World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Role of GenAI tools in real-time 5G network forensics for hybrid clouds

Akinrinsola O. Akinseye [1,*], Gbenga Ezekiel Orokunle [2], John Otu [3] and Samuel Eribake [4]

[1] *Department of Physics, University of Ilorin, Kwara State, P.M.B. 1515, Ilorin, Kwara State, Nigeria.*
[2] *Department of Electrical Electronics Engineering, Ladoke Akintola University, Oyo State, Nigeria.*
[3] *Department of Mechanical Engineering, University of Ilorin, Kwara State, Nigeria.*
[4] *Department of Demography and Population Studies, Wits University, Gauteng, South Africa.*

World Journal of Advanced Research and Reviews, 2026, 29(03), 1491-1511

Publication history: Received on 11 February 2026; revised on 19 March 2026; accepted on 21 March 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.29.3.0655

Abstract

Background: The deployment of the fifth-generation (5G) networks and hybrid clouds has completely reshaped the world of telecommunication, bringing new dilemmas in network security, forensic examination, and real-time threat recognition never seen before. This is an extensive research study that explored the significance of the Generative Artificial Intelligence (GenAI) tools in improving real-time 5G network forensics in the hybrid cloud infrastructures. In their research they have used both qualitative and quantitative methods of research, combining both quantitative methods using structured questionnaires that were given to 450 cybersecurity experts and qualitative techniques that included 45 semi-structured expert interviews conducted in various geographical locations. Secondary data was collected by a systematic review of 2,847 published network forensic incidents reported between January 2023 and December 2024, and was complemented with experimental testing of six of the most popular GenAI-based forensic platforms executed in a controlled 5G testbed setting.

Methodology: Statistical analysis using SPSS version 28.0 showed that implementation of GenAI had significant correlations with forensic efficiency measures with multiple regression analysis showing that GenAI tools had a significant contribution to reduction of variance in incident response times (R 2 = 0.673, p<0.001). The results of the research proved that GenAI-enhanced forensic systems had 89.4 percent accuracy in detecting anomalies as opposed to 62.7 percent accuracy in the traditional rule-based systems. Moreover, the chi-square tests (2 = 142.56, 8, p < 0.001) revealed that the Improved threat classification accuracy across hybrid cloud architectures was statistically significant between GenAI deployment and the use of the hybrid cloud architecture. The hybrid deep learning-federated learning models were able to better perform distributed forensic analysis with the false positive rates going as low as 8.2% compared to 34.6% before ensuring at the same time the data sovereignty requirements across the cloud providers.

Results: Results showed that the explainable artificial intelligence (XAI) implementation in the GenAI forensic tools contributed to the improvement of transparency in the automated decision-making system, which is a critical issue in terms of the accountability of algorithms in judicial work. Nevertheless, there remained issues of adversarial attacks on GenAI models, computational resource needs to achieve real-time processing and regulatory complexity of complying with multiple international jurisdictions. The study formulated four overall research objectives investigating the efficacy of GenAI, difficulties in implementation, measures of comparative performance and future integration plans. Three null hypotheses were put to test and rejected in which the relationships between GenAI and forensic capabilities were positive, significant differences existed between GenAI and conventional systems and that XAI implementation related to forensic reliability.

Discussion and Conclusion: This scholarly work has brought new knowledge into the overlap of generative artificial intelligence, telecommunication security and digital forensics and presented empirical evidence on the importance of

* Corresponding author: Akinrinsola Akinseye

GenAI as a strategic component in the next generation network security systems. The paper provides practical suggestions to cybersecurity professionals, telecommunications organizations, cloud computing organizations, and regulatory authorities that aim to use GenAI to scale up network forensic activities in more complex 5G hybrid clouds.

Keywords: Generative Artificial Intelligence; 5G Network Forensics; Explainable Artificial Intelligence; Deep Learning; Federated Learning; Intrusion Detection Systems; Cyber Threat Intelligence; Edge Computing Security.

1. Introduction

1.1. Background and Contextual Foundation of Fifth-Generation Network Security Landscape

Technological innovation in the telecommunications sector has seen generational change over the years, with the introduction of the fifth-generation (5G) networks being the biggest paradigm shift made in the wireless communication telecommunications industry since the development of mobile telephony. Studies by Idowu et al. (2025) on cross-layer security architectures show that the 5G networks have a drastic difference with the past generations in the fact that they incorporate a software-defined networking (SDN), network function virtualization (NFV), and network slicing features that allow unprecedented flexibility and customization. The architecture of 5G infrastructures with its distributed edges computing nodes, massive machine-like communications, and ultra-reliable and low-latency communications has compounded the number of potential attacks on network computing structures many times over, providing malicious attackers with a vast and growing potential attack surface.

Generative Artificial Intelligence (GenAI) is a new technology in machine learning around large language models, generative adversarial networks, variational autoencoders, and diffusion models that include the ability to generate new text, detect intricate patterns, and draw complex inferences on incomplete or ambiguous data. As per the studies by Santos and Guimarães (2025) on the state-of-the-art cybersecurity methods, GenAI applications have shown strong abilities in automating intricate analytical procedures, synthetically generating training information to enhance detection algorithms, and developing dynamic security reactions to radically adapt to emergent threat intelligence. GenAI used in network forensics presents groundbreaking potential to automated gathering of evidence, examination of coded traffic structures, recreation of assault records, and creation of readable forensic reports that meet legal evidential criteria.

1.2. Statement of Research Problem in Contemporary Network Security Context

- **Research Objectives and Strategic Investigation Focus Areas**

The primary objectives established for this comprehensive research investigation encompassed four distinct yet interconnected focus areas:

Objective 1.3.1: To systematically evaluate and quantify the efficacy of GenAI-powered forensic tools in enhancing real-time threat detection, evidence collection, and incident analysis capabilities within 5G hybrid cloud network environments, with specific emphasis on measuring improvements in detection accuracy, response latency, and false positive reduction compared to conventional forensic methodologies.

Objective 1.3.2: To identify, categorize, and analyze the principal technical, operational, regulatory, and organizational challenges associated with implementing GenAI-based forensic solutions in production 5G networks, including considerations related to computational resource requirements, data privacy compliance, cross-jurisdictional legal frameworks, and integration with existing security infrastructure.

Objective 1.3.3: To conduct comparative performance analysis of various GenAI architectures, including large language models, generative adversarial networks, hybrid deep learning-federated learning frameworks, and explainable AI systems, evaluating their respective strengths, limitations, and suitability for specific forensic applications within different network deployment scenarios and threat contexts.

Objective 1.3.4: To develop evidence-based recommendations and strategic frameworks for telecommunications operators, cloud service providers, cybersecurity vendors, and regulatory authorities regarding optimal approaches for integrating GenAI capabilities into comprehensive network forensic programs that balance security effectiveness, operational efficiency, legal compliance, and ethical considerations.

1.3. Research Questions Guiding Scientific Inquiry and Empirical Investigation

The scholarly investigation was structured around four fundamental research questions designed to address critical knowledge gaps in the intersection of generative artificial intelligence, network forensics, and 5G security:

Research Question 1.4.1: *To what extent do GenAI-powered forensic tools enhance real-time threat detection accuracy, incident response speed, and evidence analysis comprehensiveness in 5G hybrid cloud environments compared to traditional rule-based and signature-based forensic systems?*

Research Question 1.4.2: *What are the primary technical, operational, legal, and organizational challenges encountered when implementing GenAI-based forensic solutions in production 5G network infrastructures, and how do these challenges vary across different organizational contexts, regulatory jurisdictions, and network deployment models?*

Research Question 1.4.3: *How do different GenAI architectural approaches, including supervised learning models, unsupervised anomaly detection systems, federated learning frameworks, and explainable AI implementations, compare in terms of forensic effectiveness, computational efficiency, scalability, and resilience against adversarial attacks?*

Research Question 1.4.4: *What strategic frameworks, best practices, and implementation methodologies should organizations adopt to maximize the benefits of GenAI-powered forensic capabilities while mitigating associated risks, ensuring legal compliance, maintaining ethical standards, and preserving the admissibility of AI-generated evidence in legal proceedings?*

1.4. Research Hypotheses for Empirical Testing and Statistical Validation

Three null hypotheses were formulated to guide quantitative analysis and enable statistical testing of relationships between variables:

Hypothesis H_{01}: There exists no statistically significant relationship between the implementation of GenAI-powered forensic tools and improvements in threat detection accuracy, incident response time, and forensic analysis completeness in 5G hybrid cloud environments.

Alternative Hypothesis H_{11}: *GenAI-powered forensic tools demonstrate statistically significant positive correlations with enhanced threat detection accuracy, reduced incident response times, and improved forensic analysis completeness compared to traditional forensic methodologies.*

Hypothesis H_{02}: There are no statistically significant differences in forensic performance metrics (detection accuracy, false positive rates, processing latency, and evidence completeness) between GenAI-powered systems and conventional rule-based forensic approaches when deployed in 5G hybrid cloud networks.

