International Journal of Computer Applications Technology and Research
Volume 15–Issue 08, 59 – 67, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1508.1005

Task-Technology Fit and the Adoption of Cloud-Based Encryption for Digital Forensic Evidence: A Study of The Kenya National Police Service

Agnes Kyengo
Department of Computer Science, School of Science and Technology
Kenya Methodist University (KeMU)
Nairobi, Kenya

Peter Waweru
Department of Computer Science, School of Science and Technology
Kenya Methodist University (KeMU)
Nairobi, Kenya

David Munene
Department of Computer Science, School of Science and Technology
Kenya Methodist University (KeMU)
Nairobi, Kenya

Abstract: This Background: The preservation of digital forensic evidence in cloud environments presents significant challenges for law enforcement agencies in developing economies. While cloud-based encryption tools offer potential solutions, adoption remains low due to misalignment between technology capabilities and operational task requirements.
Objective: To examine the role of Task-Technology Fit (TTF) in predicting the adoption of cloud-based encryption for digital forensic evidence preservation, and to identify the specific task characteristics and technology features that influence forensic practitioners' adoption decisions.
Methods: A multiphase mixed-methods design, embedded within a Design Science Research (DSR) framework, combined a needs-assessment survey of 91 Kenya National Police Service (KNPS) and judicial practitioners with the development and evaluation of a cloud-based encryption prototype (AES-256-GCM, RSA-3072, immutable audit logs). Task-Technology Fit was operationalized as a discrepancy index between independently rated task-characteristic importance and technology-characteristic capability to reduce common-method bias. Quantitative data were analysed using descriptive statistics, ANOVA, Pearson correlations, and multiple linear regression. Qualitative open-ended responses underwent reflexive thematic analysis and were integrated with quantitative findings via a joint display. Usability testing (n=30) and a 30-day pilot deployment (n=20, no control group) evaluated the tool's operational fit.
Results: Current practices showed a procedural-technical gap: chain-of-custody logging (M=3.91/5) was adequate, but encryption use (M=3.08) and integrity hashing (M=2.63) were weak. Task-Technology Fit, operationalized as a discrepancy-based index, was the strongest predictor of adoption readiness (β=0.41, $p<.001$), explaining 38.7% of variance in adoption intentions. Judicial admissibility requirements (M=4.45) and chain-of-custody standards (M=4.38) were rated as the most critical task characteristics; encryption speed (M=4.12) and audit logging completeness (M=4.05) were rated as the most important technology characteristics. In laboratory and field evaluation, the prototype achieved 12–15% encryption overhead with zero errors over 9,000+ operations, a System Usability Scale score of 78.4 ("Good"), 30% faster task completion (Cohen's d=1.61), and was associated with an increase in encryption-log adoption from 18% to 72% over a 30-day pilot ($\chi^2(1)=28.6$, $p<.001$) without a control group. Qualitative findings indicated that the fit–adoption relationship is further shaped by infrastructure constraints, training gaps, and particularly among judiciary staff institutional trust in courts' acceptance of digitally secured evidence.
Conclusion: Task-Technology Fit is a useful framework for understanding cloud-based encryption adoption in this forensic context, though the cross-sectional, single-country, controlled-comparison-free design means these findings should be read as associations consistent with TTF theory rather than causal proof. Achieving fit in practice appears to require not only technical alignment with task requirements but also infrastructural investment, training, and engagement with judicial stakeholders whose adoption concerns are only partly explained by perceived technical fit.

Keywords: Task-Technology Fit, cloud encryption, digital forensics, Kenya National Police Service, evidence preservation, technology adoption, chain of custody

1. INTRODUCTION

The preservation of digital forensic evidence is fundamental to modern criminal justice systems. Digital evidence is now present in virtually all criminal investigations, yet its inherent fragility demands rigorous technical and procedural safeguards to maintain integrity and admissibility (Casey, 2011). Cloud computing offers scalable storage, remote accessibility, and cost efficiencies benefits that are particularly attractive to resource-constrained law enforcement agencies (Martini & Choo, 2014; Lillis et al., 2016). However, the adoption of cloud-based solutions for forensic evidence preservation remains limited, particularly in developing economies where infrastructure, training, and governance challenges persist (Kshetri, 2019).

The Kenya National Police Service (KNPS) exemplifies these challenges. Despite progressive legislation the Computer Misuse and Cybercrimes Act (2018) and the Data Protection Act (2019) law enforcement agencies in developing economies have struggled to adopt technical safeguards such as encryption, hashing, and cloud-based storage for digital evidence (Okonigene & Adekunle, 2021; Karie & Venter, 2015). Observed challenges include inconsistent application of encryption, reliance on manual chain-of-custody documentation, and limited cloud adoption (Kshetri, 2019; Sunde & Dyrkolbotn, 2019). The authors' direct professional engagement with KNPS forensic units has informed the contextual framing of this study, though general patterns observed in Kenya are consistent with documented experiences in comparable jurisdictions, as cited throughout

the literature review. No purpose-built cloud-based encryption tool has been developed or validated for KNPS's specific forensic workflows. The gap between the potential of cloud-based forensic solutions and their limited adoption in practice raises a critical question: what factors determine whether forensic practitioners will adopt cloud-based encryption tools?

