International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 8, Issue 1
January 2021

FOG COMPUTING BASED ELECTRONIC VOTING SYSTEM: A SOLUTION TO DENIAL OF SERVICE ATTACK

Mahdi Alhaji Musa[1], Bashir Saleh Maina[2], Aliyu Musa Bade[3]

1,2,3 Department of Computer Science, Yobe State University, Damaturu-Nigeria

Abstract: Fair elections are the backbone of democracy. However, voters show concern of intimidation and violence during elections. Intimidation and violence are use as tools to either prevent voters from casting their vote or forcing them to vote for undesired candidate. Although several technologies of electronic voting have been adopted to address the problem of intimidation but they do not address the issue of latency in electronic communications and high bandwidth. In this research we propose FOG computing in order to solve these problems. FOG computing provides resources over the Internet and allows many applications to be deployed to provide services for different institutions. The major bottleneck being faced currently in these cloud-based frameworks is their limited scalability and hence inability to cater to the requirements of centralized Internet of Things (IoT) based computing environments. The new paradigms of fog and edge computing provide innovative solutions by bringing resources closer to the user and provide low latency and energy efficient solutions for data processing compared to cloud domains. Still, the current fog models have many limitations and focus from a limited perspective on either accuracy of results or reduced response time but not both. In this paper, we proposed a novel framework whereby a wireless technique will connect to a fog computing node, which will in turn connect to a central cloud for real-time analysis. Polling units operate in a similar queuing design as the Automatic Teller Machines (ATMs) and the voters use their fingerprint for validation. The proposed system is configurable to various operation modes which provide the best Quality of Service as required, in diverse fog computation scenarios and for different user requirements.

I.Introduction

Electronic voting constitutes an important part of democratic governance in ICT-enable environment [1]. This is aimed at increasing the participation of citizens in nation`s electoral process at the same time improving the outcome of an election as compare to traditional voting systems. Electronic voting supports a critical electoral process including verification of eligibility, registration stage, voting stage and finally counting of votes electronically.

A lot of electronic voting systems have been proposed by different researchers. Though they all intend to solve problems there-in the conventional (manual) voting system, they however do have their shortcomings. A major problem facing these electronic voting systems is Denial of Service attack.

Hence there is need to bring out a voting system that will curb this menace of attack used as tools to either prevent voters from casting their vote or forcing them to vote for undesired candidate.

Lack of free and fair election mostly in developing countries like Nigeria through intimidation and denial of service attack as often associated with traditional paper-ballot voting systems is mostly reported and are considered very crucial and must be addressed in a fair and democratic election process. While intimidation and vote buying also occur in traditional voting systems, these threats are more dangerous in Internet voting schemes as an attacker may exercise influence and control at a larger scale without adequate security measures.

Nigeria is the most populous country in Africa and the seventh most populous in the world; by 2050 the population may exceed 289 million of which 45.7% are under 15 years [2, 3]. Naturally, this make the electoral process difficult to execute. Quadrennially, Nigerians go to the polling unit to cast their votes in accordance to the Electoral Act 2006 and the 1999 Constitution [4, 5]. Together they explain the process for [6]:

1. voter registration;
2. party and candidate registration;
3. campaign financing and regulation;
4. election observation;
5. ballot design;
6. polling stations;
7. voting, counting, and tabulation;
8. election management bodies; and
9. dispute settlement authorities.

Eligible voters cast their votes according to the guidelines in [7]. The voting process is broken into two main parts: Accreditation and voting [7]. Accreditation starts at 8:00 AM, after the Presiding Officer (PO) declare the Polling Unit open for accreditation and voting. Voters are authenticated using radio frequency identification (RFID) reader and fingerprint scanners by the Assistant Presiding Officer (APO) III. Also, APO III ensures that voters are not voting for the second time and that they are in the right polling unit. APO II records voters on the voter register and they furnished with ballot paper by the PO. Voters then proceed to the cubicle where the cast their vote. Finally, they slot the folder ballot paper in the ballot box which is out in the open. Voters are free to remain behind and observe the exercise. By 2.00 PM the PO declares the exercise closed after all those on queue have cast their vote.

