ISSN:0975-9646
Ashwani kumar yadav / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 13 (6) , 2022, 115-123

Cloud Forensic as a Service: Tools, Challenges, and Opportunities

Ashwani kumar yadav [#1], Shri Prakash Dwivedi [*2]

[1]Department of Information Technology
G. B. Pant University of Agriculture and Technology
Pantnagar, India

[2]Department of Information Technology
G. B. Pant University of Agriculture and Technology
Pantnagar, India

***Abstract*— Cloud computing is rapid provisioning of services using virtualization technology. The evolving nature of cloud computing has attracted both academia and industry. With increased adoption of cloud computing model attackers target the cloud resources. The vulnerability of Cloud computing services has also increased, further resulting in an exponential increase in cyber-attacks. Digital crimes committed in the cloud are called cloud crimes. Multi-tenancy and distributed nature of the cloud computing environment complicate the forensics data, proof, and evidence collection compared with traditional digital forensics. In cloud Forensics the investigator is connected to many suspicious cloud resources, whether under his control or not, which may sometimes lead to privacy issues for cloud users. Significant changes are required to accept currently established forensic procedures and process models in a cloud environment. This paper describes the advancing field of forensics as a cloud service; various tools used currently, the steps involved in forensic investigation, and bring to light its challenges and opportunities in the cloud computing environment.**

***Keywords*—Cloud crime (CC) · Cloud forensics (CF) · Cloud Service Provider (CSP) · Virtualization · Forensics as a Service (FaaS)**

I. INTRODUCTION

Cloud computing environment has encountered a tremendous growth in the variety, volume and velocity of data. With frequent shift of computing services to cloud computing environment, cloud repositories have became target of cyber attackers. The recent cyber-attacks on cloud repositories have also revealed enormous public and social security losses. In addition to the advanced security measures taken by cloud service providers, they are exploited by criminals. With the tremendous growth of cloud computing services used on a daily basis by various organizations, the demand for forensic investigations is increasing and the research problems in this field are expanding. Digital forensics is preliminary collection of data followed by evidence auditing, analyzing, and documenting it digitally. Digital evidence is collected from digital devices such as Smart phones, desktops, laptops, hard drives, digital cameras, and other storage devices without any modification, therefore, protecting the data integrity [1]. Forensic analysis is a challenging job due to the growing migration toward highly distributed cloud infrastructure.

Forensic investigations in the cloud must analyze the data flow, which can be related to client devices, i.e., stored data; so static and dynamic analysis can be performed to find the right reason for the loss of data integrity. Forensic analysis must ensure whether the data has been modified or the credentials used to modify the data are available. If the data has been modified, the identity of the changed data must be known, to ensure that any lost data could be reverted. Forensic analysis must also consider that a crime happened in the cloud might not have data in required format. This makes useful digital evidence collection difficult. In such cases, application layer or the operating system needs to first decrypt it, so empirical and thorough research is necessary to get the expected result. Even if the data is lost, the lost data must be recovered from client side and the cloud server.

This paper is organized as follows: Section II contains cloud computing models. Section III introduces cloud forensics as a service. Section IV provides an outline of existing cloud forensics tools. Section V contains the stages in cloud forensics process. Sections VI and VII address the challenges and opportunities. Section VII Conclusion.

II. CLOUD COMPUTING MODELS

Depending on the needs of the clients the cloud services architecture defines services to be offered by CSPs.

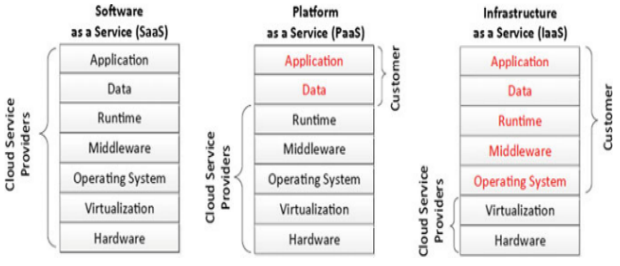

Fig. 1 General Service Models Offered by the Cloud

These services are categorized as follows:

