JAIMT
JOURNAL OF ARTIFICIAL INTELLIGENCE AND MODERN TECHNOLOGY
A Peer Reviewed (Refereed) International Journal
ISSN:1595-6261 VOLUME 7, ISSUE 1 (MAY) 2026

AI-DRIVEN CYBER THREAT DETECTION AND DIGITAL INFRASTRUCTURE PROTECTION IN NIGERIAN ORGANIZATIONS

David William [1]; Emem Godwin Young [2] & Blossom Okorie [3]

[1,2] Tetfund Centre of Excellence in Computational Intelligence Research, Akwa Ibom State Polytechnic, Ikot Osurua, Ikot Ekpene

[3] Tetfund Centre of Excellence in Computational Intelligence Research, University of Uyo, Uyo

EMAIL: onlydave_2007@yahoo.com [1], ememgodwin92@gmail.com [2], ebereokorie@uniuyo.edu.ng [3]

D.O.I.: https://doi.org/10.5281/zenodo.22082855

ARTICLE INFORMATION

Received: 30st MARCH, 2026
Accepted: 24th APRIL, 2026
Published: 29th MAY, 2026

KEYWORDS: artificial intelligence; cyber threat detection; digital infrastructure protection; cybersecurity; Nigerian organizations; cyber resilience.
JOURNAL URL: https://ijois.com/jaimt/index.php

PUBLISHER: Empirical Studies and Communication (A Research Center)
Website: www.cescd.com.ng

ABSTRACT

This study examined the relationship between artificial intelligence (AI)-driven cyber threat detection and digital infrastructure protection in Nigerian organizations, against the backdrop of a rapidly escalating threat landscape. Nigerian organizations faced an average of 4,388 cyber attacks per week in the first quarter of 2025, a 47% year-on-year increase, while the country moved sharply up the Global Threat Index (Check Point, cited in Rhizome, 2025). Adopting a cross-sectional survey design, the study drew on 384 information-technology and security personnel from banks, telecommunications firms and public-sector institutions, selected through stratified random sampling. Two objectives guided the inquiry: to determine the extent to which AI-driven threat-detection capability influences the effectiveness of cyber threat detection, and to assess the effect of AI-driven detection on digital infrastructure protection. Data were analysed using performance percentage analysis, descriptive statistics, Pearson product-moment correlation and simple linear regression at the 0.05 level of significance. Findings revealed a strong positive and statistically significant relationship between AI-driven capability and threat-detection effectiveness ($r = 0.76$, $p < 0.05$), and a significant positive effect of AI-driven detection on digital infrastructure protection ($\beta = 0.71$, $p < 0.05$, $R^2 = 0.498$). Percentage analysis showed that 82% of respondents affirmed that AI had improved the speed and accuracy of threat detection. The study concludes that AI is a decisive enabler of cyber resilience in Nigerian organizations, though skills shortages, cost and data-quality constraints limit its full realisation. It recommends sustained investment in AI security platforms, talent development, and compliance with the Cybercrime Act and the Nigeria Data Protection Act.

INTRODUCTION

The digital transformation of the Nigerian economy has been swift and far-reaching. Mobile banking penetration has exploded, e-commerce platforms are proliferating, and cloud-based business tools have become standard across sectors, while the country ranked second globally in cryptocurrency adoption for 2024, recording roughly USD 59 billion in crypto transactions between July 2023 and June 2024 (BISI, 2025). This expansion has delivered substantial economic benefit, but it has also enlarged the attack surface available to cybercriminals. Critically, the pace of digital adoption has outstripped the development of cybersecurity infrastructure, leaving many organizations particularly small and medium-sized enterprises operating without robust security frameworks and treating cybersecurity as a cost centre rather than a business imperative (OmoolaEX, 2025).

The resulting threat environment is severe and intensifying. According to Check Point Software, companies in Nigeria faced an average of 4,388 cyber attacks per week in the first quarter of 2025, a striking 47% year-on-year surge, while Nigeria's position on the Global Threat Index shifted dramatically from 35th to 13th between May and December 2024, signalling a sharp escalation in vulnerability (Rhizome, 2025). The financial toll is correspondingly large: Nigeria lost an estimated 1.1 trillion naira, approximately USD 805 million, to cybercrime across banks, telecommunications and government agencies between 2017 and 2023, with losses continuing to climb as attacks grow more sophisticated and cryptocurrencies are increasingly used for money laundering (UNODC, cited in Olurounbi, 2026).

A defining feature of the contemporary landscape is the weaponisation of artificial intelligence by attackers. Historically, Nigerian cybercrime consisted largely of simplistic "419" email solicitations that a discerning eye could identify; today, criminal actors deploy AI to dramatically amplify the scale, precision and impact of their attacks (BISI, 2025). AI-powered phishing campaigns now analyse social-media profiles and professional networks to craft highly targeted messages, malware morphs its signature to evade detection, and deepfake technology enables fraud schemes that impersonate trusted executives with alarming precision. In one 2024 incident, a Nigerian cartel used a deepfake to pose as a senior government official during a video call and convinced an international NGO to release funds for a fraudulent project (OmoolaEX, 2025).

