



JOURNAL OF PHILOSOPHY AND CONTEMPORARY ISSUES

Volume 2, Number 3 (July 2026)

ISSN: 1595-9457 (online); 3093-060X (print)

Website: <https://jppssuniuyo.com/jpci> Email: jppssuniuyo@gmail.com

Received: June 15, 2026 Accepted: July 29, 2026 Published: July 31, 2026

Citation: Yusufari, Adamu G. (2026). "Independent National Electoral Commission's Cybersecurity System and its Relevance in Curtailing Electoral Fraud in Nigeria." *Journal of Philosophy and Contemporary Issues*, 2 (3): 112-124.

Article

Open Access

INDEPENDENT NATIONAL ELECTORAL COMMISSION'S CYBERSECURITY SYSTEM AND ITS RELEVANCE IN CURTAILING ELECTORAL FRAUD IN NIGERIA

Adamu Gujungu Yusufari

Center for Peace and Security Studies, Modibbo Adama University, Yola, Nigeria

Corresponding Email: adamugujunguyusufari@gmail.com

Abstract

This study examined the Independent National Electoral Commission's (INEC) cybersecurity system and its relevance in curtailing electoral fraud in Nigeria. The study was guided by three research objectives which focused on the cybersecurity measures adopted by INEC, the extent to which these measures have reduced electoral fraud, and their influence on public confidence in the credibility of elections. A descriptive survey research design was adopted, and the population comprised electoral stakeholders including INEC officials, ICT personnel, security agencies, political party representatives, election observers, and registered voters. A sample of 286 respondents was drawn using stratified and simple random sampling techniques. Data were collected using a structured questionnaire and analyzed using mean and standard deviation. The findings revealed that INEC has adopted several cybersecurity measures including biometric voter accreditation, electronic result transmission, encryption systems, firewall protection, password authentication, and collaboration with ICT security experts to safeguard electoral processes. The study further found that these cybersecurity systems have significantly reduced electoral fraud by minimizing multiple voting, voter impersonation, ballot stuffing, and manipulation of election results, although technical and infrastructural challenges still persist. In addition, the findings indicated that cybersecurity systems positively influence public confidence by enhancing transparency, accountability, and trust in electoral outcomes, despite occasional technical glitches that may affect perception. The study concluded that INEC's cybersecurity system plays a vital role in strengthening electoral integrity and democratic credibility in Nigeria. It recommended enhanced cybersecurity infrastructure, continuous capacity building for electoral personnel, and improved national digital infrastructure to support and secure an efficient electoral process.

Copyright © 2026 By JPCI. Publishers: Omega Books

This is an open access article which permits unrestricted use provided the work is properly cited.

Keywords: BVAS, Cybersecurity System, Electoral Fraud, Electoral Integrity, Electronic Voting Technology, INEC, Public Confidence, Nigeria.

Introduction

Elections constitute the fundamental mechanism through which citizens exercise their sovereign right to choose political representatives, and the credibility of electoral processes remains indispensable to democratic consolidation. In Nigeria, Africa's most populous democracy, electoral administration has historically been undermined by pervasive fraud, including multiple voting, ballot stuffing, result manipulation, and voter impersonation (Nwangwu *et al.*, 2018). These malpractices have eroded public trust in democratic institutions and precipitated electoral violence, political instability, and a deepening legitimacy crisis (Ibeanu, 2016). Recognizing this existential threat, the Independent National Electoral Commission (INEC) has progressively integrated technology into the electoral value chain as a strategic response to curb malpractice and enhance electoral integrity. The journey toward technological intervention in Nigeria's electoral process began with the Direct Data Capture Machine for voter registration, followed by the Smart Card Reader (SCR) deployed in the 2015 general elections, which utilized biometric technology to verify Permanent Voter Cards and authenticate voters through fingerprint scans (Audu & Akuva, 2020). While the SCR represented significant improvement in addressing voter impersonation, its sole reliance on fingerprint verification proved problematic, with persistent reports of equipment failure and incomplete verification through the 2019 elections (Alebiosu, 2016). In response, INEC unveiled the Bimodal Voter Accreditation System (BVAS) in 2022, combining fingerprint verification with facial recognition technology, alongside the INEC Result Viewing Portal (IREV), designed for real-time electronic transmission and public viewing of polling unit results (Sibe & Kaunert, 2023). These innovations were institutionalized by the Electoral Act of 2022, which empowered INEC to deploy any technology deemed appropriate, providing a legal framework for electoral digitization (INEC, 2022).

