I J C R M
International Journal of Contemporary Research In Multidisciplinary

Research Article

Cybersecurity and Data Integrity in Neiti's Oil and Gas Revenue Disclosure Systems in Nigeria

Muhammed Ibrahim [1*], Amit Jain [2], Ronak Duggar [3]
[1-3] School of Computer Science & Engineering, Geeta University, Panipat, Haryana, India

Corresponding Author: *Muhammed Ibrahim

DOI: https://doi.org/10.5281/zenodo.19762061

Abstract

This paper validates the extent to which information on the Nigeria Extractive Industries Transparency Initiative (NEITI) data reporting systems is credible and valid, in reporting oil and gas revenues. To conduct a survey, 110 individuals were selected out of 150 employees. We would ask questions and discuss with significant individuals to get information. The questions were examined by professionals to ensure that they were alright. We administered a technique to determine whether the questions were trustworthy. We sussed numbers with statistics and sussed what people said in a special way. The outcomes will indicate procedures to maintain the safety of data, issues and the effectiveness of data checks in NEITI systems, to report oil and gas revenue utilising NEITI. They will also contain suggestions on how NEITI can make its revenue disclosure systems more stable and safer.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 13-04-2026
- **Accepted:** 20-04-2026
- **Published:** 25-04-2026
- **IJCRM:**5(2); 2026: 829-835

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Article

Ibrahim M, Jain A, Duggar A. Cybersecurity and Data Integrity in Neiti's Oil and Gas Revenue Disclosure Systems in Nigeria. Int J Contemp Res Multidiscip. 2026;5(2):829-835.

Access this Article Online

www.multiarticlesjournal.com

KEYWORDS: Cybersecurity, Data Integrity, Neiti, oil and gas and revenue disclosure.

1. INTRODUCTION

Oil and gas contribute greatly to the revenues of Nigeria. These sectors are highly significant as they attract the bulk of export revenue in the country and offer a significant portion of the government revenue. The industry engages in operations such as exploration of oil, its production, transportation and monetary collection. All these activities generate a lot of operational and financial data.. Digital technologies that have recently been used to improve data management's efficacy, accountability, and transparency include electronic metering, automated revenue systems, and online reporting platforms (Paul & Malachy, 2025; Nwokonkwo et al., 2024). With the increased use of digital systems, both operational and financial data may be more vulnerable to hackers or attacks. In Nigeria, these ideas were developed by NEITI created by the country to employ them in the country.. It also embraced the Extractive Industries Transparency Initiative (EITI) as a way of enhancing honesty, accountability, and transparency in the extractive industry. Besides the release of reports to enhance the level of public control, NEITI has the responsibility of reconciling and disclose revenues between government agencies and oil and gas companies. Despite all these efforts, there is an increased tendency to use digital systems in managing revenue data and as such, it is quite essential to ensure that the data remains accurate and safe against hackers in order that people trust the information. Although there are programs such as Government Integrated Financial Management, the Integrated Personnel and Payroll Information System (IPPIS), and the Treasury Single Account (TSA).

The Treasury Single Account, the Integrated Personnel and Payroll Information System and the Government Integrated Financial Management Information System have enabled management to be improved. Issues such as the inability to manage data and a lack of sufficient technical capabilities and cyber threats continue to increase.

2. LITERATURE REVIEW

Ensuring data security and accuracy is quite crucial in systems particularly with sensitive financial data. Data integrity refers to ensuring that data is correct, complete and consistent and reliable throughout. Cybersecurity is concerned with the safety of systems and networks and information against individuals who are not supposed to access them and cyber threats. Examples of this are the Treasury Single Account and the Integrated Personnel and Payroll Information System and the Government Integrated Financial Management Information System.

In money-related systems the concepts assist in maintaining information accurate and reliable to make decisions and report. Studies indicate that the oil and gas sector is vulnerable to cyber attacks, such as ransom ware and systems to manage money and work attacks.

These risks occur as old systems that are not well monitored and weak network security allow important systems to be attacked and work halted and data damaged.

Research on the system of public finance in Nigeria shows that there are still issues concerning how to control and maintain it against cyber attacks. Platforms that simplify things and make them more transparent, such as the Treasury Single Account and the Integrated Personnel and Payroll Information System and the Government Integrated Financial Management Information System tend not to be well-protected in terms of cybersecurity and data protection.

