Faculty of Natural and Applied Sciences Journal of Computing and Applications
Print ISSN: 3026-8133
www.fnasjournals.com
Volume 3; Issue 1; March 2026; Page No. 102-108.
DOI: https://doi.org/10.63561/jca.v3i1.1214

Investigating Cyber-Physical Systems Vulnerabilities and National Security in Nigeria's Power Sector Communication Networks

***Odunayo, Y.A.**
Department of Computer Science Education, Lagos State University of Education, Oto/Ijanikin Lagos

***Corresponding author email**: odunayoya@lasued.edu.ng

Abstract
Nigeria's power sector is undergoing a gradual but significant transformation as legacy electrical infrastructure becomes increasingly integrated with digital control and communication technologies. The researcher employed the use of descriptive survey research design method in this study since the design type allows for sourcing of data from different category of persons while also describing the characteristics. The population for the study comprised of power-holding and telecoms staff in South West Nigeria. Through the multi-stage sampling technique that comprised ballot procedure, proportionate sampling and simple random sampling procedure to select two thousand five hundred (1500) participants from power holding companies telecoms firms across the six geopolitical zones of the nation. A researcher-based designed instrument titled, "Cyber-Physical Systems Vulnerabilities and National Security in Nigeria's Power Sector Communication Networks Questionnaire (CSVNSNPSCNQ) consisting of 20 closed ended questions on response format of 4-Likert scale type of strongly agree, agree, disagree and strongly disagree was used for data collection. The scale was content validated and through the use of internal efficiency form of reliability, an index of .894 was derived meaning very suitable for this study. Through the identification of WhatsApp group for Telecoms and power holding staff across the six zones, an E-copy was sent through three research assistants who assisted in the delivery of the e-copy to their respectively platforms for response. Inferential statistics of correlation and regression analysis were used to analyse data and tested at significance level of .05 respectively. The findings revealed that national security of a nation greatly influences installation and operations of power sector communication networks in Nigeria. It concluded that due to rising insecurity challenges experienced and recorded incidences across most state capitals cyber-physical infrastructures would always be vulnerable to attacks in the country. Among others the study recommended for more investments in incident-response capacity, routine contingency exercises, mandatory security standards and closer public–private cooperation to share possible
.

Keywords: Cyber-Physical Systems, Threats, Vulnerabilities, National Security, Power Sector Communication Networks

Introduction

Nigeria's power sector is undergoing a gradual but significant transformation as electrical infrastructure become increasingly integrated with digital control and communication technologies. This modernization involves the adoption of cyber-physical systems that tightly couple physical power assets (like generators, substations, transformers) with networked information and control through SCADA (Supervisory Control and Data Acquisition) systems, IEDs (Intelligent Electronic Devices) and real-time telemetry links. While these advancements promise greater efficiency, responsiveness and monitoring capability, they also usher in a new class of risk through the exposure of critical infrastructure to cyber threats inherent in networked systems. The integration of CPS in power systems introduces a broad attack surface that adversaries may exploit. SCADA networks in particular have been shown to harbor inherent vulnerabilities which includes weak or missing authentication, unencrypted protocols and legacy devices not designed with security in mind (Obodoeze et al., 2018). These vulnerabilities can facilitate a range

Cite this article as:
Odunayo, Y.A. (2026). Investigating cyber-physical systems vulnerabilities and national security in Nigeria's power sector communication networks *FNAS Journal of Computing and Applications, 3*(1), 102-108. https://doi.org/10.63561/jca.v3i1.1214

