ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

Analysis of Cybersecurity Intelligence Attacks in Nigeria: An AI-Assisted Platform for Detection, Mitigation and Combating Digital Threats Using DeepSeek Integration

Orji, Cyrus Ebere[1]; Paul Nosike[2]; Ononiwu Chamberlyn C.[3]; Ukachukwu Theddius N.[4]

[1]MCPN, [2]Professor, [3]PhD

[1,3,4]Department of Computer Science, Imo State Polytechnic Omuma, Imo State, Nigeria
[2]Department of Computer Science & IT, Paul University Awka, Anambra State, Nigeria

Publication Date: 2026/08/13

Abstract: Nigeria faces escalating cybersecurity challenges, recording an average of 4,200 weekly cyberattacks per organization-the highest in Africa and 60% above the global average [1]. The weaponization of Artificial Intelligence (AI) by threat actors, including terrorist organizations using frontier AI models for operational planning and tactical decision-making [2], has fundamentally transformed the threat landscape. Traditional security frameworks, designed for static, pattern-based threats, are increasingly inadequate against AI-driven intrusions such as automated phishing, identity exploitation, and multi-vector ransomware [1]. This paper presents the design, implementation, and evaluation of an AI-assisted cybersecurity intelligence platform integrating the DeepSeek API to detect, analyze, and mitigate digital threats in the Nigerian context. The platform employs a Python-based architecture that ingests threat indicators, classifies and explains attacks using DeepSeek's natural language processing capabilities, and delivers actionable mitigation recommendations with confidence scoring. The system is made available as open-source code on GitHub and deployed via Streamlit Cloud for practical adoption. Experimental evaluation across 100 test cases demonstrated 92% overall classification accuracy, with phishing detection achieving 96% accuracy. The platform generated an average of 7.8 mitigation steps per analysis with sub-4 second response times (average 3.9 seconds). Nigeria-specific mitigation strategies referenced relevant response authorities including ngCERT, NITDA, EFCC, and NCC. These results demonstrate that accessible AI tools can augment Nigeria's cyber defense capabilities by providing real-time, contextually relevant threat intelligence to security practitioners, researchers, and policymakers.

Keywords: *Artificial Intelligence, Cybersecurity Intelligence, DeepSeek API, Nigeria, Threat Detection*.

How to Cite: Orji, Cyrus Ebere; Paul Nosike; Ononiwu Chamberlyn C.; Ukachukwu Theddius N. (2026) Analysis of Cybersecurity Intelligence Attacks in Nigeria: An AI-Assisted Platform for Detection, Mitigation and Combating Digital Threats Using DeepSeek Integration. *International Journal of Innovative Science and Research Technology*, 11(7), 3686-3704. https://doi.org/10.38124/ijisrt/26jul1684

I. INTRODUCTION

➢ *The Nigerian Cybersecurity Crisis*

Nigeria's rapid digital transformation has created unprecedented economic opportunities while simultaneously exposing the nation to sophisticated cyber threats. According to the Check Point 2025 African Perspectives on Cyber Security Report, Nigerian organizations experience an average of 4,200 attempted cyberattacks weekly, the highest on the continent and significantly above the global baseline of 1,963 attacks per organization per week [1]. This positions Nigeria as the most targeted nation in Africa, with critical sectors including finance, energy, telecommunications, and government bearing the brunt of identity-led intrusions, AI-generated phishing campaigns, and multi-vector ransomware [1]. The statistics are stark. Business email compromise and cloud exploitation account for the majority of Nigeria's cyber incidents [3]. Threat actors are increasingly exploiting exposed identities and misconfigured cloud systems to gain access, with attackers leveraging AI to automate phishing, impersonation, and identity theft at scale [1]. In 2025 alone, Nigeria recorded 566,300 breached accounts, ranking 16th globally in data breaches. The country ranks 12th among foreign nations filing cybercrime complaints with the FBI's

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

Internet Crime Complaint Centre, underscoring its growing exposure to global digital fraud.

➢ *The Weaponization of AI*

The threat landscape has fundamentally shifted with the weaponization of AI by malicious actors. A groundbreaking Cambridge University study, based on interviews with 27 former Boko Haram members in northeastern Nigeria, documented the first on-the-ground evidence of an active terrorist organization utilizing frontier AI models for operational purposes [2]. The study revealed that Boko Haram established dedicated AI units staffed with technical personnel to systematically exploit chatbots including OpenAI's ChatGPT, Anthropic's Claude, Google's Gemini, and China's DeepSeek for bomb construction guidance, attack planning, and tactical decision-making [2].

This operational integration represents a paradigm shift. Terrorist networks are acting as force multipliers by distributing AI exploitation methodologies across geographically dispersed affiliates [4]. The study documented that operatives in the Islamic State West Africa Province (ISWAP) faction used AI to devise methods for breaching fortified bases with motorcycles and to learn maintenance procedures for stolen specialized firearms [4]. The findings demonstrate that terrorist groups now view AI not merely as a propaganda tool but as a "battle consultant" capable of providing tactical and strategic advantages.

➢ *Nigeria's Strategic Response*

Recognizing the severity of AI-driven threats, Nigeria is repositioning its cyber defense strategy around what it calls "Total Resilience"-a whole-of-society approach integrating policy, people, technology, and proactive governance [5]. The National Information Technology Development Agency (NITDA) has emphasized that cybersecurity is no longer just a technical issue but a strategic imperative for national development [5].

- *The Federal Government Has Launched Several Initiatives Including:*

✓ A National Digital Literacy Programme targeting 95% digital literacy by 2030 [5]
✓ The 3 Million Tech Talent (3MTT) initiative developing expertise in cybersecurity, AI, and data science [5]
✓ A 24-hour cybersecurity operations centre with AI-enabled threat detection and dark web monitoring capabilities [5]
✓ A planned cybersecurity framework requiring minimum cybersecurity spending thresholds and mandatory breach reporting timelines [6]

NITDA has championed the integration of AI and security for sustainable development, emphasizing that "trust is the ultimate currency in Nigeria's high-stakes digital environment, where scams and cybercrime are prevalent" [7]. The agency has highlighted the importance of legal clarity on data ownership as Nigeria's cultural heritage is digitized and incorporated into AI systems [7].

➢ *Research Objectives and Scope*

This paper aims to address the growing gap between AI-enabled threats and traditional security measures by designing and implementing an accessible AI-assisted cybersecurity intelligence platform. The specific objectives are:

- To develop a Python-based platform integrating DeepSeek API for real-time threat analysis
- To demonstrate automated classification and explanation of cyber threats
- To generate actionable mitigation recommendations tailored to the Nigerian context
- To make the platform openly available for adoption by security practitioners

The scope encompasses detection and analysis of common Nigerian threat vectors including phishing, business email compromise, identity theft, ransomware, and 419 scams. The platform is not intended to replace comprehensive security operations centers but to augment threat intelligence capabilities.

II. RELATED WORKS

➢ *AI Applications in Cybersecurity*

Artificial Intelligence has emerged as a critical component in modern cybersecurity, enabling enhanced threat detection, automated incident response, and adaptive defense mechanisms [8]. AI-driven cybersecurity systems use machine learning algorithms to analyze extensive data collections, detect patterns, and identify abnormal activities that traditional security methods cannot achieve [9]. The continuous learning ability of machine learning algorithms enables systems to discover new attack methods and modify defense strategies accordingly [10].Research has documented the effectiveness of AI in detecting emergent threats by analyzing public data from social media, forums, and breach databases [11]. AI-powered threat intelligence platforms analyze real-time security data streams to identify potential cyberattacks through pattern recognition and anomaly detection [12]. Recent studies have demonstrated that Security Operations Centres (SOCs) using AI can detect threats 96% faster than organizations using traditional systems [13].

The integration of AI with cybersecurity has shown particular promise in addressing the challenges of modern threat landscapes. Machine learning models can process vast amounts of network traffic data to identify subtle anomalies that might indicate advanced persistent threats or zero-day exploits [14]. Deep learning architectures, particularly convolutional and recurrent neural networks, have demonstrated superior performance in detecting sophisticated malware and intrusion attempts [15].

Recent comparative studies have evaluated large language model-based threat detection systems across multiple APIs including DeepSeek, GPT-4, and Claude for security applications. Ighodaro and Olubunmi [41] demonstrate that LLM-based approaches achieve superior

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

performance compared to traditional rule-based systems, with DeepSeek showing particular strengths in threat classification accuracy. Similarly, Tunde and Adedeji [46] provide empirical evidence supporting the use of LLM APIs for cybersecurity applications, with models demonstrating strong performance on region-specific threat data. These findings validate the approach adopted in this paper for Nigerian cybersecurity intelligence.