The conventional voting system is depicted in the diagram below:

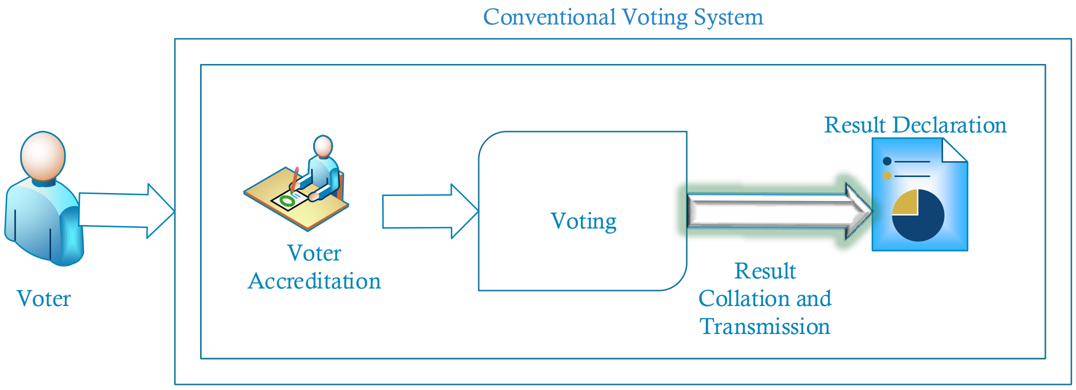

Figure 1: Conventional Voting System

The process has quite slow and inefficient base on the principles of queuing theory, because some polling units may end up with long queue while other are empty [8, 9]. Authentication and recording can be done more efficiently through automation. Furthermore, bandits can deny voters the chance to vote through intimidation. All these can be prevented through the use of fog computing-based e-voting system.

Literature Review

Typically, an e-voting protocol that protects the voter's privacy relies on the role of a trustworthy authority to decrypt and tally the votes in a verifiable manner. E-voting protocols in the literature normally distribute this trust among multiple tallying authorities using threshold cryptography; for example, see [2]. However, voters still need to trust that the tallying authorities do not collude, since then they can breach the voters' privacy.

A number of block chain e-voting systems have been designed [27, 23]. However, all of them incur substantial computational overhead of the block chain mining, which makes their implementations challenging for certain organisations or for large-scale elections. Remarkably, [24] first introduced a self-tallying voting protocol for boardroom voting with subsequent proposals by [14] and [15]. A self-tallying protocol converts tallying into an open procedure that allows any voter or a third-party observer to perform the tally computation once all ballots are cast. This removes the role of a tallying authority in an election as anyone can compute the tally without assistance. These protocols provide maximum ballot secrecy as a full collusion of the remaining voters is required to disclose an individual vote and dispute-freeness that allows any third party to check whether a voter has followed the voting protocol correctly. Unfortunately, self-tallying protocols

Election is a formal process of voting in or out: 1) a person to a public office or 2) accepting or rejecting a political proposition [23]. For democracy to flourish, elections have to be free, fair and accessible to the masses. In order to ensure the aforementioned requirements, researchers have proposed several solutions. In [20, 24] the authors proposed and electronic voting system using PHP and MySQL. The proposed systems, allow users to vote online. Therefore, the system when connected to the internet can allow abundant flexibility for voters in and out of the country. However, these proposed systems do not comply with some of the electoral laws of the Nigeria, such as the mandatory ballot paper and transparency.

However, the merits of e-voting are too god to pass. Countries all over Europe are implementing e-voting in one way or the other [25]: Britain had a trial run for local-council elections, where ballots over the Internet; Geneva, Switzerland, in its plan to wire the whole country, cast e-vote in April 2006. In addition, the European Union has provided funds for a 3year pilot program on e-voting in three major countries in Europe. By 2017, the EU has published technical and security requirements issued by the Council of Europe for e-voting systems. Lately, Helios Voting is proposed in [26], as a framework for e-voting based on the 2017 EU guidelines.