of cyberattacks, including false-data injection, denial of service and even manipulation of control commands. In Nigeria, where some control installations remain outdated, and modernization efforts are uneven, the risk is magnified (Ogundari et al., 2021). The cyber vulnerabilities in Nigeria's power infrastructure are not purely technical; they reflect deeper systemic challenges. A recent survey of Nigeria's power system by Ibanga et, al (2024) showed that threats ranging from insider risk, supply chain vulnerabilities, advanced persistent threats (APTs), and even ransomware all contribute to service disruptions, equipment damage, and reputational harm. The convergence of IT and operational technologies in Nigeria's grid continues to occur without a corresponding maturity in cybersecurity posture, thereby creating strategic risk for a sector that underpins national development. From a national security perspective, vulnerabilities in CPS could translate into far more than momentary blackouts. In a digitally connected power grid, a well-coordinated cyberattack might trigger cascading failures, destabilize large portions of the grid, or interfere with critical services such as telecommunications, healthcare, and water systems. Indeed, the very nature of CPS means that cyber intrusions can have physical effects, potentially impinging on the sovereignty and safety of the nation Jimada-Ojuolape et al., 2024). Nigeria's regulatory and institutional frameworks are only beginning to catch up with these emerging risks. While there are commendable initiatives to assess cybersecurity in the energy sector, many of these focus on policy rather than on the specific vulnerabilities of communication networks within CPS. For instance, though some frameworks propose incident-response mechanisms and lifecycle security (Ogundari et al., 2021), implementation remains uneven, and sector-wide cyber resilience is yet to be systematically enforced. Likewise, proposed design frameworks for cybersecurity often do not fully account for Nigeria's unique grid architecture and operational constraints (Ismaila et, al 2023). At the same time, there are efforts from service operators on the potential application of advanced defensive methods tailored towards CPS. For example, models using architectural segmentation (Purdue Model), AI-based anomaly detection, and resilience engineering have been proposed in the Nigerian circumstance (Ekerete, 2024). Such approaches aim to prevent, detect, and recover from attacks more effectively by recognizing the hybrid cyber-physical nature of modern power systems. It needs to be stated that empirical assessments of their viability within Nigeria's power-sector communication networks remain limited and scarce. This study, therefore, seeks to explore and investigate the specific cybersecurity vulnerabilities in Nigeria's CPS-based power-sector communication networks and analyze their implications for national security. By combining technical vulnerability analysis with threat scenario modeling and policy assessment, the research aims to produce actionable recommendations for enhancing grid resilience. Ultimately, strengthening the cyber-physical security of Nigeria's power infrastructure is not merely a matter of operational efficiency but central to safeguarding national stability and continuity of essential services.

Statement of the Problem

Since the migration to 5G, Nigeria's power sector has since relied on interconnected cyber-physical systems (CPS) such as smart meters, supervisory control and data acquisition platforms, use of intelligent sensors and communication networks to support power generation, transmission, and distribution, among others. While these technologies are known to enhance operational efficiency, they also introduce significant cybersecurity vulnerabilities capable of destabilizing critical national infrastructure. A recent report by the Nigerian Communications Commission (2024), NCC, on telecoms operators in Nigeria stated that system failures, grid collapses, unauthorized access to control systems and ransomware attacks on energy utilities demonstrate that malicious actors can exploit weaknesses in communication protocols, software configurations and network architectures. Despite outcry from different quarters on these risks, many components of Nigeria's power communication infrastructure still operate with outdated security features, weak authentication mechanisms, limited intrusion detection capability and poor cyber-resilience strategies. The national security implications of CPS vulnerabilities in the power sector are profound. Revelation has it that disruptions to communication networks that coordinate energy flows may cripple economic activities, compromise military and security operations, and threaten public safety. Power sector agencies often lack comprehensive risk-assessment frameworks, coordinated incident-response mechanisms or robust regulatory standards for CPS protection. The absence of integrated cybersecurity governance between energy operators, communication regulators, and national security bodies exposes the grid to cascading failures from cyberattacks. This persisting lacuna highlights the need for an investigation into the vulnerabilities embedded in Nigeria's power sector CPS communication networks its potential consequences for national security.

Objectives of the study

Four research objectives were formulated to guide the focus of the study:

Cite this article as:
Odunayo, Y.A. (2026). Investigating cyber-physical systems vulnerabilities and national security in Nigeria's power sector communication networks *FNAS Journal of Computing and Applications, 3*(1), 102-108. https://doi.org/10.63561/jca.v3i1.1214

1. Assess how Cyber-Physical Systems vulnerabilities affect Power Sector Communication Networks.
2. Assess how National Security affects Power Sector Communication Networks
3. Evaluate how components of Cyber-Physical Systems vulnerabilities affect Power Sector Communication Networks
4. Evaluate how components of National Security affect Power Sector Communication Networks

Hypotheses

Four hypotheses were structured and tested at .05 level of significance:

H_{01}: Cyber-Physical Systems vulnerabilities do not have any significant impact on Power Sector Communication Networks.