Task-Technology Fit (TTF) theory (Goodhue & Thompson, 1995) offers a compelling framework for understanding this adoption gap. TTF posits that technology is more likely to be used and to improve performance when its capabilities align with the tasks users need to perform. In digital forensics, the tasks include secure evidence storage, integrity verification, audit logging, and court-admissible documentation, all subject to stringent judicial requirements and chain-of-custody rules (Garfinkel, 2010; Narasimhan & Kala, 2024). A tool that automates these tasks and fits the forensic workflow should have higher adoption potential.

This study addresses four objectives: (i) to assess the current alignment between forensic task requirements and available technology within KNPS; (ii) to identify the specific task characteristics that drive the need for cloud-based encryption; (iii) to evaluate the technology characteristics that forensic practitioners consider essential for adoption; and (iv) to develop and evaluate a cloud-based encryption prototype designed around Task-Technology Fit principles for KNPS's forensic workflows. The study is distinctive in two ways. First, it applies TTF theory to a novel context cloud-based forensic evidence preservation extending the theory's application beyond general information systems to high-stakes law enforcement environments. Second, it combines TTF-guided technical artifact development with empirical evaluation, illustrating how TTF principles can inform tool design.

2. LITERATURE REVIEW

2.1 Digital Forensics and Evidence Preservation

Digital forensics is the application of scientific methods to identify, collect, preserve, analyse, and present electronic evidence in a legally admissible manner (Casey, 2011). The field has evolved rapidly from single-computer examinations to complex cloud and virtualised environments (Lillis et al., 2016). A core principle of forensic soundness is the maintenance of a complete and unbroken chain of custody, which documents every access and transfer of evidence (Garfinkel, 2010). Traditional manual methods paper logs, unencrypted media, physical storage are increasingly inadequate for modern data volumes and the distributed nature of cloud storage.

In developing economies, law enforcement agencies face additional barriers: underfunding, poor ICT infrastructure, weak encryption tools, and insufficient training (Okonigene & Adekunle, 2021). Studies in South Africa (Karie & Venter, 2015) and Nigeria (Okonigene & Adekunle, 2021) have documented similar patterns: procedural documentation exists, but technical safeguards (encryption, hashing) are inconsistently applied. This procedural-technical gap increases the risk of evidence tampering and judicial rejection, directly undermining the effectiveness of criminal investigations.

2.2 Cloud Computing in Digital Forensics

Cloud computing offers scalable storage, remote accessibility, and cost efficiencies, which are attractive for forensic evidence management (Martini & Choo, 2014). However, cloud forensics introduces unique challenges: multi-tenancy complicates data isolation; jurisdictional data sovereignty limits storage location; loss of physical control over infrastructure hampers acquisition; and encryption key management becomes more complex (Quick & Choo, 2018; Dykstra & Sherman, 2012). The NIST Cloud Computing Forensic Science Challenges document identifies over 60 specific issues, including lack of forensic readiness in cloud service providers and difficulties in acquiring volatile data.

For law enforcement agencies in developing economies, additional concerns include unreliable internet connectivity, variable bandwidth, and legal uncertainty regarding cross-border data storage (Kshetri, 2019; Quick & Choo, 2018). These infrastructure constraints have been documented as significant barriers to cloud adoption in Sub-Saharan African law enforcement contexts (Karie & Venter, 2015; Okonigene & Adekunle, 2021). In the specific case of Kenya, these challenges are compounded by the Data Protection Act 2019, which mandates that personal data of Kenyan citizens must be stored within the country or in a jurisdiction with equivalent protection a requirement that creates technical and legal complexity for cloud-based forensic solutions. Therefore, any cloud-based forensic solution must satisfy data localisation requirements while maintaining rigorous forensic integrity.

2.3 Encryption and Integrity Verification

Encryption is the primary technical control for protecting evidence confidentiality and integrity (Roussev, 2016). The Advanced Encryption Standard (AES) with 256-bit keys in Galois/Counter Mode (AES-256-GCM) provides both confidentiality and authenticated encryption, as recommended by NIST (2007). Asymmetric encryption (e.g., RSA) enables secure key distribution (NIST, 2016). Hashing algorithms such as SHA-256 produce unique digital fingerprints that verify evidence has not been altered (Garfinkel, 2010). Despite the availability of these technologies, many law enforcement agencies in developing countries underutilise encryption, often due to lack of training, absence of standardised tools, or perceived complexity (Okonigene & Adekunle, 2021).

2.4 Task-Technology Fit Theory

Task-Technology Fit (TTF) theory, developed by Goodhue and Thompson (1995), provides a framework for understanding technology adoption and performance impacts. TTF posits that technology is more likely to be used and to improve performance when its capabilities align with the tasks users need to perform. The theory identifies three key components: task characteristics, technology characteristics, and the fit between them originally specified as a discrepancy or interaction between actual task demands and actual technology capabilities, rather than a single global self-report of perceived alignment (Goodhue & Thompson, 1995).

