International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Systematic Literature Review on Cloud Forensics in Cloud Environment

Vadetay Saraswathi Bai[1]*, Prof T. Sudha[2],

Submitted: 16/11/2022 **Accepted**: 21/02/2023

Abstract: In the area of Cloud Environments, the use of cloud forensics has been developed as a result of the apparent resource, cost-effectiveness, ubiquitous nature, and flexibility of the cloud itself. This kind of cloud forensics includes private, hybrid and public models in addition to a variety of other choices such as security, database, software, and integration. The corporate organizations may realize major economic benefits from using this approach. Therefore, the traditional advanced encryption standard algorithm needs to be enhanced in order to scope with the emerging security threats in the cloud environment. This development comes with its own set of difficulties and malpractices in cloud. This article presents a comprehensive literature study addressing various existing tools and techniques in the field of cloud forensics according to AES algorithms. Further this study details about research challenges and scope of further research in automating the process of legal implications.

Keywords: *forensics, malpractices, algorithm, implications*

1. Introduction

Recovering and analysing data or artefact's from a computer or other digital device is known as digital forensics, a subfield of forensic science often performed in the context of a computer crime. This working definition of digital forensics was developed during the inaugural Digital Forensics Research Workshop, held in New York in 2001. Digital forensics is defined as "the application of scientifically derived and proven methods to the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or for assisting in the anticipation of unauthorized actions shown to disrupt planned operations."

Since its evolution, the Cloud as it exists now has seen noteworthy improvement. As cloud computing gained more significance in the IT world, hackers began their attention towards cloud services. Initially, cloud computing was plagued by security and privacy concerns. Many businesses were cautious to move their data to the cloud at first. The cloud has several drawbacks, but its benefits (especially the low price) are worth it. Implementation in the cloud has become increasingly complex as a result of technological developments in the information technology sector. Cloud problems were less severe as more people gained knowledge in this area. Innovation in fields such as IoT and Big Data Analytics were given a boost by the advent of cloud computing.

The method in which businesses provide their IT infrastructure is drastically transformed with the advent of cloud computing technologies and its wide range of services. The cloud computing migration process entails the substitution of virtualized, remote, on-demand software services, tailored to the specific

Requirements of a company, for the conventional IT hardware located in the data centre (such as servers, racks, network switches, and air conditioning units). The user's own organization may host and maintain these services (on a smaller hardware basis), or they can outsource this responsibility to another company. As a result, the organization's application's data and code might be spread out over a vast geographical area. Cloud computing is defined by the National Institute of Standards and Technology as "a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.".

1Research Scholar, Dept.of CSE,
School of Engineering and Technology,Sri Padmavati Mahila Visvavidyalayam
Email id: saihumika9@gmail.com
2Dept. of Computer Science,
Sri Padmavati Mahila Visvavidyalayam,
Email id: thatimakula_sudha@yahoo.com

The term "Cloud Forensics" refers to the use of digital forensics in a cloud computing environment. This field is considered to be as a multidiscipline area. The following definition [3] was offered by the NIST's recently formed cloud forensic working group. By identifying, collecting, preserving, examining, and reporting digital data for the purpose of facilitating the reconstruction of past cloud computing events, " Cloud Computing forensic science is the application of scientific principles, technological practices and derived and proven methods to process past cloud computing events through identification, collection, preservation, examination and reporting of digital data for the purpose of facilitating the reconstruction of these events". Layers of complexity are added to cloud forensics by the inherent characteristics of cloud environments, such as multi tenancy, jurisdiction, data duplication, and a high degree of virtualization. When CSPs engage in inter-carrier service trading, the complexity of tracking the flow of events increases. For this reason, the forensics procedure used in a conventional (non-cloud) environment is impractical when dealing with cloud data. Cloud forensics has three components: the technical, the organizational, and the legal [4]. The technical aspect includes everything that is required to carry out the forensic process in a cloud computing environment, such as the necessary protocols and tools. Data collecting, live forensics, evidence segregation, and preventative measures all fall under this category. The organizational perspective, in contrast, is concerned with the discipline of forensics as an institution. Service providers (CSPs), consumers (customers), legal counsel (clients), incident responders (responders), and objects (binding service level agreements (SLAs), rules, and guidelines) are all part of this ecosystem. Last but not least, the legal perspective encompasses the creation of regulations and agreements to guarantee that forensic activities do not break laws and regulations in the jurisdictions where the data resides or is collected, while also protecting the privacy of tenants who share the same infrastructure. There has been a recent uptick in the use of cloud computing to store data and apps for both businesses and consumers. Since forensic investigators occasionally have access to the underlying infrastructure, the widespread adoption of cloud computing routes to several difficulties. Cyber Criminals (hackers) have a strong interest in these cloud service providers because of the prosperity of information on their customers that they possess. It's also possible for cybercriminals to exploit cloud computing to facilitate the spread of malware, digital scams, and engage in other forms of illicit activities. As a result, investigating crimes committed in the cloud is a challenging aspect of research.

As cloud computing turn out to be more widely used, additional cloud-based threats have emerged. Due to the unique characteristics of the cloud, forensics in the cloud differs from conventional forensics. Trust, network forensics, evidence collecting, privacy, and data provenance are few of the forensics challenges that have come to light during the previous decade of study. Over the last decade, there have been over 145 scholarly articles published on Cloud Forensics; during the initial scrutiny of the study these are narrowed down to 83 based on topics covered, publication year, authors, and more.

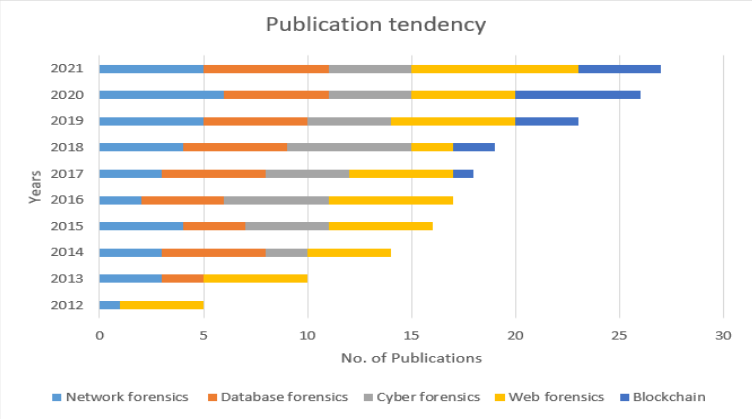

Fig. 1: Publication tendency of cloud forensics

To identify emerging topics in cloud forensics, the identified articles are deeply reviewed. Figure 1 shows the tendencies of publications over the decade relating cloud forensics. Researchers were interested in Cloud Forensics in the early part of 2010. These early articles showcase research efforts in network forensics and data preservation of cloud forensics. From 2013 on, problems in cloud forensics and frameworks to address them became apparent. The range of publications was increased in 2015. The difficulties of cloud forensics were the primary emphasis of these studies, followed by the gathering of evidence, the resolution of network problems, and the development of supporting frameworks. Recent years of published research have

shed light on unexplored facets of cloud forensics. Expertise in the cloud is growing, according to a study conducted by Gartner in 2016. We find no significant deviations in the research trend we examine. 60% of 2016's research articles focused on cloud forensics frameworks. As of 2022, block chain was widely used to solve the data provenance and security issues in cloud environment.

