ARTIFICIAL INTELLIGENCE AND CYBER SECURITY: IMPLICATIONS FOR E-TRANS AND E-ACCOUNTING IN EMERGING ECONOMIES.

Odogu Terry Keme Zuode (Ph.D.)

Department of Accounting, Management Sciences, University of Africa, Toru-Orua Bayelsa State, Nigeria.

Cite this article:

Odogu, T. K. Z. (2024), Artificial Intelligence and Cyber Security: Implications for E-Trans and E-Accounting in Emerging Economies. African Journal of Accounting and Financial Research 7(4), 152-168. DOI: 10.52589/AJAFR-SB1GX3VI

Manuscript History

Received: 14 Sep 2024

Accepted: 13 Nov 2024

Published: 25 Nov 2024

ABSTRACT: *This study was motivated by the increasing and seemingly unstoppable nature of cybercrimes and the perceived effect on data safety and reliability in accounting practice. Consequently, this study is poised to ascertain the relationship between artificial intelligence-driven electronic transactions and data loss, theft and manipulation; as well as to ascertain the effect of artificial intelligence-based electronic accounting on data safety and reliability. It adopted a survey design to obtain primary data from a sample of 492 professional accountants comprising ACAs, FCAs, CNAs, and FCNAs in the South-south geo-political zone of Nigeria, through a questionnaire. Analysis of variance and regression analysis from SPSS test results disclosed a significant nexus between artificial intelligence-driven electronic transactions and data loss, theft and manipulation. The test results also revealed that the adoption and recognition of artificial intelligence-based electronic accounting significantly affect the safety and reliability of financial data. Accordingly, this study concludes that, financial data from artificial intelligence-driven electronic transactions are significantly susceptible to data loss, theft and manipulation, and that the adoption and recognition of artificial intelligence-based electronic accounting impairs the security and reliability of financial data. Consequently, this study recommends that firms should be watchful and employ adequate trust management and web security measures and mechanisms in adopting and recognising artificial intelligence-related electronic transactions and accounting. This study further recommends that artificial intelligence technology inventors and engineers should shift focus towards a redefinition, re-engineering and reshaping of artificial intelligence technologies and platforms that can be easily governed and safely benefit users.*

KEYWORDS: Artificial intelligence, cybercrime, electronic transaction, electronic accounting, data security, data reliability, intelligence re-engineering theory.

INTRODUCTION

The widely celebrated benefits of artificial intelligence and its endearing digital technologies are fast becoming questionable due to the emergence and seemingly unstoppable nature of cybercrimes perpetrated in cyberspace. Cybercrimes are fraudulent practices committed with computers and other smart communication gadgets on the internet against targeted victims (Broadhurst & Chang, 2012). Cybercrime has occasioned a huge security challenge and threat to the financial globe, and the accounting practice and domain in particular. It challenges the convenience and efficiency associated with artificial intelligence-related electronic transactions and accounting, and the increasing vulnerability and insecurity of businesses to cybercrimes is becoming a daily concern. For example, the Daily (2018) captured a report by the Canadian National Cyber Security Strategy that Canadian businesses spend approximately $14 billion on cyber security per year. It disclosed that over one-fifth, about 21% of Canadian businesses were impacted by cyber security incidents in 2017 and as a result, about 95% of Canadian businesses employ or consult cyber security (experts) to protect themselves, their customers and their partners. This, of course, is distressing and constitutes a security threat in the cyber-space.

Shull (2018) worrisomely observed that “it is almost impossible to read the news without coming across a lead story cataloguing the latest cyber breach or misuse of data”. He noted that the number of companies that have fallen prey to digital hacking is almost too numerous to count. Evidence from the Nigerian Deposit Insurance Commission Report (2018) and O’Donnell (2019) further revealed that the banking industry in Nigeria lost N15.15 billion to cybercrime and forgeries in 2018, and this was colossally 54% greater than the preceding year’s record of N2.37 billion, with an average attack growth rate of 28,227 per month. The Security Support (2020) submitted that Nigeria suffered about N250 billion ($649 million) and N288 billion ($800 million) financial losses due to cybercrime in 2017 and 2018. Lamentably, despite this huge loss, Security Support (2020) further adduced that the above figures represent an insignificant 5% of cybercrimes perpetrated and that 95% of cybercrimes perpetrated in cyberspace go undiscovered and unreported. Adesoji (2019) opined that this frightening upswing of cybercrime is caused by the electronic-based channels and instruments, which are incontrovertibly artificial intelligence instruments legally engaged by individuals and organisations for electronic transactions and accounting in contemporary times. This is apparently nerve-racking and explicitly defines and explains the problem of this study, as it raises a lot of concern.

This study is primarily motivated by the increasing spate of cybercrime in the current industrial era of artificial intelligence. However, the study is also motivated by a perceived methodological and perception gap. First, most studies on cybercrime are either conceptual or theoretical. Emphatically, a cursory look at the available materials motivating this study revealed that most of the claims and facts on cybercrimes exist in newspapers, periodicals and theoretical and conceptual works. Secondly, most studies on artificial intelligence-related electronic transactions and accounting view their adoption and recognition from a positive perception. Consequently, the objectives of this study are to empirically ascertain the relationship between artificial intelligence-driven electronic transactions and data loss, theft and manipulation; as well as to empirically ascertain the effect of artificial intelligence-based electronic accounting on data safety and reliability.