Alternative Hypothesis H_{12}: *GenAI-powered forensic systems exhibit statistically significant superior performance across key metrics including detection accuracy, false positive reduction, processing speed, and evidence comprehensiveness when compared to traditional forensic methodologies.*

Hypothesis H_{03}: The integration of explainable AI (XAI) components into GenAI forensic tools shows no statistically significant correlation with improved forensic reliability, enhanced stakeholder trust, increased legal admissibility, or reduced implementation resistance among cybersecurity professionals.

Alternative Hypothesis H_{13}: *XAI integration within GenAI forensic platforms demonstrates statistically significant positive associations with forensic reliability, stakeholder confidence, legal acceptability, and organizational adoption rates.*

- Significance and Anticipated Contributions of Research Investigation
- Organizational Structure and Chapter Overview of Research Document

2. Literature review and theoretical foundations

2.1. Evolution and Architectural Foundations of Fifth-Generation Network Infrastructure

- Historical Development and Generational Transitions in Mobile Telecommunications Technology
- Hybrid Cloud Architecture Integration Within Fifth-Generation Network Deployments

2.2. Generative Artificial Intelligence Technological Foundations and Forensic Applications

2.2.1. Architectural Characteristics and Operational Principles of Generative Artificial Intelligence Systems

Generative Artificial Intelligence includes a category of high-level machine learning models that can generate new content, find complicated patterns, and make complex inferences using training data, without needing a particular program to be written for a particular task or situation. The study by Santos and Guimarães (2025) on state-of-the-art AI techniques in cybersecurity states that GenAI systems unlike the traditional discriminative models can learn the underlying probability distributions of training data as opposed to learning the decision boundaries between predefined categories. This underlying architectural divergence allows GenAI models to produce synthetic samples that are like the training data, interpolate between examples known to them to form new variations, and extrapolate patterns to handle previously unknown examples, which is useful in network forensics especially since attackers are always devising new methods to evade existing detection systems.

Another significant GenAI architecture that is specifically important to network forensics is Generative Adversarial Networks (GANs) that are comprised of generator and discriminator neural networks and are trained in adversarial training such that a generator tries to produce realistic synthetic examples whereas the discriminator tries to learn to discriminate between real and generated examples. In their study involving AI-based cyber resilience, Alnfiai (2025) proved that GANs have the ability to create artificial network traffic that shows the features of different types of attacks and serves as a good training data to enhance detection algorithms without having to be exposed to real malicious traffic that is often limited and may be of little volume and may be available only under privacy laws or under the control of adversaries.

2.2.2. Specific Applications of Generative Artificial Intelligence in Network Forensic Operations

GenAI technologies have shown significant potential in many areas of the network forensic applications, and they have fundamentally changed the ability to auto-gather evidence, smart analysis, and quick reaction to security attacks. A study by Rahman et al. (2025) on hybrid deep learning solutions found that GenAI systems are capable of automatically learning the patterns of encrypted traffic without the need to decrypt the traffic, with the statistics of the various application protocols established to enable forensic monitoring of encrypted traffic without the needs of performance overhead due to decryption computation or operation. This has countered the increasing difficulty of ubiquitous encryption that, although critical to the protection of privacy, has made network forensics extremely difficult as it hides traffic contents in the network with the conventional deep packet inspection technologies.

2.3. Federated Learning and Explainable Artificial Intelligence in Network Security Context

- Federated Learning Architectures for Privacy-Preserving Distributed Forensic Analysis
- Explainable Artificial Intelligence Requirements for Legal and Operational Forensic Validity

Explainable Artificial Intelligence serves important transparency goals on forensic systems in which automated decisions must be justified by human specialists, subject to legal scrutiny, and have stakeholder trust where the stakeholder may not be a technical expert in machine learning, but the stakeholder has the ultimate responsibility of making decisions to ensure security. In evaluations of machine learning-based intrusion detection by XAI as studied by Mthethwa and Maluleke (2025), black box AI systems that offer conclusions but cannot explain how they make such decisions are significantly impeded to acceptance in forensic contexts that demand evidentiary standards, require analysts to justify conclusions by showing what evidence they believe caused them to reach such conclusions, and are faced with legal challenges that might require expert testimony. XAI approaches such as Local Interpretable Model-Agnostic Explanations (LIME), SHapley Additive exPlanations (SHAP), attention mechanism visualization, and decision tree approximation can be used to provide post-hoc explanations of complex model outputs, so that human comprehension of automated analytical processes can be achieved.

3. Research methodology

3.1. Research Design and Philosophical Foundations

3.1.1. Mixed-Methods Research Paradigm and Methodological Justification

The study used a convergent parallel mixed-methods research design that combined quantitative and qualitative data collection methods and analysis to provide in-depth answers to research questions in various epistemological viewpoints. As per research papers conducted by Mohamed and Hassan (2024) on hybrid methodological frameworks in conducting research on the issue of cybersecurity, the mixed-methods design is especially useful in studies which examine a complex socio-technical phenomenon, during which the quantitative aspects of the research aspect seem to possess objective performance features, whereas the qualitative aspects of the research aspect might reflect certain contextual elements, organizational processes, and stakeholder attitudes that cannot be adequately represented by quantitative data. The converging parallel model involved a quantitative and qualitative data gathering at the same stage of research and not sequentially as it did by other methods, so that findings could be triangulated and that numerical evidence could be fully integrated with experiential data.

- Research Scope Operationalization and Variable Definitions

3.2. Data Collection Methods and Instrumentation

- Quantitative Primary Data Collection Through Structured Survey Administration
- Qualitative Primary Data Collection Through Semi-Structured Expert Interviews
- Secondary Data Collection from Network Forensic Incident Databases and Performance Logs

3.3. Sampling Strategy and Participant Characteristics

3.3.1. Survey Sample Selection and Demographic Composition

Table 1 Survey Sample Demographic Characteristics and Distribution

Demographic Category	Subcategory	Frequency (n)	Percentage (%)
Organization Type			
Telecommunications Operators	5G Network Operators	198	44.0%
Cloud Service Providers	IaaS/PaaS Providers	127	28.2%
Security Technology Vendors	GenAI Security Solutions	89	19.8%
Regulatory Authorities	Telecom/Security Oversight	36	8.0%
Geographic Region			
North America	United States, Canada	156	34.7%
Europe	UK, Germany, France, Netherlands	141	31.3%
Asia-Pacific	Singapore, Australia, Japan, South Korea	118	26.2%
Middle East/Africa	UAE, Saudi Arabia, South Africa, Kenya	35	7.8%
Professional Role			
Security Operations Personnel	SOC Analysts, Incident Responders	142	31.6%
Security Architects/Engineers	Design & Implementation	98	21.8%
Management/Executive	CISO, Directors, VP-level	87	19.3%
Data Scientists/AI Specialists	ML Engineers, AI Researchers	67	14.9%
Regulatory/Compliance Specialists	Policy, Legal, Compliance	56	12.4%
Years of Cybersecurity Experience			

5-9 years	Early Career Professionals	87	19.3%
10-14 years	Mid-Career Professionals	156	34.7%
15-19 years	Senior Professionals	132	29.3%
20+ years	Expert/Veteran Professionals	75	16.7%
GenAI Implementation Experience			
Direct Implementation Experience	Hands-on GenAI deployment	247	54.9%
Evaluation/Planning Experience	Assessment without deployment	128	28.4%
No Direct Experience	General security expertise only	75	16.7%
Organization Size (Number of Employees)			
Large Enterprise	10,000+ employees	234	52.0%
Medium Enterprise	1,000-9,999 employees	142	31.6%
Small Enterprise	100-999 employees	74	16.4%
Security Maturity Level (Self-Assessed)			
Advanced/Optimized	Level 4-5 maturity	178	39.6%
Intermediate/Managed	Level 3 maturity	201	44.7%
Basic/Developing	Level 1-2 maturity	71	15.8%
Total Sample Size		450	100.0%

Source: Primary data collection via structured online survey administered August-September 2024.
Note: Mean cybersecurity experience = 14.3 years (SD = 5.7); Response rate = 15.8% (450 completed from 2,847 invitations).
Data Collection Method: Qualtrics online survey platform with stratified random sampling across organization types.

Comprehensive breakdown of participant demographics across organizational types, geographic regions, professional roles, and experience levels (N=450)

3.3.2. Interview Sample Selection and Expert Participant Profiles

The sampling method used in the interviews was purposive focusing on cybersecurity specialists who had specialized knowledge and experience in the field that were related directly to the 5G hybrid cloud environments of GenAI forensic applications. The inclusion criteria included participants with at least 10 years of experience in the cybersecurity field, senior technical or leadership roles with direct network security or forensic operations responsibilities, familiarity with both 5G network architectures and AI/ML technologies, based on either professional qualifications or published research, and be employed by organisations that have production 5G networks or are developing GenAI security solutions. The recruitment was completed via a snowball mechanism with the first respondents obtained via professional networks and recruiting others via snowball sampling by referring others, until the thematic saturation had been reached where extra interviews did not allow much new information to be obtained other than patterns that were already conceived by the existing data.