This research paper depicts cloud forensics taxonomy derived from [55] in section 2, further section 3 specifies research methodology adopted during systematic literature study. Section 4 presents detailed review of various existing studies. Research gaps and challenges in cloud forensics are presented in Section 5.

2. Cloud Forensics: Taxonomy

Digital forensics is broken down into three distinct subfields: disc forensics, memory forensics, and network forensics. These may be accomplished via the use of various digital forensics tools and techniques, all of which are geared towards the collection of data specific evidence to support the inquiry. The cloud's evidence is derived from several data stores. Evidence might be acquired from a variety of cloud-based resources, including virtual disks, virtual memory, and network logs. The types of evidence used in investigations vary based on the service model and the deployment architecture. The goal of effective and timely forensics in the cloud requires consideration of all the forensic factors. The authors of [5] propose a taxonomy for cloud forensics solutions. The focus is on the actors, however. As shown in Figure 2, this study develops a taxonomy for cloud forensics, which encompasses the most important aspects of cloud forensics. Included in the suggested taxonomy are the difficulties associated with cloud forensics, such as gathering and analyzing evidence, dealing with problems of trust, and considering the legal implications of such actions. In what follows, we flesh out the suggested taxonomy in further depth.

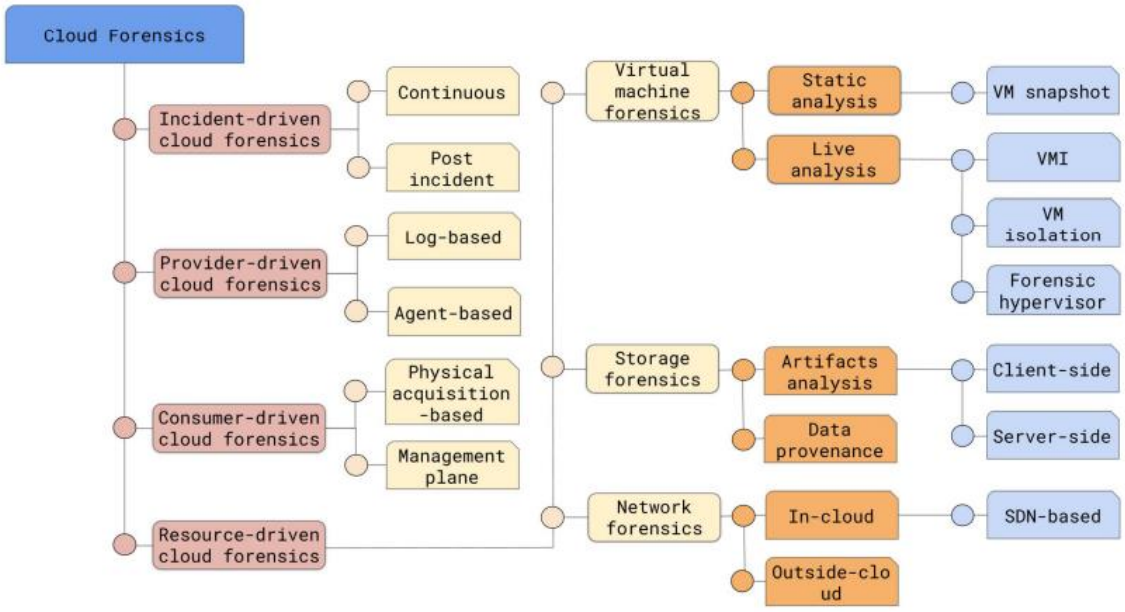

Fig. 2: Cloud Forensics taxonomy

3. Advanced Encryption Standard

In this paper, the cloud computing confidentiality framework is chosen. This framework employs a data integrity method to increase data security through the use of cryptography. The improved AES (advance encryption standard) cyphers have low power, time, and network delay consumption and can encrypt 128 bit data blocks in 1000 cycles. The frameworks' additional tasks include load balancing, establishing trust, and effectively managing network resources. The ability to safeguard a lot of data is a benefit of utilising symmetric keys.

4. Research Methodology

Research methodology is defined as "the process of conducting a planned, systematic, and theoretical evaluation of available techniques to a defined research topic" [5]. This research uses a systematic literature review (SLR) approach to analyse and assess previous studies that have tackled different cloud forensic concerns in a multi-cloud environment. It gives a bird's eye perspective of the research challenge in terms of how different computer intelligence techniques may be applied to it. Complete SLR procedure is shown in

Figure 3. Overall, there are three stages: preparation, performance, and documentation. The following procedures outline an algorithmic and methodical sequence of tasks carried out during SLR.

- Formulation of research questions is the first and most crucial step in the SLR framework (RQ). The RQs are formulated in the context of cloud forensic research in order to investigate, extract, and analyse the current uncertainty and to highlight the most promising areas in need of focused study.
- Using an effective search strategy, exclusion/ inclusion criteria, and data extraction and synthesis procedures, a systematic review protocol is developed to filter the collected data.
- Methods for selecting, composing, and discovering various crimes in cloud environment are thoroughly analysed and demonstrated, and their respective evaluation findings are documented in a review.
- Compile a summary of the review's findings to help budding researchers to fill in the knowledge gaps addressing challenges in current research of cloud forensics.

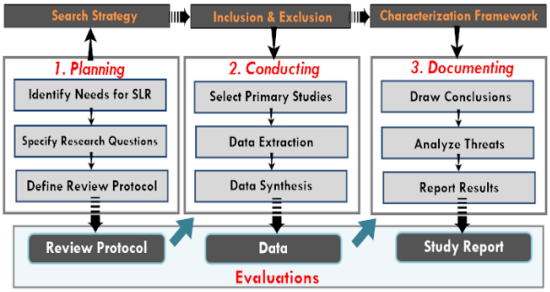

Fig. 3: Resrach Methodology

4.1 Formulation of Research Questions

This research aims to summarize the current state of forensics research using AI in cloud computing, blockchain, and the Internet of Things by reviewing previous studies and their conclusions. In Table 1, this study outlines three research questions that will serve as guidelines for our investigation. We discovered 49 main papers on the use of digital forensics in cloud computing, blockchain technology, artificial intelligence, and Internet of Things from 2016 to the beginning of 2021. Researchers in related fields may use this bibliography to further inform their own investigations. When comparing studies of a similar kind, these ones might be helpful standards. We provide an in-depth analysis of the data in these studies and offer it so that forensics' use of AI in cloud computing, blockchain, and IoT may be accurately reflected.

