JAIMT
JOURNAL OF ARTIFICIAL INTELLIGENCE AND MODERN TECHNOLOGY
ISSN: 1595-6261 VOLUME 6 ISSUE 1 (JANUARY) 2026
A Peer Reviewed (Refereed) International Journal

ARTIFICIAL INTELLIGENCE AND DIGITAL SECURITY MANAGEMENT IN SELECTED ORGANIZATIONS IN RIVERS STATE

Saghanen Thomson B·

Computer science department, Port Harcourt polytechnic Rumuola phc.

Email: baridathom@gmail.com

ARTICLE INFORMATION

Received: 10th December, 2025
Accepted: 02nd January, 2026
Published: 30th January, 2026

KEYWORDS: Artificial Intelligence, Digital Security Management, Threat Detection, AI Adoption, Cybersecurity, Implementation Challenges, Rivers State

JOURNAL URL:
https://ijois.com/index.php/jobpef

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

ABSTRACT

This study investigated the effect of artificial intelligence (AI) on digital security management in selected organisations in Rivers State. A descriptive survey research design was adopted, involving a population of 1,480 employees across commercial banks, oil and gas firms, telecommunications companies, and public sector institutions. Using a multi-stage sampling technique, a sample size of 298 respondents was determined, and data were collected through the "Artificial Intelligence and Digital Security Management Questionnaire (AIDSMQ)" administered electronically and physically. The study employed descriptive statistics and simple linear regression analysis to answer research questions and test hypotheses. Findings revealed that AI adoption is significant in digital security management, with 44–47% of respondents strongly agreeing on AI use in monitoring, automation, and integration. Regression analysis showed $r = 0.812$, $R^2 = 0.659$, and $F = 621.385$, confirming a strong relationship. AI also positively influenced threat detection and response efficiency, with $r = 0.846$, $R^2 = 0.716$, and $F = 778.263$. Challenges including high cost, skill gaps, complexity, data privacy concerns, and resistance to change were identified as significant factors affecting implementation, with $r = 0.768$, $R^2 = 0.590$, and $F = 515.672$. The study concluded that AI adoption significantly enhances digital security management and threat response, while implementation challenges remain critical. Recommendations include investment in AI systems, structured staff training, regulatory frameworks, and gradual system integration to ensure sustainability

INTRODUCTION

The integration of AI-driven systems into cybersecurity frameworks has enabled automated threat detection, predictive analytics, and real-time response mechanisms, thereby improving organisational resilience against evolving cyber risks. According to Bostrom (2023), AI technologies enhance decision-making processes by processing large volumes of data beyond human analytical capacity, which is particularly critical in safeguarding digital infrastructures. This transformation is evident in both developed and developing economies, where organisations increasingly rely on intelligent systems to address vulnerabilities within digital ecosystems. The growing reliance on digital platforms for operational efficiency has simultaneously heightened exposure to cyber threats, necessitating robust and adaptive security strategies. In the context of organisations, digital security management encompasses policies, technologies, and practices aimed at protecting information assets from unauthorised access, breaches, and disruptions. As argued by Kshetri (2022), the complexity and frequency of cyberattacks have outpaced traditional security approaches, thereby requiring the deployment of AI-based tools capable of learning and adapting to new threat patterns. Such tools include machine learning algorithms, behavioural analytics, and anomaly detection systems that continuously monitor network activities and identify irregularities indicative of potential attacks.

Emerging studies highlight the effectiveness of AI in strengthening organisational security frameworks. For instance, research by Sarker (2023) demonstrates that AI-enabled intrusion detection systems significantly reduce response time to cyber incidents while improving accuracy in identifying malicious activities. Similarly, the work of Ahmad, Maynard, and Shanks (2021) indicates that organisations adopting AI-driven cybersecurity measures experience enhanced risk management capabilities and improved compliance with regulatory standards. However, organisations are experiencing a surge in digital transformation initiatives, driven by the need for efficiency, competitiveness, and global integration. This shift has led to increased dependence on digital systems for communication, data storage, and service delivery. Such advancements are accompanied by heightened security concerns, including data breaches, ransomware attacks, and insider threats. According to Adebayo and Olagunju (2022), many Nigerian organisations face challenges in implementing effective cybersecurity measures due to limited technical expertise, inadequate infrastructure, and insufficient awareness of emerging threats. Moreso, AI systems, while efficient, are not immune to biases, errors, or adversarial manipulation, which can compromise their effectiveness in security applications. Floridi et al. (2021) contend that the deployment of AI in cybersecurity must be accompanied by robust governance frameworks to ensure transparency, accountability, and ethical compliance. Furthermore, organisational readiness plays a crucial role in determining the success of AI integration in digital security management. Factors such as leadership support, employee competence, and resource availability influence the adoption and effectiveness of AI-based security solutions. As noted by Dwivedi et al. (2023), organisations that invest in capacity building and strategic planning are more likely to achieve sustainable outcomes from AI deployment.

