Evidence Collection and Forensic Challenges in Cloud Environment

Mohamad Khairi Ishak**, Nor Rizuan Mat Noor**

* School of Computer Science, Universiti Sains Malaysia, Gelugor, 11800 Penang, Malaysia (e-mail: aakazaure@student.usm.my, aman@usm.my, najwadi@usm.my, maigari@student.usm.my)
** School of Electrical and Electronic Engineering, Engineering Campus, Universiti Sains Malaysia, Nibong Tebal,14300, Penang, Malaysia (e-mail:khairiishak@usm.my, nrmn@usm.my)

Abstract: Nowadays, cloud computing clouded with criminal activities that have caused various havoc to be private and public data stored, making the cloud unsafe for information storage. Cloud forensics deals with the incidents involving cloud infrastructure and their services in both civil litigation and criminal investigations. Regardless of the online nature of the cloud computing paradigm, the incident investigated does not necessarily have to be purely online. Cloud forensics is more complex and complicated than the typical computing devices and mobile applications forensics. This paper is aimed to highlight various challenges and difficulties faced by forensic investigators when collecting digital evidence from the cloud ecosystem. To address this problem, a forensic investigator needs to identify potential criminals through a systematic process and linked them with an offence. Thus, forensics plays a significant role in finding evidence that will be admissible in court against a suspect in the crime. However, for a forensic investigator to obtain evidential proof that will be admissible in court is always tricky and challenging due to the conventional nature of the cloud. Likewise, most of the challenges found in the domain of data collection, data analysis methodologies, evaluation, interpretation and presentation. Hence, this study highlights the cloud forensics solutions and the roles of cloud services and their deployment models as the bedrock of cloud forensics investigation in a cloud environment.

Keywords: Cloud Computing, Cloud forensics, Evidence collections, Digital Forensics

1. INTRODUCTION

Cloud computing has become the topic of discussion in recent years because of its tremendous success recorded by most of the cloud subscribers, and its currently accustomed support varied areas of human life. Cloud forensics has been introduced to assist forensic experts and investigators to find potential proof that will be used against cloud criminal activities and to protect the integrity of the data extracted for the purpose of investigation within the cloud domain [1], this paper critically reviews some of the cloud forensics problems which affects forensic examination in the cloud and their possible solutions, it also highlighted some cloud forensic challenges that affect the investigation processes

Forensic investigation, especially in the cloud, is distracted by so many challenges ranging from inadequate and proper techniques and methodology that might put in place to help forensic investigators to collect forensic evidence during the examination of digital artefact on the occurrence of the criminal activities. The heterogeneity and high volumes of data in the cloud, which is spread across different geographical locations in the data centres also is another point of concern [1]. Furthermore, Cloud forensics is a subset of digital forensics which designates the need for digital investigation in the cloud domain based on legal principles and procedures. Digital forensics is fundamental to examinations performed in a reality which is often tightly coupled with cyber extension. Modern digitally-enabled societies are subject to fraud and cybercriminal activities leading to financial losses or hazards for both government and individuals. Therefore, the new wave of forensics tools should be engineered to support independent investigations, preserve privacy, and offer scalability [2].

In recent years, cloud forensic has been introduced to help digital forensic investigators to find potential evidence against cloud criminal activities in order to maintain the integrity and security of user's data stored in the cloud. While considerable research in the area has been carried out concerning challenges and solutions, the research on forensic data acquisition from the cloud is still in its infancy stage [1]. Cloud storage and computing have greatly enhanced everyone's work productivity and life quality in many ways.

These technologies allow scalable, flexible, reliable and cost-effective data processing and storage by using databases, networked systems with virtual environments and a set of cloud management and operational solutions [3]. However, the pervasive applications of the Cloud provide potential opportunities for cybercriminals to hack and mount various attacks into the organizational and personal cloud
environments to perform malicious activities and sometimes acquire sensitive and private information [4]. In other words, the increased adoption rates of cloud computing solutions are also an opportunity for criminals to store data within cloud-based environments.

