



Veritatis Gaudium:
Multidisciplinary Journal of Postgraduate Studies

College of Postgraduate Studies,
Veritas University, Abuja, Nigeria

ISSN: 3043 - 5285

Volume 1, Number 4, August Special Edition, 2026

DOI: 10.13140/RG.2.2.17243.12321

THE IMPACT OF INFORMATION TECHNOLOGY ON FRAUD DETECTION IN JOS NORTH LGA

Bello Taofikat Akorede

Department: General Studies, Federal polytechnic N'yak, Shendam, Plateau state
taofikatakorede@Gmail.Com

&

Benjamin Sheyin Lazarus

Department: Sociology, Federal University of Lafia
benjaminsheyin@gmail.com

Abstract

Fraud has become a growing concern for organizations due to the increasing use of digital technologies and online transactions. The study examined the impact of information technology on fraud detection in Jos North LGA, focusing on artificial intelligence (AI), cybersecurity systems, and the Internet of Things (IoT). A survey research design was adopted, and data were collected from 176 professionals in financial institutions in Jos North Local Government Area, Plateau State. The findings revealed that AI significantly improves the detection and tracking of fraudulent activities, while cybersecurity systems enhance the identification and prevention of suspicious transactions. The study also found that IoT contributes to real-time monitoring and fraud detection. Overall, respondents agreed that information technology has strengthened fraud detection processes and improved organizational capacity to combat fraud. The study concludes that adopting advanced technological tools is essential for effective fraud management and recommends increased investment in cybersecurity infrastructure, AI-based systems, and professional training.

Keywords: Information Technology, Fraud Detection, Artificial Intelligence, Cybersecurity, Internet of Things, Financial Institutions.

Introduction

Fraud is a persistent global problem affecting both public and private organizations worldwide. The proliferation of digital banking, e-commerce, mobile payments and cloud computing has magnified vulnerability points while simultaneously enabling sophisticated detection mechanisms through information technology (IT). Cybercrime, identity theft, transaction manipulation, cloud based accounting systems have expanded the scope of fraudulent activities. Traditional fraud detection methods often rely on manual audits and human observation and are increasingly insufficient for detecting complex digital fraud schemes. As a result, technological fraud detection methods have become essential.

Research shows that information technology-based investigation systems significantly improve fraud disclosure by enabling digital evidence gathering, analytical review and investigative auditing (Meiryanl et al. 2023). Similarly, big data analytics and technology-driven forensic accounting methods improve fraud and cybercrime detection performance (Kabara and Aliyu2025). Consequently, information technology has become central to contemporary fraud detection strategies, enabling faster and more accurate identification of suspicious activities.

Information technology (IT) has emerged as a critical tool in fraud detection through the deployment of advanced analytics, artificial intelligence, machine learning and real-time monitoring systems. These technologies allow organizations to process vast volumes of structured and unstructured data, identify hidden patterns and detect anomalies that may indicate fraudulent behaviour. Data mining and predictive analytics support the discovery of irregular transaction patterns and behavioural deviations that are difficult to uncover using conventional audit techniques (Bolton&hand 2002). Machine learning further enhances detection by continuously learning from historical fraud cases and adapting to new fraud tactics, thereby improving detection accuracy over time (Ngsi et al., 2011).

Statement of the Problem

Fraud remains a major challenge across both public and private organizations despite regulatory controls and traditional audit practices. The growth of digital transactions, online systems and automated platforms has expanded the fraud risk exposure. However, modern fraud schemes exploit digital platforms, automated systems and connected devices, while traditional methods are insufficient for high volume digital transactions. Studies have shown that technological advancement, while promoting efficiency, has also created new channels through which fraudsters exploit system weaknesses (Albert et al., 2019).

Furthermore, the increasing reliance on digital platforms has led to the emergence of new forms of fraud

Objective of the study

- i. To explore how artificial intelligence contributes to fraud detection
- ii. To evaluate the impact of cybersecurity systems on fraud detection
- iii. To examine how the Internet of things enhance fraud detection process

Literature review

Information technology (IT)

There is no doubt that the use of IT is changing the business development within an organization in general and the nature of each function within the organization in particular. And as such, there is no doubt that the use of IT is changing the nature of fraud detection in both the public and private sectors. Exactly, without support and deep technological knowledge, it can be very challenging and hard for the auditor to give their opinions. Users of financial statements, in general, believe that one of the main objectives of IT is the discovery of fraud. Technologists' responsibilities regarding fraud in financial statements begin with a skeptical and professional attitude. Information technologists neither assume that management is not honest nor assumes no questionable integrity. In exercising

professional skepticism, the auditor should not be satisfied with less convincing evidence for the belief that management is honest. Auditors of financial statements should know enough regarding fraud, note its signs and signals, and should understand fraud and its potential situations. They require complex investigations, dealing with different fields of knowledge, such as the financial economy, law, and business practices, using traditional methods for detecting fraud. Fraud often consists of many cases or incidents involving repeated violations using the same method of Fraud cases.