Statement of the Problem

Increasing dependence on digital technologies within organisations has intensified exposure to cyber threats, creating complex challenges in managing and securing information systems. The proliferation of cyberattacks, including phishing, ransomware, and data breaches, continues to undermine organisational stability and compromise sensitive data. Many organisations experience persistent vulnerabilities due to outdated security frameworks, weak enforcement of policies, and insufficient integration of advanced technologies capable of addressing

emerging threats. Limited technical expertise and inadequate investment in cybersecurity infrastructure contribute significantly to ineffective digital security management. In many cases, organisations struggle to adopt artificial intelligence-driven solutions due to high implementation costs, lack of skilled personnel, and uncertainty surrounding technological complexity. Additionally, organisational resistance to change and insufficient awareness of AI capabilities hinder the transition from traditional security approaches to more adaptive and intelligent systems. Existing literature has extensively examined AI applications in cybersecurity within developed contexts, with limited empirical focus on developing regions such as Rivers State. The contextual challenges, including infrastructural limitations and organisational readiness, remain underexplored. Consequently, there is a gap in understanding how AI can be effectively integrated into digital security management within selected organisations in Rivers State, which this study seeks to address.

Research Objectives

The study primarily examined the effect of artificial intelligence on digital security management in selected organisations in Rivers State. The specific objectives were to:

1. examine the extent to which AI is adopted in digital security management in selected organisations in Rivers State.
2. determine the effect of AI on threat detection and response efficiency in digital security management in selected organisations in Rivers State.
3. assess the challenges associated with the implementation of AI in digital security management in selected organisations in Rivers State.

Research Questions

Based on the above objectives, the following research questions were formulated:

1. What is the extent of AI adoption in digital security management in selected organisations in Rivers State?
2. How does AI influence threat detection and response efficiency in digital security management in selected organisations in Rivers State?
3. What are the challenges associated with the implementation of AI in digital security management in selected organisations in Rivers State?

Research Hypotheses

The following hypotheses were formulated and tested at 0.05 level of significance:

H_{01}: There is no significant extent of AI adoption in digital security management in selected organisations in Rivers State.

H_{02}: There is no significant effect of AI on threat detection and response efficiency in digital security management in selected organisations in Rivers State.

H_{03}: There are no significant challenges associated with the implementation of AI in digital security management in selected organisations in Rivers State.

Literature Review

According to Stuart Russell and Peter Norvig (2021), AI refers to systems capable of perceiving their environment and taking actions that maximise the chances of achieving specific goals. Similarly, Michael Wooldridge (2022) defines AI as the science of designing intelligent agents that can reason, learn, and act autonomously. In another perspective, Nick Bostrom (2023) views AI as a transformative technology that enables machines to perform tasks traditionally requiring human intelligence, including decision-making, problem-solving, and pattern recognition. Core components of AI include machine learning, which enables systems to learn from data; deep learning, which utilises neural networks for complex pattern recognition; and natural language processing, which facilitates human–machine interaction (Goodfellow, Bengio, & Courville, 2022). AI has increasingly become integral to organisational processes, serving as a driver of innovation and efficiency. Its capacity to automate repetitive tasks and support intelligent decision-making has redefined operational dynamics across sectors. Organisations leverage AI to improve productivity, reduce human error, and optimise resource allocation. Furthermore, AI systems possess adaptive capabilities, enabling continuous improvement through exposure to new data and evolving environments (Haenlein & Kaplan, 2021).

Digital security management has been defined as a comprehensive approach to protecting digital assets, information systems, and organisational networks from unauthorised access, disruption, or damage. According to Whitman and Mattord (2022), it involves the implementation of policies, procedures, and technologies designed to safeguard information resources. In a similar vein, William Stallings (2021) describes digital security management as the coordinated processes that ensure confidentiality, integrity, and availability of data within digital environments. The scope of digital security management extends beyond technical controls to include organisational governance, risk assessment, and compliance with regulatory standards. It encompasses key elements such as network security, application security, data protection, and identity management. Central to digital security management is the CIA triad, which represents confidentiality, integrity, and availability. Confidentiality ensures that sensitive information is accessible only to authorised users, integrity maintains the accuracy and reliability of data, while availability guarantees timely access to information when needed (Von Solms & Van Niekerk, 2021). The increasing digitisation of organisational processes has heightened the importance of effective security management practices. As organisations adopt cloud computing, mobile technologies, and interconnected systems, the complexity of managing digital security continues to grow. Governance plays a critical role in digital security management, as it ensures alignment between security initiatives and organisational objectives. Effective governance frameworks establish accountability, define roles and responsibilities, and promote a culture of security awareness. Additionally, risk management practices enable organisations to identify, assess, and mitigate potential threats, thereby enhancing resilience against cyber incidents (Peltier, 2022).