The deployment of BVAS and IREV in the 2023 general elections marked a watershed moment, generating unprecedented public optimism that technology would deliver credible, transparent elections. The BVAS was deployed to over 176,000 polling units nationwide, promising to eliminate ghost voting and prevent over-voting (International IDEA, 2022). Simultaneously, the IREV portal was designed as a public repository allowing citizens, political parties, and observers to access polling unit results in real-time, creating a transparent audit trail (Ogundare *et al.*, 2025). These interventions were perceived as a progressive shift toward transparent election management that would restore public confidence in democratic institutions (Sibe & Kaunert, 2023). However, implementation revealed a troubling reality demanding scholarly interrogation. Despite institutional investment in electoral technology, the elections were marred by significant technical failures, inconsistent data transmission, and selective application of technology across geopolitical zones, reigniting fears about electoral malpractice (Ogundare *et al.*, 2025). The IREV portal experienced inexplicable delays, with some presidential results only becoming public three days after polls closed, severely undermining promised transparency (Sibe & Kaunert, 2023). The European Union Election Observation Mission (2023) noted failures with electronic transmission of results, while Yiaga Africa (2023) reported that significant delays in uploading presidential results raised fundamental questions about integrity, eroding public trust.

More alarming was the scale of cyber threats targeting Nigeria's electoral infrastructure. The Minister of Communications and Digital Economy reported 12,988,978 cyberattacks directed at INEC's servers and portals during the election period, peaking at 6.99 million on election day (Sibe & Kaunert, 2023). These attacks included Distributed Denial of Service assaults, brute force injection attempts, and path traversal, originating from both domestic and international sources. Prior attacks on INEC's portals during the 2022 Osun and Ekiti gubernatorial elections, traced to Asia, foreshadowed the 2023 onslaught (Sibe & Kaunert, 2023). These developments exposed the fragile intersection between electoral credibility and national cybersecurity, underscoring that digitization opens dangerous vulnerabilities exploitable by cybercriminals and external interests to delegitimize institutions and incite unrest (Oladele, 2025). The cybersecurity challenges are compounded by Nigeria's broader digital vulnerability. The International Telecommunication Union (2020) ranked Nigeria 47th globally in cybersecurity readiness. Combined with INEC's management of personally identifiable information for approximately 96 million registered voters, this creates fertile ground for data breaches and database manipulation (Sibe & Kaunert, 2023). The absence of a comprehensive cybersecurity framework for electoral infrastructure, lack of in-house digital forensic capability, and over-reliance on third-party vendors render the system susceptible to sophisticated exploitation. The consequences extend beyond elections. Where citizens perceive outcomes as manipulated or compromised by external interference, state legitimacy is undermined, heightening risks of civil unrest and voter apathy (Oladele, 2025). This validates the proposition that election credibility in fragile democracies depends on public perception of technological impartiality and institutional resilience (Ogundare *et al.*, 2025). Against this backdrop, examining INEC's cybersecurity system and its relevance in curtailing electoral fraud became urgent.

Statement of the Problem

Despite the introduction of digital technologies and electronic systems by the Independent National Electoral Commission to improve the credibility, transparency, and efficiency of elections in Nigeria, electoral fraud continues to pose serious challenges to the democratic process. Incidents such as hacking attempts, manipulation of voter databases, unauthorized access to electoral information systems, cyberattacks on electronic transmission platforms, identity theft, and misinformation campaigns have raised concerns about the adequacy and effectiveness of the Commission's cybersecurity infrastructure. Although the deployment of technologies such as the Bimodal Voter Accreditation System (BVAS) and the INEC Result Viewing Portal (IReV) was intended to reduce electoral malpractice, reports of technical glitches, system vulnerabilities, and allegations of digital manipulation during recent elections have undermined public trust in the electoral process. Furthermore, there is limited empirical evidence on the extent to which INEC's cybersecurity measures have contributed to curtailing electoral fraud and safeguarding electoral integrity in Nigeria. It is against this background that this study seeks to examine the relevance of the cybersecurity system of the Independent National Electoral Commission in curtailing electoral fraud in Nigeria.

Objectives of the Study

The main objective of this study is to examine the relevance of the cybersecurity system of the Independent National Electoral Commission in curtailing electoral fraud in Nigeria. Specifically, the study sought to:

- i. examine the cybersecurity measures adopted by INEC to safeguard electoral processes in Nigeria.
- ii. determine the extent to which INEC's cybersecurity system has reduced electoral fraud during elections in Nigeria.
- iii. examine the influence of cybersecurity systems on public confidence in the credibility of elections in Nigeria.

Research Questions

The following research questions guided the study:

- i. What cybersecurity measures have been adopted by INEC to safeguard electoral processes in Nigeria?
- ii. To what extent has INEC's cybersecurity system reduced electoral fraud during elections in Nigeria?
- iii. How does the cybersecurity system influence public confidence in the credibility of elections in Nigeria?

