IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 4, Ser. I (July. – August. 2023), PP 22-26
www.iosrjournals.org

The Bimodal Voter Accreditation System (BVAS) In 21st Century Nigeria Election: Security Breaches And Solutions

[1]Fergus Uchenna Onu, [2]Ikechukwu Jonathan Ezea, [3]Fubara Egbono and [4]Ogbaga Ignatius Nwoyibe
Department of Computer Science Ebonyi State University, Abakaliki
Department of Software Engineering, University of Port Harcourt

Abstract
The challenges of elections in Nigeria have led to the introduction of a technological device called the Bimodal Voter Accreditation System (BVAS). This however didn't usher in the needed free and fair elections due to the compromise of the security and the outright absence of some security features that would have made the device difficult and almost impossible for intruders to attack. The researchers took time to elucidate on the challenges, features and likely security breaches. They went further in the research to opine some solutions which in their own view would help solve the issue of security and engender free and fair election if all other factors are held constant.

Keywords: *Bimodal Voter Accreditation System* ***(BVAS),*** *Election, voter accreditation, INEC, Biometric voter accreditation*

Date of Submission: 20-07-2023 Date of Acceptance: 30-07-2023

I. Introduction

From the day of independence, Nigeria and Nigerians have been looking for credible elections that would usher in democratic government. Different electoral commissions ranging from Federal Electoral Commission (FEDECO) to National electoral Commission (NEC) and Independent Electoral Commission (INEC) were constituted and all efforts were made to have credible elections. According to Yusuf (2015), election is one of the most essential ingredients of democracy, its conduct has remained a challenge to democratic governance not only in Nigeria but also almost all over the world. Elections in Nigeria have historically been conflict ridden (Olanrewaju, 2013). To solve the challenges facing the conduct of free and fair elections, our election umpires ran from option A4 to Open ballot, to Card Reader Machine (CRM) and introduction of BVAS by Independent National Electoral Commission introduced the Bimodal Voter Accreditation System (BVAS) as a way of fighting electoral malpractices 2021. BVAS was designed in such a way that it can verify permanent voters' cards and enable human recognition through biometric verification process. This biometric process could be through facial and fingerprint verifications.

Its' focal point is the verification of voter's card and authentication of voter during accreditation. It is not to stress so much but it is a common knowledge that in the area of authentication that biometric authentication is mostly preferred and closely knitted in terms of security. This is not to say that biometric authentication has no defects.

II. Review of Related Literature.

According to Promontory Financial Group: Washington, (2017) authentication is defined as the process of verifying the user 's claimed identity by comparing the data received from an individual with those stored in the database to attest whether the person is who they claim to be. Authentication can also be said to be a process whereby a ones' claimed identities are verified successfully by comparing it with what is already stored, aimed at providing the participants with a maximum conviction that identities of each participant is known to each other. According Boyd (2013) authentication remains a fundamental safeguard against illegitimate access to the electronics device or any other sensitive application, whether offline or online. This is what ensures the security of users while using the digital devices. In information and data security, identification is the communication of an element to an information system (IS). Authentication represents one of the most promising ways concerning trust and security enhancement for commercial applications and denotes a property of ensuring the identity of the previously mentioned entities (Kotzanikolaou, 2007). These underscores while the Nigeria electoral umpire took

to digital authentication through the use of BVAS. Guma *et al.*, (2020) summarized in their research that the main mechanisms that are available to authenticate individuals with established credentials are as follows: Something you know (knowledge factor) such as a password, personal identification number (PIN), and an answer to a security question. Something you have (ownership factor) such as security token, subscriber identity module (SIM) card, one-time password (OTP) token, employee access card. Something you are (biometric factor) such as biometric fingerprint, face, iris, retina, voice, gait, keystroke dynamics, gaze gestures, signature, deoxyribonucleic acid (DNA). Below is the classification of biometric authentication according to the Kodituwakku, (2007)

