Digital Forensic Readiness to Mitigate Insider Threats in the SaaS Cloud Environment

Gabriel Shoderu, Stacey Baror, Abiodun Modupe and Sheunesu Makura
University of Pretoria, South Africa

go.shoderu@gmail.com
stacey.baror@tuks.co.za
abiodun.modupe@cs.up.ac.za
makura.sm@up.ac.za

Abstract: Insider threats continue to pose significant risks in Software-as-a-Service (SaaS) environments, where legitimate users hold varying levels of access and control. Existing mitigation measures remain largely reactive, focusing on post-incident investigation and evidence recovery, which often result in delayed detection and incomplete forensics. A proactive and forensically sound approach is therefore required to identify and contain insider activity before major compromise occurs. This paper presents the Digital Forensic Readiness to Bust Insider Threats (DFR-BUST) model, a framework that embeds forensic readiness principles within SaaS environments to enable early detection, secure evidence capture, and legally defensible investigations. The model is aligned with the ISO/IEC 27043 digital investigation process, operationalising its readiness, acquisitive, and concurrent process classes. The model was evaluated using an experimental setup based on publicly available insider-threat datasets to demonstrate its readiness and detection capability. The evaluation confirmed that the proposed architecture supports proactive evidence generation, integrity verification, and traceable anomaly detection within a controlled environment. Unlike conventional reactive approaches, DFR-BUST provides a proactive, evidence-centric mechanism that enhances both detection accuracy and forensic admissibility. Its modular design ensures adaptability across cloud platforms while maintaining compliance with international forensic investigation standards. Overall, this work bridges the gap between intelligent analytics and digital forensic readiness. By ensuring that insider detection outputs are accompanied by verified, admissible evidence, the framework contributes a practical foundation for developing forensic-aware, cloud-based security systems.

Keywords: Insider threat, Cybercrime, Digital forensic readiness, SaaS cloud, Artificial intelligence, Anomaly detection

1. Introduction

Cloud computing has transformed how organisations store, process, and share data, with Software-as-a-Service (SaaS) platforms now underpinning most enterprise operations. This model offers scalability and accessibility but introduces new forensic and security complexities due to distributed control and shared responsibility between providers and clients. Within this environment, insider threats remain a persistent and costly risk, as authorised users, employees, contractors, or third-party administrators can misuse legitimate privileges to compromise data integrity, confidentiality, or availability (Greitzer et al, 2019; Sarhan and Altwaijry, 2023; Ponemon Institute, 2022).

The forensic challenge in SaaS environments lies in visibility and accountability. Multi-tenant architectures, delegated access rights, and rapid provisioning obscure traces of insider activity, while responsibility for evidence preservation is divided between provider and customer (Alenezi et al, 2020; CERT, 2016). Existing controls detect policy violations but rarely ensure that the digital traces they generate are complete, verifiable, and admissible. This highlights the need for Digital Forensic Readiness (DFR), a proactive capability that prepares cloud systems to capture and preserve evidence before incidents occur (Rowlingson, 2004; ISO/IEC 27043, 2015).

Most current cybersecurity mechanisms are reactive, initiating investigation only after an incident has occurred (Rowlingson, 2004). Such post-event analysis often yields incomplete or inadmissible evidence, delaying response and increasing cost. Recent studies on machine-learning-based anomaly detection (Tuor et al, 2017; Sarhan and Altwaijry, 2023) show promise for identifying insider behaviour, yet they overlook forensic soundness, traceability, integrity, and legal admissibility (Tan, 2001; ISO/IEC 27043, 2015). The present research aligns with ISO/IEC 27043, which defines readiness, acquisition, investigation, and concurrent process classes for digital investigations, extending its readiness class to cloud environments through an intelligent, forensic-aware design.

To address this gap, the study proposes the Digital Forensic Readiness to Bust Insider Threats (DFR-BUST) model, which embeds readiness, archival, and audit mechanisms within SaaS environments to ensure proactive detection and preservation of admissible evidence. The model operationalises ISO/IEC 27043 process classes, readiness, acquisitive, and concurrent, to create a seamless flow from evidence generation to analysis.

The study contributes in two ways:

- It introduces the DFR-BUST framework that integrates digital forensic readiness principles with intelligent analytics aligned to ISO/IEC 27043.
- It evaluates the framework experimentally using insider-threat data to demonstrate readiness effectiveness and evidence integrity.

The design of DFR-BUST is guided by four key quality attributes derived from software-architecture principles (Bass et al, 2021): reliability, ensuring consistent log and evidence capture; security, protecting against unauthorised access; auditability, guaranteeing traceability and admissibility; and cloud compliance, supporting scalability within SaaS ecosystems.

Having established the need for proactive and forensically sound insider-threat mitigation in SaaS environments, the next section explores prior research that underpin the proposed framework.

