Ethics, Governance and Security in Technology Adoption in Nigeria

Benson Edet Ekpenyong, PhD[1]; Victor Edet Ebiefie, PhD[2]; Aniema Paul Udofia[3]

[1&3]Department of Economics, Federal College of Education, Ididep Ibiono Ibom L.G.A, Akwa Ibom State, Nigeria.

[2]Department of Economics, Edo State University, Iyamho, Edo State, Nigeria.

[1] benson.ekpenyong@fceididep.edu.ng, +234 8023033122

[2] ebiefie.victor@edouniversity.edu.ng, +234 8034122357, +234 8082096503

[3] aniemaudofia2018@gmail.com,+234 8142679488

DOI: https://doi.org/10.67487/ijfmg.v2i3.346

Citation: Ebiefie, V. E., Ekpenyong, B. E., & Udofia, A. P. (2026). Ethics, Governance and Security in Technology Adoption in Nigeria. *International Journal of Finance, Management and Governance, 2(3).* https://doi.org/10.67487/ijfmg.v2i3.346

Abstract

This study examines the relationship between ethics, governance, security, and technology adoption in Nigeria using annual time-series data covering the period 1995–2025. Specifically, the study investigates the relationship between ethical practices, security challenges and technology adoption in Nigeria. The Autoregressive Distributed Lag (ARDL) model is employed to estimate the short-run and long-run relationships among the variables. The empirical findings reveal that government effectiveness, cybersecurity, and infrastructural development have positive and statistically significant relationships with technology adoption in Nigeria, suggesting that effective public administration, enhanced digital security, and improved technological infrastructure are important drivers of technology adoption. Conversely, digital literacy and awareness, as well as institutional accountability, exhibit negative relationships with technology adoption, indicating potential challenges associated with the effectiveness of digital skills development, public awareness initiatives, and accountability mechanisms within the technology adoption process. These unexpected negative relationships may reflect implementation gaps, institutional inefficiencies, unequal access to digital resources, or possible mismatches between existing policies and practical outcomes. The findings emphasize the necessity of strengthening governance structures, investing in secure and reliable digital infrastructure, and ensuring that digital

literacy programs and accountability mechanisms translate into measurable improvements in technology adoption. The study concludes that sustainable and ethical technology adoption in Nigeria requires an integrated approach that combines effective governance, robust cybersecurity, infrastructural development, inclusive digital capacity building, and transparent institutional practices. It recommends that policymakers align digital transformation policies with measurable performance indicators, strengthen ethical and regulatory frameworks, and improve the implementation and monitoring of digital literacy and accountability initiatives.

Keywords: technology adoption, ethics, governance, cybersecurity, government effectiveness

1.1 Introduction

The adoption of digital technologies has become a significant driver of economic growth, institutional transformation, and social development across the world. Technologies such as artificial intelligence (AI), digital financial services, cloud computing, biometric identification, e-government platforms, and the Internet of Things (IoT) are increasingly transforming how governments, businesses, and individuals operate. In Nigeria, technology adoption has expanded considerably, particularly in telecommunications, financial services, education, healthcare, and public administration. This development aligns with the government's ambition to build a digitally driven economy through policies such as the National Digital Economy Policy and Strategy (NDEPS) 2020–2030. However, the increasing dependence on digital technologies has raised critical concerns regarding ethical responsibility, institutional governance, data privacy, cybersecurity, accountability, and equitable access. Consequently, the central challenge is no longer simply whether Nigeria can adopt new technologies but whether such adoption can be achieved responsibly, securely, and within an effective governance framework (Alakitan & Makinde, 2025).

The trajectory of technology adoption in Nigeria reflects a gradual transition from telecommunications liberalization and mobile connectivity to digital financial inclusion, electronic government services, digital identity management, and emerging AI applications. The expansion of mobile communications and internet-enabled services has created opportunities for entrepreneurship, financial transactions, service delivery, and citizen engagement. Nevertheless, the benefits of this transformation coexist with structural vulnerabilities, including uneven digital access, cybercrime, inadequate digital literacy, data breaches, online fraud, and the potential misuse of personal information. The Internet Society (2025) reports that approximately 41% of Nigeria's population used the internet in 2024,

illustrating both the progress achieved and the continuing challenge of extending meaningful digital access to the wider population. Furthermore, the growing deployment of AI and data-intensive technologies introduces additional concerns relating to algorithmic bias, surveillance, misinformation, transparency, and the protection of fundamental rights. These developments demonstrate that technological progress must be accompanied by institutional capacity and safeguards that protect individuals and organizations from emerging risks.

A significant trend in Nigeria's digital transformation is the gradual development of a formal governance and regulatory framework. The enactment of the Nigeria Data Protection Act 2023 and the establishment of the Nigeria Data Protection Commission (NDPC) represent important steps towards protecting personal information and strengthening accountability in data processing (Nigeria Data Protection Commission [NDPC], 2023). Similarly, national digital economy initiatives demonstrate the government's recognition of technology as an instrument for economic diversification and improved public service delivery. Despite these developments, the existence of policies and regulations does not automatically guarantee effective implementation, compliance, or public trust. Alakitan and Makinde (2025) observe that Nigerian digital technology policies have placed comparatively limited emphasis on comprehensive ethical guidelines for the design, deployment, and use of emerging technologies. This raises questions about the adequacy of regulatory enforcement, institutional coordination, transparency, and accountability in an increasingly data-driven society.

The central problem, therefore, is the potential disconnect between the rapid adoption of digital technologies and the development of effective ethical, governance, and security mechanisms to manage their consequences in Nigeria. Although technological innovation can improve productivity, inclusion, and service delivery, weak implementation of safeguards may expose users to privacy violations, cyberattacks, discriminatory automated decisions, digital fraud, and the unauthorized exploitation of personal data. This problem is particularly significant where government institutions and private organizations collect and process sensitive information without adequate transparency, robust security controls, or clearly defined accountability mechanisms. The nexus between ethics, governance, and security is therefore fundamental: ethics establishes the principles of fairness, privacy, and responsible technology use; governance provides the institutional rules, oversight, and enforcement mechanisms; while security protects digital systems, information, and users against threats and unauthorized access. Weakness in any one of these dimensions can undermine the effectiveness and legitimacy of technology adoption.

Several stylized facts characterize this relationship in Nigeria. First, digital technology adoption is expanding across economic and public institutions, creating new opportunities for innovation and service delivery. Second, internet access remains uneven, indicating that technological benefits are not equally distributed. Third, Nigeria has established a statutory data

protection framework, but effective implementation and compliance remain essential to its success. Fourth, increasing reliance on digital platforms expands the potential exposure of individuals and organizations to cybersecurity threats and unethical data practices. Fifth, the rapid development of AI and other emerging technologies creates regulatory challenges that may exceed existing institutional capacities (Alakitan & Makinde, 2025; Internet Society, 2025; NDPC, 2023). Taken together, these facts suggest that technology adoption is not merely a technical or economic process but also an institutional and societal issue.

Against this background, this study examines the relationship between ethics, governance, and security in technology adoption in Nigeria. It seeks to establish how ethical standards, regulatory institutions, and security arrangements influence the responsible adoption and effective use of digital technologies.

Objective of the Study

The main objective of this study is to investigate the impacts of ethics, governance and security in technology adoption in Nigeria. The specific objective is:

i. To determine the relationship between ethical practices, security challenges and technology adoption in Nigeria.

Research Question

To analyze the above objective, the study will attempt to answer the question:

i. What relationship exists between ethical practices, security challenges and technology adoption in Nigeria?

Research Hypothesis

To answer the question stated above, the study will test the hypothesis state in null form below:

i. There is no statistically significant relationship between ethical practices, security challenges and technology adoption in Nigeria.

