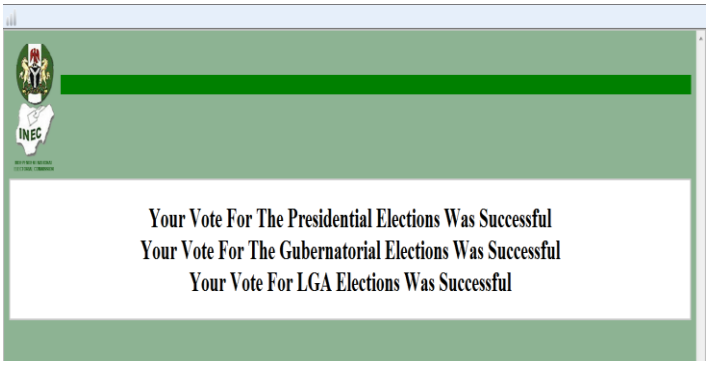

Fig. 8. Cast Vote Success Window

For each voter, a token is tight to your records. So once you have voted, that token is disabled. In an attempt to vote twice, the system displays the message shown in figure 9.

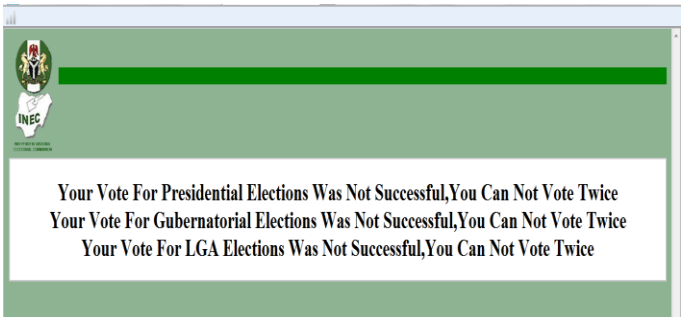

Fig. 9. Attempt to Cast Vote twice Window

Collation, Counting of Votes and Publishing of Results

Collation, counting and publishing of election results are the most technical issues in elections. In manual voting system, collation is done first at the polling units. The votes from polling units are later collated at the collation centers at the local government levels, constituency levels, state levels and finally at the national level. Because of the different levels of collation, the process is very cumbrous and requires high level of technical support. In very many cases, the rigging and compromising of election results is done at the collation centers. The electoral officers sell out votes to contestants who are financially buoyant. But in this system, the vote collation, counting and publishing of result is done by just a click of the mouse.

System Security Features

The system security architecture was designed using two encryption algorithms (AES and SHA-3) to protect the password and the vote cast respectively, from being hacked. We also have an audit trail that tracks the system transactions and then keep counts of the user's name, date and time. The algorithms are discussed below.

Advanced Encryption Standard (AES)

AES is symmetric-key block cipher created by NIST in the year 2001. It is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds. It has defined three versions, with 10, 12, and 14 rounds. Each version uses a different cipher key size (128, 192, or 256), but the round keys are always 128 bits. It makes uses four different types of transformations to provide security. These transformations include substitution, permutation, mixing, and key-adding.

AES have been tested and has proved that it can withstand the following attacks: Brute-Force Attack because of its larger-size key; Statistical Attacks because so many tests have failed to do statistical analysis of the cipher text; there are no Differential and Linear Attacks on AES yet and finally, the algorithms used in AES are so simple that they can be easily implemented using cheap processors and a minimum amount of memory.

Secure Harsh Algorithm 3 (SHA-3)

SHA-3 is an acronym for Secure Hash Algorithm 3. SHA-3 is a detachment of cryptographic ancient family called Keccak, published in 2015 by NIST because of the successful attacks on SHA-1 and SHA-0. It is capable of implementing a one way hashing which cannot be hacked at all. SHA-3 has dual phases: the

"absorption" phase and the "squeeze" phase, i.e., data is absorbed inside a sponge and thereafter, the output is squeezed out. This method is called sponge construction.

During "absorption" stage, some chunks of the message are XORed into a compartment of the absorption phase, which is further changed in totality. In the "squeeze" phase, the chunks of the output are interpreted from the same compartment of the phase, swap with phase transformations. The volume of the piece that is written and that of the piece that is read is known as "rate", while the volume of the piece that is unaffected by I/O is nicknamed "capacity". The capacity decides the safety measures that the scheme uses. The greatest security echelon is a miniature of the capacity. In SHA-3, the phase comprises of 5×5 array collection of 64-bit words, making a total of 1600 bits. On an Intel Core 2 processor, it is claim that, the speed is 12.5 cycles per byte. Nonetheless, in actual implementation of the hardware, it is remarkably faster than every supplementary finalist.

Fingerprint Authentication

One of the best methods of information systems security is biometric. It is very reliable especially if combined. In this application, the voter uses fingerprint biometric to gain access into the system.

Secure Login Credentials (User ID and Password)

The Super Admin and Admin User use secure User ID and a password to gain access into the system. The password of the Super Admin and Admin User are encrypted using SHA-3.

Distributed Database

The system uses a distributed database to enable voters to cast their votes from anywhere in the world. The voter does not need to go to where he/she registered. This is a significant difference between the half-way automated existing e-Voting System used in Nigeria today.

CONCLUSION

In this paper, we have developed an atomic e-Voting system with fingerprint biometric authentication and a distributed database. This will serve as a solution to the seeming unending problem of electoral violence, rigging and other malpractices. It provides a user friendly platform for creating elections, creating candidates, enrolling voters, verifying and authenticating voters as well as voting election. The research observes that physiological and behavioral biometrics combined with high-tech ICT tools can be used to build very robust security architecture for e-Voting system.