In response, the same technology that empowers attackers is being turned to defence. As cybercriminals leverage AI to automate attacks, Nigerian businesses are increasingly compelled to adopt AI-powered cybersecurity solutions, with AI-powered defence tools becoming indispensable in the fight against increasingly complex threats (Deloitte, 2025). AI-driven cyber threat detection refers to the use of machine-learning and related techniques to learn an organization's normal operational patterns and to flag anomalies in real time, enabling a shift from reactive incident response toward proactive, predictive defence. Digital infrastructure protection, the complementary concept, concerns the safeguarding of the networks, systems, applications and data on which organizational and national digital activity depends.

The Nigerian cybersecurity market reflects this defensive turn. Valued at USD 207.80 million in 2025, it is projected to grow at a 10.70% compound annual rate to reach USD 345.43 million by 2029, with growth driven by 5G adoption, IoT proliferation and AI-powered threat-detection systems, and reinforced by regulatory mandates including the Nigeria Data Protection Act 2023 and the Cybercrime Act (AInvest, 2025). Yet investment alone does not guarantee protection. The central question this study addresses is whether, and to what extent, AI-driven threat detection genuinely improves the detection of threats and the protection of digital infrastructure in Nigerian organizations Kindness et al. (2026).

The stakes extend beyond individual organizations to the national economy. Nigeria is home to some of Africa's fastest-growing digital-finance companies, and the integrity of their infrastructure underpins investor confidence and long-term growth (Olurounbi, 2026). When fraud networks can fabricate exchanges, manipulate market sentiment through bots and deceive investors with convincing phishing messages, the damage is not merely financial but reputational, threatening the trust on which the digital economy rests (BISI, 2025). Effective, AI-enabled defence is therefore a matter of economic security as much as organizational risk management, which lends the present inquiry a significance that transcends any single firm or sector.

This study contributes to scholarship and practice in three respects. First, it provides recent, quantitative Nigerian evidence on a relationship frequently asserted in industry reports but rarely measured empirically. Second, it links a measurable AI threat-detection capability to two security outcomes detection effectiveness and infrastructure protection. Third, it derives practical recommendations for managers, security leaders and regulators seeking to strengthen cyber resilience. The remainder of the paper states the objectives, questions and hypotheses; reviews the literature and theory; describes the method; presents and discusses the findings; and closes with conclusions and recommendations.

2. Aim and Objectives of the Study

The aim of this study is to examine the relationship between AI-driven cyber threat detection and digital infrastructure protection in Nigerian organizations. The study is guided by two specific objectives:

1. To determine the extent to which AI-driven threat-detection capability influences the effectiveness of cyber threat detection in Nigerian organizations.
2. To assess the effect of AI-driven cyber threat detection on the protection of digital infrastructure in Nigerian organizations.

3. Research Questions

The study seeks to answer the following two research questions:

1. To what extent does AI-driven threat-detection capability influence the effectiveness of cyber threat detection in Nigerian organizations?
2. What is the effect of AI-driven cyber threat detection on the protection of digital infrastructure in Nigerian organizations?

4. Research Hypotheses

Two null hypotheses were formulated and tested at the 0.05 level of significance:

$H0_1$: There is no significant relationship between AI-driven threat-detection capability and the effectiveness of cyber threat detection in Nigerian organizations.

$H0_2$: AI-driven cyber threat detection has no significant effect on the protection of digital infrastructure in Nigerian organizations.

5. Literature Review

5.1 Conceptual Clarification

Artificial intelligence in cybersecurity denotes the application of machine-learning, deep-learning and related computational techniques to the detection, prevention and mitigation of cyber threats. Its defining advantage over rule-based systems is the capacity to learn normal behaviour and to identify deviations from it, allowing the detection of novel and evolving threats that signature-based tools would miss. AI-powered threat-detection systems learn an organization's normal operational patterns and flag anomalies in real time, supporting a defensive posture that is proactive rather than reactive (OmoolaEX, 2025). Digital infrastructure protection, the second core construct, refers to the measures that secure the integrity, availability and confidentiality of an organization's networks, servers, endpoints, applications and data.

AI contributes to cyber defence through several distinct capabilities. Anomaly detection identifies unusual patterns in network traffic or user behaviour; predictive threat intelligence anticipates attacks before they materialise; automated response contains incidents at machine speed; and specialised models detect phishing, malware and, increasingly, deepfakes and synthetic fraud. The relative prominence of these capabilities among Nigerian deployments is illustrated in Figure 1.

It is useful to distinguish AI-enabled defence from traditional, signature-based security. Signature-based tools match incoming activity against a database of known threat patterns; they are effective against recognised attacks but blind to novel ones. AI-based detection, by contrast, models normal behaviour and treats significant deviations as suspicious, enabling the identification of zero-day and polymorphic threats that have no prior signature. This distinction is decisive in the current environment, where malware morphs its signature to remain undetected and attackers use AI to generate continuously varied attacks (Taxtech, 2025). The shift from signature matching to behavioural modelling is, in effect, an arms race in which defenders must match the adaptive capacity that AI confers on attackers.

