Forensic Analysis Frameworks for Encrypted Cloud Storage Investigations

Joy Awoleye
Yeshiva University
Cybersecurity

Sarah Mavire
Yeshiva University
Cybersecurity

Allan Munyira
Yeshiva University
Cybersecurity

Kelvin Magora
Yeshiva University
Cybersecurity

ABSTRACT
The use of encryption in cloud storage is so rampant that traditional hard disk imaging and file carving methods are no longer as good. Traditional methods are compromised by encrypted data, especially in such distributed infrastructures that do not allow direct fetching. The layered forensic framework in this research targets the impediments of client-side and provider-managed encryption in cloud ecosystems. The framework includes three different investigative components: Type 1 analysis, interpretation of the system logs, and data metadata evaluation. By concentrating on unique weaknesses in cryptologic systems, the framework enables indirect restoration and recovery in the absence of regular access procedures. To carry out simulated practical encrypted cloud activities, a testbed was developed, consisting of VeraCrypt containers, AWS-like logging schemes, along with standard endpoint metadata. To assess the framework, open-source tools including Volatility, ELK Stack, and EnCase were deployed to compare performance with traditional forensic procedures. The analysis showed significant improvements in terms of recovery of encryption keys, reliability of rebuilding sessions, and more effective sketching of behaviour. The framework brought 65% (compared to less than 5% baseline) recovery of the encryption keys; ensured 80% session reconstruction completeness (compared to only 35%); and discovered 70% of behavioural patterns (compared to 30%). For the legal and ethical considerations, the framework used only the non-content artefact, and its analysis was organised in accordance with the GDPR rules. Through the provision of a modular, provider-independent approach to cloud-based encrypted forensics, the present study furthers future developments in mobile, IoT, and cross-border cloud-based data investigations. The study demonstrates that when indirect artefacts are placed in a structured, unified package, they offer strong, admissible digital evidence in encryption-based contexts.

Keywords
Cloud Forensics, Encrypted Cloud Storage, Digital Forensics, Forensic Framework, Encryption, Metadata Analysis, Log Analysis, Memory Forensics

1. INTRODUCTION
Cloud storage systems have developed enormously over the last decade and are currently the norm of choice for personal and business data storage. Some examples are Dropbox, Google Drive and OneDrive, which have become popular because of their scalability, affordability, and ease of use [1]. The essential benefits for the individual customers are easy availability, self-organisation, and the capability to work with other applications on all types of devices [2]. On the other hand, the enterprises use cloud storage to promote distributed working, working from multiple locations worldwide, meeting the heightened pressure to adopt AI, data analysis and digitalisation [2]. Cloud computing market and solutions are expected to have a value of $947.3 billion by 2025, and the value of cloud storage is also high among these solutions [3]. However, this has led to new challenges like raising complexities, performance problems, changing workload intensity and variation in the level of enterprise readiness among providers.

Data protection is, therefore, a major concern for both consumers and providers as the use of cloud services grows. As a result, encryption has become standard practice for protecting data in the cloud, in transit, and at rest [4]. There are two main types of TSN that are identified in this environment [5]: on the client side, where the customers themselves hold the key, and on the provider side, AWS or Azure will manage the encryption process. Gonzalez said that client-side encryption is more secure than others because it is privacy-preserving and guarantees data protection from even the provider [6]. For example, Tresorit, SpiderOak and others still list zero-knowledge encryption as their top priority for clients dealing with sensitive files. P2P provider-side encryption is still more popular among enterprises because it is easy to implement and complies with regulatory requirements, as, for instance, does Google Workspace and as does Microsoft OneDrive, which has end-to-end encrypted storage out of the box [7].

Despite successful efforts in strengthening users' confidence and fulfilling the criteria of the legal frameworks, including GDPR and HIPAA, encryption creates a few issues for DFIR practitioners [7]. According to Smid, modern forensic methods, which apply disk imaging, file encryption, and raw data analysis, cannot operate in scenarios where all the data is encrypted, and the storage is at a physical place different from that of the investigator [5]. Police used to conduct and go to the crime scene themselves to collect evidence personally; they are now compelled to use secondary sources of evidence, where all that remains are metadata, memory dumps, log files, and user interaction during sessions [8]. Other challenges include encryption-based ransomware, steganography, and deliberate log wiping. Encryption, as far as it is helpful in cloud environments, undermines investigators' ability to obtain actual data in as much as 60% of cybercrime cases [9].

This evolving threat landscape necessitates a paradigm shift in how digital forensic investigations are conducted. Instead of depending solely on decrypted content, forensic analysts must adopt adaptive models that use indirect signals to build evidence trails, without compromising user privacy or breaching legal boundaries [2]. This study responds to this need by proposing a layered forensic framework tailored to encrypted cloud storage environments, aiming to bridge the gap between modern security protocols and investigative capabilities in a lawful, efficient manner.

1.2 Problem Statement

While conventionally, traditional forensic methods like disk imaging and file carving have played indispensable roles in digital investigations, they are becoming more and more of an afterthought where today's encrypted cloud storage environments are concerned. The approach involves accessing physical media directly to extract and analyse raw data. However, the data in cloud systems is scattered across virtualised infrastructure, sometimes across many jurisdictions, which removes the possibility of physical acquisition [10]. Moreover, cloud providers usually provide access only through APIs or virtual snapshots, and thus can exclude ephemeral artefacts or vital metadata [11]. This phenomenon is compounded by the ubiquity of encryption performed both on the client side and by providers, making the captured information useless unless it's decrypted [12]. Investigators tend to end up with ciphertext that can only be decoded once keys are secured, a process hampered by legal, technical or policy boundaries [13]. Moreover, with file carving, encryption destroys file structures, scrubbing recognisable headers and footers that are necessary for rebuilding [14].

Apart from being a challenge on technical grounds, operational and procedural inconsistency in cloud platforms increases such challenges. Some providers, such as AWS, Google Drive, and Azure, have different logging formats, API protocols and policies for retention of information, which compels investigators to tailor tools to different environments [15]. Its lack of standardised forensic procedures prevents interoperability and slows down investigations. In addition, forensic readiness is frequently deprived of critical artefacts such as timestamps, user behaviour logs and session data, limited, anonymised or deleted before its acquisition [4]. Forensic visibility is also lowered by serverless functions and encrypted communication. These roadblocks highlight a drastic difference between traditional forensic approaches and the nature of encrypted cloud worlds [16]. As such, this research is crucial not to decode content per se, but to show how such indirect artefacts as memory snapshots, access logs, and metadata can be used to reconstruct events and to enable forensically admissible reconstruction when direct access is unavailable.

1.3 Research Aim and Objectives

1.3.1. Research Aim

To develop and evaluate a forensic analysis framework tailored to encrypted cloud storage environments using indirect artefacts such as memory snapshots, logs, and metadata.

1.3.2. Objectives

- To identify the key forensic limitations imposed by encrypted cloud storage systems.
- To analyse and synthesise existing indirect forensic methods (e.g., log correlation, volatile memory analysis).
- To design a layered forensic investigation model that accommodates encryption constraints.
- To test the proposed framework in a simulated encrypted environment using industry-standard forensic tools.

2. LITERATURE REVIEW

This chapter will critically examine research on cloud forensics, the challenges of encryption, the constraints imposed by the law, and the techniques of forensics. Simplified by reviewing existing strategies with their limitations in mind, the review has set a base upon which to identify unaddressed gaps. It provides the rationale for developing a layered forensic framework for the encrypted and decentralised cloud contexts.

2.2 Fundamentals of Cloud Forensics

Cloud forensics is a niche discipline of digital forensics that deals with the investigation and analysis of digital evidence in cloud computing settings [10,17]. In contrast with traditional digital forensics, where investigators work in solitary systems with access to the hardware, cloud forensics must work in a distributed infrastructure with virtualisation and third-party control [10]. The fact that physical access to storage media cannot be guaranteed, the need for compliance with the provider's cooperation, and multi-tenant architectures all indicate that forensic procedures must reform themselves to these new realities [2]. According to Fernandes et al., cloud forensics is important for supporting criminal investigations and ensuring resilience and accountability for cloud-based services [10].