Article DOI: 10.52589/AJAFR-SB1GX3VI
DOI URL: https://doi.org/10.52589/AJAFR-SB1GX3VI

LITERATURE AND HYPOTHESES FORMULATION

The relevant concepts, theory, and empirical findings of this study are systematically appreciated and reviewed as follows:

Artificial Intelligence and Cybercrime

Artificial intelligence (AI) is the pivot of the current (4th) industrial revolution and has been severally defined by different authors and scholars at different stages of its development over the ages. For instance, Bellman (1978) defined it in the 70s as the automation of activities associated with human thinking such as learning, decision-making, problem-solving, etc. Haugeland (1985) defined it in the 80s as an exciting new effort to make computers and machines think with minds in the full and literal sense. Rich and Knight (1991) described it in the 90s as the study of how to make computers do things better than humans. Russell and Norvig (2009) defined it in the 21st Century as the creation and use of machines that mimic the cognitive functions associated with the human mind, such as learning and problem-solving. Artificial intelligence as it were is the deliberate creation of intelligent machines to simulate and mimic the human brain and intelligence, to optimally address diverse tasks that traditionally require human sophistication. Narrowing it to the accountancy profession, AI is a third-party software device incorporated into the accounting process to electronically perceive the business and accounting environment to mimic and maximise the human functions in the accounting system. The emergence of AI has recorded so many benefits through electronic transactions and accounting (Bairagi, 2011; Chavan; 2013; Khan, 2016). It amongst others reduces ordering, purchasing and selling time and cost, reduces paperwork, increases product visibility, encourages price comparison, facilitates customer enlightenment, simplifies payment and invoicing, enhances feedback and communication, allows real-time access to transaction and accounting records, saves office space, facilitates bank reconciliation and multi-currency trade.

However, there is a growing concern about the attendant cybercrimes perpetrated on these AI-generated electronic transaction and accounting platforms. Cybercrime can be interchangeably called electronic crime, computer crime, computer-related crime, hi-tech crime, technology-enabled crime, or cyberspace crime and can be simply described as a crime committed at targeted victims with computers and other smart communication gadgets on the internet (Broadhurst & Chang, 2012). Cybercrimes are regrettably perpetrated in different forms such as e-mail spoofing, fraudulent e-mails, forgery, cyber defamation, identity theft, cyber nuisance, hacking, spamming, malicious coding, service denial, cyberstalking, sale of illegal articles, malvertising, intellectual property crimes, ransomware, cyberbullying, piracy, botnets, data and airtime theft, plagiarism, fake bank alert messages, denial of service, automated teller machine spoofing and phishing, etc. (Omodunbi et al., 2016; Mupila et al., 2023). Cybercrimes, particularly Type III cybercrime are perpetrated with self-learning AI-aided instruments and require superior AI technologies to detect and manage (Lau & Chang, 2018). The evils of cyber-crime are gradually overshadowing the amplified benefits of artificial intelligence, such that scholars like Lambert (2017) and Xu et al. (2018) have started interrogating the future and prospects of the concept, particularly when our lives and businesses become extensively connected to various sophisticated intelligent devices and gadgets. It is like a cankerworm that dents the beauty of digitalisation and artificial intelligence in the (current) 4th industrial era. It denigrates and abates the dream and focus of the proponents of artificial intelligence.

The alarming rate of security threats that daily manifest in the form of hacking, laundering, data loss, data theft, etc. seems to suggest a rethink of the seemingly over-celebrated concept of artificial intelligence. The most disturbing fact is that cybercrimes are facelessly and intelligently perpetrated by employees, friends, relations and AI experts and consultants. Insistently, the emergence of artificial intelligence and its agents has exponentially increased cybercrime in the last few decades. For instance, in 2019, only the Ibadan zone of the Economic and Financial Crimes Commission (EFCC) secured 167 convictions against cybercrime offenders in Nigeria (Tade, 2019). Consequently, the Federal Government of Nigeria has listed cybercrime as one of its national security threats in its National Security Strategy (Tade, 2019). This invariably implies that cybercrime is a serious threat to electronic transactions and electronic accounting in Nigeria, and is partly the reason for the exponential increase in cybercrime studies over the last few decades (Bossler & Berenblum, 2019). There is, therefore, a need for an empirical study on the implication of artificial intelligence-induced cybercrime on the security and reliability of financial data and accounts.

Artificial Intelligence-driven (Electronic) Transactions and Cybercrime

Electronic transactions (e-transactions) can be interchangeably called electronic commerce and electronic business (Bielski, 2001; Ulgado, 2002; Horn, 2003; Hicks, 2004; Khan, 2016). It is the buying and selling of goods and services on the internet, as well as the sourcing and offering of information about the prices, quality and latest brands of goods (and services) on the internet by potential buyers and sellers (Khan, 2016). Electronic transactions began in the 1990s due to the emergence and diffusion of information communication and technology (ICT), and its transformation of the world to a global community and market, as the internet changed from an information tool to a shopping alternative. However, the emergence of e-transaction is not unrelated to convenience, availability of credit cards, mail order catalogues, overnight (home) delivery and the benefits of digital-supply-chain management that eliminates the period between ordering, delivering, invoicing and payment throughout the World Wide Web (Kariyawasam, 2008; Khan, 2016). However, despite the obvious and widely celebrated benefits of e-transactions in the business world, its recognition in accounting practice is becoming a concern to the accountant and the accounting profession.