2. Literature Review

2.1 Theoretical Literature

This study is anchored on three major theories: Institutional Theory, Deontological Ethical Theory, and Protection Motivation Theory. These theories provide a foundation for examining the influence of ethics, governance, and security on technology adoption in Nigeria. The theories explain how institutional policies and regulations, ethical responsibilities, and security concerns may influence the adoption and use of technology by individuals and organizations.

2.1.1 Institutional Theory

Institutional Theory has its roots in the work of Philip Selznick (1948, 1949). Its modern formulation in organizational sociology is associated with John W. Meyer and Brian Rowan (1977), while DiMaggio and Powell (1983) further developed the theory. Institutional Theory explains how organizations are influenced by the rules, regulations, norms, values, and expectations of the environments in which they operate. The theory suggests that organizations do not make decisions based solely on efficiency and profitability; they also respond to institutional pressures to gain legitimacy, maintain public confidence, and comply with established standards.

Meyer and Rowan (1977) argued that organizations often adopt formal structures and practices to demonstrate conformity with socially accepted institutional expectations. Similarly, DiMaggio and Powell (1983) identified three forms of institutional pressure: coercive, normative, and mimetic pressures. Coercive pressure arises from laws, regulations, and the influence of powerful institutions. Normative pressure results from professional standards, education, and accepted practices, while mimetic pressure occurs when organizations imitate other organizations, particularly under conditions of uncertainty.

In technology adoption, organizations may introduce digital systems because of government policies, regulatory requirements, professional standards, or competitive pressures. In Nigeria, organizations adopting digital technologies must consider applicable laws, data-protection requirements, cybersecurity obligations, and relevant government policies. Institutional theory is based on the following assumptions: Organizations operate within institutional environments that influence their decisions and activities; laws, regulations, social expectations, and professional standards shape organizational behavior. Organizations adopt certain practices to gain legitimacy and maintain public confidence. Institutional pressures can influence the adoption and implementation of new technologies. Organizations facing similar institutional pressures may adopt similar policies and practices, and the adoption of formal policies does not necessarily guarantee their effective implementation.

Despite its usefulness, Institutional Theory has some limitations. First, it may place excessive emphasis on institutional pressures while paying insufficient attention to individual decision-making and organizational innovation. Second, it does not always adequately explain why organizations operating under similar regulations respond differently to technological change. Third, organizations may adopt formal policies to demonstrate compliance without implementing them effectively. Finally, the theory does not independently explain the technical effectiveness of cybersecurity measures or the ethical implications of technological decisions.

Institutional Theory is relevant to this study because governance is one of the major dimensions of ethics, governance, and security in technology adoption in Nigeria. The adoption of technology is influenced by government policies, regulatory frameworks, institutional

accountability, and enforcement mechanisms. For example, organizations that collect and process personal information must consider applicable data-protection requirements and establish appropriate procedures for managing users' information. Similarly, government institutions and private organizations need effective policies to guide the responsible implementation of digital technologies. The theory helps explain how institutional arrangements can encourage or discourage adoption of technology. It also provides a basis for examining whether governance structures promote transparency, accountability, regulatory compliance, and public trust.

The implication of Institutional Theory for this study is that effective technology adoption requires appropriate governance structures, clear regulatory policies, and effective enforcement mechanisms. The study can examine how institutional policies, regulatory compliance, and accountability influence technology adoption in Nigeria. The theory also suggests that the existence of laws and policies is insufficient unless institutions have the capacity to enforce them. Therefore, the study should consider both the availability of governance frameworks and the extent to which organizations implement them. In the Nigerian context, strengthening institutional capacity, improving regulatory enforcement, and promoting accountability may contribute to more responsible and sustainable technology adoption.

2.1.2 Deontological Ethical Theory

Deontological Ethical Theory is strongly associated with the German philosopher Immanuel Kant, whose influential work, Groundwork of the Metaphysics of Morals, was published in 1785. Deontological Ethical Theory is an ethical approach that evaluates actions according to duties, obligations, and moral principles rather than judging them solely by their consequences. According to Kant's ethical perspective, individuals should be treated as ends in themselves and never merely as instruments for achieving another person's objectives. The theory emphasizes that certain actions are morally required or prohibited regardless of whether they produce immediate benefits. It stresses the importance of respecting human dignity, acting according to moral principles, and fulfilling ethical obligations.

In technology adoption, Deontological Ethical Theory suggests that organizations have a responsibility to respect users' privacy, protect personal information, obtain appropriate consent, and avoid discriminatory or deceptive practices. For instance, an organization adopting an artificial intelligence system should consider whether the system respects human dignity, treats users fairly, and protects their personal information. Similarly, a digital service provider should not misuse customers' data merely because doing so may increase profits or improve operational efficiency.

Deontological Ethical Theory is based on the following assumptions: Moral duties and obligations are central to determining whether an action is ethical, human beings possess dignity

and should be treated with respect, ethical principles should be applied consistently rather than changed solely to achieve personal or organizational benefits, certain actions may be morally wrong even when they produce favorable consequences, individuals and organizations have ethical responsibilities that should guide their decisions and conduct and respect for rights, fairness, honesty, and responsible conduct is essential to ethical decision-making.

One major criticism of Deontological Ethical Theory is that it may be difficult to determine which moral duty should take priority when ethical obligations conflict. For example, protecting an individual's privacy may conflict with the need to disclose information to prevent serious harm. Another criticism is that the theory may not adequately account for the consequences of actions. Strict adherence to a moral rule may sometimes produce undesirable outcomes. Furthermore, abstract ethical principles can be difficult to apply to complex technological situations involving artificial intelligence, digital surveillance, and automated decision-making.

The theory also provides limited practical guidance for assessing technical cybersecurity risks. Consequently, it may need to be complemented by other theories and practical frameworks when examining technology adoption. Deontological Ethical Theory is relevant to this study because ethical responsibility is a central consideration in technology adoption in Nigeria. The increasing use of digital platforms, electronic payment systems, artificial intelligence, and online services raises important questions about privacy, informed consent, transparency, fairness, and accountability.

The theory provides a moral foundation for examining whether individuals and organizations fulfil their ethical obligations when adopting and using technology. For example, organizations that collect personal information should consider whether their practices respect users' rights and comply with applicable ethical and legal requirements. Similarly, institutions using automated decision-making systems should consider whether those systems treat people fairly and avoid unjust discrimination. The theory therefore helps the researcher assess whether technology adoption is guided not only by efficiency and profitability but also by respect for human dignity and ethical responsibility.

The implication of Deontological Ethical Theory is that technology adoption should be guided by clear ethical principles and obligations. Organizations should establish policies that promote privacy protection, transparency, fairness, informed consent, and accountability. The study can examine whether ethical practices influence public trust and willingness to adopt technology in Nigeria. It can also investigate whether concerns about the misuse of personal information, discriminatory practices, or inadequate transparency discourage technology adoption.

Furthermore, the theory suggests that organizations should develop ethical guidelines for technology development and implementation. These guidelines should establish clear

responsibilities for collecting, processing, storing, and protecting users' information. The application of this theory may help identify ways to promote ethical and responsible technology adoption in Nigeria.

2.1.3 Protection Motivation Theory

Protection Motivation Theory was developed by Ronald W. Rogers in 1975 and subsequently revised by Rogers in 1983. Protection Motivation Theory explains how individuals respond to threats and decide whether to adopt protective behaviors. The theory proposes that people evaluate the seriousness of a threat, their vulnerability to it, and the effectiveness of available protective measures before deciding how to respond. The theory consists of two major processes: threat appraisal and coping appraisal.

Threat appraisal involves evaluating the seriousness of a threat and the likelihood of being affected by it. It includes perceived severity, which refers to how serious an individual considers the consequences of a threat, and perceived vulnerability, which refers to the individual's belief about the likelihood of experiencing the threat. Coping appraisal involves evaluating the effectiveness of a protective response, one's ability to carry it out, and the costs associated with taking that action. It includes response efficacy, self-efficacy, and response costs. In technology adoption, individuals may be reluctant to use digital platforms if they believe those platforms expose them to serious cybersecurity threats. However, they may be more willing to adopt such technologies when they believe effective security measures are available.