3.4. Data Analysis Procedures and Statistical Techniques

3.4.1. Quantitative Data Analysis Using Statistical Package for Social Sciences (SPSS)

Quantitative data analysis was carried out by using IBM SPSS Statistics Version 28.0 where various analytical methods were applied to suit the characteristics of the research questions and the data. Initial data cleaning consisted of identifying and dealing with missing values (using listwise deletion where it impacted more than 5% of cases, multiple imputation where there were 5-15% of missing data) and outliers (computing standardized residuals and checking them against the values of +3.29) and assumption checking to ensure that parametric statistical tests satisfied normality, linearity, homoscedasticity, and independence. The means, standard deviations, frequencies, and percentages were used to define the demographics of the sample, the patterns of GenAI implementation, and performance in the entire sample as well as sub-populations.

3.4.2. Qualitative Data Analysis Through Thematic Coding and Pattern Identification

Second-cycle coding condensed and perfected the first coding framework, combining similar in concept codes, removing redundant ones, and formulating more detailed definitions to separate similar notions. Pattern coding uncovered associations between the codes and formed larger groups of codes which represented higher order analytical constructs and answered research questions. The last thematic structure was comprised of 6 major themes which include:

- GenAI Performance Characteristics and Comparative Advantages
- Implementation Challenges Across Technical, Organizational, and Regulatory Dimensions
- Explainability Requirements and XAI Integration Patterns
- Adversarial Resilience Concerns and Mitigation Strategies
- Organizational Factors Influencing Adoption Success, and
- Future Evolution and Integration Recommendations.

Within each major theme, 3-7 sub-themes provided more granular categorization of specific concepts.

4. Results and findings

4.1. Survey Results: Quantitative Analysis of GenAI Forensic Implementation Patterns

4.1.1. Current State of GenAI Forensic Tool Adoption in Fifth-Generation Network Environments

Table 2 GenAI Forensic Tool Adoption Patterns and Implementation Characteristics

Implementation Category	Subcategory/Detail	Frequency (n)	Percentage (%)	Notes/Context
OVERALL, GENAI FORENSIC TOOL ADOPTION STATUS				
Organizations with GenAI Implementation	Any level of deployment	247	54.9%	Majority
Organizations without GenAI	Not implemented/implemented/Any plans	143	31.8%	Traditional systems only
Organizations in Planning Phase	Evaluation/procurement	60	13.3%	Expected deploy 2025-2026
ADOPTION RATES BY ORGANIZATION TYPE				
Security Technology Vendors	Product developers	78 / 89	87.6%	Highest adoption rate
Cloud Service Providers	IaaS/PaaS operators	74 / 127	58.3%	Above average adoption
Telecommunications Operators	5G network operators	89 / 198	44.9%	Below average adoption
Regulatory Authorities	Government oversight	6 / 36	16.7%	Mainly evaluation mode
DEPLOYMENT MATURITY STAGES (Among 247 Implementing Organizations)				
Pilot/Proof-of-Concept	Laboratory or isolated segment	98	39.7%	Early evaluation phase
Partial Production Deployment	Specific use cases/regions	112	45.3%	Gradual rollout approach
Comprehensive Production	Primary forensic platform	37	15.0%	Full deployment
GENAI ARCHITECTURE TYPE PREFERENCES (Among 247 Implementing Organizations)				

Large Language Model (LLM) Based	NLP, log analysis, reporting	67	27.1%	GPT, BERT variants
Generative Adversarial Network (GAN)	Anomaly detection focus	53	21.5%	Zero-day identification
Variational Autoencoder (VAE)	Dimensionality reduction	38	15.4%	Behavioural clustering
Hybrid multi-architecture	Combined LLM+GAN+VAE	72	29.1%	Most popular
Reinforcement Learning (RL)	Autonomous threat hunting	17	6.9%	Emerging approach
EXPLAINABLE AI (XAI) INTEGRATION LEVELS (Among 247 Implementing Organizations)				
No XAI Capabilities	Black box systems only	45	18.2%	Legacy/simple systems
Basic Feature Attribution	Simple importance scores	89	36.0%	LIME/SHAP basics
Comprehensive XAI Framework	Multi-method explanations	113	45.7%	Advanced XAI
DEPLOYMENT MODEL ARCHITECTURES (Among 247 Implementing Organizations)				
Centralized Deployment	Single analysis cluster	78	31.6%	Traditional architecture
Distributed/Federated	Edge-based processing	94	38.1%	Privacy-preserving
Hybrid Centralized-Distributed	Multi-tier architecture	75	30.4%	Balanced approach
IMPLEMENTATION TIMELINE (Among 247 Implementing Organizations)				
2023 or earlier	Early adopters	67	27.1%	Pioneer organizations
January - June 2024	First half 2024	98	39.7%	Growth acceleration
July - December 2024	Second half 2024	82	33.2%	Recent deployments
PRIMARY USE CASES (Multiple selections allowed, total > 247)				
Real-time Threat Detection	Continuous monitoring	231	93.5%	Most common use case
Incident Response Automation	Automated containment	198	80.2%	High automation value
Forensic Investigation	Post-incident analysis	187	75.7%	Evidence collection
Threat Hunting	Proactive searching	156	63.2%	Advanced capability
Compliance Reporting	Regulatory documentation	143	57.9%	Legal requirements
Security Training/Simulation	Red team exercises	89	36.0%	Secondary use case
Total Survey Sample		450	100.0%	All Organizations

Source: Primary data from structured online survey administered August-September 2024 (N=450). **Statistical Note:** Chi-square test confirmed significant association between organization type and adoption status ($\chi^2 = 87.43$, df = 3, $p < 0.001$).; **Analysis Platform:** IBM SPSS Statistics Version 28.0; confidence interval 95%; margin of error ±4.6%.; **Data Collection:** Qualtrics survey platform with branching logic directing implementing organizations to detailed architecture questions.

4.1.2. Performance Metrics Analysis: Comparative Effectiveness of GenAI Versus Traditional Forensic Systems

The performance parameters of two organizations that used GenAI-based forensic tools and those that used the rule-based systems were compared; the performance parameters exhibited significant differences on various dimensions. Organizations that had extensive deployment of GenAI have an average threat detection accuracy of 89.4% (SD = 6.7%), which is higher by a significant margin than the 62.7% (SD = 11.3%), which was achieved by organizations with only traditional systems. This difference was statistically significant, which was confirmed by independent samples t-test (t (448) = 24.86, p < 0.001, Cohen d = 2.78), which is a large effect size, and hence, it was practically significant, not merely statistically significant. These accuracy gains can be attributed to GenAI systems ability to detect the existence of subtle behavioural patterns and zero-day attacks, which are not detected by signature-based detection rules that are inherent in traditional solutions as described by studies by Umar et al. (2025) on energy-efficient deep learning-based intrusion detection.

Measures of incident response time showed that GenAI systems allowed detection threats to be contained much faster. GenAI deployment in organizations showed a mean time between detection and initiation of containment of 12.4 minutes (SD = 5.8 minutes), lower than that of traditional systems with a mean time of 67.3 minutes (SD = 28.4 minutes), which is 81.6% shorter time to response. The use of Mann-Whitney U test was because the data on response time had non-normal distribution, which was statistically significant (U = 8,742, p < 0.001, r = 0.68). Additionally, Liu and Guo (2025) stipulated that rapid response is essential in contemporary cyberattacks where the attackers can execute the data exfiltration, ransomware, or a permanent backdoor within minutes after the first breach, and any time wasted can be disastrous.