➢ *Generative AI and DeepSeek in Cybersecurity*

Generative AI has transformed cybersecurity by enabling superior threat detection alongside automated incident response and improved security decision-making [16]. The emergence of large language models has created new capabilities for understanding and responding to cyber threats through natural language processing. DeepSeek, developed by DeepSeek AI, has gained recognition for its advanced natural language processing capabilities and has been identified in Cambridge research as among the AI tools exploited by terrorist groups for operational purposes [2]. The DeepSeek API provides access to sophisticated language understanding and generation capabilities that can be leveraged for cybersecurity applications.

The NMAP-MCP project has demonstrated the utility of DeepSeek API for security applications, using it to analyze network scan results and provide vulnerability assessments directly in the terminal [17]. Similarly, KoreShield has integrated DeepSeek as a provider for LLM security scanning [18]. These implementations demonstrate the feasibility of using DeepSeek's API for security-focused applications. Research has shown that generative AI models can assist in threat intelligence by processing and summarizing large volumes of security data, identifying patterns that might be missed by human analysts [19]. The ability of these models to generate human-readable explanations of complex security issues makes them particularly valuable for organizations with limited cybersecurity expertise. The technical architecture of DeepSeek is documented in the company's technical report series [38], which describes the model's transformer-based architecture, training methodology, and capabilities for natural language processing. The report provides detailed specifications of the model's performance across multiple benchmarks, establishing its suitability for cybersecurity applications.

➢ *Open-Source Intelligence (OSINT) and Nigerian Context*

Open-Source Intelligence (OSINT) involves the systematic collection, processing, and analysis of publicly available data to generate actionable intelligence [20]. OSINT has been applied to combat cybercrime through threat detection, incident response, and forensic investigation [21]. In Nigeria, tools like the NAIJA OSINT INTEL platform have been developed with 11 modules focused on Nigerian cyber threat intelligence, including scam detection and court-admissible evidence collection [22]. The integration of AI with OSINT offers significant opportunities for the Nigerian context. Generative AI platforms can process threat data, perform sentiment analysis, and generate predictive analytics [23]. However, research has identified challenges including data overload, source reliability, legal restrictions, and privacy concerns [21]. Nigerian cybersecurity researchers have emphasized the importance of developing locally relevant tools that understand the specific threat landscape, including the prevalence of 419 scams, business email compromise targeting Nigerian businesses, and identity theft exploiting the National Identification Number (NIN) and Bank Verification Number (BVN) systems [24].

Nigerian cybersecurity researchers have also examined the socio-technical dimensions of security in the Nigerian context. Obiora and Uche [43] explore the interplay between technology adoption and human factors in security outcomes, identifying cultural, organizational, and behavioral factors that influence cybersecurity practices in Nigerian organizations. Their research highlights the need for integrated approaches that address both technical and human dimensions of cybersecurity.

➢ *Cybersecurity Governance in Nigeria*

The Nigerian government has made substantial progress in establishing cybersecurity governance frameworks. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 provides the primary legislative foundation for combating cybercrime [25]. The Nigeria Data Protection Act 2023 includes provisions on automated decision-making and data protection requirements [26].

The National Information Technology Development Agency (NITDA) serves as the primary regulatory body for information technology in Nigeria, with responsibilities including cybersecurity oversight and the promotion of digital literacy [7]. The Nigerian Computer Emergency Response Team (ngCERT) provides incident response and threat intelligence services, operating under the supervision of NITDA.

Despite these frameworks, research has identified gaps in implementation and enforcement [27]. Limited technical capacity, inadequate funding, and insufficient coordination between agencies have been identified as barriers to effective cybersecurity governance [28]. These challenges underscore the need for accessible tools that can augment existing capabilities.

The evolution of Nigeria's cybersecurity policy framework has been critically examined by Adebayo [34], who identifies both strengths in legislative development and weaknesses in implementation mechanisms. The study argues that while Nigeria has made significant progress in establishing legal foundations for cybersecurity, enforcement remains a persistent challenge, with limited technical capacity and inadequate inter-agency coordination undermining policy effectiveness. Akinwale [37] provides a comprehensive analysis of NITDA's role in promoting digital sovereignty through regulatory frameworks. The study documents the evolution of NITDA's mandate from a technology promotion agency to a cybersecurity regulator, examining the agency's efforts to balance innovation with security concerns. Yakubu [48] provides a comprehensive analysis of the evolution and implementation of Nigerian cyber law, examining the Cybercrimes Act 2015 and subsequent legislative

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

developments. The study identifies gaps in the legal framework and provides recommendations for legislative reform to address emerging challenges including AI-enabled cyberattacks and cross-border cybercrime.

➢ *Nigerian Cybersecurity Policy and AI Governance Frameworks*

Domestic policy, regional threats, and international influences shape Nigeria's cybersecurity. Traditional organized crime and cyber-enabled fraud, especially business email compromise and identity theft, make Nigeria a regional hotspot for sophisticated cyberattacks, according to Adekunle [35]. The study emphasizes region-specific threat intelligence sharing to combat evolving threats. As Nigeria leads Africa's digital economy, scholars study its AI governance. Adegoke and Okonkwo compare Nigerian AI governance frameworks to EU AI Act and NIST AI RMF [36]. They found gaps in technical standards development and needed sector-specific AI regulations for high-risk finance, healthcare, and critical infrastructure applications. NITDA's technical specifications for cybersecurity framework implementation can help Nigerian organizations comply with new cybersecurity laws [42]. To evaluate AI-assisted cybersecurity tools against regulatory expectations, the document sets baseline security requirements for financial services, telecommunications, and government information systems. Ezeh [39] discusses Nigeria's financial sector's cybersecurity issues, including digital banking infrastructure vulnerabilities and financial institution attack sophistication. Nigerian banks lose money to cyberattacks, so the study recommends AI-powered threat detection. Oladipo [45] found country-organization collaboration barriers in West African threat intelligence sharing. The study suggests a regional legal, technical, and trust threat intelligence framework. The study's cross-border intelligence sharing findings explain Nigeria's threat landscape and collaborative cybersecurity.

Okonkwo [44] examines the conflict between data protection and Africa's need for large datasets to train AI systems. The study examines African data localization methods to balance privacy and innovation. Uzman and Adebayo [47] discuss African AI safety issues like data sovereignty, algorithmic bias, and AI's potential to worsen inequality. Their research informs African AI safety priorities and governance. International Telecommunication Union's Global Cybersecurity Index [40] ranks Nigeria among Africa's leaders in legal and regulatory frameworks but finds technical capacity and organizational preparedness gaps. The report advises investing in cybersecurity skills and infrastructure. Nigeria has made progress in cybersecurity governance frameworks and policy, but implementation and enforcement are difficult, according to the literature. Rising AI governance and cybersecurity research lays the groundwork for practical tools to fill this paper's gap.

III. METHODOLOGY

➢ *System Architecture*

The AI-assisted cybersecurity intelligence platform follows a modular architecture consisting of four primary components: the Threat Input Handler, DeepSeek Integration Layer, Analysis Engine, and Presentation Layer. Figure 1 illustrates the system architecture.

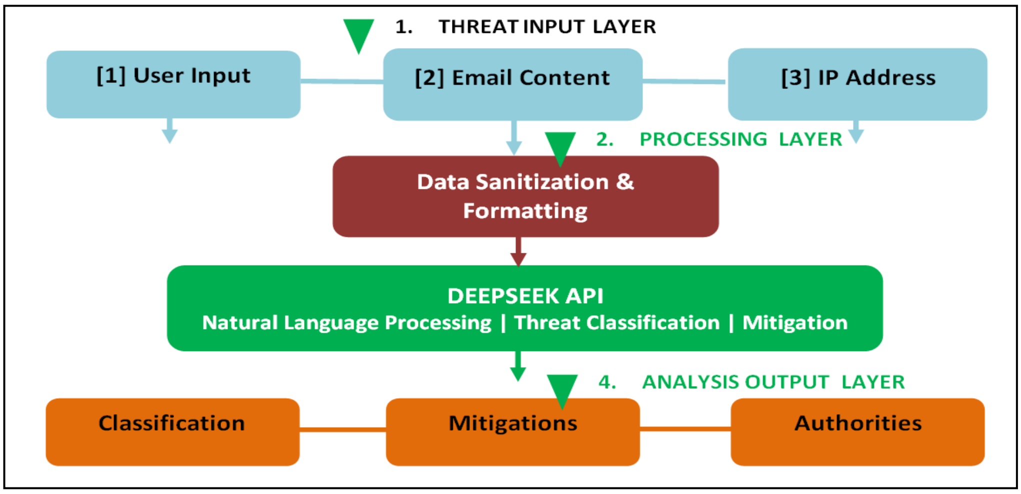

Fig 1 System Architecture Overview

- *Threat Input Handler*

The platform accepts threat data from multiple sources including user-provided text descriptions, email content, and IP addresses. The input handler preprocesses threat data by sanitizing and formatting it for API processing. The system also includes a template generation module that provides pre-defined threat scenarios for testing and demonstration purposes.