The e-Voting system may be seen as a threat to the political class in Nigeria, who in time past, have taken undue advantage of the vulnerable security and other weaknesses of the current e-Voting system to their selfish and imperial advantages. Far be it from Nigerians to watch the collapse of democracy when we have a lasting solution starring us in the face. We must wake up and pursue the collective interest of Nigeria as a country. We must put away our inordinate, imperial, sectional, ethnic and individual aspirations and interests. We must, as a Country, leverage on ICT infrastructures, considering their economy, flexibility, convenience and efficiency, to build a strong democracy using of e-Voting System. If embraced, e-Voting System could serve as a possible means of restoring the lost confidence of voters due to its transparency.

REFERENCES

Ahto, B. and Triinu, M. (2007). Practical security analysis of e-voting systems. *Proceeding IWSEC'07 Proceedings of the Security 2nd International Conference on Advances in Information and Computer Security,* Springer-Verlag Berlin Heidelberg. 320-335.

Babenko, L., Pisarev, I., and Makarevich, O. (2017). A model of a secure electronic voting system based on blind intermediaries using Russian cryptographic algorithms. *Proceedings of the 10th International Conference on Security of Information and Networks - SIN '17,* Jaipur, India, 13-15 and 45-50. doi:10.1145/3136825.3136876. Retried from sci-hub.tw/10.1145/3136825.3136876

Esteve, J. B., Goldsmith, B. and Turner, J. (2012) *International experience with e-voting: Norwegian e-vote project.* DC: International Foundation for Electoral Systems.

Gallegos, C., & Shin, D. (2015). A novel device for secure home E-voting. *Proceedings of the ACM 2015 Conference on Research in Adaptive and Convergent Systems – RACS,* 321-323, Prague, Czech Republic. doi:10.1145/2811411.2811541. Retrieved from sci-hub.tw/10.1145/2811411.2811541.

Gerck, E. (2002). Private, Secure, and auditable internet voting. In Gritzalis, D. (ed.), *Secure electronic voting*, USA: Kluwer Academic Publishers.

Gunjal, B. L., & Mali, S. N. (2012). Secure E-voting system with biometric and wavelet based watermarking technique in YCgCb color space. *2012 IET International Conference on Information Science and Control Engineering (ICISCE 2012),* Shenzhen, China, 7-9 Dec. 2012. doi:10.1049/cp.2012.2284.

Illakiya, T., Karthikeyan, S., Velayutham, U. M., & Devan, N. T. R. (2017). E-voting system using biometric testament and cloud storage. *Proceedings of the ACM 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM),* Chennai, India, 23-24. doi:10.1109/iconstem.2017.8261305. sci-hub.tw/10.1109/ICONSTEM.2017.826130

Khasawneh, M., Malkawi, M., Al-Jarrah, O., Barakat, L., Hayajneh, T. S., & Ebaid, M. S. (2008). A biometric-secure e-voting system for election processes. *2008 5th International Symposium on Mechatronics and Its Applications.* Amman, Jordan, 27-29 doi:10.1109/isma.2008.4648818. Retrieved from sci-hub.tw/10.1109/ISMA.2008.4648818.

Kimbi, S. and Zlotnikova, I. (2014). Citizens' readiness for remote electronic voting in Tanzania. *Advances in Computer Science: An International Journal*, 3(2), 150-159. Retrieved from www.ACSIJ.org,

Lambrinoudakis, C. Kokolakis, S. Karyda, M., Tsoumas, V., Gritzalis, D., and Katsikas, S. (2002). *Electronic voting systems: Security implications of the administrative workflow.*

Matej, T. (2014). Electronic Voting: To have or not to have. In *European Scientific Journal Special ed. (3)*3. 224-230.

Meraoumia, A., Bendjenna, H., Amroune, M. & Dris, Y. (2018). Towards a Secure Online E-voting Protocol Based on Palmprint Features. *2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS).* Tebessa, Algeria; 24-25

Mohammed, M., Mohammed, K., and Omar, A. (2009). Modeling and simulation of a robust e-voting system. *Communications of IBIMA*, 8:198-206. ISSN: 1943-7765

Naidu, P. S., Kharat, R., Tekade, R., Mendhe, P., & Magade, V. (2016). E-voting system using visual cryptography & secure multi-party computation. *2016 International Conference on Computing Communication Control and Automation (ICCUBEA).* Pune, India, 12-13 August 2016.

Okediran O. O., et al. (2011). A Framework for a multifaceted electronic voting system. *International Journal of Applied Science and Technology*. 1(4):135-142

Okwong, A. E. (2012). IT-based solutions to the electoral system in Nigeria. *West African Journal of Industrial and Academic Research 5(1),* 127-139.

Peralta, R. (2002). Issues, non-issues, and cryptographic tools for internet-based voting. In Gritzalis, D.A. (Ed.), *Secure Electronic Voting*, USA: Kluwer Academic Publishers.

Petcu, D. and Stoichescu, D. A. (2015). A hybrid mobile biometric-based e-voting system. *IEEE 2015 9th International Symposium on Advanced Topics in Electrical Engineering (ATEE),* Bucharest, Romania, 7-9 May 2015. doi:10.1109/atee.2015.7133676.

Tadayoshi, K., Adam, S., Aviel, D. and Dan, S. W. (2003). *Analysis of an electronic voting system.* IEEE Computer Society Press.

The Swedish Government (2002). *Internet voting final report from the election technique commission.* Retrieved from http://www.justitie.regeringen.se/propositionermm/sou/pdf/sou2000_125.pdf