2. Background Literature

This section provides an overview of the key areas that inform this study. It begins with digital forensics and the evolution toward readiness, it then examines insider threats in Software-as-a-Service (SaaS) environments, and finally, the role of artificial intelligence in behavioural analytics. Together these areas provide the basis for developing the Digital Forensic Readiness to Bust Insider Threats (DFR-BUST) model.

2.1 Digital Forensics

Digital forensics is the discipline concerned with identifying, collecting, preserving, analysing, and presenting digital evidence in a scientifically reliable and legally admissible manner (Daniel and Daniel, 2011; Tan, 2001). Traditional investigations are reactive, beginning only after an incident has occurred, often yielding partial or tampered artefacts. As computing has shifted toward distributed and virtualised infrastructures, purely reactive approaches have proven insufficient (Rowlingson, 2004).

To address this limitation, research introduced Digital Forensic Readiness (DFR), the organisational capability to maximise evidential use while minimising investigation cost (Rowlingson, 2004). DFR emphasises preparation before incidents occur through structured logging, secure storage, and clear policies for evidence handling. The ISO/IEC 27043 standard formalises this concept by defining five investigation process classes: readiness, initialization, acquisitive, investigative, and concurrent. Readiness activities prepare systems for evidence capture, while concurrent activities ensure documentation and chain-of-custody integrity throughout.

Recent studies extended DFR to cloud environments, such as Kebande and Venter's (2017) Cloud Forensic Readiness as a Service (CFRaaS) model and Singh et al's (2022) SecureRS storage scheme. These studies highlight the need for automated, tamper-resistant evidence pipelines that maintain integrity and confidentiality. Yet DFR in SaaS contexts remains immature. Multi-tenant architectures and divided provider-customer responsibilities fragment evidence sources and hinder accountability (Alqahtany et al., 2019). Without a unified readiness process that coordinates collection and preservation across both parties, investigations risk data loss and unverifiable traces.

2.2 Insider Threats in SaaS Environments

Insider threats involve harmful actions by authorised users, employees, contractors, or partners, who misuse legitimate access (Greitzer et al., 2019). Behaviour may be intentional, such as data theft, or accidental, such as misconfiguring permissions (Ponemon Institute, 2022). Detection is difficult because insiders operate with valid credentials and knowledge of internal systems.

SaaS platforms amplify these challenges. Their web-based delivery allows access from many devices and locations, broadening the attack surface (Alenezi et al., 2020). Under the cloud's shared-responsibility model, providers secure infrastructure while customers manage user activity and configuration. This division often produces visibility gaps: providers hold infrastructure-level logs, whereas customers see only application-level events.

Audit trails, logins, data exports, and privilege changes, can reveal misuse if collected and preserved correctly. However, few organisations implement systematic, forensic-ready logging. As a result, evidence of intent or negligence may be incomplete or inadmissible during investigation. The Employee Management System (EMS) scenario later in this paper illustrates these risks where a user exporting bulk employee data after hours can only

be proven malicious if immutable audit logs exist. Hence, SaaS environments require frameworks that merge behavioural analytics with forensic readiness to ensure both early detection and evidential reliability.

2.3 Artificial Intelligence in Insider Threat Detection

Artificial intelligence (AI) and machine learning (ML) enable systems to analyse large behavioural datasets and flag anomalies indicative of insider misuse (Tuor et al, 2017; Sarhan and Altwaijry, 2023). Techniques include supervised classification, unsupervised anomaly detection, and deep learning. Feature-engineering methods such as Deep Feature Synthesis automatically derive higher-level behavioural indicators from raw logs (Kanter and Veeramachaneni, 2015). Because insider events are rare, many studies address class imbalance through resampling or cost-sensitive training.

While these approaches enhance detection accuracy, they seldom address forensic soundness. Metrics such as precision and recall dominate evaluation, whereas evidential integrity, chain-of-custody, and admissibility are often overlooked (Tan, 2001). Consequently, AI systems may identify anomalies yet fail to produce trustworthy evidence for investigators.

Recent literature therefore calls for integrating AI with DFR principles (Kebande and Venter, 2017; Singh et al, 2022). Such integration ensures that every analytical output is traceable to preserved source data and that alerts can serve as verifiable forensic artefacts. In this study, AI functions as a supporting component within a broader forensic-aware architecture rather than as the primary contribution. The goal is to combine intelligent detection with ISO/IEC 27043-compliant readiness processes so that insider-threat analytics yield both timely insights and admissible evidence.

Existing research demonstrates substantial progress in digital forensics, insider-threat analytics, and AI-based anomaly detection, yet these domains often evolve independently. Current cloud frameworks either focus on detection accuracy or on evidence preservation, seldom both. This fragmentation leaves SaaS organisations without a unified mechanism that ensures forensic readiness while supporting intelligent monitoring. Addressing this gap, the present work introduces the proposed DFR-BUST model, which consolidates readiness, detection, and preservation within a single ISO-aligned framework. The following section presents this model and the requirements guiding its design.