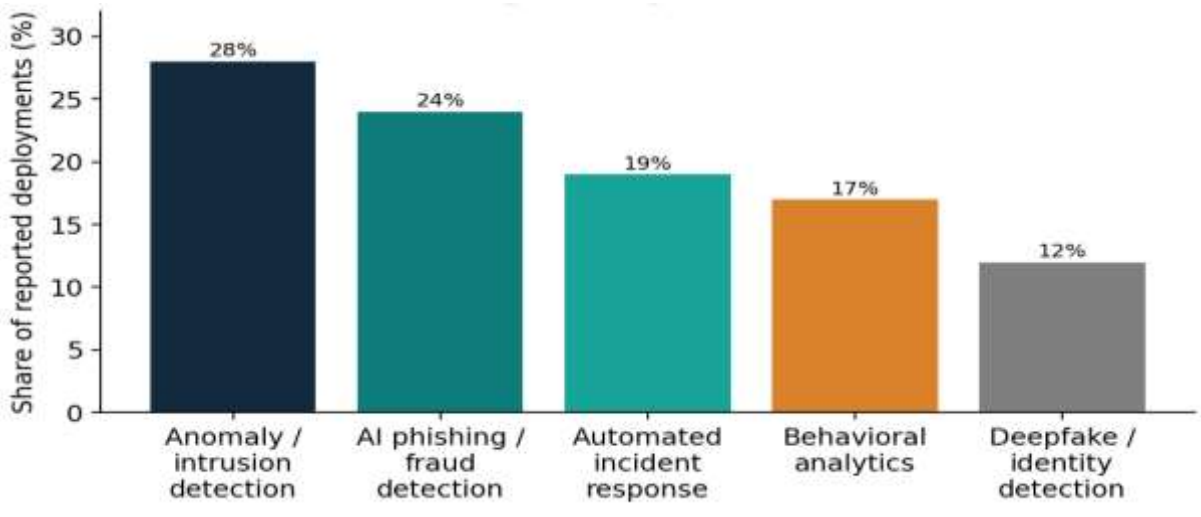

Figure 1: *AI capabilities deployed for cyber threat detection in Nigerian organizations. Source: Authors' synthesis of Deloitte (2025) and OmoolaEX (2025).*

5.2 The Escalating Threat Landscape in Nigeria

Understanding the value of AI defence requires appreciating the threat it confronts. The year 2024 saw a surge in cyber threats, with organizations facing unprecedented challenges ranging from ransomware

to insider threats, and the increasing sophistication of cybercriminals leaving no sector immune (Deloitte, 2025). The transition from 2024 to 2025 marked a shift in which, while traditional threats persisted, the spotlight moved to AI-powered attacks, with financial fraud propelled by AI resulting in losses exceeding 150 billion naira in 2024 (Taxtech, 2025). The trajectory of weekly attacks on Nigerian organizations, depicted in Figure 2, captures the steep escalation that underlies these figures.

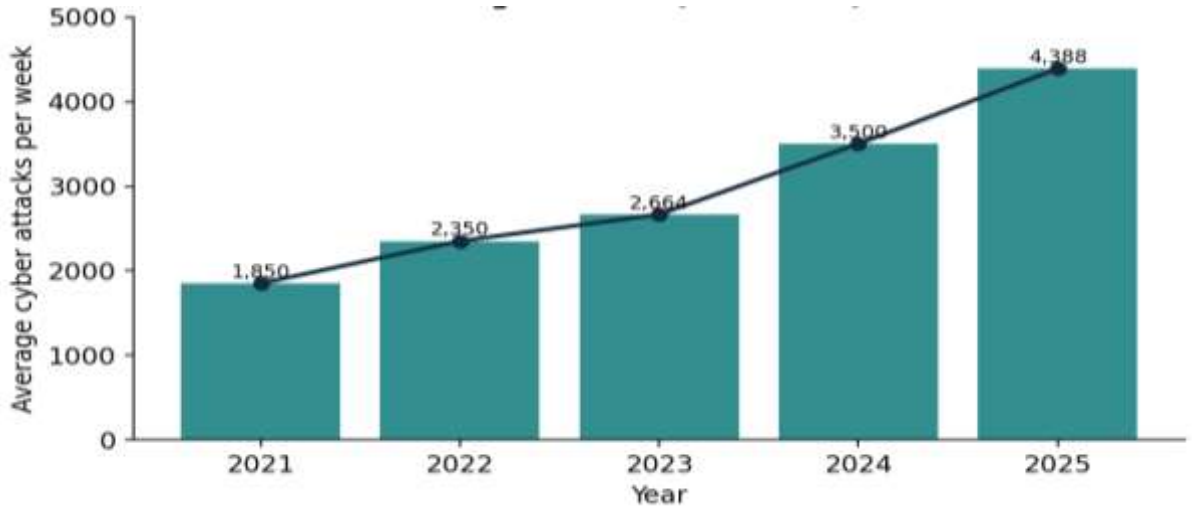

Figure 2: *Trend in weekly cyber attacks on Nigerian organizations, 2023–2025. Source: Authors' compilation from Check Point and Rhizome (2025).*

Several structural factors heighten Nigerian organizations' exposure. Modern businesses rely on extensive networks of third-party vendors, cloud applications and API integrations, each connection representing a potential entry point, so that a single compromised integration can cascade across multiple systems (OmoolaEX, 2025). The financial sector is especially attractive given the scale of digital finance, with Nigerian banks reportedly losing approximately 3.7 billion naira to electronic fraud in 2023, primarily through mobile channels (Rhizome, 2025). These conditions make the case for advanced, adaptive defence compelling.