Cloud forensics deals with incidents involving cloud infrastructure and their services in both civil litigation and criminal investigations [5]. Despite the online nature of cloud computing, the event being investigated does not necessarily have to be purely online. Cloud forensics is more complex and complicated than the typical computing devices and mobile applications forensics, comparatively due to the architectural complexity of the cloud computing technology, such as utility computing based on remotely available resources, virtualization of resources, and distributed systems [6]. For instance, conventional physical crime can be committed in the cloud infrastructure through their services (e.g., physical terrorist attack, storage of incriminating materials in the cloud,) subject to a forensic investigation.

There have been several challenges noted in the literature, to mention a few such as non-compatibility and reliability of existing tools and mechanisms to facilitate cloud forensic investigations, and the sources of evidence is normally at the server side (through cloud service providers), client-side and network side (data in transit) [7]. Furthermore, research efforts have focused on client-side forensic analysis, partly due to pragmatic constraints as it is challenging for researchers, if not impractical, to conduct forensic analysis of commercial cloud servers, such as those belonging to Amazon and Google [8]. As a result of widespread use of cloud services and the current privacy cognizant climate, for instance, the introduction of the General Data Protection Regulation (GDPR) [9], there is an increasing focus on cloud forensics. Virtualization and distributed environment are two of several factors that may hinder an investigator's capability to timely identify and acquire relevant evidential artefacts, for example, due to the challenge in pinpointing the precise physical location of the hardware resources. Jurisdiction is also another factor that may hinder an investigation, as the investigator may not have the authority of data stored in a foreign nation [10].

In this paper, we examine the cloud forensics challenges which affect the forensic investigation process while conducting a forensic investigation coupled with their possible solutions under certain jurisdictions also highlighted. The rest of this paper is organized as follows, in section 2. some of the technical backgrounds with respect to cloud forensics was highlighted, in section 3., we highlighted the cloud forensics challenges concerning evidence collection, in section 4. this section presents the analysis of some forensic challenges in the cloud domain and insertion 5. Some of the possible solutions to the earlier mentioned challenges presented, and finally, we conclude the paper in the last section.

2. TECHNICAL BACKGROUND

A. Cloud Forensics

The cloud forensics, as defined by NIST, is the applications of digital forensics in cloud computing which is a subset of network forensics. Cloud forensic is identified as a cross-discipline between cloud computing and digital forensics which attract various definitions for both cloud computing and digital forensics [11]. Cloud forensics deals with the incidents involving cloud infrastructure and their services in both civil litigation and criminal investigations. Despite the online nature of cloud computing, the event being investigated does not necessarily have to be purely online. Cloud forensics is more complex and complicated than the typical computing devices and mobile applications forensics, comparatively due to the architectural complexity of the cloud computing technology, such as utility computing based on remotely available resources, virtualization of resources, and distributed systems [6]. For instance, conventional physical crime can be committed in the cloud infrastructure through their services (e.g., physical terrorist attack, storage of incriminating materials in the cloud,) subject to a forensic investigation.

It can also be understood from the NIST definition, which defines cloud computing as an evolving paradigm with complicated steps and essential properties that drastically reduced the cost of information technology which is a driving trend globally. The global trend with rapid premeditated approaches implementing of cloud computing in both governmental and commercial industries for the sake of facility availability and cost efficiency, some of the Cloud service providers, such as Amazon, Google, Ali express and Sales force.com have data centers around the world in various jurisdictions providing cloud services [12].

The data stored in one of these data centres is replicated to numerous locations across different regions to ensure efficient service delivery and reduce the menace of failure at a single point. These points of replication and articulations of information are owned by the service providers who are potentially beneath many different dominions. Exclusion of duties between the Cloud service providers and their customs in forensic tasks becomes diverse in different service models, and connections between multiple occupants sharing the same cloud resources are different in numerous deployment models.