Literature Review

Conceptual Framework - Electoral Fraud and Electoral Integrity: Electoral fraud encompasses a broad spectrum of illegal activities designed to manipulate electoral outcomes, including multiple voting, ballot stuffing, voter impersonation, result falsification, and vote buying (Nwangwu *et al.*, 2018). In the Nigerian context, electoral fraud has been described as endemic, with scholars documenting its systematic deployment by political actors to capture state power (Omotola, 2009; Ibeanu, 2016). Electoral integrity, conversely, refers to the degree to which elections meet international standards of universal suffrage, ballot secrecy, and impartial administration (Norris, 2014). The relationship between these concepts is dialectical: where electoral fraud proliferates, electoral integrity erodes, and democratic legitimacy collapses. Cheeseman *et al.*, (2018) argued that the global adoption of electoral technology has been driven precisely by the need to bridge this gap between fraudulent practice and democratic ideal, though outcomes remain context-dependent.

Electoral Technology and Democratic Governance: The scholarly discourse on electoral technology has expanded significantly over the past two decades. Alvarez and Hall (2008) provided foundational analysis of electronic voting systems, identifying both their potential to enhance transparency and their vulnerability to technical failure and manipulation. In the African context, Cheeseman *et al.*, (2018) examined the deployment of biometric technology across the continent, noting that approximately half of all national elections now employ some form of digital intervention in voter registration, verification, or result transmission. Their analysis cautioned that technology is not a panacea; its effectiveness depends on institutional capacity, political will, and the broader electoral environment. Norris (2014) advanced the proposition that electoral integrity is multidimensional, encompassing electoral procedures, campaign media, party and candidate regulations, voter registration, and vote count. Within this framework, technology operates as an intervening variable that can strengthen or weaken integrity depending on implementation quality. This perspective is particularly relevant to Nigeria, where technological interventions have produced mixed results across successive electoral cycles (Sibe, 2015; Alebiosu, 2016).

Technology in Nigerian Elections: From SCR to BVAS

The trajectory of electoral technology in Nigeria has been extensively documented. The 2015 general elections marked the first large-scale deployment of the Smart Card Reader (SCR), a

biometric device designed to authenticate voters through fingerprint verification and PVC validation. Alebiosu (2016) documented that the SCR was introduced to prevent electoral fraud, allow votes to count, reduce litigation, and ensure transparency. Enwere and Ladan-Baki (2015) argued that the Smart Card Reader addressed rigging and multiple voting, while Agbu (2016) posited that technology in the 2015 elections made electoral figure manipulation difficult, citing transparency as an essential feature of credible elections. However, the SCR deployment was not without challenges. Alebiosu (2016) noted that all five biometric card readers deployed to the serving president's unit failed during the 2015 elections. Sibe (2015) documented a 41% failure rate in the pilot test of the Smart Card Reader technology, arguing this was too significant to ignore, yet INEC proceeded with national deployment. Audu and Akuva (2020) identified additional challenges including inadequate knowledge of device operation, lack of proper sensitization by INEC, and inability of the device to authenticate PVCs and verify biometric data in some polling units. Despite these shortcomings, they concluded that digital technology achieved transparency, fairness, and credibility in the 2015 and 2019 elections. The transition from SCR to BVAS represented a significant technological leap. Sibe and Kaunert (2023) described the BVAS as an all-in-one multifunctional integrated device serving multiple functions: verification of PVC authenticity, fingerprint and facial recognition authentication, and transmission of unit results to the IReV portal. The device was also used as the INEC voter enrolment device during voter registration. The two-factor verification option was expected to eliminate the use of incident forms that plagued previous elections. However, Odalonu and Ogu (2022) reported "severe challenges" with BVAS in the Anambra governorship elections, while the Transition Monitoring Group urged INEC to fix identified problems before the 2023 elections (Ileyemi, 2021).

Cybersecurity and Electoral Infrastructure

The cybersecurity dimension of electoral technology has emerged as a critical area of scholarly concern. Yavuz et al. (2018) emphasized the need to install necessary controls to mitigate cybersecurity risks and privacy concerns in voting systems. Springall et al. (2014) identified procedural and architectural weaknesses in Estonia's internet voting system, arguing that its simplistic model conferred trust on the integrity of voters' computers, server components, and election staff rather than technical verification. Nurse et al. (2017) noted that various concerns raised suggest vulnerabilities that malicious insiders and sophisticated external attackers may capitalize on to compromise voting systems. In the Nigerian context, Sibe and Kaunert (2023) provided the most comprehensive analysis of cybersecurity threats to electoral infrastructure. They document the 2015 defacement of the INEC website by the Nigerian Cyber Army, cyberattacks on the IReV during the 2022 Osun and Ekiti gubernatorial elections originating from Asia, and the 12,988,978 cyberattacks during the 2023 presidential election. The authors identify critical vulnerabilities including cross-border jurisdictional complexities, forensic readiness gaps in the justice system, and data protection challenges arising from INEC's management of 96 million voter records containing personally identifiable information. Oladele (2025) extended this analysis by applying securitization theory and democratic legitimacy theory to examine how compromised electoral technology becomes a driver of systemic distrust and insecurity. The study argues that insecure or poorly governed electoral technology can erode democratic legitimacy, trigger post-election violence, and deepen political instability. This finding aligns with Germann's (2023) broader argument that the security and transparency of electoral technology are procedural components that directly influence voter trust and political behavior.