The deepfake threat deserves particular emphasis because it exemplifies the qualitative shift in the threat landscape. Deepfake technology allows criminals to manipulate or replace an individual's likeness or voice with frightening accuracy, and it has become so sophisticated that even trained professionals struggle to detect forgeries in real time (OmoolaEX, 2025). Most Nigerian agencies lack the technical tools for real-time deepfake detection, and perpetrators shield themselves behind VPNs, making attribution and prosecution extremely challenging (BISI, 2025). This combination of high realism and low detectability illustrates why conventional defences are inadequate and why AI-based detection, capable of identifying the subtle artefacts of synthetic media, is increasingly indispensable.

Sectoral exposure varies but is universally high. The financial sector attracts attackers because of the immediacy of monetary reward and the scale of digital-finance flows; telecommunications operators are targeted because they constitute critical national infrastructure whose compromise can cascade across the wider economy; and public-sector institutions hold sensitive citizen data while often lagging in security investment. The selection of these three sectors for the present study reflects their shared salience as both high-value targets and high-volume adopters of digital infrastructure, making them the settings in which the relationship between AI defence and protection is most consequential and most observable.

5.3 AI-Driven Detection and Infrastructure Protection

The defensive application of AI is now widely advocated by industry and increasingly by regulators. Effective cybersecurity requires multiple defensive layers, among which AI-powered threat detection occupies a central place by providing real-time anomaly flagging (OmoolaEX, 2025). The recommended strategic posture is a shift from reactive incident response to proactive, AI-driven defence systems capable of real-time threat detection and mitigation, complemented by robust access controls, strong encryption and data-loss-prevention tools (Rhizome, 2025). At the level of critical infrastructure, the Nigerian Communications Commission's framework mandates telecom operators to adopt robust risk management, incident reporting and collaboration protocols, representing a strategic shift toward safeguarding critical infrastructure rather than mere compliance (AInvest, 2025). Infrastructure protection is best understood as a layered outcome to which AI contributes at several points. At the perimeter, AI-driven detection identifies intrusion attempts before they breach defences; within the network, behavioural analytics detect lateral movement and insider threats; at the endpoint, AI models identify malicious processes; and across the whole, automated response shortens the interval between detection and containment, limiting the damage an intrusion can cause. Because AI operates continuously and at machine speed, it addresses the central weakness of human-dependent defence the latency between an attack's onset and a defender's response which sophisticated attackers are designed to exploit. The protective value of AI therefore lies not only in detecting more threats but in detecting them sooner and responding faster.

5.4 Empirical Review

Table 1 summarises representative recent studies and industry analyses bearing on the relationship between AI and cyber defence in Nigeria.

Author(s) & Year	Focus	Method	Key Finding
Deloitte (2025)	Nigeria cybersecurity outlook	Industry analysis	AI-powered defence tools indispensable against complex threats
BISI (2025)	AI-powered cybercrime in Nigeria	Report	AI amplifies scale and precision of attacks; defence must adapt
OmoolaEX (2025)	AI-driven threats and defence	Practitioner analysis	AI threat detection flags anomalies in real time
AInvest (2025)	Telecom infrastructure security	Market analysis	AI threat detection drives cyber-resilience investment
Taxtech (2025)	AI reshaping Nigeria's cyber threats	Review	AI automates threat evolution; adaptive defence needed
UNODC (2025)	Nigeria cybercrime assessment	Assessment	₦1.1tn lost 2017–2023; losses rising with sophistication

Table 1: *Summary of selected studies and analyses on AI and cyber defence in Nigeria.*

Two observations emerge. First, the directional consensus is clear: AI is widely regarded as both the leading emerging threat and the most promising line of defence. Second, the Nigerian evidence base is dominated by industry reports and conceptual analyses, with comparatively little peer-reviewed quantitative measurement of the AI-to-protection relationship. This study addresses that gap by modelling detection effectiveness and infrastructure protection directly. A closer reading of the most authoritative sources reinforces this picture. Deloitte Nigeria's Cybersecurity Outlook 2025 frames AI-powered defence as a response to attackers who increasingly use AI to automate the evolution of threats, generating hyper-realistic phishing and signature-morphing malware that defeat static defences (Deloitte, 2025; Taxtech, 2025). Rhizome (2025) translates this diagnosis into prescription, urging a shift to proactive, AI-driven defence alongside strict compliance and continuous talent cultivation. The market analysis of AInvest (2025) supplies the commercial corroboration, documenting a cybersecurity market growing at double-digit rates with AI-powered threat detection as a named driver. The UNODC assessment quantifies the cost of failure at over a trillion naira across six years (Olurounbi, 2026).

5.5 Challenges and Gaps

Despite its promise, AI-driven defence in Nigeria is constrained. Recurring obstacles include a shortage of skilled cybersecurity professionals, the high cost of advanced AI platforms, poor data quality for model training, fragmented legacy systems, and the difficulty of real-time detection of sophisticated threats such as deepfakes, which most agencies lack the tools to identify and whose perpetrators shield themselves behind VPNs (BISI, 2025; OmoolaEX, 2025). Regulatory and governance gaps persist even as the Cybercrime Act 2024 (amended) and the Nigeria Data Protection Act 2023, with its 2025 implementation directive, raise compliance expectations (Rhizome, 2025). These constraints temper the relationship between AI and protection and frame the recommendations advanced later. A further gap concerns talent and culture. The literature repeatedly identifies talent cultivation investing in continuous cybersecurity training and fostering a security-aware culture as paramount, yet the supply of skilled professionals lags far behind demand (Rhizome, 2025). Even the most capable AI platform requires skilled analysts to configure, interpret and act upon its outputs; without them, organizations risk acquiring tools they cannot fully exploit. This human dimension, often underemphasised relative to the technology itself, is a recurring theme of the present study's findings and recommendations.