Table 1: Research Questions

RQ 1	What forensic approaches are taken into account while working with cloud computing, blockchain, and the internet of things?
RQ 2	How is forensics used in an environment that is intertwined with cloud computing, the internet of things, and blockchain technology?
RQ 3	How can artificial intelligence be used to enhance the forensic procedures that are used in digital forensics in relation to cloud computing, the internet of things, and blockchain environments?

4.2 Assessing and Selecting Research Studies

The research papers that were retrieved and collected based on the automated and manual search strategy are analyzed in a comprehensive way, and devised an inclusion and exclusion criteria to further filter the articles based on their findings. The search phrases are then adjusted in order to facilitate the extraction of information pertinent to tools and techniques in cloud forensics. The following are the factors that determine inclusion and exclusion criteria.

- Research publications that provide a detailed depiction of the hypothesized process as well as an experimental study are considered.
- Research studies that place an emphasis on the implementation of heuristic, metaheuristic, and intelligent algorithms in cloud forensics are accorded a greater priority.
- Research papers that tackle problems at any step of cloud forensics are included in the study.
- Research papers that contain quantitative evaluation methodologies and standard datasets together with evidence-based experimental analysis have been included.

5. Documenting the Review

The review of the existing studies is documented in a systematic procedure analysing various stages of cloud forensics that include, identification of security breach, Evidence collection , analysis and presenting in the court of law with legal implication of cyber law.

5.1 Studies related to occurrence of security breach in Cloud environment

In the classic approach to forensics, the process of incident detection is a simple one since the resource being investigated (the target) is a straightforward computer system. Cloud services function as collaborative service models; implementing cloud computing might be difficult. The identification of hostile activity could go undiscovered for a period of

time that is sufficient to provide the adversary ample time to flee or conceal themselves. After the incident has already taken place, cloud forensic may be performed. However, if an Intrusion Detection Mechanism (IDS) is given for incident identification in the architecture of the cloud, it may make the forensics simpler [3] and reduce the obstacles of the identification phase. If a piece of data is either sent via the resources of the network or saved on a device that is freestanding, then that data is considered to be electronic evidence (EE). The information that EE conveys is sensitive, and improper treatment or study may quickly alter, damage, or destroy it. This results in the information being exceedingly fragile. Due to the nature of EE, introducing it as evidence in a legal proceeding is a very challenging endeavor. For the aim of this endeavor, the standard ISO/IEC 27037:2012 establishes standards for the management of digital evidence. These rules mandate that electronic evidence (EE) fulfill the criteria of the applicable laws, and it should also be easily recognized within a cloud context. Not every information relevant to an event may be considered proof of that occurrence. The amount of information that is linked to the incident has to be combed through in order to identify the evidence. In order to identify evidence contained inside a cloud platform, certain architectural assistance is required [3]. For the purposes of cloud forensics, it is just as difficult to separate evidence pertaining to the resource from that pertaining to the cloud tenant [6, 7, 8, 9, 10]. Because of the cloud's decentralized nature, it is very difficult to identify the dispersed evidence [11].

5.2 Studies related to Evidence Collection and analysis pertaining to cyber crime

After the evidence has been identified, the next step in the forensics process is the collection of evidence. During the process of evidence collecting, researchers [6, 12, 13, 7, 8, 10, 14, 15] have focused on the multiple obstacles that are presented by cloud forensics. It is possible to classify some of these concerns, but this is not limited to, remote acquisition [16], physical inaccessibility [17], data that is volatile [11, 17, 14], access to devices that are connected to the cloud network [17], and access to data, evidence, and logs that are stored on the cloud [11, 17, 18]. [19] devotes a significant amount of space to discussing the issue of log forensics. It has also been recommended in [19] that a tool for automated log analysis be used in order to address some of the vulnerabilities and difficulties that may arise. It is possible that CSPs will not be able to have a mechanism for the storing of logs [20, 11, 7, 17, 10, 14], or it is possible that the logs that CSPs store will not have anything to offer in the way of evidence [7]. There is no predetermined structure for any of the data that may be entered on a cloud-based platform [7]. A significant obstacle is in the vast quantity of the data that may be located and compiled as proof. In addition to this, the offloading of such enormous volumes of data from the cloud necessitates the use of an enormous amount of bandwidth [8]. In most cases, it is the CSP's responsibility to supply the evidentiary data if the investigating authorities ask for it or if the CSP is called as a witness.

Examining the evidence at hand is necessary in order to determine whether or not the alleged incident really occurred. The study of the data is referred to as analysis, and this process has a name. Conventional approaches to digital forensics make use of several tools, including the Forensic Tool Kit (FTK), volatility, sleuth kit, CAINE, Autopsy, [77], and others. However, using these traditional methods in cloud forensics investigations for the purpose of analyzing the virtual environment of cloud computing is a challenging endeavor [6, 11, 17, 16, 10, 18]. Since the environment of the cloud is multi-tenant by design, numerous users are able to consume as well as share the services that are provided by the cloud, and there is some degree of isolation between the user's data. When there are several tenants in a building, the forensic investigation procedure has a greater potential to become more difficult [6, 11, 17, 16, 10, 18, 15]. Criminals that target cloud infrastructure often use anti-forensics techniques [13, 21]. The concealment of evidence calls for the establishment of a framework that is capable of addressing the issue of anti-forensics in the cloud. The stage that comes before the analysis, known as "collection of evidence," has a significant impact on the stage known as "analysis." It is referred to as live forensics when resources and data are evaluated at run time, even while they are being employed, and it is really a highly tough process [6, 12, 8] for cloud forensics.

The investigation of the evidence allows for the formation of a conclusion. It's possible that a significant amount of evidentiary data will be evaluated. The process of forensic interpretation might be automated, but this could have unexpected repercussions. The automation of digital forensics comes with a number of potential risks [22]. In order to evaluate the data that has been gathered via the investigation [10, 17, 14], it is possible that the crime scene may need to be rebuilt. Additionally, cloud domain expertise may be required. An investigation into a virtualized environment [8] is a laborious process that is required in order to evaluate the studied data. Cloud expertise is required of the analyst who will be conducting the investigation. The forensics investigation team has to be well-versed in cloud forensics in addition to being familiar with the most recent methodologies and technology.