3. DFR-BUST Model

This section presents a holistic model that integrates digital forensic readiness with intelligent insider-threat monitoring in Software as a Service environment. The proposed model, DFR-BUST, prepares SaaS platforms for forensic investigation before incidents occur, ensuring that evidence generated during system operation remains authentic, traceable, and legally admissible (ISO/IEC 27043, 2015; Tan, 2001).

3.1 High level view of DFR-BUST Model

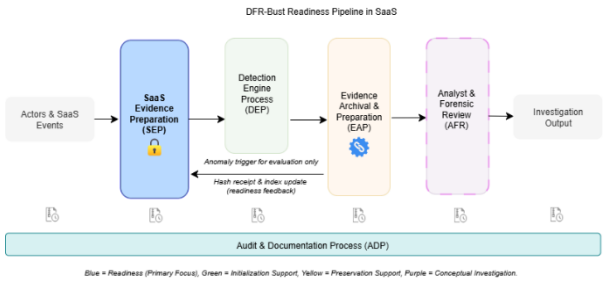

Figure 1: High-level view of the DFR-BUST readiness pipeline in a SaaS environment

Figure 1 illustrates the high-level pipeline. The SaaS Evidence Preparation (SEP) component performs pre-incident activities such as log generation, time synchronisation, normalisation, hashing, encryption, and daily archival. The Detection Engine Process (DEP) provides an initialization trigger by recognising anomalies and preserving the exact trigger context. The Evidence Archival and Preservation (EAP) component packages and verifies evidence, stores it in append-only repositories, and enforces access control (Kebande and Venter, 2017). The Analyst and Forensic Review (AFR) stage represents the conceptual hand-off to downstream examination and reporting (ISO/IEC, 2015). The Audit and Documentation Process (ADP) run across all components to maintain chain of custody, access logs, and hash receipts (Tan, 2001).

The study focuses on the readiness activities implemented in SEP, together with the preservation guarantees provided by EAP and the concurrent documentation maintained by ADP. DEP is included as a trigger and for evaluation of readiness effectiveness. AFR is included for completeness as a conceptual endpoint.

3.2 Mapping to ISO/IEC 27043

The ISO/IEC 27043 standard defines a comprehensive model for digital investigations through five process classes: readiness, initialization, acquisitive, investigative, and concurrent, each describing a stage in the life cycle of digital evidence (ISO/IEC 27043, 2015).

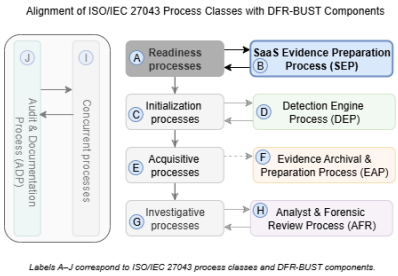

Figure 2: Alignment of ISO/IEC 27043 process classes with DFR-BUST components

To ensure methodological consistency and legal admissibility, the DFR-BUST model aligns its components with these process classes while maintaining a primary focus on forensic readiness. Figure 2 shows how each component supports a corresponding ISO process.

The SEP component directly implements the readiness class by enabling pre-incident log generation, normalization, and archival. DEP represents initialization by activating the investigation workflow once anomalies are detected. EAP performs acquisitive functions by packaging and verifying potential evidence. AFR embodies the investigative class by transforming preserved artefacts into meaningful insights. Finally, ADP operate as a concurrent layer that maintains chain of custody, provenance, and reproducibility across all stages.

This alignment demonstrates that while DFR-BUST supports the full investigative continuum, its main contribution lies in proactive readiness, ensuring that digital evidence is generated, protected, and auditable before incidents occur, creating a verifiable foundation for subsequent investigation.

Table 1: Mapping ISO 27043 to DFR-BUST Components

ISO 27043 Process Class	Primary Purpose	Corresponding DFR-BUST Component	Role in DFR-BUST Model	Evidence Outcome
Readiness	Pre-incident evidence preparation	SaaS Evidence Preparation (SEP)	Implements logging, normalisation, hashing, and archival	Structured, integrity-verified data
Initialization	Trigger and plan investigation	Detection Engine Process (DEP)	Generates anomaly-based alerts and preserves trigger context	Alert record and trigger dataset
Acquisitive	Collect and preserve evidence	Evidence Archival & Preservation (EAP)	Compiles, packages, and stores evidence immutably	Forensically packaged evidence
Investigative	Analyse and interpret data	Analyst & Forensic Review (AFR)	Examines evidence to establish intent or cause	Analytical report
Concurrent	Maintain documentation and oversight across all stages	Audit & Documentation Process (ADP)	Logs action, verifies chain of custody	Audit trail and verification receipts

3.3 Core Components of DFR-BUST Model

The DFR-BUST model comprises five coordinated components that collectively enable forensic readiness within a SaaS environment. SEP performs pre-incident collection and protection of activity logs. DEP recognises anomalies and initiates investigation triggers. EAP verifies and stores artefacts immutably. AFR supports human interpretation of preserved evidence, while the ADP maintain chain-of-custody and accountability across all stages.

