EC-Council

CLOUD FORENSICS TODAY: AN OVERVIEW OF CHALLENGES AND TRENDS

EC-Council would like to thank **Sunil Kumar**, Digital Forensic Examiner and Consultant at Forensodigital Technologies, for authoring this whitepaper.

Abstract

With cloud computing drastically changing the digital landscape through cloud adoption and migration by organizations around the globe, threats to information security in virtual environments are also growing. Hence, it has become imperative for digital forensics processes and methods to scale up to meet cloud requirements. Though cloud forensics appears to be a promising method of tracking information security compromises on virtual platforms, performing digital forensics in the cloud is not an easy feat. The complex and distributed nature of the cloud tends to present numerous challenges for investigators due to the distribution of security responsibilities across client–cloud service provider lines. To implement solutions for existing and upcoming challenges related to cloud technologies, it is imperative for cybersecurity leaders to understand current challenges and technology trends from the perspective of the cloud security and digital forensics community. The current white paper aims to highlight the current challenges and trends in cloud forensics through the perspectives and opinions of cloud security professionals, gathered through original research conducted by EC-Council's CISO MAG.

Keywords: cloud forensics, digital forensics, cloud services, cloud security, cloud service providers

Contents

Cloud Forensics Today: An Overview of Challenges and Trends

Cloud technology is transforming digital and IT infrastructures at an astounding rate. With the global COVID-19 pandemic acting as a catalyst, many businesses have migrated or are planning to migrate their digital operations and storage to the cloud. From a security perspective, cloud technology has introduced many challenges for cybersecurity leaders. Among these issues is cloud forensics, as scaling traditional digital forensics processes for the multijurisdictional, distributed cloud environment has proven to be a challenging task.

This white paper, based on a survey of cloud professionals conducted by CISO MAG, showcases the perspectives of industry experts on various trends and challenges in cloud security, specifically regarding digital forensics in cloud environments. As the complex nature of the cloud tends to present multiple challenges for the traditional forensic process, it has become imperative for security leaders to understand the state of the cloud from the perspective of existing challenges and trends so that they can develop solutions that strengthen their organization's security posture against current and future threats (Vaidya, 2020). Before describing the survey methodology and analyzing its results regarding trends and challenges in cloud forensics, we present a review of some of the major concepts in cloud technology and security.

Key Concepts in
Cloud Technology and Security

CLOUD STORAGE

A relatively simple definition of cloud storage that is understandable for non-technical and non-security personnel is the storage of a large volume of data in a virtual ecosystem. This could be described as an information storage model in which data are stored in a logical pool of servers shared by multiple users. These groups of servers, together said to represent the “cloud,” are located across the globe and are owned and managed by the organization providing the cloud service. Cloud storage services, which are accessible through applications and programming interface platforms, aim to keep the stored data secure and readily accessible, with flexible and scalable storage capacity.

CLOUD COMPUTING

Cloud computing can be described as the virtual availability of data and resources on demand around the globe. It offers a virtualized computing power, wherein the assets processing the data are not directly managed by the user or their affiliated organization. Cloud computing service operations are globally distributed, with data stored at different locations, and rely on shared resources and computing requirements to achieve affordable but highly powerful computing functions.

CLOUD ARCHITECTURE

Cloud architectures consist of computing, storage, and client network interaction layers, where cloud assets and other subcomponents interact in the virtual ecosystem to store, transfer, and process information. The entire cloud can be divided into front-end and back-end platforms (e.g., thin and thick clients, servers, storage), accompanied by network and cloud-based deliveries.

CLOUD FORENSICS

Cloud forensics can be defined as the scaling of digital forensics processes onto cloud platforms—more precisely, the application of investigative procedures in cloud computing ecosystems as a subset of network forensics. The aim of cloud forensics is similar to that of network and computer forensics: namely, to identify, detect, collect, and analyze artifacts and potential digital evidence in the wake of a security incident. Cloud forensics involves the combined application of hardware, network, digital, and mobile forensics in a virtual environment. It requires the coordination of the various parties involved in cloud operations—including the cloud service provider (CSP), client, cloud carrier, and cloud auditors—to facilitate seamless investigations in the multijurisdictional and multitenant cloud ecosystem.

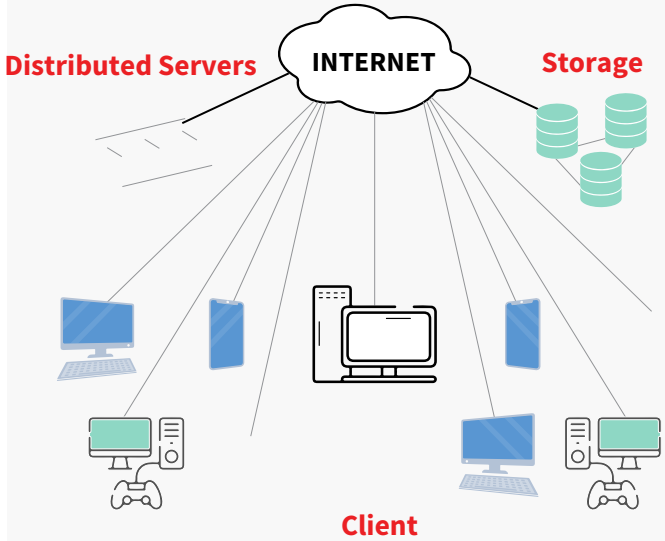
Forensics in the cloud presents many unique challenges for investigators and raises the need for specialized tools, techniques, protocols, guidelines, and governance support. The complex structure and diverse service models of the cloud further add to the challenges of collecting and studying digital evidence in the cloud—and, in some situations, before the data is lost due to its volatility. Though the virtual nature of the cloud facilitates global data access and faster processing, the concept of stored data, an application running on a virtual machine, or virtualized hardware being out of the authoritative reach of the organization to whom it belongs presents a challenge to forensic investigators in times of need.

While virtualization of data may seem to be secure, this is not always the case. Developments in cloud computing paradigms can also create opportunities for increases in cyberthreats, and the hybrid nature of the cloud provides grounds for various challenges and security threats due to its distributed and complex security architecture. Addressing the issues of digital forensics in a cloud environment requires understanding those challenges from the perspective of the digital forensics and cloud security communities, which is only possible through surveys that aim to understand the top issues in cloud technology and associated markets.

COMPONENTS OF CLIENT COMPUTING

According to Velte et al. (2010), there are three main elements in cloud solutions: clients, data centers, and distributed servers. Each element has a specific purpose and plays a significant role in delivering cloud-based applications.

Figure 1
Components of Client Computing



1 Clients

In the cloud computing context, the term “client” has the same meaning as its standard definition: a simple requestor that accesses any service available from a server through a network. From a physical perspective, a client is the device—such as a mobile phone, laptop, tablet, or desktop computer—with which end users interact to use cloud-based resources and access cloud-stored data.

2 Data Centers

A data center is a collection of physical servers where the applications to which the client subscribes are housed. A data center usually includes backup equipment, power supplies, data communication connections, and environmental controls such as air cooling and fire suppression. A data center’s main purpose is to store, provide, and facilitate the circulation of data that is used by the client and distributed servers in the cloud.

3 Distributed Servers

Distributed servers are a collection of physical servers that work together as one system across a network. Distribution means that servers do not have to be in the same location; rather, they can be geographically spread across different locations while still working as one common system. This provides more flexibility and security (Velte et al., 2010), as even if something happens that causes a failure at any part of a server in one location, the service can still be accessed through another location. In addition, if the cloud needs more physical hardware, the CSP does not have to add more servers at the same location. Instead, the provider can add new hardware at another location and make it part of the same cloud, despite its different location.

SERVICE AND DEPLOYMENT MODELS

Cloud architectures encompass multiple service models, with each applicable to various sets of business requirements. Three of the most well-known models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), whose business applications are described below.

1 Infrastructure as a Service

IaaS models provide cloud users with a basic IT infrastructure (compute, network, storage) that allows clients to run and deploy assets, virtual machines, and application containers. In this service model, the hardware and infrastructure are abstracted for the clients to manage and operate.