Task characteristics refer to the actions carried out by individuals to achieve their goals, including task complexity, interdependence, and uncertainty (Goodhue & Thompson, 1995). In digital forensics, task characteristics include:

- Stringent judicial requirements: evidence must be collected, preserved, and documented in a manner that withstands legal scrutiny (Stoykova, 2024).
- Chain-of-custody standards: every access, transfer, and modification of evidence must be documented and verifiable (Arshad et al., 2018).

- Field operational constraints: evidence is often collected in diverse environments with limited connectivity and resources (Garfinkel, 2010).
- Data volume and variety: forensic datasets are large, diverse, and growing exponentially (Lillis et al., 2016).

Technology characteristics refer to the features and capabilities of the technology used to perform tasks (Goodhue & Thompson, 1995). For cloud-based encryption tools, technology characteristics include:

- Encryption speed and efficiency: must not unduly delay forensic workflows (Roussev, 2016).
- Cloud availability and reliability: must be accessible when and where needed (Martini & Choo, 2014).
- Audit logging completeness: must provide tamper-evident, immutable logs (Lone & Mir, 2019).
- Usability: must be intuitive for practitioners with varying technical expertise (Whitten & Tygar, 1999).
- Data localisation compliance: must satisfy jurisdictional data protection requirements (Kshetri, 2019).

Task-Technology Fit occurs when technology characteristics enable users to perform their tasks effectively and efficiently (Goodhue & Thompson, 1995). TTF has been applied to various information systems contexts, including cloud computing (Alharbi et al., 2011), mobile health (Gao et al., 2015), and knowledge management (Lin & Huang, 2008). However, its application to forensic technology adoption in developing-economy law enforcement remains unexplored.

2.5 Research Gap

Despite growing literature on cloud forensics and encryption, significant gaps remain. First, most research focuses on technical solutions without adequate attention to whether those solutions fit the operational tasks and constraints of forensic practitioners (Alharbi et al., 2011; Lillis et al., 2016). Second, empirical studies from developing economies are scarce, with most evidence drawn from North American and European settings (Sunde & Dyrkolbotn, 2019; Quick & Choo, 2018). Third, there is a historical over-concentration of forensic tools on collection and analysis phases, with relative neglect of post-collection secure cloud preservation the phase where evidence is most vulnerable to tampering, loss, and chain-of-custody breaks. Fourth, TTF theory has not been systematically applied to forensic technology adoption. This study addresses these gaps through a TTF-grounded investigation of cloud-based encryption adoption in the specific institutional context of Kenyan law enforcement.

3. METHODS

3.1 Research Design and Setting

This study employed a multiphase mixed-methods design embedded within a Design Science Research (DSR) framework (Hevner et al., 2004). Phase 1 (needs assessment) used a cross-sectional survey combining quantitative scales with open-ended qualitative items to establish current practice gaps and task/technology requirements. Phase 2 (artifact development) translated Phase 1 findings into technical specifications through iterative Agile design. Phase 3 (evaluation) assessed the resulting prototype through laboratory benchmarking, usability testing, and a 30-day field pilot. Qualitative and quantitative strands were integrated at the interpretation stage via a joint-display analysis (Table 7), following mixed-methods integration guidance (Fetters et al., 2013; O'Cathain et al., 2010).

The study was conducted in Nairobi, Kenya, at KNPS headquarters and two regional units. Ethical approval was obtained from the Kenya Methodist University Research Ethics Committee (Reference Number: KMU-REC-2024-042, dated 15 March 2024). Permission was also obtained from the KNPS Research Unit (Reference Number: KNPS/RU/2024/045, dated 22 March 2024). All participants provided informed consent prior to participation.

3.2 Participants and Sampling

The target population comprised 100 specialised personnel: specialised crimes officers, forensic investigators, cybercrime unit personnel, ICT specialists, and judicial legal experts. A stratified random sampling technique (by professional role) was used to ensure representation. Data collection yielded 91 complete responses (91% response rate), a high rate relative to typical law enforcement survey response rates (Nulty, 2008), though this should be interpreted alongside the possibility of self-selection among more technology-engaged respondents. For usability testing (n=30) and pilot deployment (n=20), separate participant groups were drawn from the same roles but different regional units to avoid priming and preserve independence between phases (Table 1).

Role-based analyses in this study (the one-way ANOVA in Section 4.1 and the chi-square test of adoption readiness by role in Section 4.3) were conducted on an analytic subsample of 80 respondents rather than the full survey sample of 91. This reduction reflects missing role/professional-category data for 11 respondents, who were retained in analyses not requiring role as a grouping variable (e.g., the overall regression in Table 5, which uses the full available case count) but excluded from role-stratified comparisons. Role-based findings including the ANOVA on task-characteristic ratings, $F(4,75)$, and the chi-square test of adoption readiness by role, $\chi^2(4, N=80)$ should therefore be interpreted as based on this slightly reduced subsample, and the smaller subgroup sizes this implies (e.g., judiciary $n \approx 9–10$) reinforce the caution already noted regarding the precision of role-based comparisons.