The 2023 Elections: Performance and Critique

The 2023 general elections have generated substantial scholarly analysis. Ogundare *et al.*, (2025) examined the interplay between the Electoral Act 2022, BVAS, and IReV, arguing that while technological innovations represented a monumental leap toward electoral integrity in theory, implementation was undermined by systemic challenges including logistical failures, deliberate sabotage, and a resilient "culture of impunity" among political actors. Their findings demonstrate that technology alone is insufficient to guarantee credible elections without concomitant political will, robust institutional capacity, and societal commitment to democratic norms. The European Union Election Observation Mission (2023) corroborated these concerns, noting that while BVAS and IReV raised citizens' hopes, election day failures with electronic transmission of results, particularly for the presidential election, represented a missed opportunity to improve trust and confidence. Yiaga Africa (2023) reported that significant delays in uploading presidential results on the IReV eroded public trust, while the Commonwealth Election Observer Group (2023) confirmed that results were not uploaded in real-time as advertised. These observations collectively underscore the gap between technological promise and practical performance.

Gaps in the Literature

Despite the growing body of scholarship on electoral technology in Nigeria, significant gaps persist. First, most studies focus on the administrative and legal dimensions of BVAS and IReV deployment, with limited attention to the cybersecurity architecture protecting these systems. Second, the intersection between electoral cybersecurity and national security remains under-theorized, particularly regarding how cyber threats to electoral infrastructure can destabilize democratic governance. Third, few studies have systematically evaluated INEC's cybersecurity readiness using established frameworks for critical infrastructure protection. This study addresses these gaps by examining INEC's cybersecurity system and its relevance in curtailing electoral fraud, thereby contributing to both theoretical understanding and policy formulation.

Methodology

This study adopted a descriptive survey research design to investigate the relevance of the Independent National Electoral Commission's (INEC) cybersecurity system in curtailing electoral fraud in Nigeria. The descriptive survey design was considered appropriate because it enabled the researcher to obtain opinions and responses from respondents regarding the effectiveness, challenges, and relevance of cybersecurity measures in the electoral process. The study was conducted in Nigeria, focusing on selected stakeholders involved in electoral administration and democratic governance. The population of the study comprised INEC officials, ICT personnel, security agencies, political party representatives, election observers, and registered voters in selected states in Nigeria. A total population of 1,250 respondents was identified for the study. A sample size of 300 respondents was selected using stratified random sampling and simple random sampling techniques to ensure adequate representation of the different categories of respondents. The instrument used for data collection was a structured questionnaire titled "INEC Cybersecurity System and Electoral Fraud Questionnaire (ICSEFQ)." The questionnaire was divided into two sections. Section A elicited information on the demographic characteristics of the respondents, while Section B contained items related to cybersecurity measures, electoral fraud reduction, implementation challenges, public confidence, and improvement strategies. The items were structured on a four-point Likert scale of Strongly Agree (SA), Agree (A), Disagree (D), and

Strongly Disagree (SD). The instrument was validated by three experts in Measurement and Evaluation, Educational Technology, and Political Science from recognized universities in Nigeria to ensure content and face validity. Their observations and corrections were incorporated into the final draft of the instrument. The reliability of the instrument was determined through a pilot study conducted outside the study area using 30 respondents who were not part of the main study. Data collected from the pilot study were analyzed using Cronbach Alpha reliability statistics, which yielded a reliability coefficient of 0.82, indicating that the instrument was reliable for the study. Data were collected by the researcher with the assistance of trained research assistants. The questionnaires were administered directly to the respondents and retrieved after completion. Out of the 300 questionnaires distributed, 286 were properly completed and returned, representing a 95.33% of administered questionnaires. The data collected were analyzed using mean and standard deviation to answer the research questions. A criterion mean of 2.50 was used as the benchmark for decision making. Any item with a mean score of 2.50 and above was regarded as agreed, while items below 2.50 were regarded as disagreed.

Results

Cybersecurity Measures Have Been Adopted by INEC to Safeguard Electoral Processes in Nigeria

Table 1: Respondents Rating on Cybersecurity Measures Adopted by INEC to Safeguard Electoral Processes in Nigeria (N= 286)