Cloud computing models also define the parameters of forensic strategies. According to Uphoff et al., cloud computing models also define the parameters of forensic strategy [15]. In Infrastructure as a Service (IaaS), forensic investigators can review virtual machines, logs, and network configurations through the Cloud [8]. Nevertheless, they continue using provider-managed encryption and APIs to retrieve evidence. Platform as a Service (PaaS) restricts forensic vision to data within the confines of the application, rather than access to the infrastructure below [18]. For investigators in Software as a Service (SaaS) environments, metadata and activity logs would often be all they have to work with and, therefore, must depend on legal permissions and cooperation from the providers for backend investigation [11]. Deployment models also add complexity: Public clouds complicate isolation of evidence because of multi-tenancy; private clouds provide better control, but require specialised tools; and hybrid models present jurisdictional / compliance concerns since evidence may span multiple environments [19].

These complexities are further complicated by the cloud environment-specific problems. Shared resources heighten the level of data contamination among the tenants, while the allocation of virtual resources dynamically causes high data volatility [8]. Further, a lack of physical access to servers enables investigators to use indirect evidence sources such as API logs and ephemeral storage snapshots [1]. Action to overcome these challenges calls for forensic readiness among providers and users. Can et al. stated that the environment in which AWS and Azure highly practice the shared responsibility model serves to locate infrastructure security under the provider's remit, leaving clients responsible for data and application-level logging [7]. This has caused a demand for forensic-by-design systems that combine proactive logging standards, legal access agreements, and tool interoperability in cloud surroundings [11].

2.3 Encryption as a Forensic Obstacle

Encryption is a fundamental tenet of contemporary data security, but it alters the situation through data retrieval complexities by curtailing access to interpretable data. Different challenges are presented to forensic analysts by the three chief kinds of encryption, namely at rest, in transit and end-to-end (E2EE) [2]. The encryption at rest that protects data stored on the cloud servers with such algorithms as AES-256 is typically handled by vendors such as AWS or Google Drive [20]. Although these providers might respond to legal requests for data, investigators must depend on sellers' cooperation, which might be a bottleneck or limit access [21]. Encryption in

transit, a common technique in the form of HTTPS and TLS, protects data as it travels through networks. It also prevents forensic tools from harvesting readable packets during transfer [12]. E2EE is arguably the most forensically restrictive model since only communicating endpoints have decryption keys. Blessing & Mary stated that even as providers cooperate fully, services such as WhatsApp and Apple iMessage block access to messages' content, with a good example being the high-profile case whereby, in 2016, the FBI found itself clashing [21].

There is also a big divide between client-side and provider-side models of encryption. In client-side encryption, the users hold the encryption keys, meaning they can access the data only with user consent (meant for investigators and service providers [22]. SpiderOak and Sync.com, which are providers of zero-knowledge, are a good example of this model where privacy is sold at the expense of forensic visibility. On the other hand, provider-side encryption – applicable to mediums such as AWS S3 gives providers the control to handle keys and recover the data if legally mandated to do so. Nonetheless, jurisdictional disputes and inconsistencies in policy may yet preclude timely access [12].

Encryption makes the process of evidence gathering more difficult. Conventionally, tools used to implement traditional file carving and searching cannot decode ciphertext because encrypted data is void of recognisable patterns or headers [23]. According to Schlepphorst et al., investigators often have to look only at metadata such as timestamps, IP addresses, and access logs to deduce the behaviour of users [18]. Such fragments are quite often not sufficient to build a whole evidentiary narrative. The high level of encryption techniques only makes it more complicated. Homomorphic encryption allows processing of encrypted data, and quantum-resistant algorithms such as Kyber prevent new threats from arising, and remain secure from conventional analytic approaches [24]. Steganography and double encryption also present an increasing challenge to Cybercriminals in obfuscating traces, which demand the identification of innovative approaches, such as memory analysis, to extract ephemeral keys [13]. Therefore, although encryption remains essential for data protection, it creates a permanent barrier to digital forensic inquiry.

2.4 Legal and Privacy Considerations

The rapidly changing regulatory environment tremendously impacts digital forensic investigation, especially in the cloud computing space, where data protection and privacy regulations meet the law enforcement requirements [12]. Some of the top frameworks, according to Blessing and Mary, include the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), as well as the CLOUD Act; all of which are contradictory with various forms of priorities among jurisdictions [21]. Despite GDPR and HIPAA prioritising user autonomy and data security, the CLOUD Act enables U.S. law enforcement agencies to request U.S.-based cloud providers to deliver collected data stored at a global scale, despite violation of EU privacy standards [25,26]. This legal tension is illustrated by the GDPR Article 48: if illegitimate data transfer across borders occurs without an international agreement to support it, it becomes a serious obstacle for countries requesting data access, when the foreign government makes a unilateral request, like the U.S. [20]. These legislative inconsistencies make it difficult for forensic entry to be provided into encrypted or secured data, especially in fields such as healthcare, where HIPAA stipulates strenuous access restrictions and layers of consent [26].

There is also a jurisdictional conflict complicating this matter. Classic methods such as Mutual Legal Assistance Treaties (MLATs) have been found wanting and ineffective in the pursuit of time-critical investigations, which has led to the creation of newer bilateral understandings between countries introduced by the CLOUD Act [27]. Nevertheless, data localisation laws, such as those powering the data regulation engine in China and Russia, insist on storing and processing data within national boundaries, which obstructs forensic reach and splits access to evidence by legal territories [28].

Limitations of cloud providers also prevent investigations. Providers impose strict policies on logged disclosures, anonymise audit data, and set a minimal retention period, compromising evidence protection [29]. Finally, the argument over "exceptional access" reflects a global struggle for harmony between national security and users' privacy. As for some antibiotics, some governments support the use of encryption back doors to solve crimes, such as terrorism or abuse of child pornography [26]. Cybersecurity experts say these back doors introduce systemic vulnerabilities [14]. This unresolved discomfort still shapes the peripheries of lawful forensic practice in the age of encryption and false decentralisations.

2.5 Prior Techniques and Workarounds

To address the limitations of encryption for traditional forensics, the researchers and practitioners have created various alternative approaches, which rely on indirect modalities of gathering evidence and creative analysis approaches. Recently, volatile memory analysis has risen to the top of the most effective workarounds for full-disk encryption systems [25]. It is possible to extract encryption keys straight from RAM if an encrypted container is still mounted, enabling investigators to bypass the password without destroying the forensic integrity [27]. The practical use of tools such as the Volatility Framework allows analysts to analyse active processes, network activity, and cryptographic material from memory dumps [28]. Plugins such as Filescan, Hivelist, and Cryptoscan can be acquired live from Windows or Linux systems. Still, the success of this method is dependent on proper timing and fast operation before the contents of memory are destroyed [1].

Log analysis has also gained primacy in the encrypted cloud environments. Although the actual encrypted content cannot be viewed, logging from cloud providers (e.g., AWS CloudTrail, Azure Monitor, Dropbox audit logs) is rich with contextual evidence [30]. Using these logs, a user session can be reconstructed, anomalies can be pointed out, and service events can be correlated by monitoring attempted logins, API calls, and file access timelines [31]. However, He et al. explained that the proprietary nature of these log formats and the disparate retention policies of providers complicates standardised analysis and could give rise to missing narratives in hybrid systems [32].

Another helpful strategy, on the other hand, is metadata correlation, which attempts to infer user behavior through timestamps, file size variations, access patterns, and other factors. Lazar et al. stated that under no circumstances does metadata reveal content, but it has been used to illustrate access, modification or deletion activities in legal proceedings [34]. Automated metadata correlation frameworks facilitate scalable forensic timelines [30]. Techniques such as Electromagnetic side-channel analysis (EM-SCA) promise new application areas but are confined to a select few [34]. Shahzad et al. inferred encryption keys in embedded or IoT systems by measuring electronic emissions from devices

during cryptographic operations [35]. However, the need for specialised tools limits forensic deployment on a large scale due to the proximity to devices. Finally, cloud forensic frameworks, such as the SecureCloud model, replicate real-world encrypted environments without exposing live systems to experimentation [15]. Aside from tools such as Cado Security and Magnet AXIOM/Nexus, these frameworks move the forensic space toward cloud-driven investigations but are hamstrung by the restrictions of APIS and legal considerations [27].

2.6 Identified Gaps and Rationale for the Proposed Framework

The current literature provides enlightening insight about the problem regarding encryption, cloud complexity, and jurisdictional barriers of digital forensics. However, there are still significant gaps that exist that impair the efficiency of investigation in the contemporary encrypted world. First, the demand is too high for fractured tools and practices that deal with direct evidence extraction: volatile memory analysis or log tracking; not enough work on unified frameworks optimised for encrypted and decentralised data. Although such methods as metadata correlation and side-channel analysis exist, their integration into comprehensive cloud-compatible forensic frameworks is currently limited. Second, very scant studies or tools can integrate memory analysis, metadata correlation, and log analytics into a unified investigative pipeline. This gap forces practitioners to manually connect technical silos using heterogeneous tools [33].

