International Journal of Applied Sciences and Smart Technologies

Volume 4, Issue 2, pages 149–158

p-ISSN 2655-8564, e-ISSN 2685-9432

An Enhanced Multi-Level Authentication Electronic Voting System

Ayodeji O.J Ibitoye[1*], Halleluyah O. Aworinde[1], Esther T. Adekunle[1]

[1] Computer Science Dept., Bowen University, Iwo, Osun State, Nigeria
Corresponding Author: ayodeji.ibitoye@bowen.edu.ng

(Received 06-10-2022; Revised 01-11-2022; Accepted 14-11-2022)

Abstract

Originally, manual voting systems are surrounded with issues like results manipulation, errors and long result computation time, ineligible voters, void votes among others. Electronic voting system helped in overcoming the challenges with manual voting system, to engendered other problems of phishing, men in the middle attack alongside voter's impersonation. By these challenges, the integrity of an election results in a distributed system has become another top concern for e-voting system based on reliability. To achieve an improved voters' authentication and result validation with excellent user experience, here, a Facial Recognition Electronic Voting System that is power-driven by Blockchain Technology was developed. The entire election engineering activities are decentralised with improved security features to enhance transparency, verifiability, and accountability for each vote count. The self-service voting system was built by smart contract and implemented on the Ethereum network. The obtained reports and evaluations reflected a non-editable and self-sufficiently certifiable system for voting. It also has a competitive edge over fingerprint enabled e-voting system. Aside it's excellent usability and general acceptance, the developed method discarded to a larger extend, intended fraudulent actions from election activities by eliminating the involvement of a middleman while facilitating privacy, convenience, eligibility and satisfactory voters' right.

Keywords: blockchain technology, facial recognition, electronic voting system, smart contracts, Ethereum network.

1 Introduction

The advent of democracy as a system of government, and the freedom of expression by the citizen through voting has become a norm in the process of selecting a leader all over the world. While, the right and power of citizen through voting without malpractice cannot be underestimated, voting remains a way of resolving conflicting and inconsistent viewpoints in major decision of policies and/or who leads over a period. Although the processes may be controversial, depending on the adopted voting system, yet the unruffled decision becomes communal after each electorate has express his/her opinion [1]. For Instance, candidates belonging to a political party are elected to the Local Government, State, Or Federal either for executive or legislative positions in Nigeria over a period. With fairness and existing democratic rule as factors for consideration, the voting processes and context remains an evolving domain from manual system to electronic with the goal of building a credible, verifiable, transparent and integrity driven e-voting system. While the electronic system of voting is also filled with potential possibilities of denial-of-service attack (DOS), server hacking, hardware malfunction, administrative manipulation among others, e-voting is being investigated widely, and countless operational models have been deployed and in used as stable solution for voters' freedom and right across multifaceted faces of the society.

By this development, e-voting remains the most optimal system of voting with capacity for innovative improvement on its shortfalls when compared with the manual systems of voting. Hence, the process of improving openness, vote privacy, invulnerability and verifiability, especially in a decentralised voting ecosystem is more important today as technology keeps improving in proportionate direction with cybercrimes [2]. In more recent times, blockchain technology has been adopted for secured and transparent processes. For instance, the number of groups actions irrespective of volume and currencies can be tracked clearly and in real time despite the dispersed wallets in Bitcoin. By this, a central authority is not required on a Point to Point based system and through the use of cryptographic approach, the system is kept secured and unbroken [3].

Therefore, in e-voting, a decentralised blockchain system with end-to-end encryption can be used to address vote tampering, while promoting vote tallying in real time. However, it is important to embed such e-voting systems with biometric or computer vison infrastructure in order to curb human generated challenges of ineligibility, verifiability and impersonation in an e-voting cycle of registration, validation, collection and tallying. Several biometric features such as fingerprint with blockchain technology has been used to build an e-voting system, the essence of this work is to fuse a facial recognition software with blockchain technology in e-voting system development. Thus, in section two (2), an overview of related works on e-voting system is presented. Section 3 discussed the multi-level e-voting system using facial recognition and Blockchain technology. Sample experimental evolutions and findings is presented in section four (4) before conclusion and recommendation in section five (5).