S/N	Adopted Measures	SD	D	A	SA	$\bar{x}$	Std	Remark
1	INEC uses the Bimodal Voter Accreditation System (BVAS) to verify voters during elections.	34 (11.9%)	58 (20.3%)	102 (35.7%)	92 (32.2%)	2.88	1.00	Agree
2	INEC adopts electronic transmission of election results through the IReV portal.	36 (12.6%)	56 (19.6%)	100 (35.0%)	94 (32.9%)	2.88	1.02	Agree
3	Password authentication systems are used to secure electoral information.	40 (14.0%)	62 (21.7%)	97 (33.9%)	87 (30.4%)	2.81	1.06	Agree
4	INEC uses encryption systems to protect electoral databases from cyber threats.	38 (13.3%)	64 (22.4%)	96 (33.6%)	88 (30.8%)	2.82	1.05	Agree
5	Firewall and network security systems are employed to prevent unauthorized access.	42 (14.7%)	66 (23.1%)	95 (33.2%)	83 (29.0%)	2.76	1.09	Agree
6	INEC collaborates with ICT experts and security agencies to strengthen cybersecurity.	35 (12.2%)	60 (21.0%)	99 (34.6%)	92 (32.2%)	2.87	1.01	Agree
7	Regular monitoring of electoral systems is carried out to detect cyberattacks.	39 (13.6%)	63 (22.0%)	98 (34.3%)	86 (30.1%)	2.80	1.06	Agree
8	INEC provides cybersecurity training for electoral officials and ICT personnel.	44 (15.4%)	69 (24.1%)	92 (32.2%)	81 (28.3%)	2.73	1.11	Agree
9	Digital backup systems are used to prevent loss of electoral data.	41 (14.3%)	65 (22.7%)	96 (33.6%)	84 (29.4%)	2.78	1.08	Agree
10	Cybersecurity measures have improved the security of Nigeria's electoral process.	37 (12.9%)	59 (20.6%)	101 (35.3%)	89 (31.1%)	2.85	1.03	Agree

	Cluster Mean					2.82	1.05	Agree
--	---------------------	--	--	--	--	-------------	-------------	--------------

Note: SD = Strongly Disagree, D = Disagree, A = Agree, SA = Strongly Agree, $\bar{x}$ = Mean Response, Std = Standard Deviation.

Table 1 shows the mean responses on cybersecurity measures adopted by INEC to safeguard electoral processes in Nigeria. The results reveal that all the items fall within the mean range of 2.73 to 2.88, indicating agreement among respondents on the adoption of these cybersecurity mechanisms. The findings indicate that INEC utilizes BVAS for voter accreditation, electronic transmission of results through the IReV portal, password authentication systems, encryption technologies, firewall protection, collaboration with ICT experts, regular system monitoring, cybersecurity training, and digital backup systems to secure electoral processes. The cluster mean of 2.82 confirms the respondents' overall agreement that INEC has adopted several cybersecurity measures to strengthen electoral security and transparency in Nigeria.

INEC's Cybersecurity System and Reduction Electoral Fraud During Elections in Nigeria

Table 2: Respondents Rating on the Extent INEC's Cybersecurity System has Reduced Electoral Fraud in Nigeria (N=286)

S/N	Cybersecurity System	SD	D	A	SA	$\bar{x}$	Std	Remark
1	BVAS has reduced cases of multiple voting during elections.	32 (11.2%)	54 (18.9%)	104 (36.4%)	96 (33.6%)	2.92	0.98	Agree
2	The cybersecurity system has minimized voter impersonation during elections.	35 (12.2%)	58 (20.3%)	101 (35.3%)	92 (32.2%)	2.87	1.01	Agree
3	Electronic transmission of results has reduced manipulation of election outcomes.	38 (13.3%)	61 (21.3%)	98 (34.3%)	89 (31.1%)	2.83	1.04	Agree
4	Cybersecurity systems have enhanced transparency in election result collation.	36 (12.6%)	60 (21.0%)	100 (35.0%)	90 (31.5%)	2.85	1.03	Agree
5	The use of digital technologies has reduced ballot stuffing in elections.	40 (14.0%)	64 (22.4%)	97 (33.9%)	85 (29.7%)	2.79	1.07	Agree
6	Cybersecurity measures have reduced incidents of electoral malpractice.	37 (12.9%)	62 (21.7%)	99 (34.6%)	88 (30.8%)	2.83	1.04	Agree
7	Technical glitches still affect the effectiveness of INEC's cybersecurity system.	34 (11.9%)	57 (19.9%)	103 (36.0%)	92 (32.2%)	2.89	1.00	Agree
8	Network failures limit the effectiveness of electronic electoral systems.	36 (12.6%)	59 (20.6%)	101 (35.3%)	90 (31.5%)	2.86	1.02	Agree
9	Cybersecurity systems have not completely eliminated electoral fraud in Nigeria.	42 (14.7%)	67 (23.4%)	95 (33.2%)	82 (28.7%)	2.75	1.10	Agree
10	INEC's cybersecurity measures have improved the credibility of election outcomes.	33 (11.5%)	56 (19.6%)	103 (36.0%)	94 (32.9%)	2.90	0.99	Agree
	Cluster Mean					2.85	1.03	Agree

Note: SD = Strongly Disagree, D = Disagree, A = Agree, SA = Strongly Agree, $\bar{x}$ = Mean Response, Std = Standard Deviation.