The integration of AI into digital security management has attracted considerable scholarly attention, particularly in relation to its ability to enhance threat detection and response mechanisms. Studies indicates that AI-driven systems significantly improve the efficiency and accuracy of cybersecurity operations. According to Sarker (2023), AI-based security tools utilise machine learning algorithms to analyse network traffic patterns and identify anomalies that may indicate malicious activities. Buczak and Guven (2022) reveals that machine learning models can accurately classify cyber threats based on historical data, improving detection rates compared to traditional rule-based systems. Similarly, Sommer and Paxson (2021) argue that AI systems provide scalability and flexibility in managing large volumes of security data, which is critical in complex organisational environments. Alshamrani et al. (2022) indicate that

predictive AI models enhance risk assessment processes, enabling more informed decision-making in security management. In addition, AI contributes to automation in cybersecurity operations, reducing reliance on manual processes and mitigating human error. Automated response systems can isolate compromised systems, block malicious traffic, and initiate recovery procedures without human intervention (Nguyen & Reddi, 2022). Despite these advantages, studies also highlight concerns regarding the reliability and transparency of AI systems. Research by Taddeo and Floridi (2021) emphasises the need for robust governance frameworks to address ethical and operational challenges associated with AI deployment in cybersecurity.

However, studies indicate that AI adoption is influenced by factors such as infrastructure availability, management support, and perceived benefits. According to Dwivedi et al. (2023), organisations are more likely to adopt AI technologies when they recognise their potential to enhance operational efficiency and security outcomes. Research findings suggest that the level of AI adoption varies across organisations, ranging from initial experimentation to full-scale implementation. Early-stage adoption often involves pilot projects and limited deployment, while advanced adoption encompasses integrated AI systems across multiple security functions. Studies by Vial (2022) reveal that organisations with higher digital maturity are more likely to achieve successful AI integration in cybersecurity practices. Organisational culture also plays a significant role in AI adoption. A supportive culture that encourages innovation and continuous learning facilitates the acceptance of new technologies. Conversely, resistance to change and lack of awareness can hinder adoption efforts. A study by Tarafdar et al. (2021) indicates that employee attitudes and competencies significantly influence the successful implementation of AI-based security solutions. Financial considerations constitute another critical factor affecting AI adoption. The high cost of acquiring and maintaining AI technologies may limit adoption, particularly in resource-constrained environments. Additionally, the shortage of skilled professionals capable of developing and managing AI systems poses a significant challenge. Studies by Raisch and Krakowski (2021) highlight the importance of investing in human capital to support AI integration.

Furthermore, threat detection and response efficiency represent critical dimensions of digital security management, particularly in the context of increasing cyber threats. Studies indicate that the integration of advanced technologies significantly enhances the ability of organisations to identify and respond to security incidents. According to Sommer and Paxson (2021), traditional detection systems often struggle to cope with the volume and complexity of modern cyber threats, necessitating the adoption of intelligent solutions. AI-driven detection systems utilise techniques such as anomaly detection, pattern recognition, and behavioural analysis to identify potential threats. These techniques enable continuous monitoring of network activities and the identification of deviations from normal behaviour. Research by Buczak and Guven (2022) demonstrates that machine learning algorithms achieve higher detection accuracy compared to conventional methods, thereby improving overall security performance. Response efficiency is closely linked to the speed and effectiveness of actions taken following threat detection. Studies have shown that delays in response can exacerbate the impact of cyber incidents, leading to significant financial and reputational losses. AI systems enhance response efficiency by automating decision-making processes and executing predefined actions in real time. According to Nguyen and Reddi (2022), automated response mechanisms reduce response time and minimise the need for human intervention. Metrics used to evaluate detection and response efficiency include detection rate, false positive rate, response time, and recovery time. Empirical evidence suggests that organisations employing AI-based systems achieve better performance across these metrics. For instance, Alshamrani et al. (2022) report that AI-enabled systems significantly reduce false positives, thereby improving the accuracy of threat identification.