2 Platform as a Service

PaaS models enable clients to create and manage the entire software development life cycle while providing complete computing platforms and solution stacks for application development and deployment. The PaaS model helps organizations deploy applications and layouts without incurring the significant expenditures associated with hosting and managing the underlying assets and other capabilities.

3 Software as a Service

The SaaS model refers to an “on-demand” software platform. Under this model, the client can access the application, software, and databases, but the underlying infrastructure and capabilities are managed by the CSP.

Methodology

CISO MAG conducted a survey targeting professionals in the cybersecurity industry with sufficient knowledge of cloud forensics to provide their opinions on the various challenges associated with different tasks, phases, and service platforms involved with digital forensics in cloud environments. We were specifically interested in gathering respondents' thoughts on the global nature of the cloud arising from the availability of CSPs and data server farms situated around the world, as this geographic dispersion creates various complications in cloud forensics, especially regarding data acquisition, identification, and privacy. Respondents were encouraged to take the survey to contribute toward the development and normalization of the understanding of cloud forensics among their peers and within the broader cybersecurity community. The results of this survey are expected to enable interested parties to better understand the current state of cloud forensics by providing new insights into current challenges in cloud forensics and their possible causes and highlighting future trends and developments.

DEMOGRAPHICS

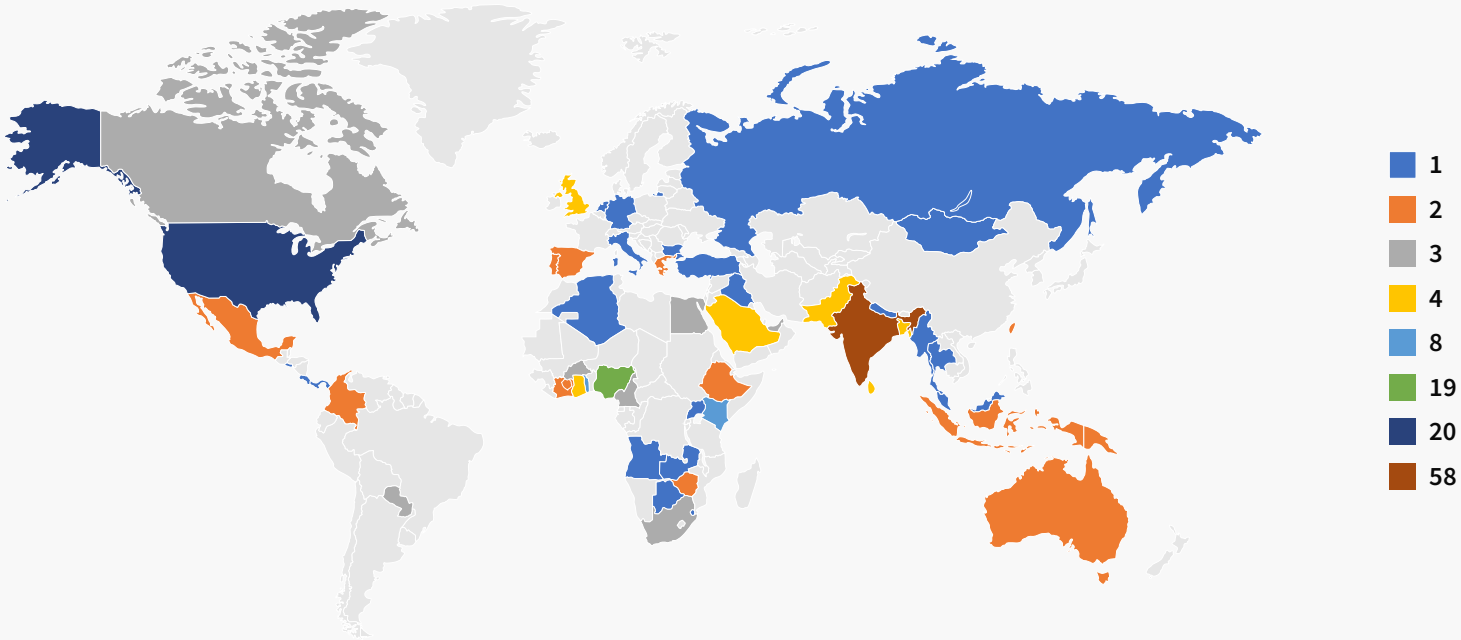
Respondents were limited to individuals employed in an IT or cybersecurity department (for an organization in any industry) whose work directly concerned cloud technology and who understood digital or cloud forensics. Over a period of 3 weeks, we received responses from over 210 valid respondents, representing a cross-section of organizations and institutions across 56 countries (see Table 1 and Figure 2).

Table 1 : Respondents' Job Positions

JOB POSITION		
Analyst	Information security lead	Professor
Assistant manager	Information security consultant	Programmer
Associate consultant	Information security director	Project consultant
Chief executive officer	Instructor	Penetration tester
Chief information security officer	Integration engineer	Researcher
Chief technology officer	IT administrator	Senior executive
Cybersecurity analyst	IT analyst	Senior information and communications technology
Cybersecurity consultant	IT architect	officer
Data analyst	IT audit manager	Security operations center analyst Solution architect
Developer	IT consultant	Student
Director of technology	IT manager	System engineer
Ethical hacker	Learning solution specialist	Systems analyst
Forensic expert	Lecturer	Telecommunications engineer
Forensics analyst	Network administrator	Vulnerability management specialist
Incident analyst	Operations manager	

Figure 2 : Respondents' Locations

AFRICA	58
ASIA	100
AUSTRALIA	2
EUROPE	16
NORTH AMERICA	27
SOUTH AMERICA	7



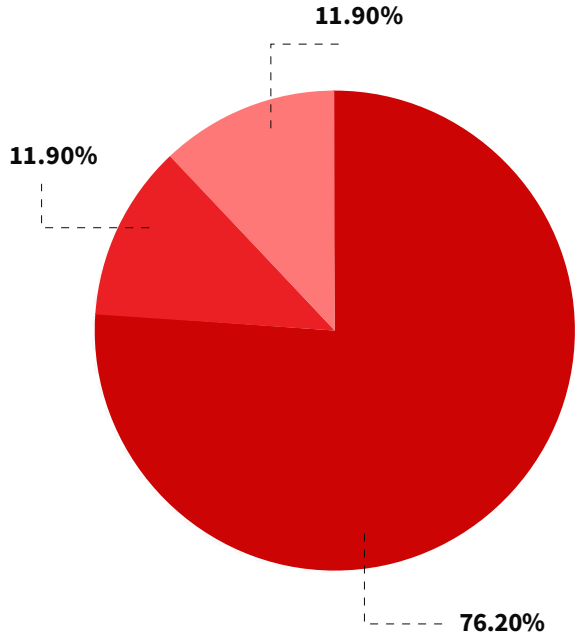
Understanding the Need for Cloud Forensics

Before exploring the challenges and trends associated with cloud forensics, respondents' views on its necessity should be discussed. As with any forensics process, a cloud forensic investigation generally comes on the heels of a security incident, examines that incident, and determines what is needed to maintain business continuity. This was supported by over three-quarters (**76.20%**) of survey respondents, who listed investigating security incidents and maintaining business continuity as the top reason for cloud forensics, but there also exist other reasons for performing forensic operations in the cloud (Figure 3). Respondents also mentioned troubleshooting security issues in cloud environments (11.90%) and recovering sensitive or deleted data (11.90%) as reasons to perform cloud forensics.