Table 2 shows the mean responses on the extent to which INEC's cybersecurity system has reduced electoral fraud during elections in Nigeria. The results reveal that all the items fall within the mean range of 2.75 to 2.92, indicating agreement among respondents that cybersecurity systems have contributed to reducing electoral fraud. The findings indicate that BVAS has reduced multiple voting and voter impersonation, while electronic transmission of results has minimized result manipulation and enhanced transparency in election result collation. The study also revealed that cybersecurity measures have reduced ballot stuffing and other forms of electoral malpractice. However, respondents agreed that technical glitches and network failures still affect the effectiveness of these systems and that electoral fraud has not been completely eliminated. The cluster mean of 2.85 confirms the respondents' overall agreement that INEC's cybersecurity system has reduced electoral fraud in Nigeria to a considerable extent.

INEC Cybersecurity System and Public Confidence in the Credibility of Elections in Nigeria

Table 3: Respondents Rating on the Influence of Cybersecurity Systems on Public Confidence in the Credibility of Elections in Nigeria (N =286)

S/N	Cybersecurity System and Public Confidence	SD	D	A	SA	$\bar{x}$	Std	Remark
1	The use of BVAS has increased public trust in the electoral process.	33 (11.5%)	57 (19.9%)	102 (35.7%)	94 (32.9%)	2.90	0.99	Agree
2	Electronic result transmission enhances transparency in elections.	31 (10.8%)	55 (19.2%)	105 (36.7%)	95 (33.2%)	2.92	0.97	Agree
3	Availability of election results on the IReV portal improves public confidence.	35 (12.2%)	58 (20.3%)	101 (35.3%)	92 (32.2%)	2.87	1.01	Agree
4	Cybersecurity systems reduce suspicion of election result manipulation.	37 (12.9%)	61 (21.3%)	99 (34.6%)	89 (31.1%)	2.84	1.04	Agree
5	Digital technologies improve accountability in electoral processes.	36 (12.6%)	60 (21.0%)	100 (35.0%)	90 (31.5%)	2.85	1.03	Agree
6	Effective cybersecurity systems strengthen the credibility of elections.	32 (11.2%)	56 (19.6%)	103 (36.0%)	95 (33.2%)	2.91	0.98	Agree
7	Technical failures during elections reduce public confidence in INEC.	38 (13.3%)	63 (22.0%)	97 (33.9%)	88 (30.8%)	2.82	1.06	Agree
8	Delays in uploading election results negatively affect public trust.	40 (14.0%)	65 (22.7%)	96 (33.6%)	85 (29.7%)	2.79	1.07	Agree
9	Cybersecurity systems encourage citizens' participation in elections.	39 (13.6%)	62 (21.7%)	98 (34.3%)	87 (30.4%)	2.81	1.06	Agree
10	Public confidence in elections increases when electoral systems are secure.	34 (11.9%)	58 (20.3%)	101 (35.3%)	93 (32.5%)	2.89	1.00	Agree
	Cluster Mean					2.86	1.02	Agree

Note: SD = Strongly Disagree, D = Disagree, A = Agree, SA = Strongly Agree, $\bar{x}$ = Mean Response, Std = Standard Deviation.

Table 3 shows the mean responses on the influence of cybersecurity systems on public confidence in the credibility of elections in Nigeria. The results reveal that all the items fall within the mean range of 2.79 to 2.92, indicating agreement among respondents that cybersecurity systems positively influence public confidence in elections. The findings indicate that the use of BVAS, electronic transmission of election results, and the IReV portal enhance transparency, accountability, and trust in the electoral process. Respondents also agreed that secure electoral systems reduce suspicion of result manipulation and encourage citizens' participation in elections. The cluster mean of 2.86 confirms the respondents' overall agreement that cybersecurity systems significantly enhance the credibility of elections in Nigeria.