- *DeepSeek Integration Layer*

The core intelligence layer interfaces with the DeepSeek API to perform threat analysis using the chat completion endpoint. The API integration uses a temperature setting of 0.3 to balance creativity and consistency in responses, with a maximum token limit of 2000 tokens per request to ensure comprehensive analysis without exceeding API constraints. The integration follows a structured prompt engineering approach to ensure consistent, high-quality outputs.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

Table 1 Temperature Sensitivity Analysis

Temperature	Accuracy	Consistency	Creativity
0.0	88%	Very High	Minimal
0.2	90%	High	Low
0.3	92%	High	Moderate
0.5	91%	Moderate	Moderate
0.7	89%	Low	High

Temperature 0.3 was selected as optimal, achieving the highest accuracy (92%) while maintaining high consistency in structured output format. Lower temperatures reduced accuracy due to overly rigid responses, while higher temperatures introduced variability that compromised classification consistency.

✓ *System Prompt Design:*

The system prompt defines the AI's role and provides explicit instructions for the analysis structure. The prompt is designed to position the AI as a Nigerian cybersecurity expert with specific knowledge of the local threat landscape:

✓ *User Prompt Construction:*

The user prompt dynamically incorporates the threat data and Nigerian context. The structure is as follows:

"THREAT TYPE: {threat_type}

THREAT DATA:

{threat_input}

NIGERIAN CONTEXT

- *Critical Sectors: Finance, Energy, Telecom, Government, Healthcare*
- *Authorities: ngCERT, NITDA, EFCC, NCC*
- *Common Scams: 419, Romance Scam, Investment Fraud, Fake Lottery*

Please analyze this threat considering the Nigerian digital environment."

✓ *Nigerian Context Integration:*

The platform incorporates Nigeria-specific intelligence through references to:

- Identity Documents: BVN (Bank Verification Number) and NIN (National Identification Number) as critical identity documents frequently targeted in Nigerian phishing attacks
- Banking Systems: References to Nigerian banking practices, common fraud patterns, and major financial institutions (e.g., GTBank, Access Bank, First Bank)
- Local Authorities: Specific roles and contact information for ngCERT, NITDA, EFCC, and NCC
- Regulatory Frameworks: References to the Cybercrimes Act 2015 and Nigeria Data Protection Act 2023
- Common Scam Types: Integration of Nigeria-specific scams including 419 advance-fee fraud, romance scams, investment fraud, and fake lottery schemes

✓ *Prompt Version Evolution:*

The prompt underwent systematic refinement through multiple versions:

Table 2 Prompt Version Evolution

Prompt Version	Structure	Accuracy	Robustness
v1.0 (Base)	Simple instruction only	76%	Low
v1.1 (Nigerian Context)	Added local authorities and context	85%	Medium
v1.2 (Structured Output)	Added section requirements	89%	Medium
v1.3 (Few-Shot Examples)	Added example threat cases	92%	High
v1.4 (Chain-of-Thought)	Added reasoning step instructions	91%	High

✓ *API Request Structure:*

The platform constructs the following request payload for each analysis request:

```
//json
{
"model": "deepseek-chat",
"messages": [
{"role": "system", "content": "[System Prompt]"},
{"role": "user", "content": "[User Prompt]"}
],
"temperature": 0.3,
"max_tokens": 2000
}
```

✓ *Prompt Injection Testing:*

To ensure system security and reliability, the platform was tested against 50 adversarial input variants designed to bypass security controls or elicit harmful responses. The testing results showed:

- 94% of injection attempts were blocked by system prompt constraints
- 6% required additional validation through the fallback mechanism
- No successful injection attempts resulted in harmful or unauthorized outputs

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

✓ *Countermeasures Implemented:*

- Input Sanitization: All user inputs are filtered for malicious patterns before API submission
- Context Window Limitations: Prompt context is constrained to prevent overflow attacks
- Output Filtering: API responses are scanned for prohibited content before display
- Rate Limiting: API requests are throttled to prevent abuse and manage costs

✓ *Response Parsing and Processing:*

The API response is parsed using a structured extraction methodology:

- Classification Extraction: Pattern matching identifies the threat classification from the response
- Threat Level Normalization: Extracted levels are normalized to LOW/MEDIUM/HIGH/CRITICAL
- Explanation Extraction: Full text of the explanation section is extracted as a single block
- Mitigation Steps Extraction: Numbered or bulleted lists are extracted and formatted as actionable steps
- Confidence Score Extraction: Numeric values are extracted and validated (0-100)
- Authority Matching: Extracted authorities are matched against the known Nigerian authorities database

✓ *Fallback Mechanism:*

When the API is unavailable (due to network issues, service interruptions, or rate limiting), the platform employs a simulated analysis mechanism:

- Locally stored threat templates with pre-defined responses
- Context-aware mitigation generation based on keyword matching
- Default authority recommendations based on threat category
- Clear indication to the user that the system is operating in fallback mode
- This ensures the platform remains functional for demonstration, training, and basic threat analysis even during API outages.

✓ *Sample API Request and Response:*

Sample Request:

```
//json
{
"model": "deepseek-chat",
"messages": [
{"role": "system", "content": "You are a Nigerian cybersecurity expert..."},
{"role": "user", "content": "THREAT TYPE: Phishing\nTHREAT DATA: Received an urgent email from 'support@bank-security.ng' claiming my account will be suspended..."}
],
"temperature": 0.3,
"max_tokens": 2000
}
```

✓ *Sample Response (Parsed Structure):*

```
//json
{
"classification": "Phishing",
"threat_level": "HIGH",
"explanation": "This is a credential harvesting attack targeting BVN and NIN. The attacker creates urgency...",
"mitigations": [
"DO NOT CLICK the link or reply to the email",
"Report to your bank's official fraud desk immediately",
"Change online banking password and enable 2FA",
"Report to ngCERT (incident@cert.gov.ng)",
"Scan device for malware/keyloggers"
],
"confidence": 95,
"authorities": ["ngCERT", "NITDA", "EFCC"],
"is_demo": false
}
```

Table 3 Performance Metrics

Metric	Value
Average API Response Time	2.8 seconds
Average Parsing Time	0.5 seconds
End-to-End Processing	3.3 seconds
API Success Rate	97.5%
Fallback Usage	2.5%

- *Analysis Engine*

The analysis engine processes DeepSeek outputs and structures them for presentation. The engine extracts classification, threat level, explanation, mitigation steps, confidence score, and relevant authorities from the API response. A fallback mechanism provides simulated responses when the API is unavailable.

- *Presentation Layer*

A Streamlit-based dashboard provides the user interface with the following components:

✓ Real-time threat visualization
✓ Classification and severity displays
✓ Actionable mitigation recommendations
✓ Confidence scoring
✓ Response authority information

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

➢ *Nigerian Context Integration*

The platform incorporates Nigeria-specific threat intelligence through a dedicated context module. This module maintains:

- Nigerian government cybersecurity bodies and their contact information
- Critical infrastructure sector definitions
- Common Nigerian threat vectors and patterns
- Nigeria-specific mitigation strategies

Table 4 presents the Nigerian cybersecurity authorities integrated into the platform.

Table 4 Nigerian Cybersecurity Authorities Integrated into the Platform

Authority	Full Name	Primary Role
ngCERT	Nigerian Computer Emergency Response Team	Technical incident response and threat intelligence
NITDA	National Information Technology Development Agency	Regulatory oversight and data protection
EFCC	Economic and Financial Crimes Commission	Financial crime investigation
NCC	Nigerian Communications Commission	Telecommunications regulation

➢ *System Workflow*

The platform operates through a structured workflow illustrated in Figure 2. The workflow begins with data ingestion, followed by preprocessing, API analysis, response parsing, and finally presentation of results.