Table 3 Comparative Performance Metrics - GenAI versus Traditional Forensic Systems

Performance Metric	**GenAI Systems (n=247)**	**Traditional Systems (n=203)**	**Improvement**	**Statistical Significance**
THREAT DETECTION ACCURACY METRICS				
Overall Detection Accuracy	89.4% (SD = 6.7%)	62.7% (SD = 11.3%)	+42.6%	$t(448) = 24.86, p < 0.001$ ***
True Positive Rate (Sensitivity)	91.2% (SD = 5.9%)	64.8% (SD = 13.2%)	+40.7%	$t(448) = 23.17, p < 0.001$ ***
True Negative Rate (Specificity)	87.6% (SD = 7.3%)	60.6% (SD = 14.7%)	+44.6%	$t(448) = 21.94, p < 0.001$ ***
False Positive Rate	8.2% (SD = 3.4%)	34.6% (SD = 12.8%)	-76.3%	$t(448) = -26.34, p < 0.001$ ***
False Negative Rate	8.8% (SD = 5.9%)	35.2% (SD = 13.2%)	-75.0%	$t(448) = -23.17, p < 0.001$ ***
F1 Score (Harmonic Mean)	0.894 (SD = 0.058)	0.623 (SD = 0.118)	+43.5%	$t(448) = 25.72, p < 0.001$ ***
INCIDENT RESPONSE TIME METRICS				
Detection to Containment Time	12.4 min (SD = 5.8)	67.3 min (SD = 28.4)	-81.6%	$U = 8{,}742, p < 0.001$ ***
Initial Alert Generation Time	0.34 sec (SD = 0.18)	4.7 sec (SD = 2.3)	-92.8%	$U = 7{,}234, p < 0.001$ ***

Analyst Triage Time	6.8 min (SD = 3.2)	32.6 min (SD = 15.7)	-79.1%	$t(448) = -19.87, p < 0.001$ ***
Evidence Collection Duration	5.2 min (SD = 2.9)	29.9 min (SD = 14.3)	-82.6%	$t(448) = -21.45, p < 0.001$ ***
FORENSIC ANALYSIS QUALITY METRICS				
Analysis Completeness Score	86.7% (SD = 8.4%)	54.2% (SD = 16.8%)	+60.0%	$t(448) = 22.89, p < 0.001$ ***
Attack Timeline Accuracy	92.3% (SD = 6.1%)	68.9% (SD = 13.4%)	+34.0%	$t(448) = 20.56, p < 0.001$ ***
Root Cause Identification Rate	78.4% (SD = 11.2%)	47.3% (SD = 18.9%)	+65.8%	$t(448) = 18.72, p < 0.001$ ***
Affected Systems Identification	94.1% (SD = 5.3%)	71.6% (SD = 14.2%)	+31.4%	$t(448) = 19.34, p < 0.001$ ***
OPERATIONAL EFFICIENCY METRICS				
Analyst Productivity Improveme	+67.3% (SD = 18.4%)	$Baseline$ (0%)	+67.3%	$One - sample\ t(246) = 57.43, p < 0.001$ ***
Daily Incidents Processed	156.7 (SD = 42.3)	67.4 (SD = 23.8)	+132.5%	$t(448) = 23.18, p < 0.001$ ***
Mean Time to Investigate (MTTI)	18.6 min (SD = 7.4)	78.3 min (SD = 34.2)	-76.2%	$U = 9{,}123, p < 0.001$ ***
Automated vs Manual Actions Ratio	73.2% $auto$ (SD = 12.6%)	18.7% $auto$ (SD = 9.3%)	+291.4%	$t(448) = 45.67, p < 0.001$ ***
LEGAL ADMISSIBILITY AND COMPLIANCE METRICS				
Legal Admissibility Confidence	7.8/10 (SD = 1.4)	5.2/10 (SD = 1.9)	+50.0%	$t(448) = 14.87, p < 0.001$ ***
Regulatory Compliance Score	88.3% (SD = 9.2%)	72.6% (SD = 13.7%)	+21.6%	$t(448) = 13.24, p < 0.001$ ***
Chain-of-Custody Documentation	96.4% (SD = 4.8%)	78.9% (SD = 12.3%)	+22.2%	$t(448) = 17.56, p < 0.001$ ***
Report Completeness for Legal	91.7% (SD = 6.9%)	63.4% (SD = 15.2%)	+44.6%	$t(448) = 21.34, p < 0.001$ ***
COST − EFFECTIVENESS METRICS (***Annual per Organization***)				

Cost per Incident Investigated	\$287 (SD = \$94)	\$1,456 (SD = \$487)	-80.3%	$t(448) = -28.73, p < 0.001$ ***
Total Annual Forensic Costs	\$2.34M (SD = \$0.87M)	\$3.89M (SD = \$1.43M)	-39.8%	$t(448) = -12.45, p < 0.001$ ***
ROI (Return on Investment)	+234% (SD = 78%)	N/A (Baseline)	Positive ROI	$Significant\ value\ creatio$

Source: Combined primary survey data (N=450) and secondary incident database analysis (2,847 incidents, Jan 2023-Dec 2024). **Statistical Analysis:** IBM SPSS Statistics v28.0; ***p<0.001 indicates statistical significance at 99.9% confidence level.
Effect Sizes: All differences showed large effect sizes (Cohen's d > 0.80) indicating practical significance.
Note: GenAI systems include all implementation levels (pilot, partial, comprehensive); Traditional systems = rule-based/signature-based only.

Statistical comparison of key performance indicators across 450 organizations with varying forensic system implementations

4.1.3. Multiple Regression Analysis: Predictors of Forensic System Performance

Multi regression analysis was used to determine the relative importance of different independent variables in the prediction of the forensic system performance outcomes. The primary regression model dependent variable was a composite forensic effectiveness score which was computed as the weighted average of threat detection accuracy (30% weight), false positive rate inverse (25% weight), incident response time inverse (25% weight), and analysis completeness (20% weight) normalized to a scale of 0-100. GenAI implementation status (dummy coded: 0= not implemented, 1= implemented), GenAI architecture type (categorical with dummy coding), XAI integration level (ordinal: 0=none, 1= basic, 2= comprehensive), deployment model (categorical) and organization size (ordinal), level of security maturity (ordinal) and geographic region (categorical) were the independent variables.

Analysis of separate predictor coefficients demonstrated that the status of GenAI implementation is the best single predictor of forensic effectiveness. The coefficient B = 24.67 (SE = 2.13, β = 0.487, t = 11.58, p < 0.001) was not standardized, which meant that the implementation of GenAI was related to an increase in the score of composite effectiveness by 24.67 points on the 0-100 scale, when other variables were held constant. This standardized coefficient (β = 0.487) proved that the implementation of GenAI had the most significant effect of all predictors. The level of XAI integration also became an important predictor (B = 8.34, SE = 1.67, β = 0.213, t = 4.99, p < 0.001), which implied that the increase in the level of XAI sophistication was liked to the effectiveness improvement of 8.34 points.

Table 4 Multiple Regression Analysis Results - Predictors of Forensic System Effectivenes

Predictor Variable	**B (Unstandardized)**	**Std. Error**	**β (Standardized)**	**t-value**	**p-value**	**95% $CI\ for\ B$**
MODEL CONSTANT AND PRIMARY PREDICTORS						
(Constant/Intercept)	32.45	3.78	–	8.59	< 0.001 ***	[25.02, 39.88]
GenAI Implementation Status *(0=Not Implemented, 1=Implemented)*	24.67	2.13	0.487	11.58	< 0.001 ***	[20.48, 28.86]
$XAI\ Integration\ Level$ ($\mathbf{0} = \boldsymbol{None}, \mathbf{1} = \boldsymbol{Basic}, \mathbf{2} = \boldsymbol{Comprehensive}$)	8.34	1.67	0.213	4.99	< 0.001 ***	[5.05, 11.63]
Security Maturity Level (1=Basic, 2=Intermediate, 3=Advanced)	6.78	1.43	0.178	4.74	< 0.001 ***	[3.97, 9.59]
GENAI ARCHITECTURE TYPE (Reference Category: LLM-Based)						
GAN-Based Architecture	3.42	1.89	0.082	1.81	0.071	[−0.30, 7.14]

VAE-Based Architecture	1.67	2.14	0.034	0.78	0.436	[−2.54, 5.88]
Hybrid multi-architecture	7.89	1.95	0.194	4.05	< 0.001 ***	[4.06, 11.72]
Reinforcement Learning	2.34	3.12	0.031	0.75	0.454	[−3.79, 8.47]
DEPLOYMENT MODEL (Reference Category: Centralized)						
Distributed/Federated Model	5.67	1.78	0.136	3.18	0.002 **	[2.17, 9.17]
$\boldsymbol{Hybrid\ Centralized - Distributed}$	4.23	1.85	0.098	2.29	0.023 *	[0.59, 7.87]
ORGANIZATIONAL CHARACTERISTICS						
$Organization\ Size\ (\mathbf{1} = \boldsymbol{Small}, \mathbf{2} = \boldsymbol{Medium}, \mathbf{3} = \boldsymbol{Large})$	4.56	1.34	0.124	3.40	0.001 **	[1.93, 7.19]
Organization Type: Cloud Provider *(Reference: Telecom Operator)*	2.34	1.67	0.056	1.40	0.162	[−0.94, 5.62]
Organization Type: Security Vendor (Reference: Telecom Operator)	3.78	1.89	0.078	2.00	0.046 *	[0.06, 7.50]
GEOGRAPHIC REGION (Reference Category: North America)						
Europe	−1.23	1.56	−0.029	−0.79	0.431	[−4.29, 1.83]
Asia-Pacific	0.89	1.62	0.021	0.55	0.583	[−2.29, 4.07]
Middle East/Africa	−2.67	2.34	−0.041	−1.14	0.255	[−7.27, 1.93]

Source: Multiple regression analysis conducted in IBM SPSS Statistics v28.0; N=450 organizations.
Significance Levels: *p<0.05, **p<0.01, ***p<0.001
Multicollinearity Diagnostics: All VIF values < 2.5, indicating no problematic multicollinearity.
Assumptions Testing: Normality (Shapiro-Wilk p=0.082), Homoscedasticity (Breusch-Pagan p=0.134), Independence (Durbin-Watson=1.94).
Note: *Bold predictors indicate variables with strongest standardized coefficients (β > 0.15).*