H_{02}: National Security do not have any significant impact on Power Sector Communication Networks

H_{03}: Components of Cyber-Physical Systems vulnerabilities do not have any significant impact on Power Sector Communication Networks

H_{04}: Components of National Security do not have any significant impact on Power Sector Communication Networks

Methodology

The researcher employed the use of descriptive survey research design method in this study since the design type allows for the sourcing of data from different categories of persons while also describing the characteristics. The population for the study comprised of power-holding and telecoms staff in South West Nigeria. Through the multi-stage sampling technique that comprised ballot procedure, proportionate sampling, and a simple random sampling procedure to select two thousand five hundred (1500) participants from power holding companies' telecoms firms across the six geopolitical zones of the nation. A researcher-based designed instrument titled, "Cyber-Physical Systems Vulnerabilities and National Security in Nigeria's Power Sector Communication Networks Questionnaire (CSVNSNPSCNQ) consisting of 20 closed-ended questions on response format of 4-Likert scale type of strongly agree, agree, disagree, and strongly disagree was used for data collection. The scale was content validated, and through the use of an internal efficiency form of reliability, an index of .894 was derived, meaning very suitable for this study. Through the identification of a WhatsApp group for Telcoms and power holding staff across the six zones, an E-copy was sent through three research assistants who assisted in the delivery of the e-copy to their respective platforms for response. Inferential statistics of correlation and regression analysis were used to analyse data and tested at a significance level of .05, respectively.

Results

H_{01}: Cyber-Physical Systems vulnerabilities do not have any significant impact on Power Sector Communication Networks.

Table 1: Correlation analysis showing Cyber-Physical Systems vulnerabilities and Power Sector communication Networks

Deliverables	N	Mean	Sd	p	r.cal	Sig.
Cyber-Physical Systems vulnerabilities		2.48	.69			
Power Sector Communication Networks	1500	1.80	.72	.05	.779	.002[a]

Table 1 shows that 1500 respondents participated in the study, at r-value of .779, it implies the existence of a positively strong relationship between variables of Cyber-Physical Systems vulnerabilities and Power Sector Communication Networks, while at alpha value of .05, and significant at .002 ($p<.05$) the null hypothesis rejected. This reveals that the vulnerability of Cyber-physical Systems has direct impact on Power Sector Communication Networks in Nigeria.

Cite this article as:
Odunayo, Y.A. (2026). Investigating cyber-physical systems vulnerabilities and national security in Nigeria's power sector communication networks *FNAS Journal of Computing and Applications, 3*(1), 102-108. https://doi.org/10.63561/jca.v3i1.1214

H_{02}: National Security does not have any significant impact on Power Sector Communication Networks

Table 2: Correlation analysis showing National Security and Power Sector communication Networks

Deliverables	N	Mean	Sd	p	r.cal	Sig.
National Security		1.46	.32			
Power Sector Communication Networks	1500	1.80	.72	.05	.694	.008[a]

Table 2 shows that 1500 respondents participated in the study, at r-value of .694, it implies the existence of a strongly positive relationship between the variables of National security and Power Sector Communication Networks, while at an alpha value of .05, and significant at .008 ($p<.05$) the null hypothesis rejected. This reveals that failure to maintain National Security have direct impact on Power Sector Communication Networks in Nigeria.

H_{03}: Components of Cyber-Physical Systems vulnerabilities do not have any significant impact on Power Sector Communication Networks

Table 3: Linear regression analysis showing components of Cyber-Physical Systems vulnerabilities on Power Sector Communication Networks Coefficients[a]

Model	Unstandardize Coefficients		Standardized Coefficients	T	Sig.
	B	**Std. Error**	**Beta**		
(Constant)	2.489	.246		10.129	.000
Control/Operational layer	.722	.567	.620	0.827	.018
Human and organisational	.645	.504	.750	1.631	.024
.Communication/Network layer	.758	.652	.774	1.420	.014
Cyber/Software layer	.465	.582	.683	1.386	.003
Physical Layer	.778	.493	.886	1.980	.000
(Constant)	2.000	.041	2.34	12.888	.000

a. Dependent Variable: Power sector Communication Networks

From table 3 above it shows that five intervening variables are all good predictors and significant contributors to power sector communication networks as significant values of .018, .024, .014, .003, and .000, all less than the alpha value of .05 ($P<.05$), hence the null hypothesis is rejected, and the alternative is retained. However, to determine the relative contribution of the intervening variable, the beta values are used as determinants where the Physical layer contributes the most with .886, the communication layer with .774, the human and organizational with .750, the cyber/software layer with .683, and the control operational layer with .620, respectively.