Figure 3

Reasons to Perform Cloud Forensics

- To investigate security incidents in the cloud infrastructure and maintain business continuity
- To troubleshoot and resolve security issues in the cloud environment
- To recover sensitive/deleted data

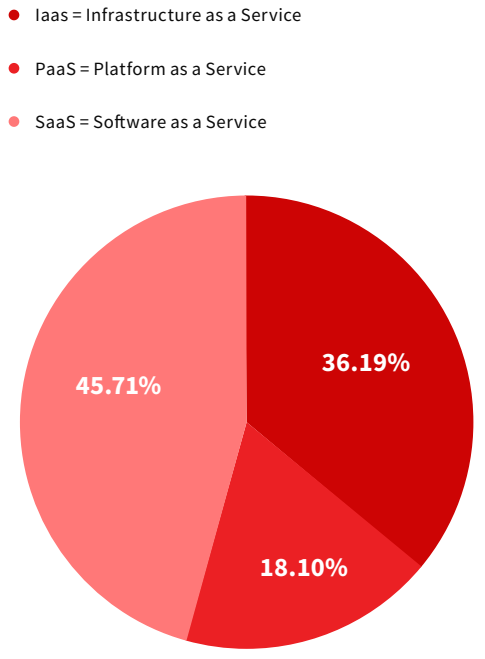


Cloud Forensics Challenges

Though the advantages of cloud computing platforms far exceed their corresponding challenges and drawbacks, many people do not fully understand cloud operations due to their complex nature. This complexity stems from the inherent flexibility of cloud technology, which can provide various integrated services—such as IaaS, PaaS, and SaaS—over public, private, and hybrid platforms. When posed the question of which cloud service model presents the most challenges when it comes to digital forensics, nearly half of respondents (45.71%) stated that they believed it to be SaaS, followed by IaaS (36.19%) and PaaS (18.10%; Figure 4). Traditional digital forensic frameworks were designed to operate in an environment where data and assets were within physical reach of forensic investigators, thus simplifying forensic processes. Cloud forensics, in contrast, involves shared security and multiple jurisdictions by nature, placing much of the data and assets needed for forensics outside the physical and authoritative reach of investigators.

Figure 4

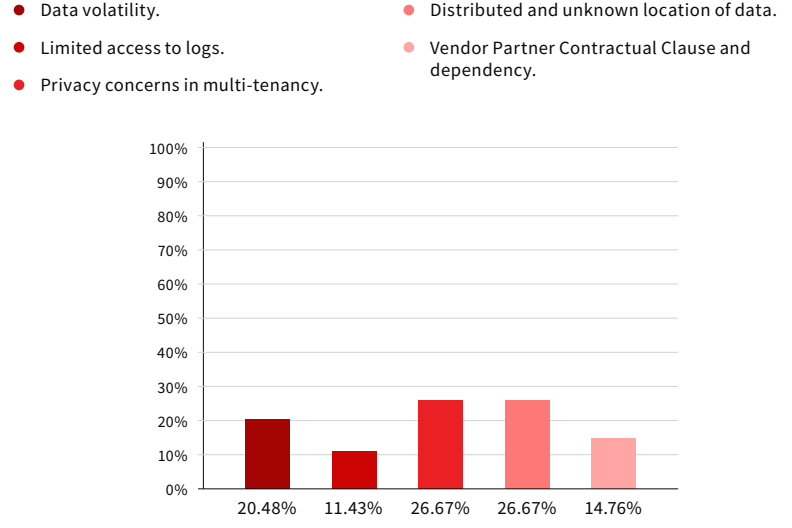
Respondents' Views on Which Cloud Service Model Presents the Most Digital Forensics Challenges



This gives rise to various challenges across technological, legal, and organizational process domains, including data volatility due to shutting down physical and virtual machines and limited access to logs. Similarly, issues related to vendor partner contractual clauses and dependencies are also leading causes of concern. The lack of knowledge regarding where required data and assets are located and privacy concerns in a multitenant environment are also major challenges when considering cloud forensics as a whole. When questioned about the most pressing challenges in the cloud forensics context, multitenancy-related privacy issues and distributed locations of data were considered equally challenging, with roughly one-fourth of respondents highlighting each as a top concern (Figure 5). Data volatility (20.48%), vendor partner contractual clauses and dependencies (14.76%), and limited access to logs (11.43%) were some of the other challenges that demanded respondents' attention.

Figure 5

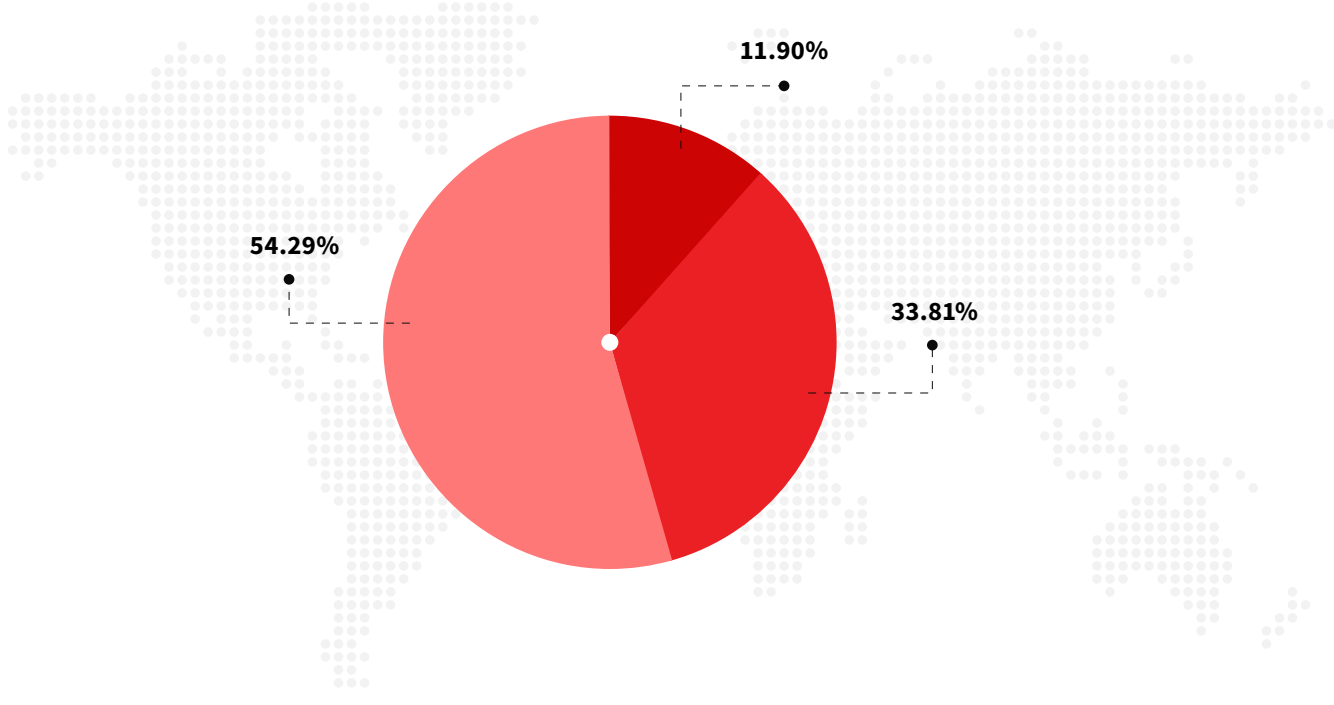
Respondents' Views on the Most Pressing Challenges in Cloud Forensics



Cloud deployment models provide cloud storage and migration flexibility through various services and functionalities, depending upon business requirements. Based on these aspects, cloud deployment environments can be classified as public, private, or hybrid. All types of cloud deployment environments have certain benefits and challenges, which vary with regard to different aspects of cloud forensics. The majority of respondents believed hybrid clouds (54.29%) to be most challenging from a cloud forensics perspective, followed by public (33.8%) and private (11.9%; Figure 6). This may be due to the complex architecture of hybrid clouds, which involve elements of both public and private clouds. This includes issues related to multiple-hypervisor environments, network layer connectivity, and virtual network overlays, among others.