2 Sample Related Works

In a democratic system, voting remains an important tool for people to express their opinion regarding policies, choice of leadership and more. Over the years, different methods have been integrated to define a sustainable election process. Some of this include the use of paper wherein voters use pencil or thumb print on the preferred candidate. Then, an optical scanner [4] or hand counting is used in tallying, and results are computed on Microsoft Excel sheet or calculated using modern calculator in some instances. As the world evolve with technology, some countries still trust the paper ballot voting system either for its disadvantage in order to satisfy self-interest or genuinely due to problems of digital infrastructure, change process or its advantages. As the technologically growth spans, an electronic system for recording, storing and processing voters' data into digital form was developed. E-voting, as an instance uses digital ballot instead of the paper ballot; then, the entire voting cycle from registration to result computation is also performed electronically. For instance, a Direct Internet and Electronic (DRE) machines as a portable computer has been built for the exhibition of ballot choices from electronic recording votes. By pressing the touch screen, voters' decision is authenticated [5] and vote audit of recount has the case may be is possible through the Voter-Verified (or Verifiable) Paper Audit Trail (VVPAT). [6] also encoded fingerprints on smart card through secret splitting algorithm to develop an Electronic Biotechnology Voting System (EBTVS), for voter's verification.

Consequently, with the advent of blockchain technology, several e-voting systems have been developed overtime. [7] deployed an e-voting system, which uses a biometric device for validation during registration on a smart contract through an Ethereum network. The application explores the latent use of decentralised networks to audit and understand electoral procedures. Similarly, the application of blockchain technology for the deployment of a distributed e-voting system was appraised by [8]. It also recognised the legal and technological restrictions of using blockchain technology as a service for e-voting systems.

In the bid to advance the need for blockchain technology in e-voting, [9] encouraged electoral involvement through a decentralised blockchain technology; the solution addresses vote tampering, upheld transparency in vote cast while protecting the voters. Indeed, as the call for a decentralised voting system heightens, [10] projected a decentralised e-voting system with blockchain. The developed two-level architectural system provided a safe voting process that is exclusive of redundancy. The application also ensured that necessary voting criteria are satisfied for an anonymous but transparent vote count. Subsequently, a permission driven multichain platform for voting was developed by [11]. The software allows a distinct administrator to arrange the Blockchain based desired specification while voter’s distinctiveness was confirmed through a fingerprint recognition system to secure vote cast. Aside, a crypto-voting system by [12] through two linked blockchains, [13] provided perquisite information to voters on the difficulties and risk associated with blockchain e-voting system through an Architecture Trade-off Analysis Method (ATAM). Computational cryptographic trust has proven to be more reliable than human trust in voting. By this and more, smart contact was also deployed by [14] with to goal to address challenges with voting accuracy, security and privacy. Futhermore, hashing was deployed by [15] to ascertain that each vote count while preserving the anonymity of the voter. This is related to the electronic voting protocols by [16], whose system ensures the security of the identity of every voter while recorded vote results are tamper-proof. No doubt, Blockchain technology has continued to provide positive support for e-voting system with fingerprint technology. It is secured from human corruption, however, due to the fallouts of fingerprint technology and the fast adoption of facial recognition systems, a blockchain distributed facially recognised e-voting system is presented in section three (3) for consideration.

3 Multi-level Authentication E-voting System

The object detection model used here is YOLO V3. The raspberry pi, due to its limited computing power, cannot be used to implement the original YOLO model. Hence, we use YOLO Tiny, a tiny and yet efficient version of YOLO. For the datasets we used Google's open images dataset V6. To train the model, we have to set the number of batches for the datasets so as to determine the iteration of training the model. The ideal number of iterations should be 2000 batches per number of objects. In our case we are dealing with 7 objects so the batches should be 14,000. While the model is training the prime objective of the algorithm is to decrease the average loss. We started with average loss of 4.5 and reached to an average loss of 1.08. Figure 1 shows the graph depicting the decrease in average loss as the number of iteration increases.