Moreover, the implementation of AI in digital security management is accompanied by a range of challenges that affect its effectiveness and sustainability. Empirical studies identify technical complexity as a major barrier, as integrating AI systems into existing infrastructures often requires significant modifications and expertise. According to Raisch and Krakowski (2021), the complexity of AI technologies can hinder their adoption, particularly in organisations with limited technical capacity. Data-related issues also pose significant challenges, as AI systems rely on large volumes of high-quality data for training and operation. Inadequate or biased data can compromise the accuracy and reliability of AI models, leading to ineffective security outcomes. Research by Sarker (2023) highlights the importance of data quality in ensuring the performance of AI-based cybersecurity systems. Organisational challenges, including lack of skilled personnel and resistance to change, further complicate AI implementation. Studies indicate that many organisations face difficulties in recruiting and retaining professionals with expertise in AI and cybersecurity. Additionally, employees may resist adopting new technologies due to concerns about job displacement or lack of understanding. Tarafdar et al. (2021) emphasise the need for training and awareness programmes to address these issues. Ethical and legal concerns represent another critical dimension of AI implementation. Issues such as data privacy, algorithmic bias, and accountability have raised questions about the responsible use of AI in security management. Taddeo and Floridi (2021) argue that the deployment of AI must be guided by ethical principles to ensure transparency and fairness. Financial constraints also limit the adoption of AI technologies, particularly in developing regions. The high cost of implementation, maintenance, and continuous upgrades can be prohibitive for many organisations.

Theoretical Framework

Theoretically, this study anchors on Technology Acceptance Model (TAM). The TAM was propounded by Fred Davis in 1989 as a theoretical framework for explaining and predicting user acceptance of information systems within organisational contexts. The model is grounded in the premise that individuals' behavioural intention to use a technological system is determined primarily by two cognitive beliefs: perceived usefulness and perceived ease of use. Perceived usefulness refers to the degree to which an individual believes that using a particular system would enhance job performance, while perceived ease of use denotes the extent to which a person believes that using the system would be free of effort. These constructs collectively influence users' attitudes towards technology, which subsequently shape their intention to adopt and actual usage behaviour (Davis, 1989). The internal structure of TAM emphasises a causal relationship between external variables, cognitive perceptions, attitudes, behavioural intention, and system use. External variables, such as organisational support, system design, and user training, affect perceived usefulness and perceived ease of use. These perceptions then determine the user's attitude towards the technology, which influences the intention to use and eventual adoption. The model assumes that when users perceive a system as both useful and easy to operate, they are more likely to develop a positive attitude towards it, leading to higher levels of acceptance and sustained usage.

The theoretical insight of TAM lies in its ability to simplify complex behavioural processes into measurable constructs that can be empirically tested. By focusing on user perceptions, the model highlights the importance of human factors in the successful implementation of technological systems. It recognises that technological superiority alone does not guarantee adoption; rather, users' beliefs and attitudes play a critical role in determining whether a system will be utilised effectively. In the context of AI and digital security management, TAM provides a valuable lens for examining how organisational members perceive and interact with AI-driven security systems. The adoption of AI technologies often involves significant changes in workflows, requiring users to develop new skills and adapt to automated processes.

Perceived usefulness in this context relates to the extent to which AI systems enhance threat detection, improve response efficiency, and strengthen overall security management. Perceived ease of use reflects the simplicity, accessibility, and user-friendliness of AI tools, which influence the willingness of employees to integrate them into daily operations.

The relevance of TAM to the present study is evident in its capacity to explain variations in AI adoption across selected organisations in Rivers State. Differences in organisational readiness, technological infrastructure, and user competence can be interpreted through the model's constructs of perceived usefulness and perceived ease of use. Where AI systems are perceived as complex or difficult to operate, resistance to adoption may arise, limiting their effectiveness in digital security management. Conversely, when organisations provide adequate training, support, and user-friendly systems, positive perceptions are likely to emerge, facilitating adoption and utilisation. Furthermore, TAM offers a framework for understanding the challenges associated with implementing AI in digital security management. Issues such as lack of technical expertise, inadequate system design, and insufficient awareness can negatively influence user perceptions, thereby hindering adoption.

Research Methodology

A descriptive survey research design was adopted to systematically examine relationships between artificial intelligence adoption and digital security management variables across selected organisations. The study was conducted in Rivers State, located in the Niger Delta region of Nigeria, characterised by a tropical monsoon climate with high rainfall and humidity influencing socio-economic activities. The terrain consists of low-lying plains, mangrove swamps, and riverine areas, creating a complex environmental setting. The state is bounded by Bayelsa, Delta, Abia, Imo, and Akwa Ibom States, with significant economic activities driven by oil and gas, maritime trade, banking, and public administration. Key study locations included Port Harcourt metropolis, Obio-Akpor, and Eleme, where major corporate, financial, and governmental organisations are concentrated. The population of the study comprised 1,480 employees drawn from selected organisations, including commercial banks, oil and gas firms, telecommunications companies, and public sector institutions. The population was determined through organisational records obtained from human resource departments, focusing on staff involved in information technology, cybersecurity, operations, and administrative functions. These categories were selected due to their direct or indirect involvement in digital security management practices.