5.3 Legal Implications

The presentation stage of the process is the next step in the procedure. During this stage, the findings of the investigation are submitted in court. The difficulty in exhibiting the results of the study in court [15] is a direct result of the complexity of the architecture of the cloud [18]. It is difficult to maintain the authenticity of electronic evidence due to the fact that it is exceedingly fragile [16]. A multi-jurisdictional view of the data is one of the key concerns of cloud forensics at this specific level [6, 11, 17, 16, 10, 15]. In addition, there are other problems such as privacy legislations like the General Data Protection Regulation (GDPR) [14], the requirements of the Service Level Agreement (SLA) [11, 7, 17, 9, 10], and SLA verification [9], which only make it more difficult to accept evidence in a court of law. [6, 17, 16, 14, 18] One of the most important challenges in cloud forensics is ensuring that the chain of custody is maintained during the whole of the inquiry.

5.4 Related Work: Frameworks, Techniques and Algorithms

Each of the elements of the process of digital forensics becomes more challenging when it is carried out in a cloud environment. According to the results of the preliminary survey that we carried out in the previous part of this chapter, one of the primary problems raised by research is the gathering of evidence. In the field of cloud forensics, academics have developed a number of different frameworks in recent years in an effort to find solutions to the problem of evidence collecting. This section includes a comprehensive overview of the methodologies and frameworks that were used.

Agent-based methods, such as the (controversial) employment of bots and botnets as a forensic agent, have also been advocated in the literature. Bots are malicious software that spread from one hacked computer or IoT device to another in an attempt to infect as many systems as possible and take advantage of security flaws in network devices. These infected computers may subsequently coalesce into a botnet, a network of (malicious) agents programmed to carry out certain actions at specific times or in response to commands from a central server or master [20]. This category of publications includes those that provided proactive measures to extract information in a no malicious way to aid in forensic investigations after an occurrence. For instance, Kebande and Venter suggested implanting a bot agent inside each virtual machine in order to collect data from them and store it in a database.

From infected virtual machines, Kebande and Venter collected volatile and non-volatile data, including network traffic, and sent it to a central repository for proof. Botnet-as-a-Service (BaaS) [41] and Agent-Based-Solution-as-a-Service (ABSaaS) [42] allow data to be collected and stored for later use in forensic investigations. In addition, Liu and Zou [50] developed a system architecture including a forensic center and a forensic query server, both of which are based on the use of forensic agents to solve the problem. It is the job of the forensics center to take the raw data collected during an investigation and transform it into a set of tuples suitable for database storage. Access to the system's logs, open files, network connections, processes, auto-run services, and other forensic data was made possible via a centralized interface given by the forensic query server. However, the authors did not take into account the possibility of a compromised VM instance collecting manipulated evidence through a forensic agent. We also mentioned that the deployment of bot malware to infect the suspect's or target's system might cause legal problems for BaaS. Therefore, it is strongly advised that the legal team be informed before attempting such a strategy.

Simou, Stavros, and others [17] have discussed a model titled Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems that might be of use in a forensics inquiry. Although this model does not particularly discuss any platform for the collecting or processing of evidence, it does show the relationship between the pieces that make up a forensics investigation. AlmaNebula [23] puts up the concept of forensics as a service and attempts to depict it. In the article, there is a suggestion for a newly developed application for digital forensics that makes use of a cloud operating system that operates at the hypervisor level. For the purpose of forensics, the author makes advantage of the hypervisor's Application Programming Interfaces (API). Despite this, the concept presented in the research is entirely speculative and is not based on any findings from experiments. In their proposal [24, 25], Zawoad, Shams, Amit Kumar Dutta, and Ragib concentrate primarily on logs of VMs and provide a system that provides safe access. It makes it possible for the forensics professionals to log in and do analysis on logs. Both the logs themselves and the evidence of the gathered logs are kept in separate places for safekeeping. The authors have provided a discussion on a threat model as well as a potential event in which the confidence placed in any configuration by the user, the investigator, or the CSP is called into question. In circumstances such as these, the SecLaas model is used to ensure that the logs maintain their completeness and authenticity. In order to safely collect the logs, the implementation of this proposal takes use of both a one-way accumulator and a Bloom's Filter as the proof unit.

Pichan, Ameer, Mihar, Lazarescu, and Sie Teng Soh [26] have proposed an idea for a structure that is log-based

while also taking into consideration the business requirements of the forensics user. The logging process is one of the most difficult aspects of cloud forensics. The CFLOG [45] architecture is responsible for storing the user log so that the evidence may maintain its confidentiality. A heuristic cloud forensics model was proposed by Povar, Digambar, and G. Geethakumari [27], who also contributed to the work. In order to keep the information associated with each virtual machine (VM) distinct in the event of many tenants, the authors have provided a framework. They have furthermore integrated a query-dependent unit that is able to access logs in a distant location. Ahsan, MA Manazir, and others [28] have a proposal for a framework that is similar to SecLaaS [24] that would preserve logs in addition to collecting evidence. [28] There are substantial discrepancies in the ways in which SecLaaS [24] and CLASS [28] gather evidence in their respective processes. By using a public key for each user to encrypt cloud records, CLASS ensures that the privacy of cloud users is protected. This is an important aspect of CLASS. In the event that there is an investigation, it also makes it easier to retrieve logs. Jiang, Ci-Bin, and colleagues [29] have developed a concept for a distributed log system within the context of a network architecture, coupled with an increased log collection load in a cloud environment. The writers have added a discussion of the effects that using up bandwidth and having traffic in the background might have on the overall system.

Almulla, Sameera, Yousef Iraqi, and Andrew Jones [30] provide a system for the collecting of evidence as well as the reconstruction of events. The idea of using distributed snapshots as a backup strategy is fundamental to this approach. In this approach, snapshots are taken not just of the storage but also at the application level simultaneously. The evidence analysis that uses map-reduce is discussed in the testbed for the Hadoop Distributed File System. Sampana and Stephen S propose the FoRCE [31] architecture as a method for separating the cloud's evidence, collecting it, and storing it. The FoRCE template performs its duties on a private virtual private cloud that is installed on the target cloud. After it has succeeded in isolating the target instance, it will produce a snapshot and collect evidence. A cloud forensic model that the authors Raju, BKSP Kumar, and G. Geetha kumari suggest in [32] is referred to as SNAPS. This model is built from a series of photographs taken in the time leading up to the occurrence of the event. This strategy also places an emphasis on two additional difficulties, namely, the supply of minimum storage for the snapshots and the problem of determining the gravity of the data.

