Review of Cloud Forensics: Challenges, Solutions and Comparative Analysis

Poorvi Jain
Department of Computer Science and Engineering
Sushila Devi Bansal College of Technology, Indore, M.P- 453331, India

Ajitabh Mahalkari
Department of Computer Science and Engineering
Sushila Devi Bansal College of Technology, Indore, M.P- 453331, India

ABSTRACT
Every technology has some benefits and some limitations. Cloud computing has its own set of them. Cloud computing has various advantages i.e. reliability, cost effective, scalability, fault tolerance, backup. But there are also some security issues in cloud computing because data is stored on worldwide platform. Many attackers can use cloud services to create vulnerability in the cloud system. There are some forensics tools implemented to find information about these attacks in cloud environment. This complete process to find evidence in cloud environment is known as cloud forensics. This paper presents a study about cloud forensics methods, technology used, comparative study to provide awareness of tools, methods, challenges in cloud forensics. This information will help to find new techniques to improve forensics process in cloud forensics.

Keywords
Cloud Computing, Cloud Crime, Cloud Forensics, Digital Forensics, Forensics Methods, Incidents, Investigation challenges.

1. INTRODUCTION
Before Cloud computing was introduced, there were limited services available to the users. After cloud computing technology various types of services were introduced so that the consumer can get access for different kind of services over the network. These services are of three types named as Infrastructure as a service, Software as a service, platform as a services.

These models differ from each other in the terms of their accessibility for the users. All the services are given to the consumers by four cloud deployment model i.e. public cloud, private cloud, community cloud and hybrid cloud. Computers and mobile user's uses cloud services to save the data. In the cloud computing user data is stored in different- different servers anywhere is the world and this data is stored or accessed over the network hence there are various attackers are available who can breach security of the data.

To find attackers or to reduce crime a forensics procedure is used by digital forensics tools in cloud environment which is known as cloud forensics.

"Cloud Computing Forensic Science" is defined in (NIST, 2014b) [1] as The application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination and reporting of digital evidence.

Today's network technology is helpful to people in ways like to connect over the internet to meet their demands. Organizations are looking for higher profit margin and minimum cost to establish their business. To fulfil these demands of organizations a new technology invented which is known as "Cloud computing".

This technology is not owned by any company. Cloud service providers sign a contract with few companies which offers cloud services such as Amazon, Microsoft, Google, Adobe, VMware, IBM Cloud, Rackspace, and Red Hat. This Technique is based on "Pay as you go" model

Cloud computing is based on three service models Infrastructure as a service (IaaS), platform as a service (PaaS) and Software as a service (SaaS). These models are different from each other in the terms of control of users on the software, platform, and infrastructure. In the SaaS model cloud service providers has control on client side and server side, on the other hand in the PaaS model users have more control then SaaS model. And in the IaaS model users have highest level of control then SaaS and PaaS model

There are also four deployment models Public cloud, Private cloud, Hybrid cloud, community cloud are introduced. When services and infrastructure are open to the public over the network it is under Public cloud. When services offered to a particular organization then it is considered under private cloud.

When an organization wants to include variety of services from two or more clouds from different service providers then it is known as Hybrid Cloud. When a single community provides services to several organizations with same purpose it is categorized in Community cloud.

Several characteristics like cost-effectiveness, scalability, reliability and flexibility of cloud computing makes impact on users to adopt this technology.

Nowadays various crimes are emerging with the help of digital devices. To resolve it and get justice the Law enforcement agents and investigators are struggling to find suitable evidence. This complete process to find evidence from digital device is part of "Digital Forensics".

Digital Forensics is basically related to computer crime. It is basically a combination of two processes that is recuperation and analysis of material or data in digital device. Forensic processes are used in digital forensics to search any evidence on a device in order to present the evidence in the court or in front of any company's juries.

Various tools and techniques have been invented to complete investigation process. There is basically a process in every digital forensics techniques to acquire, preserve, and analyze evidence. To make any evidence admissible in the court integrity and chain of custody of digital evidence should be maintained.

There are many barriers in cloud computing environments because of its multi tenancy nature. Attackers can use cloud to do crime successfully. To resolve all the crimes in cloud environment a branch of digital forensics is introduced called "Cloud Forensics". Cloud Forensics can be done with the help of digital forensics techniques in Cloud environment. It has to deal with several issues related to Jurisdiction, dependency on CSP and multi tenancy.

To prevent cloud system from attacks, there are several efforts made by cloud service provider (Kim-Kwang Raymond Choo et.al., 2017). For e.g. to find child abuse material, Microsoft designs a PhotoDNA software.

According to National Institute of Standards and Technology (NIST) [9], cloud computing forensic science is defined as "the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation and reporting of digital evidence".

Evidence identification is the major task in cloud forensics because it is comprised of different kind of services and deployment models. Data is spread all over the world so there is no chance to seize any physical device to get evidence.