For example, Nigerian consumers may be more confident in using digital banking applications when service providers implement multifactor authentication, transaction alerts, fraud-detection systems, and effective procedures for reporting unauthorized transactions. Protection Motivation Theory is based on the following assumptions: Individuals evaluate potential threats before deciding how to respond, Perceived severity influences how seriously individuals consider a threat, Perceived vulnerability influences individuals' assessment of their likelihood of experiencing harm, Individuals consider whether protective measures are effective in reducing threats, Confidence in one's ability to take protective action influences security-related behavior, The financial, practical, or personal costs of protective measures may discourage their adoption and Perceptions of threats and available protective measures can influence decisions about technology use.

Protection Motivation Theory has some limitations. First, it focuses primarily on protective behavior and may not fully explain technology adoption motivated by convenience, economic benefits, or social influence. Second, individuals do not always assess security threats rationally. Their decisions may be influenced by misinformation, previous experiences, emotions, or limited knowledge of cybersecurity. Third, perceived security may differ from

actual security. Users may trust a vulnerable system or avoid a well-protected system because they misunderstand the risks. Fourth, the theory does not directly explain the influence of governance frameworks, institutional accountability, or ethical obligations. Finally, individuals may have limited control over security measures when technologies are provided by employers, financial institutions, or government agencies.

Protection Motivation Theory is relevant to the security component of this study because cybersecurity concerns may influence the willingness of individuals and organizations to adopt technology in Nigeria. The growing use of digital banking, electronic commerce, online education, electronic government services, and other digital platforms creates concerns about cybercrime, phishing, identity theft, data breaches, and unauthorized access to information. Individuals who perceive these threats as serious may avoid certain digital services. Conversely, users who believe that adequate security measures are available may be more willing to adopt and continue using technology. The theory therefore provides a basis for examining how perceived security risks, confidence in protective measures, and cybersecurity awareness relate to technology adoption.

The implication of Protection Motivation Theory is that technology providers and policymakers should implement effective security measures and improve public awareness of cybersecurity threats. The study can investigate how security concerns influence technology adoption and whether confidence in protective measures is associated with greater willingness to use digital services in Nigeria. The theory also suggests that organizations should provide clear security information, strengthen authentication procedures, establish effective incident-reporting systems, and educate users about safe technology practices. Furthermore, the study should distinguish between perceived security and actual security because users' perceptions do not always reflect the technical strength of a system.

In Nigeria, improving cybersecurity awareness, strengthening technical safeguards, and ensuring appropriate institutional responses to security incidents may help create a more secure environment for technology adoption.

2.2 Empirical Review

The adoption of digital technologies has increased across several sectors in Nigeria, including banking, healthcare, education, electronic commerce, and public administration. Although these technologies offer opportunities for improved efficiency, service delivery, and economic development, their adoption also raises concerns relating to ethical practices, governance, data privacy, cybersecurity, and public trust. Recent studies have examined these issues from different perspectives. Some have focused on government policies and ethical guidelines, while others have investigated data-protection compliance, cybersecurity threats, privacy concerns, and the factors influencing users' willingness to adopt digital technologies. The following

empirical review examines relevant studies and identifies their methodologies, findings, and recommendations.

Alakitan and Makinde (2025) examined where the ethical guidelines are. The study specifically examines the governance of digital technologies and AI in Nigeria and investigates the extent to which Nigerian government policies incorporate ethical considerations into digital technology and artificial intelligence governance. The authors reviewed policy documents associated with the administrations of Muhammadu Buhari and Bola Tinubu. Their findings indicated that, although both administrations introduced initiatives to promote digital transformation, insufficient attention was given to ethical guidelines governing data protection, privacy, and the responsible use of digital technologies. The study concluded that ethical considerations should be integrated into technology policies to address emerging security and accountability challenges. However, its focus on policy documents leaves room for further empirical investigation into how ethical governance influences actual technology adoption. The study is particularly relevant to the present research because it directly examines the relationship between ethics, governance, and digital technology in Nigeria.

AbdulKareem and Oladimeji (2024) investigated the role of trust and digital literacy in citizens' adoption of electronic government services in Nigeria. Grounded in the Technology Acceptance Model, the researchers surveyed 876 citizens who had used electronic filing services and analyzed the data using partial least squares structural equation modelling. The study examined how trust and digital literacy relate to the perceived usefulness and perceived ease of use of e-government services. Their research provides evidence of the importance of citizens' confidence and digital capabilities in the adoption of government technology. Nevertheless, its focus on electronic filing services leaves questions about the applicability of the findings to other digital platforms. The study is relevant to the present research because it demonstrates why effective governance, digital competence, and public trust should be considered when examining technology adoption.

Chukwu et al. (2022) conducted a literature-based study examining how data protection and privacy influence the adoption of electronic government services in Nigeria. The researchers reviewed existing literature to develop a structured discussion of the relationship between privacy concerns, data protection, and citizens' willingness to use digital government services. The study highlighted the importance of protecting citizens' personal information in the adoption of electronic government services. Concerns about data scandals, unauthorized disclosure of personal information, and the misuse of customer or employee records can weaken citizens' confidence in digital platforms. The researchers' analysis indicates that privacy and data protection should be considered important elements of electronic government adoption. Citizens may be reluctant to use government digital services if they believe that their personal information will not be adequately protected. The study supports strengthening data-protection

measures and ensuring that government institutions communicate clearly about how personal information is collected, processed, stored, and protected. It also suggests that policymakers and public institutions should address privacy concerns as part of their efforts to increase the use of electronic government services.

Paul and Victor (2023) examined the factors affecting the adoption of public electronic services in Nigeria through a narrative review of existing literature. The authors identified individual, social, and infrastructural barriers, including age, income, trust, language, limited broadband access, and the cost of digital infrastructure. They recommended digital literacy programs, capacity building, and the development of online content in Nigerian languages to improve adoption. Their findings demonstrate that technology adoption depends not only on the availability of digital services but also on users' socioeconomic circumstances, digital competence, and confidence. Nevertheless, the study concentrated primarily on digital inequality rather than the combined effects of ethics, governance, and cybersecurity. The present study can build on their findings by examining how ethical safeguards and effective governance influence public confidence in technology adoption.

Akinola and Ashaolu (2023) investigated security, privacy, and trust concerns associated with electronic commerce in Nigeria. The study used a survey-based approach to investigate security-related concerns and proposed a model integrating security, trust, and privacy to support electronic commerce. The study identified security, privacy, and trust as important concerns affecting electronic commerce in Nigeria. Although online shopping provides consumers with convenient ways to purchase goods and services, concerns about the safety of online transactions and the protection of personal information remain challenges. The researchers argued that addressing technical security vulnerabilities alone may not be sufficient to establish confidence in electronic commerce. Users also need assurance that their personal information will be handled responsibly and that online transactions can be conducted with an acceptable level of security. The study recommended an integrated approach to electronic commerce security that goes beyond technical safeguards. Online businesses should consider privacy protection, access control, transaction security, and measures that strengthen users' trust in digital platforms. The proposed model also highlights the importance of incorporating users' concerns into the design and management of electronic commerce systems.

Oke and Sibomana (2025) conducted a scoping review to examine the development and adoption of digital health technologies in Nigeria. The researchers followed the Arksey and O'Malley scoping review methodology and the PRISMA-ScR reporting guidelines. They searched databases including PubMed/MEDLINE, Google Scholar, the Directory of Open Access Journals, and African Journals Online. The search initially identified 1,840 studies and other sources. Following screening, 230 studies were included in the review. The researchers extracted information from the selected literature and used descriptive statistics to examine

publication trends, research methods, and the different categories of digital health technology investigated in Nigeria. The study found that research on digital health technology in Nigeria had expanded substantially between 2010 and 2024. The technologies examined included mobile health, electronic health services, telemedicine, health information systems, digital health devices, and other technological applications. Cross-sectional studies constituted the largest category of included research, accounting for 36.5%, followed by literature reviews at 27.8% and qualitative studies at 13.0%. The researchers recommended greater collaboration among government institutions, private sector organizations, and other stakeholders to finance digital health research and implementation. They also emphasized the need to train health technology professionals and strengthen the capacity of healthcare institutions to integrate digital solutions effectively.