Recently, [26] developed a facial recognition system for internet of Things (IoT) based e-voting system. The proposed system authenticates voters using their voter ID and their facial features. Although the proposed system enhances voting process by speeding it up and securing it, the IoT as well as the cloud cannot cope with the traffic since pictures will be downloaded and upload for every voter. To ensure machine-machine security, [28] proposed a distributed electronic voting system using block-chain technology. However, the proposed system is too complex for IoT devices.

Currently, existing electronic voting systems are generally classified into two [29]. The first class is where the use of private booth is employed such that voters can cast their ballots privately example [30]. When it’s difficult to tap communication between the booth and collection server, then vote selling and denial of service attack can be mitigated. The system is having limitation of having the presence of voter at the polling unitjust like in the case of traditional paper-ballot systems.

The second class which is an internet based involve registration of voters such that voters can cast their votes from any geographical location using internet access [31]. The second class uses combination of cryptographic and protocols like blind signatures and etc in order to secure the election.

Methodology

In this research, we proposed a distributed e-voting system using IoT and fog computing. The introduction of fog computing will help ensure improved quality of services and reduced latency. Fog nodes will be deployed along with IoT devices. The IoT devices request for credential of voter from the fog node. Only when the fog node encounters a miss that a recursive request is made to the cloud. We do believe that the proposed system will ensure accurate and secured voting which can be implemented in real election exercises.

To achieve this, a flowchart of the system is designed and described in Figure 2 below:

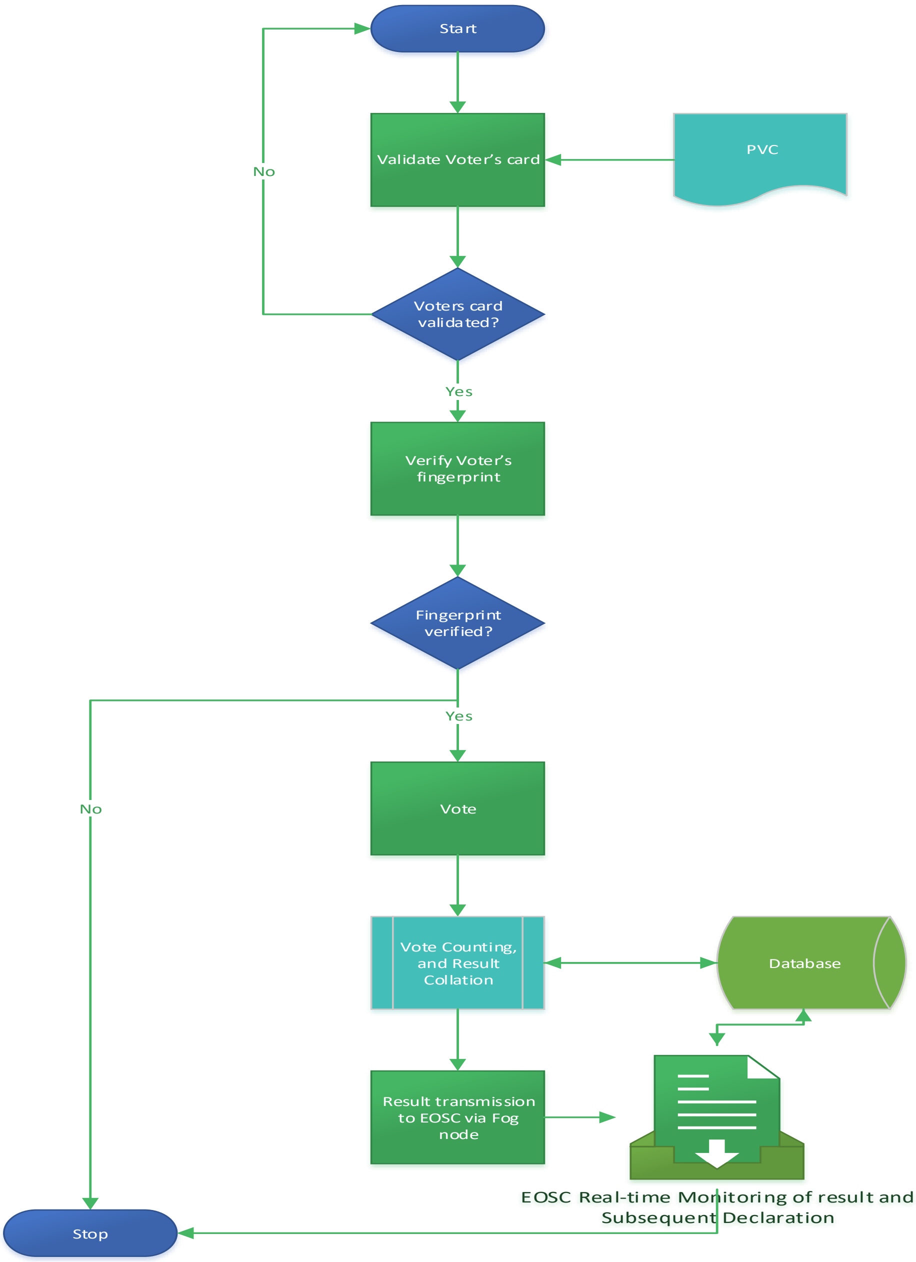
Start
Validate Voter's card
PVC
No
Voters card validated?
Yes
Verify Voter's fingerprint
Fingerprint verified?
Yes
No
Vote
Vote Counting, and Result Collation
Database
Result transmission to EOSC via Fog node
EOSC Real-time Monitoring of result and Subsequent Declaration
Stop