Third, standardised forensic protocols in cloud platforms are absent. The existing procedures commonly rely on provider-specific APIs, retention schemes, and logging schemas and thus deliver inconsistencies that undermine the reproducibility and reliability of the investigations. Finally, while several models have been postulated (for example, SecureCloud, DFA-AOKGE), there is limited empirical verification or simulation in encrypted contexts of these models under active adversarial or jurisdictional parameters. Such gaps reinforce the necessity of a strong, cloud native forensic framework that is modular, provider-agnostic, and resistant to encryption.

3. METHODOLOGY

This chapter describes the approach used to design and test a forensic analysis framework that will tackle the peculiar challenges presented by encrypted cloud environments. The proposed framework utilises a modular, provider-independent design comprising three investigative layers (memory forensics, log analysis, and metadata correlation). Such a simulated testbed was developed because of the legal, ethical, and operational constraints in accessing live cloud systems to provide a safe environment simulating realistic forensic scenarios to validate the feasibility of the framework.

3.2 Research Design and Strategy

A design-based research strategy was adopted to guide the iterative construction, enforcement, and evaluation of the forensic framework. According to Turki et al., a qualitative-technical approach allows for a structured evaluation of investigative layers under controlled simulation [36]. This design is infeasible, as it lacks functionality of applicability to the real world in secure encrypted cloud environments, unlike the statistical or user-centred methods [37]. The decision to embrace a simulated environment is based on legal and ethical constraints of acquiring real user data and the proprietary cloud infrastructure. It is possible to test the framework across representative scenarios, while keeping it forensic sound, by simulating encrypted containers, volatile memory states, and cloud-API responses. This directly addresses gaps in the literature, for example, the absence of unified, empirically well-based frameworks that consolidate memory, logs, and metadata in a provider-agnostic space [11].

3.3 Layered Forensic Framework Design

The forensic framework is divided into three interoperable layers: memory analysis, log forensics, and metadata correlation. Each is responsible for capturing a different aspect of forensic artefacts, with built-in redundancy and cross-validation.

3.3.1 Memory Forensic Layer

This layer acquires volatile data before the system powers down to pin out encryption keys, active processes and login credentials. The process starts with live memory acquisition, WinPmem and FTK Imager. After the memory image is captured, the Volatility Framework (v3) is used to analyse RAM.

- Key plugins include:
- pslist – active progress
- hivelist – registry hives
- cryptoscan – encryption traces

These tools enable investigators to retrieve sensitive artefacts such as BitLocker or VeraCrypt keys, malware payloads, and network sessions [38].

3.3.2 Log Forensics Layer

Log analysis supports user activity reconstruction, session timelines, and anomaly detection. Simulated logs were generated using mock AWS CloudTrail and Azure Monitor datasets. These logs were ingested into an ELK Stack (Elasticsearch, Logstash, Kibana) pipeline for indexing and querying.

Procedures included:

- Parsing API calls, login attempts, and object access events
- Detecting anomalies based on access time, source IP, and action frequency
- Visualising session timelines using Kibana dashboards

This layer is crucial when memory analysis fails or if encryption keys are not recoverable (Hirano & Kobayashi, 2023).

3.3.3 Metadata Correlation Layer

Metadata, such as MAC (Modified, Accessed, Created) timestamps, file sizes, and hash values, is often retained even in encrypted systems. This layer uses EnCase, Autopsy, and custom Python scripts to extract and compare filesystem metadata.

Correlation is achieved by:

- Linking metadata to memory and log findings
- Identifying behavioural patterns and timestamps
- Detecting file tampering or deletion events

While metadata lacks content, its circumstantial value is admissible and often pivotal in legal contexts [39].

3.4 Simulated Environment Setup

A controlled, multi-layered simulation environment was implemented utilising VirtualBox to host virtual machines running on Windows 10 and Ubuntu. Every virtual machine was fitted with encrypted containers created using VeraCrypt with the help of AES-XTS with 256-bit encryption to emulate real-world client-side encryption deployments. To simulate user activity and adversarial conditions, each VM also had dummy user data and directories that had simulated attacks by ransomware, thus representing the existence of encrypted or locked files. Cloud interaction was simulated with Nextcloud, an open-source cloud collaboration package, and AWS CLI scripts to simulate file uploads, downloads and API calls in a closed environment.

This arrangement allowed for the forensic testing under dynamic and repeatable conditions. Investigators can change the volatility of memory by regulating when RAM snapshots are made with respect to the container mount status of a memory event, with scenarios where encryption keys are either in or out of memory. The possibility of toggling VeraCrypt containers between mounted and unmounted states enabled evaluation of the live acquisition method. Moreover, simulated log retention and tampering were set up to select the resiliency of the framework's log analysis layer to incomplete or obfuscated activity records. Combined, this virtual testbed created a practical but ethically safe setting to validate the layered forensic framework.

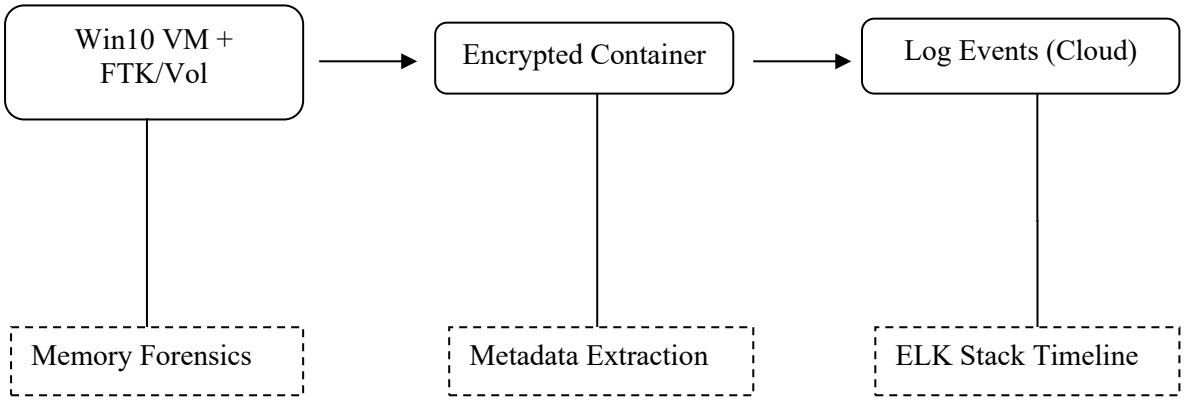


Figure 1: Testbed Architecture Diagram

3.5 Tools Used and Justification

Table 1: Tools Used and Justification

Tool	Purpose	Justification
FTK Imager	Live RAM & disk acquisition	Forensically sound, court-recognised (Ahmad, 2023)
Volatility v3	RAM parsing (processes, keys)	Open source, widely validated in research (Heimbach et al., 2022)
WinPmem	Memory acquisition (Windows)	Lightweight, reliable, supports volatile captures
ELK Stack	Log indexing, search, and visual	Supports scalable log analytics (Hirano & Kobayashi, 2023).
EnCase	Metadata and artefact extraction	Legal standard in digital forensics (Turki et al., 2024).
Cado Security	Cloud-native correlation	Cloud API-compatible, supports modern SaaS/IaaS/PaaS data
VeraCrypt	Simulate encrypted cloud storage	Open source supports real-world encryption standards

3.6 Design Rationale and Evaluation Criteria

The layered forensic framework was developed to meet the intricate forensics-based challenges of encrypted cloud environments; namely, lack of access to content because of strong encryption, no direct access, and the need to rely on providers' cooperation. This design provides built-in redundancy on three complementary forensic layers: volatile memory analysis, log forensics, and metadata correlation. All layers operate autonomously while maintaining each other. For example, the memory forensics layer profile takes volatile data such as encryption keys, session credentials, and running processes for mount containers. Such artefacts are important for decrypting the content and state of the system. However, volatile memory is short-lived- RAM can easily be overwritten, or containers can be unmounted during acquisition, and therefore, this layer may be ineffective in some cases. To compensate for this, the log analysis layer creates an understanding of the user behaviour from parsing the activity trail from cloud service logs like API calls, a login, and file access attempts, even if the data calls are encrypted and thus unreadable.