In [33], Hemdan, Ezz El-Din, and D. H. Manjaiah propose a method that makes use of intelligence. It takes snapshots of each Virtual Machine (VM) that is operating in the cloud at predetermined intervals. There is a reliable center server that not only monitors but also records the VM's current condition and any snapshots that have been taken. The forensic server is the one that does the forensic analysis. An Open Cloud Forensic (OFC) Model has been proposed by Zawoad, Shams, Ragib Hasan, and Anthony Skjellum [29], and it is based on the principle of continual synchronization of data obtained from the cloud. The fundamental objective of this strategy is to forestall the CSP from conspiring with the adversary with the intention of misleading the inquiry in any way. APIs guarantee that the evidence will be made accessible to the appropriate parties. In addition, the OFC has an integrity check module that may be used for the purposes of the court. The authenticity of the evidence that is made public may be checked by the court if necessary.

Chronos is a method that was developed by E. Zawoad, Shams, and Ragib Hasan [51] that makes use of a timestamp management system that is secure and reliable for the purpose of identifying malicious behavior on the part of users. Chronos is a technique that was developed by E. Zawoad, Shams, and Ragib Hasan [51]. There are some parallels to be seen between this method and CURE [52], which was proposed as a method for identifying any changes in time. Another strategy of this kind for controlling one's time was proposed by Kao, DaYu, and Ying-Hsuan Chiu in [53]. [53] This strategy makes use of the meta-data included inside the file to match the timestamps of the date and time. On the other hand, this solution has only been validated on a Windows platform.

Table 2: Analysis of Existing Techniques

References	Evidence Collection Techniques	Forensics Analysis	Framework Proposed	Implementation Details	AI/Machine Learning	Trust Provenance
C. Federici et.al	✓	✓		✓	✓	✓
Zawoad et.al	✓		✓			

Povar et.al		✓	✓		✓	✓
M. Ahsan et.al	✓	✓		✓		
S. Almulla et.al		✓	✓	✓	✓	✓
S. S. Sampana et.al	✓	✓	✓			
E. Hemdan et.al				✓	✓	✓
R. Battistoni et.al	✓	✓		✓	✓	
Kao et.al		✓	✓	✓		✓
Roussev et.al		✓		✓	✓	

Pătraşcu, Alecsandru, and Victor Valeriu Patriciu [35] have developed a solution that integrates the software and hardware management of available resources. In addition to it, the authors propose a forensic investigation software framework. The safety and dependability of the users is the key emphasis of this strategy, and this suggestion makes it easier for investigators to enter into virtual machines (VMs) at different levels. Roussev, Vassil, and others [36] have developed a proposal for a research that argues in favor of the implementation of a forensics toolset for the cloud environment. The authors explain the limitations of gathering evidence on the client's end and suggest the use of APIs that are provided by the CSP. The work that was done by the authors comprises a case study of several methods that may be used to get evidentiary data from the cloud. In addition to that, this case study delves into the topic of collecting evidence and analyzing google documents. The researchers Rani, Deevi Radha, and G. Geetha Kumari [37] have centered their research on the anti-forensics strategies that are used in cloud computing. They give a taxonomy of anti-forensics approaches that are now in existence in the cloud and have come up with a strategy for dealing with the antiforensics. However, the result as well as how their strategy might be used has not been disclosed in the study at any point.

A forensic monitoring plane, also known as an FMP, has been included into Alex, M. Edington, and R. Kishore's [38] architecture for cloud forensics. This framework comes preconfigured with various forensics tools, such as FTK, that may be used to monitor traffic and store data on a forensic server that is separate from the framework's own storage. [39] Qi, Zhengwei, and others have developed a concept for a framework that they refer to as Foren Visor. This architecture features a hypervisor that is specialized to the capture and storage of evidence data for trustworthy live forensics. This lightweight hypervisor also has a means for protecting the evidence that has been included into its design. Secure Cloud is a system that was developed by Uphoff, Maximilian, and their co-authors [40] for the use of forensics tools such as Autopsy. With this structure, it is possible to encrypt forensics data and store it on the cloud. This technique does not make use of any automated procedures that might potentially increase the efficiency of the system. Raju, BKSP Kumar, Bhupendra Moharil, and G. Geethakumar icame up with the idea of FaaSec, which is a framework that is outfitted with an engine for the investigation of cloud forensics. Cloud Forensics Toolkit is the organization that is in charge of gathering the evidence (CFT). In addition to this, the method is able to recognize sequences in any of the application logs that have an ominous appearance to them.

Pătraşcu, Alecsandru, and Victor Valeriu Patriciu have developed a solution that integrates the software and hardware management of available resources. In addition to it, the authors propose a forensic investigation software framework. The safety and dependability of the users is the key emphasis of this strategy, and this suggestion makes it easier for investigators to enter into virtual machines (VMs) at different levels. Roussev, Vassil, and others have developed a proposal for a research that argues in favor of the implementation of a forensics toolset for the cloud environment. The authors explain the limitations of gathering evidence on the client's end and suggest the use of APIs that are provided by the CSP. The work that was done by the authors comprises a case study of several methods that may be used to get evidentiary data from the cloud. In addition, this case study describes the process of gathering evidence as well as analyzing google documents. The researchers Rani, Deevi Radha, and G. Geetha Kumari [55] have centered their research on the anti-forensics strategies that are used in cloud computing. They give a taxonomy of anti-forensics approaches that are now in existence in the cloud and have come up with a strategy for dealing with the antiforensics. However, the result as well as how their strategy might be used has not been

disclosed in the study at any point. A forensic monitoring plane, also known as an FMP, has been included into Alex, M. Edington, and R. Kishore's [56] architecture for cloud forensics. This framework comes preconfigured with various forensics tools, such as FTK, that may be used to monitor traffic and store data on a forensic server that is separate from the framework's own storage.

Raju, BKSP Kumar, and G. Geethakumari [61] provide a novel approach to the detection of attackers operating inside a cloud-based infrastructure. This approach makes use of both distance and a search that is based on ranking in order to identify the VM that has been attacked. This solution does not need the storage of any additional data on the VM. In addition to that, the method incorporates an introspection unit with the purpose of enhancing the identification of unwanted guests. In their paper [62], Datta, Suchana, and coauthors provide a concept for the detection of a malicious host inside a cloud infrastructure. This technique takes snapshots of the events that have occurred on the VM. After the snapshots have been gathered, they are sorted, and then features that are relevant to the event are investigated in order to identify a probable hostile host. In their suggested architecture, Nissim, Nir, and coauthors [63] make use of a Machine Learning (ML) approach for identifying malicious software. Memory dumps obtained from the VMs are accessed and used in this method. The MinHash approach, which is the most effective one for locating binary files that are very similar to one another, is used in the following research. Additionally, additional locality-sensitive hashing was performed by the authors, which helped to improve the classifier's ability to learn. An extensive amount of study was done on the process of evidence collecting in cloud forensics.