As a result of different jurisdictions and multitenancy have turn out to be a default setting for cloud forensics, thereby creating much more legal challenges. The Erudite collaborations between the Cloud service providers and the clients, or between various tenants sharing similar resources, or among international law enforcement which are required in most of the cloud forensics cases. To examine the problem more broadly, and to emphasize the fact that cloud forensics is a multi-dimensional issue as a substitute of only a technical
issue, we would like to extend the definition of cloud forensics across three significant dimensions; organizational, legal and technical, as shown in Figure 1.

![Cube Model for Cloud Forensics](image)

**Fig. 1. Cube Model for Cloud Forensics [11]**

**a) Legal Dimensions**

The Cloud physical properties are virtualised to be used by numerous clients via a multitenant model; they are similarly and enthusiastically assigned according to the demands. The major issue is the tradeoff amongst multitenancy's and client's data privacy and security. Another lateral consequence of the on-demand bounciness is the banquet of customers and providers data under diverse dominions, in many cases also the service level agreement do not include data about the manner for influential data ownership or what can be the jurisdiction to deliberate, specifically whether the one related to the physical location of the client, or to benefactors machines. In this case, the agreements might be tailored to include appropriate constraints; very few suggestions exist in the literature deliberating and addressing this issue.

**b) Organizational Dimensions**

Conducting a forensic examination in the cloud might involve information and services belonging to both providers and clients. There might also be circumstances where the cloud providers outsource some services from third parties which makes the scope of the investigation to becomes broader. Moreover, such contract out services is based on cloud architecture, henceforth all the problems related to the replication of data on various data centres positioned possibly under different physical jurisdictions deteriorates. Lack of legal expertise specifically for these features shows that there is significant uncertainty about the actions to undertake in case of cross providers or third parties' resources providing.

**c) Technical**

Cloud services are flexible, meaning that they are provisioned and released answering to client’s various demands. The services run on an infrastructure consist of several machines located potentially in different terrestrial zones without precise routing information; this resource is virtualised using some virtual machines (VMs). From a forensic viewpoint, these features determine reduced forensic access to information because the providers deliberately hide the data location to facilitate pervasive access and replicas from the clients.

Besides, the physical control of the architectural components of the cloud is lacking; it is also differing for the three services models becoming larger when a client moves to the bottom of the architecture. Alternatively, the issues in cloud architectures point of concerns are the heterogeneity of the log files since it has no standard file formats, each provider can tailor its own files log type. However, there is no timestamps synchronization between numerous data centres and server machines under a single providers scope, as well as amongst different providers components.

**B. Cloud Service Models**

The cloud service models classified according to the service models and this model has different layers. The types of the models used by the cloud service providers (CSP's) consists of Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service, respectively. Figure 3. below illustrate these three service models used by cloud computing architecture. This model provides customers with the capability of using a cloud service provider's software application functioning on cloud infrastructure [13]. This approach is quite different from traditional software packages distributed to various entities or organizations. This model does not require any software distribution, and the clients can access the application via web browsers on their personal computers or mobile smartphones.

The three-cloud model architecture may occasionally differ according to the number of clients who receive services in an organization. In this model, the client does not have any control over the network, operating systems, servers, storage, or even on the application layers except some access control management for multiuser applications [14]. Some of the examples of SaaS include Google Drive, Dropbox, Salesforce and Google calendar services. However, in Platform as a service (PaaS), the customers can deploy and customizes their own applications od SaaS applications used on the cloud infrastructures and pay according to the bandwidth usage and other service applications.

In this context, they do not accomplish or control the fundamental cloud infrastructures including the servers, operating systems, networks or storage. Still, they usually have control over the deployed applications and some applications hosting domains configurations. The clients can only use the applications developments environment, which generally supported by the platform as a service (PaaS)
providers such as Google App Engine (GAE), Windows Azure [15]. Clients can easily host their developed web-based applications on these platforms. Customers can host their developed web-based application on these platforms. This model permits a client to rent processing power and storage to launch his virtual machine VM, and it also eliminates the cost of the processes and maintains the data centres. It alleviates the costly process of maintaining a personal data centre [13].

iv. **Community cloud.** If several organizations with common concerns (e.g., mission, security requirements, policy, and compliance considerations) share cloud infrastructure, then this model is referred to as a community cloud.