IT auditor's role in controlling and preventing fraud all auditors are responsible for detecting, determining and using anti-fraud programs. Auditing standards emphasize that auditors should exercise their professional skepticism to determine the risk posed by fraud. They require auditors to assess fraud-related activity as a component of the internal audit function. It is very difficult to prevent fraud, which is considered under three main issues: prevention, detection, and investigation. IT internal audit should help in preventing and detecting fraud. Some of the measures to be taken to prevent fraud are: Internal Audit (IA) must help to ensure the prevention of fraud by communicating information to the Internal Audit Committee and other related managerial committees; Insurance activity control of the IA should support the necessary confidentiality, anonymity, providing obvious evidence; Internal audit team can be instrumental in developing the risk profile of fraud within the organization and design audit programs to find areas of business thought to increase risk; IA can help to assess whether the tone and culture within a business is enough to recognize fraud as unacceptable behavior; Individuals must be receptive to the possibility of fraud and IA may play a role in auditing and efficiency of procedures for the detection and apprehension of fraud. An element that helps in detecting fraud is a combination of internal audit work, internal control and external audits. However, there is a doubt about who discovers fraud, evaluates and tests the operating effectiveness of controls adopted. But in what percentage of fraud cases are discovered by the auditor and especially by the IT auditor? Consequently, most of the IT audit programs appear to be focused on compliance with established procedures, standards of IT systems and internal control questionnaires (ICO), run in such a way to discover potential fraud and ensure the effectiveness of anti-fraud controls. This is because there are gaps in the IT auditors, such as: orientation towards technology or trends that have the IT auditors waiting for fraud to be discovered by the financial auditor. In completing the assessment of fraud risk associated with IT processes and controls, the IT auditor can build an ICO (internal control questionnaire) to evaluate and test the control, including antifraud program. While the financial auditor can evaluate the controls over financial data business, the IT auditor should focus on the area around the system ICT (information control technology) and processes related to ICT.

IA helps gather information about the existence and nature of the reporting structure and in handling reporting allegations. IA should see the trends and symptoms so that they focus attention on their future work and ensure the lessons of past fraud. The use of ICT in businesses nowadays includes evidence to be put to work in a favorable way for verification and confirmation of an occurrence of fraud. Evidence collected by the ICT system can be used very well to find fraud cases. IT auditors tend to have the best teams specializing in IT systems, so they are able to detect fraud. IT audits begin investigations in many activities, such as generating and reviewing reports, identifying the 3 (SAS) 99, AICPA (American Institute of Certified Public Accountants). The use of technology in preventing and detecting fraud involves records and computer systems, in terms of logical analysis of the computer system (analysis of the legality of the system, etc.). Structured risk assessment of fraud, adjusted to the size of the organization, the complexity, industry and goals, should be performed and updated periodically. An organization should understand the risks of fraud and the specific risks that directly or indirectly apply to the organization to protect itself and its stakeholders in an effective and efficient fraud. Assessment can be integrated with a general assessment of organizational risk, but should, at a minimum level, include risk identification, risk assessment of the likelihood and importance of risk response. Assessment of the risk of fraud by evaluating the likelihood and importance of fraud is related to IT processes. The first industries that used techniques to analyze data to prevent fraud are phone companies, insurance companies and banks (Decker, 1998). An early

example of successful implementation of the techniques of data analysis in the banking industry is fraud in the Falcon system, which was based on a computer network (Brachman et al., 1996). Retail industries also suffer from POS fraud. Some supermarkets have begun to make use of digitized television closed-circuit (CCTV), together with details of POS transactions more susceptible to fraud (Eeir, 2001). Transactions of the internet recently have raised major concerns. Kerr (2002) suggests that fraud in transactions on the internet is 12 times higher than fraud in shops. Fraud involving mobile phones, insurance claims, tax returns, transactions with credit cards, etc., poses significant problems for governments and businesses, but is not a simple task of fraud detection and prevention. Fraud is an adaptive crime, so it needs special methods of intelligent data analysis to detect and prevent it. These methods exist in the areas of Knowledge Discovery in Databases (KDD), the use of machinery and statistics. They successfully offer solutions and applications in various areas of fraud.