Figure 2: Flowchart of the proposed System

Implementation and Discussion of Results

Figure 2 below shows the proposed system. The polling units operate in a similar queuing design as the Automatic Teller Machines (ATMs): The voters use their finger print and voters' card if a voter is validated the voter is then presented with the ballot paper else access is denied. After the user has voted, a summarized copy of the voting will be printed (ballot paper) which he will then place in the ballot box. The polling unit will also transmit a copy of the results to the INEC's Electoral Operations Support Center (EOSC) where the election is observed in real-time

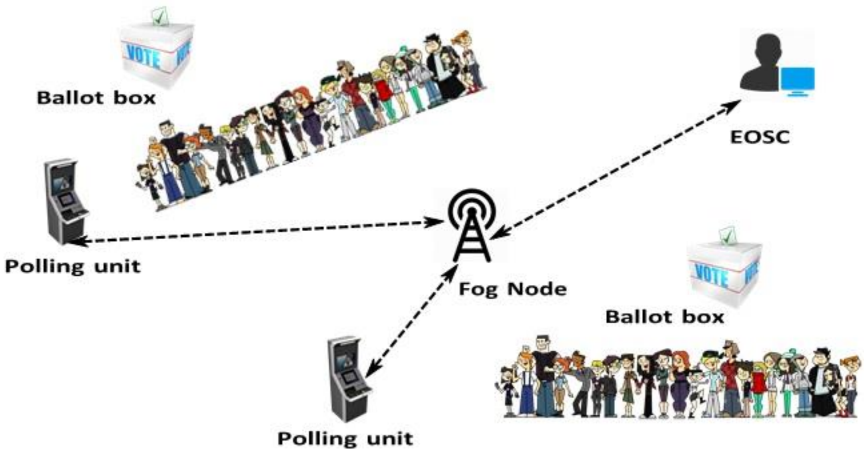

Figure 3: Proposed System

RFID Scanner was used for reading voters' PVC. This is to verify the PVCs tendered by voters are the original ones issued by the INEC and the voter is at the right poling unit. Each RFID Scanner is mapped to a particular poling unit; hence each poling unit has the capacity to scan and validate PVCs registered only to that particular unit.

After successful verification of the PVC, Fingerprint Scanner was used for thumb printing. This is to verify PVC card holders are the authentic bearers of the PVC they tendered. Also, to verify voters, Raspberry Pi Camera was used to re-verify voters.