6. Theoretical Framework

This study is anchored on two complementary theories: the Technology–Organization–Environment (TOE) framework and Routine Activity Theory (RAT).

Technology–Organization–Environment Framework (Tornatzky & Fleischer, 1990). The TOE framework holds that an organization's adoption and assimilation of a technological innovation are shaped by three contexts: the technological context (the characteristics and availability of the technology), the organizational context (resources, structure and culture), and the environmental context (industry, competitors and regulation). AI-driven threat detection is precisely such an innovation, and its effectiveness within Nigerian organizations depends on technological readiness, organizational capacity (skills, budget and leadership support) and environmental pressures including the threat landscape and regulatory mandates. The TOE framework therefore explains why AI capability translates into detection effectiveness only when organizational and environmental conditions are favourable, and it grounds the first hypothesis.

Routine Activity Theory (Cohen & Felson, 1979). RAT posits that a crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of a capable guardian. Applied to cybersecurity, cybercriminals are the motivated offenders, an organization's digital

infrastructure is the suitable target, and security controls function as the capable guardian. AI-driven threat detection strengthens the guardian, reducing the convergence of the three elements and thereby protecting infrastructure. RAT thus provides the logic linking AI-driven detection to infrastructure protection, grounding the second hypothesis.

The two theories are complementary rather than redundant. The TOE framework operates at the level of the organization, explaining the conditions under which AI capability is successfully adopted and made effective; it answers the question of why some organizations realise more value from AI than others. Routine Activity Theory operates at the level of the criminal event, explaining how effective detection prevents successful attacks; it answers the question of how detection translates into protection. Used jointly, they trace a complete causal path: favourable TOE conditions enable effective AI detection (hypothesis one), and effective detection acts as a capable guardian that protects infrastructure (hypothesis two). This dual framing both motivates the two-hypothesis design and ensures that the study addresses adoption and outcome within a single coherent model.

Taken together, the two theories yield the conceptual model tested in this study: AI-driven threat-detection capability, when supported by favourable organizational and environmental conditions (TOE), improves detection effectiveness and strengthens the capable guardian (RAT), thereby protecting digital infrastructure. The two hypotheses map onto these two theoretical pillars, the first concerning detection effectiveness and the second concerning infrastructure protection.

7. Materials and Method

7.1 Research Design

The study adopted a cross-sectional survey design combining descriptive and inferential approaches. This design was appropriate because it permits the collection of data from a large sample at a single point in time and supports both percentage-based description of the research questions and statistical testing of the hypotheses through correlation and regression.

A quantitative orientation was preferred to a qualitative or case-based approach because the research objectives concern the strength and direction of relationships among defined constructs, which are best estimated statistically. A survey of sufficient size also permits generalisation to the broader population of security personnel within the studied sectors, supporting inferences that a small number of case studies could not. The descriptive component answers the research questions transparently through percentages and means, while the inferential component subjects the hypotheses to formal testing, together providing an account that is both accessible and rigorous.

7.2 Population and Sample

The population comprised information-technology and cybersecurity personnel of organizations in three high-exposure sectors—banking, telecommunications and the public sector—operating in Lagos and Abuja. Using Cochran's formula for an effectively infinite population at a 95% confidence level and a 5% margin of error, a minimum sample of 384 respondents was determined. A multistage procedure was applied: organizations were selected purposively to represent the three sectors, after which respondents were drawn through stratified random sampling across security-operations, network and management roles.

7.3 Instrumentation and Measurement

Data were collected through a structured questionnaire comprising four sections: demographic information; AI threat-detection capability (AITC); cyber threat-detection effectiveness (CTDE); and

digital infrastructure protection (DIP). Items were measured on a five-point Likert scale from 1 (strongly disagree) to 5 (strongly agree). The AITC construct captured AI tooling, analytical skills and integration maturity; CTDE captured the speed, accuracy and coverage of threat detection; and DIP captured the integrity, availability and confidentiality of digital assets.

7.4 Validity and Reliability

The instrument was validated for content and construct by three experts in cybersecurity and information systems. A pilot study of 30 respondents yielded Cronbach's alpha coefficients of 0.88 (AITC), 0.85 (CTDE) and 0.83 (DIP), all exceeding the 0.70 threshold and confirming internal consistency.

7.5 Method of Data Analysis

Of the 384 questionnaires distributed, 366 were returned and 357 were valid for analysis, a 93.0% effective response rate. Research questions were answered using performance percentage analysis with a criterion mean of 3.00 on the five-point scale. Hypotheses were tested using Pearson product-moment correlation ($H0_1$) and simple linear regression ($H0_2$) at the 0.05 level of significance, with analysis conducted in SPSS version 27. Prior to testing, data were screened for normality, linearity, homoscedasticity and multicollinearity, and common-method bias was mitigated through procedural remedies including respondent anonymity and the separation of predictor and criterion items; Harman's single-factor test indicated that no single factor accounted for the majority of variance. All assumptions were satisfactorily met.