Research indicates that poor decision-making on rules and failure to apply security technologies effective and lack of awareness of security in organizations can expose systems to vulnerability to cyber threats. The Government Integrated Financial Management Information System and the Integrated Personnel and Payroll Information System and Treasury Single Account require the protection of data.

This demands management controls and technical security, such as encryption and access control and monitoring systems. There is need to protect the Government Integrated Financial Management Information System and the Treasury Single Account and the Integrated Personnel and Payroll Information System.

We also have insights through research on transparency initiatives in Nigeria. Transparency in itself will not translate to results of governance. That is the case when we are in the revenue disclosure programs such as that by the Nigeria Extractive Industries Transparency Initiative. These programs open up information to the public and enhance accountability.

get information out in the open and enhance accountability.

The Nigeria Extractive Industries Transparency Initiative is a difference maker since it assists people to know what is involved. Nevertheless these efforts might not have a considerable effect due to internal controls, challenges within the institution and ineffective reporting. That we are taught by the studies of Ejiogu and others in 2019 Moses and others in 2023 and Rotimi and Abdul-Azeez in 2013.

These findings inform us that the reliability and soundness of the underlying data is equally crucial to the credibility of revenue disclosure systems as the availability of data. The Nigeria Extractive Industries Transparency Initiative and other transparency initiatives should ensure that the information is right and reliable.

Prior research has looked at cybersecurity risks. Their impact on how organizations perform using different methods like systematic literature reviews and empirical surveys. In 2025, it is demonstrated by Ebelogu and others. In 2024, Aidonojie and others. All this work notwithstanding there remains a gap in research since cybersecurity threats and integrity of data in the Nigeria Extractive industries Transparency Initiatives revenue disclosure systems have not been studied extensively.

To fill this gap this study will look at data integrity procedures, cybersecurity practices and related risks that affect the accuracy of revenue disclosures, in Nigerian industry. Nigeria Extractive Industries Transparency Initiative is relevant to this industry hence the need to know how to improve its revenue disclosure systems and make them more secure.

2.1 Comparative Analysis of Studies

Table 1: Overview of important research in Cybersecurity, Data Governance and Transparency

Study	Methodology	Key Findings	Research Gaps
Ebelogu et al., 2025	Systematic literature review	Identified ransomware, advanced persistent threats and weak cybersecurity controls in Nigeria's oil and gas sector	Limited consideration of cybersecurity implications for revenue disclosure systems, particularly within NEITI
Aidonojie et al., 2024	Mixed method (legal review and survey of 303 respondents)	Digital tax systems improve transparency but face weak data protection and cybersecurity frameworks	Focused on tax systems rather than extractive revenue disclosures
Ejiogu et al., 2019	Qualitative case study	Transparency initiatives may conceal weaknesses in reporting systems	Insufficient attention to technical dimensions such as cybersecurity and data integrity
Aguboshim et al., 2023	Narrative review	Data governance and cybersecurity are essential for protecting organisational data	Absence of empirical investigation within specific public sector institutions such as NEITI
Anyanwu et al., 2024	Literature review	Multi-layer security controls improve protection of financial data integrity	Study limited to financial organisations
Familoni & Shoetan, 2024	Comparative review	Nigeria's financial sector faces challenges in cybersecurity infrastructure and skills	Sectoral focus limits applicability to extractive industry revenue transparency frameworks

The table shows an increasing attention to the risks of cybersecurity, but a lack of research on the issue of data integrity in extractive revenue systems. This paper fills this gap by looking at the systems of revenue disclosure established by NEITI.

3. METHODOLOGY

This paper follows a descriptive and explanatory survey design based research study and focused mainly on a quantitative approach but with the addition of qualitative insights. The population at risk is 200 members of the Nigeria Extractive Industries Transparency Initiative (NEITI) and identified partner agencies in the areas of oil and gas revenue reporting. Yamane formula applied in coming up with the sample of 132 respondents was applied and stratified random sampling technique was applied to represent the outcome in relation to the different concerned departments. The data were gathered using a structured questionnaire in the five-point Likert scale, according to data integrity practices, employee compliance and controls on cybersecurity.