Techniques for detecting fraud

The techniques used for detecting fraud are divided into two main classes: statistical techniques and artificial intelligence (Palshikar, 2002). Examples of techniques of statistical data analysis are: (1) Techniques of data processing for discovery, validation and error correction. (2) Calculation of various statistical parameters such as averages, performance, probability distributions and so on. (3) Probability distribution models of various business activities, or different terms or parameters of probability distributions. (4) Classification of data to find patterns and differences between groups of data. (5) Compatibility algorithms to detect anomalies in the behavior of transactions compared with patterns and known profiles. Techniques are necessary to eliminate false alerts, assess risk, and predict the future of the current transaction. Management fraud is a knowledge-intensive activity. The main techniques used for management of fraud include: (1) Classification, aggregation and segmentation of data, so that these data can create interesting patterns,

Fraud

Idowu and Adedokun (2013) define fraud as a deliberate deception with the design of securing something by taking unfair advantage of others' loss by means of cheating dishonestly duplication, or imposition. Fraud is also defined in law as an intentional misrepresentation of material existing fact made by one person to another with knowledge of its falsity and for the purpose of inducing the other person to act, and upon which the other person relies with resulting injury or damage. Fraud may also be made by an omission or purposeful failure to state material facts, which nondisclosure makes further statements deceptive. Korpelainen (2011) also stressed that the international guidelines consider an act fraudulent if it takes the following forms: manipulation, falsification, or alteration of records or documents; misappropriation of assets; suppression or omission of transaction records or documents; encoding transactions without substance; misappropriation of accounting policies; if it is material and deceitful. Fraud may also be made by an omission or purposeful failure to state material facts, which nondisclosure makes other statements misleading and can either come by consumer fraud, corporate fraud, and insurance fraud, (Jaya, Mohd & Azwadi, 2012) It can also be deduced from those earlier definitions stated, that the following elements are common to the definitions and when combined will give a clear idea of the nature of fraud: Criminal acts, an act with the intention to act and actually carrying out such acts are injurious to the society and forbidden by law; Illegal acts, these are acts that are not authorized both by law or owner of the property fraudulently obtained; Tortuous acts, wrongful acts either by commission or omission, which affects the rights of another individual and therefore affects the society; Deceptive acts, acts that are engaged in to deceive another person with the intension to enjoy some benefits at the expense of the person being deceived. Deception is also known as the top dog of fraud (Wells 2005); concealed acts, these are criminal deceptive acts such that their perpetrators are hidden from the knowledge of others. As a result of this, both private and public sectors are vigorously investigating how to stay ahead of these swindlers by increasing the level of technological sophistication ahead of fraud culprits.

Theoretical framework

This study adopted two theories, namely routine activity theory and deterrence theory. Routine activity theory was developed by Cohen and Felson 1979 to explain how crime occurs based on everyday activities and environmental conditions. The theory states that crime is likely to occur when three elements come together: a motivated offender, a suitable target, absence of capable guardians. The theory emphasizes that crime is not only influenced by criminal motivation but also by opportunity and situational factors. Applying it to the topic, information technology plays a major role in disrupting the three elements of crime identified by Routine Activity Theory, particularly by strengthening guardianship and reducing opportunities for fraud acts as a capable guardian by monitoring financial transactions and detecting suspicious behaviour. Information technology serves as a modern guardian that protects systems and transactions from fraudulent activities; for example artificial intelligence, biometric systems, fraud detection software and machine learning technologies monitor and reduces financial transactions and identify suspicious patterns, while IT strengthens surveillance and makes it difficult for fraudsters to exploit victims. This theory is widely used to explain how IT reduces fraud opportunities by increasing monitoring and security controls. Critics argue that the theory focuses mainly on situational factors and neglects social, psychological and economic causes of crime such as poverty, unemployment and inequality. Also, the theory emphasizes that crime occurs due to opportunity and fails to explain why some individuals become motivated offenders and others do not. In conclusion, routine activity theory provides a strong framework for explaining how information technology improves fraud detection by increasing guardianship, reducing targets' vulnerability and limiting opportunities for fraud. However, the theory has limitations because it does not fully address the root causes of crime or the complexity of cyber fraud. Combining routine activity theory with other theories can provide a more comprehensive understanding of the impact of information technology on fraud detection.