H_{04}: Components of National Security do not have any significant impact on Power Sector Communication Networks

Cite this article as:
Odunayo, Y.A. (2026). Investigating cyber-physical systems vulnerabilities and national security in Nigeria's power sector communication networks *FNAS Journal of Computing and Applications, 3*(1), 102-108. https://doi.org/10.63561/jca.v3i1.1214

Table 4: Linear regression analysis showing components of National Security on Power Sector Communication Networks Coefficients[a]

Model	Unstandardize Coefficients		Standardized Coefficients	T	Sig.
	B	**Std. Error**	**Beta**		
(Constant)	2.489	.246		10.129	.000
Political security	.683	.702	.785	1.404	.000
Energy security	.701	.581	.485	1.631	.016
Economic security	.693	.559	.882	1.564	.003
Cyber/Information	.504	.675	.786	1.221	.001
Physical security of infrastructure	.699	.576	.803	.805	.000
(Constant)	2.000	.041	2.34	12.888	.000

a. Dependent Variable: Power sector Communication Networks

Table 4 above it shows that five intervening predictors determine the extent of national security of a nation, especially in Nigeria. To determine the extent of prediction, all significant values for intervening variables are less than the alpha value of .05 ($p<.05$), as a result, the null hypotheses are rejected and the alternative retained. However, in order to determine the relative contribution of the intervening variables, the beta values are used as determinants where economic security contributes the highest with .882, physical security of infrastructure with .803, cyber/information with .786, political security with .785 and the least contributor is energy security.

Discussion

Data from hypothesis one revealed that the protection of cyber-physical systems has a positive impact on Power Sector Communication Networks. These cyber-physical systems (CPS) vulnerabilities include outdated/poorly patched control software and firmware, insecure communication protocols, weak network segmentation, inadequate authentication and access controls, among others. The findings align with studies by Ogundari, (2020); Sun et al., (2016); Qu et al. (2023); IJITC (2024), who alluded that the destruction of cyber-physical networks impairs the integrity, availability and timeliness of power-sector communications in Nigeria. This vulnerability weakens and enables deception, data manipulation and denial attacks that can corrupt sensor/SCADA data or block control signals, while limited incident response capacity and poor network design lengthen recovery times and increase the chance that local faults escalate into wide-area outages (Ogundari, 2020; Sun et al., 2016; Qu et al., 2023; IJITC, 2024). Data from hypothesis two also reveals that national security has a great impact on a nation's power sector communication network. National security threats directly degrade the integrity, availability, and timeliness of power sector communications in Nigeria. A nation beclouded with national security challenges is bound to encounter corrupt sensor data, blocked control signals, longer recovery times, and increased risk of local faults cascading into wide-area outages. These findings of this work align with studies by Ogundari (2020), and Qu et al. (2024) that noted any attack on telecom and transmission infrastructures would severely affect communication paths used by control centres and smart devices, thereby amplifying outage duration even where cyber defenses exist. This combined effect is a systemic vulnerability where degraded communications undermine operators' situational awareness and incident response, turning manageable faults into national security risks for critical services and economic activity. They advised for timely resilient measures where device hardening, secure protocols, segmentation, physical protection, and faster response capacity be put in place to help mitigate risks and challenges associated with national security. Data from hypothesis three reveals that components of Cyber-Physical Systems vulnerabilities do have a significant impact on power sector communication networks in Nigeria. Findings show that a specific cyber-physical system (CPS) could

Cite this article as:
Odunayo, Y.A. (2026). Investigating cyber-physical systems vulnerabilities and national security in Nigeria's power sector communication networks *FNAS Journal of Computing and Applications, 3*(1), 102-108. https://doi.org/10.63561/jca.v3i1.1214