3.1 RESEARCH DESIGN

The research design is descriptive and explanatory cross-sectional survey design since quantitative and qualitative methods on data collection were implemented to assess NEITI oil and gas revenues reports on cybersecurity operations and data integrity in the disclosure system. The quantitative component will enable one to make statistical inferences on the controls, compliance and integrity correlations and the qualitative interviews will provide the contextual richness that is similar to the mixed methods approach to the study on cybersecurity in Nigeria.

3.2 Population and Sample

The sample group in the research is the staff of the Nigerian Extractive Industries Transparency Initiative, who deal with the management of the revenue system and the digital system. These include; ICT, data and reconciliation, audit staff, monitoring and evaluation and administrative or management staff. Further on, the targeted population of the study will be the selected the liaison officers of the partner government agencies that take part in oil and gas revenue reporting. The number of its employees is 200. The sample size formula developed by Yamane can be used to take a sample of 132 respondents in the study. The stratified random sampling is employed because it is necessary to have an adequate representation of the various departments. The respondents are selected to presenting department based on the proportional share to the entire population.

Table 2: Population and Proportional Sample Allocation

Department / Category	Population (N)	Proportion (%)	Allocated Sample (n)
ICT Personnel	30	15%	20
Data / Reconciliation Officers	40	20%	26
Audit Staff	35	17.5%	23
Monitoring & Evaluation Officers	25	12.5%	17
Administrative / Management Staff	50	25%	33
Liaison Officers (Partner Agencies)	20	10%	13
Total	200	100%	132

A sample of 132 respondents was taken based on the stratified sampling of the study population of 200 staff based on the department. There was good representation of all categories as Administrative/Management staff (33), Data/Reconciliation officers (26) Audit staff (23), ICT personnel (20), Monitoring and Evaluation officers (17), and Liaison officers (13) had the highest number of representations.

3.3 Instruments

The study data will be collected by means of a questionnaire. This questionnaire will have items that people can answer using a 5-point Likert scale. This questionnaire will be used to collect study data using the responses of study data such as Disagree, Disagree, Agree and Strongly Agree. There are three constructs of the questionnaire. Cybersecurity controls this involves network security, access control, encryption, system logging and incident response practices. Employee cybersecurity compliance such as password management practices, phishing threat and incident reporting behaviour awareness. And Data integrity does it in terms of data validation, audit trail and reconciliation process and published revenue report reliability.

3.4 Validity and Reliability

In a bid to achieve quality of the research tool content validity will be abducted by having experts, including information technology and research methodology experts, to review the research tool. The pilot-test that is planned to include about 10-15 members of the staff will be done to clarify unclear questions and to enhance the questionnaire structure. Cronbach alpha will be utilized in determining the reliability of the

instrument. Each construct will be allowed to have a reliability coefficient of 0.70 and above, which will be considered as an acceptable internal consistency of the questionnaire items.

3.5 DATA COLLECTION AND ANALYSIS

We will give questionnaires to people at NEITI and some other offices. We will give them out on the computer and on paper. We want least 70 percent of the people to answer the questionnaires. Then we will look at the answers using a computer program called SPSS or Microsoft Excel.

We will do a things to understand the answers. First we will look at the information like the average score how much the answers vary and how often people gave certain answers. We will also see how cybersecurity rules what employees do and how people keep data safe are related to each other.

We will do another analysis to see if what we think is true really is. We want to know how much the cybersecurity practices affect the accuracy of the data at NEITI when they tell people how money they get from oil and gas. We will look at the data, from NEITI and the other offices to find the answers. The questionnaires will help us understand what is going on with cybersecurity and data integrity at NEITI.

4. RESULTS

4.1 Response Rate and Demographic

Table 3: Response Rate

Item	Number	Percentage
Questionnaires distributed	150	100%
Questionnaires returned	132	88%
Valid for analysis	128	85.3%

The following table shows survey response rate of survey conducted to carry out the study. The questionnaires sent out 132 of 150 response forms were sent back, and this translates to 88 percent response rate. After the screening on completeness, 128 questionnaires were classified as valid to be analyzed, which included 85.3 percent of the questionnaires sent out. This is believed to be a sufficient response rate to statistically analyze and interpret.