Deterrence theory originates from classical criminology and was developed by Beccaria (1764) and Bentham (1789). This theory is based on the assumption that individuals are rational actors who make decisions by weighing the potential benefits of committing crime against the risk and consequences associated with it. According to this theory, crime can be prevented when punishment is characterized by certainty, swiftness and severity. Information technology enhances the likelihood of detecting fraud through real-time monitoring systems. Digital audit trails make it easier to track fraudulent transactions and the increased chance of being caught discourages individuals from committing fraud. This theory explains how IT improves the speed at which fraud is detected and investigated; automated fraud detection systems generate instant alerts when suspicious activities occur, and it also allow investigators to conduct faster and more efficient fraud investigations.

Methodology

Research Design

The study adopted a survey research design, which is suitable for collecting data from a large population sample to assess the impact of information technology on fraud detection.

The survey research design helps to obtain data from IT Professionals, Internal Auditors, and front desk officers in Financial institutions in Jos North LGA.

Sample size and Sample procedure

The study adopted the Yamane (1967) formula for sample size; the Yamane sample size was chosen for its simplified formula used to determine an appropriate sample size (n) from a finite population (N) with a pre-determined margin of error (e).

The study measures the impacts of information technology on fraud detection in Jos North LGA. The study employed a purposive sampling procedure to collect data on the impacts of information technology on fraud detection. Jos North LGA was selected due to the prevalence of fraud and attempts by security agencies to detect such fraudulent activities.

Sources of Data

Data were collected using the Questionnaire method of data collection; a questionnaire was employed to collect important information for the research. The questionnaire was titled “Questionnaire on the impacts of Information technology on fraud detection in Jos North Local Government Area, Plateau State. It was organized into sections.

Method of Data Collection

The Data were collected with a structured questionnaire using a 5-point Likert-scale type; the responses were categorized into: Strongly Disagree (1), Disagree (2), Neutral (3), Agree (4), and Strongly Agree (5). A criterion mean of 3.00 was recognized for decision purposes, in that a mean score of 3.00 and above shows agreement and scores below show disagreement. The questionnaires were collected through face-to-face interaction by the researchers.

Method of Data Analysis

The data collected were analyzed using descriptive statistics such as frequencies percentage for Table 1. (Demographics of respondents) and Descriptive Mean for Section B.

Results and Discussion

Table 1.

Demographic of Respondents

Guide	Various items	Frequency	Percentage
Department/Unit			
	Internal Audit	32	18.18
	Cyber Security	40	22.73
	Risk Management	29	16.48
	Fraud Desk	38	21.59
	Others.	37	21.02
	Total	176	100
Years of professional Experience			
	0-3	58	32.95
	4-7	67	38.06
	8-11	34	19.32
	Above 12 years	17	
9.67	Total	176	100
Highest Qualification			
	HND/BSC	103	
58.52	MSc/MBA/MA	39	22.16
	PhD	13	7.39
	Others	21	11.93
	Total	176	
100			
Relevant Professional Certification (s)			
	ACA/ACCA/ANAN/ICAN	69	
39.20	CISA/CISM/CISSP	33	
18.75	CFE-Certified Fraud Examiner	48	
27.27			

8.52	ACIB	15	
3.98	Non yet	7	
2.27	Others	4	
	Total	176	99.99

Please note that the total percentage is 99.99% due to rounding.

The Demographic distribution of Department shows that Cyber security experts percentage is 22.73% indicating they have a vast knowledge of the research topic and that adequate response will be given, followed slightly by fraud Desk officers 21.59% fraud desk officers are trained officers who track fraud , monitor and stop fraud transactions, this high percentage shows the propability of getting the right experts opinion of the impact of information technology on fraud detection, internal audit officers 18.18%, risk management 16.48%, others 21.02%. The Departmental demography shows that the respondents include experts in various departments with vast knowledge of information technology and fraud detection.

Years of experience of respondents in financial institutions, respondents with (4-7) years has the highest percentage of 38.06%, also respondents with (0-3) experience has 32.95%, while respondents with higher level experience (8-11) years participated in the research with 19.32%, finally, respondents with 12 years and above of experience have 9.67%. In general the research captures all level of officers with different years of professional experience, however officers with (4-7) 38.06 % has the highest participation rate.