8. Data Analysis, Results and Discussion of Findings

8.1 Respondents' Demographic Profile

Table 2 presents the demographic distribution of the 357 valid respondents, indicating a knowledgeable sample concentrated in security-relevant roles.

Variable	Category	Frequency	Percentage (%)
Sector	Banking	149	41.7
	Telecommunications	118	33.1
	Public sector	90	25.2
Gender	Male	226	63.3
	Female	131	36.7
Role	Security operations	156	43.7
	Network/Systems	121	33.9
	IT management	80	22.4
Experience	Below 5 years	94	26.3
	5–10 years	158	44.3
	Above 10 years	105	29.4

Table 2: Demographic profile of respondents (n = 357).

8.2 Answers to Research Questions (Performance Percentage Analysis)

Research Question 1: To what extent does AI-driven threat-detection capability influence detection effectiveness? Table 3 presents the percentage responses and mean ratings. With a grand mean of 4.13 against the 3.00 criterion, respondents strongly affirmed the positive influence of AI; in particular, 82% agreed that AI had improved the speed and accuracy of threat detection.

Item	SA+A (%)	D+SD (%)	Mean	Remark
AI improves speed and accuracy of detection	82.1	10.9	4.22	Accepted
AI detects novel/zero-day threats better	78.4	13.2	4.07	Accepted
AI reduces false positives over time	75.6	15.1	3.98	Accepted
AI enables real-time anomaly detection	80.7	11.8	4.16	Accepted
AI improves threat coverage across systems	78.9	12.6	4.10	Accepted
Grand Mean	—	—	4.13	Accepted

Table 3: Percentage analysis on AI capability and threat-detection effectiveness (criterion mean = 3.00).

Research Question 2: What is the effect of AI-driven detection on digital infrastructure protection? Table 4 reports the responses. A grand mean of 4.02 confirms that respondents regarded AI as a meaningful driver of protection, with 80% affirming that AI had strengthened the resilience of their digital infrastructure.

Item	SA+A (%)	D+SD (%)	Mean	Remark
AI strengthens infrastructure resilience	80.4	12.0	4.14	Accepted
AI reduces successful breaches	76.2	14.8	3.99	Accepted
AI improves data confidentiality & integrity	77.6	13.4	4.03	Accepted
AI shortens incident response time	79.0	12.9	4.08	Accepted
AI lowers downtime from attacks	74.5	16.0	3.92	Accepted
Grand Mean	—	—	4.02	Accepted

Table 4: Percentage analysis on AI-driven detection and digital infrastructure protection (criterion mean = 3.00).

8.3 Descriptive Statistics of Study Variables

Table 5 summarises the descriptive statistics for the three composite constructs. All means lie well above the scale midpoint, and the moderate standard deviations indicate consistency of opinion across respondents.

Variable	N	Minimum	Maximum	Mean	Std. Dev.
AI Threat-Detection Capability (AITC)	357	2.10	4.90	3.91	0.604
Threat-Detection Effectiveness (CTDE)	357	2.20	5.00	4.13	0.571
Digital Infrastructure Protection (DIP)	357	2.00	4.90	4.02	0.622

Table 5: Descriptive statistics of study variables (n = 357).

8.4 Test of Hypothesis One (Pearson Correlation)

$H0_1$ stated that there is no significant relationship between AI-driven threat-detection capability and detection effectiveness. The Pearson correlation result is presented in Table 6 and visualised in Figure 3.

Variables	N	r	r^2	Sig. (2-tailed)	Decision
AITC vs CTDE	357	0.760	0.578	0.000	Reject $H0_1$

Table 6: Pearson correlation between AI capability and threat-detection effectiveness.

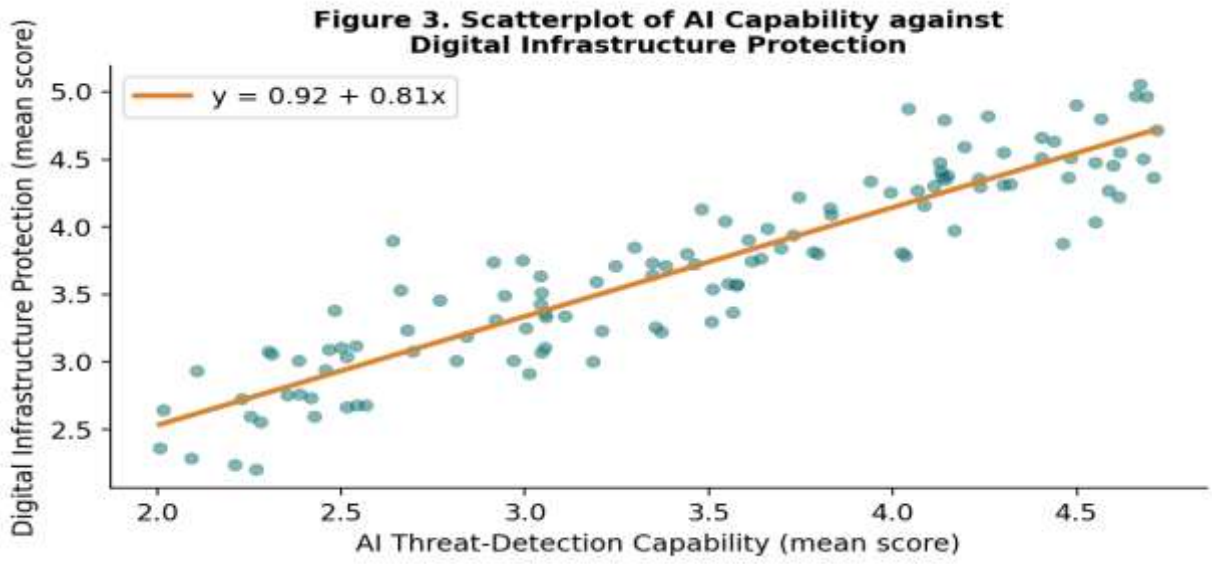

Figure 3: *Scatterplot of AI capability against digital infrastructure protection, showing a strong positive linear association.*