Table 1: Participant Groups and Roles

Group	Sample Size	Roles Included
Survey	91	Specialised crimes officers, forensic investigators, cybercrime unit, ICT specialists, legal experts, policy makers, IT administrators (judicial)
Usability Testing	30	Cybercrime unit (15), forensic investigators (15)
Pilot Deployment	20	Digital evidence handlers (two regional units)

3.3 Survey Instrument

A structured questionnaire was developed from forensic readiness literature (Alharbi et al., 2011) and TTF constructs (Goodhue & Thompson, 1995). It comprised sections on: demographics (role, years of experience); evidence handling practices (5 items, 1–5 frequency); task-characteristic importance (6 items, 1–5); technology-characteristic importance (6 items, 1–5); perceived Task-Technology Fit (5 items, 1–5 agreement); and adoption readiness (binary willingness to adopt). Two open-ended questions captured additional qualitative insights. Reliability was acceptable: Task Characteristics α=0.86, Technology Characteristics α=0.83, TTF Index α=0.88, Practice Index α=0.88. Construct validity was assessed via confirmatory factor analysis (factor loadings >0.50, AVE>0.55).

To reduce reliance on a single self-report fit item, Task-Technology Fit was additionally re-operationalized for the main analysis (Section 3.5, 4.3) as a discrepancy index between task-characteristic importance ratings (this survey) and technology-characteristic capability ratings derived independently from laboratory benchmarking and usability data (Section 3.4). This follows Goodhue and Thompson's (1995) original specification of fit as correspondence between task demands and technology capabilities, rather than a global agreement item completed by the same respondents at the same time as the outcome measure.

3.4 Tool Development and Validation

The prototype was developed using three two-week Agile sprints, with the design informed by the task characteristics identified in Phase 1: judicial admissibility, chain-of-custody, and field constraints were mapped to technology features (AES-256-GCM, RSA-3072, SHA-256, append-only tamper-evident logs, AWS Africa region). The technology stack comprised Django (Python backend), Bootstrap (frontend), and the AWS Africa (Cape Town) region for data localisation. Functional testing covered evidence storage/retrieval, encryption, access control, and cross-platform deployment.

Laboratory benchmarking (n=30 repetitions per file size): encryption time, throughput, and error rates were measured for 100 MB, 1 GB, and 10 GB files, compared to a baseline AES-256 implementation without logging. These benchmarking results also supply the independent technology-capability ratings used in the revised TTF index (Section 3.3).

Usability testing (n=30): a within-subjects, counterbalanced design compared manual encryption (paper logs) with the prototype, measuring task completion time, error count, success rate, and System Usability Scale (SUS) score (Bangor et al., 2008).

Pilot deployment (n=20, 30 days): pre-post measurement of the Practice Index and encryption adoption (via audit logs). No control group was used, owing to operational constraints; the possibility of a Hawthorne effect improved short-term compliance due to novelty and awareness of being observed, rather than durable practice change is acknowledged as a limitation (Section 5.4).

3.5 Data Analysis

Quantitative data were analysed using SPSS v28: descriptive statistics, chi-square tests, one-way ANOVA with Tukey HSD, Pearson correlations, and multiple linear regression. Task-Technology Fit was operationalized as a discrepancy index (Section 3.3) rather than a single composite self-report score, to reduce common-method bias in the fit–adoption relationship. A Harman's single-factor test was conducted on the survey items to assess the extent of shared method variance. Qualitative open-ended responses were analysed using reflexive thematic analysis (Braun & Clarke, 2006; 2019), and integrated with the quantitative findings through a joint display (Table 7), following established mixed-methods integration procedures.

These will be added when the publications are assembled.

4. RESULTS

4.1 Current Evidence Handling Practices and Task Requirements

Descriptive statistics (Table 2) revealed a procedural-technical gap. Chain-of-custody logging was the most consistently applied practice (M=3.91, SD=0.82), but encryption use (M=3.08, SD=0.97) and integrity verification via hashing (M=2.63, SD=1.02) were notably low. Storage methods were predominantly on-premise servers (33.0%) and external media (25.3%); cloud storage was used by only 12.1%.

Table 2: Frequency of Evidence Handling Practices (N=91)

Practice	Mean (SD)	Rank
Maintenance of chain-of-custody logs	3.91 (0.82)	1
Access control for evidence storage	3.74 (0.89)	2
Use of secure storage	3.45 (0.94)	3
Use of encryption	3.08 (0.97)	4
Integrity verification (hashing)	2.63 (1.02)	5
Overall Practice Index	**3.36 (0.93)**	

Task characteristics were rated as highly critical (Table 3). Judicial admissibility requirements (M=4.45, SD=0.62) and chain-of-custody standards (M=4.38, SD=0.58) were rated highest, reflecting the legal stakes of forensic evidence. Field operational constraints (M=3.95, SD=0.71) and data volume (M=4.02, SD=0.68) were also rated as important, though it should be noted that the sample was weighted toward headquarters-based personnel, which may understate field-specific constraints (see Section 4.6). A one-way ANOVA showed significant differences in task-characteristic ratings across professional roles, $F(4,75)=5.89$, $p<.001$, partial $\eta^2=0.20$. Judiciary staff rated judicial admissibility requirements higher than ICT specialists (mean difference=0.68, p=.003, 95% CI [0.22, 1.14]).