A. Software as a service

SaaS model is the provisioning of software applications in cloud computing environment. Multiple users can assess the instances of the applications hosted by varied CSPs anywhere on the globe. All the layers in this model are owned by the CSPs. The customer only indirectly controls the underlying operation in the infrastructure. This is a cost effective model as the client needs to pay only for operations she perform on the cloud infrastructure, thus, reducing maintenance cost. From the eyes of a forensic analyst, this model is considered a forensic goldmine. Almost all SaaS programs record all events and keep extensive logs. Every detail is critical in a forensic investigation, from user logs to timestamps.

Common examples are Microsoft 365, Citrix, Google Docs, etc.

B. Platform as a Service

PaaS model is the provisioning of platform that allows users to deploy their own applications by means of software components embedded in middleware. This is cost effective model as it provides a rapid development, deployment, and testing of customer-deployed applications. At the application level, the customer has full control. As part of forensic analysis, this model provides vital information when the client performs substantial logging in order to aid the investigation process.

Apprenda, Heroku, and Google App Engine are examples of the PaaS model.

C. Infrastructure as a Service

IaaS model is the provisioning of the complete cloud computing infrastructure including physical/virtual machines, network components, firewalls, etc. In this model CSPs manage the entire IT ecosystem setup, by directly responding to customer requests. Basically, users outsource entire IT ecosystems. This model creates snapshots of a virtual machine's physical memory and disks in case forensic investigation is required.

Common examples are Amazon Web Services (AWS), Google Computer Engine, and Microsoft Azure

III. CLOUD FORENSICS AS A SERVICE

The rapid adoption of cloud computing by businesses and governments has been due to the reduced IT cost. The global nature of cloud computing allows CSPs to maintain data centers all around the world. The CSPs in cloud computing architecture ensures availability of services to customers across the globe by maintaining its data centers. Cloud computing can be defined as a shared collection of configurable, interconnected resources (storage, applications, services, servers, networks, etc.). These resources can be quickly reconfigured with minimal effort [8].

Traditionally, Computer forensics was conducted over the standalone devices that were collected from the attacker's location. Cloud forensics considers the outcomes of Digital forensics, traditional computer forensics and the network forensics. With application of digital forensics principles of computer science are implemented to recover electronic evidence. Network forensics is related to investigation of data in flow i.e., forensic investigation of networks [7]. It is the study of data in motion with a focus on obtaining evidence that would be presented later in court. The architecture of CC is based on pervasive network access. Therefore, follows the implementation of network forensics using techniques tailored by cloud computing architecture.

Cloud forensics investigation requires the interaction between the client and the CSP's, both being participants in forensic analysis. Forensic investigation must also consider that it does not hamper the resource sharing across multiple tenants, and work in accordance with international law enforcement agencies. In order to reduce the risk of failure the CSP's store the multiple copies of data in different geographic locations. Implementing FaaS obliges the parties to have some forensic responsibilities. The service model for FaaS considers the division of duties between clients and the CSPs. Similarly, interactions among multiple tenants sharing the same resources depend on cloud model.

To provide a more comprehensive analysis of the cloud forensics domain the technical, organizational, and legal dimensions of cloud forensics have been described.

A. *Technical Dimension*

This dimension includes the tools and procedures necessary to carry out forensic processes. Cloud Forensic analysis involves data collection from CSPs and cloud clients. The technical dimension of cloud forensic emphasis on identifying, labeling evidence segregation, recording and collecting data for further analysis. It works in virtualized environments wherein data might be residing in provider infrastructure. The tools and the procedures used to collect data depend on applicable data responsibility. Live forensics is carried out using the cloud environment therefore, preventative measures are must. It must adhere to the laws or regulations of the jurisdiction and maintain the confidentiality of resources that are being shared. A public cloud may require tenant isolation in a provider-side artefact, while a private cloud may not have such need. Some of the characteristic categorized under technical dimension are as follows:

1) Virtualization and hypervisor investigation:

A key technology for implementing cloud services is virtualization. Virtual machines are implemented in cloud using hypervisor technology that is similar to kernel in an operating system. In order to carry on investigation in a virtualized environment, there exists a need to develop forensic tools that could investigate the hypervisor. In spite of all the operations in cloud are virtualized, investigations

typically need for the retrieval of evidence from physical sites. Hypervisor probe methods are virtually inexistent resulting in cloud security breach i.e., the loss of data control [3].