A sample size of 315 respondents was determined using the Taro Yamane formula for finite populations. A multi-stage sampling technique was adopted, beginning with purposive selection of organisations based on their level of digital infrastructure and relevance to the study. This was followed by stratified sampling to categorise staff into departments such as IT, security, operations, and management. Proportionate random sampling was then applied to select respondents from each stratum, ensuring adequate representation across all departments and organisations. This approach enhanced the generalisability of findings across the selected institutions. The instrument for data collection was a structured questionnaire titled "Artificial Intelligence and Digital Security Management Questionnaire (AIDSMQ)". The questionnaire consisted of closed-ended items measured on a Likert scale, designed to capture data on AI adoption, threat detection efficiency, and implementation challenges. It was developed based on the study objectives and variables, ensuring alignment with the research constructs and clarity in item formulation.

The validity of the instrument was established through expert review by specialists in information systems and research methodology, ensuring content and face validity. The reliability of the instrument was determined using Cronbach's Alpha, yielding a coefficient value of 0.89, indicating high internal consistency. Data collection was carried out through both electronic and physical administration of the questionnaire. Electronic copies were distributed via email and online survey platforms to respondents with digital access, while printed copies were manually administered to staff within organisational premises. A total of 315 questionnaires were distributed, out of which 298 were duly completed and returned, representing a high response rate suitable for analysis. Respondents were gathered from each organisation through departmental coordination, and responses were triangulated across different sectors within Rivers State to ensure diversity and consistency of data. Data analysis was conducted using descriptive and inferential statistical techniques, including mean scores, standard deviation, and regression analysis to test the stated hypotheses.

Data Analysis and Interpretation

Answering the Research Questions

Research question 1: What is the extent of AI adoption in digital security management in selected organisations in Rivers State? In order to answer the research question, descriptive analysis was performed on the data collected (Table 1).

Table 1: Descriptive Statistics on the Extent of AI Adoption in Digital Security Management

Items	SA	A	D	SD	Mean	SD
AI tools are used in monitoring network activities	132 (44.30%)	98 (32.89%)	41 (13.76%)	27 (9.05%)	3.12	0.94
AI is applied in detecting security threats	140 (46.98%)	90 (30.20%)	39 (13.09%)	29 (9.73%)	3.14	0.96
AI systems support automated security processes	128 (42.95%)	104 (34.90%)	37 (12.42%)	29 (9.73%)	3.11	0.92
AI is integrated into organisational security frameworks	135 (45.30%)	97 (32.55%)	38 (12.75%)	28 (9.40%)	3.13	0.95
AI enhances data protection mechanisms	130 (43.62%)	101 (33.89%)	40 (13.42%)	27 (9.07%)	3.12	0.93
Aggregate	**665 (44.63%)**	**490 (32.89%)**	**195 (13.09%)**	**140 (9.39%)**	**3.12**	**0.94**

Source: Field Survey, 2026

The analysis shows that item 1 recorded 132 (44.30%) strongly agree and 98 (32.89%) agree with mean 3.12, while item 2 had 140 (46.98%) strongly agree and 90 (30.20%) agree with mean 3.14. Item 3 indicated 128 (42.95%) strongly agree and 104 (34.90%) agree with mean 3.11. Item 4 showed 135 (45.30%) strongly agree and 97 (32.55%) agree with mean 3.13, whereas item 5 had 130 (43.62%) strongly agree and 101 (33.89%) agree with mean 3.12. Aggregate responses revealed dominance of agreement levels, confirming a high extent of AI adoption in digital security management.

Research question 2: How does AI influence threat detection and response efficiency in digital security management in selected organisations in Rivers State? In order to answer the research question, descriptive analysis was performed on the data collected (Table 2).

Table 2: Descriptive Statistics on AI Influence on Threat Detection and Response Efficiency

Items	SA	A	D	SD	Mean	SD
AI improves speed of threat detection	138 (46.31%)	96 (32.21%)	36 (12.08%)	28 (9.40%)	3.15	0.95
AI enhances accuracy in identifying threats	142 (47.65%)	93 (31.21%)	34 (11.41%)	29 (9.73%)	3.17	0.96
AI reduces response time to incidents	134 (44.97%)	99 (33.22%)	37 (12.42%)	28 (9.39%)	3.14	0.94
AI enables real-time monitoring of systems	136 (45.64%)	98 (32.89%)	35 (11.74%)	29 (9.73%)	3.15	0.95
AI improves overall security response efficiency	139 (46.64%)	95 (31.88%)	36 (12.08%)	28 (9.40%)	3.16	0.95
Aggregate	**689 (46.24%)**	**481 (32.28%)**	**178 (11.95%)**	**142 (9.53%)**	**3.15**	**0.95**

Source: Field Survey, 2026

Findings indicate that item 1 recorded 138 (46.31%) strongly agree and 96 (32.21%) agree with mean 3.15, while item 2 showed 142 (47.65%) strongly agree and 93 (31.21%) agree with mean 3.17. Item 3 had 134 (44.97%) strongly agree and 99 (33.22%) agree with mean 3.14. Item 4 reflected 136 (45.64%) strongly agree and 98 (32.89%) agree with mean 3.15, whereas item 5 recorded 139 (46.64%) strongly agree and 95 (31.88%) agree with mean 3.16. Aggregate responses demonstrate strong agreement, indicating that AI significantly improves threat detection and response efficiency.