Educational level of respondents indicates that 58.52% of the respondents obtained HND/BSC Degree, which proves that large percentage of the respondents are literate and able to respond appropriately to the questionnaire. 22.16% of the respondents obtained MSc/MBA or MA; this shows a higher level of literacy of the participants. 7.39% obtained a PhD, and 11.93% with other qualifications.

For relevant professional certificates 39.20 % are certified ACA, ACCA, ANAN, ICAN; they are considered professionals in the field. 27.27% are certified fraud Examiners, while 18.75 are certified by CISA/CISM/CISSP. ACIB-certified officers represent 8.52% of the respondents, 3.98% are yet to be certified and others represent 2.27%. A large percentage of the respondents are certified professionals in the financial institutions and fraud related departments.

Section B; Impacts Of Information Technology On Fraud Detection

Table 2

S/N	EFFECTS OF ARTIFICIAL INTELLIGENCE ON FRAUD DETECTION	Level of agreement					X			
		SD	D	N	A	SA	Mean	Std.Dev	Decision	
1.	Artificial intelligence is effective in fraud detection	12	28	17	42	77	3.82	1.33	Agree	
2.	The use of Artificial intelligence has reduced fraud in the past 5 years	8	29	9	47	83	3.95	1.26	Agree	
3.	The use of Artificial Intelligence improves tracking of Fraudsters	6	10	16	46	98	4.25	1.06	Strongly Agree	

Grand Mean

4.01

Agree

Please note. N176. SD=Strongly Disagree, D =Disagree, N= Neutral, A = Agree, SA = Strongly Agree.

Std. Dev= Standard Deviation. Criterion mean= 3.00. Decision rule: 1.00-1.80=Strongly Disagree, 1.81-2.60=Disagree, 2.61-3.40=Neutral, 3.41-4.20=Agree, 4.21-5.00=Strongly Agree

Table2. Presents the descriptive statistics on respondent's views on the effects of Artificial Intelligence on fraud detection. The above results indicate that all items were accepted with mean score ranging from 3.82 to 4.25 on a 5-point scale.

The respondents strongly agreed that the use of artificial intelligence improves tracking of fraudsters, the item recorded the highest mean of M=4.25, SD=1.06. This aligns with Lee et al. (2025) who found that AI Models demonstrate superior predictive power in identifying complex fraudulent patterns that elude traditional systems. They also agreed that the use of Artificial intelligence has reduced fraud in the last 5 years (M=3.82, SD=1.33).

The values of the Standard Deviation indicate moderate spreading in responses. Item 3 recorded the lowest standard Deviation of 1.06, suggesting a strong consensus among respondents that the use of AI improves tracking of fraudsters. Item 1 recorded the highest standard deviation of 1.33, indicating respondents were relatively more divided on the general effectiveness of AI in fraud detection. This disparity may reflect broader challenges in the field; Moura et al. (2025) stated that attention to ethical, regulatory, and organizational issues in AI fraud prevention remains limited. With a Grand Mean of 4.01, the findings imply that respondents agree that artificial intelligence has Positive effects on fraud detection.

Table 3

S/N	THE IMPACTS OF CYBER SECURITY ON FRAUD DETECTION	Level of agreement of					X			
		SD	D	N	A	SA	Mean	Std.Dev	Decision	
1.	Cyber Security has greatly improved fraud detection	2	3	6	56	109	4.52	0.75	Strongly Agree	
2.	Cyber Security prevents fraud from occurring	6	8	26	47	89	4.16	1.06	Agree	
3.	Cyber security detects fraudulent transaction	8	7	17	46	98	4.24	1.08	Strongly Agree	
	Grand Mean						4.31		Strongly Agree	

Please note. N176. SD=Strongly Disagree, D =Disagree, N= Neutral, A = Agree, SA = Strongly Agree.

Std. Dev= Standard Deviation. Criterion mean= 3.00. Decision rule: 1.00-1.80=Strongly Disagree, 1.81-2.60=Disagree, 2.61-3.40=Neutral, 3.41-4.20=Agree, 4.21-5.00=Strongly Agree.

Table 3. Presents the descriptive statistics on respondents' opinions of the impacts of Cyber Security on fraud detection. The results on the table shows that all items were accepted with mean score ranging from 4.16 to 4.52 on a 5 –point scale.