2) Rapid elasticity and live forensics

One of cloud computing main attributes is rapid elasticity. With rapid elasticity, it is possible to provision and de-provision computation and storage resources in the cloud as and when needed, therefore cloud investigation tools must also be flexible.

3) Resource pooling

Resource pooling is a technique used by the cloud service provider to manage the multitenant cloud environment. In it, the CSPs aggregate the cloud resources that are provisioned to the client without their control and knowledge of the process involved. A multi-tenant environment reduces IT costs by resource sharing. However, compartmentalization is required in the cloud to separate evidence [3]. Tools for cloud forensics must be designed considering data integrity of the multitenant environment.

4) Lack of data control

The lack of data control is another challenge. Forensic tools can use specific time stamps for physically locating forensic data. Jurisdictional issues should also be considered. Proactive measures greatly facilitate forensic investigations in the cloud. Object level auditing, tracking of access control and gathering snapshots of periodic storage are some of the suggestions to be implemented in designing tools for forensic investigation

B. *Organizational Dimension*

In a cloud forensics environment at least two parties are involved in the organizational dimension: the customer and the CSP. With rapid evolution of cloud computing the CSPs have to provision the services depending on the ever increasing demands of the client. This leads to CSPs outsourcing their services. Many cloud applications have dependencies on multiple CSPs. These dependencies in the CSP and customer chain can be very dynamic and therefore widen the scope of forensic investigation. In such situations, investigating each link in the chain is must for cloud forensic investigations. The scenario presented can create a serious problem if there is no proper coordination of responsibilities among the parties involved, or there is some corrupt link in the chain.

The organization dimension focus on building proper organization policies and updating of SLAs in order to facilitate communication and collaboration around forensic activities. CSPs can take help of academia that can suggest for amendments in SLAs and provide technical expertise to improve the investigation process. Cloud entities must make available internal and external support to establish cloud forensics capabilities that carry out the following roles:

1) Incident Handlers

They handle security incidents such as illegal data access, fortuitous data leaks and losses, violation in tenant confidentiality, improper system usage, insider attacks, malicious system infection, and DOS attacks. The cloud entities must consider the categorization of various security incidents according to cloud layers and hire team of incident handlers having required expertise.

2) Investigators

Investigators are responsible for cooperating with outside law enforcement while investigating misconduct allegations. The cloud entities must have sufficient expertise to conduct probe of its own assets and to collaborate with other entities during forensic investigations.

3) IT Professionals

IT Professionals include an umbrella of organizational entities that is, cloud security architects, security administrators, system hackers, network, engineering and support staff [11]. These entities helps investigator in access crime scenes and provide expertise to collect data on behalf of investigators.

4) Legal Advisors

They are aware of multi-tenancy and multi jurisdictional problems in the cloud. Forensic activities must not violate laws and regulations and should protect the privacy of other clients sharing resources. The SLA should make clear the steps to be followed in the forensic investigation. The SLA document drafting must involve an in-house counsel of legal advisors covering all the CSP's jurisdictions. Legal advisors also hold the responsibility of communicating and cooperating with external law enforcement agencies.

5) External Assistance

The involvement of external entities is important as the services provision multi tenant demanding resources from multiple CSPs. It is sagacious for cloud entities to depend on external parties to perform forensic investigation. Therefore it is a necessity for CSPs to have pre-determined actions to be taken from external parties. The guidelines, relevant policies, contracts and agreements must be clear to law enforcement agencies.