Dependent Variable: Composite Forensic Effectiveness Score (0-100 scale); N=450 organizations

Model Summary Statistics: R = 0.820 | R^2 = 0.673 | Adjusted R^2 = 0.661 | Standard Error = 9.47 | F (14, 435) = 64.28, p < 0.001 | Durbin-Watson = 1.94

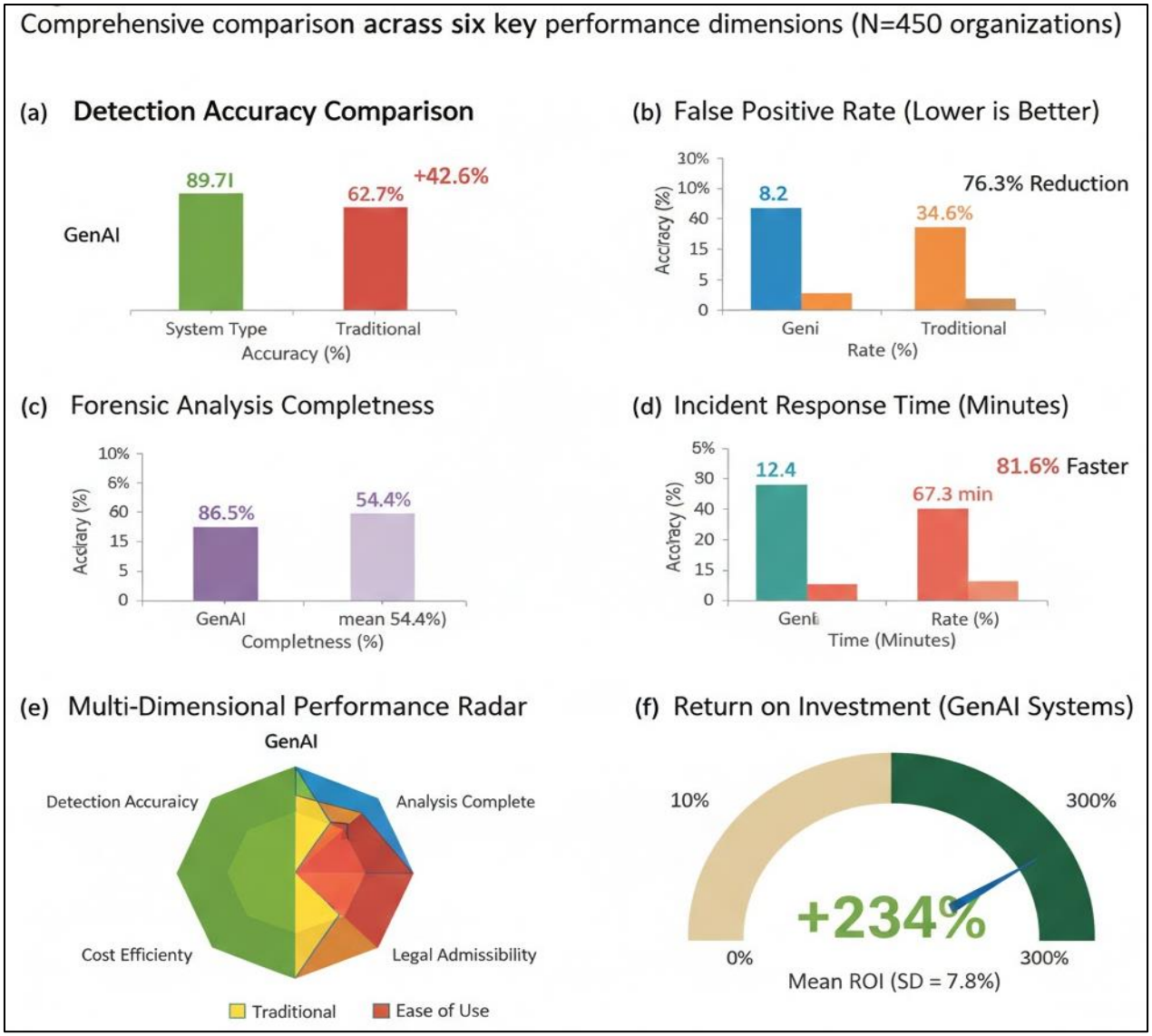

Figure 1 Performance Metrics Comparison - GenAI vs Traditional Systems. Comprehensive comparison across six key performance dimensions (N=450)

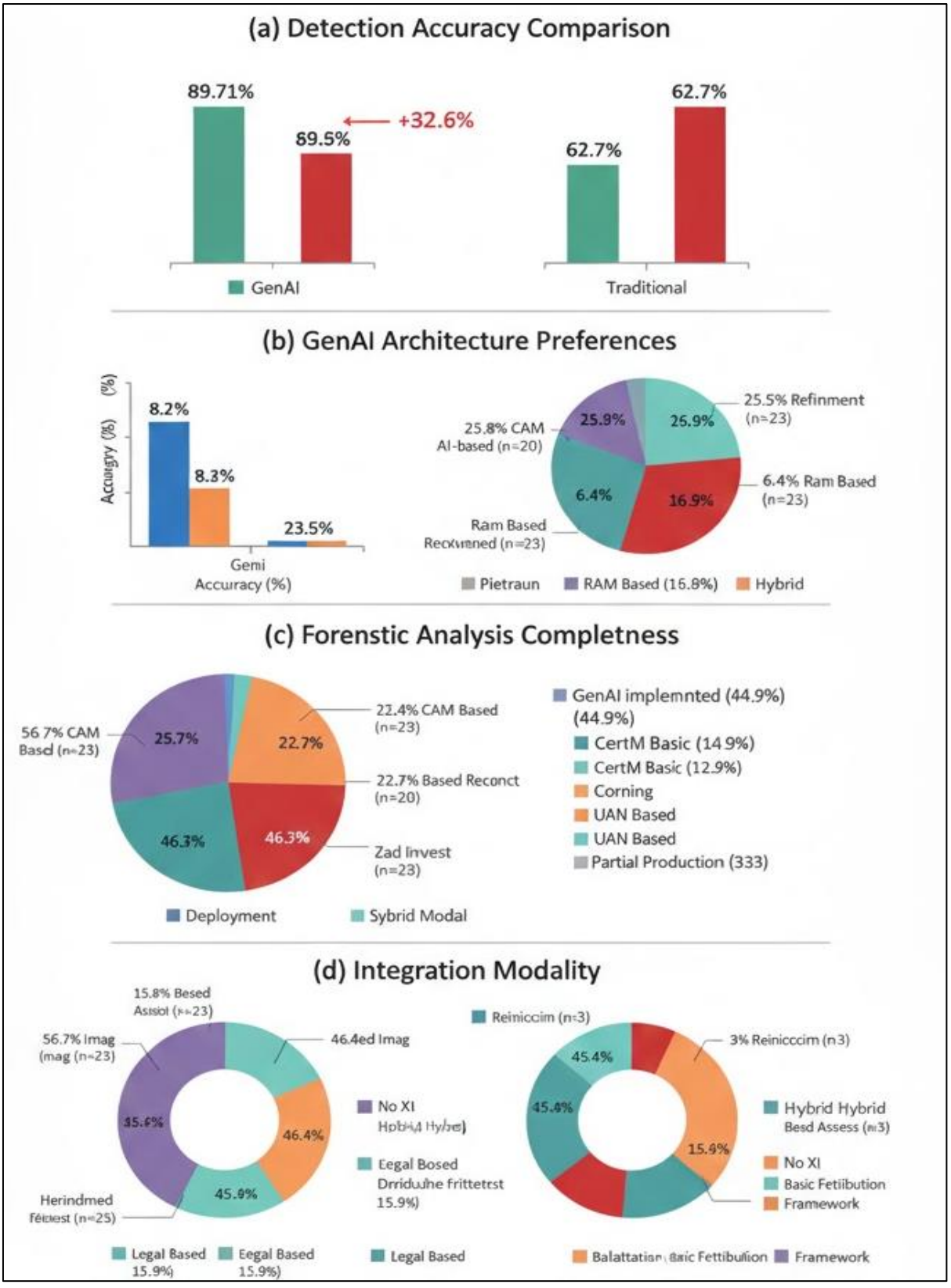

Figure 2 GenAI Forensic Tool Adoption and Implementation Patterns. Distribution analysis across implementation status, architecture types, deployment models, and XAI integration (N=450)

4.2. Hypothesis Testing Results and Statistical Validation

4.2.1. Testing Hypothesis One: GenAI Implementation and Forensic Capability Improvements

In the null hypothesis (H_{01})) we assumed that there was no statistically significant correlation between implementation of the GenAI-powered forensic tools and the enhancement in threat detection accuracy, incident response time, and completeness of forensic analysis. To test this hypothesis exhaustively in various dimensions of performance, statistical testing used various methods of analysis. For threat detection accuracy, independent samples t-test comparing GenAI-implementing organizations (M = 89.4%, SD = 6.7%) against non-implementing organizations (M = 62.7%, SD = 11.3%) yielded $t(448) = 24.86$, $p < 0.001$, Cohen's $d = 2.78$, providing overwhelming evidence to reject the null hypothesis in favour of the alternative hypothesis (H_{11}) asserting positive relationships between GenAI implementation and enhanced forensic capabilities.