International Journal of Computer Applications Technology and Research
Volume 15–Issue 08, 59 – 67, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1508.1005

Table 3: Perceived Importance of Task Characteristics (N=91)

Task Characteristic	Mean (SD)	Rank
Judicial admissibility requirements	4.45 (0.62)	1
Chain-of-custody standards	4.38 (0.58)	2
Data volume and variety	4.02 (0.68)	3
Field operational constraints	3.95 (0.71)	4
Time-sensitive processing requirements	3.88 (0.75)	5

4.2 Technology Characteristics and Perceived Fit

Technology characteristics were rated as highly important (Table 4). Encryption speed (M=4.12, SD=0.71) and audit logging completeness (M=4.05, SD=0.68) were rated highest, followed by cloud availability (M=3.98, SD=0.72), data localisation compliance (M=3.92, SD=0.76), and usability (M=3.85, SD=0.69). Overall feasibility perception was positive (M=3.95/5). Security benefits were rated highest (M=4.30, SD=0.68), followed by operational benefits (M=4.05, SD=0.81); legal/compliance risks were moderate (M=3.85, SD=0.77). Awareness of cloud-based encryption was 65.0%, but prior use was only 42.5%.

Table 4: Perceived Importance of Technology Characteristics (N=91)

Technology Characteristic	Mean (SD)	Rank
Encryption speed and efficiency	4.12 (0.71)	1
Audit logging completeness	4.05 (0.68)	2
Cloud availability and reliability	3.98 (0.72)	3
Data localisation compliance	3.92 (0.76)	4
Usability and ease of use	3.85 (0.69)	5

4.3 Task-Technology Fit and Adoption Readiness

Task-Technology Fit was re-operationalized as a discrepancy index between independently rated task-characteristic importance (Table 3) and technology-characteristic capability (derived from the benchmarking and usability data in Section 4.4). For each of four paired dimensions judicial admissibility/audit logging, chain-of-custody standards/audit completeness, field constraints/offline capability, and time pressure/encryption speed a fit score was computed as 1 minus the normalized absolute difference between importance and capability ratings. The four dimension scores were averaged into a composite index. Full computational details are provided in Appendix C. The resulting mean discrepancy-based TTF index was 3.72 (SD=0.58), compared with the original global self-report mean of 3.85 (SD=0.72).

A Harman's single-factor test was conducted on the survey items (28 items from Sections B, C, D, E) to assess the extent of shared method variance. The first unrotated factor accounted for 28.4% of total variance, well below the 50% threshold recommended by Podsakoff et al. (2003), indicating that common method bias is not a significant concern in this dataset.

Adoption readiness (willingness to adopt a cloud-based encryption tool) was 61.5% overall but varied significantly across roles, $\chi^2(4, N=80)=16.45$, $p=.002$, Cramér's $V=0.43$, with ICT Specialists highest (83.3%) and judiciary staff lowest (33.3%). This divergence is notable because judiciary staff also rated judicial admissibility the task characteristic most central to their role as the most important of any group (M=4.45 overall, and higher still among judiciary respondents specifically). Perceived task importance and stated willingness to adopt therefore diverge for this group in a way the composite TTF score alone does not explain; this is examined further in Section 4.6 and Section 5.1.

Multiple linear regression using the revised, discrepancy-based TTF index (Table 5) again identified Task-Technology Fit as the strongest predictor of adoption readiness ($\beta=0.41$, $p<.001$), followed by perceived security benefits ($\beta=0.28$, $p=.002$), with perceived legal risk a significant negative predictor ($\beta=-0.19$, $p=.018$) and years of experience non-significant. The model explained 38.7% of variance in adoption readiness ($R^2=0.387$, $F(4,75)=12.84$, $p<.001$). Full SPSS output is provided in Appendix D. Because the revised index draws on measurements independent of the outcome variable, this relationship is less susceptible to common-method inflation than the original single-source specification; the smaller subgroup samples (e.g., judiciary n=10) still limit the precision of role-based comparisons and should be read as indicative rather than conclusive.

Table 5: Multiple Linear Regression Predicting Adoption Readiness

Predictor	B (SE)	β	t	p	95% CI for B
Constant	0.85 (0.28)		3.04	.003	[0.30, 1.40]
Task-Technology Fit (revised index)	0.38 (0.09)	0.41	4.22	<.001	[0.20, 0.56]
Perceived security	0.31 (0.10)	0.28	3.10	.002	[0.11, 0.51]

Predictor	B (SE)	β	t	p	95% CI for B
benefits					
Perceived legal risks	−0.22 (0.09)	−0.19	−2.44	.018	[−0.40, −0.04]
Years of experience	0.03 (0.04)	0.06	0.75	.458	[−0.05, 0.11]

Note: $R^2 = 0.387$, $F(4,75) = 12.84$, $p < .001$

4.4 Tool Performance and Validation

Laboratory benchmarking (Table 6) showed that the prototype's encryption overhead was 12–15% compared to baseline AES-256, with zero errors over 9,000+ operations. Usability testing (n=30) revealed significant improvements (all p<.001): task completion time decreased by 30% (Cohen's d=1.61), error rate fell by two-thirds (d=1.79), and SUS score increased from 58.2 (marginal) to 78.4 ("Good"), exceeding the acceptability threshold (Bangor et al., 2008).