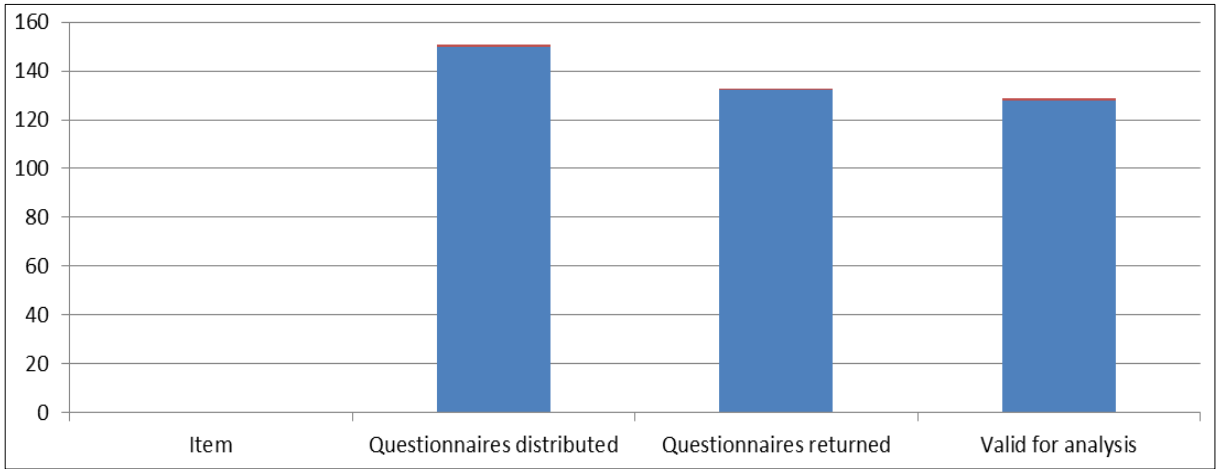

Fig 1: Response rate

4.2 Objective 1: Cybersecurity Measures in Neiti's Systems

Table 4: NEITI's for Cybersecurity Controls

Control Item (1–5 scale)	Mean	SD	Interpretation
Firewalls and network segmentation are implemented	3.9	0.8	High
Regular software updates/patching	3.2	1.0	Moderate
Multi-factor authentication for critical systems	3.0	1.1	Moderate
Formal incident response procedures	2.8	1.0	Low–Moderate
Continuous security monitoring/logging	2.6	1.1	Low–Moderate

These findings imply that the most fundamental of cybersecurity measures, including firewalls and network segregation, have been implemented fairly well within the systems of NEITI. The remainder of the controls, such as incident response procedures and continuous monitoring, have lower descriptive means scores. This speaks to the fact that although there are basic security measures, such as the more thorough cybersecurity operations, such as threat detection and sound incident response have to be strengthened.