Appositely, Abbiati (2003) observed that the greatest trust barrier in the recognition of e-transaction is the protection of sensitive customers and suppliers, which the accountant relates with financially through electronic payments. The use of e-transactions by firms and their recognition in accounting practice requires the accountant to provide web assurance services to gain customers' confidence. This is because the emergence and adoption of e-transactions in the business world have created a “trust gap” between buyers and vendors over the years, which has given the accountant the responsibility of ensuring data security, reliability and confidentiality (Khan, 2016). Specifically, the adoption and recognition of e-transactions have opened the financial doors of firms to cybercrimes and threats from hackers in cyberspace. Unfortunately, these threats and crimes are facelessly meted and perpetrated individually by employees, friends, business partners and rivals inadvertently or intentionally or collectively by unfamiliar external cyder robbery syndicates.

Unequivocally, Cybercrime is the trending bane of e-transaction and accounting in the digital age. It impairs businesses, making the business environment difficult for start-ups and small and medium-sized enterprises, as well as discouraging investment. Consequently, Davis (2016) lamented that the application of artificial intelligence-driven technologies is gradually leading

Article DOI: 10.52589/AJAFR-SB1GX3VI
DOI URL: https://doi.org/10.52589/AJAFR-SB1GX3VI

us to a world of unfamiliarity, uncertainty and insecurity. On this note, Teegmark (2017) cautioned that if artificial intelligence goals are not safely aligned with human goals it might be catastrophic. For instance, cyberspace recorded an international stock price pump-and-dump fraud of over $50 billion in 2017 (Romney, & Steinbart 2017). Back home in Nigeria, the Nigerian Deposit Insurance Commission Report (2018) and Adesoji (2019) separately and differently estimated that the Nigerian banking sector lost N15.15 billion and N15 billion respectively to cyber-crime and forgeries in 2018. In the same direction, Security Support (2020) noted that Nigeria lost N250 billion ($649 million) to cybercrime and fraud in 2017 and that 95% of cybercrimes committed go unreported. Above all, Akintaro (2023) submitted that Fintech firms in Nigeria suffered over N5 billion loss to hackers in 2023. This is nerve-racking and subtly interrogates and challenges the goals and the projected and recorded benefits of the adoption and recognition AI driven transactions in accounting practice. On this premise, the first hypothesis of this study is stated in the null form as:

Hypothesis I (H_1): Artificial intelligence-driven transactions do not significantly increase data loss, theft and manipulations in accounting practice.

Artificial Intelligence-based (Electronic) Accounting and Cybercrime

This is a recent concept in accounting practice and is also called online accounting (Hunton, 2002). It is an improvement in electronic data processing, as well as a response to electronic transactions and AI dynamics and demands. Electronic accounting (e-accounting) is a modern accounting practice where all financial transactions and events are digitally recorded and kept in an online (internet) database or server similar to a website or web blog and are accessed with a login ID and password. Electronic accounting is similar to cloud computing, which entails the permanent storage of (financial) data in web blogs of remote servers of ICT service providers, and the use of a web-based software called software-as-a-service (SaaS). Obviously, electronic accounting is practised with relevant accounting software and programs such as Oracle, Sage, FreshBooks, QuickBooks Online, Xero, Zoho Books, Net Suit ERP, Bright Pearl, Pentana, MSAB- XEC 5.3, Netwrix, Pro-inspector, Myob, Free Agent, Zenefits, AccountEdge, Expensify, Odoo, Tipalti, Intacet, Wave financial, etc. It reduces paperwork, stores large business records, facilitates invoicing, bank reconciliation, and multi-currency trade, as well as enables users to access multiple sites (Fitriati & Mulyani, 2015).

However, the adoption of e-accounting requires a huge capital outlay and a high broadband internet connection (Rogoff, 2012; Oladipupo, & Ajabe, 2013; Prisecaru, 2016; Peters, 2017). Furthermore, the emergence and adoption of e-accounting is gradually changing the language of business from accounting to information and communication technology and has worrisomely opened the door of the accounting profession to every Tom, Dick and Harry that is good at information and communication technology, subjecting the accountant to web designers and ICT experts, and eroding the pride and honour of the accounting profession and its practitioner. Thus,

the advancement and influence of AI in and on the accounting industry are seemingly pressurizing practitioners to acquire new AI skills or face the risk of losing their irrelevance and jobs to AI experts. Most worrisomely, the emergence of e-accounting has made accounting information and records susceptible to hackers and different forms of cybercrime and or fraud, which can result in irrecoverable data and financial losses. For example, the websites of

Article DOI: 10.52589/AJAFR-SB1GX3VI
DOI URL: https://doi.org/10.52589/AJAFR-SB1GX3VI

Citibank and WeaKnees.com were hacked and about $10 million and $50 billion were artificially stolen by Russian hackers (Romney & Steinbart, 2018).

Back home in Nigeria, Akintaro (2023) documented in Tech News that three Nigerian Fintech firms suffered a huge financial loss of about N5 Billion to hackers in the first 8 months of 2023. Similarly, Michael (2024) reported in Business Day that in 2023 the Nigerian inter-bank settlement scheme recorded N9.37 billion and N2.43 billion losses to social engineering and website/server hackers in Nigeria's cyberspace. Furthermore, Adepetun (2024) reported in the Guardian that there was an attempt by hackers to compromise the website of Guarantee Trust Bank (GTB) on the 16th of August, 2024, which significantly disrupted its operations and transactions. The ills of cybercrime are grossly overshadowing the recorded and anticipated benefits of artificial intelligence-based accounting (Goode, 2018). Except superior technologies are urgently innovated and applied to check and neutralise this menace and practice, the fear is, that cyberspace might soon become a beautiful snare or the biblical white sepulchre, which most probably might limit and defeat the ultimate goals of artificial intelligence in modern accounting practice. Against this backdrop, the second hypothesis of this study is stated in the null form as:

Hypothesis II (H_2): Artificial intelligence-based accounting does not significantly threaten the reliability of financial data.