Together, these components form a continuous readiness cycle in which evidence is captured, verified, and auditable before any incident occurs.

3.3.1 SaaS evidence preparation (SEP)

This component ensures that the SaaS environment produces logs that are structured, reliable, and legally admissible before incident occurs. It underpins forensic readiness by ensuring every action in the SaaS system can later be examined if necessary.

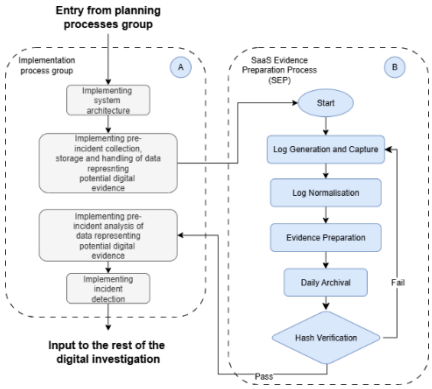

Figure 3: Integration of SEP process into the readiness process class of ISO/IEC 27043

The main activities include:

- Log Generation and Capture: Collects SaaS activities such as logon, logoff, device usage, file access, and web browsing in real time with synchronised timestamps.
- Log Normalisation: Standardises captured logs into a common format, removing duplicates and correcting inconsistencies.
- Evidence Preparation: Appends metadata such as department, user ID, and system identifiers; applies hashing and digital signatures to guarantee authenticity.
- Daily Archival: Batches and stores logs in secure repositories that preserve immutability and support later access.
- Hash Verification: After each archival cycle, verifies integrity through hash comparison. Successful checks confirm maintained readiness; failures trigger re-initialisation of log collection.

These steps ensure continuous evidence integrity and compliance with ISO/IEC 27043 readiness requirements. All generated logs and archives are concurrently registered in ADP for traceability.

3.3.2 Detection engine process (DEP)

This component represents the anomaly detection and behavioural analytics engine. It identifies deviations from behavioural baselines, flags potential insider threats, and initiates the investigative workflow.

Figure 4 illustrates the initialisation process in detail

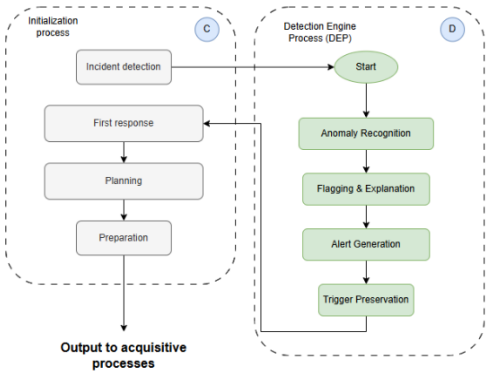

Figure 4: Integration of DEP within the initialization process class of ISO/IEC 27043

The main activities include:

- Anomaly Recognition: Applies detection models to SaaS logs and behavioural features, identifying patterns that deviate from established baselines.
- Flagging and Explanation: For each suspicious event, the system generates a flag accompanied by an explanation, such as unusual login time or abnormal data transfer.
- Alert Generation: Alerts are raised with structured contextual information, enabling investigators to understand the significance of the anomaly quickly.
- Trigger Preservation: Preserves datasets and metadata associated with each flagged anomaly to support further forensic analysis.

These activities ensure timely anomaly identification and systematic transition to investigation. The detection engine refines its baselines through adaptive learning while leaving validation and interpretation to analysts. Alert metadata and trigger details are automatically logged within ADP to maintain reproducibility.

3.3.3 Evidence archival and preservation process (EAP)

This component compiles, packages, and preserves all relevant data once an anomaly has been flagged, ensuring that contextual evidence remains complete, authentic, and admissible.

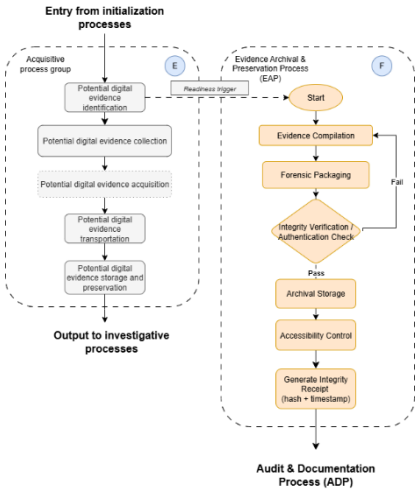

Figure 5: Integration of EAP within the acquisitive process class of ISO/IEC 27043

The main activities include:

- Evidence Compilation: Collects all relevant logs, engineered features, and contextual metadata surrounding a flagged anomaly, including before-and-after activity.
- Forensic Packaging: Bundles compiled information into a structured archive; applies hashing and digital signatures to confirm authenticity.
- Integrity Verification: Checks packaged evidence for alteration; failed checks trigger re-packaging before archival.
- Archival Storage: Stores verified evidence in immutable, access-controlled repositories.
- Accessibility Control: Monitors evidence accesses to preserve chain of custody.
- Integrity Receipt: Generates a hash and timestamp for every archived bundle and forwards them to ADP for verification.