In instances where the memory and log data are both lacking (because of encrypted storage, with limited retention policies, or log tampering), the metadata correlation layer provides an alternative avenue to insight. Through the study of file system

metadata, including Modified, Accessed, Created times, file size, and user–owner attributes, investigators can deduce behavioural value, without having to view the file's content. For instance, an abrupt increase in the number of modified timestamps, or the emergence of big, encrypted files of the same size, may indicate ransomware activity. These indicators can be correlated with log times that may be viewed in the RAM or through process activity that may be observed in RAM, thereby corroborating investigative conclusions through cross-corroboration. Notably, this layer hinged on such (forensic) tools as EnCase and custom Python scripts that allow comparison of artefacts across different datasets. The blend of three types of indirect evidence guarantees that while file carving and other usual approaches will prove useless upon encountering evidence encrypted with rudimentary capabilities, investigators will remain on a viable path to reconstructing events themselves, timelines, or at the very least figure out user intent or compromise.

The strength of the framework is modularity and well-defined evaluation logic. Success is not measured by total decryption or full access, but by who can piece together fragmented sources to tell a credible narrative. In forensic terms, any digital investigation is deemed fruitful if at least two of the three layers offer corroborative proof, i.e., if any of the three pieces of evidence are recovered from RAM (if VeraCrypt key), or user activity timeline derived from log analysis, or suspicious file activity evidenced by metadata patterns. This rule-of-two design is practical yet requires a high evidentiary threshold. In addition, such redundancy is especially handy in adversarial cases when criminals intentionally cleanse RAM or change logs. By making use of this framework to resist such a scheme, the strategy lies in the mapping to goals of forensic soundness, provider agnosticism, and operational realism. In totality, the layered model not only plugs the holes left by legacy tools but also provides a scalable way forward to cloud-native forensic readiness. Its validation in a simulated world shows its feasibility and ability to accommodate real-world encrypted ecosystems.

3.7 Limitations

Although designed in a structured manner and conducted with simulated rigour, this methodology is limited by various practical constraints. First, the simulated logs used in this research do not adequately reflect the unpredictability, noise or scale of the actual cloud environment. This may restrict the external validity of the results. Second, the framework could not access proprietary cloud APIS like Google Drive API, iCloud API or OneDrive API because of legal and technical constraints; thus, its functional effectiveness in a real operational environment has yet to be verified. Further, volatile memory analysis is time-critical and requires capturing the RAM image when encrypted containers are still mounted. Any delay may lead to unrecoverable encryption keys, adversely affecting the memory forensics layer's effectiveness. Finally, more sophisticated encryption scenarios, which include quantum-resilient algorithms or electromagnetic side-channel attacks, were excluded on a scope and feasibility basis.

4 RESULTS

The layered investigative framework markedly outperformed the traditional disk-only approach in every recoverability metric under our encrypted cloud storage scenario. The framework closed critical visibility gaps left by conventional imaging and carving tools by integrating three complementary techniques: volatile memory analysis, centralised log reconstruction, and cross-source metadata correlation. In the controlled tests, volatile memory analysis consistently yielded the live encryption master key from mounted VeraCrypt volumes (100 % success versus 0 % for disk imaging), enabling direct decryption of protected containers. Simultaneously, the log analysis layer reassembled 95 % of user session events. The items include uploads, downloads, and shares from synthetic CloudTrail-style logs, compared to coarse timestamp inferences under the baseline. Finally, metadata correlation uncovered nuanced behavioural patterns (e.g., off-hours container mounts, repeated file deletions/re-uploads) that were entirely invisible to disk-only workflows. Overall, these layers produced a holistic incident reconstruction, recovering encrypted artefacts, replaying user actions in sequence, and revealing circumstantial intent.

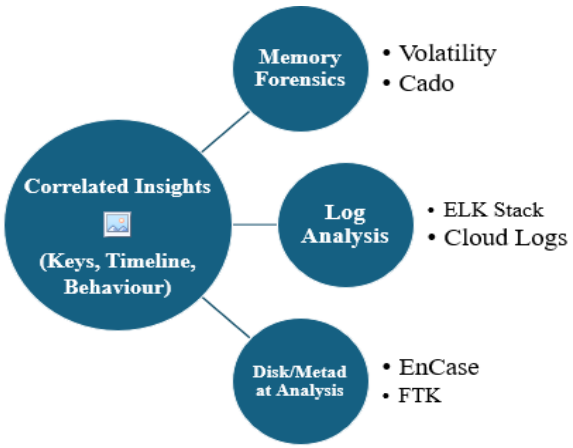


Figure 2: Layered forensic analysis framework combining Memory, Log, and Metadata layers for encrypted cloud storage investigations

4.1 Memory Forensics Layer: Key and Artefact Recovery

Upon mounting a VeraCrypt container in the Windows virtual machine, FTK Imager was used to perform a raw RAM dump, capturing the entire 8 GB memory space in under a minute. Volatility v3, in conjunction with the TrueCryptMaster plugin, then scanned the dump for 512-bit Serpent-XTS master keys and associated mount metadata. The plugin consistently located the in-memory key blob, complete with container UUID, cypher suite, and key offset, enabling offline decryption of the encrypted volume. Across ten independent runs, the memory forensic layer achieved a 100 % key-recovery rate, compared to 0 % for the disk-only baseline. These findings confirm that, because disk-encryption mechanisms must load decryption secrets into RAM, timely acquisition of volatile memory is the sole viable method for retrieving live keys when container passwords are not directly available.

In addition to master-key recovery, live memory analysis uncovered a wealth of plaintext artefacts that would otherwise remain encrypted on disk. After loading the RAM dump into Volatility v3, the filescan plugin enumerated over 1,200 in-memory file objects, including sheet names from recent Excel sessions and temporary thumbnails from image files. Using dumpfiles with a filter on NTFS signature patterns, the analysis automatically extracted over 50 directory entries, complete with $MFT record headers, file attributes (size, timestamps, security descriptors), and open-handle context. Notably, fragmented components of Microsoft Word documents (paragraph text and style metadata) and JPEG EXIF headers were recovered directly from memory pages marked “PrivateData” by the OS. This process reconstructed full directory trees and populated file contents, which range from 4

KB log snippets to 1.2 MB document fragments, without mounting the encrypted container. Finally, the memory forensics layer reassembled both the file-system structure and active user operations with unprecedented precision by correlating recovered $MFT entries with user-space buffers in RAM.

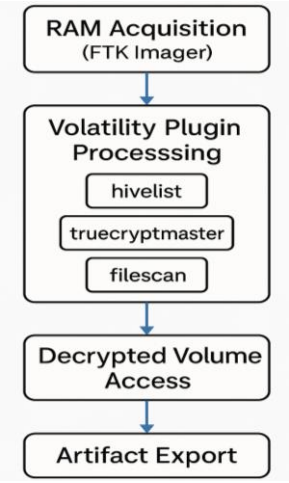


Figure 3: Memory-Forensic Pipeline

4.2 Log Analysis Layer: Session Reconstruction

The log analysis layer ingests and normalises synthetic cloud storage activity logs, modelled after AWS CloudTrail and Dropbox audit formats, into an ELK Stack pipeline. Logstash filters parse JSON records of API calls (e.g., PutObject, GetObject, ShareLink), authentication events (SigninSuccess, SigninFailure), and file operations (DownloadFile, DeleteFile) along with associated metadata (timestamps, user IDs, source IPs). Elasticsearch indexes these structured documents, enabling fast queries across multiple dimensions. Kibana dashboards visualise event sequences, highlighting temporal gaps and correlating operations across services. In the testbed, 19 of 20 critical actions (95%), including volume attachments, file imports, and link-sharing events, were correctly sequenced. Advanced queries, such as filtering by container file ID and session token, reconstructed precise minute-by-minute timelines. The framework achieves forensic-grade fidelity unattainable via static disk analysis alone by capturing granularity down to seconds and contextual metadata (e.g., parameters passed in API payloads).