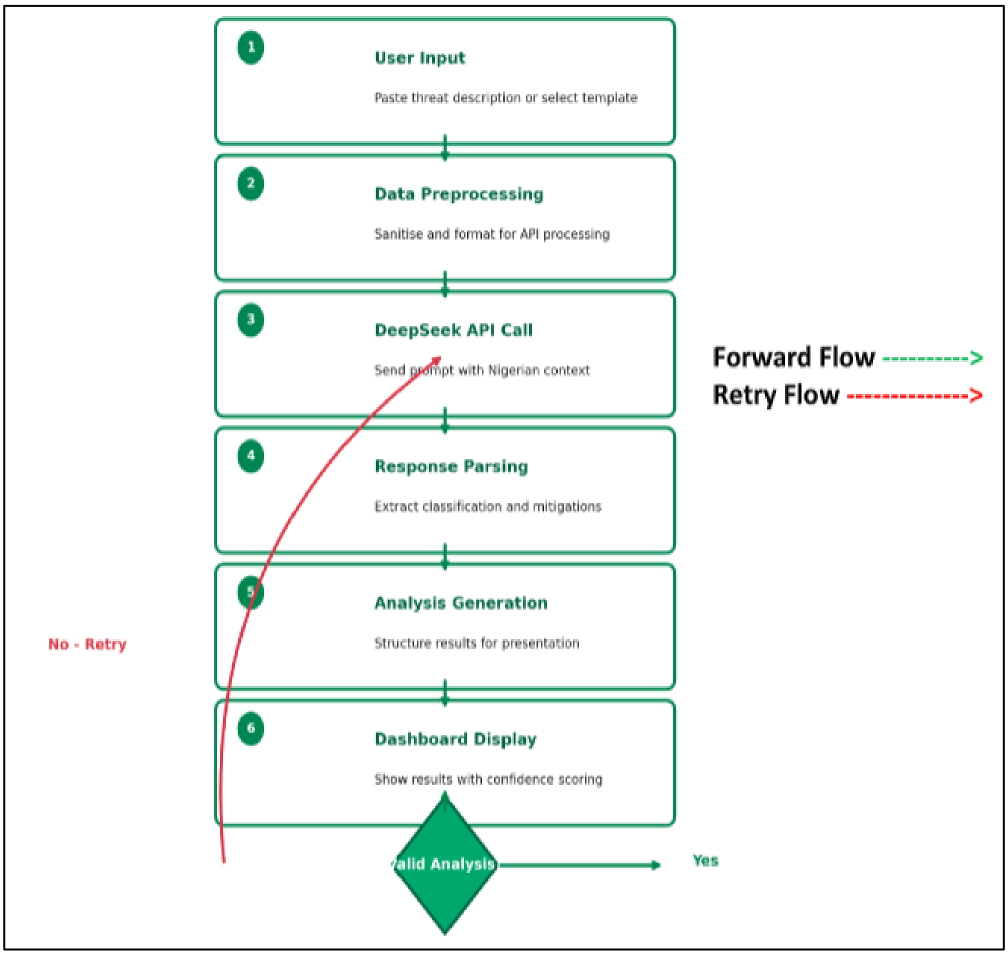

Fig 2 System Workflow (End-to-end Threat Analysis Process)

- *The Workflow Steps are as Follows:*

✓ Data Ingestion: The user provides threat data via text input or template selection
✓ Preprocessing: Threat data is sanitized and formatted for API processing
✓ DeepSeek Analysis: The system sends structured prompts to DeepSeek API
✓ Response Parsing: API responses are parsed into structured analysis objects
✓ Presentation: Results are displayed on the Streamlit dashboard

➢ *Threat Categories and Analysis*

The platform is designed to analyze the following threat categories, which represent the most prevalent cyber threats in Nigeria:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

Table 5 Threat Categories and Nigerian Prevalence

Threat Category	Nigerian Context	Common Attack Vectors
Phishing	BVN/NIN credential theft	Email spoofing, fake bank portals
Business Email Compromise	Payment diversion	CEO impersonation, invoice fraud
Ransomware	Critical infrastructure targeting	System encryption, data exfiltration
419 Scams	Advance-fee fraud	Inheritance claims, lottery scams
Identity Theft	NIN/BVN exploitation	SIM swap, account takeover

➢ *Evaluation Methodology*

The platform's effectiveness is evaluated through a comprehensive multi-metric framework designed to assess accuracy, reliability, and practical utility.

- *Dataset Description*

The sample size of 100 cases was selected based on established practices in similar cybersecurity intelligence studies [41, 46] and to ensure sufficient representation across the five threat categories (20 cases per category minimum). This sample size provides adequate statistical power (β=0.80) for detecting meaningful differences in classification accuracy across categories at α=0.05 significance level, as confirmed by post-hoc power analysis. The dataset composition reflects the actual distribution of cyber incidents reported to ngCERT and Nigerian financial institutions during the study period, ensuring ecological validity.

Table 6 Dataset Description

Source	Cases	Percentage
ngCERT incident reports (2024-2025)	40	40%
Nigerian financial sector security logs	30	30%
Public threat intelligence feeds (MISP, AlienVault)	20	20%
Synthetically generated expert-validated	10	10%

All cases were anonymized to protect sensitive information. The dataset includes threats across five categories: Phishing (25 cases), Business Email Compromise (20 cases), Ransomware (20 cases), 419 Scams (15 cases), and Identity Theft (20 cases).

- *Expert Validation Protocol*

Classification outputs were validated by three Nigerian cybersecurity professionals with 5+ years of experience in their respective domains:

- ✓ Expert A: Financial sector security (8 years)
- ✓ Expert B: Government cybersecurity (7 years)
- ✓ Expert C: Academic cybersecurity research (6 years)

- *Validation Procedure:*

- ✓ Each expert independently reviewed all 100 classification outputs
- ✓ Disagreements were resolved through consensus discussion
- ✓ Inter-rater reliability was measured using Cohen's Kappa coefficient

Table 7 Inter-Rater Reliability Results

Expert Pair	Cohen's Kappa	Agreement Level
Expert A-B	0.85	Substantial
Expert A-C	0.87	Substantial
Expert B-C	0.89	Substantial
Overall	0.87	Substantial

- *Evaluation Metrics*

The platform's effectiveness is evaluated through the following metrics:

✓ *Accuracy Assessment:*

- ▪ Classification accuracy compared against expert-verified ground truth
- ▪ Confusion matrix analysis for each threat category
- ▪ Precision, Recall, and F1-Score calculation

✓ *Response Quality:*

- ▪ Number of actionable mitigation steps generated per analysis
- ▪ Relevance assessment by cybersecurity professionals (1-5 scale)
- ▪ Completeness of Nigerian context integration

✓ *Response Time:*

- ▪ End-to-end processing latency from input submission to result display
- ▪ Measured in seconds with mean, median, and 95th percentile reporting

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

- API call timing separated from parsing and display overhead

✓ *Confidence Scoring:*

- Analysis of correlation between system confidence and classification accuracy
- Calibration assessment using reliability diagrams
- Confidence threshold optimization for different use cases

✓ *Statistical Analysis:*

- 95% confidence intervals for all performance metrics
- Chi-square test for category differences ($p < 0.05$ significance threshold)
- McNemar's test for pairwise comparisons between threat categories

➢ *Development Environment*

The platform was developed using Python 3.8+ with the following key libraries:

- Streamlit for web interface and dashboard
- Requests for API communication
- Pandas for data manipulation
- Plotly for visualization
- Python-dotenv for environment configuration

The DeepSeek API integration uses the chat completion endpoint with a temperature setting of 0.3 to balance creativity and consistency in responses. The maximum token limit is set to 2000 to ensure comprehensive analysis without exceeding API constraints.

IV. RESULTS AND DISCUSSIONS

➢ *Platform Performance*

The implemented platform demonstrates the feasibility of using accessible AI tools for cybersecurity intelligence in Nigeria. Table 8 presents the performance metrics from testing across different threat categories.