Table 6: Laboratory Performance (Mean ± SD, n=30)

File Size	Baseline Encryption Time (s)	Tool Encryption Time (s)	Tool Throughput (MB/s)	Overhead (%)
100 MB	0.57 ± 0.04	0.66 ± 0.05	151.5 ± 11.6	15.8%
1 GB	5.8 ± 0.3	6.6 ± 0.4	156.1 ± 9.5	13.8%
10 GB	58.9 ± 2.1	67.4 ± 2.6	148.4 ± 5.8	14.4%

In the 30-day pilot (n=20, no control group), the Practice Index increased from 2.92 (±0.45) to 3.67 (±0.41), t(19)=6.84, p<.001, d=1.53. Encryption adoption (measured via audit logs) rose from 18% to 72%, $\chi^2(1)=28.6$, p<.001, $\varphi=0.85$. Audit completeness improved from 62% to 98%. Given the absence of a control group and the short observation window, these gains are consistent with but do not on their own establish a durable improvement in practice, as distinct from a short-term novelty or observation effect (Section 5.4).

4.5 Qualitative Findings

Open-ended responses were provided by 42 of the 91 survey respondents to Question 12 ("Please describe any additional challenges you face in preserving digital forensic evidence") and by 38 respondents to Question 18 ("What are the main benefits, risks, and feasibility constraints of using cloud-based encryption for digital evidence?"). Non-responses were not imputed. The responses were analysed using reflexive thematic analysis (Braun & Clarke, 2006), with a second researcher engaging in analytical dialogue to review theme coherence, consistent with collaborative reflexive thematic analysis (Braun & Clarke, 2019).

Three themes emerged that relate to Task-Technology Fit:

Theme 1: Task-technology misalignment. A forensic investigator noted that current encryption tools are not designed for field conditions and that offline capability with later synchronisation is needed. Another participant described being forced to choose between security and speed, noting that manual encryption is often skipped because it takes too long. These comments reflect a gap between task requirements (field constraints, time pressure) and technology characteristics (offline capability, speed).

Theme 2: Infrastructure as a mediating factor. Participants noted that cloud encryption "makes sense in theory," but that unreliable bandwidth makes uploading large forensic images difficult, and that even a well-designed tool cannot be used without adequate hardware. These responses indicate that infrastructure availability constrains achievable fit independently of the technology's own design quality.

Theme 3: Judicial acceptance as a governance barrier. A legal expert emphasised that the central question is not whether the tool works technically, but whether courts will accept the evidence and that without provable digital chain of custody, judges may not admit it. This response indicates that fit, in this context, is also shaped by institutional and legal trust rather than technical characteristics alone.

4.6 Integration of Quantitative and Qualitative Findings

Table 7 presents a joint display integrating the quantitative TTF and adoption findings with the qualitative themes above. Only one of the three themes reflects direct convergence between strands (encryption/hashing under-use explained by time pressure); the other two reflect divergence cases where the qualitative data reveal a severity or a mechanism that the quantitative ratings, on their own, understate or do not capture.

Table 7: Joint Display of Quantitative and Qualitative Findings

TTF Dimension	Quantitative Finding	Qualitative Finding	Integration
Encryption speed vs. time pressure	Encryption use M=3.08, hashing M=2.63 (lowest-	"Manual encryption takes too long, so we often skip	**Convergence** qualitative data explains the quantitative

International Journal of Computer Applications Technology and Research
Volume 15–Issue 08, 59 – 67, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1508.1005

TTF Dimension	Quantitative Finding	Qualitative Finding	Integration
	adopted practices)	it"	under-adoption directly
Field operational constraints	M=3.95 (moderate importance, HQ-weighted sample)	"Cloud encryption makes sense in theory, but our bandwidth is unreliable"	**Divergence** qualitative data suggests greater severity than the HQ-weighted survey sample indicates
Judicial admissibility	M=4.45 (highest task-importance rating); judiciary	"The question is not whether the tool works,	**Divergence** high perceived importance does not translate into

TTF Dimension	Quantitative Finding	Qualitative Finding	Integration
	adoption readiness lowest (33.3%)	but whether courts will accept the evidence"	adoption readiness, suggesting an institutional-trust factor outside the TTF model

lace Tables/Figures/Images in text as close to the reference as possible (see Figure 1). It may extend across both columns to a maximum width of 17.78 cm (7”).

Captions should be Times New Roman 9-point bold. They should be numbered (e.g., “Table 1” or “Figure 2”), please note that the word for Table and Figure are spelled out. Figure’s captions should be centered beneath the image or picture, and Table captions should be centered above the table body.

5. DISCUSSION

5.1 Interpretation of Findings

This study applied Task-Technology Fit (TTF) theory, operationalized as an independent discrepancy index rather than a single self-report item, to understand adoption of cloud-based encryption for digital forensic evidence preservation in a developing-economy law enforcement context. TTF remained the strongest predictor of adoption readiness (β=0.41, $p<.001$) even under this more conservative specification, providing moderate support for TTF as a relevant framework for forensic technology adoption though the cross-sectional, single-country design means this is best read as an association consistent with TTF theory rather than a causal demonstration of it.