3. **CLOUD FORENSICS CHALLENGES**

By knowing the usual digital forensic investigation practices, now, it is intense that the nature of cloud computing is in direct conflicts with digital forensics investigation. Except in the IaaS cloud model that provides an environment logically like a machine, none of the programs and approaches for digital data collection is feasible for the cloud computing models. For example, collecting the system processes and observing system status is not possible because SaaS and PaaS do not provide any access to the operating system commands. Based on the type of problem that occurred in the forensic investigation stage, the following are problems investigators face. Cloud services are applications running in the Cloud Computing infrastructures through an internal network or the Internet. Cloud computing environments are multi-domain environments in which each domain can use any security, privacy, and trust needs and potentially employ various mechanisms, interfaces, and semantics (Tari, 2014). Such domains could signify individual enabled services or other infrastructural or application components. Service-oriented architectures are naturally relevant technology to facilitate such multi-domain formation through service composition and orchestration. The table below highlight some of the cloud forensics challenges that affect the cloud forensics investigations, especially for cloud embedded infrastructures. Figure 2 shows the major Challenges at each stage of Cloud Forensics Investigation in the cloud computing domain [6].
The National Institute of Standards and Technology released a draft report in 2014 (NIST 2014), highlighting the requirement for cloud forensics standards to aid law enforcement. In that report, NIST identified 65 challenges in 9 major groups that forensics investigators face in gathering and analysing digital information stored in the cloud. The nine major groups are architecture, data collection, analysis, Anti-forensics, incident first responders, role management, legal, standards, and training. Cloud Security Challenges

In cloud computing, the users are unaware of the exact location of their sensitive data, because the Cloud Service Providers (CSP's) maintain data centres in geographically distributed locations resulting in several security challenges and threats. The traditional security techniques such as firewalls, host-based antivirus software and intrusion detection systems do not offer adequate security in virtualized systems due to the rapid spread of the threats via virtualized environments.

A. Network Level Security Challenges

Some of the characteristics that need to be addressed at the network layer level consist of the confidentiality and integrity of the network components which includes the issue of reused IP addressing, Sniffer attacks, Prefix Hijacking in usually is gateway protocol and Domain Name Server Attacks respectively.

B. Computational Level Security Challenges

Some of the challenges faced at the computational level in the cloud are the implementation of the virtualization concept, which is the most significant computational challenges. This virtualization consists of Application virtualization, Network virtualization, Desktop virtualization, Server and Machine virtualization abstraction.

C. Data Level Security Challenges

The heterogeneous level of data stored in the cloud brings a lot of data security challenges such as the data leakages. The data breach is identified as the most serious security challenge to all levels of security provided to the data in the cloud [18]. The data in the cloud is the most fundamental basic entry that is needed to be highly secured; it is obvious to protect the integrity and privacy of this data to ensure smooth services received by the clients.

One of the most significant differences in Cloud computing compared with digital forensics is the shift from physical to virtual. Virtual machines transported from the cloud are significantly expended, unlinked from their physical settings. The transference and the management of these devices technical and procedural approaches potential to entangle only Virtual machines VM. This catch in a common cloud condition renders seizure and imaging of physical equipment unrealistic; possibly revolving away forensic investigations [19]. Table 1. shows the major Challenges at each stage of Cloud Forensics Investigation in the cloud computing domain [6].