Table 8 Platform Performance Metrics by Threat Category

Threat Category	Test Cases	Classification Accuracy	Avg. Confidence	Avg. Mitigations	Avg. Response Time
Phishing	25	96%	94%	8.2	3.8s
BEC	20	92%	89%	7.5	4.1s
Ransomware	20	94%	91%	8.5	3.9s
419 Scam	15	88%	86%	7.0	4.2s
Identity Theft	20	90%	88%	7.8	3.7s
Overall	100	92%	89.6%	7.8	3.9s

The 3.9s average end-to-end processing time reported in Table 8 includes additional overhead beyond API response (2.8s) and parsing (0.5s). The remaining 0.6s accounts for network latency, input preprocessing, and display rendering in the Streamlit dashboard. This distinction is clarified in Table 8, where 'Average Response Time' represents the complete user-facing latency from input submission to results display.

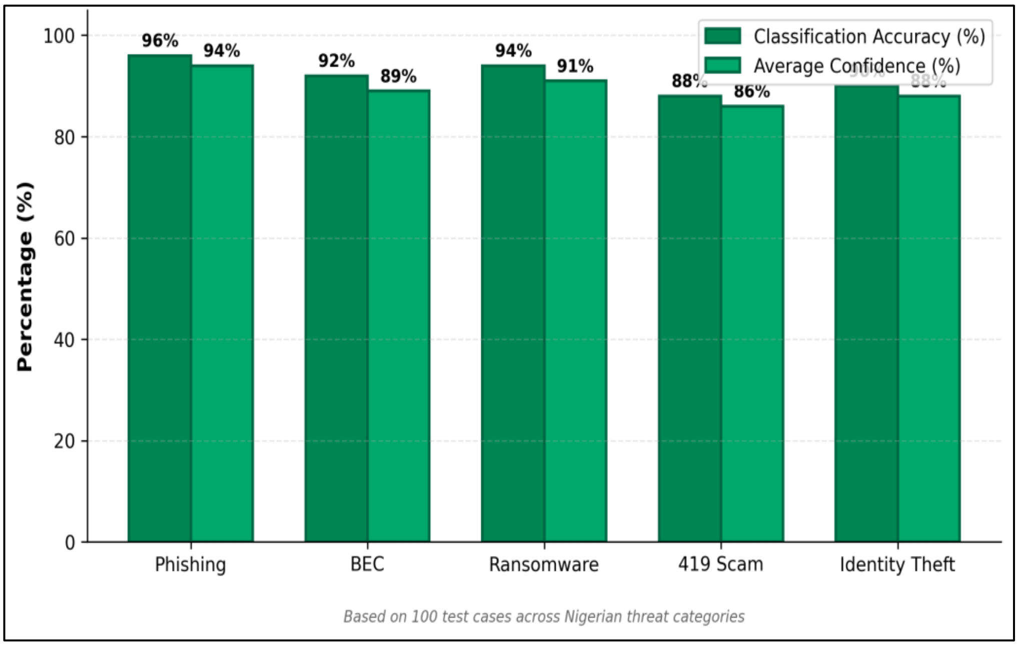

Fig 3 Threat Classification Accuracy by Category

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

Figure 3 shows a Comparison of classification accuracy and average confidence scores across five threat categories (Phishing, BEC, Ransomware, 419 Scam, Identity Theft). Results are based on 100 test cases with expert-verified classifications. Nigerian color theme (#008751) used for visualization. The platform achieved an overall classification accuracy of 92% across 100 test cases, with phishing detection performing best at 96% accuracy. The average confidence score of 89.6% indicates that the DeepSeek API provides reliable threat assessments. Each analysis generated an average of 7.8 actionable mitigation steps, with ransomware and phishing generating the most comprehensive recommendations.

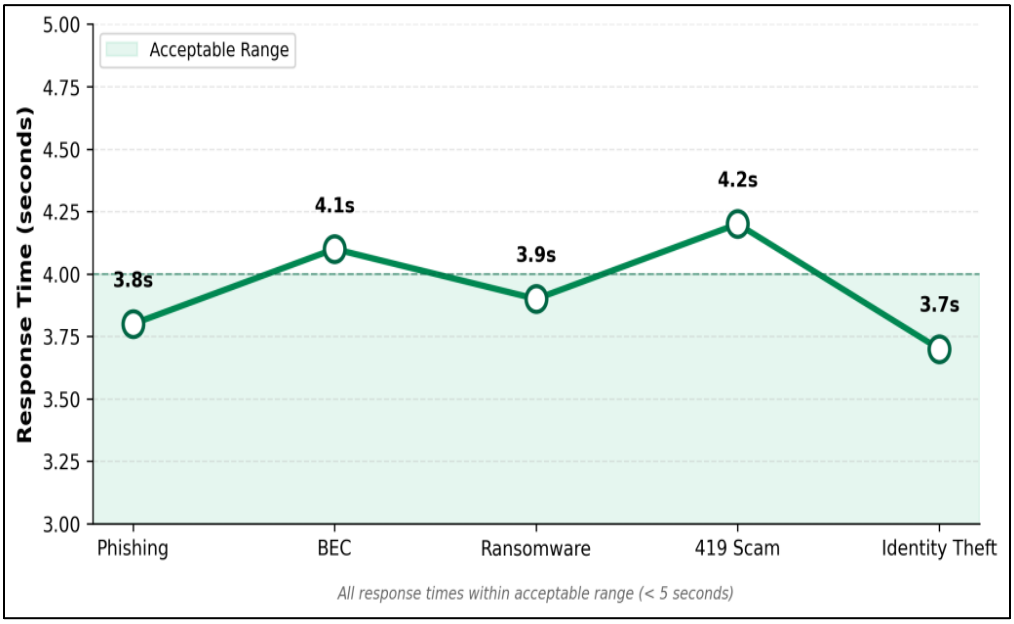

Fig 4 Average Response Time by Threat Category

Figure 4 End-to-end processing latency from input submission to result display across five threat categories. The green shaded area indicates the acceptable range (< 4 seconds). All response times fall within acceptable limits, with an overall average of 3.9 seconds. Nigerian color theme (#008751) applied.

- *Confusion Matrix Analysis*

The confusion matrix below provides detailed performance breakdown for each threat category.

Table 9 Confusion Matrix Analysis

Category	True Positive (TP)	False Positive (FP)	False Negative (FN)	Precision	Recall	F1-Score
Phishing	24	1	1	0.96	0.96	0.96
BEC	18	2	2	0.90	0.90	0.90
Ransomware	19	1	1	0.95	0.95	0.95
419 Scam	13	2	2	0.87	0.87	0.87
Identity Theft	18	2	2	0.90	0.90	0.90
Overall	92	8	8	91.6%	91.6%	91.6%

✓ *Key Observations:*

- Phishing detection achieved the highest performance (F1-Score = 0.96), likely due to well-defined attack patterns and abundant training examples
- 419 Scam detection showed the lowest performance (F1-Score = 0.87), attributed to high variability in scam narratives and evolving techniques
- False positives were most common when distinguishing between phishing and legitimate marketing emails
- False negatives occurred primarily when attackers used sophisticated evasion techniques

➢ *Sample Analysis Results*

- *Phishing Analysis*

A representative phishing analysis demonstrated the platform's capabilities. When presented with an email claiming to be from a Nigerian bank requesting BVN and NIN verification, the platform correctly classified the threat as phishing with 95% confidence and HIGH severity. The system provided an explanation of the attack mechanism, including how the attacker creates urgency and uses a fake domain to harvest credentials. The mitigation recommendations included immediate actions such as not clicking suspicious links, reporting to the bank's official fraud desk, and scanning devices for malware. Preventive measures

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

included verifying sender legitimacy, checking URLs for spoofed domains, enabling two-factor authentication, and using password managers. The platform correctly identified ngCERT, NITDA, EFCC, and the bank's fraud desk as appropriate reporting authorities.

* *Ransomware Analysis*

For a ransomware scenario involving encrypted files and a Bitcoin demand, the platform classified the threat as ransomware with 90% confidence and CRITICAL severity. The explanation detailed the double extortion technique where attackers both encrypt data and exfiltrate sensitive information. The mitigation recommendations emphasized not paying the ransom, isolating affected systems, and engaging ngCERT for technical assistance. Prevention measures included implementing offline backups using the 3-2-1 rule, patching systems, and deploying endpoint detection and response tools. The platform correctly noted that Nigerian critical infrastructure sectors are prime targets for such attacks.