Figure 6

Respondents' Views on the Most Challenging Cloud Deployment Model



Governance Dimension

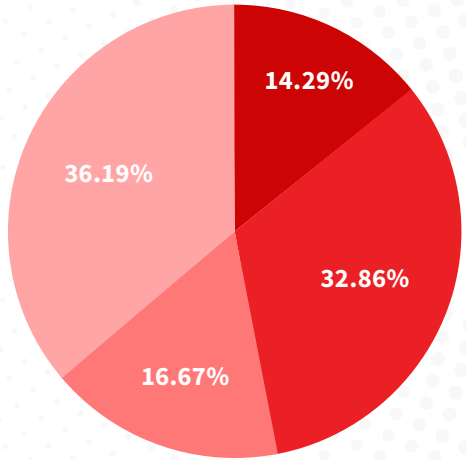
The governance dimension of cloud forensics deals with challenges associated with non-technical entities, such as the issues that forensic investigators face with regard to the managerial structure and functioning of an organization as well as legal and jurisdictional matters. This is associated with the layers of abstraction between the consumer and the CSP, which increase both the scope and challenges of cloud forensics. It involves catering to and satisfying all the parties involved with the data and assets to conduct the investigation process in an effective way (Ruan et al., 2011). When questioned about the most important reason why forensic investigations in cloud-based environments are more complex than traditional investigations, a plurality of respondents (36.19%) stated that the distributed and dynamic nature of the cloud model makes it difficult to demonstrate the integrity and authenticity of the evidence acquired (Figure 7). Other respondents stressed a lack of talent with the technical expertise to perform cloud forensics (32.86%), lack of service-level agreement (SLA) clauses covering cloud data forensics (14.29%), and lack of physical access and dependence on CSPs (16.67%).

Figure 7

Reasons for Increasing Complexity of Forensic Investigations in Cloud Environments

- Lack of SLA clauses regarding cloud data forensics.
- Lack of cloud technical expertise to perform forensics.
- Lack of physical access and dependence on CSP.
- The distributed and dynamic nature of the cloud model makes it difficult to demonstrate the integrity and authenticity of the evidence acquired.

Note:
SLA = service-level agreement;
CSP = cloud service provider.



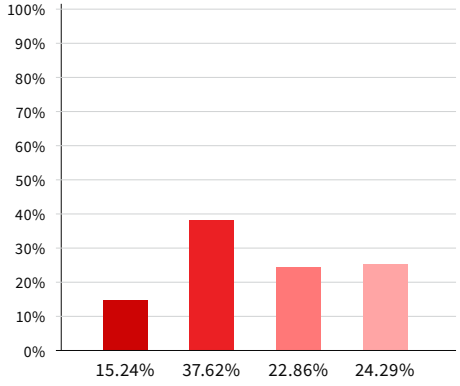
1 Organizational Factors

Some of the prime challenges in cloud forensics include the lack of visibility of third-party contractual clauses and difficulty coordinating among investigators, engineers, management, and legal teams. Similarly, lack of strategy, policies, standards, procedures, skills, and training for personnel also pose considerable challenges. When asked about the organizational factors influencing existing challenges in cloud forensics, over one-third of respondents (37.62%) stated that there exists a lack of coordination among the parties involved in cloud forensics, such as investigators, engineers, management, and legal teams (Figure 8). Though not as significant as the lack of coordination, other challenges mentioned by respondents included lack of visibility of third-party contractual clauses (15.24%); lack of cloud forensics strategy, policy, standards, and procedures (22.86%); and lack of cloud forensics skills and training for personnel (24.29%).

Figure 8

Organizational Factors Influencing Cloud Forensics Challenges

- Lack of visibility of the third-party contractual clause.
- Lack of coordination between parties such as investigators, engineers, management, and legal team.
- Lack of cloud forensics strategy, policy standards, and procedures.
- Lack of cloud forensics skills and training for personnel.



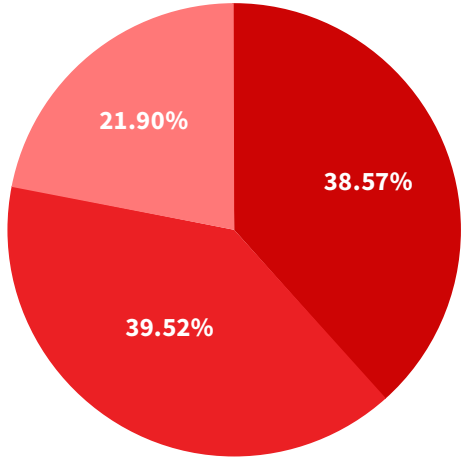
2 Legal Factors

Legal factors are generally associated with the multijurisdictional and multitenant nature of the cloud and largely revolve around the challenges related to SLAs. These elements could be considered the top legal concerns in cloud forensics and include judicial issues related to restrictions surrounding access to data, a lack of effective channels for international communication and cooperation during an investigation, and missing terms in contracts and SLAs (Ruan et al., 2012). Among the prominent legal factors that influence existing challenges in cloud forensics, nearly 40% of respondents said that a lack of channels for international communication contributed greatly to the legal challenges faced by cloud forensics investigators, while 38.57% and 21.90% of respondents respectively believed that jurisdictional issues affecting legal access to data and missing terms in contracts and SLAs were the most prominent challenges (Figure 9).

Figure 9

Legal Factors Influencing Cloud Forensics Challenges

- Identifying and addressing issues of jurisdictions for legal access to data.
- Lack of effective channels for international communication and cooperation during an investigation.
- Missing terms in contracts and servicelevel agreements.



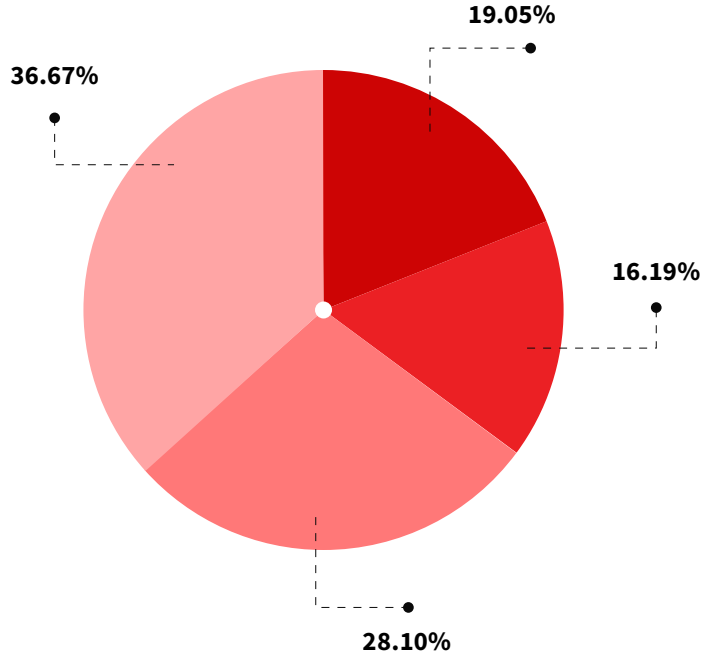
SLAs are legally binding documents that set forth the responsibilities of the client and CSP. SLA-related issues are a subset of the legal factors impacting cloud forensics challenges with regards to the shared responsibility for cloud data security. However, SLAs have also come under criticism for not providing transparency regarding certain aspects of the cloud environment, which limits the client's access to some of the knowledge related to security incidents. As SLA limitations are one of the most prominent obstacles in the path of effective cloud forensics, many amendments have been suggested by the forensic community. For example, SLAs might be amended to shield CSPs from legal liability for the actions of cloud service users and could provide the CSP with the authority to remove or ban undesirable content from the service. Transparency regarding division of duties between the CSP and the user and explicit mentioning of what data to collect, when, and for what purpose—along with related liabilities—is another change that has been suggested for SLAs.

When asked what recommendations they would make for amendments to SLAs to allow for an efficient cloud forensics process, a majority of respondents (36.67%) recommended that SLAs include explicit details about data collection, use, and legal liabilities (Figure 10). The other suggestions were as follows:

- 28.10% of respondents recommended that SLAs add terms and conditions regarding the division of duties between the CSP and the user.
- 19.05% of respondents recommended that SLAs protect the CSP from legal action arising from the malicious actions of a cloud user.
- 16.19% of respondents recommended that SLAs grant the CSP the right to remove or block objectionable content.

Figure 10

Service-Level Agreement Amendment Recommendations



Note:
CSP = cloud service provider.