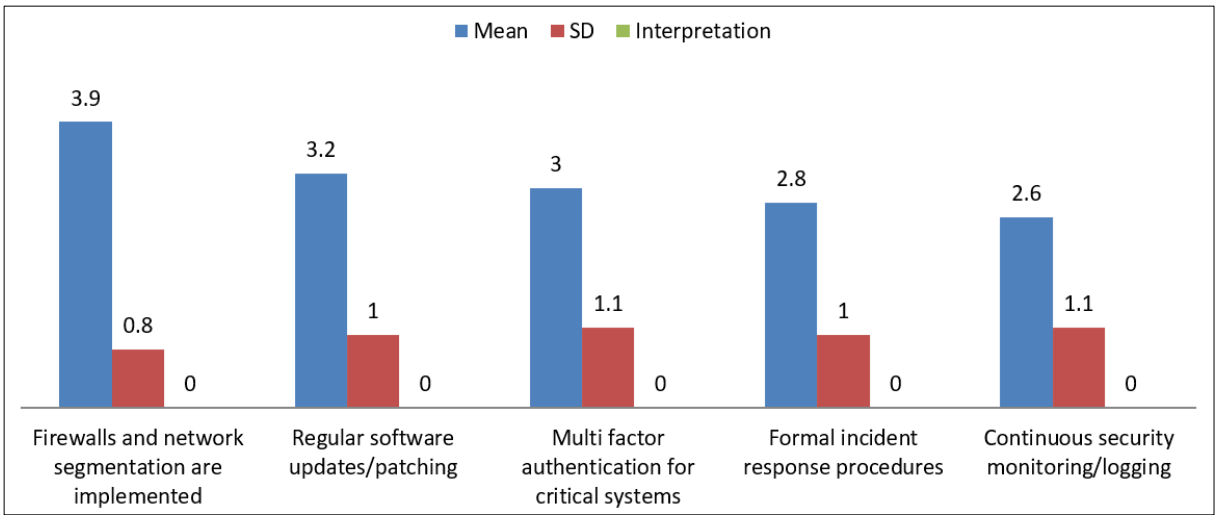

Fig 2: NEITI's cybersecurity control

4.3 Objective 2: Mechanisms for Ensuring Data Integrity

Table 5: Enhancing Data Integrity Practices

Practice	Mean	SD	Interpretation
Standard templates for data submission from agencies	4.1	0.7	Strong
Reconciliation between the company and the government data	4.0	0.8	Strong
Automated validation/error checks in IT systems	3.1	1.0	Moderate
Detailed audit trails and version control	3.0	1.1	Moderate
Independent technical audit of datasets before publication	2.7	1.2	Weak–Moderate

The findings show that data reconciliation and standardised templates are effective steps that NEITI has undertaken to create data integrity. However, automated validation systems, audit trails and independent technical audits had an average to low score. It is an indication that conventional types of reconciliation work but technical data integrity controls can be improved.

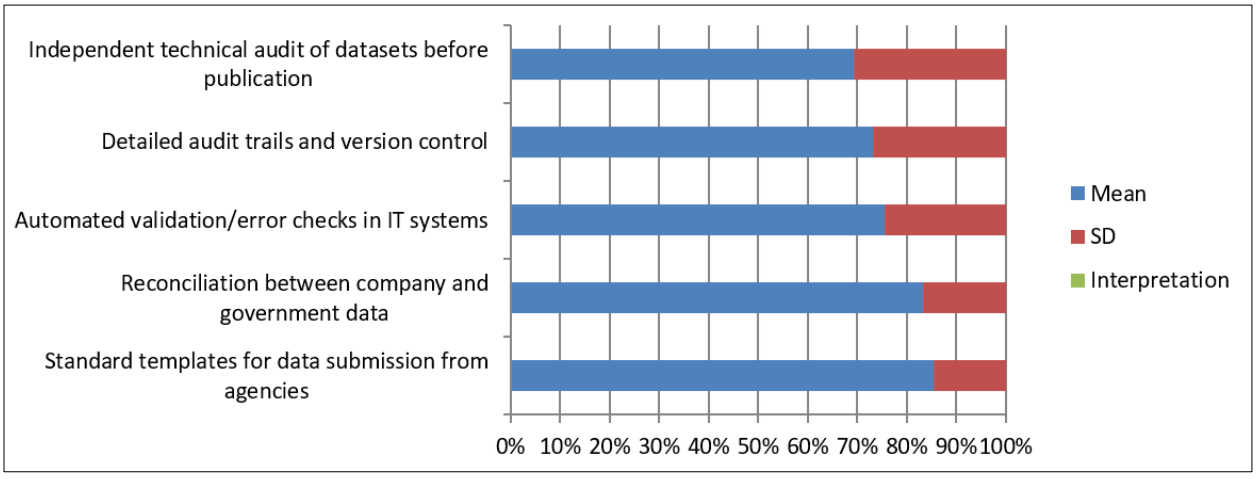

Fig 3: Representation of data integrity practice

4.4 Objective 3: Major Cybersecurity Threats and Vulnerabilities

Table 6: Cybersecurity Threats

Type of Threat / Vulnerability	Frequency (n)	Percentage (%)
Phishing	48	36.4
Ransomware	32	24.2
Unauthorized Access	28	21.2
Data Loss / Corruption	24	18.2
Total	132	100

According to the table, phishing attacks are most commonly described by the respondents as the highest cybersecurity threat. Other typical results were ransomware attacks then unauthorized access and the loss or corruption of data. These results point to a more vigorous user education, additional access controls, and enhanced surveillance to safeguard valuable revenue information.