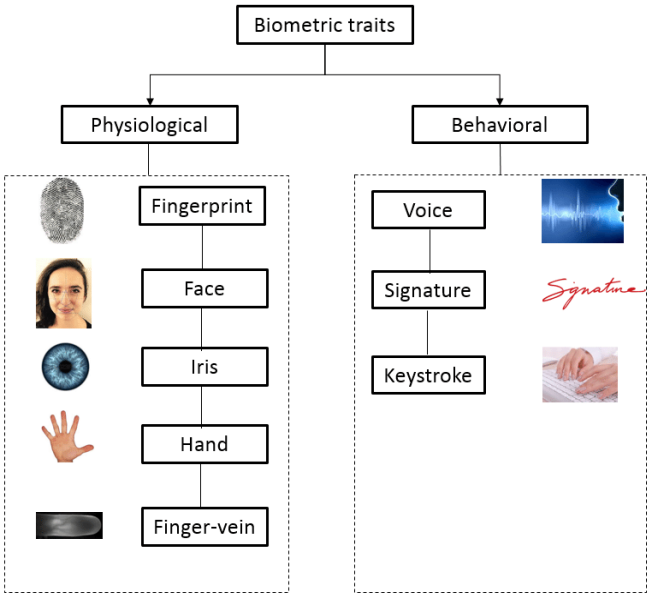

Figure 1: Classification of Biometrics Source Biometric authentication: A review

From the above figure, one can clearly say that biometric verification is divided into two-the physiological which has to do with our bodily parts and the behavioral which has to with our reactions to stimulus.

The research conducted by Shena and Shena in (2014) as summarized in table 1discussed different biometric technologies under five best acceptable criteria.

Table 1 Comparison of different biometric technologies

Characteristic	Face	FP	Voice/Speech	Hand	Iris	Signature
Ease of Use	Medium/High	High	High	High	Medium/High	High
Accuracy	Medium	High	Medium	Medium	High	Medium/High
Acceptability	High	Medium	High	Medium/High	Medium/High	High
Security	Medium	High	Medium	Medium	High	Medium/High
Permanence	Medium	High	Medium/High	Medium/High	High	Medium/High

Source: Multimodal Biometric System Sheena and Sheena (2014)

To allude to why INEC decided to use facial or fingerprint verification for BVAS, the analysis below will assist on unveiling them:

i. **Voice recognition:** Voice verification simply applies when the system uses smart senses to recognize and authenticate the customer. Although the voice recognition is agreed that is not prune to brute force or other forms of security breaches but it has many drawbacks ranging from one's state of health and environmental influences like anger and other emotions and human developmental changes. Today we have many individuals who can mimic people and animals perfectly. It is possible to have a sensor that mimics the voice of a customer (Hautamäki, *et al*, 2015) and thereby giving access to a wrong customer.

ii. **Facial recognition**: The facial recognition for authentication is also another biometric authentication employed to have access to digital applications. The system uses three dimensional pictures stored in the system to authenticate the user. One drawback of this type is the identical twin issue and culture and religion where women are not allowed to open their faces. However, this type of verification is easy, accessible and since voter registration is updated before any election it is possible to update any facial changes due to age and other human development. These are the reasons why INEC chose to use facial recognition.

iii. **Fingerprints:** The human fingers have underlying lines that make each finger unique and peculiar to a user. Jain *et al* (2006) and Maltoni, *et al* (2009), all agreed that although its usability is easy. According De Luca et *al*, (2015) one drawback of the fingerprint authentication is that the integration is very high. Another challenge in finger print is the finger mismatch. Instances were one of the fingers were not authenticated abound. This makes access difficult and sometimes impossible. Also, some natural occurrences like accidents can distort authentication where a user loses one of more of the fingers. However, due to its accessibility and permanence in nature, INEC found it one of the best ways to verify user.

iv. Iris or Ocular Recognition: The iris or ocular recognition is complex mathematical computation that is required to analyze the image and also the high-quality device that is required for the type of authentication concluded (Bowyer & Burge,2016). The advantage of the iris is that each human being has a unique own even identical twin, their iris is different (Sheethal, 2011). However, INEC wouldn't have applied this in elections because of its complexities and judging also that most of the workers are mere ad hoc staff and people who barely knows how to operate a technological device.

v. Hand Geometry recognition: In this type of authentication, the individual's hand is captured using a camera or scanner and then it is extracted into a measurable template. It may also be complex to capture since it involves finger lengths, palm thickness and diameter. Also, a defect in any of the fingers may disenfranchise an individual and hence not the best verification mechanism for an election which is time bound.

From the above analysis, it is evident that the INEC chose the two biometric verifications for two reasons of:

I. Every voter must be a human and so should have a face of ginger print.

II. It is easy to administer since as a common means of biometric authentication.

Other behavioral biometric verification could not be considered because like signature it requires a level of literacy and it is also not easy to get exact signatures all the time and this can disenfranchise voters at the point of voting. Key stroke like signature also has the same challenges and hence could not be considered for verification of voters during accreditation.

III. BVAS: Security and Breaches.

The Bimodal Verification Accreditation System has the server and the client end which is where the operators operate on. Looking at the schema in Figure 2, it is clear there are three points of likely failures or breaches-the server, the network and the client end.