trigger legacy/poorly patched control software and firmware, insecure communication protocols and network segmentation, weak authentication and access controls, vulnerable field devices (RTUs/PLCs), and telemetry links, which can cause threats to communications infrastructure that directly degrade the integrity, availability, and timeliness of power-sector communications in Nigeria. These vulnerabilities bring about an increase in the risk of mis-operations, delay restoration, and large outages. This finding is in agreement with studies by IJITC (2024), Ogundari (2020); Sun (2016); Qu et al. (2023), and Chen (2024) that these vulnerabilities enable deception and disruption attacks that can corrupt sensor/SCADA data or block control signals, while poor network design and limited incident-response capacity make containment and recovery slower and costlier. They affirmed that strengthening device hardening, secure protocols, network segmentation, access management, and physical protection improve communication resilience and reduces the likelihood that a local failure escalates into a system-wide event. Also, from hypothesis 4 the data revealed that the components of National Security have a significant impact on Power Sector Communication Networks in Nigeria. Findings indicate that of all the several components of national security, cybersecurity, physical security of infrastructure, energy/operational security, information/communications integrity, and governance/regulatory capacity have a significant impact on power-sector communications in Nigeria. This finding corroborates studies by Ogundari, (2020) and Ebelogu, (2025), identification of cybersecurity weaknesses in legacy SCADA/communication systems and increasing digitalisation exposes transmission and distribution communications to malware, ransomware and false data attacks that can disrupt control signals and trigger large outages. Physical insecurity (theft, vandalism, and attacks on sites) and poor site access also degrade the availability and maintenance of communication links for substations and microgrids, slowing restoration and increasing outage duration (Punch Editorial, 2024; Clean Technology Hub, 2022). Weak policy coordination, limited incident-response capacity and gaps in standards and workforce skills reduce resilience and delay containment when incidents occur, turning technical failures into broader national-security risks (National Security Strategy, 2019; BusinessDay, 2025).

Conclusion

From the findings, the study concluded that, due to rising insecurity challenges recorded across most state capitals of the country, cyber-physical infrastructures would remain vulnerable to attacks by miscreants. Nigeria's power sector communication networks are confronted with outdated firmware and weak authentication to exposed field devices and infrastructure, which can undermine system integrity, availability, and operator situational awareness, thereby transforming routine faults into national-security risks. The outcome of this study is relevant to undergraduates (students), especially those in the field of electrical engineering, cybersecurity and information systems, because it would deepen their knowledge on how modern power systems integrate digital and physical components and how vulnerabilities in these systems can cause real-world consequences. This knowledge would equip them with contemporary skills and perspectives needed for future careers in power systems engineering, cyber-physical systems design, ICT security, and national infrastructure management. For researchers, the study provides a foundation for advancing scholarly work on cyber-physical system security, critical infrastructure resilience, and threat modeling in developing economies. It would also add empirical evidence to the limited body of research on Nigeria's power sector cybersecurity posture and identify specific gaps where further investigations can be executed. By offering structured analysis, the study serves as a valuable reference point for interdisciplinary research across cybersecurity, power engineering, policy analysis and national security-related areas. Network providers like telecom companies and ICT service operators supporting grid communication links, too, would benefit from the outcome of this study as they become abreast with a clearer understanding of the security expectations and vulnerabilities associated with critical infrastructure connectivity. It would also highlight areas where secure communication architectures, robust network monitoring tools, and compliance with cybersecurity standards need be strengthened to protect power sector operations in the country. By identifying weaknesses in data transmission pathways and remote-access channels, the outcome would also encourage network providers to adopt best practice configurations, enhance service reliability, and collaborate more effectively with power utilities on secure infrastructure deployment. For the government, the study holds significant value as it underscores the national security implications of cyber vulnerabilities within the power sector—one of Nigeria's most vital critical infrastructures. The insights enable policymakers and security agencies to refine regulatory frameworks, develop targeted cybersecurity policies, and strengthen inter-agency coordination on critical infrastructure protection. By revealing how cyber threats can escalate into economic disruption, social instability, or strategic vulnerability, the study supports more informed decision-making regarding investment priorities, sector oversight, emergency response planning, and national-security strategy formulation.

Cite this article as:
Odunayo, Y.A. (2026). Investigating cyber-physical systems vulnerabilities and national security in Nigeria's power sector communication networks *FNAS Journal of Computing and Applications, 3*(1), 102-108. https://doi.org/10.63561/jca.v3i1.1214

Recommendations

Among others the researcher recommended the following:

1. Policymakers and operators should prioritise a layered resilience strategy where they urgently harden and patch devices, adopt secure communication protocols and strict access controls, and enforce network segmentation and redundancy
2. Strict measures must be undertaken to strengthen the physical protection of fibre/towers.
3. There must be investment in incident-response capacity, routine contingency exercises, mandatory security standards, and closer public–private cooperation to share threat intelligence
4. Advocacy for a hardened cyber defense, secure sites, clarification of regulatory roles and building response capabilities would help improve the reliability and security of power-sector communications and reduce national-security exposure.