The electronic facial recognition e-voting system uses Ganache blockchain technology to manage voters and administrative activities in a voting cycle. The voting procedures are deployed using Smart contract on an Ethereum network (Blockchain). The architecture of this system as presented in Figure one (1) showed how several modules of the system synergises to attain the goal of authentic, verifiable, invulnerable, convenience and transparent voting system.

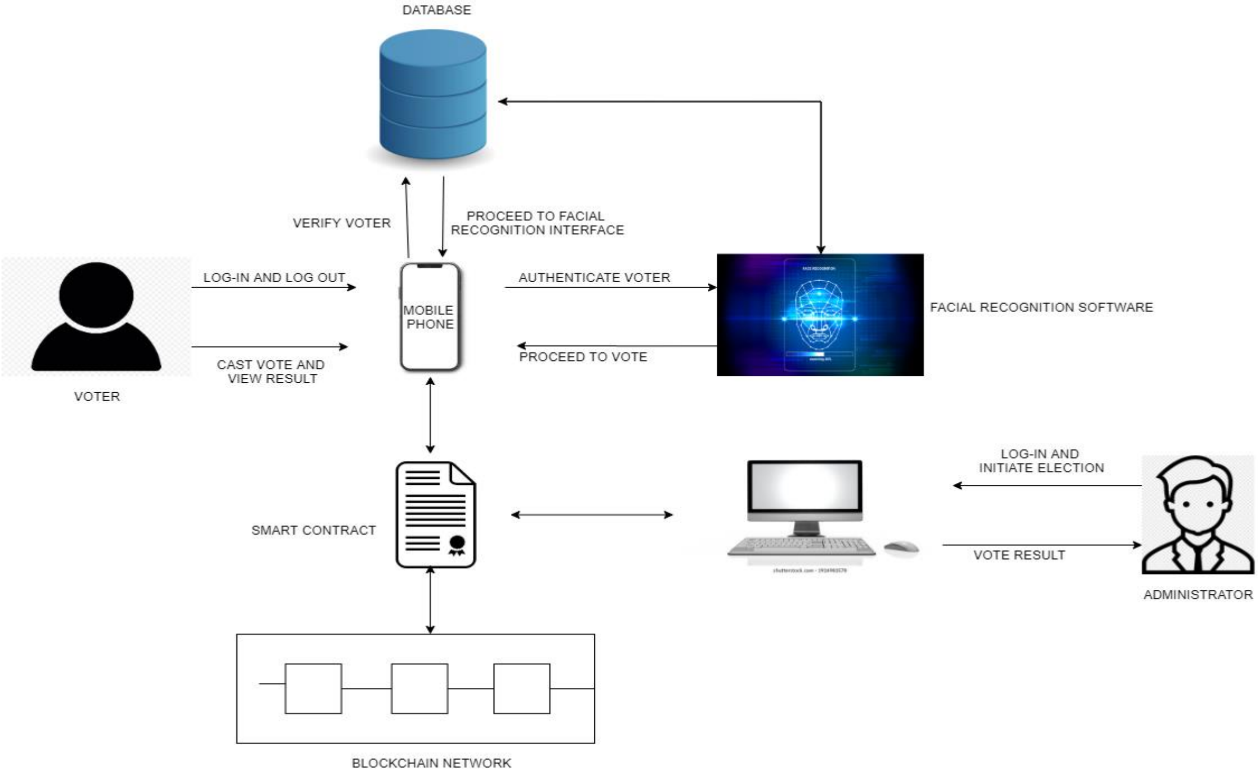

Figure 1. Facial Recognition E-voting System Using Blockchain

Initially, from the available dataset, voters who do not satisfactorily meet the voting criteria were eliminated to avoid data repetition and inconsistency. Then, 215 voters with the right voting criteria validated their preregistered information to obtain an Ethereum private key as a vote accreditation certificate. At this instance, multiple user images were captured from different angles for a more detailed training set. By this, the voters' data, which also included their faceprint are matched and stored in the database. From Figure one above, the face geometry, which included the users, length of the jawline, the form cheekbones, the depth eye sockets, and more were captured and analysed, using the Local Binary Pattern (LBP) algorithm. In order to vote, the voter's login to the mobile application; first, with the unique username and password before validating the user face with the embedded LBP facial recognition algorithm as a two-factor authentication procedure.