C. *Legal Dimension*

Conventional forensic professionals recognize the challenges of multiple jurisdictions and multiple tenancies as their top legal concerns. In order to make it clear that forensic activities do not violate the laws and regulations of the jurisdiction in which the data reside, the legal aspect of cloud forensics

requires the development of regulations and agreements. Additionally, confidentiality must be preserved for other tenants using the same infrastructure. The SLA document must include the following terms related to forensic investigation:

1) The course of action of conducting investigations in a multi-jurisdictional environment without violating privacy policies, applicable laws, client confidentiality, and regulations.
2) The technologies supported, the services provisioned, and the access granted to clients during forensic investigations by CSP;
3) Roles and responsibilities, and trust boundaries between CSP and Client in relation to forensic investigations.

IV. AN OUTLINE OF THE EXISTING TOOLS USED IN CLOUD FORENSIC

Currently, the majority of cloud service providers supply their clients with specific forensic tools that they can be utilized to do cloud forensic investigations. Digital forensics limitations can be defined in the areas of legal aspects, data volume, tool capacity, automation, and visualization of forensic analysis. These existing limitations make it even more essential for new cloud forensics tools to be designed.

TABLE I
VARIOUS FORENSIC TOOLS USED DURING INVESTIGATIONS

S.No	Tool name	Application
1.	Digital forensics frameworks (DFF)	A popular digital-only platform that is easily handled by both non-professionals and professionals. It can also be used to recover hidden and deleted files. It's open source with GPL license.
2.	Open computer forensics architecture (OCFA)	This tool is freely available and implements using PostgreSQL database. It has a custom content addressable storage. It is also used to store data, and runs on the Linux platform.
3.	CAINE	Using this tool is convenient for integrating software modules from existing software tools that run in a user-friendly way. The computer-aided investigative environment is an open source
4.	X-Ways forensics	This tool is used in various dimensions such as cloning, disk imaging, bulk hash calculations, and even supports maximum existing file formats. The digital reviewers see it as an advanced stand. It can run on almost every version of Windows.
5.	SIFT	It is a versatile forensic operating system that has all the tools needed for use in digital forensic processes with an integrated platform on top of Ubuntu.
6.	EnCase	It is a paid tool. This tool has a multi-purpose forensic platform that collects information very quickly from various devices and also creates report-based evidence.
7.	Registry recon	This tool is known for its registry analysis, which can be used to gather registry information from evidence, rebuild the registry, and recover the registry of both previous and current Windows. This is a paid tool,
8.	Sleuth Kit (+Autopsy)	There are many tools used for disk image analysis and detailed file system analysis. This is a Windows and Unix-based forensic analysis tool [13].
9.	Libforensics	It consists of various libraries required for digital forensics applications. In Libforensics various demo tools are available for extracting information from different types of evidence. This tool is developed by Python.
10.	Volatility	This tool is a memory-based forensic framework [25]. It is used for malware analysis, This tool helps extract information from running processes and can also extract information from Windows crashes.

11.	WindowsSCOPE	This tool can be used to analyze virtual and physical memory and Windows kernel drivers [14].It works as a reverse engineering tool and can also be used for volatile memory analysis.
12.	Corner's toolkit	This tool is used to retrieve data from Unix-based device operating systems.
13.	Oxygen forensic Suite	One may extract information from a mobile device using this tool, as well as recover calendar data, call logs, contacts, messages, and deleted messages. The results produced by this tool are also quite simple to analyze.
14.	Bulk extractor	This utility is useful for scanning disc images and extracting important information from files because it does not adhere to any file system structure while extracting data from files.
15.	Xplico	This open-source tool for forensic investigation may extract data from apps that use network and Internet protocols. It supports various protocols, including TCP, UDP, SIP, HTTP, IMAP, as well as both IP6 and IP4, and SQLite databases are used to store the output.
16.	Mandiant Redline	When a process is active on the host, it gathers data for file and memory analysis. Metadata, registry information, and Internet history are also useful when creating reports.
17.	COFEE	Computer forensics professionals use this toolkit. This toolkit was developed by Microsoft to collect evidence within Windows systems [23]. It is very fast, finishing the analysis in less than 20 minutes, so it can be installed on your system using an external hard drive or USB stick.
18.	P2eXplorer	It is an image mounting tool and the images are mounted to hard drive and analyzed by File Explorer. More photos can be mounted here in a short time.
19.	PlainSight	The Linux distribution is a CD-based Knoppix useful for collecting Internet history information, extracting password hashes, checking Windows firewalls, creating data, and checking USB device usage.
20.	XRY	Developed by Micro Systemation, it will help to recover important scan data from mobile phones. This tool is a combination of hardware and software.
21.	HELIX3	It is a fully virtual and incident responsive CD-based forensics suite. It also includes a hex editor tool for password cracking, record carving, and is available as a free version.
22.	Cellebrite UFED	Collecting mobile data information with excessive accuracy can be very useful, and using this device can also help extract mobile data; UFED field series design is done in a way that unifies the workflow between the lab and the field.