6. Research Gap

6.1 Problems in Cloud Forensics

The following are some of the issues that researchers have found to be obstacles in the field of cloud forensics: Data Provenance in the Cloud, Virtual Machine Introspection, Service Level Agreements, Trusted Platform Modules, Isolating a Cloud Instance, and Digital Forensics for Cloud Storage Services.

Collection and Acquisition of Forensic Data: In cloud forensics, one of the most difficult steps is collecting and acquiring data from cloud infrastructure. If a CSP offers a web-based management interface, like Amazon Web Services' (AWS), it may play an important role at this juncture. The IaaS paradigm might benefit from the cloud management plan proposed by Dykstra et al... The console panel allows users and investigators to gather digital evidence such as images, network traffic, processes, and logs from virtual machines. The solution's one and only flaw is that it requires an additional layer of confidence, namely, faith in the management layer. This degree of confidence is unnecessary in the traditional method of gathering evidence, as they have direct access to the system. Guest application/data, Guest operating system, Virtualization, Host operating system, Physical hardware, and Network are the six levels of trust that Dykstra et al. presented. The farther one goes down the stack, the lower the cumulative trust need becomes. The collecting of data for cloud forensics is difficult for a number of reasons. Problems with digital evidence include its inaccessibility due to its location online, reliance on the CSP, data volatility in the cloud, less control over cloud infrastructure, legal and trust concerns, several tenants sharing a single instance, and high bandwidth requirements.

Log Information: Forensic investigators often rely on log information as a crucial piece of digital evidence. Researchers have discovered cloud-related logs. Decentralization, log volatility, many tiers and levels, log accessibility, log dependency on the CSP, and a lack of key information in logs are just a few of the difficulties associated with log information in cloud forensics.

Robust Service Level Agreement (SLA): The existing Service Level Agreement (SLA) is severely lacking in recent times, as it does not explain the obligation of the cloud service provider (CSP) at the time of various harmful acts nor their participation in the digital forensic investigation. SLAs between cloud service providers and their customers were a major focus of the studies [18, 19]. The problems with openness may be addressed if the CSP establishes a solid foundation of trust with its clients. Providers' responses to cloud-based crimes, including if and to what degree they aid in forensic investigations, should be included in a solid SLA. Relatedly, one may wonder how one would know whether or not a SLA is strong. Utilizing the services of a reliable outsider may help guarantee the SLA's reliability (TPA).

Data Provenance in the Cloud: When conducting a forensic investigation in the cloud, it is crucial to have access to an object's history, which may be gleaned through its provenance. The use of secure provenance allows us to get crucial forensic data, such as the data's current owner, the people who have accessed the data, and the times at which they did so. Provenance theory has been used by some academics to inform cloud forensics practices. Chain of custody may be guaranteed in cloud forensics with the help of secure provenance, which records who accessed the data, when, and how it was processed and stored. Though there have been several cloud security provenance initiatives [22], [23], to yet no CSP has operationally deployed any of the techniques proposed by these projects.

Trusted Platform Module (TPM): Several scholars have offered a method using Trusted Platform Module (TPM) to protect the data's authenticity and privacy. A number of authors [24, 25] have advocated a TPM for cloud computing as a means of establishing and maintaining confidence in this infrastructure. TPM allows for the authentication and signing of machines as well as the encryption of data in hardware, safe key storage, and the attestation of events. Integrity of the operating virtual instance, trustworthy log files, and trusted deletion of data may all be provided to clients. Dykstra et al. [14] claimed, however, that TPM is not completely secure and that it is feasible to alter a running process without the TPM noticing. In addition, as it is, only few CSPs have TPM, and their hardware is quite diverse. This means that in the future, the CSPs will not be able to guarantee a standardized hardware environment that employs TPM.

Forensic Analysis for Cloud Storage Services: Criminals may hide sensitive materials like those related to terrorism or child pornography in the cloud, and then wipe all local storage devices clean with the help of forensic cloud storage services. There are 32 different cloud computing services, including cloud storage services, that might be used by hackers to either steal data from or tamper with data stored in the cloud. To acquire digital evidence for analysis and examination in a forensic manner to be admissible in court, forensic practitioners and law enforcement agencies face a new challenge as data increasingly resides in cloud storages that are remotely distributed on cloud servers in overseas jurisdictions rather than in local machines. There is information in cloud storage accounts (such as Dropbox, Microsoft SkyDrive, and Google Drive) that is not accessible on user computer which may either access an account through web browser or is synced to an account using the client software, according to research by Quick and Choo [27–30]. The user's computer name, IP address, and the timestamps and dates connected with any changes made to the files stored in his cloud storage account are all examples of identifying information.

6.2 Research Tools and Search Environments

Experts in the area of digital forensic investigation have developed specialized test environments and forensic tools to facilitate the investigation process. Computer forensics makes use of a wide variety of specialized tools, such as Encase and FTK. Some study is needed in the field of cloud forensics to either improve upon already forensics tools or to provide brand new tools specifically designed to fit the needs of cloud forensics. To illustrate, most cloud service models include some type of infrastructure outsourcing, which in turn increases the need for remote analysis and inspection tools. On top of that, digital forensics instruments are required to capture and analyze memory and network dumps. Table 4 summarizes the results of the most popular methods for extracting and analyzing digital evidence.

Table 4: Cyber Forensic Tools

Virtual Forensics Computing [43]	Forensic Image of a suspect is booted
Wireshark [44]	Captures network traffic between VM and the CSP
Microsoft Expression Encoder4 [45]	VM windows video recorder
FTK Imager [46] , EnCase [47]	Memory and disk images acquisition.
Encase Remote Agent [48]	Acquisition of Windows and Linux live system
FROST [48]	Digital forensics tools for the OpenStack cloud platform
Xen Access [49]	Xen VM introspection library (Hypervisor level)

Scientists and researchers need to choose a suitable cloud test environment for their experiment testbed in order to assess the efficacy of the theoretical approaches. Table 5 is a summary of 34 test settings that were utilized to see whether they were suitable for cloud computing projects and cloud forensics situations. In order to accommodate the specific architecture and features of cloud computing, certain settings have been optimized.