Theoretical Framework

This study is underpinned by intelligence re-engineering theory, which in this context believes that the ills associated with the adoption and recognition of artificial intelligence-driven transactions and accounting can be checked and controlled by re-engineering AI tools and gadgets with precautionary measures and techniques. This theory proposes a shift of focus from absolute trust and reliance on artificial intelligence machines to a new science of safety engineering, that will neither allow AI machines the privilege to begin and end transactions or accounting tasks nor give them the absolute right to make decisions (Yampolskiy, 2013). The proponents of this theory believe that the attribution and assignment of moral agency and rights to intelligent machines, infrahuman and superhuman AIs are misguiding and that the behaviour of AIs should be constrained to limit their negative effects, and therefore propose an AI re-engineering development that would make intelligent systems have human-friendly values (Yampolskiy & Fox, 2016). This is in response to the increasing cybercrimes associated with the adoption and recognition of AI-driven transactions and accounting, and is in agreement with the philosophy of Tegmark (2017) that, "civilisation would flourish and guarantee a safe future if we amplify our human intelligence with artificial intelligence and manage to keep the technology beneficial".

Accordingly, this theory proposes that, as AI technologies inexorably shift from simple digitisation to multi-network-digitization, engineers and managers must innovatively re-engineer and re-strategize to timely and safely align AI goals with socio-corporate goals (Xu et al., 2018). It is against this backdrop that Schwab & Davis (2018) remarked that, as the digital world is fast becoming an invisible fabric, the survival of corporate entities largely depends on a set of cyber-physical systems, which urgently require new ways of thinking about technologies and ourselves. It calls for the development and application of some safe agents and learning programmes such as interruptible/ignorant/inconsistent/bounded agents and inverse reinforcement learning (Kose, 2018). This is arguably the solution to the report by

Article DOI: 10.52589/AJAFR-SB1GX3VI
DOI URL: https://doi.org/10.52589/AJAFR-SB1GX3VI

Scalar Decisions Inc. (2018) that in 2017, nine out of ten Canadian businesses suffered cybersecurity breaches that resulted in financial theft and loss of sensitive data. The argument is cybercrimes are perpetrated with human-made smart AI software, programmes and tools by smart AI experts, and can therefore be checked through preventive re-engineering and redesigning because machines on their own don’t have objectives (Russell, 2019). This entails a recognition of the strengths and limits of AI software, programmes, applications, platforms and machines to develop technologies for humans and computers to safely work together (Gillon, 2019).

Empirical Review

As earlier noted, most studies on cybercrime and AI-driven (electronic) transactions and or accounting are conceptual in methodology and consider only the positive aspect of electronic transactions and accounting. However, Haque et al. (2009) empirically investigated the perception of Malaysians about electronic transactions and found that electronic transaction platforms are prone to scams and are not always trusted by users. The study adopted a survey design to obtain primary data from 250 Malaysian online transaction and banking platform customers through a questionnaire. Factor analysis and structural equation model results revealed that only protected transactions have a significant impact on consumers’ perception of electronic transaction security. Mshana (2015) also conducted an empirical study on the impact of cybercrime on society and submitted a negative impact. Primary data were obtained through questionnaires and interviews from multiple respondents comprising students of educational institutions, musicians, actors and staff of companies in Tanzania, and the findings from inferential statistics revealed that cybercrimes negatively impact all sectors of society in a significant manner. Inarguably, as a universal profession that is often considered the language of business, the accounting practice, systems and domain cannot be an exception. Affirmatively, Ghamri (2017) exploratively investigated the positive and negative effects of electronic banking on bank customers and entrepreneurs in the Western Region of Saudi Arabia and reported a negative effect. Three hundred (300) Saudi bank customers and entrepreneurs were randomly sampled for primary data through a questionnaire. SPSS (Version 22) test and analysis revealed that electronic transactions are susceptible to the risk of internal and external hacking.

Unarguably, it can be inferred from the forgoing empirical submissions that, the susceptibility of electronic transaction platforms to cybercrime can equally impair the security and reliability of the details of transactions. Incontrovertibly, the susceptibility of electronic transactions to cyber-attacks and manipulations in the business world has a negative (multiplier) interpretation and implication for electronic accounting, because accounting is generally referred to as the language of business. This was the finding and submission of Mupila et al. (2023) who conducted an empirical study on cybercrimes and cybersecurity awareness. The study employed correlation and regression analysis techniques to test secondary data with SPSS. The findings from inferential statistics revealed a significant correlation between cybercrime rates and low cybersecurity awareness levels. This implies that the adoption and recognition of AI-related electronic transactions and accounting in accounting practice and domain have a high cybersecurity implication. It further implies that AI-related electronic transactions and accounting are capable of compromising the reliability of financial data and are, therefore, not technological innovations firms can carelessly venture into. This is supported by a similar study by Otozi, et al. (2024). The study adopted a mixed method to investigate the prevalence and negative impacts of cybercrime in developing countries. The study conducted interviews and administered questionnaires to a sample of 68 University students in the Southern part of Nigeria, and the findings from SPSS analysis revealed that cybercrime in Nigeria is on the increase and adversely affects the business world and the economy of the country. This again, has an interpretation for as well as interrogates the reliability of financial data recognized and used in the accounting and financial system and statements of firms.