Technical Dimension

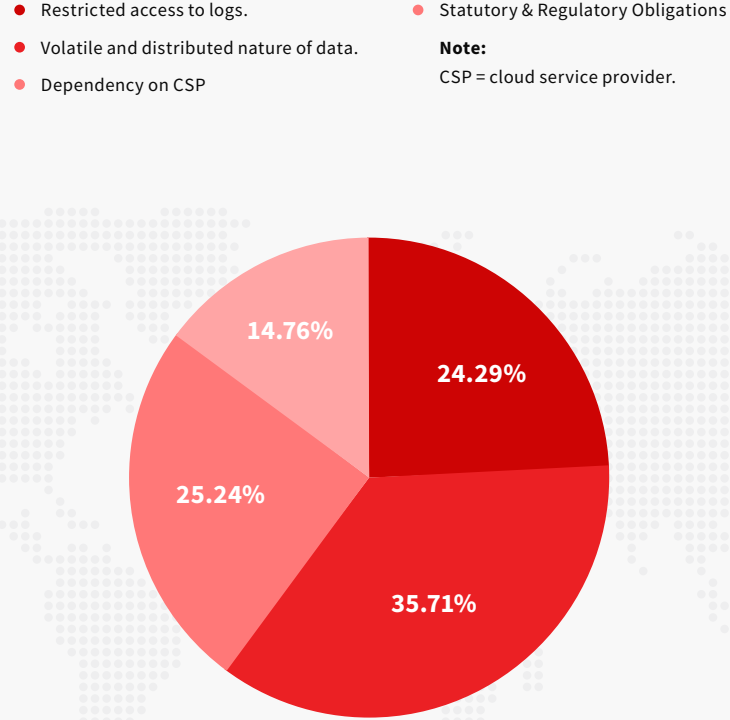
The entire forensic process can be divided into four phases: identification, collection, examination or analysis, and presentation. The first three represent the technical process of identifying, obtaining, and analyzing the artifact and lie at the core of any discussion related to the challenges involved in cloud forensics.

1 Identification Phase

Identifying a compromised asset in a dynamic cloud architecture is difficult due to the distributed nature of such architectures. As data in the cloud is hosted in multiple locations and data centers, it can be difficult for investigators to identify issues due to limitations such as restricted access to logs and volatile and distributed data. Dependency on CSPs for data identification and statutory and regulatory obligations are some of the other prime challenges. When asked to name the most important challenge that investigators and organizations face while performing forensics in a cloud environment during the identification phase, 35.71% of respondents cited the volatile and distributed nature of data in the cloud, while 25.24% and 24.29% named dependency on CSPs and restricted access to logs, respectively (Figure 11). Statutory and regulatory obligations were believed to be a prime challenge by 14.76% of respondents.

Figure 11

Challenges Faced During the Identification Phase in a Cloud Environment



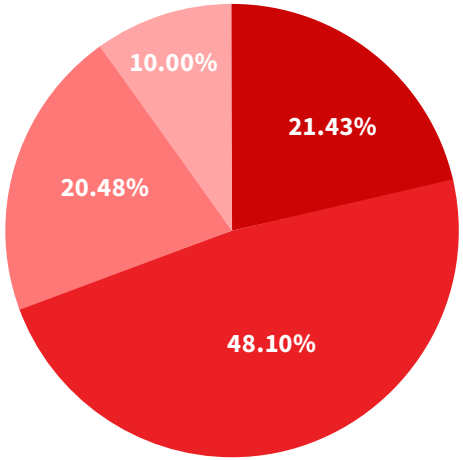
2 Data Collection

Although it is essential, collecting and preserving artifacts of digital evidence as supporting material entails notable challenges. One of these challenges is locating the artifacts in the cloud environment, which—given that the cloud is by nature a large, distributed, and dynamic system—is a very difficult process. Moreover, the shared service model of the cloud makes it difficult for investigators to access the forensic data of one tenant without breaching the confidentiality of others (Herman et al., 2020). Data integrity in a multitenant environment, where data is shared among multiple computers in multiple locations and accessible by multiple parties, and the recovery of deleted data are some prominent issues. When asked about the most important challenges faced during the collection phase of forensics in a cloud environment, 48.10% of respondents reported that data integrity in a multitenant environment was the most significant (Figure 12). Another 21.43% believed it was locating forensic artifacts in large, distributed, and dynamic systems; 20.48% believed it was accessing the data of one tenant without breaching the confidentiality of others; and 10% believed it was recovery of deleted data in a shared and distributed virtual environment.

Figure 12

Challenges Faced During the Collection Phase in a Cloud Environmentt

- Locating forensic artifacts in large, distributed, and dynamic systems.
- Data integrity in a multi-tenant environment where data is shared among multiple computers in multiple locations and accessible by multiple parties.
- Accessing the data of one tenant without breaching the confidentiality of other tenants
- Recovery of deleted data in a shared and distributed virtual environment



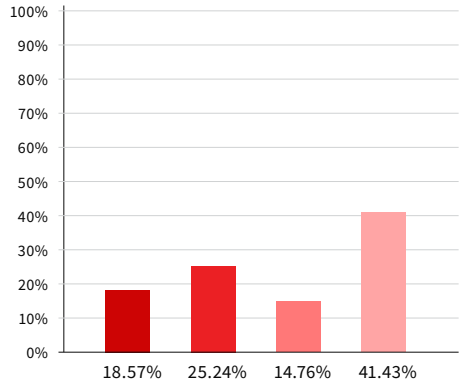
3 Examination

The examination of identified and isolated artifacts for incident reconstruction could be considered the core cloud forensic investigation process. The large volume of data, data encryption, unifying log formats, and timeline analysis of log data—including synchronization of timestamps—are some of the important challenges faced during this phase. When asked about the most important challenge faced during the examination phase of forensics in a cloud environment, 41.43% of respondents cited the timeline analysis of log data and timestamp synchronization, followed by data encryption (25.24%), volume of data (18.57%), and unification of log formats (14.76%; Figure 13).

Figure 13

Challenges Faced During the Examination Phase in a Cloud Environment

- Volume of data.
- Encryption of data
- Unification of log formats
- Timeline analysis of log data, including synchronization of timestamps



Recommendations for Improving Efficiency

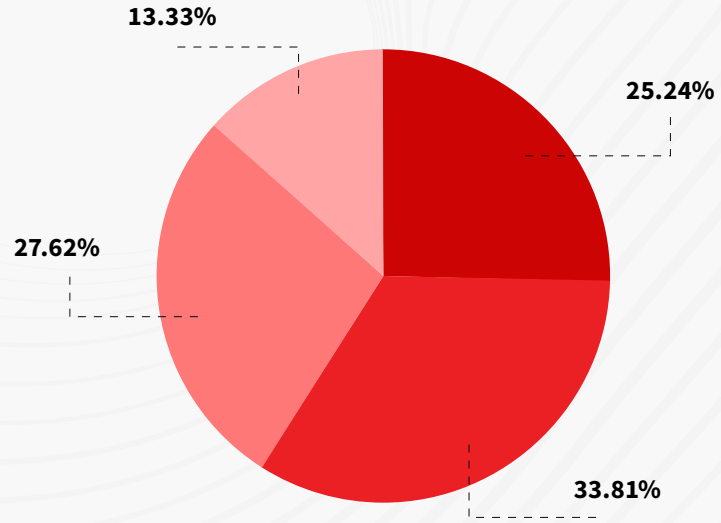
Various technologies and frameworks have been proposed as solutions to the obstacles to effective forensic process implementation in cloud environments. While this manuscript does not dwell on the details of specific solutions, we asked respondents to make generalized recommendations that they felt could help improve the efficiency of the cloud forensics process. One-third of respondents (33.81%) felt that procuring or increasing training on cloud computing skills and the use of better forensics tools for imaging and retrieving evidentiary data would be impactful in increasing the efficiency of the forensic process (Figure 14). Approximately one-fourth of respondents (27.62%) believed that utilizing SLAs and standard operating procedures with CSPs to enable cloud forensics readiness would be most useful. Another quarter of respondents (25.24%) believed in establishing better forensics frameworks, keeping the volatile nature of the cloud environment in mind, while 13.33% said that introducing services that automate forensics and incident response in the cloud would be of help.

Figure 14

Recommendations for Improving Efficiency in Cloud Forensics

- Establishing better forensics frameworks, keeping the volatile nature of cloud environment in mind.
- Training on cloud computing skills and use of better forensics tools for imaging and retrieving evidentiary data.
- Utilizing SLAs and SOPs with CSP to enable cloud forensics readiness.
- Introducing services that automate forensics and incident response in cloud.