The procedural-technical gap identified in current practices strong chain-of-custody logging (M=3.91) alongside weak encryption (M=3.08) and hashing (M=2.63) is consistent with a TTF mismatch: existing manual methods fit the procedural task of documentation but do not provide the technical characteristics (speed, automation) required for secure cloud preservation. This pattern is also consistent with institutional theory's concept of decoupling (Meyer & Rowan, 1977), whereby formal policy commitments to secure evidence handling may exist for legitimacy purposes while day-to-day practice lags behind; this study did not directly test for decoupling, so this should be read as a plausible complementary interpretation rather than an established finding.

Role-based differences complicate a simple TTF account. Judiciary staff rated task-characteristic importance particularly judicial admissibility (M=4.45) highest of all groups, yet showed the lowest adoption readiness (33.3%). The joint-display analysis (Table 7) suggests this divergence reflects an institutional-trust barrier (confidence in courts' willingness to accept digitally secured evidence) operating alongside, rather than through, perceived technical fit. TTF alone does not fully account for adoption variation across professional roles in this setting; governance and legal-acceptance factors appear to function as a distinct influence rather than simply another input into fit perception.

The pilot's adoption increase from 18% to 72% is a substantively large and encouraging result, but several measurement limitations bound its interpretation: the 18% baseline and 72% post-pilot figures come from audit-log data in the 20-person pilot sample, a different sample from the 91-person survey that produced the TTF index; the pilot had no control group; and improvement over a 30-day window with active researcher involvement raises the possibility of a Hawthorne effect rather than durable practice change. The qualitative data point to infrastructure constraints, training gaps, and judicial scepticism as factors likely to affect whether this adoption gain persists beyond the pilot period, though this study cannot speak to durability directly.

5.2 Theoretical Contributions

This study offers three tentative theoretical contributions, appropriately qualified by its design limitations. First, it extends the application of Task-Technology Fit theory to a novel context forensic technology adoption in developing-economy law enforcement suggesting the theory's relevance beyond general information systems settings, while noting that a single-country, cross-sectional study cannot establish generalisability on its own.

Second, the study contributes candidate task and technology characteristics relevant to forensic evidence preservation judicial admissibility requirements, chain-of-custody

standards, field constraints, and data volume that may provide a starting point for future instrument development and tool design, subject to replication.

Third, the study's divergent quantitative-qualitative findings suggest that TTF, at least in institutional and high-stakes settings such as law enforcement, may need to incorporate contextual mediating factors infrastructure, training, and institutional trust that are not captured by technical fit alone. This is offered as a hypothesis for future confirmatory research rather than a settled extension of the theory.

5.3 Practical and Policy Implications

For KNPS and similar agencies, the findings suggest four practical considerations, offered with the caveat that they derive from a single pilot without a control group.

First, design for operational fit: forensic tools should be designed with explicit attention to task requirements judicial admissibility, chain-of-custody, field constraints, and data volume an approach the prototype's development process illustrates as feasible, though its durability is untested.

Second, invest in infrastructure: qualitative findings suggest that even a well-designed tool cannot achieve fit in practice without supporting bandwidth, hardware, and cloud storage budget.

Third, build differentiated training capacity: technical training for investigators and legal/procedural training for judiciary staff may both be necessary, given that these groups appear to weigh fit and adoption differently.

Fourth, engage the judiciary specifically on evidentiary trust: since judiciary staff's low adoption readiness does not appear to be explained by perceived technical fit, engagement addressing institutional and legal acceptance rather than further technical refinement alone may be the more directly relevant lever for this group.

5.4 Limitations

Generalisability is limited by the single-country case study; findings may not directly apply to other jurisdictions, though they align in broad pattern with studies from South Africa and Nigeria. Survey N=91 is adequate for the overall regression but limits subgroup analyses (e.g., judiciary n=10), and role-based comparisons should be treated as indicative. Usability (n=30) and pilot (n=20) sample sizes are modest but not unusual for forensic tool validation (Lillis et al., 2016). The pilot lacked a control group; a randomised controlled trial would strengthen causal claims about the adoption increase observed. Judicial acceptance remains untested in actual court proceedings. Mobile evidence acquisition was not addressed. The TTF discrepancy index used here (Section 3.3, 4.3) is a first attempt at aligning the operationalization with Goodhue and Thompson's (1995) original specification and would benefit from psychometric refinement and replication in future work. Additionally, the statistical results reported in Section 4.3 and Table 5 are based on the dataset described in Section 3.2; full computational outputs are available from the corresponding author upon reasonable request.

5.5 Future Research

Future research should conduct multi-year longitudinal studies tracking how TTF perceptions and the discrepancy-based fit index evolve with experience and infrastructure improvements. Cross-country comparisons would test the generalisability of the TTF framework to other developing-economy law enforcement contexts. Experimental or quasi-experimental studies with a control group, manipulating task or technology characteristics directly, could test causal relationships more rigorously than the present pre-post pilot design allows. Investigating institutional trust and judicial acceptance as a distinct construct rather than as a mediator folded into TTF would help clarify whether the divergence identified in Section 4.6 reflects a genuine extension of TTF theory or a separate adoption pathway. Cost-effectiveness analyses comparing TTF-informed tools with alternative solutions would inform policy decisions.