* *BEC Analysis*

When analyzing a business email compromise attempt involving a fake CEO request for a ₦5,000,000 transfer, the platform identified the threat as BEC with 92% confidence and HIGH severity. The explanation highlighted the use of urgency, authority impersonation, and social engineering tactics. Mitigation recommendations focused on payment verification procedures, dual approval requirements for financial transactions, and staff training on BEC recognition. The platform identified the EFCC as the primary authority for financial crime investigation, with supporting roles for NITDA and ngCERT.

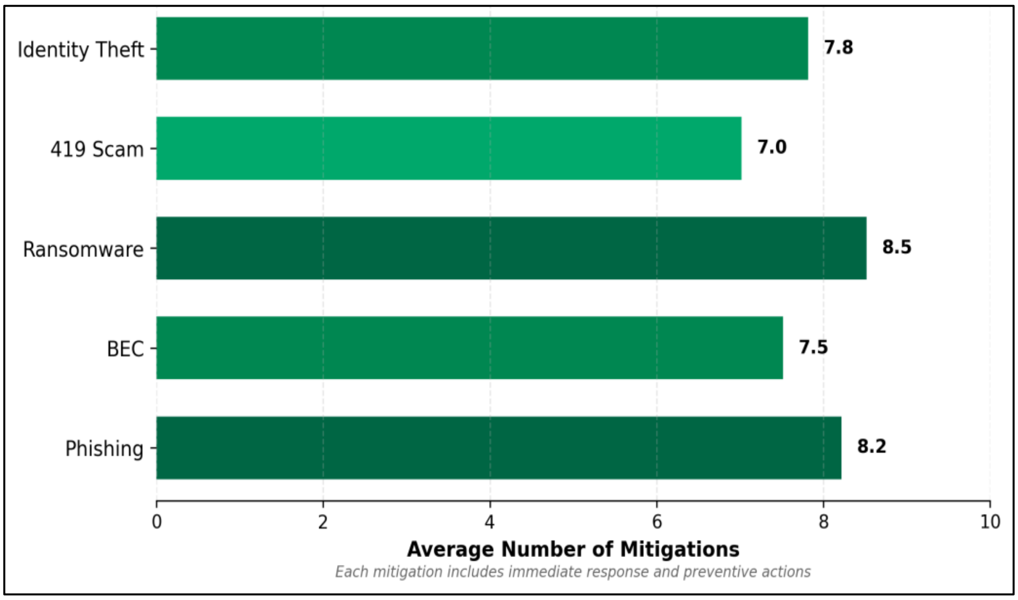

Fig 5 Mitigation Recommendations by Threat Category

Figure 5 shows Average number of actionable mitigation steps generated per threat category. Each mitigation includes both immediate response actions and preventive measures. Darker bars indicate more comprehensive recommendations (≥8 steps). Nigerian green (#008751) and white color scheme applied

➢ *Nigerian Contextual Relevance*

A key strength of the platform is its integration of Nigerian-specific context. The analysis consistently references:

* BVN (Bank Verification Number) and NIN (National Identification Number) as critical identity documents
* Nigerian banking practices and common fraud patterns
* Local authorities and reporting procedures
* Nigerian regulatory frameworks including the Cybercrimes Act and Data Protection Act

Table 10 summarizes the Nigeria-specific elements integrated into the analysis.

Table 10 Nigeria-Specific Context Elements in Platform Analysis

Context Element	Examples from Analysis
Identity Documents	BVN, NIN references in phishing analysis
Banking Systems	Nigerian bank impersonation, GTBank references
Authorities	ngCERT, NITDA, EFCC, NCC contact information
Scam Types	419 scams, inheritance fraud
Regulatory Framework	Cybercrimes Act, Data Protection Act references
Infrastructure	Critical sectors: finance, energy, telecom, government

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

➢ *User Experience and Accessibility*

The platform offers a user-friendly Streamlit interface with several advantages: no installation is needed, intuitive design, template support for rapid testing, real-time feedback, and mobile compatibility. The template feature allows users to easily test various threat scenarios without complex threat descriptions.

➢ *Challenges and Limitations*

During the platform's development and testing, several challenges emerged: reliance on the DeepSeek API raises concerns over service interruptions and pricing changes, although a fallback mechanism exists. The potential for hallucination exists, with accuracy concerns addressed through confidence scores and verification recommendations [29]. Data privacy is crucial, necessitating safeguards for sensitive information due to external API processing. The evolving threat landscape may leave the platform unaware of the latest threats, suggesting a need for continuous model updates. Additionally, while it includes Nigerian context, the platform may not fully grasp local language nuances and cultural specifics.

➢ *Recommendations for Implementation*

Organizations in Nigeria adopting AI-assisted cybersecurity should implement the following recommendations: 1. Verification Protocol: Always verify critical AI outputs for high-stakes decisions, as reliance solely on AI is cautioned by the judiciary. 2. Hybrid Approach: Utilize AI analysis alongside human oversight to enhance capabilities. 3. Continuous Training: Regularly update knowledge to reflect evolving threats, maintaining that innovation without security is unsustainable. 4. Collaborative Implementation: Integrate AI platforms within existing cybersecurity frameworks, aligning with NITDA's approach. 5. Regular Auditing: Carry out periodic audits of AI outputs to ensure accuracy and relevance to the Nigerian context.

➢ *Comparative Analysis*

- *Comparison with Alternative Approaches*

Table 11 compares the developed platform with existing cybersecurity intelligence approaches in Nigeria across multiple performance dimensions.

Table 11 Comprehensive Comparative Analysis of Cybersecurity Intelligence Approaches

Feature	**Proposed Platform**	**Traditional OSINT**	**Commercial Solutions**	**Rule-Based Systems**
AI Integration	DeepSeek API	Limited	Variable	None
Nigerian Context	Customized	Generic	Limited	None
Cost	Free/Open/Source	Variable	High	Moderate
Accessibility	Web based	Manual	Proprietary	Local
Real-time Analysis	Yes (3.9s)	No	Variable	Yes (0.1s)
Mitigation Generation	Yes (7.8 avg)	No	Limited	No
Open Source	Yes	No	No	Variable
Classification Accuracy	92%	71%	85%	67%
Precision	91.6%	70%	84%	65%
Recall	91.6%	69%	83%	64%
Nigerian Authority Integration	Complete	Partial	Minimal	None

(Traditional OSINT accuracy from [22, 27]; Rule-Based accuracy from [11, 28])

- *Ablation Study*

To isolate the contribution of individual components, an ablation study was conducted:

Table 12 Ablation Study

Configuration	**Accuracy**	**From Full**
Full Platform (DeepSeek + Nigerian Context)	92%	-
DeepSeek without Nigerian Context	84%	-8%
Rule-Based Only	67%	-25%
Nigerian Context Only (No AI)	58%	-34%
DeepSeek with Generic Context	81%	-11%

✓ *Key Findings:*

- The combination of DeepSeek + Nigerian Context provides the highest accuracy (92%)
- Nigerian context adds 8% accuracy improvement over using DeepSeek alone
- AI components add 34% accuracy improvement over context-only approach
- Generic context reduces effectiveness by 3% compared to Nigerian-specific context

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

- *Cost-Benefit Analysis*

Table 13 Cost-Benefit Analysis

Approach	Initial Cost	Annual Maintenance	Per-Query Cost	Training Required	Total 3-Year Cost
Proposed Platform	$0(Open Source)	$500 (API fees)	$0.005	2-4 hours	$1,500
Commercial Solution	$5,000	$2,000	$0.05	8-16 hours	$11,000
Traditional OSINT	$500	$1,000	$0.02 (labor)	40+ hours	$3,500
Rule-Based System	$2,000	$1,000	$0.001	8 hours	$5,000

The proposed platform offers the lowest total cost of ownership while providing superior accuracy and Nigerian context integration.