These activities transform flagged anomalies into forensically reliable evidence bundles ready for investigation or legal review.

3.3.4 Analyst and forensic review process (AFR)

This component provides the human analytical layer where preserved evidence is examined, interpreted, and reported. Figure 6 illustrates the investigative process in detail.

The main activities include:

- Examination of Evidence: Validates whether anomalies flagged by the detection engine correspond to genuine insider behaviour.
- Contextual Analysis: Assesses evidence against insider-threat scenarios and organisational policies.

- Interpretation: Determines whether behaviour indicates malicious intent, negligence, or benign anomaly, ensuring that conclusions remain evidence-based and traceable.
- Reporting: Compiles findings into structured forensic reports, logged concurrently in ADP for audit tracking.

AFR bridges intelligent detection with human reasoning, ensuring that automated outputs are converted into defensible investigative insight.

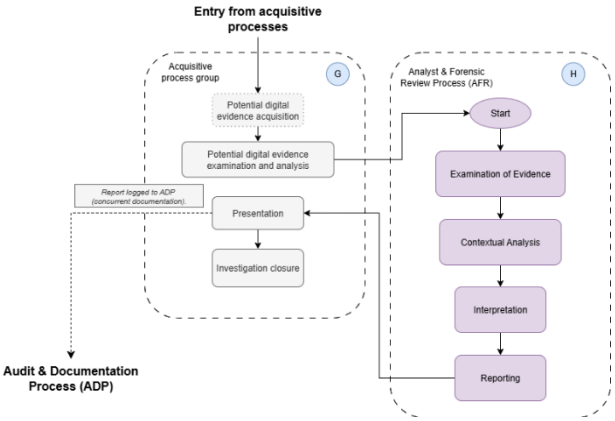

Figure 6: Integration of AFR within the investigative process class of ISO/IEC 27043

3.3.5 Audit and documentation process (ADP)

This component operates concurrently across all other processes to ensure documentation, reproducibility, and chain-of-custody assurance. The main activities include:

- Audit Trails: Automatically record every action from log capture to evidence analysis.
- Chain of Custody: Track and document access to evidence bundles.
- Reproducibility: Structure archived data and investigative steps so identical results can be reproduced.
- Quality Assurance: Conduct periodic integrity checks to confirm that forensic records remain complete and defensible.

As shown in Figure 1, the ADP runs concurrently beneath all components, reinforcing forensic integrity, traceability, and accountability at every stage of the digital investigation process. This concurrent layer ensures that DFR-BUST remains both operationally transparent and legally defensible.

The DFR-BUST model thus integrates the principles of ISO/IEC 27043 into a unified readiness-driven framework. Through its five components: SEP, DEP, EAP, AFR, and ADP, the model ensures that digital evidence in SaaS environments is captured, validated, and traceable before, during, and after incidents. While the framework spans all ISO process classes, its distinctive contribution lies in advancing forensic readiness, the capacity to generate reliable, auditable, and legally defensible evidence proactively.

This conceptual foundation also defines the logical structure upon which the intelligent forensic-readiness system is built. In the next section, DFR-BUST is operationalised as an adaptive system that embeds automated behavioural analytics, dynamic anomaly detection, and evidence-handling intelligence. This implementation translates readiness principles into active system behaviour, reinforcing the reliability, security, and auditability requirements identified earlier.

4. Intelligent Detection Engine

This section operationalises the Detection Engine Process (DEP) of the proposed DFR-BUST model. Machine-learning methods are embedded within this layer to detect behavioural deviations in a forensic-ready manner, ensuring that every anomaly flag remains traceable and admissible as digital evidence (Tan, 2001; ISO/IEC, 2015).

4.1 Dataset and Context

Experiments used the CERT r6.2 insider-threat dataset (Glasser and Lindauer, 2013), which extends earlier r4.2 and r6.1 versions to around 4,000 users across logon, device, file, and web logs. Unlike the older datasets, which contained approximately 1,000 users and multiple insiders per scenario, CERT r6.2 models a more realistic

enterprise with only five insider incidents, one per scenario. This design increases complexity and better reflects real-world conditions. Analysis focused on the Sales, Security, and Engineering departments containing these known insider cases, following some methodological precedents by Tuor et al (2017) and Sarhan and Altwaijry (2023).