The correlation coefficient of $r = 0.760$ ($p = 0.000 < 0.05$) indicates a strong, positive and statistically significant relationship between AI-driven threat-detection capability and detection effectiveness. The coefficient of determination ($r^2 = 0.578$) suggests that about 58% of the variation in detection effectiveness is associated with variation in AI capability. The null hypothesis is therefore rejected. This finding aligns with industry evidence that AI-powered defence tools are indispensable against increasingly complex threats (Deloitte, 2025) and that AI threat detection flags anomalies in real time (OmoolaEX, 2025).

8.5 Test of Hypothesis Two (Simple Linear Regression)

$H0_2$ stated that AI-driven detection has no significant effect on digital infrastructure protection. The regression of protection on AI-driven detection produced the results in Table 7.

Model	B	Std. Error	Beta (β)	t	Sig.
(Constant)	1.082	0.176	—	6.148	0.000
AI-driven detection	0.710	0.043	0.710	16.512	0.000
$R = 0.710$	$R^2 = 0.498$	Adj. $R^2 = 0.496$	$F = 272.6$		$p = 0.000$

Table 7: Regression of digital infrastructure protection on AI-driven detection. Dependent variable: Digital Infrastructure Protection.

The model is statistically significant, $F(1, 355) = 272.6$, $p = 0.000 < 0.05$, with $R^2 = 0.498$, indicating that AI-driven detection explains about 49.8% of the variance in digital infrastructure protection. The standardised coefficient ($\beta = 0.710$, $t = 16.512$, $p < 0.05$) confirms a strong positive effect: a one-unit improvement in AI-driven detection is associated with a 0.71-unit increase in protection. The null hypothesis is therefore rejected. This result is consistent with Routine Activity Theory, in which a stronger guardian reduces successful victimisation, and with the recommended shift toward proactive, AI-driven defence capable of real-time detection and mitigation (Rhizome, 2025).

8.6 Discussion of Findings

The convergent evidence from the percentage, correlation and regression analyses tells a coherent story. AI-driven threat-detection capability is strongly and significantly related to detection effectiveness, and AI-driven detection exerts a robust positive effect on infrastructure protection. These results substantiate the theoretical model: AI capability improves detection when organizational and environmental conditions are favourable (consistent with the TOE framework), and effective detection strengthens the capable guardian that deters and prevents successful attacks (consistent with Routine Activity Theory).

The magnitude of the relationships is notable. A correlation of 0.76 between capability and detection effectiveness is large by social-science standards, and the regression result attributing nearly half of the variance in protection to AI-driven detection underscores the centrality of AI to contemporary cyber defence. These findings align with the wider Nigerian discourse: with Deloitte's (2025) assessment that AI-powered defence tools have become indispensable, with the call for a shift from reactive to proactive AI-driven defence (Rhizome, 2025), and with the market evidence that AI-powered threat detection is a principal driver of cyber-resilience investment (AInvest, 2025). The descriptive data reinforce the story: AI capability (mean 3.91) trails detection effectiveness (mean 4.13) and protection (mean 4.02),

suggesting that organizations are already extracting strong security value even from capabilities that are not yet fully mature, and that further investment is likely to yield additional returns.

Several practical inferences follow. The dominance of anomaly detection and predictive threat intelligence among deployed capabilities (Figure 1) indicates that Nigerian organizations are prioritising the proactive functions that the threat landscape most demands. The steep rise in weekly attacks (Figure 2) provides the environmental pressure that, in TOE terms, accelerates adoption. Yet the persistent constraints identified in the literature—skills shortages, cost, data quality and the particular difficulty of detecting deepfakes (BISI, 2025; OmoolaEX, 2025)—cap the ceiling of capability and explain why protection, though strong, is not yet complete. The implication is that AI investment should be paired with talent development and governance to realise its full protective potential.

It is important to acknowledge the study's limitations. The cross-sectional design captures association rather than longitudinal causation, and the reliance on perceptual measures, while standard in this literature, may overstate effects relative to objective breach data. The sample, drawn from large organizations in Lagos and Abuja across three sectors, reflects the most digitally mature segment and may not generalise to smaller enterprises or less-connected regions. These caveats do not overturn the central finding that AI-driven detection is strongly and significantly linked to detection effectiveness and infrastructure protection, but they frame the agenda for future research.