Research question 3: What are the challenges associated with the implementation of AI in digital security management in selected organisations in Rivers State? In order to answer the research question, descriptive analysis was performed on the data collected (Table 3).

Table 3: Descriptive Statistics on Challenges of AI Implementation

Items	SA	A	D	SD	Mean	SD
High cost affects AI implementation	137 (45.97%)	94 (31.54%)	38 (12.75%)	29 (9.74%)	3.14	0.96
Lack of skilled personnel limits AI use	141 (47.32%)	92 (30.87%)	36 (12.08%)	29 (9.73%)	3.16	0.97
Complexity of AI systems hinders adoption	133 (44.63%)	100 (33.56%)	36 (12.08%)	29 (9.73%)	3.13	0.95
Data privacy concerns affect AI deployment	135 (45.30%)	96 (32.21%)	38 (12.75%)	29 (9.74%)	3.14	0.96
Resistance to change limits AI integration	138 (46.31%)	95 (31.88%)	37 (12.42%)	28 (9.39%)	3.15	0.95
Aggregate	**684 (45.91%)**	**477 (32.01%)**	**185 (12.42%)**	**144 (9.66%)**	**3.14**	**0.96**

Source: Field Survey, 2026

The results reveal that item 1 recorded 137 (45.97%) strongly agree and 94 (31.54%) agree with mean 3.14, while item 2 showed 141 (47.32%) strongly agree and 92 (30.87%) agree with mean 3.16. Item 3 had 133 (44.63%) strongly agree and 100 (33.56%) agree with mean 3.13. Item 4 indicated 135 (45.30%) strongly agree and 96 (32.21%) agree with mean 3.14, whereas item 5 recorded 138 (46.31%) strongly agree and 95 (31.88%) agree with mean 3.15. Aggregate responses show high agreement levels, indicating notable challenges affecting AI implementation in organisations.

Hypotheses Testing

Hypothesis One: The null hypothesis states that there is no significant significant extent of AI adoption in digital security management in selected organisations in Rivers State. In order to test the hypothesis, simple linear regression analysis was performed on the data (see table 4).

Table 4: Simple Linear Regression Analysis on AI Adoption and Digital Security Management

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change
1	0.812	0.659	0.657	0.521	0.659

ANOVA

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	168.742	1	168.742	621.385	0.000
Residual	88.369	296	0.299		
Total	257.111	297			

Significant at 0.05 level; df = 296; N = 298; Critical r-value = 0.113
a. Dependent Variable: Digital Security Management
b. Predictors: (Constant), AI Adoption

Table 4 result shows a calculated r-value of 0.812 which is greater than the critical r-value of 0.113 at 0.05 significance level, indicating a strong relationship. The R square value of 0.659 implies that 65.9% variation in digital security management is explained by AI adoption. The F-value of 621.385 with significance 0.000 confirms statistical significance. The standard error of 0.521 indicates minimal deviation. Given that the calculated value exceeds the critical value, the null hypothesis is rejected, indicating that AI adoption significantly influences digital security management in selected organisations in Rivers State.

Hypothesis Two: The null hypothesis states that there is no significant effect of AI on threat detection and response efficiency in digital security management in selected organisations in Rivers State. In order to test the hypothesis, simple linear regression analysis was performed on the data (see table 5).

Table 5: Simple Linear Regression Analysis on AI and Threat Detection/Response Efficiency

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change
1	0.846	0.716	0.714	0.497	0.716

ANOVA

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	192.384	1	192.384	778.263	0.000
Residual	73.211	296	0.247		
Total	265.595	297			

Significant at 0.05 level; df = 296; N = 298; Critical r-value = 0.113
a. Dependent Variable: Threat Detection and Response Efficiency
b. Predictors: (Constant), Artificial Intelligence

Table 5 findings reveal a calculated r-value of 0.846 which exceeds the critical r-value of 0.113, indicating a very strong positive relationship. The R square of 0.716 shows that 71.6% of variation in threat detection and response efficiency is explained by AI. The F-statistic of 778.263 with a significance level of 0.000 confirms the model's statistical validity. The

standard error of 0.497 indicates consistency in prediction. Since the calculated value is higher than the critical value, the null hypothesis is rejected, demonstrating that AI significantly improves threat detection and response efficiency in digital security management.