4.5 Relationship between Cybersecurity Controls and Data Integrity

Table 7: Correlation between cyber security control and data integrity

Variables	1	2	3
1. Cybersecurity controls index	1.00		
2. Employee cybersecurity compliance	0.52	1.00	
3. Data integrity index	0.60	0.55	1.00

*Note: *p< 0.01

Correlation findings indicate that cybersecurity controls have a positive and statistically significant relationship with data integrity and that the same data integrity relationship can be seen between employee compliance with cybersecurity and data integrity. This implies that the level of reliability of the revenue data is linked to a better level of cybersecurity and compliance by the workers.

Table 8: Regression of Data Integrity on Cybersecurity Controls and Employee Compliance

Predictor	β (Standardised)	t value	Sig.
Cybersecurity controls	0.42	4.80	0.000
Employee compliance	0.35	3.90	0.000

$R^2 = 0.52$; $F(2,125) = 68.3$, $p < 0.001$

The regression analysis also demonstrates that both cybersecurity controls and compliance by employees have a significant positive impact on data integrity. The model accounts about 52 percent of the variation in the data integrity index. These findings confirm the study hypotheses that cybersecurity practices and employee behaviour are important in ensuring the reliability of the NEITI revenue disclosure system.

4.6 Cybersecurity Control Domains in Nesiti

The analysis of the cybersecurity control domains shows that the security levels are not the same in all areas. The highest mean score was recorded in the areas of network security and access control, indicating that these areas are well established. The staff training domain was also found to have a moderate score, indicating that the employees are somewhat aware of the importance of cybersecurity. However, the monitoring and logging mechanisms, as well as the incident response, scored the lowest, indicating that these areas are likely to be weak in the cybersecurity system adopted by NEITI. The organization might not be able to detect and respond to cybercrime, and this could easily lead to data breaches or manipulation, affecting the reliability of the revenue disclosure system.

5. THE FINDINGS

Illustrate that transparency programs cannot work all on their own to realize higher rates of accountability in the management of revenues made through the selling of oil and gas. Though there have been improvements in disclosure of information about revenues and audit reports by transparency initiatives through Nigeria Extractive Industries Transparency Initiative (NEITI) there has not been incomplete improvements of accountability and control of corruption. Although transparency has improved the access to information regarding revenues, different challenges encountered regarding the system have continued to affect their effectiveness.

6. CONTRIBUTION

By examining the intersection of cybersecurity practices, data integrity systems and revenue transparency systems, the study aids an understanding of transparency and accountability in the extractive industries sector in Nigeria.

The research aims to provide empirical evidence on the effect of cybersecurity practices on the credibility of the information reported on the revenues reported in the extractive industries sector under the Nigeria Extractive Industries Transparency Initiative.

The study reveals the limitations of transparency initiatives in achieving greater levels of accountability in managing revenues generated in the extractive industries sector

7. CONCLUSION

Conclusively, the paper has examined the relationship between cybersecurity, data integrity and transparency in NEITIs revenue disclosure practices. The paper has identified that despite the enhancing transparency, accountability and control over corruption have not been increased. The study has also revealed that there are still challenges in terms of reporting, data understanding, and implementation of audit recommendations, among others.

The paper has also found that effective and trustworthy revenue disclosure practices require a well-developed cybersecurity, data integrity and better frameworks.

8. Future Work

This research has brought about various possibilities of future research. Further studies can be devoted to the efficiency of implementing enhanced cybersecurity measures into transparency and accountability mechanisms of extractive sector institutions. More advanced digital tools such as automated validation and using data analytics and distributed ledger system to enhance the overall credibility of the extracted data could also be explored in future studies. The comparative research in different countries that are members of the Extractive Industries Transparency Initiative to understand the impact of the institutional and governance structures added to the effectiveness of transparency and accountability systems could be one more area to conduct further research. The effectiveness of public engagement and the extent of accessibility of data in using publicly disclosed extractive sector revenue data by the public and civil society organizations could be the subject of further research. Finally, the use of digital governance technologies could be implemented in the extractive sector and could yield valuable research findings towards the development of stronger and more reliable transparency systems in the management of natural resource revenues in various countries.