METHODOLOGY

The study adopted an explorative survey design to obtain primary data from an unknown population of professional members of the Institute of Chartered Accountants of Nigeria (ICAN) and Association of National Accountants of Nigeria (ANAN) in the South-south geo-political zone of Nigeria, with a 5-point Likert structured questionnaire. The sample size (492) was ascertained with the Cochran Sample Size Determinant Formula, under the assumption that the research instrument (questionnaire) would be administered to one-quarter of the unknown population at a desired level of confidence of 96%. The research questionnaire was vetted by a Fellow Chartered Accountant in the Bayelsa State Treasury and an Associate Professor in the accounting department of Federal University, Otuoke for content validity. Twenty-five copies of the research instrument were administered as a pilot survey on accounting lecturers in higher institutions in Bayelsa and Delta States of Nigeria for reliability, and the Cronbach Alpha Internal Consistency Test result was 0.799, which is above the benchmark of 0.700.

The study measured one dependent variable (data security and reliability) and two independent variables (artificial intelligence-driven transactions and artificial intelligence-based accounting), as expressed and stated in the following model:

$DAS = f(AIT + AIA)$ …………..……………………….………..………1

$DAS = \beta_0 + \beta_1\ AIT_1 + \beta_2\ AIA_{2\ +}\ \mu_i$ …………………………...………….. 2

Where:

$\beta_{0\ =}$ the constant that defines where the linear trend line intercepts the Y axis;

$\beta_{1,}\ \beta_1$ = the coefficients that represent the rate of change in the dependent variable;

DAS = Data security, as a proxy for data loss, theft and manipulations, and data reliability;

AIT = artificial intelligence-driven transactions;

AIA = artificial intelligence-based accounting;

μ_i = Error term.

DATA ANALYSIS AND FINDINGS

Data Presentation

The demographic details of respondents and their responses are presented as follows:

Table 1: Details of professional accountants and copies of questionnaire administered

1	**Professional Bodies**	ICAN	ANAN
2	**Gender:**		
	Male	83	220
	Female	26	52
	Number of Respondents	**109**	**272**
3	**Membership Status/Nomenclature:**		
	Associate	98	228
	Fellow	11	44
	Number of Respondents	**109**	**272**
4	**Number of Years as Member**		
	1 – 10 Years	80	113
	10 Years and Above	29	59
	Number of Respondents	**109**	**272**
5	**Branch/Chapter:**		
	Akwa-Ibom State	5	9
	Bayelsa State	31	107
	Cross Rivers State	5	9
	Delta State	23	71
	Edo State	15	21
	Rivers State	30	55
	Number of Respondents	**109**	**272**
6	**Total Number of Respondents**	**381**	

Source: *Field Report from Research Instrument (2024)*

Table 1 displays the professional membership, gender, nomenclature, professional experience and branch of respondents. Remarkably, a total of 492 copies of the questionnaire were administered through the chapter presidents of the two accountancy professional bodies in Nigeria by hand mail, but only 381 copies were successfully retrieved. This, however, represents 77% of the total copies of the questionnaire administered were retrieved, which is adequate and acceptable.

Table 2: Respondents' Opinions to Questionnaire Items and the Related Codes

Research Variables and Questionnaire Items		Opinion	SA	A	NO	D	SD
		Code	5	4	3	2	1
	Data security and reliability in AI-driven transactions and accounting						
1	AI-driven transactions are not absolutely under the control of the initiators and beneficiaries.	Outcome	109	178	0	78	16
		%	29	47	0	20	4
2	AI-driven transactions always require the services of an expert third party.	Outcome	118	213	0	13	37
		%	31	56	0	3	10
3	AI-driven transaction platforms are an open online faceless market for all	Outcome	134	136	0	42	69
		%	35	36	0	11	18
4	AI-based accounting requires the services of a third-party web service provider.	Outcome	164	179	0	38	0
		%	43	47	0	10	0
5	Firms do not enjoy absolute custody of financial records in AI-based accounting.	Outcome	52	155	39	106	29
		%	14	41	10	28	7
6	AI accounting software and systems can be electronically manipulated by unauthorized persons.	Outcome	107	244	19	11	0
		%	28	64	5	3	0
	Relationship between AI-driven transactions and cybercrime						
7	E-transactions are highly prone to cyber-attacks and manipulations.	Outcome	306	53	0	22	0
		%	80	14	0	6	0
8	There is a high breach of information in electronic transactions	Outcome	304	60	0	17	0
		%	80	16	0	4	0

Article DOI: 10.52589/AJAFR-SB1GX3VI
DOI URL: https://doi.org/10.52589/AJAFR-SB1GX3VI

9	The use of e-transactions requires adequate AI knowledge and safety measures.	Outcome	308	59	0	14	0
		%	81	15	0	4	0
	Relationship between AI-based accounting and cybercrime						
10	Most e-accounting systems are susceptible to cybercrimes and fraud	Outcome	138	232	0	11	0
		%	36	61	0	3	0
11	E-accounting requires good and adequate trust management and web security measures.	Outcome	118	258	0	5	0
		%	31	68	0	1	0
12	Data confidentiality and reliability are major challenges associated with e-accounting	Outcome	125	248	0	8	0
		%	33	65	0	2	0

Source: *Author's Computation from Research Instrument (2024)*

The 5 Likert-scale qualitative primary data obtained from professional accountants were numerically coded and converted to quantitative data, for SPSS analysis to obtain descriptive and inferential statistics and other indices to test the two hypotheses of the study at 0.05 (5%) level of significance.

Data Analysis and Hypothesis Testing

The hypotheses of the study were tested with SPSS test results at a predetermined significant level of 0.05 (5%), and the decision was to reject H_0 if P-value is less than 0.05 (that is, reject H_0: if P value < 0.05), and accept H_0 if P-value is greater than 0.05 (that is, accept $H_{0,}$ if P value > 0.05).