23.	FTK imager	This tool is used for evaluating folders and documents which can be stored on network drives, DVD / CD, hard drives. It is also useful for developing MD5 or SHA1 hash files and you can also get deleted documents from the Recycle Bin as well.
24.	DEFT	This tool is useful for hashing, data retrieval, community forensic analysis, and cellular forensic analysis. It is a Linux-based CD with no. of free open source and forensic tools;
25.	Cloud Bulk extractor	This tool is useful for scanning folders, disk images, email address, credit card number, numerous ZIP files and URLs.

V. STEPS TO BE CARRIED OUT FOR CLOUD FORENSICS PROCESS

The following steps are incorporated in a cloud forensic process.

A. *Incident Confirmation*

This is the main level of investigation. In this level, the incident is confirmed via intrusion detection alarms and the snapshots collected. Through these means, it could be confirmed that the incident has occurred.

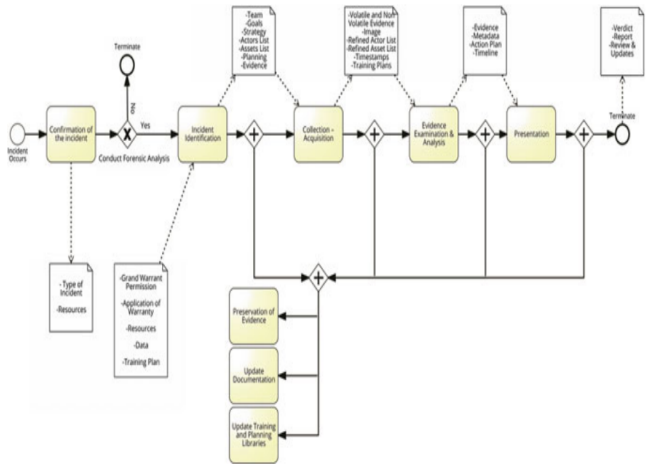

Fig. 2 Process of Investigating Cloud Forensic

B. *Incident-identification*

Incident identification is second step after confirmation of the happening of the incident, it's far vital to affirm the identification of the incident [4], i.e., the way it was executed, what changed into the loss, to what extend the client will get affected by the loss.

C. *Collection–Acquisition*

Direct or indirect clues need to be gathered properly, as the lead the forensic investigation post the occurrence of crime; it's far recommended to be speedy on the way to accumulate the records, and there are probably possibilities in which an outsider can also sometimes forcefully attempt deleting the clues.

D. *Examination–Analysis*

Amassed records examination need to be executed either through the usage of the predefined methods or the brand new methods, whichever is probably the aspect however the evaluation needs to be executed in an accurate manner on the way to get the appropriate results.

E. *Presentation*

When all the vital facts associated with the investigation are collected, it need to be supplied in a nice manner, because the clues or facts that is amassed is associated with methodological aware group and it needs to be defined to the people that aren't conscious about the technical concepts. It needs to be give an explanation that could be presented in courtroom; method, concepts which are being used, in order that the people that are associated with it need to get a entire picture of the aspect of crime and that they get insight of the idea of the cloud crime, and the way it had been committed.