Note:
SLA = service-level agreement;
SOP = standard operating procedure;
CSP = cloud service provider.



Trends in Cloud Service Technology

Technical trends are mostly related to processes, methodologies, or tools. In the area of cloud forensics, we focused on the cloud service platforms that provide flexible services and have unique procedures. Of the IaaS, PaaS, and SaaS models, the most trending is the IaaS model, which is designed to offer an entire IT computing infrastructure to the client that is managed and operated on a cloud platform. The aim of IaaS is to provide users with a virtual environment and associated IT facilities (i.e., hosting, virtual machines, networking, servers, storage and backup, operating systems, middleware, and applications) as novel development and testing environments, along with greater computing capacity. Marked as industry leaders in Gartner's Magic Quadrant for cloud infrastructure and platform services (Bala et al., 2021), Amazon Web Services (AWS) Cloud, Microsoft Azure, and Google Cloud Platform are best suited for studying such trends. In this survey, we focused on AWS Cloud and Azure.

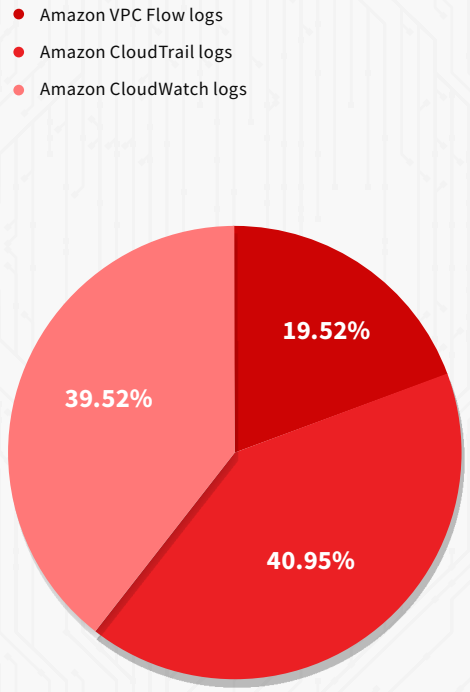
1 Amazon Web Services Cloud

To research preferences related to various AWS Cloud suites and soft ware, we assumed a scenario in which the respondents, as part of a cloud forensics team, had been assigned to investigate a security incident in the AWS Cloud environment and needed to check the log data to identify the instance.

AWS Cloud has a variety of log features, including virtual private cloud (VPC), CloudTrail, and CloudWatch. The VPC flow logs enable the capture of IP traffic information between network interfaces in the AWS VPC. Flow logs help security professionals diagnose restrictive security group rules, monitor traffic to their instances, and so on. The CloudTrail logging application monitors events for an account and captures those trails to the Amazon S3 bucket. Similarly, CloudWatch centralizes logs from all systems, applications, and AWS services in a single location (AWS, 2021a). When asked which log files should be checked first to gain relevant data faster, CloudTrail (40.95%) and CloudWatch (39.52%) were nearly equally popular choices for gaining relevant data quickly during forensic investigations in an AWS Cloud environment (Figure 15). Amazon VPC flow logs were the least common choice at 19.52%.

Figure 15

Popularity of Amazon Web Services Cloud Log Files for Forensic Investigations



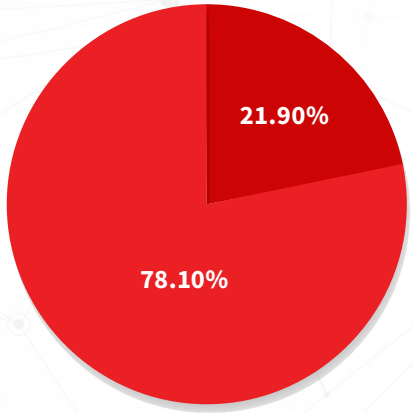
Similarly, we studied respondents' preferences regarding conduct and best practices for cloud forensic investigations with regard to the immediate process following the data collection but prior to analysis. When asked whether they preferred directly starting analysis after collection or first transferring the collected evidence to a different account for examination, the majority of respondents (78.10%) stated that it was best practice to collect the evidence and transfer it to a different AWS security account for forensic analysis, whereas the remaining 21.90% did not, preferring to initiate the examination process immediately rather than transferring evidence to another account (Figure 16).

Figure 16

Best Practices for Evidence Handling and Transfer in Amazon Web Services Cloud

- Collect the evidence and start the forensic analysis in the same AWS account
- Collect the evidence and transfer it to a different AWS security account for forensic analysis

Note: AWS = Amazon Web Services.



Amazon Elastic Compute Cloud (EC2) provides instance types to users, which are designed and optimized according to various requirements and use cases. These instance types consist of various assets—such as CPU, storage, and network assets—and related capacities in varying combinations as per the requirement to provide a flexible resource package for the user's application hosting and operations. The aim of the EC2 instance is to provide a balance among assets, computing capacity, storage, and networking for managing diverse workloads (AWS, 2021b), hence making its security highly important.

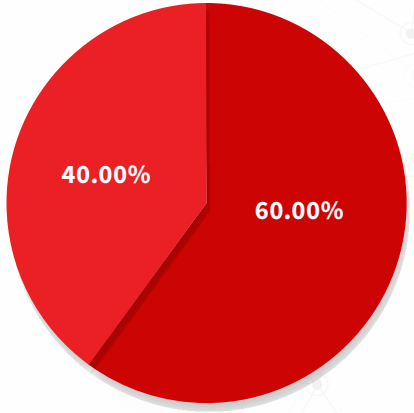
To determine respondents' views on EC2 trends and best practices, we posed a hypothetical question related to a suspected security breach investigation in an AWS Cloud environment. When asked what should be the immediate step following the detection of an EC2 instance breach, a majority of respondents (60%) opted to quarantine the instance by attaching to it a restrictive security group that does not allow outbound traffic (Figure 17). The remaining 40% of respondents opted to create an offline snapshot of the instance's Elastic Block Store (EBS) volume, take backups of necessary data, and then terminate it.

Figure 17

Best Practices After Detecting an Amazon Elastic Compute Cloud Breach

- Quarantine the instance by attaching a restrictive security group to it that does not allow outbound traffic.
- Create an offline snapshot of its EBS volume, take backups of necessary data, and terminate it.

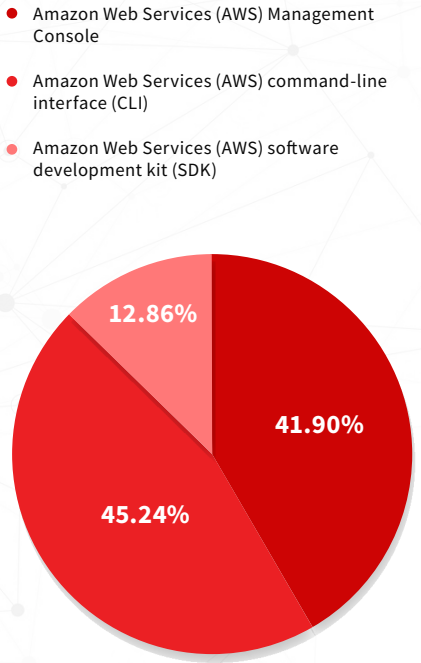
Note: EBS = Elastic Block Store.



The AWS Management Console enables the building of new applications, account management, and more in the AWS Cloud environment for all types of devices. The console is designed to facilitate the processes of configuring services, enabling and viewing service usage, upgrading, and troubleshooting. The AWS command-line interface (CLI) tool helps manage multiple AWS services and automate them via scripts. It also provides various features, such as improved installers and new configuration options like AWS single sign-on. Similarly, the AWS software development kit (SDK) is a collection of software tools for application and library creation that allows developers to access AWS by directly running code. Respondents were asked to choose among the AWS CLI, Management Console, and SDK to conduct a forensic investigation in an AWS Cloud environment. Almost half of respondents (45.24%) believed the AWS CLI to be the most effective, likely due to its extensive features, with the AWS Management Console a close second at 41.90% (Figure 18). Only 12.86% of respondents chose AWS SDK.