4.2 Feature Engineering

Behavioural features were derived per user-day, representing actions such as after-hours logins, removable-drive use, file transfers, and device changes. Department-level aggregation reduced noise while preserving contextual meaning. Initially, features were manually selected based on domain knowledge, but model performance remained inconsistent until Deep Feature Synthesis (DFS) was incorporated. Following Kanter and Veeramachaneni (2015), DFS automatically generated higher-level features, such as frequency ratios, deviations, and temporal distributions, which were combined with manually selected ones to improve detection accuracy and behavioural representation within each department.

4.3 Models and Tuning

Two complementary anomaly-detection models were implemented within the DEP layer:

- One-Class SVM (OC-SVM): an unsupervised anomaly detector tuned via nu and contamination parameters to manage class imbalance. It was effective for identifying rare or subtle deviations.
- Isolation Forest (iForest): a tree-based ensemble method that isolates anomalies efficiently and is robust to noise and scaling issues.

Both models underwent iterative hyper-parameter tuning. PCA dimensionality reduction was tested for iForest to improve interpretability. Precision–recall balance was maintained through threshold and contamination adjustments. Together, the models form the analytical core of the DFR-BUST detection layer as shown in Figure 7, complementing forensic readiness by generating verifiable anomaly alerts.

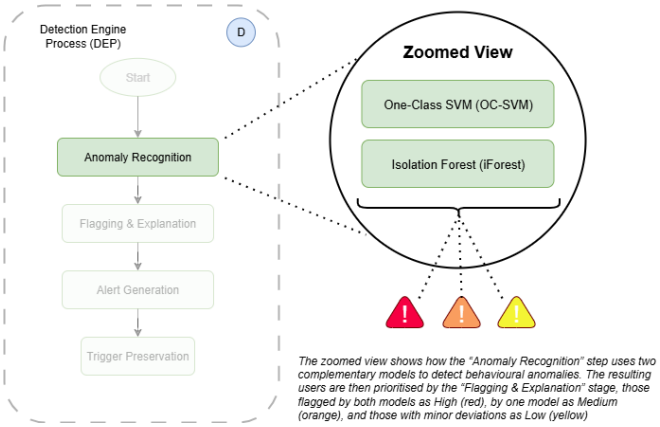

Figure 7: Integration of OC-SVM and iForest Models within the DEP Layer

4.4 Dataset Scenario 1: Model Performance Comparison

The first insider scenario depicts a user who began logging in after hours, using a removable drive, and uploading sensitive data externally before resignation. To benchmark results, Table 2 compares outcomes by Bin Sarhan and Altwaijry (2023) on the older CERT r4.2 dataset with results from this study using CERT r6.2.

Table 2: Comparison of Model Performance on Insider Scenario 1

Model	Dataset Version	Users	Insiders per Scenario	Precision	Recall	F1	Accuracy
OC-SVM (Bin Sarhan & Altwaijry, 2023)	CERT r4.2	~ 1,000	Multiple	0.94	0.86	0.89	0.86
iForest (Bin Sarhan & Altwaijry, 2023)	CERT r4.2	~ 1,000	Multiple	0.92	0.91	0.88	0.91
OC-SVM (This Study)	CERT r6.2	~ 4,000	1 per scenario	1.00	0.50	0.67	0969

Model	Dataset Version	Users	Insiders per Scenario	Precision	Recall	F1	Accuracy
iForest (This Study)	CERT r6.2	~ 4,000	1 per scenario	1.00	0.50	0.67	0.969

The expanded dataset and the single-insider structure naturally lowered recall but maintained high precision and accuracy, demonstrating practical forensic applicability rather than purely statistical optimisation.

4.5 All-Scenario Performance Summary

Performance across all five CERT r6.2 scenarios is summarised in Table 3. These include:

1. a user exfiltrating data before resignation
2. a user soliciting competitors while using removable drives
3. a user installing keyloggers and sending mass emails
4. a user accessing others' machines for file exfiltration
5. a user uploading company data to personal cloud storage

Table 3: Summary of Model Performance Across All Scenarios (CERT r6.2)

Scenario	Department	Model	Precision	Recall	F1	Accuracy
1	Sales	OC-SVM	1.000	0.500	0.667	0.969
1	Sales	iForest	1.000	0.500	0.667	0.969
2	Sales	OC-SVM	1.00	0.50	0.67	0969
2	Sales	iForest	1.000	1.000	1.000	1.000
3	Security	OC-SVM	0.333	1.00	0.500	0.935
3	Security	iForest	1.000	1.000	1.000	1.000
4	Engineering	OC-SVM	1.000	0.500	0.667	0.969
4	Engineering	iForest	0.182	1.000	0.308	0.719
5	Engineering	OC-SVM	0.000	0.000	0.000	0.938
5	Engineering	iForest	0.143	1.000	0.250	0.625

These results highlight the trade-off between model sensitivity and precision. iForest achieved perfect recall in Sales and Security scenarios, while OC-SVM offered higher selectivity. Together, they provide complementary strengths, balancing false-positive control with anomaly coverage. In addition, results indicate that departmental context significantly affects performance. For each department, the feature model pairing that best replicates its behavioural characteristics should be chosen, for example, engineering activity patterns differ greatly from those in sales or security. Therefore, the current combination performs well in some departments and could be replaced or fine-tuned in others to improve overall detection fidelity.