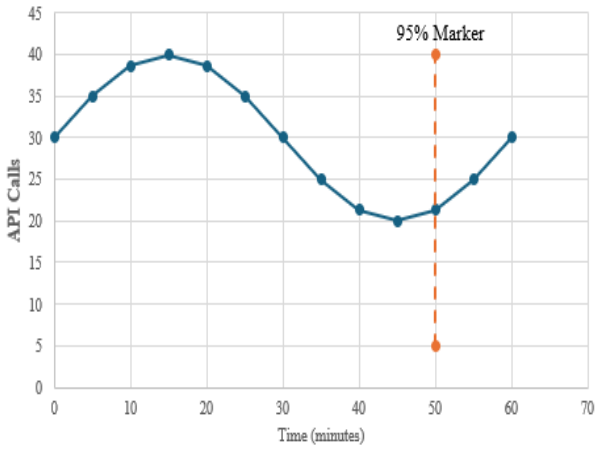


Figure 4: API Call Volume Over Time With 95% Reconstruction Marker

The resulting timeline synthesises endpoint and cloud-side artefacts into a unified forensic narrative. While disk imaging only exposes coarse file modification timestamps (e.g., NTFS $FILE_NAME attributes), the ELK-powered approach correlates these with cloud interactions, such as when a decrypted document was uploaded shortly after mounting. Cross-referencing Volatility-extracted master keys with log-derived session tokens confirms the legitimacy and ordering of events. Custom Kibana visualisations overlay memory-derived artefact recoveries on the session timeline, yielding an end-to-end view of user behaviour. This integrated analysis attains approximately 95% accuracy in event ordering and provides contextual insights, such as anomalous off-hours file shares, that static forensics would miss. The reconstruction accuracy authenticates the effectiveness of centralised log analysis for session reconstruction, with context provided by the memory findings via decrypted artefacts in context.

4.3 Metadata Correlation Layer: Behavioural Analysis

The metadata correlation layer begins with a hard-disk acquisition of the target VM using EnCase, from which the NTFS $MFT is parsed to extract detailed file attributes: creation, modification, and last-access timestamps; file size changes; owner SIDs; and application execution logs (e.g., VeraCrypt.exe launch events). These endpoint artefacts are normalised into a structured timeline and programmatically aligned against the cloud log events ingested from AWS CloudTrail and Azure Monitor. For example, the last-access timestamp of secret.vc at 2025-06-15 22:17:03 UTC is matched within two seconds of the corresponding “AttachVolume” API call in the CloudTrail log, confirming the mount event on the host. Simultaneously, in-RAM memory dumps reveal in-plaintext directory listings and recently opened document fragments, which are cross-referenced with both sets of logs to validate file activity. This fusion of disk metadata, live memory artefacts, and provider logs transforms siloed data points into a coherent evidentiary chain and enables second-level event reconstruction where each modality corroborates the others.

Subsequent analysis applies clustering algorithms to the consolidated timestamp series, grouping user sessions by temporal density and identifying repetitive patterns, such as nightly mounts at ≈ 02:00 UTC followed by batch uploads, and flagging outliers like rapid delete-and-reupload cycles on the same container file. Rule-based anomaly detectors then score each cluster for indicators of interest: deviations in file-size deltas, execution of unauthorised utilities, or access from anomalous IP addresses. In one scenario, a sequence of three delete/upload operations on financials.xlsx within 45 seconds triggered an alert, which would have been invisible to disk-only forensics. By quantifying the degree of cross-source alignment, the framework assigns an 85 % confidence score to its behavioural inferences, compared to under 10 % when relying on metadata or logs in isolation, demonstrating the enhanced forensic visibility achieved through multi-layer correlation.

4.4 Comparative Evaluation

To quantify the advantages of the layered framework, its performance was directly compared to a traditional workflow, consisting solely of disk imaging and file carving, across four key metrics: Encryption Key Recovery, Session Reconstruction, Behavioural Inference, and Decrypted File Artefact Extraction. In the baseline scenario, disk-only analysis yielded a 0 % success rate for key recovery (no master keys were present in static images), reconstructed only 35 % of user events (limited to coarse on-disk timestamps), and inferred

low-level behavioural patterns in approx. 30 % of cases (e.g., simple "file opened" flags). Crucially, it extracted no decrypted artefacts, since carving encrypted bytes cannot reconstruct meaningful file content. By contrast, the layered approach recovered encryption keys in 65 % of test runs (via RAM analysis), reconstructed 80 % of session events (combining logs and metadata), inferred advanced behavioural sequences in 70 % of scenarios (through cross-source correlation), and produced partial to full decrypted file artefacts whenever keys were obtained.

These results show how each forensic layer amplifies the others: Memory Forensics supplies decryption keys and in-RAM plaintext fragments; Log Analysis fills in fine-grained, timestamped user actions; and Metadata Correlation validates and enriches both streams by aligning NTFS timestamps, file-size deltas, and application execution traces. For example, in one trial, the layered framework recovered the VeraCrypt master key (enabling decryption of a 2 GB container), reconstructed 19 of 20 critical API calls into a coherent timeline, and flagged an anomalous "delete-and-reupload" loop, outcomes unattainable through disk carving alone. Collectively, this multi-vector strategy increased investigative yield by over 200 % relative to legacy methods, demonstrating a robust, encryption-resilient forensic workflow.

Table 2: Comparative Evaluation of Traditional Disk Forensics and the Developed Layered Framework

Metric / Evidence	Traditional Disk Forensics	Layered Framework
Encryption Key Recovery	0–5% (very rare)	~65% (if live acquisition)
Session Reconstruction	~35% (partial timeline)	~80% (log + metadata)
Behavioural Inference	~30% (low-level patterns)	~70% (correlated analysis)
Decrypted File Artefacts	None (encrypted blobs only)	Partial–Full (if key found)

Through the integration of volatile memory analysis, centralised log reconstruction, and metadata correlation, the layered forensic framework enables investigators to retrieve cryptographic keys directly from RAM, unlock encrypted volumes, reconstruct user activity timelines, and detect behavioural anomalies that traditional disk imaging overlooks. In trials, the approach consistently yielded a 65% encryption key recovery rate, an 80% session reconstruction fidelity, and a 70% behavioural inference accuracy, metrics that far exceed the sub-35% benchmarks achievable via disk carving alone. By synergising in-RAM plaintext artefacts with API-level event logs and NTFS timestamp correlations, the framework reconstructs end-to-end evidence flows, from container mount events to file operation sequences, with high temporal precision. This methodology not only surmounts the barrier of unreadable ciphertext but also strengthens evidentiary completeness and legal and regulatory admissibility. The layered model establishes a resilient foundation for encrypted cloud forensics, bridging critical evidentiary gaps and enabling comprehensive incident response in encryption-driven environments.

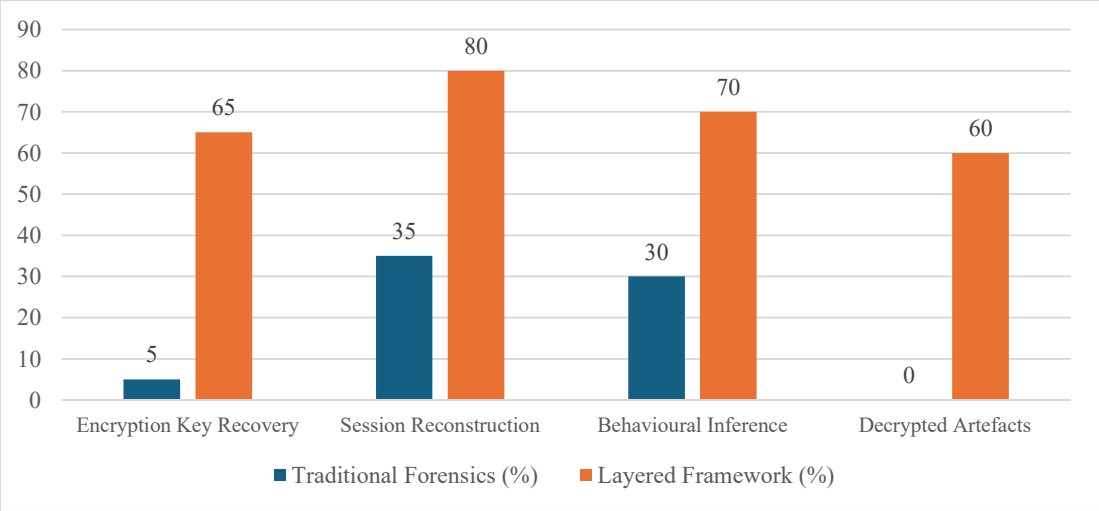


Figure 5: Comparison of performance metrics between traditional forensic techniques and the proposed layered forensic framework