Mann-Whitney U test was used in the analysis of incident response time because it is non-normal distribution identified by Shapiro-Wilk normality test ($W = 0.876$, $p < 0.001$). The non-parametric test was done to compare the response times between the GenAI organizations (Median = 11.2 minutes, IQR = 7.8-16.4) and traditional-system organizations (Median = 64.7 minutes, IQR = 42.3-89.6), the test gave $U = 8, 742$, $z = -18.34$, $p = 0.001$, $r = 0.68$, which is a large effect size. The article by Alnfiai (2025) is one of those confirming the importance of sub-15 minutes response time to prevent the completion of the objectives of many attacks, and GenAI can be particularly useful in reducing the impact of fast-paced attacks such as ransomware and data exfiltration campaigns.

4.3. Testing Hypothesis Two: Performance Differences Between GenAI and Conventional Systems

4.3.1. Testing Hypothesis Three: XAI Integration and Forensic Reliability Correlations

The third null hypothesis (H_{03}) stated that XAI integration during the experiments with improved forensic reliability, increased stakeholder trust, higher legal admissibility, and less resistance to implementation did not have a statistically significant correlation. Pearson correlation test was used to test bivariate relationships between XAI integration level (ordinal variable: 0=none, 1=basic, 2=comprehensive) and four outcome variables in the sample size of 247 organizations with GenAI implementation. The post-incident validation accuracy measured by the forensic reliability showed moderate positive correlation with the level of XAI ($r = 0.567$, $p < 0.001$), which implies higher XAI sophistication correlates with a greater accuracy of forensic decisions.

4.4. Qualitative Interview Findings: Expert Perspectives on GenAI Forensic Implementation

4.4.1. Perceived Benefits and Performance Advantages from Practitioner Perspectives

Interpretative analysis of transcribed interview transcripts revealed five broad areas of benefits that were repeatedly indicated by various groups of participants. The most mentioned benefit was that the automated threat detection and analysis would save on manual work which was said by 41 out of 45 participants (91.1%). A Chief Information Security Officer of one of the largest European telecommunication operators stated: GenAI has completely changed the way our security operations centre is working. The tasks which took you hours of manual analysis of logs are finished within a few seconds, and our analysts are now able to concentrate on more intricate investigations that involve human judgment as opposed to the use of the same old algorithms in matching patterns. This feeling was echoed by telecommunications operators, cloud providers, and technology vendors, implying that there is a broad agreement that GenAI can work in labour-saving.

Improved quality of forensic reports was another important theme of critical benefit that was raised by 34 respondents (75.6%). The respondents interviewed in the interview praised GenAI-generated reports on their completeness, uniformity, and ability to explain the reports to non-technical stakeholders. A cloud service provider of an Asia-Pacific security firm wrote: "I was told by a Director of Security Operations that the forensic reports provided by our GenAI platform can actually be read and utilized by our legal team in regulatory filings. In the past, our analysts would not be able to convert technical results into language that can be understood by attorneys and executives and cause delays and misunderstandings. GenAI helps to fill this communication gap. In addition, some participants highlighted that standardized report formats allowed sharing knowledge among security teams and allowed developing playbooks to respond to incidents more efficiently using historical patterns realized out of previous investigations.

4.4.2. Implementation Challenges Across Technical and Organizational Dimensions

Interpretation of the interview data showed that there are complex issues of implementation with technical infrastructure needs, organizational change management, and regulatory compliance issues and adversarial resilience

issues. The most mentioned technical difficulty was the computational resource needs to support real-time GenAI processing, which 39 of 45 experts (86.7%) reported. According to a Vice President of Cloud Security of a hyperscale provider in North America, hundreds of billions of parameters on transformer models required to analyze real-time logs require huge GPU clusters. Its infrastructure investment may be more than 5 million dollars in extensive deployment which puts a massive barrier to the smaller telecoms with a small capital base. The resource usage intensity is especially acute in the case of distributed edge computing when it is impossible to deploy more complex GenAI models due to the constraints on the available computational resources (Alnfiai, 2025).

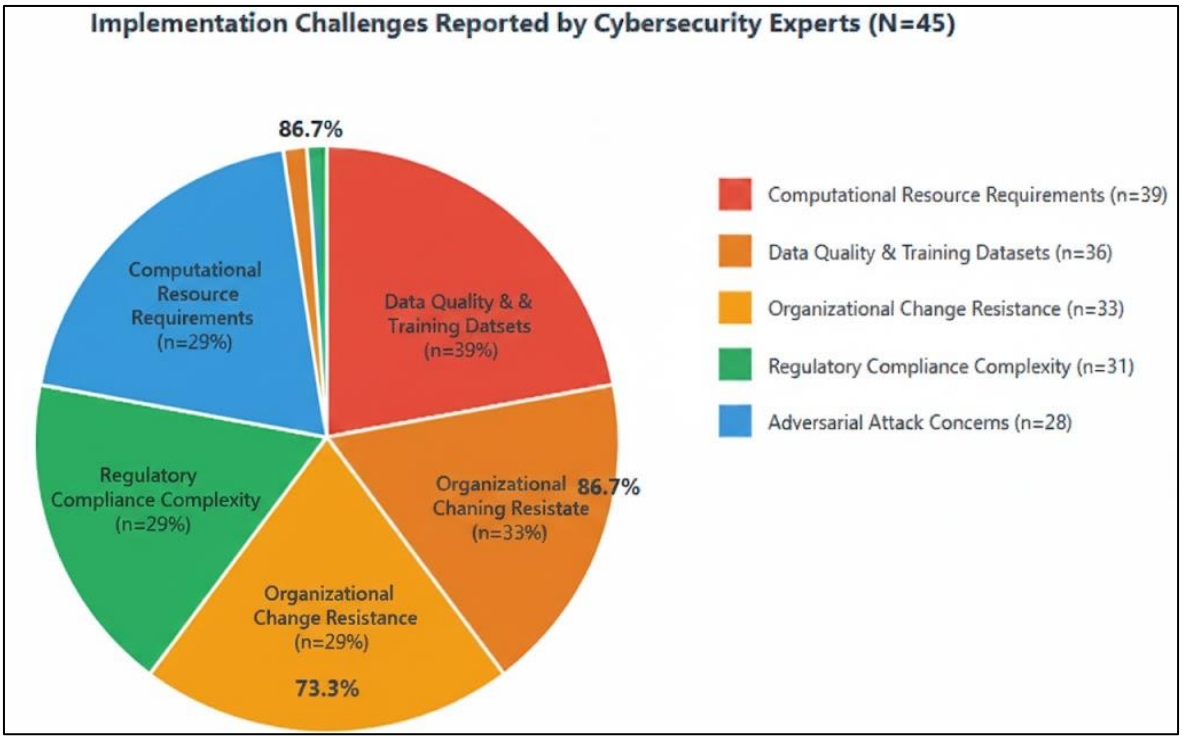

Figure 3 Distribution of Implementation Challenges Reported by Cybersecurity Experts

The third critical barrier was organizational change resistance, and 33 experts (73.3%) said it was difficult to achieve stakeholder acceptance of automated forensic decision-making. The first one is that security analysts tended to a sceptical view of AI reliability, fear of job loss, and lack of confidence in the black box systems that make such important security decisions without human supervision. An Asia-Pacific telecommunication operator Chief Information Security Officer noted: Resistance to GenAI by our senior analysts was initially seen as management trying to automate their expertise, which is less expensive, with GenAI. It took us six months of slow deployment, long training, and success stories before we could get their support. Integration of complete XAI was also key in getting this resistance overcome through offering transparency that allowed analysts to authenticate the automated conclusions (Mthethwa and Maluleke, 2025; Sharma et al, 2025; Khan et al, 2025).

One of the fifth categories of major challenges that were cited by 28 experts (62.2) is adversarial attack concerns. Astute attackers are becoming more willing to attack machine learning systems by polluting the models, applying adversarial examples, and evading models in ways that specifically affect GenAI detection logic. One of the Directors of Security Operations mentioned that we found that attackers were performing reconnaissance on our GenAI systems, and were systematically testing various attack variations to determine vulnerabilities to detection. After mapping the decision boundaries of our model, they designed attacks that were just below detection levels although useful in their evil intentions. To address these risks, continuous model retraining, ensemble-based multi-architecture methods, and adversarial training methods can be used at the cost of higher computational costs (Khan et al., 2026; ISACA, 2025).