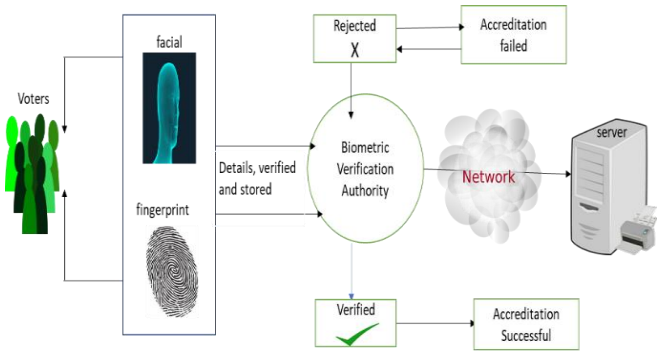

Figure 2: Schema for the Bimodal Verification Accreditation System

Security breaches of BVAS could take place at the following ends:

The Client/Operator end:

This is the interface where the operator uses. The security breaches can occur in the following ways:

a. **Misuse of access privileges:** A compromised operator with access privileges can misuse their access to gain unauthorized access to restricted areas or swap information or approve an authentication even when it is not validated.

b. **Tampering with biometric data:** An operator can tamper with biometric data by deleting biometric data on the BVAS therefore disenfranchising genuine voters. This is a form of denial of service.

c. **Physical compromise of biometric sensors:** This is a typical connivance where an operator can physically allow and expert user to install sensors to allow unauthorized access or compromise biometric sensors and to gain access to the biometric data. For example, an operator can install a fake sensor or bypass the sensor altogether. This can also be done, and the system will be misled to verify even incorrect biometric information.

The Server End:
The server end contains the database and the biometric verifications application. The security of the data could be compromised by the server administrator in some many ways which include the followings:

a. Unauthorized access: An administrator having unauthorized access to the database when compromised can transpose, modify or delete data to influence a particular outcome.

b. Data theft: Data theft is common practice especially when there is no dual control on login and no established checks and balances. Theft enables an administrator to copy data and sell for money, and this can be presented in a manner that an unauthorized person can have access and manipulate the data.

c. Data tampering: Biometric data can be tampered with by the administrator especially when established policies and procedures are not followed to track the changes made to the database and to get the logs and establish when and who did anything.

d. Weak security practices: Unsecured or weakly secured BVAS or the server can be a bigger problem. When a system is not secured adequately, it becomes vulnerable and is open to hackers. Administrators may inadvertently leave the server exposed, or they may not follow best practices for security, such as using strong passwords, keeping software up to date, or restricting access to the server.

Network Point
This is the third failure point of the BVAS. The Client connects to the server through a wireless access or even in some cases on standalone and connects back when network is achieved. The open connection makes the integrity of the data doubtful. This is because the data could be compromised in several ways through an open and wireless connection which is not administered by anyone. The following are the security breaches that can occur.

i. **Network interception**: There can be interception when the protocol is open and not secure. Such intercept can come in form of Man in the Middle Attack- where a user is verified without knowing that an intruder has gained access by masquerading as a legitimate user in each session, Oracle attack: this attack is where an intruder masquerades as either of the participants and gains access to start a new communication as a legitimate participant, phishing, replay and eavesdropping
ii. **Exploiting vulnerabilities:** A network administrator could exploit a known vulnerability in the server's operating system or software to gain control of the system to the data base and reconfigure the verification rule either denying service to genuine voters or verifying the wrong people. This could be used to verify every voter especially area where a candidate is strong and deny voters at a place where a candidate is not popular.
iii. **Weak network security:** If the network is not adequately secured, it may be vulnerable to attacks by hackers or other malicious actors. A network administrator may inadvertently leave the network exposed, or they may not follow best practices for security, such as using strong passwords, keeping software up to date, or restricting access to the network.
iv. **Insider Attack:** This includes all those in the network team who have one kind of access to the network and can intentionally or unintentionally delete data. This will affect the security and verification of voters on BVAS.

IV. Proposed Solutions

The solutions will be taken from the perspective of the breaches. For instance, currently, the BVAS does not have a tamper alert. There should be a tampered alert system which will trigger an alert to the system administrator in INEC-both hardware and software administrators to alert them once the system is opened or a foreign device is inserted. This will check the reconfiguration of the sensors to make it behave abnormal and accept data which it was not supposed to accept or reject data it was supposed to accept.