4.6 Flag Prioritisation and Forensic Integration

Within the DEP, outputs from both models were merged into a prioritised flagging system:

- High Priority: Users flagged by both OC-SVM and iForest.
- Medium Priority: Users flagged by one model but with high anomaly scores.
- Low Priority: Weak or inconsistent anomaly detections retained for reference.

Each flag is logged with model parameters and timestamps, then archived by ADP to ensure traceability and reproducibility. This process converts statistical anomaly detection into forensically admissible digital evidence.

5. Case Scenario of DFR-BUST Model

To illustrate the practical application of the proposed model, the following case scenario describes how the DFR-BUST framework operates within a cloud-based Employee Management System (EMS).

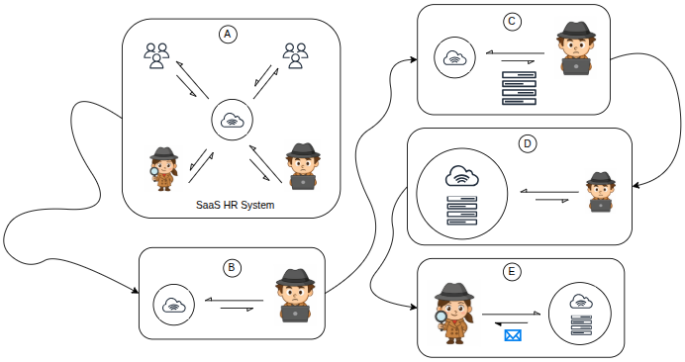

Figure 8: Case Scenario of DFR-BUST Model using Alice and Bob

At the readiness phase (A), the EMS continuously collects and prepares logs. A user (B) performs data-access activities outside business hours, triggering a deviation from baseline behaviour. The monitoring layer (C) captures detailed metadata, timestamps, file paths, and access volumes, and forwards it to the Detection Engine (D), where both OC-SVM and iForest models flag the event as anomalous. A structured alert is generated, and the Analyst and Forensic Review (E) process validates the findings, packaging the related data through the archival and audit layers.

This sequence demonstrates how DFR-BUST converts raw logs into actionable forensic intelligence while maintaining compliance and traceability. The model operationalises ISO/IEC 27043 by ensuring that evidence preparation, detection, preservation, analysis, and documentation function cohesively. Collectively, these processes uphold reliability, security, auditability, and cloud compliance, achieving the ISO goal of maintaining evidence that is both credible and legally defensible. The model's layered design confirms readiness through proactive preparation, traceable detection, and verifiable preservation.

6. Comparison with Related Work

Compared with prior studies, the DFR-BUST model offers a distinct integration of forensic readiness and intelligent anomaly detection. Tuor et al (2017) demonstrated that deep learning models could detect insider threats on early CERT datasets, but their approach remained performance-driven and did not address evidence admissibility or forensic soundness. Sarhan and Altwaijry (2023) explored hybrid supervised–unsupervised detection methods with strong precision metrics, yet without a readiness framework to preserve alerts for legal review. Similarly, Glasser and Lindauer (2013) introduced the CERT synthetic datasets to support insider research but did not propose a readiness model for operational environments.

In contrast, this study extends the forensic dimension by embedding AI models within the ISO/IEC 27043 process classes, ensuring that each anomaly flag is traceable, verifiable, and stored with chain-of-custody guarantees. The integration of Deep Feature Synthesis (DFS) and department-specific behavioural baselines provides contextual intelligence absent in prior work.

Moreover, while earlier studies emphasised accuracy over reliability, the proposed DFR-BUST model aligns with four critical dimensions. (Rowlingson, 2004; Tan, 2001; Greitzer et al, 2019; ISO/IEC 27043, 2015; Alqahtany et al, 2019)

- Reliability, as represented by the DFR principle, ensures that evidence remains consistent, complete, and scientifically defensible.
- Security, aligned with insider threat mitigation, focuses on proactively identifying and containing malicious activity.
- Auditability, rooted in forensic methodology, maintains an unbroken chain of custody and transparent documentation.
- Cloud Compliance, adherence to legal, operational, and privacy requirements across distributed SaaS infrastructures.

Collectively, these dimensions position DFR-BUST as both a technically adaptive and legally defensible advancement in insider-threat mitigation, bridging the gap between intelligent detection and forensic credibility in cloud environments.