F. *Handling Concurrent Activities*

Evidence collected is maintained and investigation-related documentation is updated concurrently with the investigation process, thus updating training and planning libraries.

VI. CHALLENGES

This section describes his eight challenges in building cloud forensics capabilities, covering technical, organizational, and legal aspects.

A. *Data Collection*

In order to use information for forensic analysis, inquiry, or review, it must be legally possible to gather it from a device or cloud-based source and image it. The cloud service and delivery models are responsible for deciding the way to get the forensics data. [1]. Infrastructure as a Service (IaaS) customers provides an unlimited access to data for use in forensics. Software-as-a-Service (SaaS) customers provide no access or in some cases limited access to data.

With the denial of access to data for forensics and geographically diverse location it is not feasible to have right investigation. CSP's follow the service model which provide customer abstract information about location. They hide location data for easy movement of service data and manage

its replication for handling robustness of the services provided. The forensic investigator also need access to CSP's Client access logs. In case of IaaS, she also needs details of virtual machines and up-to data disk images. Presently, SLA's have not been updated to facilitate cloud forensic which presents a limitation to cloud customers to self monitor them with meta data and log files.

B. *Virtualized Environments*

Virtualization is the backbone of Cloud computing. CSP's provide services through virtualization, running multiple instances of virtual machines which are controlled by a hypervisor. Hypervisor is equivalent to kernel in operation system. The limitation to forensic investigation is posed with increasing number of attacks on hypervisors. This problem is intensified with the fact that there exists a lack of established procedure, policy, technique for investigation of hypervisors [1].

Another big problem in this aspect mirroring of data across geographically diverse locations and confusion created to forensics investigator leading to seize of machines in which jurisdiction is applicable. This led to violation of laws, and regulations by forensic investigator. With distributive nature of cloud computing forensic investigation need a strong international cooperation, especially when the cloud resources to be seized are all over the world.

C. *Segregation*

In the cloud, segregation of data is a challenge. The users on the cloud are isolated from each other with use of virtualization. A cloud user has no access to raw disk device. The technology of provisioning and de-provisioning of cloud resources has improved. The major challenge with the CSP's as well as the law enforcement agencies is that the investigating should not violate the confidentiality of other tenants using the cloud services [3].

Another issue is that the user-friendly features of the cloud model contribute to a weak registration system. This promotes anonymity, making it easier for criminals to disguise their identities. CSP's encrypts sensitive that that is being uploaded. In absence of this feature user should first encrypt the data before uploading it to cloud so as to minimize its vulnerability to attack. SLA's must be updated to provide chain of separation and the cryptographic system used should be formalized in contract.

D. *Trained internal staff*

Another major challenge is posed due to lack of trained staff having technical and legal know how to work in changing nature of forensics. The current forensic research is far behind the evolving cloud computing environment. The forensic investigation staff must have appropriate expertise to work in cloud environment rather than using conventional forensic procedures and tools.

E. *Elastic Forensics*

The increase in IOT and mobile end devices connectivity to cloud, it presents challenges to evidence gathering and discovery of data. The crime committed has proliferated impact that makes investigation workload to be overwhelmingly high. Precise time synchronization is required to create a timeline of events. Since the data ids residing in different geographic locations on multiple physical machines it may be exchanged between cloud infrastructures and end points. Its Synchronizing time is complicated in the cloud by the sheer volume of data logs and the proliferation of proprietary log formats.

F. *External Dependencies and identification of chain*

Any forensic investigation in the cloud should examine every link in the dependency chain. There are virtually no procedures, policies, and agreements associated with multi-vendor forensic investigations. In multi vendor model the CSP's get request from other CSP's for availability of services. For example a CSP providing vide call facility may need IaaS from other CSP for hosting log files. In this case they rely on other cloud for services. This presents a challenge to forensic investigation.