Hypothesis I: This was tested with SPSS test analysis in Tables 3, 4 and 5:

Table 3: Analysis of Variance for AI-driven Transactions and Data Loss, Theft and Manipulations

	Sum of Squares	df.	Mean Square	F	Sig.
Regression	30.710	2	36.355	3.355	.006
Residual	4308.503	419	10.283		
Total	4339.213	421			

Source: Author's Computation from SPSS (2024)

a. Dependent Variable: DAS.

b. Predicator: (Constant) AIT

The F statistics which measure the ratio between the means of the predictor and response variables in Table 3 is 3.355. This is statistically greater than required and suggests a rejection of the first null hypothesis because a general rule of thumb in ANOVA requires the rejection of the null hypothesis if F is greater than 1.0, and F=3.355 > 1.0. This infers that, "artificial intelligence-driven (electronic) transactions significantly increase data loss, theft and manipulations in accounting practice".

Table 4: AI-driven Transactions as a Predictor of Data Loss, Theft and Manipulations

R	R^2	Adjusted R^2	Std. Error of Est.	R^2 Change	F Change	df 1	df 2	Sig. F Change
.420	.176	.002	3.207	.170	.527	1	419	.468

Source: *Author's Computation from SPSS (2024)*
a. Predictor: (Constant) AIT

The R^2 in Table 4 is 0.176 (18%). This implies that the adoption and recognition of AI-driven (electronic) transactions in accounting practice accounts for and or occasions 18 percent variance in data security, (resulting in data loss, theft and manipulations).

Table 5: Coefficients for AI-driven Transaction as a predictor of Data Loss, Theft and Manipulation

	B	Std. Error	β	t	Sig.	VIF
(Constant) **AIT**	16.626 .501	2.509 .139	 .180	6.626 5.078	.000 .004	 1.020

Source: *Author's Computation from SPSS (2024)*
a Dependent Variable: DAS
B = Unstandardized Coefficients, β = Standardized Coefficients

Significantly, the beta coefficient (β) in Table 5 (0.180) shows that the adoption and recognition of AI-driven (electronic) transactions in accounting practice is positively related to data loss, theft and manipulations. It implies that a unit increase in the adoption and recognition of AI-driven (electronic) transactions in accounting practice results in an increase in data loss, theft and manipulation, by less than one unit (0.18). This again, suggests a rejection of the null hypothesis in favour of the alternate. Affirmatively, the probability (p) value (0.04) in Table 5 is less than the chosen alpha value of 0.05 (P = 0.04 < 0.05), and requires the rejection of the null hypothesis for the alternative, which emphatically implies that "the adoption and recognition of AI-driven (electronic) transactions significantly increase data loss, theft and manipulations in accounting practice".

Hypothesis II: This was tested with SPSS test analysis in Tables 6, 7 and 8:

Table 6: Analysis of Variance for AI-based Accounting and Financial Data Reliability

	Sum of Squares	df.	Mean Square	F	Sig.
Regression	36.005	3	12.002	1.166	.322
Residual	4303.208	418	10.295		
Total	4339.213	421			

Source: *Author's Computation from SPSS (2024)*
a. Dependent Variable: DAS.
b. Predicator: (Constant) AIA

The F statistics which measure the ratio between the means of the predictor and response variables in Table 6 is 1.166. This is statistically greater than required and suggests a rejection of the second null hypothesis because a general rule of thumb in ANOVA requires the rejection of the null hypothesis if F is greater than 1.0, and F=1.166 > 1.0. This implies that "artificial intelligence-based (electronic) accounting significantly threatens the reliability of financial data.

Table 7: AI-based Accounting as a Predictor of Reliability of Financial Data

R	R^2	Adjusted R^2	Std. Error of Est.	R^2 Change	F Change	df 1	df 2	Sig. F Change
.091	.008	.001	3.209	.168	.514	1	418	.474

Source: *Author's Computation from SPSS (2024)*
a. Predictor: (Constant) AIA

The R^2 in Table 7 is 0.008 (0.8%). This implies that the adoption of AI-based (electronic) accounting occasions 0.8 percent variance in data security.

Article DOI: 10.52589/AJAFR-SB1GX3VI
DOI URL: https://doi.org/10.52589/AJAFR-SB1GX3VI

Table 8: Coefficients for AI-based Accounting as a predictor of Financial Data Reliability

	B	Std. Error	β	t	Sig.	VIF
(Constant)	14.382	2.872		5.007	.000	
AIT	.526	.185	.189	4.297	.000	1.053

a Dependent Variable: DAS
B = Unstandardized Coefficients, β = Standardized Coefficients
Source: *Author's Computation from SPSS (2024)*

Interestingly, the beta coefficient (β) in Table 8 (0.189) shows that the adoption of AI-based (electronic) accounting is positively related to financial data reliability. It infers that a unit increase in the adoption of AI-based (electronic) accounting increasingly threatens the reliability of financial data, by less than one unit (0.19). This again implies a rejection of the null hypothesis in favour of the alternate. More so, the probability (p) value (0.00) in Table 8 is less than the chosen alpha value of 0.05 (P = 0.00 < 0.05), and necessitates the rejection of the null hypothesis for the alternative, which insistently infers that "the adoption of AI-based (electronic) accounting significantly threatens the reliability of financial data".