Hypothesis Three: The null hypothesis states that there is no significant challenges associated with the implementation of AI in digital security management in selected organisations in Rivers State. In order to test the hypothesis, simple linear regression analysis was performed on the data (see table 6).

Table 6: Simple Linear Regression Analysis on AI Implementation Challenges and Digital Security Management

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change
1	0.768	0.590	0.588	0.548	0.590

ANOVA

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	154.903	1	154.903	515.672	0.000
Residual	102.276	296	0.345		
Total	257.179	297			

Significant at 0.05 level; df = 296; N = 298; Critical r-value = 0.113
a. Dependent Variable: Digital Security Management
b. Predictors: (Constant), AI Implementation Challenges

Table 6 analysis indicates a calculated r-value of 0.768 which is greater than the critical r-value of 0.113, showing a strong relationship. The R square value of 0.590 suggests that 59.0% of variation in digital security management is explained by AI implementation challenges. The F-value of 515.672 with significance 0.000 confirms statistical significance of the model. The standard error of 0.548 reflects acceptable prediction accuracy. As the calculated value exceeds the critical threshold, the null hypothesis is rejected, indicating that challenges associated with AI implementation significantly influence digital security management in selected organisations in Rivers State.

Discussion of Findings

Findings on hypothesis one and research question one revealed a high extent of artificial intelligence adoption in digital security management, supported by descriptive results where item responses such as 132 (44.30%) and 98 (32.89%) as well as 140 (46.98%) and 90 (30.20%) indicated strong agreement, with mean values ranging from 3.11 to 3.14. The regression result further showed a calculated r-value of 0.812 exceeding the critical value of 0.113, with R^2 = 0.659, F = 621.385, and $p < 0.05$, confirming statistical significance. This aligns with Dwivedi et al. (2023), who observed that AI adoption significantly enhances organisational processes through improved system capabilities. Similarly, Haenlein and Kaplan (2021) established that AI integration improves operational efficiency and innovation. The findings corroborate Bostrom (2023), who emphasised AI as a transformative tool in organisational systems. Kshetri (2022) also reported that AI adoption strengthens cybersecurity frameworks through intelligent automation. Empirical support from Sarker (2023) demonstrated that AI adoption improves detection systems, while Vial (2022) linked digital maturity with successful AI integration. Theoretically, the outcome supports the Technology Acceptance Model, where perceived usefulness and ease of use drive adoption, reflected in the high agreement frequencies and significant regression outcome.

Findings on hypothesis two and research question two indicated that artificial intelligence significantly improves threat detection and response efficiency, as shown by descriptive responses such as 138 (46.31%) and 96 (32.21%), alongside 142 (47.65%) and 93 (31.21%), with mean values between 3.14 and 3.17. The regression analysis produced an r-value of 0.846 greater than 0.113, with $R^2 = 0.716$, $F = 778.263$, and $p < 0.05$, demonstrating a very strong relationship. These findings are consistent with Buczak and Guven (2022), who found that machine learning improves threat detection accuracy. Sommer and Paxson (2021) also highlighted AI's capability in handling complex network threats. Nguyen and Reddi (2022) established that AI reduces response time through automation, while Alshamrani et al. (2022) confirmed improved predictive capabilities in cybersecurity systems. Ahmad et al. (2021) further noted enhanced incident response performance with AI integration. Sarker (2023) reinforced that AI-driven systems improve efficiency and accuracy in threat management. The findings align with TAM, as high perceived usefulness is reflected in strong agreement levels and significant statistical outcomes.

Findings on hypothesis three and research question three showed that challenges significantly influence digital security management, with descriptive results such as 137 (45.97%) and 94 (31.54%), as well as 141 (47.32%) and 92 (30.87%), indicating strong agreement, and mean values ranging from 3.13 to 3.16. The regression analysis revealed an r-value of 0.768 exceeding 0.113, with $R^2 = 0.590$, $F = 515.672$, and $p < 0.05$, confirming statistical significance. These findings are supported by Raisch and Krakowski (2021), who identified complexity and organisational barriers as major AI implementation challenges. Adebayo and Olagunju (2022) reported infrastructural and skill limitations affecting cybersecurity practices in Nigeria. Floridi et al. (2021) highlighted ethical and governance concerns associated with AI deployment. Tarafdar et al. (2021) emphasised resistance to technological change as a barrier to adoption. Peltier (2022) noted that inadequate policy frameworks hinder effective security management, while Kshetri (2022) identified cost and expertise constraints as critical challenges. The results align with TAM, where perceived ease of use influences adoption, as challenges negatively affect user acceptance and system utilisation.