Precisely, respondents strongly agreed that cybersecurity has greatly improved fraud detection, as this item recorded the highest mean score of $M=4.52$, $SD=0.75$. “This aligns with Polak et al. (2020), who assert that fraud detection mechanisms help detect unusual transactions and prevent cybercrime.” Respondents also strongly agreed that Cyber Security detects fraudulent transactions ($M=4.24$, $SD=1.08$). Nevertheless, respondents only agreed that cyber security prevents fraud from occurring ($M=4.16$, $SD=1.06$), which recorded lowest mean.

The low standard deviation of 0.75 for item 1 indicates strong consensus among respondents that cyber security has improved fraud detection. “This consensus reflects findings by Polak et al. (2020) that fraud detection mechanisms help detect unusual transactions and prevent cybercrime. However, the relatively lower mean for prevention ($M=4.16$) aligns with UNODC (2024) observations that fraudsters now leverage AI for more adaptive schemes, suggesting that while detection capabilities are widely acknowledged, preventive measures face evolving challenges. SDs of 1.06 and 1.08, respectively showed moderate distribution. Generally, the grand mean of 4.31 shows that respondents strongly Agree that cyber security has significant positive impacts on fraud detection in Jos North LGA.

Table 4.

S/N	ASSESSING THE IMPACTS OF INTERNET OF THINGS ON FRAUD DETECTION	Level of agreement of					X		
		SD	D	N	A	SA	Mean	Std.Dev	Decision
1.	Internet of Things detects fraud in real time	22	8	12	56	78	3.91	1.35	Agree
2.	Internet of Things tracks fraudulent transactions	13	17	32	45	69	3.80	1.26S	Agree
3.	Internet of Things prevents fraudulent activities	7	11	9	65	84	4.18	1.05	Agree
Grand Mean							3.96		Agree

Rule: 1:00-1.80=SD, 1.81-2.60=D, 2.61-3.40=N, 3.41-4.20=A, 4.21-5.00=SA

Note. N=176. SD=Strongly Disagree, D=Disagree, N=Neutral, A= Agree, SA=Strongly Agree.

Std. Dev = Standard Deviation. Criterion mean =3.00. Decision rule: 1.00-1.80 =Strongly Disagree, 1.81 -2.60 = Disagree, 2.61 -3.40=Neutral, 3.41 -4.20 =Agree, 4.21 – 5.00 = Strongly Agree.

The table above shows descriptive statistics respondents views of the impact of internet of Things on fraud detection. The results reveals that all items were accepted, with a mean score between 3.80 and 4.18 on a 5-point scale.

Respondents agreed that the Internet of Things prevents fraudulent activities; it recorded the highest mean of $M=4.18$, $SD=1.05$. They also agreed that the Internet of Things detects fraud in real time (Mean=3.91, $SD=1.35$) and tracks fraudulent transactions. “This supports findings by Zenobo (2024) that AI analytics platforms enable real-time fraud detection through pattern analysis” ($M= 3.80$, $SD=1.26$), which had the lowest mean.

Moderately high standard deviation of 1.35 for item 1 highlights division in responses, it shows respondents were mostly divided on IoT’s ability to detect fraud in real time, for item 3 it recorded the lowest SD of 1.05, it shows that a strong consensus that IOT Prevents fraudulent activities. A

grand mean of 3.96 reveals that respondents agree that the Internet of Things has a positive impact on fraud detection.

Summary

1. The findings of the research show that artificial intelligence is effective in tracking fraudsters.
2. The respondents, who are mainly experts in the field, generally agree that Artificial intelligence is a major booster in reducing fraudulent activities in the past 5 years in Jos North LGA.
3. The findings reveals that, respondents unanimously accept that application of cyber security prevents fraud from occurring.
4. In addition, the results from the research reveal that the Internet of Things detects fraudulent activities in real time.

Recommendations

1. The Study recommends that financial institutions like banks, insurance Companies should priorities the use of Improved Cyber Security features for their operations.
2. The study recommends that periodic training and retraining should be held for IT professionals, internal auditors and other frontline officers in the financial institutions on modern Cyber security tools in detecting fraud.
3. It is recommended that internet of things should be utilized to detect fraud in real time.
4. It is recommended that the Nigerian Police Cyber Crime Unit should collaborate with financial institutions to report fraudulent activities in real time for investigation and prosecution.