7. Discussion and Conclusion

The findings confirm that embedding anomaly detection within a forensic-ready architecture enhances both detection reliability and evidential value. Although recall remains moderate, precision and admissibility are maintained, showing that AI-driven detection and forensic soundness are complementary rather than competing objectives (Tan, 2001; ISO/IEC 27043, 2015). The combined use of One-Class SVM and Isolation Forest balances sensitivity and precision while ensuring that all alerts remain traceable and legally defensible.

This study advances current practice by integrating Digital Forensic Readiness (DFR) and intelligent behavioural analytics within a unified, ISO-aligned framework. The proposed DFR-BUST model demonstrates that proactive evidence preparation, anomaly detection, archival, and audit documentation can operate cohesively in cloud environments, enabling organisations to generate verifiable and legally defensible digital evidence.

Some limitations remain. Detecting privileged or low-activity users (as in Scenario 5) was challenging due to limited behavioural signals. Computational constraints also restricted experimentation to selected departments, which may affect generalisability. Future implementations should therefore include richer telemetry, such as HR metadata and cross-departmental context, to improve detection coverage.

Further work should explore adaptive, multimodal learning that integrates enterprise telemetry with behavioural analytics while maintaining forensic traceability. Testing across additional datasets and live SaaS environments will help validate scalability and reliability. Addressing these aspects will enable DFR-BUST to mature into a robust, domain-independent framework that strengthens organisational resilience and supports trustworthy digital investigations.

Ethics Declaration: This study used only publicly available datasets and secondary scholarly sources. No human participants or personal data were involved; therefore, ethical clearance was not required.

AI Declaration: OpenAI's ChatGPT was used to assist with editing and summarizing reviewed materials for clarity and structure. All conceptual development, data analysis, experimental design, interpretation of results, and final decisions regarding structure, argumentation, and inclusion of content were made by the author, ensuring originality and accuracy.

References

Alenezi, M., Alarifi, A. and Alsaeedi, A. (2020) "Cloud forensic readiness: A framework for proactive digital investigations in SaaS environments", Journal of Cloud Computing, Vol. 9, No. 23, pp. 1–18.

Alqahtany, S., Clarke, N.L. and Furnell, S. (2019) "Developing a forensic readiness framework for cloud computing", Journal of Information Security and Applications, Vol. 45, pp. 1–11.

Bass, L., Clements, P. and Kazman, R. (2021) Software Architecture in Practice, Addison-Wesley, Boston.

Bin Sarhan, B. and Altwaijry, N. (2023) Insider Threat Detection Using Machine Learning Approach. Applied Sciences, 13 (1), 259. https://doi.org/10.3390/app13010259

CERT (2016) Common Sense Guide to Mitigating Insider Threats, 5th ed., Software Engineering Institute, Carnegie Mellon University, Pittsburgh.

Daniel, J. and Daniel, G. (2011) "Digital forensics: An overview of challenges in evidence collection and analysis", International Journal of Computer Applications, Vol. 36, No. 11, pp. 1–7.

Glasser, J. and Lindauer, B. (2013) "Bridging the gap: A pragmatic approach to generating insider threat data", Proceedings of the IEEE Security and Privacy Workshops, San Francisco, pp. 98–104.

Greitzer, F.L., Kangas, L.J. and Noonan, C.F. (2019) "A comprehensive framework for insider threat detection", Computers & Security, Vol. 87, pp. 101580–101590.

ISO/IEC (2015) Information Technology — Security Techniques — Incident Investigation Principles and Processes (ISO/IEC 27043:2015), International Organization for Standardization, Geneva.

Kanter, J.M. and Veeramachaneni, K. (2015) "Deep Feature Synthesis: Towards automating data science endeavours", IEEE International Conference on Data Science and Advanced Analytics (DSAA), Paris, pp. 1–10.

Kebande, V.R. and Venter, H.S. (2017) "A cloud forensic readiness as a service model", Computers & Security, Vol. 70, pp. 773–785.

Ponemon Institute (2022) 2022 Cost of Insider Threats: Global Report, Ponemon Institute, Traverse City, MI.

Rowlingson, R. (2004) "A ten step process for forensic readiness", International Journal of Digital Evidence, Vol. 2, No. 3, pp. 1–28.

Sarhan, M. and Altwaijry, H. (2023) "A hybrid machine learning framework for insider threat detection", Expert Systems with Applications, Vol. 219, pp. 119634–119642.

Singh, A., Tripathi, M. and Kumar, S. (2022) "SecureRS: A secure cloud-based forensic-ready storage architecture", Future Generation Computer Systems, Vol. 129, pp. 214–229.

Tan, J. (2001) Forensic Readiness, @Stake, Cambridge, MA.

Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N. and Robinson, S. (2017) “Deep learning for unsupervised insider threat detection in structured cybersecurity data streams”, Proceedings of the IEEE Workshop on Cybersecurity and Machine Learning, Prague, pp. 1–7.