Ale Felix et al. (2025) employed a quantitative survey approach to investigate adherence to data-protection and privacy policies in Nigeria. The researchers collected data from 590 participants comprising information technology professionals and decision-makers from different organizations. A structured questionnaire was administered through Google Forms, with questions covering data-protection and privacy practices. The questionnaire used three-point and five-point Likert scales. Data collection took place over five months, and the responses were analyzed using statistical methods. The study found that some organizations in Nigeria took data protection seriously, but many organizations did not have formal data-protection policies in place. The findings also indicated that respondents perceived adherence to data-protection and privacy requirements as generally low, despite the existence of a regulatory framework. This suggests a difference between the existence of data-protection regulations and their practical implementation within organizations. The researchers recommended stronger enforcement of data-protection regulations, increased public awareness, and training programs for organizations and their employees. They also emphasized the importance of institutional measures to improve the protection of sensitive information across public and private sector organizations.

Umoh et al. (2026) examined Artificial Intelligence (AI) as a Catalyst for Business and Social Development in Nigeria, the study specifically examined the potential of artificial intelligence to promote business productivity, employment generation, financial inclusion, and socioeconomic development in Nigeria. The study employed the Autoregressive Distributed Lag (ARDL) econometric technique using time-series data obtained from the Central Bank of Nigeria Statistical Bulletin and the World Development Indicators covering the period 2000–2024. The findings revealed that financial technology, employment opportunities, and business productivity had positive and statistically significant relationships in the short and long run. However, the effects of AI adoption were not immediately positive, suggesting that businesses require adequate time, infrastructure, skills, and financial resources to integrate AI effectively

into their operations. The authors concluded that AI could contribute significantly to Nigeria's economic and social development if supported by appropriate infrastructure, digital skills acquisition, entrepreneurship, and effective governance.

Femi et al. (2025) adopted a mixed-methods research design to evaluate compliance with the Nigeria Data Protection Regulation across six sectors: finance, telecommunications, education, healthcare, small and medium-sized enterprises, and the public sector. The study collected data from 615 respondents in 30 organizations using questionnaires, interviews, and document analysis. The researchers assessed compliance against relevant data-protection benchmarks, including lawful processing, consent procedures, and responses to data breaches. They also used regression analysis to investigate relationships between compliance-related factors and cybersecurity outcomes. The study found differences in data-protection compliance across the sectors examined. Financial and telecommunications organizations demonstrated relatively high compliance, which the researchers associated with regulatory pressure and stronger technical capacity. In contrast, small and medium-sized enterprises and public institutions demonstrated lower levels of adherence. The findings also indicated that data-protection compliance, staff training, and cybersecurity investment were significant predictors of improved cybersecurity outcomes. The researchers further identified weak enforcement and limited penalties as factors undermining the deterrent effect of the regulatory framework. The study therefore suggests that effective data governance requires both organizational capacity and credible enforcement mechanisms. The researchers recommended stronger regulatory oversight, reforms to address legal and structural weaknesses, and interventions tailored to the needs of different sectors.

Auwal (2025) employed a conceptual and thematic approach based on multidisciplinary literature, policy documents, regulatory frameworks, and secondary sources. Rather than conducting primary fieldwork, the author examined the ethical, institutional, and human factors that may compromise the security of Internet of Things (IoT) infrastructure in Nigeria. The analysis considered sectors such as healthcare, finance, energy, and governance, focusing on insider threats, institutional accountability, procurement practices, and digital ethics. The study argued that IoT security challenges in Nigeria cannot be explained solely by external cyberattacks or technical weaknesses. Instead, the author emphasized the significance of insider negligence, weak accountability, institutional corruption, poor regulatory enforcement, and limited cybersecurity awareness. The study suggested that technical safeguards may be undermined when employees, contractors, or public officials fail to observe security procedures or when institutional practices compromise the integrity of digital systems. The analysis also highlighted the relationship between ethical conduct, institutional accountability, and the protection of digital infrastructure. The study recommended stronger institutional accountability, regular security audits, compulsory digital ethics education, and more effective

enforcement against individuals and organizations responsible for compromising digital systems.

Dauda et al (2025) adopted a cross-sectional quantitative research design to investigate the relationship between cybersecurity concerns, trust, and mobile banking adoption among fintech customers in Nigeria. The researchers collected data using structured questionnaires administered to 498 active mobile banking users selected through multistage sampling across urban and semi-urban locations. The instrument was assessed by expert review, and its reported reliability coefficient was 0.81 using Cronbach's alpha. The researchers analyzed the data using regression-based mediation techniques and bootstrapping procedures. The study found that perceptions of fraud, financial loss, and system reliability significantly reduced mobile banking adoption through their effects on trust. However, privacy concerns did not show a statistically significant indirect influence through trust in the model examined. The researchers identified trust as an important mechanism linking cybersecurity perceptions with users' willingness to adopt mobile banking services. The findings suggest that technical capabilities alone may not be sufficient to sustain adoption when users lack confidence in the reliability and security of digital financial services. The researchers recommended integrated cybersecurity governance frameworks that emphasize real-time fraud monitoring, transparent data management, and continuous user education. They also emphasized the need to strengthen consumer trust as part of efforts to support sustained mobile banking adoption.

3. Methodology

3.1 Research Design

The design adopted in this study is an ex post facto (after the fact) design. Hence, this study used secondary sources information and therefore time series data sourced from various publications of Central Bank of Nigeria Statistical Bulletin and world development indicators (WDI). The models for this study were estimated using data on ethical practice, governance framework and security in technology adoption indicators, which include: digital literacy measure by internet users as percentage of population (DIGLIT), institutional accountability measured by institutional accountability (INSTACC), cybersecurity measure with secure internet server per million people (CYSEC), government effectiveness (GOVEFF) and security in technology adoption (TECHAD) as a dependent variable for the period 1995-2025.A multiple regression analysis was used, predicated on various data diagnostics including Augmented Dickey-Fuller (ADF) and Philip-Peron (PP) unit root tests, bound testing method for co integration and the autoregressive distributed lag technique (ARDL.) was employed in this study to determine the relationship between ethical practices and technology adoption in Nigeria and to investigate the security challenges affecting technology adoption in Nigeria.

3.2 Model Specification

The model for this study is anchored on the institutional theory which has its roots in the work of Philip Selznick (1948, 1949). Its modern formulation in organizational sociology is associated with John W. Meyer and Brian Rowan (1977), while DiMaggio and Powell (1983) further developed the theory. The theory explains how organizations are influenced by the rules, regulations, norms, values, and expectations of the environments in which they operate and therefore implied that effective technology adoption requires appropriate governance structures, clear regulatory policies, and effective enforcement mechanisms. Hence, the model is as specified below:

3.2.1 Ethical practices, governance framework and security challenges affecting technology adoption equation:

SETECH= F (ETHP, GOVF) Equation 3.1

Equation 3.1 states that security in technology adoption is dependent upon ethical practices and governance framework variables. In demystifying the above model, the security in technology and ethical practices, governance framework will be capture by the following variables listed below. It follows that Equation 3.1 will be the formula presented by Equation 3.2 as follows:

TECHAD = F (GOVEFF, CYSEC, DIGLIT, INSTACC) Equation 3.2

The functional form of the model for ethical practices, governance framework and security challenges affecting technology adoption equation is highlighted below:

The econometric form of the model is given as:

$$TECHAD_t = \beta_0 + \beta_1 GOVEFF_t + \beta_2 CYSEC_t + \beta_3 DIGLIT_t + \beta_4 INSTACC_t + U_t$$

Equation 3.3

Where:

$TECHAD_t$ = Security in technology proxied by technology adoption effectiveness in time t

$GOVEFF_t$= Governance framework measured by Governance Effectiveness in time t

$CYSEC_t$ = Cybersecurity proxied by secure internet server per million people in Nigeria in time t

$DIGLIT_t$ = Digital Literacy/ Awareness proxied by internet users as percentage of population in time t

$INSTACC_t$ = Institutional accountability in time t

U_t– Error term

A priori Expectation shows that β_1(-), β_2 (-), β_3 (+), and β_4 (-).