G. *Updated SLA Document*

The field of cloud forensics meets another challenge as present SLAs lacks in giving details of forensic investigations. Most cloud users are unaware of the potential issues and their significance during cloud forensic investigations. CSPs are generally reluctant to increase transparency due to a lack of expertise on technical and legal issues and a lack of regulations requiring increased transparency. It may be because of low customer awareness, limited CSP transparency, and lack of international regulation.

H. *Multi Tenancy and jurisdiction challenge*

The multi-jurisdictional nature and multi-tenancy presents significant challenges to forensic investigations. The storage, acceptability, Chain of Evidence and Control, lack of a global regulatory body impacts the cloud forensic investigations.

VII. OPPORTUNITIES

With advances in cloud computing environment the forensic investigation faces many challenges. With these challenges there are also new opportunities that must be explored so as to advance forensic investigation.

A. *Cost Effectiveness*

Security and Forensics Services are cost-effective when implemented on a large scale. Cloud computing is attractive to small businesses because it reduces IT costs. Organizations

without dedicated in-house or external forensics capabilities may benefit from cost-effective cloud forensics services.

B. *Data Abundance*

Amazon S3 and Amazon Simple DB Ensure object durability by storing objects multiple times across multiple Availability Zones when they are on initial write. The object is then further replicated to reduce the risk of device unavailability or bit rot failure [1]. This duplication also reduces the chances of critical evidence being permanently erased.

C. *Scalability and Flexibility*

Cloud computing scalable and flexible resource usage, also applies to forensic services. Pay as you go model of cloud computing provides the systematized working of forensics without sacrificing performance [27]. Scalability in cloud provides log indexing searching and querying in an efficient manner.

D. *Overall Robustness*

Some technologies can help improve the overall robustness of cloud forensics. [1]. The IaaS offering supports on-demand cloning of virtual machines. As a result, if a security breach is suspected, customers can image live virtual machines for offline forensic analysis, reducing downtime. Also, using multiple image clones allows you to parallelize your investigation tasks for faster analysis. This will improve security's analysis of incidents and increase the likelihood of tracking down attackers and patching vulnerabilities. For example, Amazon S3 uses versioning to allow customers to retain, retrieve, and restore any version of any object stored in an S3 bucket [1]. This provides a wealth of information to help investigate anomalies and incidents.

VIII. CONCLUSION

Cloud computing pushes the boundary of digital forensics. Implementation of forensics in cloud computing environment has brought many challenges and opportunities. These are categorized as technical, organizational, and legal challenges. Some of these challenges are specific to cloud forensics. However, cloud forensics offers a unique opportunity to improve the effectiveness and speed of forensics investigations greatly. Available digital forensics tools can help in investigations, but their scope is limited to desktops, laptops, smart phones, or smart devices of any kind. These tools give results, but they are not at a satisfactory level. Dedicated cloud-based forensic tools can be used to improve forensic investigations and achieve positive results. The data under investigation is fragile. The data is in changed format and requires investigators to conduct investigations of data located on remote servers rather than at crime scenes and to access such types of data on remote servers that contains data of other clients, violating privacy and possibly leading to modification of existing data, breaking the concept of data integrity. In our paper, we have reviewed various digital forensic tools and studied their viability to be used in cloud forensics. There exists a necessity to have a specific tool that is dedicated to cloud computing environment to carry out forensic investigations.

REFERENCES

[1] Amazon, AWS Security Center, Seattle, Washington (aws.amazon .com/security).

[2] N. Beebe, Digital forensic research: The good, the bad and the unaddressed, in Advances in Digital Forensics V, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 17–36, 2009.

[3] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, San Francisco, California (www .cloudsecurityalliance.org/csaguide.pdf), 2009.

[4] Henry, P., et al.: The SANS survey of digital forensics and incident response. Technical report, SANS (July 2013)

[5] EurActiv, Cloud computing: A legal maze for Europe, Brussels, Belgium (www.euractiv.com/en/innovation/cloud-computinglegal-maze-europe-linksdossier-502073), 2011. 46 ADVANCES IN DIGITAL FORENSICS VII

[6] European Network and Information Security Agency, Cloud Computing: Benefits, Risks and Recommendations for Information Security, Heraklion, Crete, Greece (www.enisa.europa.eu/act/rm/files /deliverables/cloud-computing-risk-assessment), 2009

[7] K. Kent, S. Chevalier, T. Grance and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.