REFERENCES

1. Adelokun A. A literature review on cybersecurity in Nigeria. SSRN Electronic Journal. 2024. doi:10.2139/ssrn.4818525.

2. Aguboshim F, Obiokafor I, Emenike A. Sustainable data governance in the era of global data security challenges in Nigeria: a narrative review. World Journal of Advanced Research and Reviews. 2023;17(2). doi:10.30574/wjarr.2023.17.2.0154.
3. Aidonojie P, Majekodunmi T, Eregbuonye O, Ogbemudia I. Legal issues concerning data security and privacy in automated income tax systems in Nigeria. Hang Tuah Law Journal. 2024;8(1). doi:10.30649/htlj.v8i1.223.
4. Akanbi H. A literature review on cybersecurity in Nigeria. SSRN Electronic Journal. 2024. doi:10.2139/ssrn.4816087.
5. Alsalama A, Alzahrani M. Cybersecurity in oil and gas 4.0: a systematic literature review of challenges, threats, and mitigating measures. Abu Dhabi International Petroleum Exhibition and Conference. 2024. doi:10.2118/222581-MS.
6. Anyanwu A, Olorunsogo T, Abrahams T, Akindote O, Reis O. Data confidentiality and integrity: a review of accounting and cybersecurity controls in superannuation organizations. Computer Science and Information Technology Research Journal. 2024;5(1). doi:10.51594/csitrj.v5i1.735.
7. Arpaci I, Sevinc K. Development of the cybersecurity scale (CS-S): evidence of validity and reliability. Information Development. 2021;38:218–226. doi:10.1177/0266666921997512.
8. Bature B. An empirical study of the Nigerian Extractive Industries Transparency Initiative. 2014.
9. Benz M, Chatterjee D. Calculated risk? A cybersecurity evaluation tool for SMEs. Business Horizons. 2020;63:531–540. doi:10.1016/j.bushor.2020.03.010.
10. Ebelogu C, Prasad R, Bisallah H, Hammawa B, Musa I. Investigation of cybersecurity vulnerabilities and mitigation strategies in Nigeria's oil and gas industry. ABUAD Journal of Engineering Research and Development. 2025;8(1). doi:10.53982/ajerd.2025.0801.15-J.
11. Egbon O. Accountability through Extractive Industries Transparency Initiative: whose accountability. 2015.
12. Ejiogu A, Ejiogu C, Ambituuni A. The dark side of transparency: does the Nigeria extractive industries transparency initiative help or hinder accountability and corruption control? British Accounting Review. 2019. doi:10.1016/j.bar.2018.10.004.
13. Faklaris C, Dabbish L, Hong J. Do they accept or resist cybersecurity measures? Development and validation of the 13-item security attitude inventory (SA-13). arXiv. 2022. doi:10.48550/arXiv.2204.03114.
14. Familoni B, Shoetan P. Cybersecurity in the financial sector: a comparative analysis of the USA and Nigeria. Computer Science and Information Technology Research Journal. 2024;5(4). doi:10.51594/csitrj.v5i4.1046.
15. Haapamäki E, Sihvonen J. Cybersecurity in accounting research. Managerial Auditing Journal. 2019. doi:10.1108/MAJ-09-2018-2004.
16. Hamad W, Pupovac S, Moerman L. Transparency and public accountability: does the Nigerian extractive industries transparency initiative deliver? Extractive Industries and Society. 2024. doi:10.1016/j.exis.2024.101514.
17. Kannelønning K, Katsikas S. A systematic literature review of how cybersecurity-related behavior has been assessed. Information and Computer Security. 2023;31:463–477. doi:10.1108/ICS-08-2022-0139.
18. Li Y, Umair M, Guliyeva S, Shakaraliyeva Z. The extractive industries transparency initiative: achieving disclosure, but falling short on corruption reduction. Extractive Industries and Society. 2025. doi:10.1016/j.exis.2024.101602.
19. Ling J, Feng K, Wang T, Liao M, Yang C, Liu Z. Data modeling techniques for pipeline integrity assessment: a state-of-the-art survey. IEEE Transactions on Instrumentation and Measurement. 2023;72:1–17. doi:10.1109/TIM.2023.3279910.
20. Mehdiyev S, Hashimovv M. Analysis of threats and cybersecurity in the oil and gas sector within the context of critical infrastructure. International Journal of Information Technology and Computer Science. 2024. doi:10.5815/ijitcs.2024.

About the corresponding author

Muhammed Ibrahim is affiliated with the School of Computer Science & Engineering at Geeta University. His academic interests include computer science, data analysis, and emerging technologies. He is actively engaged in research, focusing on innovative solutions in computing, and contributes to academic writing and scholarly activities in his field.