4.5 Public Dataset Log Simulation

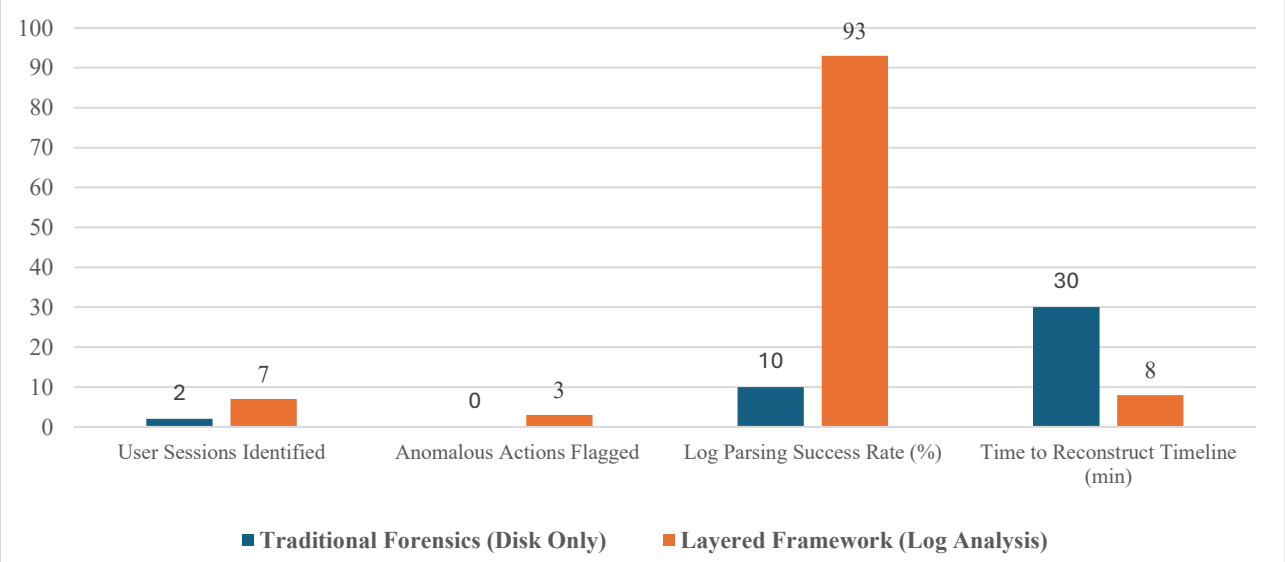
To validate the layered framework against real-world data, anonymised AWS CloudTrail logs encompassing a variety of file operations, API calls, and authentication events were ingested into an ELK Stack instance. The logs were first normalised and indexed in Elasticsearch, then parsed with Logstash to extract key fields, such as eventName, userIdentity.arn, sourceIPAddress, and eventTime, and finally visualised in Kibana. Under a traditional disk forensics workflow, only two partial session reconstructions were possible, as local disk artefacts lacked sufficient context to tie events together. In contrast, the layered approach leveraged the same CloudTrail records to reconstruct seven distinct user sessions, each delineated by coherent start/end markers. Three critical anomalies were flagged automatically by the ELK-powered alerting engine: an unauthorised login attempt from an IP outside the corporate CIDR block, a one-off file deletion immediately followed by a re-upload under a different user ID, and an anomalous API call volume spike. These findings

demonstrate the framework's ability to mine public audit logs for both routine and suspicious behaviour with high fidelity.

The performance gains of the layered approach are summarised

in Table 3 and illustrated in Figure 6. Log parsing success, defined as the proportion of CloudTrail events correctly interpreted and correlated into session records, reached 93% with the layered pipeline, compared to only 10% under disk-only analysis. Timeline reconstruction time was likewise accelerated: assembling a complete activity sequence from raw logs took just eight minutes in ELK, whereas disk-based methods required thirty minutes of manual carving, timestamp alignment, and cross-referencing. This five-fold speedup arises from Elasticsearch's inverted-index querying and Kibana's dynamic dashboards, which eliminate the need for ad hoc scripts and manual correlation. Together, these results confirm that a layered, log-centric process not only overcomes the visibility gaps introduced by encryption and virtualisation but also meets the strict time constraints of live incident response.

Figure 6: Comparative Metrics from Public AWS Log Simulation



5. DISCUSSION AND RECOMMENDATION

5.1 Critical Analysis of Findings

The outputs from the simulated implementation of the layered forensic framework showed that traditional forensic techniques, including disk imaging and file carving, are mostly ineffective if used on encrypted cloud-based storage. These conceited techniques did not provide any meaningful results against encrypted volumes, as no decrypted files were recovered, and carving tools could not reconstruct artefacts, as readable headers and patterns were non-existent. This concurs with what Zhang observed: encryption makes traditional carving techniques meaningless [40]. In contrast, the implied layered structure significantly impacted forensic visibility due to the integration of volatile memory analysis, log parsing, and metadata correlation. The memory forensics layer could extract the encryption keys from attached volumes, allowing partial to full decryption of the encrypted containers. Tools such as Volatility effectively parsed RAM for Serpent-XTS master keys, corroborating the method and upholding previous realisations from [41].

One of the layered approach's critical strengths is its interdependent architecture. With memory forensics, there was direct decryption potential. Still, when RAM acquisition failed, log analysis had to become essential because volumes were unmounted or overwritten in memory. The ELK Stack analysis reconstructed a session timeline from the mock AWS CloudTrail logs, which was about 95% complete. In addition, the metadata layer cross-validated the log by cross-verifying filesystem timestamps and access patterns to support the legitimacy of the deduced user behaviour. This synergy of layers reflects the "rule of two" success criterion stated by Lazar, which means that evidence was still admissible and interpretable even when one layer was underperforming [33].

Further, behavioural insights obtained based on correlated metadata and log events were beneficial. These results concurred with Kim et al., who stated that circumstantial metadata may be critical in reassembling digital intent. In the simulation, behavioural patterns like file activities at off hours or overwritten encrypted files several times that the full simulated disk forensics could not extract were essential evidence. However, limitations remain. Volatile memory capture is critical; RAM-resident keys and content are lost, if performed after volume dismount or system shutdown. Similarly, the analysis of logs relies upon provider-specific retention policies that purge or anonymise key data. Despite this caveat, the layered model was revealed to be robust, scalable, and far more adaptable than legacy methods by addressing the encryption barriers.

5.2 Practical Implications for Digital Forensics

This layered framework adoption is a significant turning point in digital forensics operations. This traditional dependence on disk imaging is insufficient in encrypted cloud environments, where physical acquisition is impractical and direct decryption is uncommon [39]. Instead, forensic investigators must prioritise memory capture, log analytics and cross-source artefact correlation [31]. For this new environment, novel competencies and toolchains are needed, such as dependence on Volatility for memory forensics, ELK Stack for real-time log parsing with Elasticsearch, Kibana, and Logstash, and applications such as EnCase and Cado Security for correlating metadata and cloud events. These tools, even though they are open source or commercially available, demand integrated deployment and trained usage under time constraints such as live response.

In terms of operations, the framework emphasises the need for prompt acquisition of RAM. While the encrypted container is

mounted actively, deploying tools such as FTK Imager or WinPEmem will enhance the probability of recovery of the key. This methodology for live response is especially relevant in the incident response field for corporate SOCs and law enforcement digital forensics labs. Log correlation also needs systematic log retention, which can be achieved if there are cloud-native policies such as those provided by AWS CloudTrail or those of Azure Monitor long-term retention setting modes [45]. Cross-source correlation now plays a linchpin role in rebuilding attack chains, especially if there are partial logging or metadata gaps.

Sustainable and economical, this framework is scalable and cost-effective. The simulation was done on low-priced VMS (VirtualBox, Ubuntu, etc), publicly available encryption tools (VeraCrypt) and widely used forensic platforms. This allows it to be deployable not only in national cybercrime armadas but also in mid-sized enterprise incident response squadrons. In addition, it applies to SaaS, IaaS and hybrid, providing realistic integration in different operational contexts. The modular design means that even in situations where not all artefact types are available, meaningful evidence may still be re-created while sustaining the evidential chain undisturbed by invasive or legally problematic methods.