Sequel to the existing training and preprocessing procedures for registered images, the face of the voter is scanned to ascertain a matching degree from the array of images in the database whenever the voting system is being used, as the voters face is presented, the following procedures takes effect:

1. LBPs are extracted before the resulting histograms from each of the cells are weighted and concatenated differently just like the training data.
2. k-NN (with $k=1$) is subsequently performed with the x^2 distance with the goal of finding the closest face in the e-voting training data.
3. The user face print is associated with the smallest x^2 distance in the final classification if found.

These extracted features as further illustrated in Figure two (2) is packaged to activate face remembrance at every authentication and validation protocol call. This is possible through direct conversion of facial analog information to a digital equivalence tagged faceprint. Then, features are extracted from the faces through vector point analysis before the classification is obtained. While each faceprint is unique to an individual just like the thumbprint, face validation activities are executed to match and compare the users face with the stored information during capturing for further decision support before a voter or administrator access the developed e-voting system. Therefore, if there exists a match, the voter is granted approval to cast a vote by choosing the choice candidate then clicking the button "Vote". In addition, voters can also ascertain that his/her vote decision is not manipulated in an ongoing electoral process. Once schedule election period is over, vote collection takes place before tallying. Then. the Administrator announces the vote results with satisfactory evidence.

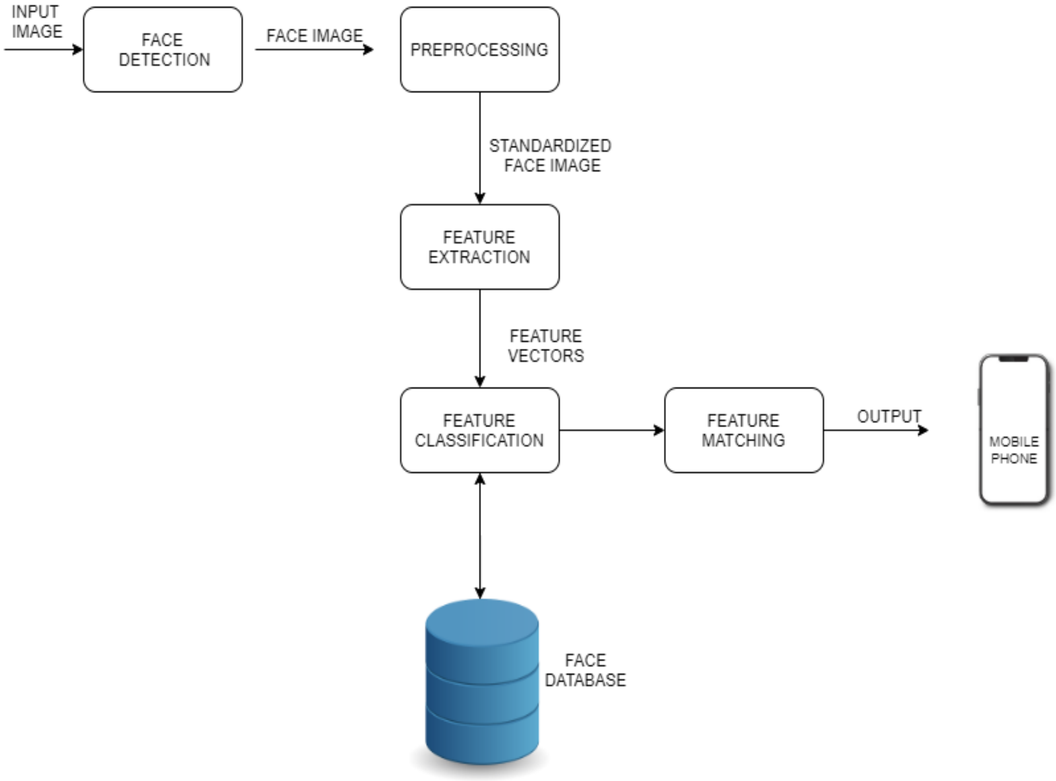

Figure 2. Block Diagram of a Facial Recognition System.