[8] P. Mell and T. Grance, The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 (Draft), National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.

[9] M. Meyers and M. Rogers, Computer forensics: The need for standardization and certification, International Journal of Digital Evidence, vol. 3(2), 2004.

[10] J. Oberheide, E. Cooke and F. Jahanian, CloudAV: N-version antivirus in the network cloud, Proceedings of the Seventeenth USENIX Security Conference, pp. 91–106, 2008.

[11] R. Perry, E. Hatcher, R. Mahowald and S. Hendrick, Force.com cloud platform drives huge time to market and cost savings, IDC White Paper, International Data Corporation, Framingham, Massachusetts (thecloud.appirio.com/rs/appirio/images/IDC Force.com ROI Study.pdf), 2009.

[12] V. Roussev, L. Wang, G. Richard and L. Marziale, A cloud computing platform for large-scale forensic computing, in Advances in Digital Forensics V, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 201–214, 2009.

[13] Ting, Y.-H., et al.: Design and implementation of a cloud digital forensic laboratory. In: Symposium on Cryptography and Information Security (2013)

[14] Roussev, V., Ahmed, I., Barreto, A., McCulley, S., Shanmughan, V.: Cloud forensics–tool development studies and future outlook. Digital Investigation. 18, 79–95 (2016)

[15] Ashwani Kumar Yadav and Hardwari Lal Mandori," Study of Task Scheduling Algorithms in the Cloud Computing Environment: A Review" International Journal of Computer Science and Information Technologies, Vol. 8 (4) , pp.462-468, 2017

[16] R. Broadhurst, Developments in the global law enforcement of cyber crime, Policing: International Journal of Police Strategies and Management, vol. 29(2), pp. 408–433, 2006.

[17] Federal Bureau of Investigation, Regional Computer Forensics Laboratory, Annual Report for Fiscal Year 2007, Washington, DC (www .rcfl.gov/downloads/documents/RCFL Nat Annual07.pdf), 2007.

[18] S. Liles, M. Rogers and M. Hoebich, A survey of the legal issues facing digital forensic experts, in Advances in Digital Forensics V, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 267–276, 2009.

[19] F. Gens, IT cloud services forecast – 2008 to 2012: A key driver of new growth (blogs.idc.com/ie/?p=224), October 8, 2008.
[20] Dedicated Server, Managed Hosting, Web Hosting by Rackspace Hosting. http://www.racksp ace.com
[21] Mishra, A.K., et al.: Cloud forensics: state-of-the-art and research challenges. In: International Symposium on Cloud and Services Computing (2012)
[22] Mohiddin, S.K., Yalavarthi, S.B., Sharmila, S.: A complete ontological survey of cloud forensic in the area of cloud computing. In: Deep, K., et al. (eds.) Proceedings of Sixth International Conference on Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing, vol. 547. Springer, Singapore (2017)
[23] Microsoft: NW3C-Microsoft COFEE (2014). https://cofee.nw3c.org
[24] Mitrokotsa, A., et al.: Intrusion detection in MANET using classification algorithms: the effects of cost and model selection. Ad Hoc Netw. 11(1), 226–237 (2013). ISSN: 15708705. https://d oi.org/10.1013/j.adhoc.2012.05.006
[25] Volatility: Volatility Introduction—volatility—Introduction to volatility—An advanced memory forensics framework (2014)
[26] Slay, J., et al.: Advances in Digital Forensics V, Volume 306 of IFIP Advances in Information and Communication Technology, pp. 37–47. Springer, Berlin, Heidelberg (2009)
[27] Al Fahdi, M., et al.: Challenges of digital forensic—a survey of researchers and practitioners attitudes and opinions. In: Information Security for South Africa, pp. 1–8. IEEE (Aug 2013)