DISCUSSION OF FINDINGS

The findings of this study require the acceptance of the two null hypotheses, which imply that the adoption and recognition of AI-driven (electronic) transactions and accounting significantly increase data loss, theft and manipulations, as well as threaten the reliability of financial data. This is tangent with the conceptual concerns raised in the Nigerian Deposit Insurance Commission Report (2018) that says the Nigerian banking industry lost N15.15 billion to cyber-crime and forgeries in 2018. It also affirms the conceptual observation and submission of Adesoji (2019) that Nigerian banks were badly hit by cyber fraud stars and lost about N15 billion in 2018. The findings of this study further support the conceptual observation and claim of Akintaro (2023) which says that Nigerian Fintech firms suffered over N5 billion financial loss to hackers in 2023. This is sickening and seriously threatens the security and reliability of financial data used in accounting practice, and is subtly interrogating and eroding the amplified benefits and widely celebrated advantages of AI-related transactions and accounting in the accounting profession and domain.

The findings of this study further uphold the empirical finding of Haque et al. (2009) which says that only protected transactions have a significant impact on consumers' perception of electronic transaction security. They also validate the empirical result of Mshana (2015), which claims that cybercrimes negatively impact all sectors of society in a significant manner in Tanzania. The findings of this study are also in agreement with the empirical conclusion of Ghamri (2017) that electronic transactions are susceptible to the risk of internal and external hacking. The implication is that AI-driven transaction platforms are open online faceless markets for all and are, therefore, not absolutely under the control of the initiators and the proposed (original) beneficiaries. This further implies that firms do not enjoy absolute custody of financial records in AI-related transactions and accounting, and confirms the empirical submission of Mupila et al. (2023) that there is a significant correlation between cybercrime rates and low cybersecurity awareness levels. Finally, the findings of this study complement the empirical results of Otozi et al. (2024), which indicated an upsurge in cybercrime that adversely affects the firms and the economy of Nigeria, suggesting that, the adoption and recognition of AI-related electronic transactions and accounting require good and adequate trust management and web security measures for data confidentiality and reliability.

CONCLUSION AND RECOMMENDATION

This study concludes from the descriptive and inferential analytical outcomes and the findings that, financial data from AI-driven electronic transactions are significantly susceptible to loss, theft and manipulation, and that the adoption and recognition of AI-based electronic accounting impairs the security and reliability of financial data. Consequently, this study recommends that firms should be watchful and employ adequate trust management and web security measures and mechanisms in adopting and recognizing AI-related electronic transactions and accounting. This study further recommends that AI technology inventors and engineers should shift focus towards a redefinition, re-engineering and reshaping of AI technologies and platforms that can be easily governed and safely benefit users.

REFERENCES

Agnew, H. (2016). Auditing: Pitch battle. *Financial Times*. Retrieved on February 22, 2023, from https://www.ft.com/content/268637f6-15c8-11e6-9d98-00386a18e39d

Adesoji, B. S. (2019). Banks lost N15 billion to fraud, and cyber-crime in 2018. *Business News.* Retrieved on July 1,6 202,4 from https://nairametrics.com/2019/08/02/banks-lost-n15billion-to- fraud-cyber-crime-in-2018/

Akintaro, S. (2023). Nigerian Fintechs suffered over N5B losses to hackers. *Tech News,* November 2, 2023.

Bairagi, A.K. (2011). The utilisation of e-commerce can change the auction culture of Bangladesh especially in public sector. *IJCIT*, 2(1), 55-61.

Bellman, R. (1978). *Artificial Intelligence: Can Computers Think?* Boyd & Fraser Publishing Company

Bielski, L. (2001). E-commerce gets real. *American Bankers Association Banking Journal,* 93(10) 60-63.

Bossler, A. M. & Berenblum, T. (2019). Introduction: New direction in cybercrime research. *Journal of Crime and Justice*, 42(5), 495-499.

Broadhurst, R., & Chang, L. (2012). Cybercrime in Asia: Trends and challenges. *Asian Handbook of Criminology*. Retrieved on January 30, 2024, from http://dx.doi.org/10.2130/ssrn.2118322

Fitriati, A. & Mulyani, S. (2015). Factors that affect accounting information system success and its implication on accounting information quality. *Asian Journal of Information Technology*, 14(5), 154-161.

Ghamri, N. S. (2017). Positive and negative effects of using electronic banking on customers and small entrepreneurs: An exploratory study in Western Region of Saudi Arabia. *Business and Economic Research*, 7(2),311-331 doi:10.5296/ber.v7i2.11999

Goode, L. (2018). Everything is connected, and there's no going back. *The Verge*. Retrieved on July 8, 2023, from https://www.theverge.com/2018/1/17/16898728/ces-2018-tech-trade- shows-gadgets-iot

Haque, A., Tarofder, A. K., & Rahman, S. (2009). Electronic transaction of Internet banking and its perception of Malaysian online customers. *African Journal of Business Management*, 3(6), 248-259.

Haugeland, J. (1985). *Artificial Intelligence: The Very Idea*. Cambridge: MIT Press.

Hicks, J. (2004). E-commerce and its impact on the accounting profession: A literature review. *UNC Greensboro Journal of Student Research in Accounting*, 1, 1-16.

Horn, J. Rosenband, L. & Smith, M. (2010). *Conceptualizing the Industrial Revolution. Cambridge MA, London: MIT Press.*

Horn, P. (2003). Taxation of e-commerce. *Journal of American Academy of Business*, 2(2), 329-338.

Hunton, J. (2002). Blending information and communication technology with accounting research. *Accounting Horizons*, 16, 55. Retrieved on March 12, 2020 from http://dx.doi.org/10.2308/acch. 2002.16.1.55.