References

- Albert, A., Umar, M., & Bello, S. (2019). Information technology and fraud management in modern organizations. *Journal of Accounting and Financial Management*, 5(2), 45–58.
- Beccaria, C. (1764). *On crimes and punishments*. Milan: Publisher.
- Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, 17(3), 235–249.
- Brachman, R., Khabaza, T., Kloesgen, W., Piatetsky-Shapiro, G., & Simoudis, E. (1996). Mining business databases. *Communications of the ACM*, 39(11), 42–48.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608.
- Decker, J. (1998). Data analysis techniques in fraud detection. *International Journal of Risk Management*, 6(1), 20–34.
- Idowu, A., & Adedokun, A. (2013). Fraud prevention and control in organizations. *International Journal of Business and Management Review*, 1(3), 45–56.
- Jaya, I., Mohd, R., & Azwadi, A. (2012). Fraud detection and prevention strategies in organizations. *Asian Journal of Finance & Accounting*, 4(2), 123–137.
- Kabara, A., & Aliyu, M. (2025). Big data analytics and forensic accounting in cybercrime detection. *Journal of Digital Financial Studies*, 8(1), 77–92.
- Kanu, I. A. & Ndubisi, J. O. E. (2022). “Artificial intelligence and socio-economic development in Africa.” *OCHENDO: An African Journal of Innovative Studies*. 3(1), 2-21.
- Onyiah, S. C.; Ndubisi, J. O. E.; Kanu, A. I. (2024). “Navigating the Ethical Implications of Artificial Intelligence through Carol Gilligan’s Ethics of Care.” *Aquino Journal of Philosophy*. 4(2), 1-12.
- Kanu, A. I.; Addidi, T. D.; Kanu, C. C. (2024). “Artificial intelligence and cybercrime in Nigeria: Towards an Ethical framework”. *Dialogue and Universalism*, 32(1), 143-158.
- Kanu, A. I. (2025). “Philosophical roots of Artificial Intelligence: Theoretical and practical foundations.” *La Ciudad de Dios, Revista Augustiniana*. 238(1), 235-258.

- Kanu, I. A. & E. J. O. Nsubisi (2026). "Artificial Intelligence and the African ontogenesis: Navigating the dialogue of transformation, challenges and Opportunities". *African Journal of Religion, Philosophy and Culture*. 7(1), 161-177
- Kanu, I. A. & Okpokwasili, O. A. (2025). "Artificial Intelligence, Development and Ethics of Care: A Feminist Perspective on Human-Technology Relations". Nwadiolor, K.; Ulpogu, N.; Adamy, J. N. (Ed.). *Artificial Intelligence, Ethics and Indigenous Wisdom: Rethinking Africa's Cultural and Philosophical Future- Proceedings of the 2025 International Conference of the Association for the Promotion of African Studies (APAS)* (pp. 56-78). Abuja: Association for the Promotion of African Studies
- Kerr, D. (2002). Internet transaction fraud and prevention mechanisms. *Cybersecurity Review*, 3(2), 14–28.
- Korpelainen, P. (2011). Fraud risk management and organizational controls. *European Journal of Business Studies*, 7(1), 60–73.
- Meiryani, M., Susanto, A., & Warganegara, D. (2023). Information technology-based investigation systems and fraud disclosure effectiveness. *International Journal of Accounting Information Systems*, 49, 100612.
- Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559–569.
- Palshikar, G. K. (2002). The hidden truth about fraud. *Computers & Security*, 21(1), 13–27.
- Wells, J. T. (2005). *Principles of fraud examination*. Hoboken, NJ: John Wiley & Sons.
- Ahmed, M., Mahmood, A.N., & Islam, M. R. (2016). A survey of anomaly detection techniques in financial domain. *Future Generation Computer Systems*, 55, 278-288.
- Moura, L., Barcaui, A., & Payer, R. (2025). AI and financial fraud prevention: Mapping the trends and challenges through a bibliometrics lens. *_ MDPI, information*, 16 _ (6), 484.
- Polak, P., Nelischer, C., Guo, H., & Robertson, D.C. (2020). "Intelligent" finance and treasury management: what we can expect. *_ AI & Society*, 35 _ (3), 715- 726.
- UNODC. (2024, October). Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape. United Nations Office on Drugs and Crime.
- Zenodo. (2024). Fraud detection using database analytics – case studies on database queries and Anomaly detection.