References

BusinessDay Editorial. (2025, May 29). *Nigeria's electricity crisis is a 'National Security' threat*. BusinessDay. Retrieved *from* https://businessday.ng/editorial/article/nigerias-electricity-crisis-is- a-national-security-threat/.

Ebelogu, C. U. (2025). Investigation of cybersecurity vulnerabilities and mitigation strategies in Nigeria's critical energy infrastructure (working paper). *Ajayi Crowther University Journals*.

Ekerete, E.D. (2024). Cyber-physical systems for enhancing security in critical infrastructure: Addressing Nigeria's security challenges. *Academic World Journal of Scientific and Engineering Innovation*.

Ibanga, I.J., Fwah, K.G., & Idowu, A.J. (2024). Assessing the vulnerabilities: Cybersecurity challenges in power system infrastructure in Nigeria. *International Journal of Information Technology & Computer Engineering, 4*(4), 22–35. DOI**:** https://doi.org/10.55529/ijitc.44.22.35

Ismailaila, I., Adeleke, I., Anogie Uduimoh, A., & Tom, J. (2023). Design framework of cyber security solutions to threats and attacks on critical infrastructure of electricity power systems of Nigeria companies. International *Journal of Computing, Intelligence and Security Research, 2*(1), 17–23.

Jimada-Ojuolape, B., Teh, J., & Lai, C.M. (2024). Securing the grid: A comprehensive analysis of cybersecurity challenges in PMU-based cyber-physical power networks. *Electric Power Systems Research*, 233, 110509. Retrieved from KwasuSpace Repository.

National Counter Terrorism Centre (NCTC). (2019*). National Security Strategy* (NSS-2019). Retrieved from https://nctc.gov.ng/wp-content/uploads/2024/01/NSS-2019.pdf.

Nigerian Communications Commission. (2024*). Highlights — Closing the digital divide: expanding 4G/5G coverage into underserved rural regions* (NCC media release). Nigerian Communications Commission. Retrieved 2025, from https://ncc.gov.ng/media/3586/view

Nigerian Communications Commission. (2025). 2023 year-end performance report (Year-end Performance Report). Retrieved from https://ncc.gov.ng/sites/default/files/2025-04/2023-YEAR-END-PERFORMANCE-REPORT.pdf.

Obodoeze, F.C., Obiokafor, I.N., & Asogwa, T.C. (2018). SCADA for national critical infrastructures: Review of the security threats, vulnerabilities and countermeasures. *International Journal of Trend in Scientific Research and Development, 2*(2), 974–982. https://doi.org/10.31142/ijtsrd9556

Ogundari, I. (2020*). Cyber security assessment of Nigeria's electric power infrastructure* (AJSPIM). https://ajspim.oauife.edu.ng/index.php/ajspim/article/download/79/43.

Ogundari, I., Otuyemi, F., Momodu, A., & Salu, L. (2021). Cyber security assessment of Nigeria's electric power infrastructure. *African Journal of Science Policy and Innovation Management, 1*(2), 87–104.

Punch Editorial. (2024, November 3). Blackout, a national security threat. The Punch. Retrieved from https://punchng.com/blackout-a-national-security-threat/.

Qu, Z., Li, X & Kiu, C. (2023). *Electric power cyber-physical systems vulnerability assessment under cyber-attacks*. Frontiers in Energy Research.

Qu, Z., Li, X., & Chen, Y. (2024). Cybersecurity challenges in power system infrastructure: implications for resilience. *International Journal of Information Technology and Communications* (IJITC), 17 June 2024.

Sun, C.C., & Xie, L., (2016). *Cyber-physical system security of a power grid: State-of-the- art. Electronics, 5*(3), 40. https://doi.org/10.3390/electronics5030040

Cite this article as:
Odunayo, Y.A. (2026). Investigating cyber-physical systems vulnerabilities and national security in Nigeria's power sector communication networks *FNAS Journal of Computing and Applications, 3*(1), 102-108. https://doi.org/10.63561/jca.v3i1.1214