Figure 18

Preferences for Amazon Web Services Cloud Management Platforms



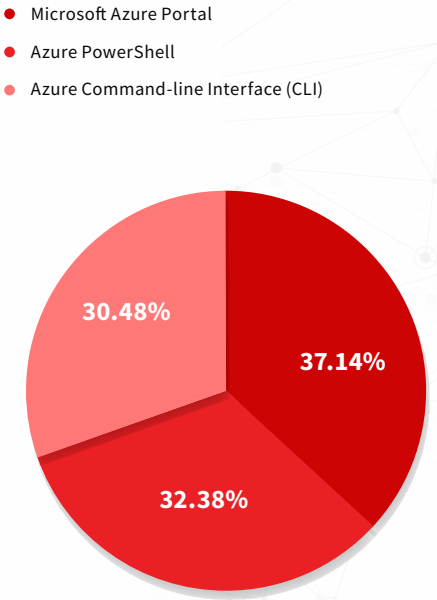
2 Microsoft Azure

To research respondents' preferences related to various Microsoft Azure suites and software, we assumed a scenario in which the respondents, as part of a cloud forensics team, had been assigned to investigate a security incident in a Microsoft Azure cloud environment, including data acquisition and analysis.

The Azure portal is a unified console that helps users build, manage, and monitor their applications, processes, and deployment in a complex cloud environment. It has optimized user experience and accessibility features and is designed for resiliency and continuous availability (Microsoft, 2022b). Azure PowerShell is a set of command-lets (cmdlets) that help users directly manage resources from the command line (Microsoft, 2022c). Similarly, the Azure CLI is a set of commands that can be used to create and manage elements and resources in Azure through automating processes (Microsoft, 2022a). When asked which Azure platform for cloud computing they preferred to use when conducting cloud forensic acquisition and analysis operations, respondents were fairly evenly split, with a slight preference (37.14%) for the Microsoft Azure portal (Figure 19), possibly due to its varied features and optimal user experience. PowerShell was the next most popular at 32.38%, followed by Azure CLI at 30.48%.

Figure 19

Preferences for Microsoft Azure Cloud Management Platforms



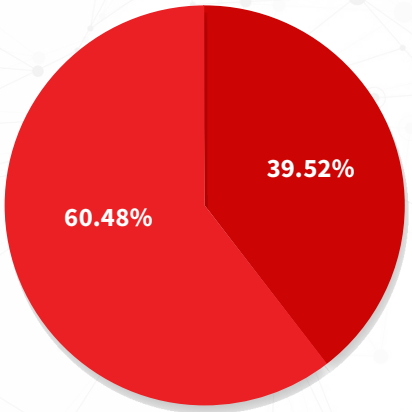
Similarly, we inquired about respondents' preferences for the collection of data of evidentiary value in Azure environments. A majority of respondents (60.48%) chose a security information and event management (SIEM) solution like Splunk or IBM QRadar, while the remaining 39.52% chose Azure Monitor (Figure 20).

Figure 20

Preferences for Data Collection Services in Microsoft Azure Environments

- Azure Monitor
- SIEM solution like Splunk or IBM QRadar

Note: SIEM = security information and event management.



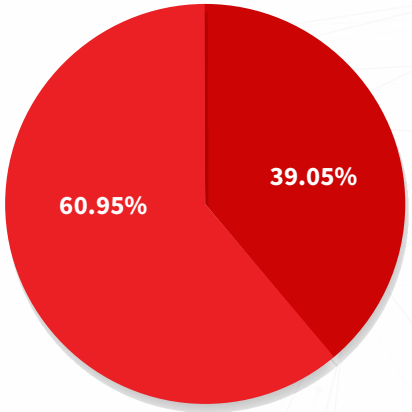
When discussing Azure technology trends and best practices, it is important to discuss the practices related to operating system (OS) disk snapshots. The cloud-based backup solutions in the Azure platform manage and secure the information on a disk, helping users recover data in the event of a disaster (Microsoft, 2022d). The Azure platform provides snapshot life cycle management solutions for information security on disks, which is made possible through periodic snapshot creation and retention as backups. Regarding the storage of disk snapshots, we investigated trends among respondents by posing a question about storage preferences. Most respondents (60.95%) preferred to store snapshots in a storage account under a different resource group, while 39.05% preferred saving them to a storage account in the resource group where the virtual machine (VM) was deployed (Figure 21).

Figure 21

Preferences for Operating System Disk Snapshot Storage

- A storage account in the Resource group where the VM is deployed
- A storage account under a different Resource group

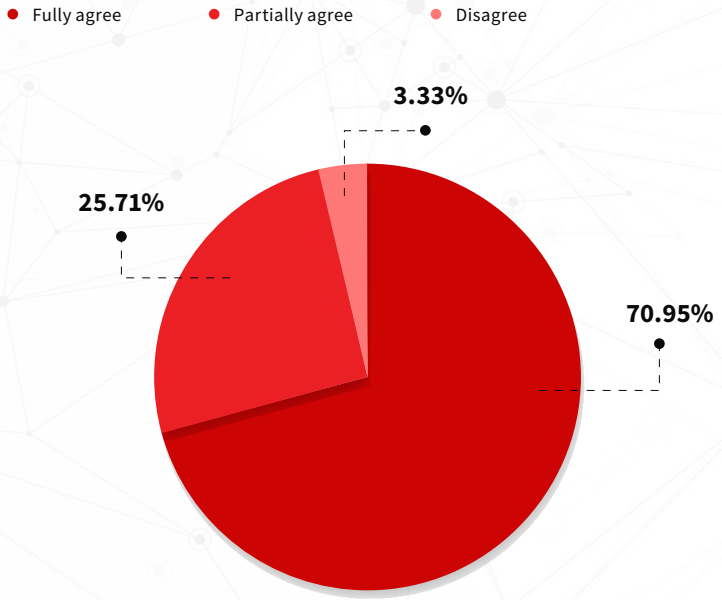
Note: VM = virtual machine.



The previous question aimed to determine investigators' storage and backup preferences during the forensic process in Microsoft Azure environments. Following up on the same, we posed a question concerning whether respondents considered it good practice to create a backup copy of the OS disk snapshot of an affected VM in Azure before conducting a forensic examination. While many respondents fully agreed (70.95%), a surprisingly high proportion either partially agreed (25.71%) or disagreed (3.33%; Figure 22).

Figure 22

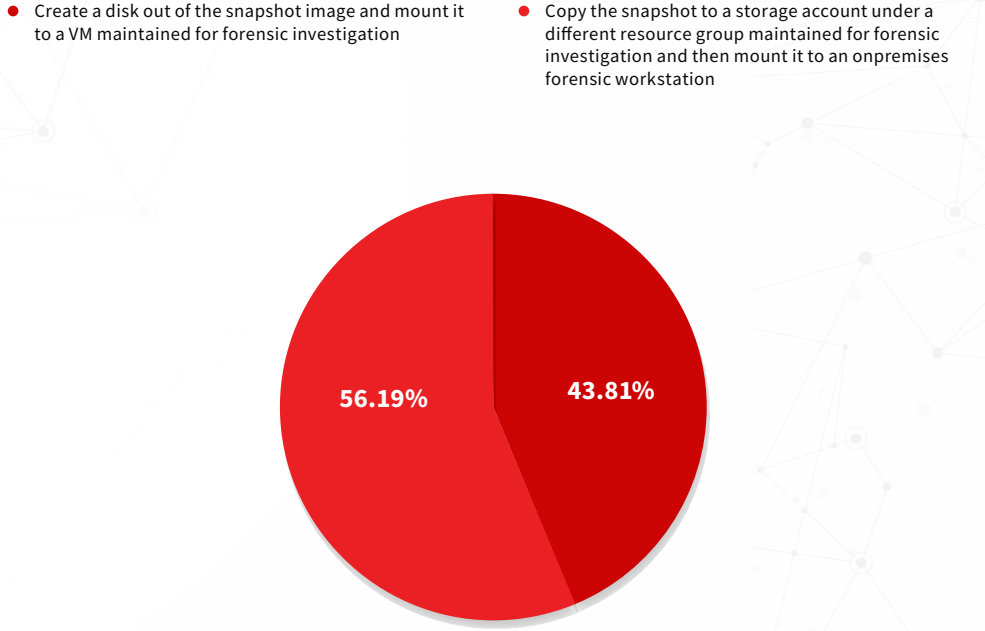
Preferences Regarding Creation of Operating System Disk Snapshot Backups



In a scenario where the investigators have taken an OS disk snapshot of an affected VM in Azure, the next step is conducting the forensic examination. We therefore posed a question regarding respondents' preferences for this step. While 43.81% of respondents preferred to create a disk out of the snapshot image and mount it to a VM maintained for forensic investigation, more than half (56.19%) preferred to copy the snapshot to a storage account under a different resource group maintained for forensic investigation and then mount it to an on-premises forensic workstation (Figure 23).