<table>
<thead>
<tr>
<th>Sr. no.</th>
<th>Problem</th>
<th>Challenges</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data Acquisition</td>
<td>Remote and Dynamic nature</td>
<td>Trust on the cloud service provider and live forensics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Large Capacity for storing Evidence</td>
<td>Cloud for data storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lack of suitable forensics tools</td>
<td>Efficient Logs management tools</td>
</tr>
<tr>
<td>2</td>
<td>Examination and Analysis</td>
<td>Difficult to Segregate Evidence from Large data set</td>
<td>Efficient data mining techniques</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chain of Custody</td>
<td>Tools for remote forensics</td>
</tr>
<tr>
<td>3</td>
<td>Preservation</td>
<td>Data Integrity</td>
<td>Hashing Techniques</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A large amount of Storage</td>
<td>Tools for evidence segregation</td>
</tr>
<tr>
<td>4</td>
<td>Presentation</td>
<td>Difficulties in proving the originality of the evidence</td>
<td>Rigid service level agreement SLA</td>
</tr>
</tbody>
</table>

4. CLOUD FORENSICS ANALYSIS CHALLENGES

In today’s IT-driven environment, security incidents are becoming a norm, and examples include violation of security policies and their implementation or enforcement measures. For example, according to a study by McAfee [9], organizations reportedly faced more than 23 distinct threats monthly on average, and these threats are increasing at a rate of more than 18% per year. Security incidents are generally the trigger of a digital investigation; in this work, forensic analysis of incidents is categorized pre-incident forensics and post-incident forensics [20]. Pre-incident forensics is considered a continuous process and repeatedly linked as forensic readiness in the literature. In the continuous sub-category of forensic analysis, the focus is on the forensic capable cloud architecture and similar solutions. In a post-incident forensics analysis, the forensic models and procedures concerning the digital investigation linking cloud infrastructure and services are examined. Incident driven is the base solutions for evidence collection from the cloud storage ecosystem.

• Continuous: This includes the evaluation of forensic abilities for an organization’s cloud infrastructure. Usually, the forensic system is a post-incident evaluation process. Though, due to the popularity of cloud services and the steady evolving technological and cyber threat landscape, it is pivotal that
forensically pleasant cloud is in welcoming for continuous evidence collection, aggregation, and storage [1]. This subcategory includes methods following continuous forensics through valuable logging. The different subcategory (put up-incident forensics) has two options for artefact series typically through cloud client's credentials and by request to the cloud service provider.

- Post Incident: Has been significantly studied by many researchers, although several demanding situations stay unsolved. For example, Dykstra and Sherman [2] propose FROST, a forensic toolkit, which focuses on evidence acquisition for virtual disks, API logs, and guest firewall logs. Alex and Kishore [3] additionally targeted at the evidence collection stage through a centralized server, since investigators within an organization may also have access to the server to collect evidential artefacts. Other researchers which include [4], focused on collecting relevant evidence from virtual machine VM files for reconstructing events and further analysis. Qi et al. [5] developed a forensic hypervisor to perform dependable collection and preservation of evidential artefacts from a compromised system, including the malicious guest operating system.

The traditional digital forensic process undergoes different processes when collecting digital evidence. Evidence is collected through the extracting the data from the victim's hardware machines. Extracting the evidence in the cloud has a different approach considering its different service architecture and deployment models.

Different approaches used in many types of research indicate that it is difficult to collect evidence in the cloud due to the heterogeneity and high volume of data which spared across different locations and it has the following steps.

- Identification of digital evidence describes the requirement for evidence administration, knowing the specific locations and its whereabouts. It is also imperative to identify any malicious actions of non-authorize users. This action considered as a threat to organizations when any individual or Cloud service providers CSP authority chairs their complaints against unwanted issues. This segment includes two categories of identification which includes Evidence Identification and Incident Identification, respectively.

Most of the devices necessitating forensic examination has grown significantly since 1999 [21]. Cloud computing, for instance, improves new requirements for forensics investigation. Identification of cloud computing services used on a seized device might become a more critical part of the standard forensic identification processes for the victims confiscated devices.

- Collection and Preservation usually are concerned with ensuring evidential data collected remains unchanged or unaltered entirely. For instance, if a forensic investigator desires to recuperate data from a device, it is significant to make sure that the data is recovered using the appropriate methods that are forensically sound, i.e. means they do not write to the original data source as evidence such as the last time file accessed.