4. Results and Discussion of Findings

4.1 Descriptive statistics and matrix of correlations

Table 4.1: Descriptive Statistics

	TECHAD	GOVEFF	CYSEC	DIGLIT	INSTACC	INFRAST
Mean	4.42	-1.03	15.16	31.10	-1.32	84.17
Median	3.82	-1.04	11.50	22.00	-1.32	84.05
Maximum	9.49	-0.10	40.06	90.00	-0.10	88.68
Minimum	2.46	-1.38	0.01	0.01	-2.79	80.64
Std. Dev.	1.82	0.20	14.46	30.51	0.37	2.36
Skewness	1.39	2.99	0.44	0.68	-0.88	0.27
Kurtosis	4.23	15.59	1.76	2.07	12.91	1.75
Jarque-Bera	11.95	251.37	2.99	3.49	130.97	2.39
Probability	0.00	0.00	0.22	0.17	0.00	0.30
Sum	137.04	-31.93	469.88	964.11	-40.98	260.91
Sum Sq. Dev.	99.66	1.24	627.05	279.19	4.07	167.02
Observations	**31**	**31**	**31**	**31**	**31**	**31**

Source: Researcher's computation (2026), using E-Views 9.

Table 4.1 presents the descriptive statistics of the variables used in the study from 1995 to 2025. The results show that technology adoption (TECHAD) recorded an average value of 4.42 about 3.82%, maximum and standard deviation of 9.49%, 1.82%, indicating low technology adoption due to lack of awareness, poor infrastructure provision, while government effectiveness (GOVEFF) had debilitating low mean value of -1.03% and maximum of -0.10%, suggesting that government is ineffective in its infrastructure provision, awareness creation or education provision on and human capital development in Nigeria. Cybersecurity (CYSEC) records an average of 15.16% and a maximum and standard deviation of 40.06% and 14.14% respectively indicating a moderate level of cybersecurity provision and therefore reflecting relatively moderate improvements in cybersecurity contribute to increased technology adoption within the studied period. Meanwhile, digital literacy/awareness (DIGLIT) exhibited considerable high variation, as reflected by the mean value of 31.10% and maximum of 90.00% as well as high standard deviation of 30.51%, indicating increase in digital literacy/awareness is associated with a significant increase in technology adoption within the study period. Also, institutional accountability (INSTACC) exhibited a low averaged of -1.32% and maximum of -0.10%, implying substantial low institutional accountability. On the contrary, infrastructural

development (INFRAST) exhibited an extremely high level as evidence by the average mean of 84.17% and maximum value of 88.68% with standard deviation of 2.36%, implying that the availability of infrastructure may translate into greater technology adoption within the period under review. The skewness result shows that only GOVEFF is positive skewed showing a peak distribution. The result of the kurtosis shows that only TECHAD, GOVEFF and INSTACC is leptokurtic (kurtosis > 3), indicating peaked distributions. The Jarque-Bera probabilities indicate that CYSEC, DIGLIT and INFRAST are normally distributed, whereas TECHAD, GOVEFF, and INSTACC deviate from normality due to variability and macroeconomic instability with the standard deviation of 1.86, 0.20 and 0.37 respectively.

Table 4.2: Correlation Matrix

	TECHAD	GOVEFF	CYSEC	DIGLIT	INSTACC	INFRAST
TECHAD	1					
GOVEFF	0.15	1				
CYSEC	-0.19	-0.03	1			
DIGLIT	-0.03	-0.28	0.54	1		
INSTACC	-0.15	-0.07	0.41	0.37	1	
INFRAST	0.17	0.02	-0.22	0.05	-0.01	1

Source: Researcher's computation (2026), using E-Views 9.

The correlation matrix of the variables is as shown in Table 4.2 above. From the table therefore, TECHAD has a positive correlation coefficient with GOVEFF and INFRAST. This therefore indicates that the variables tend to move in the same direction. Meanwhile CYSEC, DIGLIT and INSTACC has a weak negative correlation (-0.19, -0.03 and -0.15) indicating that as TECHAD increases CYSEC, DIGLIT and INSTACC tends to decrease. Also, from the table, there exist positive correlation coefficient between GOVEFF and INFRAST; CYSEC and DIGLIT, INSTACC; as well as DIGLIT and INSTACC, INFRAST respectively. Also, GOVEFF exhibit negative relationship with CYSEC, DIGLIT and INSTACC, while CYSEC exhibit negative relationship with INFRAST as well as INSTACC and INFRAST respectively.

4.1.2 Unit Root Test

The Augmented Dickey Fuller and the Philip-Perron unit root tests were conducted to examine the stationarity condition of the variables. As indicated in Table 4.3 below, DIGLIT and GOVEFF were stationary at level in ADF, and PP, while TECHAD, INSTACC, INFRAST, DIGLIT and CYSEC were stationary after first differencing in both ADF and PP. In other words, the variables are integrated of order zero and one (i.e., I (0) and I(I)). Where some of the variables are I (0) while others are I (1) one suggests the problem of unit root-= in the equations.

It becomes imperative to perform co-integration tests to determine the presence of equilibrium relationship amongst the variables in each equation. The study adopts the ARDL bound testing technique for co-integration, as the variables are integrated of diverse orders (i.e., order zero and order one).

Table 4.3: ADF and Philip-Perron Unit Root Test Results

Variables	ADF Level	1st Difference	Order of integration	Level	PP 1st Difference	Order integration
TECHAD	-2.991109	-4.685435	I(1)	-	-	I(1)
GOVEFF	-9.078432	-	I(0)	-	-	I(0)
CYSEC	1.628638	-4.176768	I(1)	-	-	I(1)
DIGLIT	-	-	I(0)	3.258634	-	I(0)
INSTACC	-2.008058	-6.126417	I(1)	-	-	I(1)
INFRAST	-1.852662	-6.017970	I(1)	-	-	I(1)

Source: Researcher's computation (2026), using E-Views 9.

Note: Mackinnon critical values for ADF at 1, 5 and 10% levels are -3.60, -2.93 and -2.60 respectively, and for PP are 3.605, 2.936 and 2.606, respectively. ** means significant at 5% level.

4.1.3 Lag Length Selection

Table 4.4: lag length criteria

Lag	LogL	LR	FPE	AIC	SC	HQ
0	-266.5347	NA	11.46942	19.46676	19.75224	19.55404
1	-138.5631	191.9574	0.017164	12.89736	14.89567*	13.50826
2	-108.4916	32.21943	0.038979	13.32083	17.03197	14.45536
3	-19.52011	57.19595*	0.003295*	9.537151*	14.96113	11.19531*

Source: Researcher's computation (2026), using E-Views 9.

The efficiency and validity of an error correction model depends on the lag structure. The study used VAR lag order selection criteria to determine the lag lengths. The study employed the Akaike Information Criterion (AIC) and Schwarz Criterion (SC) and the result shows three optimal lag lengths for the model of ethics, governance and security in technology adoption in Nigeria as shown in Table 5 above. In order to reduce the possibilities of underestimation whilst

maximizing the likelihood of recovering the true lag (Venus, 2004), the study used three and four as the maximum lag lengths, respectively.