Jain, N., & Shrivastava,V. (2014). Cybercrime changing everything-an empirical study. *International Journal of Computer Application*, 4(1), 76-87

Joseph, A. (2006). Cybercrime definition. *Computer Crime Research Centre*. Retrieved on July 16, 2020 from http://www.crime-research.org/articles/joseph06.

Khan, A.G. (2016).Electronic commerce: A study on benefits and challenges in an emerging economy. *Global Journal of Management and Business Research,* 16 (1), 19-22.

Lambert, L. (2017). The four challenges of the Fourth Industrial Revolution. *Market Mogul*. Retrieved on July 8, 2020, from https://themarketmogul.com/industry-4-0-challenges /?hvid=2Gt2CE

Lau, L. Y. C. & Chang, L. Y. C. (2018). Responding to cybercrime: Current trends. *Police Practice and Research*, 19(6), 515-518)

Michael, C. (2024). Social engineering, website hacking lead channels Nigerian bank customers lost money in 2023, *Business Day*, June 18, 2024.

Mshana, J. A. (2015). Cybercrime: An empirical study of its impact in the society-A case study of Tanzania https://www.ajol.Ifo>article

Mupila, F. K., Gupta, H., & Bhardwaj, A. (2023). An empirical study on cybercrimes and cybersecurity awareness. Retrieved February 22, 2024, from https://doi.org/10.21203/rs.3.rs-3037289/v1

O'Donnell, L. (2019). Threat List: Nigerian cybercrime surged 54 percent in 2018. *Threat Post.* Retrieved on July 17, 2020, from https://threatpost.com/threatlist-nigerian-cybercrime-surged-54-percent-in-2018/144561/

Oladipupo,M & Ajabe K. (2013). Computer-based accounting systems in small and medium enterprises: Empirical evidence from a randomized trial in Nigeria. *Universal Journal of Management*, 1(1) 13-21.

Omodunbi, B., Odiase, P.O., Olaniyan, O. & Esan, A. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention.

Otozi, U. J., Bernard, E., & Idris, A. (2024). Cybercrime and its negative effects in developing countries. *Journal of Mobile Computing and Application*, 11(4), 10-16. DOI:109790/0050- 11041016

Peters, M. A. (2017). Technological Unemployment: Educating for the Fourth Industrial Revolution. *Journal of Self-Governance and Management Economics,* 5(1), 25-33.

Article DOI: 10.52589/AJAFR-SB1GX3VI
DOI URL: https://doi.org/10.52589/AJAFR-SB1GX3VI

Prisecaru, P. (2016). Challenges of the Fourth Industrial Revolution. *Knowledge Horizons Economics*, 8(1), 57-62.

Rich, E., & Knight, K. (1991). *Artificial Intelligence.* McGraw-Hill, New York

Russell, S., & Norvig, P. (2009). *Artificial Intelligence: A Modern Approach, 3rd ed.* Upper Saddle River, NJ: Prentice Hall

Rogoff, K. (2012). The impact of technology on employment. A Paper Presented at the World Economic Forum. Retrieved on January 16, 2023 from https://www. weforum.org//agenda /2012/10/king-ludd-is-still-dead.

Romney, M. B. & Steinhart, P. J. (2018). Accounting Information Systems (14th ed.). New York: Pearson.

Russell, S. (2019). How to stop superhuman AI before it stops us? *New York Times,* https://www.nytimes.com/2019/10/08/opinion/artificial-intelligence.html

Scalar Decisions Incorporation. (2018). Cyber Security Readiness of Canadian Organisations. Retrieved on March 13, 2023, from http://www.scalar.ca/en/landing/2018-scalarsecurity -study.

Security Support (2020). Cybercrime in Nigeria: Causes and effects. Retrieved on July 16, 2024, from https://www.proshareng.com/news/Security---Support/Cybercrime-in-Nigeria--Causes-and-Effect/49035

Shull, A. (2018). Governing cyberspace during a crisis in trust. https://www.cigionline.org/articles/governing-cyberspace-during-crisis-trust?gclid=EAlal QobChMlmup8x5PN6gIVF_IRCh1wAQqFEAAYASAAEgL1pvD_BwE

Tade, O. (2019). Nigeria: EFCC and cybercriminals in Southwest Nigeria. *The Vanguard.* Retrieved on July 16, 2024, from https://allafrica.com/stories/201912190571.html

Tegmark, M. (2017). Benefits and risks of artificial intelligence-coming techs. *The Future of Life Institute.* Retrieved on May 8, 2023, from comingtechs.com/benefit-risks-artificial-intelligence.

The Nigerian Deposit Insurance Commission Report (2018). The Nigerian banking industry lost N15.15 billion to cyber-crime and forgeries in 2018. Retrieved on July 18, 2020, from https://ndic.gov.ng//wp-cotent/uploads/2019/07/ndic-2018-annual-report-executive-

Ulgado, F.M. (2002). Country-of-origin effects on e-commerce. *Journal of American Academy of Business*, 2(1), 250-253.

Xu, M., David, J. M. & Kim, S. H. (2018). The fourth industrial revolution: Opportunities and challenges. *International Journal of Financial Research*, 9 (2), 90-95.

Yampolskiy, R.V. (2013). Artificial intelligence safety engineering: Why machine ethics is a wrong approach. *Philosophy and Theory of Artificial Intelligence*, 5, 389-396.

Yampolskiy, R.V. & Fox, J. (2016). Safety engineering for artificial general intelligence. *Springer*, 1-11. Retrieved on April 27, 2023, from https://wwwresearchgate .net/ publication/256169424

Article DOI: 10.52589/AJAFR-SB1GX3VI
DOI URL: https://doi.org/10.52589/AJAFR-SB1GX3VI