a. every configuration both at the client side or server end, there must be a two-step authentication – a maker and a checker. This will ensure that no single individual has the right over the BVAS machine.
b. For any reason that an alert system is received from a client, the data will be rejected because it is compromised.
a. Since some locations do not have telecommunications presence, INEC should have a way of comparing data captured, accredited, and verified for voting to what is in the machine. This could be done by setting a status flag to raise a flag of disparity once the machine comes to a network area to upload. The set flag should be set to that once the client is on the network it compares the data on the client to what is on the server and flags a reject when the data integrity is compromised.
b. On the server end, a multifactor authentication level with the good protocol should be implemented and complete separation of duties should be employed here to avoid having a sole access to the server and without compromise. Here we recommend Kerberos protocol which according to (Anbu Malar & Prabhu, 2021)), is one of the authentication protocol designs with a Trusted Third party (TTP) known as Kerberos Authentication Server (KAS). It has its major target as safeguarding the sensitive information of its' users by

maintaining a cache, where the Ticket Granting Ticket (TGT) confirms the usage status of the authenticator to avert a replay attack. If this authentication protocol is implemented on the server communication, the issues of hacking will be a thing of the past or at least reduced to an acceptable low level.

c. Most importantly is the integrity of the ad hoc INEC staff who operate the machines during election. INEC should evaluate the integrity of the staff used for this type of election to ensure that right from onset the wrong people are not hired to do the job which has impact on the nation and inhabitants.

V. Conclusions

Election is as very important as governance. Democracy and good governance are built around free, fair and credible elections. There are many layers on the process down to the voters who are supposed to be the appropriate deciders of who wins the election and who governs. Now that technology has been deployed, it will be good that the process of implementation of the technology driven process be safe and secure to elucidate trust from voters. This can only be done when the technology is safe and secure and without compromise.

References:

[1]. Ali, Guma, Mussa Ally Dida, And Anael Elikana Sam. (2020). "Two-Factor Authentication Scheme For Mobile Money: A Review Of Threat Models And Countermeasures" *Future Internet* 12, No. 10: 160. Https://Doi.Org/10.3390/Fi12100160

[2]. Anbu Malar, M. B. B., & Prabhu, J. (2021). Trust Based Authentication Scheme (Tbas) For Cloud Computing Environment With Kerberos Protocol Using Distributed Controller And Prevention Attack. International Journal Of Pervasive Computing And Communications, 17(1), 78–88. Https://Doi.Org/10.1108/IJPCC-03-2020-0009

[3]. Bowyer, K.W., And Burge, M.J. (2016) Handbook Of Iris Recognition; Springer: Berlin, Germany

[4]. De Luca, A.; Lindqvist, J. (2015) : Is Secure And Usable Smartphone Authentication Asking Too Much? Computer2015,48, 64–68.

[5]. Ellison, N. B. & Boyd, D. (2013). Sociality Through Social Network Sites. In Dutton, W. H. (Ed.), The Oxford Handbook Of Internet Studies. Oxford: Oxford University Press, Pp. 151-172.

[6]. Hautamäki, R.G.; Kinnunen, T.; Hautamäki, V And Laukkanen, A.M.(2015) Automatic Versus Human Speaker Verification: The Case Of Voice Mimicry.Speech Commun.2015,72, 13–31.

[7]. Kodituwakku S. (2015): "Biometric Authentication: A Review," International Journal Of Trend In Research And Development, Vol. 2, Pp. 2394-9333,

[8]. Kotzanikolaou, C. D. (2007) Network Security Current Status And Future Directions, Chapter Computer Network Security: Basic Background And Current Issues. 2007,Trondheim, Norwa

[9]. Jain, A.; Bolle, R.; And Pankanti, S. (2006) Biometrics: Personal Identification In Networked Society; Springer: Berlin,Germany, 2006; Volume 479.

[10]. Maltoni, D.; Maio, D.; Jain, A.; Prabhakar, S.Handbook Of Fingerprint Recognition; Springer: Berlin,Germany, 2009.

[11]. Olanrewaju Fagbohun, (2013) : Nigeria's Democracy And The Crisis Of Political Instability: An Audit Of The Electoral System. Lagos Nigeria

[12]. Promontory. Biometric Authentication In Payments: Considerations For Policymakers; Promontory Financial Group: Washington, DC, USA, 2017. [Google Scholar]

[13]. Sheena S, And Sheena Mathew: (2014): A Study Of Multimodal Biometric System IJRET: International Journal Of Research In Engineering And Technology Eissn: 2319-1163 | Pissn: 2321-730, India.

[14]. Sheethal R. (2011) : ATM Card Authentication With Hardened Retina Based Fuzzy Vault For Highest Level Of Security: International Journal Of Advanced Research In Computer Science, Vol 2, No 6 (2011)

[15]. Yusuf Isma'ila And Zaheruddin Othman (2015): Challenges Of Electoral Processes In Nigeria's Quest For Democratic Governance In The Fourth Republic: Research On Humanities And Social Sciences Www.Iiste.Org ISSN (Paper)2224-5766 ISSN (Online), Kedah,Universiti Utara, Malaysia