Discussion of Findings

The findings of the study revealed that the Independent National Electoral Commission (INEC) has adopted various cybersecurity measures to safeguard electoral processes in Nigeria. These measures include the use of the Bimodal Voter Accreditation System (BVAS), electronic transmission of election results through the IReV portal, password authentication systems, encryption technologies, firewall protection, regular monitoring of electoral systems, and collaboration with ICT experts and security agencies. The study further indicated that these digital mechanisms were introduced to strengthen transparency, improve electoral administration, and reduce vulnerabilities associated with manual electoral processes. The finding is in agreement with Audu and Akuva (2020), who observed that the introduction of smart card reader technology in Nigerian elections significantly improved voter verification and minimized irregularities associated with manual accreditation systems. According to Audu and Akuva, the deployment of digital electoral technologies enhanced the credibility of elections by reducing opportunities for identity manipulation and unlawful voting practices. In a related perspective, Sibe (2015) maintained that the integration of technological systems into Nigeria's electoral process represented a strategic effort toward improving transparency and administrative efficiency in elections. The author emphasized that the adoption of electronic devices and digital security measures contributed to modernizing electoral administration and reducing procedural weaknesses that often encouraged electoral malpractice. Similarly, Ogundare, Ikwuoma, and Afolabi (2025) explained that the 2023 Nigerian general elections witnessed significant technological reforms through the introduction of BVAS and IReV, which were aimed at strengthening electoral integrity and improving public trust in election outcomes. The authors further stressed that cybersecurity mechanisms became necessary because digital electoral systems are often exposed to threats such as hacking, unauthorized access, and data manipulation. This position aligns with the view of Nurse, Buckley, Legg, Goldsmith, Creese, Wright, and Whitty (2017), who argued that cybersecurity measures are essential in protecting digital infrastructures from malicious attacks and ensuring the reliability of electronic systems in modern societies. Therefore, the convergence of these scholarly positions supports the present finding that INEC's adoption of cybersecurity measures has become an important strategy for safeguarding electoral processes in Nigeria.

The findings of the study revealed that INEC's cybersecurity system has contributed significantly to reducing electoral fraud during elections in Nigeria. The study showed that the use of digital electoral technologies minimized incidents of multiple voting, voter impersonation, ballot stuffing, and manipulation of election results. The findings also indicated that electronic transmission of results enhanced transparency in result collation and improved the credibility of election outcomes. However, the study acknowledged that

technical glitches and network-related challenges still affect the complete effectiveness of the cybersecurity system in eliminating electoral fraud in Nigeria. The finding is in agreement with Nwangwu, Onah, and Ohi (2018), who asserted that electoral fraud has historically undermined democratic consolidation in Nigeria through practices such as vote manipulation, ballot snatching, and falsification of results. According to the authors, the introduction of digital technologies into the electoral process became necessary to address these persistent electoral malpractices and strengthen democratic governance. In support of this position, Oladele (2025) explained that the deployment of BVAS and IReV during the 2023 general elections improved transparency and limited opportunities for manipulation in the electoral process. The author emphasized that the use of biometric accreditation and electronic result transmission reduced human interference in result collation and contributed to enhancing electoral credibility. Likewise, Germann (2023) maintained that electronic voting technologies and secure digital electoral systems can improve the accuracy and integrity of elections by ensuring that votes are properly recorded and protected from interference. The study further noted that cybersecurity frameworks are essential in protecting electoral systems from manipulation and maintaining public confidence in democratic institutions. Furthermore, Sibe and Kaunert (2023) observed that although technological innovations in Nigeria's electoral process improved election management and transparency, issues such as cyber threats, poor network infrastructure, and technical failures continued to pose challenges to the effective implementation of these systems. This observation corresponds with the present study, which found that while cybersecurity systems have reduced electoral fraud to a large extent, operational and technological limitations still hinder the complete elimination of electoral malpractice in Nigeria. Consequently, the reviewed studies provide strong empirical support for the present finding.

The findings of the study indicated that cybersecurity systems positively influence public confidence in the credibility of elections in Nigeria. The study showed that the use of secure digital technologies such as BVAS and IReV enhanced transparency, accountability, and trust in the electoral process. The findings further indicated that the availability of election results on electronic platforms enabled citizens and stakeholders to verify outcomes independently, thereby reducing suspicion of manipulation and increasing confidence in electoral administration. Nevertheless, the study also revealed that technical failures and delays in uploading election results negatively affected public trust in some instances. The finding is in agreement with Omotola (2009), who stated that credible elections are fundamental to democratic consolidation because they strengthen citizens' confidence in governance and political institutions. According to Omotola, transparency and accountability in electoral administration are essential factors that determine public trust in democratic processes. In a similar vein, Oladele (2025) argued that technology-driven electoral systems such as BVAS and IReV improved public perception of electoral credibility during the Nigerian general elections by enhancing transparency and reducing opportunities for result alteration. The author further maintained that the protection of electoral technologies through cybersecurity frameworks was necessary for sustaining public confidence in elections. Supporting this position, Germann (2023) explained that secure electronic voting systems can improve voters' trust in election outcomes when adequate cybersecurity measures are implemented to protect electoral data and voting processes from interference. The study emphasized that public confidence in elections increases when citizens perceive electoral systems as secure, transparent, and resistant to fraud. Furthermore, Sibe and Kaunert (2023) observed that despite the benefits of technological innovations in elections,

technical glitches and cyber vulnerabilities may negatively affect public perception if not properly managed. This observation aligns with the present study, which found that failures in digital electoral systems could reduce trust in electoral institutions. Therefore, the reviewed studies support the present finding that effective cybersecurity systems contribute significantly to improving public confidence in the credibility of elections in Nigeria.