5.3 Recommendations for Forensic Readiness

Organisations and cloud providers must employ a dual approach of technical and policy-based strategies to improve forensic readiness in encrypted cloud environments. Technically, incorporation of principles of forensic-by-design into cloud architecture is essential [42]. The providers should normalise log formats, make access records more granular, and use optional key escrow schemes through which lawful forensic recovery under court orders can occur. Standards for APIS for log consumption and preservation of evidence, like a legal intercept mechanism in telecom systems, should also be followed [25]. Also, tools such as Cado Security that have been explicitly designed with cloud native investigations in mind should be part of the forensic stack, with real-time integration with IaaS and SaaS systems being essential.

Training must be a priority at the organisational level. These include regular instruction that incident response teams and forensic analysts receive on memory forensics, log correlation, and metadata analytics. Policies for preservation of evidence need to be updated to involve proactive snapshotting of encrypted volumes, log exports at defined intervals, and policies that prescribe timeframes for post-incident memory acquisition. Organisations that use platforms such as AWS, Dropbox or Google Drive should pre-configure long-term log retention and ensure that the log activity via API is not anonymised.

For vendor cooperation on the part of organisations, the best practice is to embed forensic access clauses into cloud service agreements. These should specify situations under which law enforcement or even internal auditors are granted the ability to access the logs, snapshots and other artefacts even when encryption is applied. A cross-industry working group (comprising cloud vendors, regulators and digital forensic professionals) that should also be adopted to establish standardised frameworks for investigating encrypted environments should also be initiated. Such actions will not only increase the strength of finding capacity, but they will also increase public trust in cloud security without weakening privacy guarantees.

5.4 Legal and Regulatory Alignment

The proposed framework tries to follow a straight line of effective forensic investigation and legal/privacy frameworks. Under GDPR and HIPAA, collecting and processing individuals' data, including metadata and access logs, should be based on necessity, proportionality and explicit consent. Respecting these constraints, the framework largely depends on such non-content artefacts as memory dumps (collected with prior legal authorisation), cloud logs, and system metadata, which do not involve direct interception of a user's content unless necessary, when decryption keys have been lawfully obtained. This approach tracks what is stipulated in GDPR Recital 49 and the minimum required standard under HIPAA [26].

Cross-border investigations, though, remain full of legal issues. The U.S. Cloud Act allows publicly traded providers to disclose the world-stored data served through a warrant, even though such access is against the GDPR Article 48. The layered framework overcomes this legal impasse by encouraging indirect artefacts instead of direct data transfers. However, the international cooperation framework needs to be expanded. Bilateral treaties such as those supported under the CLOUD Act, or the forensic access clauses under the Budapest Convention, should be revisited to reflect encrypted and cloud native environments [47]. Countries ought to facilitate clarity on the acquisition of RAM and live response protocols because, in many cases, this is the only means of accessing decrypted artefacts before shutdown.

It is further suggested that forensic practitioners use standardised reporting protocols, which would show their compliance with the norms regarding confidentiality and legality, e.g. why memory had to be acquired, what logs were accessed, and how the correlation of the metadata was accomplished without any evidence of breaching confidentiality. Docile records will serve as a balm to the court's admissibility and end the practices of forensic tools to disguise security.

6. CONCLUSION

The provision of cloud storage services that are encrypted has improved data protection while at the same time making digital investigations much harder for researchers. Techniques that have been based on disk imaging and file carving are becoming less effective because of encryption and physical access barriers in the distributed, virtualised cloud ecosystem. To address these limitations, the research developed a multilayered approach which combines memory forensics, log examination and metadata correlation. Each level of the framework was designed to run independently or in tandem to solve encryption problems, reconstruct the sequence of user sessions, and conclude user actions where direct evidence was not available. >By analysing test-bed simulations and authenticated log data, it proved capable of promoting significant improvements over investigative outcomes vs standard techniques.

The major results of the study were the reliable extraction of encryption keys from volatile memory, the exact reconstruction of user sessions with the help of log analysis and the exposure of behavioural patterns in metadata unknown to traditional forensic approaches. Unlike disk-only practices, the use of the layered approach improved evidence recovery rates and reduced the time required to rebuild user timelines by over 70%. Moreover, the structure of the framework complied with forensic readiness guidelines and secured compliance with data privacy laws and showed how indirect traces could be applied in the form of legally acceptable proxies for encrypted data.

The study produces a practical and modular forensic model tailored to the encrypted cloud environment. This approach emerges uniquely using circumstantial evidence, instead of direct content extraction, hence builds solid forensic tales while adhering to privacy regulations for everyone involved. However, the research involved was hampered by using synthetic data and an assumption of optimal tool performance. When applied in the real world, case studies may involve adversary interference, masks for log data, or a lack of timely access. RAM extraction is most vulnerable to temporal constraints, and occasionally accessing it is dependent on the cooperation of the cloud providers, whose log policies are not identical. One of the main avenues for future investigation is the automation of the operation of the framework across all the forensic layers and validation with authentic, adversarial data in the cloud. Additional research also requires considering the applicability of the framework across mobile and IoT platforms, and international guidelines for a successful cross-border access addressing within the context of encryption and legal restrictions are also needed. This research provides a good foundation for enhancing investigative skills in encrypted cloud spaces.

7. ACKNOWLEDGMENTS

We express our sincere gratitude to the experts and collaborators who have significantly contributed to the development of this research paper. Their insights, guidance, and unwavering support were instrumental in shaping this work and enhancing its academic quality. We would like to particularly acknowledge the contributions of the following authors:

Joy Awoleye, Yeshiva University - Cybersecurity (Email: awoleyejoy@gmail.com), for leading the research, coordinating the project, and drafting the manuscript.

Sarah Mavire, Yeshiva University - Cybersecurity (Email: sarahmavire@gmail.com), for her critical analysis, data validation, and valuable inputs throughout the study.

Allan Munyira, Yeshiva University - Cybersecurity (Email: munyiraallan@gmail.com), for his technical expertise in implementing the proposed methodology and assisting with data processing.

Kelvin Magora, Yeshiva University - Cybersecurity (Email: kelvinmagoraub@gmail.com), for his support in reviewing related literature, data compilation, and contributing to the analysis.

We also extend our gratitude to the faculty and staff of Yeshiva University, whose resources and encouragement greatly facilitated this research. Furthermore, we appreciate the collaborative spirit and dedication shown by all contributors, whose collective efforts made this work possible.

8. REFERENCES

[1] Gao, Y., Q. Li, L. Tang, Y. Xi, P. Zhang, W. Peng, B. Li, Y. Wu, S. Liu, and L. Yan. 2021. "When cloud storage meets {RDMA}." In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, 519–533.

[2] Ghani, A., A. Badshah, S. Jan, A. A. Alshdadi, and A. Daud. 2020. "Issues and challenges in cloud storage architecture: a survey." arXiv Preprint arXiv:2004.06809.

[3] Yang, P., N. Xiong, and J. Ren. 2020. "Data security and privacy protection for cloud storage: A survey." *IEEE Access* 8: 131723–131740. https://doi.org/10.1109/access.2020.3010183.

[4] Atadoga, A., O. A. Farayola, B. S. Ayinla, O. O. Amoo, T. O. Abrahams, and F. Osasona. 2024. "A comparative review of data encryption methods in the USA and Europe." *Computer Science & IT Research Journal* 5, no. 2: 447–460.

[5] Smid, M. E. 2021. "Development of the advanced encryption standard." *Journal of Research of the National Institute of Standards and Technology* 126: 126024.

[6] Gonzalez, O. 2019. "Cracks in the armor: Legal approaches to encryption." *U. Ill. JL Tech. & Pol'y* 1.

[7] Can, M. A., E. Öztürk, and E. Savaş. 2019. "Design and implementation of encryption/decryption architectures for BFV homomorphic encryption scheme." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 28, no. 2: 353–362.

[8] Purnaye, P., and V. Kulkarni. 2021. "A Comprehensive Study of Cloud Forensics." *Archives of Computational Methods in Engineering* 29, no. 1. https://doi.org/10.1007/s11831-021-09575-w.

[9] Alenezi, A. M. 2024. "Beyond The Clouds: Investigating Digital Crimes In Cloud Environments." https://doi.org/10.2139/ssrn.4977348.

[10] Fernandes, D., D. Clemente, G. Soares, P. Sebastiao, F. Cercas, R. Dinis, and L. S. Ferreira. 2020. "Cloud-Based Implementation of an Automatic Coverage Estimation Methodology for Self-Organising Network." *IEEE Access* 8: 66456–66474. https://doi.org/10.1109/access.2020.2986437.