Table 5: Test Environments used for Cloud Forensics

Bon Fire [50]	An EU project enables operating a multi-site cloud-based facility on top of different infrastructure

	testbeds such as Emulab
Eucalyptus [51]	A software used to build Amazon Work Station (AWS) private and public cloud
Cloud Sim [52]	A solution to create large-scale cloud computing data center, virtual hosts, and capability of analysis for network traffic
OpenStack [53]	A project used to create various IaaS architectures such as storage, compute and network
Rack space [54]	Based on OpenStack and provides IaaS.

Category	Component addressed in Cloud Forensics	Park et.al [6]	R. Montasari et.al [7]	S. Ali et.al [8]	A. Hosseinian et.al [9]	N. Raza et.al [10]	W. Mahmood et.al [11]	D. Freet et.al [12]	Simou et.al [13]	Zargari et.al [14]	Shahet.al [15]	A. Mishra et.al [16]	Pichan et.al [17]	X. Feng et.al [18]	L. Chen et.al [19]	Poisel et.al [20]
Event Identification	Architectural Support			✓												
	Distributed Evidence					✓										
	Evidence Segregation		✓					✓		✓		✓	✓			
Collection	Access to cloud network devices.							✓			✓					
	Access to Data/ Evidence/Logs on cloud		✓		✓					✓			✓	✓	✓	
	Bandwidth Limitation			✓				✓			✓					✓
	Dependency on CSP		✓			✓			✓			✓				
	Logging	✓					✓							✓		
	Remote Acquisition	✓			✓			✓					✓			
Analysis	Anti-forensics	✓		✓				✓				✓				
	Evidence disappearance /deletion	✓										✓			✓	✓
	Forensic Tools						✓	✓	✓	✓				✓		
	Forensics Enable Services			✓		✓			✓							
	Virtualized environment		✓		✓						✓	✓			✓	
Interpretation	Cloud Forensic Expertise/Internal Staffing	✓				✓		✓			✓					
	Crime scene reconstruction								✓					✓		
	Investigations in virtualized environments	✓					✓					✓				
Presentation and Legal	Multijurisdiction	✓		✓					✓						✓	
	Service Level Agreement (SLA)	✓														
	Chain of Custody							✓								

6.3 Future Scope

The following are open research challenges observed from literature study:

- To analyse some of the cutting-edge methods used in Cloud Forensics taxonomy according to Digital Forensics and Advanced Encryption Algorithm in cybercrimes.
- To effectively execute the framework for data adaptation and distribution. In order to stop further data collection and duplication, provide evidence of content tampering prevention.
- To evaluate the efficiency levels in proposed framework using forensic techniques and tools.

7. Conclusion

With time, the technology cloud changes. There will undoubtedly be additional risks as the cloud develops.

We believe that this is mostly due to increasing domain knowledge and growing cloud use in the IT industry. At each stage of the forensics process, cloud forensics meets difficulties. The detailed literature review included in the research illustrates the shift occurring in cloud forensics towards the use of Advanced Encryption algorithm for evidence provenance. In the study, the three cloud dimensions that have an impact on the forensics procedure are also highlighted. In this study, we provide a fresh taxonomy for cloud forensics that takes into account difficulties, logistics for gathering evidence, analysis, trust, and legal ramifications. Our forthcoming project will focus on creating a framework for gathering evidence utilizing our suggested taxonomy using Cipher test as password for protecting data. We also compared the current frameworks using the suggested taxonomy as metrics. The results of the study make it clear that effective cloud forensics may be facilitated by careful collection of prospective evidence and semi-automated examination of the data. Although trust problems cannot be entirely eliminated, the adoption of a provenance-

based system may provide the confidence element required for the inquiry.

References

[1]. R. M. Blank, "Guide for conducting risk assessments," Citeseer, 2011.

[2]. United Nations Conference on Trade and Development (UNCTAD), "Cybercrime Legislation Worldwide," 2021.

[3]. Right Scale, "state-of-the-cloud-report," 2019.

[4]. International Data Corporation (IDC), "Worldwide Public Cloud Services revenue," 2021.

[5]. National Crime Records Bureau India (NCRB), "Crime in india 2020," 2020.

[6]. Park, Jun-Hak, Sang-Ho Na, Jun-Young Park, Eui-Nam Huh, Chul-Woo Lee, and Hyoung-Chun Kim, "A Study on Cloud Forensics and Challenges in SaaS Application Environment," in 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/Smart City/DSS), IEEE, 2016.

[7]. R. Montasari, "An Overview of Cloud Forensics Strategy: Capabilities, Challenges, and Opportunities," in Strategic Engineering for Cloud Computing and Big Data Analytics, Cham, Springer International Publishing, 2017, pp. 189-205.

[8]. S. Ali, S. Memon and F. Sahito, "Challenges and Solutions in Cloud Forensics," in Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing - ICCBDC'18, 2018.

[9]. A. Hosseinian, "Challenges of Cloud Forensics." Enterprise Security: Second International Workshop," in Revised Selected Papers, vol. 10131, Vancouver, BC: Springer, 2015.

[10]. N. Raza, "Challenges to network forensics in cloud computing," in 2015 Conference on Information Assurance and Cyber Security (CIACS), 2015.

[11]. W. Mahmood, H. Jahankhani and A. Ozkaya, "Cloud Forensics Challenges Faced by Forensic Investigators," in Communications in Computer and Information Science, Cham, Springer International Publishing, 2015, pp. 74-82.

[12]. D. Freet, R. Agrawal, S. John and J. Walker, "Cloud forensics challenges from a service model standpoint," in Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital Eco Systems - MEDES '15, 2015.

[13]. Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S, "Cloud forensics: identifying the major issues and challenges," in International conference on advanced information systems engineering, Springer, 2014.

[14]. Zargari, Shahrzad, and David Benford "Cloud forensics: Concepts, issues, and challenges," in 2012 Third International Conference on Emerging Intelligent Data and Web Technologies, Bucharest, 2012.

[15]. Shah, J. J., and Latesh G. Malik, "Cloud forensics: issues and challenges," in 2013 6th International Conference on Emerging Trends in Engineering and Technology, 2013.

[16]. A. Mishra, P. Matta, E. Pilli and R. Joshi, "Cloud Forensics: State-of-the-Art and Research Challenges," in 2012 International Symposium on Cloud and Services Computing, IEEE, 2012.

[17]. Pichan, Ameer, Mihai Lazarescu, and Sie Teng Soh, "Towards a practical cloud forensics logging framework," Journal of information security and applications, vol. 42, pp. 18--28, 2018.