Conclusion

The study concluded that the cybersecurity system of the Independent National Electoral Commission (INEC) plays a significant role in curtailing electoral fraud and enhancing the credibility of elections in Nigeria. The findings established that the adoption of digital electoral technologies such as the Bimodal Voter Accreditation System (BVAS), the INEC Result Viewing Portal (IREV), encryption systems, and other cybersecurity mechanisms has improved transparency, accountability, and security in the electoral process. The study further revealed that these technologies have reduced incidents of multiple voting, voter impersonation, ballot stuffing, and manipulation of election results, thereby strengthening public confidence in electoral outcomes. However, the study also concluded that challenges such as technical glitches, inadequate network infrastructure, cyber threats, and operational limitations still affect the full effectiveness of the cybersecurity system. Therefore, the study emphasized the need for continuous improvement in cybersecurity infrastructure, staff training, and technological support to ensure more credible, secure, and transparent elections in Nigeria.

Recommendations

- i. The Independent National Electoral Commission should further strengthen its cybersecurity infrastructure by investing in more advanced encryption systems, robust firewalls, and real-time threat detection technologies to reduce vulnerabilities in electoral processes and ensure continuous protection of sensitive electoral data.
- ii. INEC should expand regular training and capacity-building programmes for electoral officers and ICT personnel on cybersecurity awareness, digital system management, and emergency response strategies in order to minimize technical errors and improve the efficient use of electoral technologies such as BVAS and IREV.
- iii. The Federal Government, in collaboration with INEC and telecommunications providers, should improve network infrastructure and provide stable internet connectivity across all polling units in Nigeria to reduce delays, technical glitches, and disruptions during electronic accreditation and result transmission processes.

References

- Alebiosu, A. (2016). Smart card reader and the 2015 general elections in Nigeria: A critical assessment. *Journal of African Elections*, 15(1).
- Alvarez, R. M., & Hall, T. E. (2008). *Electronic elections: The perils and promises of digital democracy*. Princeton, NJ: Princeton University Press.
- Audu, A., & Akuva, I. I. (2020). Smart card reader machines and general elections in Nigeria from 2015 to 2019: Gains and challenges. *Studies in Politics and Society*, 9(1), 1–18.
- Cheeseman, N., Lynch, G., & Willis, J. (2018). Digital dilemmas: The unintended consequences of election technology. *Democratization*, 25(8), 1397–1418.
- Commonwealth Election Observer Group. (2023). *Report on Nigeria's 2023 general elections*. London: Commonwealth Secretariat.
- European Union Election Observation Mission. (2023). *Nigeria 2023: Final report – General elections*. Brussels, Belgium: European Union.

- Germann, M. (2023). Making votes count with internet voting. *Political Behavior*, 43, 1511–1533.
- Ibeanu, O. (2016). *The conduct of elections in Nigeria: A critical review*. Ibadan, Nigeria: John Archers Publishers.
- Ileyemi, A. (2021). TMG urges INEC to fix BVAS challenges before 2023 elections. *Premium Times*.
- International Institute for Democracy and Electoral Assistance. (2022). *Inspiring confidence in the BVAS and electronic transmission of election results: Seven urgent actions for INEC*. International IDEA.
- International Telecommunication Union. (2020). *Global cybersecurity index 2020*. ITU.
- Norris, P. (2014). *Why electoral integrity matters*. Cambridge, UK: Cambridge University Press.
- Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2017). Cybersecurity and safety in the digital age. *Computers & Security*, 70, 674–683.
- Nwangwu, C., Onah, E., & Ohi, C. (2018). Electoral fraud and democratic consolidation in Nigeria's Fourth Republic. *African Journal of Political Science and International Relations*, 12(2), 17–26.
- Ogundare, S., Ikwuoma, S. U., & Afolabi, O. S. (2025). Electoral reforms, technological innovation, and the conduct of Nigeria's 2023 general elections. *International Journal of Advanced Research in Global Politics, Governance and Management*, 5(1).
- Oladele, F. S. (2025). Technology security and electoral credibility in Nigeria: A national security review of BVAS and IReV in the 2023 general elections. *International Journal of Intellectual Discourse*, 8(3).
- Omotola, J. S. (2009). Nigerian elections and democratic consolidation: Dynamics and challenges. *Mediterranean Journal of Social Sciences*, 10(4), 125–136.
- Sibe, R. T. (2015). Technology in elections: The Nigerian experience. *Journal of African Elections*, 14(2).
- Sibe, R. T., & Kaunert, C. (2023). Technology, cyber security and the 2023 elections in Nigeria: Prospects, challenges and opportunities. *Journal of African Elections*, 22(2), 67–84.
- Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014). Security analysis of the Estonian internet voting system. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 703–715.
- Yavuz, A. Y., Koc, C. K., & Savas, E. (2018). Security and privacy in voting systems. *IEEE Security & Privacy*, 16(2), 52–59.
- Yiaga Africa. (2023). *2023 election observation report*. Abuja, Nigeria: Yiaga Africa.