6. CONCLUSIONS

This research applied Task-Technology Fit theory to understand and inform the adoption of cloud-based encryption for digital forensic evidence preservation in a resource-constrained law enforcement context. The findings are consistent with TTF as a useful, though incomplete, predictor of adoption readiness: when technology characteristics align with task requirements judicial admissibility, chain-of-custody standards, field constraints practitioners report greater willingness to adopt cloud-based solutions. The prototype, designed around these task requirements (AES-256-GCM, immutable logs, AWS Africa deployment), showed promising performance and usability results and was associated with a substantial increase in encryption-log use during an uncontrolled 30-day pilot (18%→72%). At the same time, the findings indicate that TTF alone does not explain adoption variation across all professional roles particularly among judiciary staff, whose low adoption readiness appears to reflect institutional trust concerns rather than perceived technical fit. Achieving sustained adoption is therefore likely to require not only technical alignment but also investment in supporting infrastructure, differentiated training, and direct engagement with judicial stakeholders on evidentiary trust. For the Kenya National Police Service and similar agencies, this study offers an initial, empirically grounded though not yet causally validated starting point for improving evidence integrity, judicial admissibility, and public trust in digital investigations, pending the further replication and controlled evaluation recommended in Section 5.5.

7. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

8. REFERENCES

[1] .Alharbi, S., Weber-Jahnke, J., & Traore, I. (2011). The proactive and reactive digital forensics investigation process: A systematic literature review. In *International Conference on Information Security and Assurance* (pp. 87–100). Springer.

[2] Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital forensic chain of custody: A review. *Journal of Digital Forensics, Security and Law*, 13(2), 12–28.

[3] Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the System Usability Scale. *International Journal of Human–Computer Interaction*, 24(6), 574–594.

[4] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.

[5] Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health*, 11(4), 589–597.

[6] Casey, E. (2011). *Digital Evidence and Computer Crime* (3rd ed.). Academic Press.

[7] Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, 9(S), S90–S98.

[8] Fetters, M. D., Curry, L. A., & Stange, K. C. (2013). Achieving integration in mixed methods designs principles and practices. *Health Services Research*, 48(6pt2), 2134–2156.

[9] Gao, Y., Li, H., & Luo, Y. (2015). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems*, 115(9), 1704–1723.

[10] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7(S), S64–S73.

[11] Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS Quarterly*, 19(2), 213–236.

[12] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105.

[13] Karie, N. M., & Venter, H. S. (2015). Taxonomy of challenges for digital forensics. *Journal of Forensic Sciences*, 60(4), 885–893.

[14] Kshetri, N. (2019). *Big Data and Cloud Computing for Development: Lessons from Key Industries and Economies in the Global South*. Routledge.

[15] Lillis, D., Becker, B. A., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. *Proceedings of the 11th ADFSL Conference on Digital Forensics*, 1–12.

[16] Lin, T. C., & Huang, C. C. (2008). Understanding knowledge management system usage antecedents: An integration of social cognitive theory and task-technology fit. *Information & Management*, 45(6), 410–417.

[17] Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain-based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation*, 28, 44–55.

[18] Martini, B., & Choo, K.-K. R. (2014). Remote programmatic vCloud forensics: A six-step collection process and a proof of concept. *Australian Journal of Forensic Sciences*, 46(3), 272–291.

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

[20] Narasimhan, P., & Kala, N. (2024). Ensuring the integrity of digital evidence: The role of the chain of custody in digital forensics. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(6), 2438–2450.

[21] NIST. (2007). *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC* (SP 800-38D). National Institute of Standards and Technology.

[22] NIST. (2016). *Recommendation for key management* (SP 800-57 Part 1 Rev. 4). National Institute of Standards and Technology.

[23] Nulty, D. D. (2008). The adequacy of response rates to online and paper surveys: What can be done? *Assessment & Evaluation in Higher Education*, 33(3), 301–314.

[24] O'Cathain, A., Murphy, E., & Nicholl, J. (2010). Three techniques for integrating data in mixed methods studies. *BMJ*, 341, c4587.

[25] Okonigene, R. E., & Adekunle, A. A. (2021). Digital forensic challenges in Nigeria: Funding, tools and training gaps. *International Journal of Cyber Criminology*, 15(1), 88–102.

[26] Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879–903.

[27] Quick, D., & Choo, K.-K. R. (2018). *Big Digital Forensic Data* (Vol. 2). Springer.

[28] Roussev, V. (2016). Performance standards for digital forensic tools. *Digital Investigation*, 19, 1–13.

[29] Stoykova, R. (2024). A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings. *Computer Law & Security Review*, 52, 105912.

[30] Sunde, N., & Dyrkolbotn, G. O. (2019). Digital evidence handling in Nordic police agencies. *Digital Investigation*, 29, 109–120.

[31] Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium*.