4 Evaluation Report

The developed blockchain e-voting system with face recognition achieved excellence when evaluated based on the principles of:

a. **Eligibility:** The ability to allow only registered voters to vote just once based on the defined electoral procedures. Thus, with the two-factor authentication, only authorised voters can access the voting system.

b. **Privacy:** The ability to leverages cryptographic properties of blockchain towards ensuring that each vote is kept secret through vote hashing.

c. **Verifiability:** The ability of a voter to track vote statues in the tallying system through the unique Ethereum ID

d. **Convivence:** The ability of an eligible voter to vote easily without biases or discrimination

e. **Usability:** The ability to measure how well a user can use the application based on process and design flow.

The following analysis as presented in Figure 3 is obtained

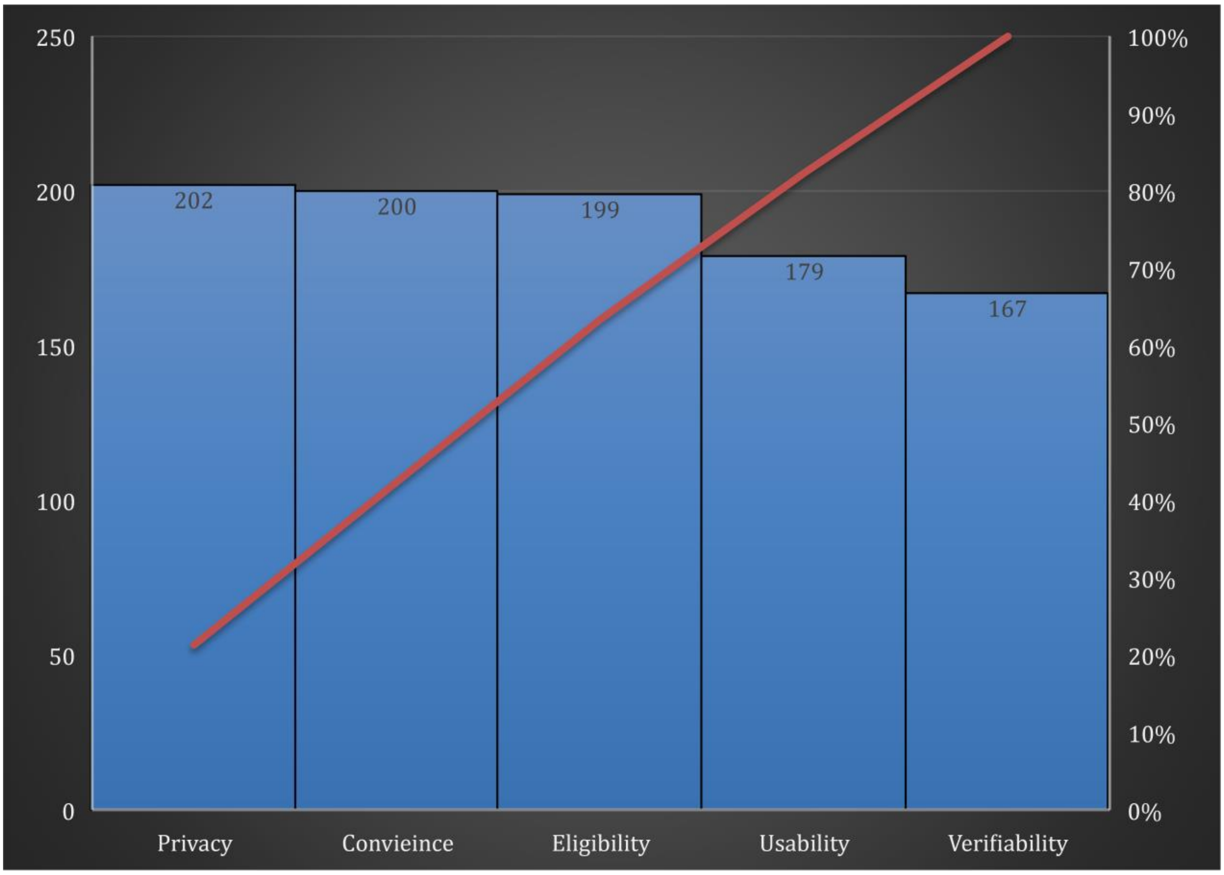

Figure 3. Sample Voters Evaluation Report

Overall, the Facial Recognition voting system also helped in resolving the challenge of varying fingerprint patterns, which cannot be recreated or rendered. In addition, with the new normal where people are encouraged to touch less, a self-service remote face ID verification can be achieved. However, voters disguising or wearing face shield remains a challenge for future development and not withing the scope of this research activities.