[18]. X. Feng and Y. Zhao, "Digital Forensics Challenges to Big Data in the Cloud," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (Green Com) and IEEE Cyber, Physical and Social Computing (CPS Com) and IEEE Smart Data (Smart Data), IEEE, 2017.

[19]. L. Chen, L. Xu, X. Yuan and N. Shashidhar, "Digital forensics in social networks and the cloud: Process, approaches, methods, tools, and challenges," in 2015 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2015.

[20]. Poisel, Rainer, and Simon Tjoa, "Discussion on the challenges and opportunities of cloud forensics," in International Conference on Availability, Reliability, and Security, 2012

[21]. Pichan, Ameer, Mihai Lazarescu, and Sie Teng Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," Digital investigation, vol. 13, pp. 38--57, 2015.

[22]. S. Khan, "Cloud log forensics: Foundations, state of the art, and future directions," " ACM Computing Surveys (CSUR), vol. 49, p. 1–42, 2016.

[23]. D. Gonzales, J. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," IEEE Transactions on Cloud Computing, vol. 5, pp. 523-536, 2015.

[24]. C. Federici, "Alma Nebula: A Computer Forensics Framework for the Cloud," Procedia Computer Science, vol. 19, pp. 139-146, 2013.

[25]. Zawoad, Shams, Amit Kumar Dutta, and Ragib Hasan., "forensics, Sec LaaS: secure logging-as-a-service for cloud," in Proceedings of the 8th ACM

SIGSAC symposium on Information, computer and communications security, 2013.

[26]. S. Zawoad, A. Dutta and R. Hasan, "Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service," IEEE Transactions on Dependable and Secure Computing, vol. 13, pp. 148-162, 2015.

[27]. Povar, Digambar, and G. Geetha kumari, "A heuristic model for performing digital forensics in cloud computing environment," in International Symposium on Security in Computing and Communication, 2014

[28]. M. Ahsan, M. Ahsan, A. Wahab, M. Idris, S. Khan, E. Bachura and K.-K. R. Choo, "CLASS: Cloud Log Assuring Soundness and Secrecy Scheme for Cloud Forensics," IEEE Transactions on Sustainable Computing, pp. 1-1, 2016

[29]. Kumar Raju, B. K. S. P., and G. Geetha kumari, "Event correlation in cloud: a forensic perspective," Computing, vol. 98, no. 11, pp. 1203--1224, 2016.

[30]. S. Almulla, Y. Iraqi and A. Jones, "A Distributed Snapshot Framework for Digital Forensics Evidence Extraction and Event Reconstruction from Cloud Environment," in 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, vol. 1, IEEE, 2013.

[31]. S. S. Sampana, "Force (Forensic recovery of cloud evidence): A digital cloud forensics framework," in 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019

[32]. J. James and P. Gladyshev, "Challenges with automation in digital forensic investigations," 2013.

[33]. E. Hemdan, D. El-Din and Manjaiah, in CFIM: Toward Building New Cloud Forensics Investigation Model." Innovations in Electronics and Communication Engineering, Singapore, Springer, 2018, p. 545–554.

[34]. S. Zawoad and R. Hasan, "Chronos: Towards Securing System Time in the Cloud for Reliable Forensics Investigation," in 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), vol. 1, IEEE, 2016.

[35]. Zhang, Wei-Zhe, Hu-Cheng Xie, and Ching-Hsien Hsu., "Automatic Memory Control of Multiple Virtual Machines on a Consolidated Server," IEEE Transactions on Cloud Computing, vol. 5, pp. 2-14, 2015.

[36]. Roussev, Vassil, Irfan Ahmed, Andres Barreto, Shane McCulley, and Vivek Shanmughan, "Cloud forensics--Tool development studies & future outlook," Digital investigation, vol. 18, pp. 79--95, 2016.

[37]. Rani, Deevi Radha, and G. Geetha Kumari, "A framework for detecting antiforensics in cloud environment," in 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016.

[38]. Alex, M. Edington and R. Kishore, "Forensics framework for cloud computing," Computers & Electrical Engineering, vol. 60, p. 193–205, 2017

[39]. Ruan, Keyun, Joe Carthy, Tahar Kechadi, and Ibrahim Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results," Digital Investigation, vol. 10, no. 1, pp. 34--43, 2013.

[40]. Uph off, Maximilian, Matthäus Wander, Torben Weis, and Marian Waltereit, "Secure Cloud: an encrypted, scalable storage for cloud forensics," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (Trust Com/Big Data SE), IEEE, 2018, pp. 1934--1941.

[41]. Rani, Deevi Radha, and G. Geetha Kumari, "A framework for detecting antiforensics in cloud environment," in 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016.

[42]. Raju, Bksp Kumar, and G. Geetha kumari, "A novel approach for incident response in cloud using forensics," in Proceedings of the 7th ACM India Computing Conference, 2014.

[43]. GetData, Virtual Forensics Computing, (https://www.virtualforensiccomputing.com/), [Accessed 30 June, 2015].

[44]. Wireshark, (https://www.wireshark.org/), [Acce ss ed 30 June, 2015].

[45]. Microsoft, Microsoft Expression Encoder4., (http://www.microsoft.com/en-us/ download/details.aspx?id=18974), [Accessed 30 June, 2015].

[46]. FTK. Forensics tool kit (FTK) computer forensics software, (http://accessdata.com/ solutions/digital-forensics/forensic-toolkit-ftk), [Accessed 30 June, 2015].

[47]. En Case,. Guidance Software. (https://www.guidancesoftware.com/ products/Pages/encase-forensic/overview.aspx), [Accessed 30 June, 2015].

[48]. Dykstra, J., & Sherman, A, "Design and implementation of FROST: digital forensic tools for the OpenStack cloud computing platform", Digital Investigation, Vol.10, Page: 87-95, 2013.

[49]. Xen Acess Library. (http://code.google.com/ p/xenaccess/), [Accessed 30 June, 2015]

[50]. Bon Fire, Bon Fire. (http://www.bonfire-project .eu /services), [Accessed 30 June, 2015].
[51]. Eucalyptus, HP Helion Eucalyptus, (https:// www.eucalyptus.com/),[Accessed 30 June, 2015]
[52]. Cloud Sim, The Cloud Computing and Distributed Systems (CLOUDS) Laboratory, University of Melbourne, (http://www.cloudbus.org/cloudsim/), [Accessed 30 June 2015].
[53]. OpenStack, (https://www.openstack.org/), [Accessed 30 June, 2015]
[54]. Rack space, (http://www.rackspace.com/), [Accessed 30 June, 2015]