When all these are done successfully, the Polling unit then transmits a copy of the results to INEC EOSC where the election is observed in real-time. A test was carried out with a set of twenty (20) voters who were screened and later-on allowed to cast their vote. The time taken for the process as well as the efficiency were found to be impressive and more efficient than the conventional voting system and/or other electronic voting systems.

Also, the collation and transmission of results is another issue in which the proposed Fog computing based electronic voting system will increase efficiency and fairness in the voting system. This is so because the election result is transmitted via the fog node in a fast, reliable and secured mode.

Conclusion and Recommendations

This fog-based electronic voting system is emerging as significant alternative to the conventional systems in the delivery of reliable, trusted elections, reduces man power, no need to store EVM's for counting purpose, gives and monitor election results in real-time and most importantly resolve denial-of-service-attack. By developing and implementing this prototype fog-based electronic voting system, we demonstrate encouraging improvements in several aspects of the electronic voting systems, including security, efficiency and usability.

This shows that the fog-based e-voting has promising potential for further research and adoption by the government electoral commission (INEC) and other private corporations for adoption. This is because, with this system in place, Intimidation and violence which are used as tools to either prevent voters from casting their vote or forcing them to vote for undesired candidate will be drastically resolved.

In future research, we plan to extend our study to remote e-voting and also to accommodate more complex voting schemes, such as Single Transferable Vote (STV).

Acknowledgement

This research is sponsored by TERTIARY EDUCATION TRUST FUND (TETFund) under Institution Based Research Fund (IBRF) 2019 intervention for Yobe State University.

REFERENCES

[1] Reuven Hazan, 'Candidate Selection', in Lawrence LeDuc, Richard Niemi and Pippa Norris (eds), *Comparing Democracies 2*, Sage Publications, London, 2002

[2] Nigeria–UNSDPF , “United nations sustainable development partnership framework,” United Nations, Tech. Rep., 2017, accessed 4th March, 2019. [Online]. Available: https://www.unicef.org/nigeria/media/1556/file

[3] educateachild.org, “Nigeria: Educate a child,” 2019, accessed 4th March, 2019. [Online]. Available: https://educateachild.org/ our-partners-projects/country/nigeria

[4] Federal Republic of Nigeria, “Constitution of the federal republic of nigeria 1999,” 1999, accessed 9th May, 2019. [Online]. Available: https://publicofficialsfinancialdisclosure.worldbank.org/sites/fdl/files/assets/law-library-files/Nigeria_Constitution_1999_en.pdf

[5] —, “Electoral act, 2006,” 2006, accessed 9th May, 2019. [Online]. Available: http://www.nassnig.org/document/download/5794

[6] E. R. Aiyede, “Electoral laws and the 2007 general elections in nigeria,” Journal of African elections, vol. 6, no. 2, pp. 33–54, 2007.

[7] INDEPENDENT NATIONAL ELECTORAL COMMISSION, “Regulations and guidelines for the conduct of elections,” 2019, accessed 9th May 2019. [Online]. Available:

https://www.inecnigeria.org/wp-content/uploads/2019/01/Regulations-and-Guidelines-2019.pdf

[8] A. Willig, “A short introduction to queueing theory,” Technical University Berlin, Telecommunication Networks Group, vol. 21, 1999.

[9] M. Zukerman, “Introduction to queueing theory and stochastic teletraffic models,” arXiv preprint arXiv:1307.2968, 2013.

[10] F. Computing, “the internet of things: Extend the cloud to where the things are,” 2016.

[11] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the internet of things,” in Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, 2012, pp. 13–16.

[12] S. Khan, S. Parkinson, and Y. Qin, “Fog computing security: a review of current applications and security solutions,” Journal of Cloud Computing, vol. 6, no. 1, p. 19, 2017.

[13] CISCO, “Cisco fog computing solutions: Unleash the power of the internet of things,” 2015, accessed – 15th April, 2019. [Online]. Available: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/ docs/computing-solutions.pdf

[14] Huawei, “Huawei edge-computing-iot solution enables predictive maintenance for industrial manufacturing,” 2017, accessed – 15th April, 2019. [Online]. Available: https://e.huawei.com/en/tech-topic/en/ 201708031600

[15] S. Dave, “Computing at the edge of iot,” 2018, accessed – 15th April, 2019. [Online]. Available: https://medium.com/google-developers/ computing-at-the-edge-of-iot-140a888007bd

[16] H. Li, K. Ota, and M. Dong, “Learning iot in edge: Deep learning for the internet of things with edge computing,” IEEE Network, vol. 32, no. 1, pp. 96–101, Jan 2018.