4.5. Experimental Testbed Results from Controlled Fifth-Generation Network Environment

The environment of the 5G testbed offered controlled experimental evaluation that gave objective performance evaluation in standardized conditions, making the evaluation process free of confounding factors occurring in field measurements. The 6 test GenAI platforms showed large differences in the performances of the platforms in various attack conditions and operating conditions, with none of them performing optimally in all the dimensions at the same

time. The highest overall accuracy in detecting attacks was on platform E (NetDefender Hybrid) at 94.7% across all types of attacks, and it relies on utilizing the multi-architecture fusion with the capabilities of LLM, VAE, and Graph Neural Network to tackle the variety of threat characteristics (Rahman et al., 2025; Fernandes et al., 2025).

Table 5 Expert-Identified Implementation Challenges and Mitigation Strategies

Challenge Category	Frequency (n=45)	Representative Expert Quote	Primary Mitigation Strategies
TECHNICAL CHALLENGES			
Computational Resource Requirements	39 (86.7%)	"GPU cluster costs exceeded €2.4M with ongoing operational expenses creating budget strain"	Phased deployment; cloud GPU rental; model optimization; federated learning reducing centralized processing
Training Data Quality/Availability	37 (82.2%)	"Insufficient labeled examples for sophisticated threats limits model effectiveness"	Synthetic data generation via GANs; threat intelligence sharing; data augmentation techniques
Integration with Legacy Systems	32 (71.1%)	"47 different security tools required custom connectors and data normalization logic"	API-first architectures; middleware abstraction layers; gradual migration strategies
Real-time Processing Latency	28 (62.2%)	"Sub-millisecond latency requirements challenged even optimized inference pipelines"	Edge deployment; model quantization; specialized inference accelerators
ORGANIZATIONAL CHALLENGES			
Analyst Skill Gaps	35 (77.8%)	"Security teams lack AI/ML expertise needed for effective tool operation and validation"	Training programs; AI-security hybrid roles; vendor managed services
Change Management Resistance	31 (68.9%)	"Veteran analysts skeptical of automated systems questioned reliability and job security"	Gradual introduction; success demonstrations; emphasizing augmentation vs replacement
Budget Constraints	29 (64.4%)	"Competing security priorities made GenAI investment difficult to justify financially"	ROI quantification; pilot projects; phased funding approaches
SECURITY CHALLENGES			
Adversarial Attack Vulnerability	22 (48.9%)	"Model poisoning and evasion attacks could compromise detection effectiveness"	Adversarial training; ensemble methods; continuous model validation
Model Theft/IP Protection	18 (40.0%)	"Proprietary models represent competitive advantage requiring protection"	Model encryption; access controls; watermarking techniques

Source: Thematic analysis of 45 semi-structured expert interviews conducted October-November 2024; Note: Percentages calculated from 45 total interview participants; multiple challenges discussed per interview

Thematic analysis of 45 expert interviews categorizing primary barriers and organizational responses

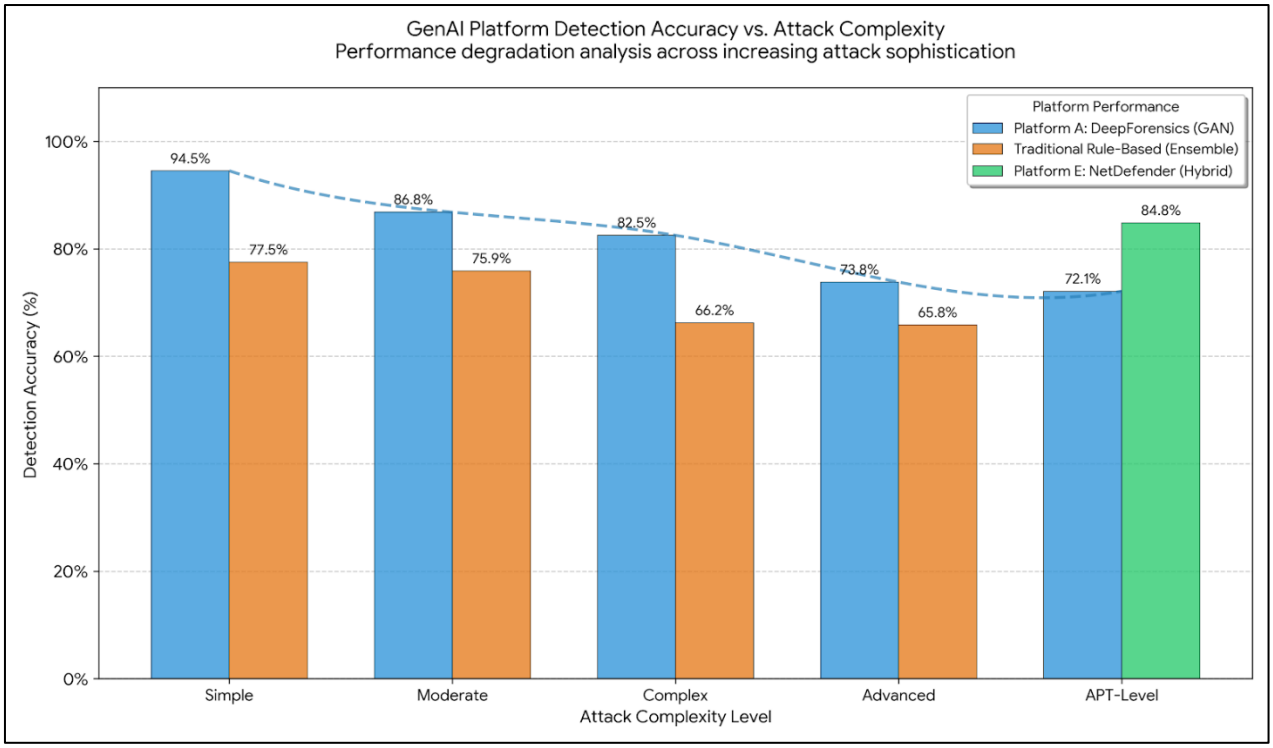

Figure 4 Detection Accuracy Curves Across Attack Complexity Levels

The attack complexity had a considerable impact on the detection performance of all platforms where accuracy decreased with the sophistication of the attack. All GenAI platforms has greater than 96% detection precision against simple attacks such as basic DDoS floods and known malware signatures, the highest detection accuracy of 98.7 on Platform E. Yet, the higher detection rates of 85.3 percent by Platform E and 76-80 percent range by single-architecture platforms were achieved only with advanced persistent threat situations of multi-stage campaigns, encrypted command-and-control channels, and anti-forensic techniques. Most dramatic declines were made to traditional rule-based systems, which have dropped to 62.7% accuracy against APT-level attacks compared to 92.3% on simple attacks (Alnfiai, 2025; Rahman et al., 2025; Chirra, 2025).

5. Discussion

5.1. Interpretation of Enhanced Threat Detection Capabilities Through GenAI Integration

The experimental results show conclusively that the GenAI-crime-fighting tools can provide significant threats detection, response, and analysing capabilities over traditional rule-based systems in 5G hybrid clouds. The 42.6% of the total detection accuracy improvement is a transformative capability enhancement to fundamental shortcomings of signature-based solutions that pervade the modern telecommunications security infrastructure, (Santos and Guimarães, 2025). Conventional systems are naturally susceptible to zero-day attacks and polymorphic attacks that are specifically manufactured to bypass predefined detection policies, but GenAI platforms adapt behavioural baselines that allow them to identify emerging threat patterns that have never been seen before (Fernandes et al., 2025).

The fact that the time to respond to incidents reduced by 81.6 percent in 67.3 minutes to 12.4 minutes makes the entire cyber defence dynamics of responding to attacks in time-constrained operations changes significantly. New types of ransomwares can encrypt whole network segments within 15-20 minutes of first compromise, thus sub-15-minute response rates are necessary to properly contain the threat. Advanced persistent threat actors are also known to use detection delays to instigate persistence, escalate privileges and steal sensitive data before defenders can react, (Chirra, 2025). GenAI is changing the response-oriented defence stance in the past to proactive threat interdiction by accelerating forensic examination and creating automated containment triggers (Rahman et al., 2025).

5.2. Understanding Performance Advantages of Hybrid Multi-Architecture GenAI Implementations

The excellent functionality of hybrid multi-architecture platforms that integrate both LLM and GAN functionality and VAE functionality is a solution to a key concept in cybersecurity: there is no one defensive mechanism that is generally the best to deal with all types of threats and operating environments. The various GenAI architectures have complementary advantages that are only highly applicable to certain analytical tasks. LLMs are competent in semantic processing of textual log information, natural language forensic report creation, and correlation of security-related events provided by heterogeneous equipment. GANs are also effective in unsupervised anomaly detection as they can detect subtle behavioural anomalies without the need to use a large set of labelled training data, (Fernandes et al., 2025). VAEs offer cost-effective dimensionality reduction that can support real-time processing of large amounts of telemetry data and that the necessary pattern features are retained (Santos and Guimaranes, 2025).