5 Conclusion

Overall, the Facial Recognition voting system also helped in resolving the challenge of varying fingerprint patterns, which cannot be recreated or rendered. In addition, with the new normal where people are encouraged to touch less, a self-service remote face ID verification can be achieved. However, voters disguising or wearing face shield remains a challenge for future development and not withing the scope of this research activities.

References

[1] Y. Xie, “Who Over reports Voting?”, *J J.Am.Polit.Sci.Rev.* **80**, 613–624, 2017.

[2] C. Ayo, O. Daramola, A. Azeta, “Developing A Secure Integrated E-Voting System”, In *Handbook of Research on E-Services in the Public Sector: E-Government Strategies and Advancements*, IGI Global, USA, 278–287, 2011.

[3] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” Available: https://bitcoin.org/bitcoin.pdf, 2009.

[4] M. Rockwell, “Bitcongress – Process for block voting and law”, Available: http://bitcongress.org/ [Accessed: December 2017].

[5] A. Ndem, “Three risks posed by electronic voting - The Election Network”, Available: http://theelectionnetwork.com/2018/10/25/three-risks-posed-by-electronic-voting/, 2018.

[6] O.O Adeosun. Ayodeji O.J. Ibitoye, J.O Alabi, “Real Time E-Biotechnology Voting System; Using Secret Splitting”, *International Journal of Electronics Communication and Computer Engineering*, **6**(6), 2015.

[7] A. Benny, “Blockchain based E-voting System”, *SSRN Electronic Journal*, 2020.

[8] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, G. Hjalmtysson, “Blockchain-Based E-Voting System”. *IEEE International Conference on Cloud Computing, CLOUD, 2018-July*, 983–986., 2018.

[9] H. V. Patil, K. G. Rathi, M. V. Tribhuwan, Science, C., College, D. Y. P. A. C. S., “A Study on Decentralized E-Voting System Using Blockchain Technology”, *International Research Journal of Engineering and Technology (IRJET)*, **5**(11), 48–53, 2018.

[10] K. Isirova, A. Kiian, M. Rodinko, A. Kuznetsov, “Decentralized electronic voting system based on blockchain technology developing principals”, *CEUR Workshop Proceedings*, *2608*, 211–223, 2020.

[11] K. K. Sharma, J. Raghatwan, M. Patole, V. M. Lomte, “Voting system using multichain blockchain and fingerprint verification”, *International Journal of Innovative Technology and Exploring Engineering*, **9**(1), 3588–3597, 2019.

[12] F., Fusco, M. I. Lunesu, F. E. Pani, A. Pinna, “Crypto-voting, a blockchain based e-voting system”, *IC3K 2018 - Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, **3**, 223–227, 2018.

[13] D. Thebus, O. Daramola, “E-voting System for National Elections Using a Blockchain Architecture”, In *Pan African International Conference on Science, Computing and Telecommunications Book of Proceedings*, University of Swaziland, Kwaluseni, Swaziland, 2019.

[14] K. Sadia, M. Masuduzzaman, R. K. Paul, A. Islam, “*Blockchain Based Secured E-voting by Using the Assistance of Smart Contract”*, 2019.

[15] R. Suganya, A. Sureshkumar, P. Alaguvathana, S. Priyadharshini, K. Jeevanantham, “Blockchain Based Secure Voting System Using IoT”, *International Journal of Future Generation Communication and Networking*, **13**(3), 2134–2142. 2020.

[16] C. C. Z. Wei and , C. C. Wen, “Blockchain-based electronic voting protocol”. *International Journal on Informatics Visualization*, **2**(4–2), 336–341, 2018.