4.1.4 Co-integration Test Results

From the bound testing result reported in Table 4.5 below, long run relationship exists amongst the variables in all the estimated equations, given that the values of the F-statistic are greater than the critical values at five per cent level in both the upper and the lower bounds. Therefore, the null hypothesis of absence of co-integration is rejected, while the study proceeds to estimate the long run coefficient of each of the equations.

Table 4.5: Co-Integration Test Results

5% critical value					
Equation	K	F-Stat	I (0)	I (1)	
Outcome					
TECHAD (GOVEFF, CYSEC, DIGLIT, INFRAST, INSTACC)	5	3.88	2.62	3.79	co integrated

Note: K =number of parameters

Source: Researcher's computation (2026), using E-Views 9.

4.2 Findings, Presentation and Analysis of Econometric Results of the Long run coefficients of the impact of ethics, governance on security in technology adoption in Nigeria Equation Results.

Table 4.6: Dependent variable: TECHAD

Variable	Coefficient	Std. Error	t-Statistic	Prob.
GOVEFF	0.275590	0.117887	2.337757	0.0395
CYSEC	0.015795	0.006403	2.466716	0.0463
DIGLIT	-0.011918	0.004298	-2.772836	0.0496
INFRAST	0.074222	0.041334	1.795677	0.0894
INSTACC	-1.646576	0.430764	-3.822452	0.0012
C	-6.500952	3.642390	-1.784804	0.0912

Source: Researcher's computation (2026), using E-Views 9.

The long-run relationship to determine the impact of ethics, governance on security in technology adoption in Nigeria equation variables is presented in Table 4.6 above. Based on the ARDL long-run estimates, the findings reveal the following insights:

The coefficient for government effectiveness (GOVEFF) is positive and statistically significant, indicating that a unit increase in GOVEFF results in 27.55% increases in technology adoption (TECHAD). This finding is in line with a priori expectation, indicating that that improvements in the quality of public institutions, policy implementation, regulatory enforcement, and public service delivery contribute significantly to increased technology adoption. This suggests that an effective government creates an enabling environment for technological development by formulating and implementing supportive policies, providing essential infrastructure, strengthening institutional capacity, and promoting investment in digital technologies. In the context of ethics, governance, and security, government effectiveness can enhance public trust in digital systems by ensuring transparency, accountability, the protection of users' rights, and the enforcement of cybersecurity and data protection regulations.

Conversely, the coefficient of cybersecurity (CYSEC) is positive and statistically significant, indicating that a unit rise in CYSEC results in 1.57% increases in TECHAD. This result is not in line with a priori expectation, suggesting that improvements in cybersecurity contribute significantly to increased technology adoption. This suggests that a secure digital environment encourages individuals, businesses, and public institutions to adopt and utilize technological innovations by reducing the risks associated with cyber threats, data breaches, identity theft, online fraud, and unauthorized access to sensitive information. In the context of ethics, governance, and security, effective cybersecurity mechanisms enhance users' confidence and trust in digital platforms by ensuring the confidentiality, integrity, and availability of information. Furthermore, stronger cybersecurity frameworks, effective data protection policies, and the enforcement of relevant digital security regulations can reduce uncertainties surrounding technology use and encourage greater participation in digital economic activities. In the Nigerian context, sustained improvements in cybersecurity can promote the adoption of digital banking, electronic commerce, e-government services, and other technology-driven innovations, thereby supporting productivity, financial inclusion, and economic development.

Conversely, digital literacy and awareness (DIGLIT) exhibits a negative and statistically significant relationship with TECHAD. Therefore, a one-unit increase in DIGLIT is associated with – 1.19% decreases in TECHAD. This result is in line with a priori expectations, showing that an increase in digital literacy/awareness is associated with a significant reduction in technology adoption, contrary to the conventional expectation that greater digital knowledge should promote technological uptake. This unexpected relationship may suggest that increased awareness of digital risks, including cybercrime, online fraud, data breaches, privacy violations,

and the unethical use of personal information, makes individuals and businesses more cautious about adopting digital technologies. In the context of ethics, governance, and security, greater digital awareness may enable users to recognize the potential dangers associated with technology use, thereby increasing their reluctance to adopt digital platforms when adequate safeguards, institutional trust, and regulatory protections are lacking. Furthermore, the negative relationship may reflect the possibility that digital literacy alone is insufficient to encourage technology adoption in Nigeria, particularly where users face inadequate digital infrastructure, high internet costs, unreliable electricity supply, limited access to digital devices, and concerns about online security.

More so, the coefficient of infrastructural development (INFRAST) is positive and insignificantly related to TECHAD. Specifically, a unit rise in INFRAST will lead to 7.42% increases in TECHAD. This result is in line with a priori expectation, implying that the availability of infrastructure may not necessarily translate into greater technology adoption without complementary measures such as effective governance, adequate cybersecurity, data protection, digital literacy, and public trust in digital platforms. The finding therefore suggests that although infrastructural development has the potential to support technology adoption, its long-run contribution may depend on the effectiveness of institutional frameworks and the availability of complementary technological and socioeconomic conditions.

Finally, the coefficient for institutional accountability (INSTACC) is negative and statistically significant, indicating that a one-unit increase in INSTACC will lead to a -16.46% decreases in technology adoption (TECHAD). This finding is in line with a priori expectation, indicating that increased accountability requirements, when accompanied by excessive bureaucratic procedures, regulatory complexities, administrative delays, or rigid compliance requirements, could constrain the adoption and implementation of new technologies. Within the context of ethics, governance, and security, institutions may impose stricter oversight mechanisms, reporting obligations, and compliance standards to ensure transparency, protect users' privacy, and minimize cybersecurity risks. Although these measures are intended to promote responsible technology use, their implementation may increase the financial and administrative costs of adopting digital technologies, particularly for small businesses and institutions with limited resources. Furthermore, the negative relationship may suggest that accountability mechanisms are not yet sufficiently coordinated with technology adoption policies, potentially creating institutional barriers that discourage technological innovation.

In summary, the long-run analysis highlights the complex interplay between the ethical practices, security challenges and technology adoption in Nigeria. While government effectiveness (GOVEFF), Cyber security (CYSEC) and infrastructural development (INFRAST) positively influenced technology adoption (TECHAD) in Nigeria, others such as digital literacy/awareness (DIGLIT) and institutional accountability (INSTACC) posed

significant challenge. These findings underscore the need for Nigerian government to adopt an integrated strategy that promotes digital competence, strengthens institutional transparency, simplifies regulatory procedures, and builds public confidence in technology by redesigning digital literacy and awareness programs to focus not only on the technical use of digital technologies but also on cybersecurity, data privacy, ethical technology use, and the benefits of digital innovation.

4.2.1 Findings, Presentation and Analysis of Econometric Results of the short run coefficients of the impact of ethics, governance on security in technology adoption in Nigeria Equation Results.

Table 4.7: Dependent variable: TECHAD

Variable	Coefficient	Std. Error	t-Statistic	Prob.
D(GOVEFF)	0.248548	0.735998	0.337702	0.7395
D(CYSEC)	0.014245	0.031700	0.449375	0.6585
D(DIGLIT)	-0.010748	0.014774	-0.727536	0.4763
D(INFRAST)	0.066939	0.043797	1.528411	0.1438
D(INSTACC)	-0.447233	0.206334	-2.167523	0.0438
D(INSTACC(-1))	0.310596	0.276301	1.124123	0.2757
D(INSTACC(-2))	0.761368	0.254932	2.986548	0.0079
CointEq(-1)	-0.901875	0.217637	-4.143941	0.0006

R-squared	0.684343	Mean dependent var	1.431786
Adjusted R-squared	0.526514	S.D. dependent var	0.375066
S.E. of regression	0.258084	Akaike info criterion	0.401390
Sum squared resid	1.198932	Schwarz criterion	0.877177
Log likelihood	4.380543	Hannan-Quinn criter.	0.546843
F-statistic	4.335988	Durbin-Watson stat	2.428778
Prob(F-statistic)	0.003942		

Source: Researcher's computation (2026), using E-Views 9.