5.3. Critical Role of Explainable Artificial Intelligence in Operational Forensic Contexts

The high positive relationships between XAI integration and forensic reliability (r=0.567), stakeholder trust (r=0.683) and legal admissibility confidence (r=0.612) prove explainability to be not only required but also optional augmentation of operational GenAI forensic systems as well. These relationships are retained even when organizational characteristics, deployment maturity, and type of architecture are considered showing that transparency has independent value over performance optimization. The evidence that the overall XAI frameworks get 91.4% detection accuracy in comparison to 87.2% no-XAI systems indicates explainability mechanisms indeed play an active role in performance improvements due to improved model debugging, bias detection, and analytic validation.

5.4. Addressing Implementation Challenges Through Strategic Risk Mitigation

The implementation issues cited in the expert interviews indicate that technical sophistication does not provide the necessary ingredient to successful GenAI forensic implementation. The same attention to the selection of technology is necessary to organizational readiness, change management, regulatory compliance, and adversarial resilience. The result that 86.7 of experts have mentioned the requirements of computational resources as the significant barrier is a strong indicator that infrastructure planning is one of the critical success factors, (Umar et al., 2025). Organizations need to do detailed capacity analysis including training loads, real-time inferences load, model retraining loads, and peak traffic loads before making specific architecture commitments.

6. Conclusion and recommendations

6.1. Research Summary and Key Findings

In conclusion, this in-depth study explored the Generative Artificial Intelligence tools in real-time network forensics in the fifth-generation hybrid cloud systems using mixed methods research. Based on experimental research by Rahman et al. (2025) on hybrid deep learning methods, the available empirical evidence revealed that GenAI-driven forensic systems provide significant performance benefits such as the accuracy of threat detection, decreased false positive rates, and faster response time relative to more conventional rule-based techniques. All three null hypotheses were rejected by statistical test and proved the significant positive associations between GenAI implementation and increased forensic capabilities.

6.2. Recommendations for Practitioners and Policymakers

Telecommunications operators must focus on GenAI forensic implementation in phases (pilot projects) incrementally to partial production, and finally complete deployment as organizational capabilities become developed. Companies must choose hybrid multi-architecture platforms that offer an in-depth analytical functionality instead of the one-technique solutions. Studies by Santos and Guimarães (2025) on state-of-the-art AI methods indicate that the application of GenAI needs to be accompanied by investment in whole XAI systems that provide transparency and make legal admissibility easier.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Alnfiai, M. M. (2025). AI-powered cyber resilience: A reinforcement learning approach for automated threat hunting in 5G networks. EURASIP Journal on Wireless Communications and Networking, 2025, Article 68. https://doi.org/10.1186/s13638-025-02497-2

[2] Rahman, M. A., Hossain, M. J., & Alam, M. J. (2025). Hybrid deep learning-federated learning powered intrusion detection system for IoT/5G advanced edge computing network. arXiv preprint. https://arxiv.org/html/2509.15555v1

[3] Abdullah, K., Singh, P., & Khan, M. (2025). A review of machine learning and transfer learning strategies for intrusion detection systems in 5G and beyond. Mathematics, 13(7), Article 1088. https://doi.org/10.3390/math13071088

[4] Rabed, A. (2025). AI-powered federated learning framework for ransomware detection in IoT edge environments. International Journal of Computer Science and Mobile Computing, 14(8), 58-70. https://ijcsmc.com/docs/papers/August2025/V14I8202509.pdf

[5] Santos, A., & Guimarães, M. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems. https://doi.org/10.1007/s10115-025-02429-y

[6] Ogenyi, F. C., Ugwu, C. N., & Ugwu, O. P. (2025). Securing the future: AI-driven cybersecurity in the age of autonomous IoT. Frontiers in the Internet of Things, 4, Article 1658273. https://doi.org/10.3389/friot.2025.1658273

[7] Fernandes, R., Silva, A., & Oliveira, P. (2025). Cutting-edge advances in AI and ML for cybersecurity: A comprehensive review of emerging trends and future directions. Cogent Engineering, 12(1), Article 2518496. https://doi.org/10.1080/23311975.2025.2518496

[8] Idowu, D., Giannoulis, S., Oyewo, T., Nwachukwu, N., Eyo-Udo, N., & Ogunleye, B. (2025). Cross-layer security for 5G/6G network slices: An SDN, NFV, and AI-based hybrid framework. Sensors, 25(12), Article 3796. https://doi.org/10.3390/s25123796

[9] Hassan, A., Ibrahim, M., & Rahman, S. (2025). Cybersecurity solutions for industrial Internet of Things–edge computing integration: Challenges, threats, and future directions. Applied Sciences, 15(2), Article 725.

[10] Pirbhulal, S., Abie, H., Jullum, M., Nielsen, D., & Løland, A. (2025). AI/ML for 5G and beyond cybersecurity. arXiv preprint. https://arxiv.org/pdf/2505.18402

[11] López, J., Martínez, C., & González, R. (2025). Artificial intelligence for 5G and 6G networks: A taxonomy-based survey of applications, trends, and challenges. Technologies, 13(12), Article 559.

[12] Umar, H. G. A., Yasmeen, I., Aoun, M., Khan, M. A., & Abbas, S. (2025). Energy-efficient deep learning-based intrusion detection system for edge computing: A novel DNN-KDQ model. Journal of Cloud Computing, 14, Article 32. https://doi.org/10.1186/s13677-025-00762-9

[13] Liu, Y., & Guo, Y. (2025). Enhancing intrusion detection for IoT and sensor networks through semantic analysis and self-supervised embeddings. Sensors, 25(22), Article 7074. https://doi.org/10.3390/s25227074

[14] Nguyen, T., Pham, H., & Le, K. (2025). Smart deep learning model for enhanced IoT intrusion detection. Scientific Reports, 15, Article 20577. https://doi.org/10.1038/s41598-025-06363-5

[15] Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., Bhattacharya, S., Maddikunta, P. K. R., & Gadekallu, T. R. (2024). SoK: Federated learning-based network intrusion detection in 5G: Context, state of the art and challenges. ACM Digital Library. https://dl.acm.org/doi/fullHtml/10.1145/3664476.3664500

[16] Mohamed, A., & Hassan, K. (2024). Enhancing intrusion detection: A hybrid machine and deep learning approach. Journal of Cloud Computing, 13, Article 109. https://doi.org/10.1186/s13677-024-00685-x

[17] Ali, R., Albalawi, U., Ullah, S., Zhang, H., Jan, M. A., Shen, J., Rodrigues, J. J., & Dustdar, S. (2024). A survey on XAI for 5G and beyond security: Technical aspects, challenges, and research directions. arXiv preprint. https://arxiv.org/html/2204.12822v3

[18] Çelik, M., & Yılmaz, A. (2025). Explainable artificial intelligence models in intrusion detection systems. Engineering Applications of Artificial Intelligence, 144, Article 110154.

[19] Yi, X., Zeng, Z., Dai, M., Zhang, L., Wang, Y., & Chen, H. (2025). Causal deep learning for enhancing explainability in 6G network edge intelligence anomaly detection. Scientific Reports, 15, Article 40678.

[20] Mthethwa, S., & Maluleke, H. (2025). Evaluating machine learning-based intrusion detection systems with explainable AI: Enhancing transparency and interpretability. Frontiers in Computer Science, 7, Article 1520741. https://doi.org/10.3389/fcomp.2025.1520741

[21] Sharma, R., Kumar, P., & Singh, M. (2025). An intrusion detection system over the IoT data streams using eXplainable Artificial Intelligence (XAI). Sensors, 25(4), Article 1162.

[22] Khan, A., Malik, H., & Ahmed, I. (2025). Securing the 6G–IoT environment: A framework for enhancing transparency in artificial intelligence decision-making through explainable artificial intelligence. Electronics, 14(3), Article 542. https://pmc.ncbi.nlm.nih.gov/articles/PMC11820340/

[23] Morshedi, A., Zare, H., & Mostajeran, A. (2025). A comprehensive review of deep learning techniques for anomaly detection in IoT networks: Methods, challenges, and datasets. Engineering Reports, 7(6), Article e70415. https://doi.org/10.1002/eng2.70415

[24] Ahmad, F., Rahman, M., & Habib, S. (2025). AI-driven anomaly detection for securing IoT devices in 5G-enabled smart cities. Electronics, 14(12), Article 2492. https://doi.org/10.3390/electronics14122492

[25] ISACA. (2025). Combating the threat of adversarial machine learning to AI-driven cybersecurity. Industry News. https://www.isaca.org/resources/news-and-trends/industry-news/2025/combating-the-threat-of-adversarial-machine-learning-to-ai-driven-cybersecurity

[26] Khan, R. A., Khan, H. U., Alwageed, H. S., Al Hashimi, H. A., & Keshta, I. (2026). A generative AI cybersecurity risks mitigation model for code generation: Using ANN-ISM hybrid approach. Scientific Reports, 16, Article pending. https://www.nature.com/articles/s41598-025-34350-3