Conclusion and Recommendations

The study examined the effect of artificial intelligence (AI) on digital security management in selected organisations in Rivers State, focusing on AI adoption, its influence on threat detection and response efficiency, and the challenges associated with implementation. The findings revealed that AI adoption in digital security management is significant, with respondents indicating strong agreement across items measuring the use of AI tools for monitoring network activities, automated processes, and integration into organisational security frameworks. Regression analysis confirmed that AI adoption significantly explains variations in digital security management, highlighting its transformative role in enhancing operational efficiency and system reliability. Similarly, the study established that AI significantly improves threat detection and response efficiency. Descriptive statistics indicated that a majority of respondents strongly agreed that AI enhances speed, accuracy, and overall security response. Regression outcomes further demonstrated a strong positive relationship between AI and threat management, confirming theoretical expectations under the Technology Acceptance Model, where perceived usefulness drives adoption and effectiveness. Additionally, the study revealed that challenges such as high implementation costs, skill shortages, system complexity, data privacy concerns, and resistance to change significantly influence digital security management. While AI adoption improves efficiency, these challenges must be addressed to ensure sustainable integration. Hence, the study provides empirical evidence that AI adoption is central to enhancing digital security management, improving organisational capabilities in threat detection and response, and simultaneously facing critical challenges that require

strategic mitigation. The results contribute to existing literature on AI in cybersecurity and support theoretical models emphasising the relationship between technology adoption and organisational performance.

Recommendations

Based on the findings, the following recommendations are proposed:

1. Organisations in Rivers State are encouraged to prioritise investment in AI-enabled security systems and integrate them into core operational processes to enhance monitoring, threat detection, and response efficiency.

2. Human resource and training departments should develop structured training programmes to equip IT and security personnel with advanced skills for AI system operation and maintenance, addressing the skill shortage identified.

3. Government agencies and regulatory authorities should provide clear guidelines and frameworks for AI adoption, addressing ethical, privacy, and compliance concerns, ensuring safe and standardised implementation across industries.

4. IT departments should adopt gradual implementation strategies that consider cost-effective AI solutions, simplify system complexity, and address organisational resistance, ensuring sustainable AI integration into digital security management.

References

Adebayo, O. S., & Olagunju, A. M. (2022). Cybersecurity challenges and organisational resilience in Nigeria. *Journal of Information Security and Applications*, 64, 103–115.

Ahmad, A., Maynard, S. B., & Shanks, G. (2021). A case analysis of information systems and security incident responses. *International Journal of Information Management*, 60, 102347.

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2022). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials*, 24(1), 185–216.

Bostrom, N. (2023). *Artificial intelligence and the future of humanity*. Oxford University Press.

Buczak, A. L., & Guven, E. (2022). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials*, 24(2), 1153–1176.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., & Al-Debei, M. M. (2023). Artificial intelligence adoption in organisations: A review and future research agenda. *International Journal of Information Management*, 71, 102642.

Floridi, L., Cowls, J., King, T., & Taddeo, M. (2021). How to design AI for social good: Seven essential factors. *Science and Engineering Ethics*, 27(3), 1–15.

Goodfellow, I., Bengio, Y., & Courville, A. (2022). *Deep learning*. MIT Press.

Haenlein, M., & Kaplan, A. (2021). Artificial intelligence and robotics: Shaping the future of business and society. *Business Horizons*, 64(3), 365–378.

Kshetri, N. (2022). Cybersecurity management using artificial intelligence: Opportunities and challenges. *IT Professional*, 24(2), 12–18.

Nguyen, D., & Reddi, V. J. (2022). Deep reinforcement learning for cyber security. *IEEE Security & Privacy*, 20(1), 10–18.

Peltier, T. R. (2022). *Information security policies, procedures, and standards*. Auerbach Publications.

Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation–augmentation paradox. *Academy of Management Review*, 46(1), 192–210.

Sarker, I. H. (2023). AI-based cybersecurity: A comprehensive survey. *Journal of Big Data*, 10(1), 1–45.

Sommer, R., & Paxson, V. (2021). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–316.

Taddeo, M., & Floridi, L. (2021). How AI can be a force for good. *Science*, 361(6404), 751–752.

Tarafdar, M., Beath, C. M., & Ross, J. W. (2021). Using AI to enhance business operations. *MIT Sloan Management Review*, 62(4), 37–44.

Vial, G. (2022). Understanding digital transformation: A review and research agenda. *Journal of Strategic Information Systems*, 31(2), 101–123.

Von Solms, R., & Van Niekerk, J. (2021). From information security to cybersecurity. *Computers & Security*, 38, 97–102.