The short-run dynamics to determine the impact of ethics, governance and security in technology adoption in Nigeria Equation Results is as presented in Table 4.7, which reveal several significant findings.

The coefficient for government effectiveness (GOVEFF) is positive and insignificant in the short run, indicating that a unit increase in GOVEFF will results in 24.85% increases in TECHAD. This result is in line with a priori expectation, indicating that government effectiveness alone may be insufficient to generate an immediate and measurable increase in

technology adoption. Although effective governance may provide the institutional foundation for technological advancement, its influence may depend on the extent to which government policies are implemented consistently, public resources are managed transparently, ethical standards are upheld, and adequate cybersecurity and data protection measures are established. Furthermore, the insignificant result suggests that improvements in government effectiveness do not necessarily guarantee greater technology adoption in the short run, particularly where institutional improvements are not accompanied by adequate technological infrastructure and public confidence in digital systems.

Also, the coefficient of cybersecurity (CYSEC) is positive and insignificantly related to TECHAD in the short run, therefore, a unit rise in CYSEC will results in 1.42% increases in TECHAD in the short run. This result is in line with a priori expectation, suggesting that in the short run, cybersecurity alone may not be sufficient to generate an immediate and measurable increase in technology adoption. Although stronger cybersecurity measures can help reduce the perceived risks of using digital platforms, their effectiveness may depend on complementary institutional and ethical factors, including transparency, accountability, responsible data management, compliance with data protection regulations, and the enforcement of appropriate security standards. In addition, persistent concerns about online fraud, identity theft, data breaches, and the misuse of personal information may continue to discourage some individuals and businesses from adopting digital technologies, even when cybersecurity measures are improving.

More so, digital literacy/awareness (DIGLIT) exhibits a negative and insignificant relationship with TECHAD in the short run. Therefore, a one-unit increase in DIGLIT is associated with -1.07% decreases in TECHAD in the short run. This result is not in line with a priori expectations, implying that raising digital literacy and awareness may not be sufficient, on its own, to generate an immediate and statistically significant increase in technology adoption. Digital literacy initiatives may be more effective when complemented by ethical digital practices, transparent governance, effective cybersecurity measures, stronger data protection, and public education on how to use digital platforms safely. These measures can help ensure that increased awareness translates into greater confidence, willingness, and capacity to adopt digital technologies.

The coefficient of infrastructural development (INFRAST) is positive and insignificantly related to TECHAD in the short run, therefore, a unit rise in INFRAST will lead to 6.69% increases in TECHAD. This result is in line with a priori expectation, suggesting that infrastructure development alone may be insufficient to stimulate technology adoption in the short run. The effectiveness of infrastructure in promoting technology adoption may depend on the broader institutional environment, including ethical practices, effective governance, transparency, accountability, and adequate cybersecurity measures. For instance, even where

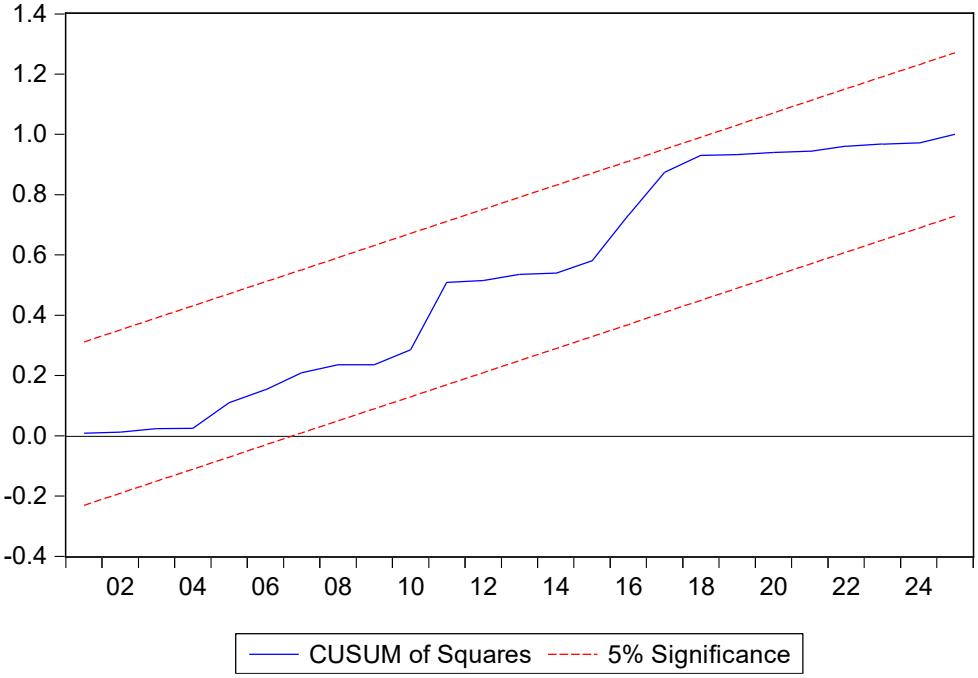
digital infrastructure is available, weak institutional trust, concerns about data privacy, cybercrime, and inadequate regulatory enforcement may discourage individuals and businesses from adopting digital technologies. Similarly, governance challenges that affect infrastructure provision, maintenance, and equitable distribution may limit its immediate contribution to technology adoption.

Finally, the coefficient for institutional accountability (INSTACC) is negative and significant in current period, positive but insignificant in first period, positive and significant in second period lag, indicating that a one-unit increase in INSTACC will lead to -44.72% decreases in TECHAD in current period, 31.05% and 76.13% increases in TECHAD in first and second period lags of the short run. The result of the current period is in line with a priori expectation, while the result of the first and second period lags do not conform to theoretical expectations, indicating that the findings highlight the importance of institutional accountability as a governance mechanism that may influence the adoption of digital technologies over time. Ethical conduct, transparent decision-making, effective oversight, and accountability in the management of digital systems can help build trust in technology-enabled services. Furthermore, accountable institutions may be better positioned to enforce cybersecurity regulations, protect users' data, address complaints, and ensure that digital platforms operate within established legal and ethical frameworks. These conditions can encourage greater acceptance and utilization of technology among individuals, businesses, and public institutions.

The ECM coefficient (-0.901875) is correctly signed and statistically significant, indicating that approximately 90.18% of short-run disequilibria adjust to the long-run equilibrium within a year. The t-statistic (-4.143941) confirms the significance of the ECM at the 5% level.

The R-squared value (0.684343) and adjusted R-squared (0.526514) demonstrate that approximately 68% of the variation in TECHAD is explained by the included variables (both current and lagged), with 32% attributable to factors outside the model. The F-statistic (4.33) confirms the joint significance of the model's variables, ensuring a good overall fit. Additionally, the Durbin-Watson statistic (2.42) indicates no autocorrelation, affirming the reliability of the results for forecasting and policy formulation.

The stability test using the cumulative sum (CUSUM) test in figure 4.1 below further shows that the variables included in the TECHAD equation were stable within the period of the study. This is evidenced by the swing of the trends within the CUSUM bound at the ± five percent significance level. The study, therefore, infers that the equation is stable and consistent to be adopted for economic policies and forecast.



Source: Researcher's computation (2026), using E-Views 9.

Figure 4.1: Ethics, Governance and Security in Technology Adoption in Nigeria equation CUSUM.