- Analysis changes the level of data collected that is collected in the last two earlier stages into evidence acceptable by the court of law. In the cloud computing domain, all the data analyzed using suitably and legally acceptable techniques so that it does not been altered and can be justifiable.

though, the information stored on the cloud including the network data that might be collected when communicating between the client and the cloud with any data stored on the client such as cache data needs to be investigated.

- Finally, Reporting and presentation is the final stage during the forensics investigation process. After completion of the investigation, the report must be presented containing the details of the investigation will be presented to the jury in terms of providing expert evidence on the analysis of the investigation. This component is mostly concerned with legal presentation and is normally unchanged irrespective of the computing platform being analyzed.

Recently the spread of advanced cybercrimes related to the dissemination of cloud computing, where everything runs virtualized in a diversity of geographically distributed data centres, has led to significant changes in traditional digital investigations. Cloud forensics has been acquainted and introduce to assist investigators find potential proof against cloud crimes and keep up the security and integrity of the data put away in the Cloud. A portion of the difficulties faced by the forensic examiners towards information securing in a cloud domain comprises of the accompanying [22].

1. Physical detachment: The Shreds of proof is dissipated and spared in various areas because of the exceptional qualities and heterogeneous nature of the Cloud. It prompts indifference towards the acquisition and collection process.

2. Cloud service providers utilize volatile information Virtual Machines for provisioning their clients. In this Virtual machine, unpredictable information like registry entities or unstable web documents will be lost if it does not synchronize with capacity gadgets like Amazon S3, for example, all data in Virtual Machine may be deleted when the Virtual machine gets restarted or shutdown.

3. Trust issue: The trust issue is another issue which is protected by the third party for gathering proof in the Cloud. It is pointed out in child phonography case after a
search warrant was issued, the investigator who is investigating the case needs an internal staff to assist him in collecting the data. In some cases, this person may be from the same cloud service provider or may not be a certified investigator, and of course, this will affect the integrity of the data to be provided and presented to the jury [23].

4. Multi-Tenancy: In Cloud computing different clients may share individual resources for one reason or the other, perhaps during forensic examinations while acquiring evidence from the Cloud two critical issues must be addressed by the investigator, such as proving that the extracted data does not mingle or mixed off with others data, and the integrity of the other data must be maintained.

5. Chain of Custody: This is one of the most significant issues in cloud forensics investigation which is indicating the nature and type of evidence also collected when and how the evidence was collected and presented to the court of low.

6. Cross Border Law: most of the data centres owned by the cloud service providers are distributed and spared across different part of the world. Due to the disparity of cross border laws, the forensic investigations must be carried out according to the specific laws of in that domain whereas the measures for preserving the data and chain of custody differ according to the jury; therefore, the entire investigation process might be affected by the cross-border law.

In all blends of cloud computing services and deployment models, the cloud client faces the test of diminished access to forensic data. Access to forensic data differs reliant on the cloud model; IaaS clients appreciate moderately simple access to all information required for a measurable examination, while SaaS clients may have practically zero access to information required [24]. Diminished access to forensic information implies the cloud client has no control over the precise physical locations of their information and may just have the option to locate the area at a higher level of abstraction, ordinarily as an object or container recognized. Cloud service providers deliberately conceal the location of information from clients to encourage information movement and replication [25].

Cloud forensic processes involve different phase investigators used to collect evidence in the cloud which consist of Identification, Collection/Acquisition, Preservation, Examination and analysis and finally the presentation of Results. Cloud forensics is a very new area that has emerged due to dynamic multi-tenant and black box architecture of the cloud. The traditional digital forensic technique becomes blurred with the advent of cloud technology [26].

The traditional digital forensics assumes that the computer being investigated is within reach of an investigator. Still, in the context of cloud, this process becomes out of reach of any investigator. To gain access to computer the investigator has to rely on Cloud service provider which is again impossible in case of cloud as data being investigate resides in virtual instance and shutting down the situation and seizing for forensic investigation may force other virtual instance which is running to shut down which is not again the policy of cloud providers.