[17] E. Zeydan, E. Bastug, M. Bennis, M. A. Kader, I. A. Karatepe, A. S. Er, and M. Debbah, “Big data caching for networking: moving from cloud to edge,” IEEE Communications Magazine, vol. 54, no. 9, pp. 36–42, Sep. 2016.

[18] F. Aliyu, T. Sheltami, and E. M. Shakshuki, “A detection and prevention technique for man in the middle attack in fog computing,” Procedia Computer Science, vol. 141, pp. 24–31, 2018.

[19] Independent Electoral Commission, “Eosc operational manual,” 2019, accessed 9th May, 2019. [Online]. Available: https://www.inecnigeria.org/wp-content/uploads/2019/01/ EOSC-Operational-Manual-Updated-EDITED.pdf

[20] M. A. Musa and F. M. Aliyu, “Design of electronic voting systems for reducing election process,” Int. J. Recent Technol. Eng, vol. 2, no. 1, pp. 183–186, 2013.

[21] O. Nkwocha, Effective Leadership in Nigeria: Practical Ways to Build Effective, Inspiring, Transformational and Visionary Leadership and Governance in Nigeria. AuthorHouse, 2012. [Online]. Available: https://books.google.com.sa/books?id=C0pvwzkJamYC

[22] A. M. Ibrahim, The Case of Nigeria: A State Stuck in Transition. Cham: Springer International Publishing, 2015, pp. 101–120. [Online]. Available: https://doi.org/10.1007/978-3-319-18383-1_5

[23] D. W. Paul and E. Heinz, “Election: Political science,” 2015, 10th May, 2019. [Online]. Available: https://www.britannica.com/topic/ election-political-science/Plurality-and-majority-systems

[24] A. Azeta, V. Azeta, O. Olaniyan, A. Azeta, and G. Ayeni, “Implementing an e-democracy system in nigeria,” Journal of Resources Development and Management, vol. 4, 2015.

[25] T. M. Vinod Kumar, E-Governance for Smart Cities. Singapore: Springer Singapore, 2015, pp. 1–43. [Online]. Available: https: //doi.org/10.1007/978-981-287-287-6_1

[26] L. Panizo Alonso, M. Gasco, D. Y. Marcos del Blanco, J. A. Hermida Alonso, J. Barrat, and H. Alaiz Moreton, “E-voting system evaluation based on the council of europe recommendations: Helios voting,” IEEE Transactions on Emerging Topics in Computing, pp. 1–1, 2019.

[27] K. Srikrishnaswetha, S. Kumar, and M. Rashid Mahmood, “A study on smart electronics voting machine using face recognition and aadhar verification with iot,” in Innovations in Electronics and Communication Engineering, H. S. Saini, R. K. Singh, G. Kumar, G. Rather, and K. Santhi, Eds. Singapore: Springer Singapore, 2019, pp. 87–95.

[28] R. Tso, Z.-Y. Liu, and J.-H. Hsiao, “Distributed e-voting and e-bidding systems based on smart contract,” Electronics, vol. 8, no. 4, 2019. [Online]. Available: http://www.mdpi.com/2079-9292/8/4/422

[29] X. Yi , E. Okamoto , Practical internet voting system, Journal of Network and Computer Applications 36 (1) (2013) 378–387 .

[30] T. Moran , M. Naor , Split-ballot voting: everlasting privacy with distributed trust, ACM TISSEC 13 (2) (2010) 16.

[31] P.Y.A. Ryan , P.B. Ronne , V. Iovino , Selene: Voting with transparent verifiability and coercion-mitigation, in: International Conference on Financial Cryptography and Data Security, pp. 176-192, 2016 .