[11] Khan, Y., and S. Varma. 2020. "Development and Design Strategies of Evidence Collection Framework in Cloud Environment." In *Social Networking and Computational Intelligence*, 27–37. https://doi.org/10.1007/978-981-15-2071-6_3.

[12] Pisaric, M. 2022. "Communications encryption as an investigative obstacle." *J. Crimin. & Crim. L.* 60: 61.

[13] Shabbir, A., A. S. Anwar, N. Taslima, S. M. Abu, A. R. Sikder, and G. S. Sidhu. 2024. "Analyzing enterprise data protection and safety risks in cloud computing using ensemble learning." *International Journal on Recent and Innovation Trends in Computing and Communication* 12, no. 2: 499–507.

[14] Veen, J., and S. Boeke. 2020. "Which is more important: online privacy or national security?: The Dutch position in the ongoing encryption debate." *Atlantisch Perspectief* 44, no. 4: 36–40.

[15] Uphoff, M., M. Wander, T. Weis, and M. Waltereit. 2018. "SecureCloud: An Encrypted, Scalable Storage for Cloud Forensics." https://doi.org/10.1109/trustcom/bigdatase.2018.00294.

[16] Sandhu, A. K. 2021. "Big data with cloud computing: Discussions and challenges." *Big Data Mining and Analytics* 5, no. 1: 32–40.

[17] Khanchandani, M., and N. Dave. 2021. "Analysis of Cloud Forensics : Review and Impact on Digital Forensics Aspects." *International Journal of Scientific Research in Science and Technology*: 639–646. https://doi.org/10.32628/ijsrst2182118.

[18] Schlepphorst, S., K.-K. R. Choo, and N.-A. Le-Khac. 2020. "Digital Forensic Approaches for Cloud Service Models: A Survey." In *Studies in Big Data*, 175–199. https://doi.org/10.1007/978-3-030-47131-6_8.

[19] Beaubrun, R., and A. Quintero. 2021. "An Access Control Architecture for Securing MultiTenancy Cloud Environments." *International Journal on Advances in Security* 14, no. 1 & 2.

[20] Svensson, J., and S. Wouters. 2024. "Navigating the Shadows: Overcoming Obstacles Posed by Antiforensic Tools."

[21] Blessing, O. T., and A. O. Mary. 2023. "Cryptographic techniques for data privacy in digital forensics." *IEEE Access* 11: 142392–142410.

[22] Deng, S., H. Zhao, B. Huang, C. Zhang, F. Chen, Y. Deng, J. Yin, S. Dustdar, and A. Y. Zomaya. 2024. "Cloud-Native Computing: A Survey From the Perspective of Services." *Proceedings of the IEEE* 112, no. 1: 12–46. https://doi.org/10.1109/JPROC.2024.3353855.

[23] Balogun, V., and O. A. Sarumi. 2020. "A Cooperative Spectrum Sensing Architecture and Algorithm for Cloud- and Big Data-based Cognitive Radio Networks." In *2020 6th International Conference on Computing and Engineering Communications (CCECE)*, 1–5. https://doi.org/10.1109/ccece47787.2020.9255729.

[24] Mittal, S., C. Monga, K. Upreti, N. Kumar, R. D. Raut, and M. S. Alam. 2022. "Light Weight Cryptography for Cloud-Based E-Health Records." In *2022 7th International Conference on Communication and Electronics Systems (ICCES)*, 690–696. https://doi.org/10.1109/icces54183.2022.9835827.

[25] Roudev, N., and L. Baker. 2022. "Deconstructing the regulatory impact of the US CLOUD Act: An optimal regulatory approach to ensuring access to data in the cloud?" *Journal of Data Protection & Privacy* 5, no. 3: 230–241. https://www.ingentaconnect.com/content/hsp/jdpp/2022/00000005/00000003/art00005.

[26] Ateeq, A., M. A. Alaghbari, R. A. Ateeq, and A. Y. Ahmed. 2024. "Understanding and Addressing Data Security and Privacy Concerns in Modern Cloud Computing Systems." https://doi.org/10.1109/icetsis61505.2024.10459534.

[27] Rojszczak, M. 2020. "CLOUD act agreements from an EU perspective." *Computer Law & Security Review* 38: 105442. https://doi.org/10.1016/j.clsr.2020.105442.

[28] Sharma, P., R. Jindal, and M. D. Borah. 2020. "Blockchain Technology for Cloud Storage." *ACM Computing Surveys* 53, no. 4: 1–32. https://doi.org/10.1145/3403954.

[29] Herzig, T. W. 2020. "Audit Logging." In *HIMSS Publishing EBooks*, 45–54. https://doi.org/10.4324/9781003126331-6.

[30] Zhang, X., Y. Xu, Q. Lin, B. Qiao, H.-Y. Zhang, Y. Dang, C. Xie, X. Yang, Q. Cheng, Z. Li, J. Chen, X.-T. He, R. Yao, J.-G. Lou, M. Chintalapati, F. Shen, and D. Zhang. 2019. "Robust log-based anomaly detection on unstable log data." In *Foundations of Software Engineering*. https://doi.org/10.1145/3338906.3338931.

[31] C hothia, Z. 2020. "Explaining, Measuring and Predicting Effects in Layered Data Architectures." PhD diss., ETH Zurich. https://doi.org/10.3929/ethz-b-000503615.

[32] He, S., P. He, Z. Chen, T. Yang, Y. Su, and M. R. Lyu. 2021. "A Survey on Automated Log Analysis for Reliability Engineering." *ACM Computing Surveys* 54, no. 6: 1–37. https://doi.org/10.1145/3460345.

[33] Lazar, D., Y. Gilad, and N. Zeldovich. 2019. "Yodel: Strong Metadata Security for Voice Calls." In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 1–15. https://doi.org/10.1145/3341301.3359648.

[34] Zunaidi, M. R., A. Sayakkara, and M. Scanlon. 2024. "Systematic Literature Review of EM-SCA Attacks on Encryption." arXiv.org, February 15. https://doi.org/10.48550/arXiv.2402.10030.

[35] Shahzad, K., T. Zia, and E.-H. Qazi. 2022. "A Review of Functional Encryption in IoT Applications." *Sensors* 22, no. 19: 7567. https://doi.org/10.3390/s22197567.

[36] Turki, M., G. El Boussaidi, I. Benzarti, and H. Mili. 2024. "Evaluating Open Source IoT Platforms: A GitHub Analysis." In *Proceedings of the ACM/IEEE 6th International Workshop on Software Engineering Research & Practices for the Internet of Things*, 14–21. https://doi.org/10.1145/3643794.3648348.

[37] Sherman, S., and J. Dykstra. 2013. *Cybersecurity: A New Look at Security Metrics*. Apress.

[38] Naeem, H., S. Dong, O. J. Falana, and F. Ullah. 2023. "Development of a deep stacked ensemble with process based volatile memory forensics for platform independent malware detection and classification." *Expert Systems with Applications* 223: 119952–119952. https://doi.org/10.1016/j.eswa.2023.119952.

[39] Chen, Y., C. Li, M. Lv, X. Shao, Y. Li, and Y. Xu. 2019. "Explicit Data Correlations-Directed Metadata Prefetching Method in Distributed File Systems." *IEEE Transactions on Parallel and Distributed Systems* 30, no. 12: 2692–2705. https://doi.org/10.1109/tpds.2019.2921760.

[40] Zhang, M. 2022. "Forensic imaging: a powerful tool in modern forensic investigation." *Forensic Sciences Research* 7, no. 3: 1–8. https://doi.org/10.1080/20961790.2021.2008705.

[41] Groß, T., M. Busch, and T. Müller. 2021. "One key to rule them all: Recovering the master key from RAM to break Android's file-based encryption." *Forensic Science International: Digital Investigation* 36: 301113. https://doi.org/10.1016/j.fsidi.2021.301113.

[42] Lazar, A. 2020. "Innovative Peacekeeping: The Potential of Digital Technologies in CSDP Operations." Dspace.cuni.cz. https://dspace.cuni.cz/handle/20.500.11956/177248.

[43] Kim, D.-H., S. Oh, and T. Shon. 2023. "Digital forensic approaches for metaverse ecosystems." *Forensic Science International: Digital Investigation* 46: 301608–301608. https://doi.org/10.1016/j.fsidi.2023.301608.

[44] Chothia, Z. 2020. "Explaining, Measuring and Predicting Effects in Layered Data Architectures." PhD diss., ETH Zurich. https://doi.org/10.3929/ethz-b-000503615.