5. CLOUD FORENSICS SOLUTIONS

As revealed from the literature various authors propose different solutions with regards to cloud forensics,

a) Provider Driving Forensics

The role cloud service provider during forensics investigations is paramount, especially when they host and control the fundamental hardware infrastructure upon which user's application and data reside predominantly. The service models also affect the degree of control over a working environment and play a significant role in forensics as well. In this form, the cloud service provider categorized as a dependent solution which can be considered as log-based solutions and agent-based solutions respectively. It is observed that most of the provider-driven solutions emphasized on the forensic readiness of the fundamental cloud infrastructure and on the continuous collection of evidence in a centralized manner. A primary focus of most approaches in this category is on ongoing evaluation by CSPs, which they provide as a service to the consumers and investigators.

i. Log-based Solutions

Logging in forensics evidence collection is a continuous process that documents each event of the system, including the hardware and software components in a set of files which is referred to as log files [27]. The functions of log files vary and rely upon the software and applications that generate the events. In addition to fault tolerance, logs are an essential aspect of security control and digital investigations as they can help the organizations to detect incidents, security violations, and malicious activities. For instance, investigators can determine the source and timeline of relevant events, including reconstruction of events [28] for forensic purposes. Central logging is another potential solution owing to the distributed nature of cloud computing [29]. In the cloud, identification and collection of data is not a trivial task due to virtualization and data distribution. Central logging allows forensic investigators to have timely and efficient identification and collection of digital evidence by using a single storage location [30].

Cloud architecture produces and stores numerous types of logs including virtual machine, system, network, security, application, audit logs and web-server [31] at manifold levels.
might be questioned in a court of law, due to the use of bot malware to compromised the suspect's or target's machine. Hence, it is highly recommended that the legal team be consulted prior to using such an approach.

b) Consumer Driving Forensics

It is generally accepted that CSPs play a crucial role in cloud forensics, as mentioned earlier. In other words, less visibility/control in the cloud environment, especially in Platform as a service (PaaS) and Software as a Service (SaaS). The forensic investigators need to collaborate with CSPs during the collection of evidence. There are several legal and operational challenges [36]. For example, CSPs have the right to reject a request from a foreign investigator (e.g. legal jurisdiction restrictions) or consumers (for example, if the request is not part of the Service Level Agreements (SLAs). Even when the cloud service providers work together, there is need to consider issues such as the integrity and reliability of the evidence and the chain-of-custody. There is, therefore, a need to develop solutions that are consumer-oriented compared to CSP-oriented or dependent and trusting solutions

i. Physical Acquisition-based Solutions

Physical acquisition is an essential part of the traditional digital investigation process. Investigative teams identify and acquire potential sources of digital artefacts that can provide useful insight into the ongoing investigation. However, cloud computing differs from the traditional computing environment, and such an example is the multi-tenancy environment through resource virtualization. Besides, the distributed nature of resources and jurisdiction further complicate the physical acquisition of cloud resources. In this work, attention is focused on cloud-side forensics to client-side forensics.