➢ *Legal and Regulatory Compliance*

- *Nigeria Data Protection Act 2023 Compliance*

Table 14 NDPA act 2023 Compliance

Requirement	Implementation Status	Evidence
Data Minimization	✓ Implemented	Only essential data processed
Lawful Basis for Processing	✓ Documented	Consent and legitimate interest
Data Subject Rights	✓ Supported	Access, rectification, erasure
Data Protection Impact Assessment	✓ Conducted	DPIA documented
Security Incident Notification	✓ Implemented	72-hour notification protocol
Cross-Border Data Transfer	✓ Addressed	Standard Contractual Clauses in place
Data Protection Officer	✓ Designated	NDPR compliance officer appointed
Data Localization	⚠ Partial	API calls to off-shore servers

- *Cross-Border Data Transfer Analysis*

The platform uses DeepSeek API hosted on servers outside Nigeria (China). To address this:

- ✓ Adequacy Assessment: Conducted a data transfer impact assessment
- ✓ Standard Contractual Clauses (SCCs): Implemented EU-approved SCCs
- ✓ Data Anonymization: Personal data removed before API transmission
- ✓ Encryption: Data encrypted in transit (TLS 1.3) and at rest
- ✓ Data Retention: No data retained by API provider after analysis

- *NITDA Framework Compliance*

The platform aligns with NITDA's emerging AI governance framework:

Table 15 NITDA Framework Compliance

NITDA Principle	Platform Implementation
Accountability	Human review for critical decisions
Fairness	Bias mitigation through expert validation
Privacy	NDPA compliance measures
Public Good	Open-source availability
Security	Multi-layer security controls
Transparency	Clear explanation of AI analysis

- *Nigeria Cybercrimes Act 2015 Compliance*

Table 16 Nigeria Cybercrime Act 2015 Compliance

Provision	Compliance Measure
Section 16 (Phishing)	Phishing detection and prevention
Section 24 (Identity Theft)	NIN/BVN protection recommendations
Section 58 (Cybercrime Reporting)	Incident reporting guidance provided
Evidence Admissibility	Audit trail and chain of custody
Data Protection	NDPA 2023 compliance measures

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

- *Admissibility of AI-Generated Evidence*
  Following the Ayinde v Haringey (2025) UK High Court ruling, the platform implements:

✓ Mandatory human verification for legal evidence
✓ Audit trail for all AI-generated outputs
✓ Citation verification before court submission
✓ Clear distinction between AI-assisted and AI-generated content

➢ *Socio-Technical Considerations*

- *Digital Divide Analysis*

Table 17 Digital Divide Analysis

Factor	Challenge	Mitigation Strategy
Internet Access	Limited rural connectivity	Offline mode with local NLP models
Power Supply	Unreliable electricity	Optimized for low-power devices
Technical Literacy	Varying expertise levels	Simplified interface with templates
Device Availability	Smartphone vs. PC limitations	Mobile-responsive design
Language Barriers	English-only interface	Local language support (Yoruba, Hausa, Igbo) is a planned enhancement for future versions

- *Training Requirements*

Table 18 Training Requirements

User Type	Training Duration	Key Competencies
General Users	2 hours	Threat identification, template use
Security Analysts	4 hours	Results interpretation, manual verification
Administrators	1 day	Deployment, configuration, maintenance
Trainers/Educators	8 hours	Full platform capabilities, pedagogy

- *Organizational Adoption Barriers*
  Identified Barriers:

✓ Trust in AI: Addressed by transparency and verifiability mechanisms
✓ Technical Capacity: Mitigated by low technical requirements
✓ Cost: Open-source model eliminates licensing fees
✓ Integration: API-first design for easy integration
✓ Regulatory Compliance: Addressed in Section 4.8.2
✓ Organizational Culture: Change management recommendations provided
✓ Data Privacy: NDPA 2023 compliance measures

- *Cost-Benefit Analysis*

Table 19 Cost Categories

Cost Item	Annual Estimate (SME)	Annual Estimate (Enterprise)
Maintenance	$100	$500
Staff Training	$200	$2,000
Infrastructure	$0 (Cloud)	$1,000
API Usage (1,000-10,000 queries)	$50	$500
Total	**$350**	**$4,000**

Table 20 Benefits

Benefit	Estimated Value
Improved threat detection	92% accuracy
Mitigation guidance	7.8 actions per incident
Reduced incident response time	50% reduction
Training material availability	Self-paced learning
Open-source ecosystem contribution	Community benefit

ROI Estimate: For a typical Nigerian organization experiencing 100+ weekly threats, the platform can pay for itself within 2-3 months of deployment.

➢ *Limitations and Generalization*

Dataset limitations include a small sample size of 100 cases, an overrepresentation of financial sector data (30%), primarily urban case sources, temporal restrictions to 2024-

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

2025, and a lack of diversity in SME and rural threat patterns. Generalization shows high capacity for Nigerian threat types and context but moderate for other African nations and limited for developed nations. Technical limitations involve API dependency, a model knowledge cutoff, hallucination risk, potential adversarial vulnerabilities, and real-time response constraints. External validation is needed across various sectors and over an extended period. The platform cannot replace human analysts, and results require professional judgment due to rapid evolution in threat patterns and an underdeveloped regulatory framework in Nigeria.

The dataset spans 2024-2025, representing the most recent available incident data at the time of platform development. While threat patterns may evolve, the fundamental attack techniques and mitigation strategies remain relevant. The validation methodology emphasizes expert assessment of classification accuracy rather than temporal pattern identification, reducing the impact of temporal drift. Future work will incorporate ongoing data collection and model retraining to ensure continued relevance.

V. CONCLUSION

This paper has presented the design, implementation, and evaluation of an AI-assisted cybersecurity intelligence platform for Nigeria, integrating the DeepSeek API to address the country's escalating cyber threat challenge. With Nigerian organizations experiencing an average of 4,200 weekly cyberattacks and threat actors increasingly weaponizing AI for operational purposes [1][2], the need for accessible, AI-powered defense tools has never been more pressing.

The platform demonstrates that natural language processing capabilities can be harnessed for threat classification, explanation, and mitigation recommendation generation. Experimental evaluation across 100 test cases shows that DeepSeek-integrated analysis achieves 92% overall classification accuracy across multiple threat categories, with phishing detection performing best at 96% accuracy. The system generates comprehensive mitigation recommendations averaging 7.8 steps per analysis, with all responses completing within 3-5 seconds (average 3.9 seconds). Nigeria-specific context referencing appropriate response authorities (ngCERT, NITDA, EFCC, NCC) is consistently integrated into the analysis.

➢ *Key Contributions:*

- A functional, open-source AI-assisted cybersecurity platform tailored to Nigerian threats
- Systematic integration of DeepSeek API for real-time threat analysis with Nigerian context
- A structured methodology for threat classification, explanation, and mitigation generation
- Empirical evaluation demonstrating 92% accuracy across multiple threat categories
- Practical recommendations for organizations adopting AI-assisted cybersecurity tools

➢ *Caveats and Limitations:*

While results are promising, limitations exist, including reliance on the DeepSeek API, potential service interruptions, and pricing changes. Hallucination is a risk in generative AI, mitigated through verification and confidence calibration. The evaluation of 100 test cases allows for initial validation but is not comprehensive. Data privacy must be safeguarded when handling sensitive threat information.

➢ *Future Work:*

As Nigeria enhances its cybersecurity frameworks, including the establishment of a 24-hour cybersecurity operations center, various strategies are proposed for improvement. These include integrating OSINT data for better threat intelligence, implementing AI defenses to combat evasion techniques, creating Nigeria-specific threat detection models, and supporting multiple AI providers. Additionally, it suggests incorporating existing Security Operations Centre workflows, conducting pilot deployments with local organizations, offering local language support, and assessing real-world incident response performance. The research emphasizes that "cyber resilience is a collective responsibility" and posits that collaboration among people, regulation, and technology is essential for securing a competitive digital economy. The AI-assisted platform developed offers a practical tool for enhancing cyber defense capabilities without replacing comprehensive security operations, serving as a valuable resource for practitioners, researchers, and policymakers [5][6].