Figure 23

Forensic Process Preferences After Procuring Operating System Disk Snapshot



3 Future Trends

As the underlying technologies and techniques for cloud computing develop at an astounding rate, notable changes related to cloud infrastructures and their security are bound to occur. Due to the ballooning demand for cloud technologies, the stress on cloud security and forensics teams, in particular, has greatly increased. There exist multiple opinions within the digital forensics community regarding security implementations for stable and secure cloud functioning. Forensics as a Service (FaaS) solutions have been proposed as a unique means for CSPs to address digital forensics problems by offering an in-house solution (Vaidya, 2020). Similarly, many in the community also expect their data to be segregated from that of other tenants and readily available on centralized platforms for collection, irrespective of the region or location in which the data are physically stored. New data imaging methods and capabilities were also deemed essential for preserving data integrity and maintaining a proper chain of custody.

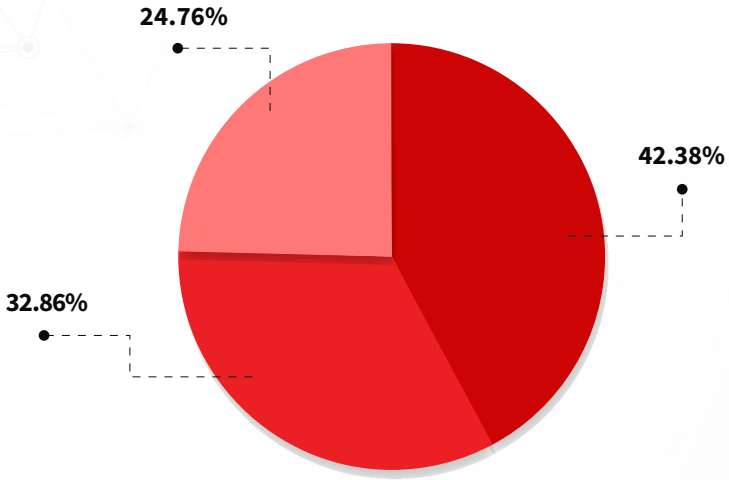
When questioned about their predictions for upcoming trends in cloud forensics, a majority of respondents (42.38%) believed that FaaS, as a single-platform solution, would be an upcoming trend in cloud forensics, while 32.86% believed data segregation and explicit availability, irrespective of service or storage region, to be the most likely upcoming trend (Figure 24). Finally, 24.76% believed that new data imaging methods and capabilities would be developed to preserve data integrity and maintain a proper chain of custody.

Figure 24

Respondents' Predictions for Upcoming Trends in Cloud Forensics

- CSPs will offer solutions, such as Forensics as a Service, that create unique propositions for resolving the challenges related to digital forensics under one roof
- Data will be segregated from other tenants and readily available on centralized platforms for collection irrespective of which region or location it is actually stored in.
- New data imaging methods and capabilities will be developed to preserve data integrity and maintain proper chain of custody.

Note: CSP = cloud service provider.



Conclusion

The survey analyzed here aimed to understand the current state of cloud forensics, including existing challenges and upcoming trends. In this regard, this white paper has explored new challenges in cloud forensics due to the cloud's unique architecture and diverse service models and their level of incorporation into IT and digital supply chain processes. This report divided cloud forensics challenges into general, governance, and technical domains and discussed the struggles of forensic investigators in gaining access and control to data and resources, along with analyzing and examining those data across cloud-integrated architectures. From the visible changes in cloud storage and operation domains, it can be inferred that the cloud services threat landscape will change drastically. Thus, it is imperative for security leaders to look at cloud security—especially cloud forensics—from a perspective that helps understand current and future trends and challenges.

The survey results indicate that many such challenges plague the field of cloud forensics as a whole, from multitenancy to unknown data location and hybrid cloud deployment. Moreover, each specific domain (i.e., governance and technical) has its own, further varied challenges. Where the governance domain faces issues related to lack of coordination between parties, lack of channels for international communication, and growing demand for SLAs to provide transparency with regard to data collection, purpose, and liabilities, the technical domain of cloud forensics was plagued by the volatile and distributed nature of data, data integrity in a multitenant environment, timestamp synchronization, and related challenges in the identification, collection, and examination of forensic evidence. The report also showcases preferences and trends in the popular AWS Cloud and Microsoft Azure cloud service platforms. Where CloudTrail logs and CLI tools were popular AWS Cloud services, the Microsoft Azure portal was considered a one-stop optimal platform for obtaining effective results with cloud forensic processes.

Acknowledgments

We would like to thank Hosam Badreldin (IT director, cloud strategy, transformation, and security, Thales); Rakesh Sharma (vice president, cloud and container security, Standard Chartered Bank); and Arpita Kundu (research associate, EC-Council) for their assistance in compiling, editing, and reviewing the questionnaire.

References

Amazon Web Services. (2021a, October 29). ***AWS CloudTrail features***. AWS CloudTrail. https://aws.amazon.com/cloudtrail/features/

Amazon Web Services. (2021b, November 30). ***Amazon EC2 instance types***. Amazon EC2. https://aws.amazon.com/ec2/instance-types/

Bala, R., Gill, B., Smith, D., Wright, D., & Ji, K. (2021). ***Magic quadrant for cloud infrastructure and platform services***. Gartner. https://www.gartner.com/doc/reprints?id=1-26YXE86I&ct=210729&st=sb

Herman, M., Iorga, M., Salim, A. M., Jackson, R. H., Hurst, M. R., Leo, R., Lee, R., Landreville, L. M., Mishra, A. K., Wang, Y., & Sardinas, R. (2020). ***NIST cloud computing forensic science challenges*** (NISTIR 8006). National Institute of Standards and Technology, U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8006

Microsoft. (2022a). ***Azure command-line interface (CLI) documentation***. Azure. https://docs.microso t.com/en-us/cli/azure/

Microsoft. (2022b). ***Azure portal documentation***. Azure. https://docs.microsoft.com/en-us/azure/azure-portal/

Microsoft. (2022c). ***Azure PowerShell documentation***. Azure. https://docs.microsoft.com/en-us/powershell/azure/?view=azps-6.3.0

Microsoft. (2022d). ***Overview of Azure disk backup***. Azure. https://docs.microsoft.com/en-us/azure/backup/disk-backup-overview?context=/azure/virtual-machines/context/context

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud forensics. In G. Peterson & S. Shenoi (Eds.), ***Advances in digital forensics VII: IFIP international conference on digital forensics*** (pp. 35–46). Springer. https://doi.org/10.1007/978-3-642-24212-0_3

Ruan, K., James, J., Carthy, J., & Kechadi, T. (2012). Key terms for service level agreements to support cloud forensics. In G. Peterson & S. Shenoi (Eds.), ***Advances in digital forensics VIII: IFIP international conference on digital forensics*** (pp. 201–212). Springer. https://doi.org/10.1007%2F978-3-642-33962-2_14

Vaidya, N. (2020). Cloud forensics: Trends and challenges. ***International Journal of Engineering Research & Technology, 9***(9), 744–745. https://www.ijert.org/cloud-forensics-trends-and-challenges

Velte, A. T., Velte, T. J., & Elsenpeter, R. (2010). ***Cloud computing: A practical approach***. McGraw-Hill

EC-Council

www.eccouncil.org