ii. Management Plane-based Solutions

The management plane is an interface/dashboard that allows users to access cloud services without the intervention of the CSP. It manages all aspects of the cloud infrastructure, including monitoring, resource usage, and security information. This is clearly CSP-independent because it centralizes the management of cloud resources through an API and web browser and supports evidence collection. There are only two main solutions in this category that the Management Console proposed as a CSP-independent forensic solution. Dykstra and Sherman [1] designed and implemented a solution called FROST that included forensic tools for the OpenStack public cloud platform to gather evidence in the form of virtual disks, API protocols, and guest firewall protocols. The authors added a new set of APIs to the NOVA project to enable consumers/investigators to conduct a forensic acquisition of the cloud infrastructure regardless of Cloud service provider intervention.
The management console consists of a set of software APIs for deploying, monitoring, and managing the cloud services via the Internet. Software APIs become the de facto standard for organizations to deliver their products and services to their consumers as APIs allow applications to communicate with each other. However, APIs may have vulnerabilities that can be exploited. For example, a Smart Bear report identified API security as one of the biggest challenges for organizations. The Cloud Security Alliance (CSA) also identified insecure interfaces and APIs as one of the keys Security threats in a cloud computing environment. Security assessment of APIs is critical as APIs can be used as an attack vector. In Lit. [2] However, there was no discussion or assessment of API security. FROST also requires confidence in the underlying cloud infrastructure and Insider threats, including malicious CSP’s, were not considered. In Reference [3], both FMP and Forensic Servers are vulnerable to various attacks, including MITM and eavesdropping due to placement and may have serious safety and forensic effects if compromised and controlled by malicious units. In addition, FMP and the forensic server may also cause the service to become unavailable and cause an impact on safety.

c) Resource Driving Forensics

Utility computing and resource measurement are fundamental to cloud computing Pay-as-you-go model that provides resources as services to consumers. In the cloud, virtualization is not limited to servers, storage, and network virtualization is considered a key component in a cloud environment. However, the cloud’s gain is the loss of forensics, i.e. Virtualization helps the cloud improve hardware utilization, but introduces new barriers to the forensic process. However, multi-tenancy, data distribution, and redundancy are characteristics of a cloud. These features become challenges for forensics; there are three basic services CSPs provide, compute, storage, and networking. In the cloud, "compute" does not refer to the nude physical hardware, more virtual hardware in the form of virtual machines with vCPUs, and Storage and Network refer to virtual disks and virtual networks. For forensics, we focus on these three basic resources which are divided into three categories of virtual machines forensics, storage forensics, and network forensics.

i. Virtual Machine Forensics-based Solutions

Virtual machine forensics is divided into two subcategories: static analysis and live Analysis. Static analysis is an analysis processed after an incident occurs by forensic investigators. Once they have collected relevant evidence and kept it in persistent storage. In the Cloud, live analysis is also a preferred forensic method as it works without the Cloud / VMs. Static analysis. Static analysis is a process of investigation and analysis of stored and preserved data permanently. The main objective of this approach is to carry out a critical task Evaluation of the collected data and evidence to facilitate the digital investigation that can stand in the court of law. Static analysis can help investigators by detecting the origin or by Create a timeline for the entire incident. The static analysis presents several solutions that A copy of the VM is created that records the status and data to protect a Runtime condition of the VM for subsequent recovery. The status of the VM contains the operating status VM, including all configuration parameters, and the data includes the hard drive, storage, and Network files. All this content is the basic elements of almost all digital investigations. Cases that make VM snapshot a viable forensic proof. Analysis. The live analysis is a process of examining the current state of the running system. Live analysis overcomes the shortcomings of traditional static analysis that fails to gather volatile and continuously changing information, including process list, memory contents, open ports, and connections. Live analysis in a cloud environment is possible due to the remote accessibility feature, and it does not require any shutdown of VMs. In the cloud model, service availability is an important factor, and shutting down VMs for each occurrence of a security incident is not feasible.

6. CONCLUSION

The cloud forensics and digital forensics are interrelated computing paradigm which provides solutions to many problems. Cloud computing is a business model that brings different issues to digital forensics investigators and the digital forensics community in general. This paper presents different aspects of cloud forensics challenges, especially during forensic examination in the cloud, all issues related to the internet and computers are applicable to the cloud, including threats. However, traditional digital methods and technology fail to do forensics in cloud environment due to its dynamic nature.

Cloud computing is a business model which presents a range of new issues to digital forensics practitioners and the digital forensics community in general. There is an urgent need for forensic investigators to adapt existing forensic practices and develop an evidence-based forensically sound methodology that would enable forensic investigators to identify, preserve, collect, examine and analyses data fragments in the cloud computing environment.

REFERENCES