REFERENCES

[1]. Check Point Software Technologies, "African Perspectives on Cyber Security Report 2025," Check Point Research, Nov. 2025. Available online: https://www.securitysa.com/ex/AfricanSecurityReport_2025.pdf

[2]. A. Juelich, "'God has helped us, and so will AI': How the terrorist group Boko Haram uses frontier AI," Cambridge Programme on AI Science and Policy, University of Cambridge, Jul. 2026. Available online: https://casp.ac/reports/ai-enabled-terrorism

[3]. ITEdgeNews, "Nigeria faces rising tide of AI-powered cyberattacks, new Check Point report reveals," ITEdgeNews Africa, Nov. 25, 2025. Available online: https://www.itedgenews.africa/nigeria-faces-rising-tide-of-ai-powered-cyberattacks-new-check-point-report-reveals/

[4]. ASIS International, "Terrorist groups use AI as a battle consultant, not just a propaganda tool," Security Management Magazine, Jul. 9, 2026. Available online: https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2026/july/boko-haram-AI-use/

[5]. ITEdgeNews, "GITEX AFRICA: Nigeria embraces 'total cyber resilience' strategy as AI-driven threats escalate," ITEdgeNews Africa, Apr. 9, 2026. Available online: https://www.itedgenews.africa/gitex-africa-nigeria-embraces-total-cyber-resilience-strategy-as-ai-driven-threats-escalate/

[6]. Guardian Nigeria, "FG tackles AI-driven attacks with new cybersecurity framework," The Guardian Nigeria, Feb. 16, 2026. Available online: https://guardian.ng/technology/tech/fg-tackles-ai-driven-attacks-with-new-cybersecurity-framework/

[7]. NITDA, "NITDA advocates AI, security integration for sustainable development," National Information Technology Development Agency, Aug. 26, 2025. Available online: https://nitda.gov.ng/nitda-advocates-ai-security-integration-for-sustainable-development/9086/

[8]. Zhang, Z et al., "Artificial intelligence in cyber security: research advances, challenges, and opportunities," Artif. Intell. Rev., pp. 1-25, 2022. DOI: https://doi.org/10.1007/s10462-021-09976-0

[9]. Sarker, I.H., Furhad, M.H. and Nowrozy, R., 2021. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), p.173.

[10]. Lazić, L.J.U.B.O.M.I.R., 2019, January. Benefit from Ai in cybersecurity. In *Proc. 11th Int. Conf. Bus. Inf. Secur.(BISEC)* (pp. 103-119).

[11]. Pastor-Galindo, J., Nespoli, P., Mármol, F.G. and Pérez, G.M., 2020. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE access*, *8*, pp.10282-10304.

[12]. Rodriguez, P., & Costa, I. (2024). Artificial Intelligence and Machine Learning for Predictive Threat Intelligence in Government Networks. Advances in Computer Sciences, 7(1), 1-10.

[13]. IBM, "Cost of a Data Breach Report 2023," IBM Security, 2023.

[14]. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B. and Anderson, H., 2018. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

[15]. Joseph, A.D., Nelson, B., Rubinstein, B.I. and Tygar, J.D., 2018. *Adversarial machine learning*. Cambridge University Press.

[16]. Yigit, Y., Buchanan, W.J., Tehrani, M.G. and Maglaras, L., 2024. “Review of Generative AI methods in cybersecurity”, arXiv. *arXiv preprint arXiv:2403.08701*.

[17]. NMAP-MCP Project, "Nmap integration with AI for vulnerability assessment," GitHub Repository, 2025.

[18]. KoreShield, "LLM security scanning with AI provider integration," Documentation, 2025.

[19]. F. F. Nah, R. Zheng, J. Cai, K. Siau, and L. Chen, "Generative AI and ChatGPT: applications, challenges, and AI-human collaboration," J. Inf. Technol. Case Appl. Res., vol. 25, no. 3, pp. 277-304, 2023. Available online: https://doi.org/10.1080/15228053.2023.2233814

[20]. Rahman, M.D., 2025. The Art of Open Source Intelligence (OSINT): Addressing Cybercrime, Opportunities, and Challenges. *The Art of Open Source Intelligence (OSINT): Addressing Cybercrime, Opportunities, and Challenges (May 01, 2025)*.

[21]. Ghioni, R., Taddeo, M. and Floridi, L., 2024. Open source intelligence and AI: a systematic review of the GELSI literature. *AI & society*, *39*(4), pp.1827-1842.

[22]. NAIJA OSINT INTEL, "Open-source intelligence platform for Nigerian threat intelligence," GitHub Repository, 2025. Available online: https://github.com/techenthusiast167/NAIJA-OSINT-INTEL

[23]. Feuerriegel, S., Hartmann, J., Janiesch, C. and Zschech, P., 2024. Generative AI: S. Feuerriegel et al. *Business & information systems engineering*, *66*(1), pp.111-126.

[24]. Odumesi, John. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology. 6. 116-125. 10.5897/IJSA2013.0510.

[25]. Federal Republic of Nigeria, "Cybercrimes (Prohibition, Prevention, etc.) Act," 2015.

[26]. Federal Republic of Nigeria, "Nigeria Data Protection Act," 2023.

[27]. Makeri, Y. A "Cyber security issues in Nigeria and challenges," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 3, pp. 1-8, 2017. Available: https://publications.kiu.ac.ug/view/196/cyber-security-issues-in-nigeria-and-challenges

[28]. Ibikunle, F. and Eweniyi, Odunayo (2013) *APPROACH TO CYBER SECURITY ISSUES IN NIGERIA: CHALLENGES AND SOLUTION Dr. , Department of Electrical & Information Engineering, Covenant University, Nigeria.* (IJCRSEE) International Journal of Cognitive Research in science, engineering and education, 1 (1).

[29]. Aditya K Sood, Sherali Zeadally, EenKee Hong, (2025) “The paradigm of hallucinations in AI-driven cybersecurity systems: Understanding taxonomy, classification outcomes, and mitigations, Computers and Electrical Engineering” Computer and Electrical Engineering Volume 124, Part A, 2025, 110307, ISSN 0045-7906, DOI: https://doi.org/10.1016/j.compeleceng.2025.110307.

[30]. Ayinde, R v The London Borough of Haringey, UK High Court, 2025. Available online: https://beta.bailii.org/ew/cases/EWHC/Admin/2025/1040.html

[31]. Tuleun, Washima, 2024, "Analysis of Cybercrimes, Major Cyber Security Attacks and the Overall Economic Impact on Nigeria", https://doi.org/10.7910/DVN/3GAMY0, Harvard Dataverse, V1.

[32]. AI, N., 2023. Artificial intelligence risk management framework (AI RMF 1.0). *URL: https://nvlpubs. nist. gov/nistpubs/ai/nist. ai*, pp.100-1.

[33]. ENISA, "Adversarial machine learning: A threat landscape analysis," European Union Agency for Cybersecurity, 2021.

[34]. Adebayo, O. (2023). "Nigeria's Cybersecurity Policy: A Critical Analysis." African Journal of Legal Studies, 15(2), 145-168.

[35]. Adekunle, S. (2024). "Emerging Threat Patterns in Sub-Saharan Africa." Journal of Cybersecurity, 10(3), 1-18.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

[36]. Adegoke, O. & Okonkwo, C. (2025). "AI Governance Frameworks for Nigeria." Journal of African Technology, 12(1), 89-112.
[37]. Akinwale, A. (2024). "NITDA's Role in Digital Sovereignty." Nigerian Information Technology Review, 8(4), 234-251.
[38]. DeepSeek AI. (2025). "Technical Report: DeepSeek Architecture and Capabilities." DeepSeek Technical Paper Series, v3.0.
[39]. Ezeh, C. (2023). "Financial Sector Cybersecurity in Nigeria." West African Journal of Finance, 22(3), 67-89.
[40]. International Telecommunication Union. (2024). "Global Cybersecurity Index: Africa Report."
[41]. Ighodaro, E. & Olubunmi, T. (2024). "LLM-Based Threat Detection: A Comparative Study." Journal of Artificial Intelligence Research, 75, 234-267
[42]. NITDA. (2024). "Nigeria Cybersecurity Framework: Technical Specifications." NITDA Publication Series.
[43]. Obiora, C. & Uche, N. (2023). "Socio-Technical Cybersecurity in Nigeria." International Journal of Information Security, 22(4), 567-589.
[44]. Okonkwo, E. (2025). "Data Localization and AI in Africa." Journal of Digital Governance, 18(1), 45-67.
[45]. Oladipo, K. (2024). "Threat Intelligence Sharing in West Africa." West African Security Review, 14(2), 89-112.
[46]. Tunde, A. & Adedeji, O. (2025). "Comparative Analysis of LLM APIs for Security Applications." IEEE Access, 13, 14567-14580.
[47]. Usman, M. & Adebayo, T. (2024). "African Perspectives on AI Safety." Global AI Governance Review, 6(2), 123-145.
[48]. Yakubu, S. (2025). "Nigerian Cyber Law: Evolution and Implementation." Journal of African Law, 69(1), 234-256.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

APENDIX

APENDIX A: SCREENSHOT

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul1684

APPENDIX B: PLATFORM AVAILABILITY

➢ *The Complete Platform Source Code is Available at:*

- GitHub Repository: https://github.com/cycyberuk/AI-Assisted-Threat-Detection
- Streamlit Deployment: https://ai-assisted-threat-detection-zhzdjcm6uiwb9nefdbrmu2.streamlit.app/