4.3 Discussion of Findings

The short run and the long run ARDL dynamics shows an intriguing insight as the regression result shows that three variables of ethics, governance and security in technology adoption: government effectiveness (GOVEFF), cybersecurity (CYSEC) and infrastructure development in technology (INFRAST) offers a positive and significant relationship with the dependent variable technology adoption (TECHAD). The result suggests that increases in government effectiveness, cybersecurity and infrastructural development in technology in essence will lead to corresponding increases in technology adoption in Nigeria. This finding therefore suggests that technology adoption in Nigeria is associated with the combined influence of institutional capacity, digital security, and infrastructure availability. Government effectiveness provides an institutional framework for policy implementation and public-service delivery; cybersecurity strengthens trust and confidence in digital systems; while infrastructure development provides the physical and digital facilities required for technological access and utilization. The findings are in line with the assertion of Dauda et al. (2025), Auwal (2025), Akinola & Ashaolu (2023), who opined that government effectiveness, cybersecurity, trust and infrastructure are panacea for effective technology adoption and ethical promotion.

However, digital literacy/awareness (DIGLIT) and institutional accountability (INSTACC) exhibited an expected negative relationship with technology adoption in both short and long run periods. The negative impact of digital literacy/awareness and institutional accountability suggest that these factors may not independently produce measurable improvements in ethics, governance, and security in Nigeria within the period examined. In the short run, their effects may be constrained by weak institutional capacity, inadequate digital skills, poor regulatory enforcement, and cybersecurity challenges. In the long run, these constraints may continue to limit the benefits of technological development unless appropriate reforms and complementary investments are implemented. This finding is in tandem with the propositions of Umoh et al. (2026), Alakitan and Makinde (2025), Paul and Victor (2023) who assert that ethical considerations should be integrated into technology policies to address emerging security and accountability challenges as awareness or literacy and institutional accountability will help improved technology adoption. The authors also identified individual, social, and infrastructural barriers, including age, income, trust, language, limited broadband access, and the cost of digital infrastructure.

Specifically, institutional accountability exhibited a dual impact on technology adoption as the empirical review shows a negative, positive, significant and insignificant influence in both current, first and second period lags of the short run and long run periods suggesting that institutional accountability can have either a negative or a positive and statistically significant influence on technology adoption in Nigeria, depending on the effectiveness, design, and implementation of accountability mechanisms. A negative and significant relationship may reflect excessive bureaucracy, compliance costs, and institutional constraints, while a positive and significant relationship may reflect improved transparency, public trust, regulatory compliance, and digital security, therefore, the central policy challenge is to ensure that institutional accountability promotes ethical technology use, effective governance, and security while creating an enabling environment for innovation and digital transformation in Nigeria.

The models were estimated using the error correction mechanism (ECM) and the outcome of the key urbanization and economic development equations revealed positive and significant relationship among the variables in both the short run and long run. The result of the heteroscedasticity shows absence of heteroscedasticity. Therefore, the errors are homoscedastic. Hence, the long run results succeed all tests and thus useful for analyses and forecasting.

The Error Correction coefficients in all the estimated models met the three criteria for its acceptability given that it is negative, fractional and statistically significant. Consequently, the estimated result confirms the presence of long run relationship among the variables in the models. It also shows that the speed of adjustments is moderate in all the estimated models. The value of the adjusted R-squared implies that the models have good fit as the independent variables have high explanatory powers. The Durbin-Watson Statistic connotes absence of

autocorrelation in the estimated equations. The study, therefore, accepts the null hypotheses of no serial correlation in the models. This further implies that the error terms of different periods are not serially correlated. The stability test using the cumulative sum tests showed that the variables included in all the models were stable within the period of the study.

5. Conclusion and Policy Recommendation

The study examined the impact of ethics, governance and security in technology adoption in Nigeria. Specifically, the study determines the relationship between ethical practices, security challenges and technology adoption in Nigeria using data from 1995-2025 and adopted the autoregressive distributive lag model (ARDL). The empirical findings reveal a positive and significant relationship government effectiveness (GOVEFF), cybersecurity (CYSEC) and infrastructure development in technology (INFRAST) which analyzed the relationship between ethical practices, security challenges and technology adoption with the dependent variable technology adoption (TECHAD) in Nigeria. This result therefore suggests that technology adoption in Nigeria is associated with the combined influence of institutional capacity, digital security, and infrastructure availability.

In addition, the study revealed a shocking and expected negative relationship between digital literacy/awareness (DIGLIT) and institutional accountability (INSTACC) and technology adoption in Nigeria. The finding suggests that these factors may not independently produce measurable improvements in ethics, governance, and security in Nigeria within the period examined.

5.1 Recommendations

Therefore, we recommend that Nigerian government should strengthen practical digital education, align digital transformation policies with measurable performance indicators, strengthen ethical and regulatory frameworks, and improve the implementation and monitoring of digital literacy and accountability initiatives.

References

Abdulkareem, A. K., & Oladimeji, K. A. (2024). Cultivating the digital citizen: Trust, digital literacy and e-government adoption. *Transforming Government: People, Process and Policy,* 18(2), 270 – 286.

Alakitan, M., & Makinde, E. (2025). *Where are the ethical guidelines? Examining the governance of digital technologies and AI in Nigeria. Policy & Internet,* 17(1), Article e416.

Akinola, O., & Ashaolu, O. (2023). A trust, privacy and security model for e-commerce in

Nigeria. *Nigerian Journal of Technology,* 42(1), 152 – 159.

Ale Felix, A., Abdullahi, A., Momoh, J., Ikpaya, I.D., & Juliet, I.O. (2025). Strengthening data privacy and protection in Nigeria: Recommendations for a comprehensive approach. *In proceedings of the 8th URSI-NG Annual Conference* (URSI-NG 2024) (pp.27 -38). Atlantis Press.

Auwal, A. M. (2025). Invisible intrusions, internal threats and ethical vulnerabilities in Nigeria's internet of things. *Discover Internet of Things*, 5, Article 128.

Chukwu, J., Conrad, M., & Crosbie, T. (2022). Data protection and privacy determinants of e-government adoption in Nigeria. In M. B. Nunes, P. Isaias, P. Powell, & L. Rodrigues (Eds.), *Proceedings of the 15th IADIS International Conference Information Systems* 2022, IS 2022 (pp.223 -227). IADIS Press.

Dauda, A., Musa, O. F., Hamidu, R., Adamu, F., Ibrahim, F. M., & Atoyebi, K. M. (2025). Exploring the relationship between cybersecurity concerns and mobile banking adoption among fintech customers in Nigeria. *Nigerian Journal of Rural Finance and Entrepreneurship,* 3(3), 135 – 147

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review,* 48(2), 147–160.

Femi, A. G., Adenomon, M. O., Aimufua, G. I. O., & Ibrahim, U. (2025). Evaluating the level of compliance with the Nigeria Data Protection Regulation (NDPR): Insights from organizations across key sectors. *Journal of Cyber Security,* 7(1), 377 – 394.

Internet Society. (2025). Country Report for Nigeria. https://pulse.internetsociety.org/en/reports/NG

Kant, I. (1785). Groundwork of the Metaphysics of Morals.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology,* 83(2), 340–363.

Nigeria Data Protection Commission. (2023). Nigeria Data Protection Annual Report 2023. https://ndpc.gov.ng/wp-content/uploads/2024/07/Annual Report2023.pdf.

Oke, G.I., & Sibomana, O. (2025). Adoption of digital health technology in Nigeria: A scoping review of current trends and future directions. *Advances in Public Health,* 2025, Article 4246285.

Paul, C., & Victor, E. V. (2023). Digital divide and uptake of public e-service in Nigeria: A narrative review. *Journal of Technology Innovations and Energy*, 2(4), 27 – 41.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology,* 91(1), 93–114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo and R. E. Petty (Eds.), Social Psychophysiology: A Sourcebook. Guilford Press.

Selznick, P. (1949). TVA and the Grass Roots: A Study in the Sociology of Formal Organization. University of California Press.

Venus, K.L. (2004).Which Lag Length Selection Criteria Should We Employ? Economic Bulletin, Vol. 3 No. 33 pp 1 – 9.