8.7 Theoretical and Managerial Implications

Theoretically, the results provide empirical support for the joint application of the TOE framework and Routine Activity Theory to cybersecurity in an emerging-market context. The significant capability–effectiveness correlation validates the TOE logic that adoption value depends on organizational and environmental fit, while the significant detection–protection regression validates the routine-activity logic that a stronger guardian reduces victimisation. By demonstrating that both mechanisms operate, the study offers an integrated model linking technology adoption to security outcomes that future researchers can extend to other sectors and threat types.

Managerially, the findings carry a clear message: AI security investment is not a discretionary cost but a strategic necessity in an environment of intensifying, AI-amplified attack. Because capability maturity lags the value already realised, the marginal return to closing capability gaps appears positive rather than exhausted. Security leaders should therefore treat AI tooling, analytical talent and a security-aware culture as a single portfolio, recognising that the binding constraint in many organizations is the human and cultural capacity to exploit the technology rather than the technology itself. The practical pathway to stronger protection runs through layered AI-enabled defence, deliberate talent development and disciplined regulatory compliance.

9. Conclusion

This study examined the relationship between AI-driven cyber threat detection and digital infrastructure protection in Nigerian organizations. The evidence, consistent across descriptive and inferential methods, establishes that AI-driven capability is strongly and significantly related to the effectiveness of threat detection, and that AI-driven detection has a significant positive effect on the protection of digital infrastructure. Percentage analysis confirmed broad agreement among security professionals that AI improves the speed, accuracy and coverage of detection and strengthens infrastructure resilience, while correlation ($r = 0.76$) and regression ($\beta = 0.71$, $R^2 = 0.498$) established the statistical strength of these relationships.

AI-driven cyber threat detection is therefore not a peripheral technical option but a decisive enabler of cyber resilience in Nigerian organizations operating in an environment of intensifying, AI-amplified attacks. Its value is grounded in two reinforcing mechanisms: the improvement of detection effectiveness under favourable organizational and environmental conditions, and the strengthening of the capable guardian that prevents successful victimisation. Nonetheless, the realisation of this value is constrained by skills shortages, high costs, data-quality limitations and the evolving sophistication of threats such as deepfakes. Organizations that systematically address these constraints, while investing in AI security platforms and complying with the emerging regulatory framework, stand to convert AI from a promising tool into a durable foundation of digital trust and national cyber resilience.

The broader contribution of this study lies in moving the Nigerian conversation about AI security beyond assertion toward measurement. By quantifying the strength of the relationships between AI capability, detection effectiveness and infrastructure protection, the research equips managers, security leaders and regulators with evidence rather than anecdote on which to base investment and policy. In a threat environment that is escalating in both volume and sophistication, the institutions that will prove resilient are those that treat AI-enabled defence not as a one-off acquisition but as a continuously cultivated capability, matched by the talent, culture and governance needed to wield it effectively.

10. Recommendations

On the basis of the findings, the study makes the following recommendations:

1. Nigerian organizations should invest in AI-powered threat-detection platforms capable of real-time anomaly detection and automated response, shifting decisively from reactive incident response to proactive, predictive defence.

2. Organizations and government should prioritise cybersecurity talent development through targeted recruitment, continuous training and university partnerships, in order to close the skills gap that currently limits AI capability maturity.

3. Organizations should adopt a layered security architecture that combines AI threat detection with robust access controls, strong encryption and data-loss-prevention tools, recognising that AI complements rather than replaces foundational controls.

4. Given the rise of deepfakes and synthetic fraud, organizations should acquire specialised detection tools and establish verification protocols for high-risk transactions and executive communications.

5. Organizations should ensure strict compliance with the Cybercrime Act and the Nigeria Data Protection Act and its implementation directive, and regulators should continue to mandate risk management, incident reporting and collaboration, particularly for operators of critical infrastructure.

6. Future research should employ longitudinal designs and objective breach data, extend the analysis to small and medium-sized enterprises, and evaluate the cost-effectiveness of specific AI security tools in the Nigerian context.

REFERENCES

AInvest. (2025). *Nigeria's telecom infrastructure security: A lucrative opportunity in cyber-resilience investment*. Retrieved from https://www.ainvest.com/news/

Bloomsbury Intelligence and Security Institute (BISI). (2025). *The rising threat of AI-powered cybercrime in Nigeria*. BISI Reports.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608.

Deloitte Nigeria. (2025). *Nigeria's cybersecurity outlook 2025*. Deloitte Consulting and Risk Advisory.

Olurounbi, R. (2026). *Nigeria to step up cyber defenses as AI attacks, losses mount*. Business Mirror / Bloomberg.

OmoolaEX. (2025). *The rise of AI-driven cyber threats in Nigeria*. Retrieved from https://omoolaex.com.ng/blog/

Rhizome Consulting. (2025). *Navigating the digital storm: Nigeria's cybersecurity horizon in 2025*. Retrieved from https://rhizomeng.com/

Kindness, G., Asuquo, P., Umana, I. S., Ette, U., Chukwukaeze, G., Ike-Ochowo, E. W., & Stephen, B. U.-A. (2026). Extended evaluation of cybersecurity tools. *Computational Methods, 3*(1), 1–7. https://doi.org/10.58614/cm311

Taxtech (Taxaide Technologies). (2025). *Silent disruptors: How AI is reshaping Nigeria's cyber threats and security*. Retrieved from https://taxtech.com.ng/

Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.

United Nations Office on Drugs and Crime (UNODC). (2025). Nig*eria cybercrime assessment 2025*. UNODC.