Cloud Computing is very advance technology and there is need to invent new tools, frameworks and tools are required to perform forensic procedure inside the cloud. To present evidence in the court, investigator must ensure that the evidence is not altered by any third party because cloud service provider has also signed contract with third parties to provide services to the consumers.

Chain of custody is most important to present evidence in the court; a single fall down in chain of custody can create big loss of information in the court. When forensic procedure is required in Public cloud model, investigators are not able to seize any physical device, in addition to if the premises uses internal Private cloud model then forensic procedure can be same as traditional forensic procedure but if organization uses external private cloud model then the investigator needs to depends on CSP to collect data or log files.

2. BACKGROUND

Cloud Computing

To avail services to users on demand basis is fulfilled by this technology [2]. User can store there data, run their program over the network and many other work. There are various types of software available which will be good example of cloud computing services i.e. Google drive, Google cloud platform, Microsoft azure, I-cloud, Cloud foundry etc.

Evolutionary changes in the technology done by cloud computing because of its services. Which is known as Software as a service, Platform as a service and Infrastructure as a service. Every service differs from each other in the terms of user's control on layers of service model.

These service models can be defined as:

Software as a service (SaaS): In this variety of services, applications are delivered over the internet. e.g. Google mail.

Platform as a service (PaaS): In this type of services, application development platform provided to the users to make their applications. e.g. Microsoft Azure.

Infrastructure as a service (IaaS): The server, hardware, storage services provided to the users. e.g. Amazon storage services, Google drive etc.

Cloud services deployed by four deployments model, These models can be defined as:

Public cloud: In this type of cloud, cloud services re available to general public on the basis of pay per use model, although sometime companies available free services to users. All the data stored in third party server.

Private cloud: In this type of cloud, companies own their personal cloud structure for the security purpose.

Community cloud: As name suggest, in this type of cloud model, private cloud extends to the organizations within the same area.

Hybrid cloud: It is the amalagation of two or more than two clouds. This model adopts benefits of all models based on the combination of model type.

In cloud computing resources shared to achieve coherence and economics of scale. Enterprises using cloud computing to run their applications in faster way because resources are available based on requirements.

This technology came to make cost effective system so that enterprises can run their process smoothly without any IT obstacles. A technology called virtualization invented in cloud computing to divide physical device into one or more virtual device so that resources can be utilize in best manner.

Cloud computing is similar like grid computing. There are several characteristics which makes this technology useful-

- Maintenance is easy of cloud applications because of its accessibility.
- Multi tenancy is a good feature to share resources and cost.
- Complete system is designed as a loosely coupled system so that service provider can monitor performance of the system.
- Productivity increased because all data management done by online.
- Security can be achieved in this because of it's centralize design structure.

Digital Forensics

People know digital forensics is similar as computer forensics [3] but this is different by expanding it to all type of devices which can store digital data. To find any evidence electronically, digital forensics used. For example, in the case or murder, theft and assault against a person, digital forensics is helpful to support or refute a hypothesis. It is also helpful in intrusion detection system.

Digital Forensics: by Palmer, 2001 "The use of scientifically derived and proven methods towards the preservation, collection validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from the digital sources for the purpose of facilitating the reconstruction of the events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations."

Digital Forensics: by NIST, 2006 Proposed simple definition:"The applications of science to identify, collection, examination and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for data."

Types of Digital Forensics
Static forensics: The process of collecting evidence from Powered off digital media is known as static forensics. Apart from its advantages there is disadvantage that it cannot collect the evidences from the RAM, which may contain keys or network related data.

Live Forensics: This is the method of collecting volatile data evidences like network related or user data.

The issue with the live forensics is, by its temporal nature, it will not be able to reproduce same results if required.

Most of the researchers consider live forensics best for the cloud environment

In case of SAAS, PAAS live forensics will be best suited but in case of IAAS static forensic is better choice.

In digital forensics, a suspected electronic device is seizure to analyze and collect evidence. All the process completed mainly in three steps i.e. imaging of exhibits, analysis and report in the form of submissive evidence to present in front of juries.

In digital forensics, a broader and time consuming task is investigation of evidence to make a hypothesis. Evidence can be analyzed with the help of some tools and methodology to make forensics process easier. There are two major issues in the process of digital forensics i.e. Integrity and Authenticity. Integrity can be defined in the terms of no modifications in the collected evidence through the acquired media to store. Authenticity ensures integrity in the collected evidence.

Cloud Forensics
As we know that cloud computing is a revolutionary technology [4], which is increasing day by day as per user requirements. Many malicious users are making cloud computing as their weapon to attack system of users. To find these attackers some digital forensics methods used in the cloud environment, this procedure to find culprit is known as cloud forensics.

Cloud forensics can be defined as the use of digital forensic best practices in cloud environment.

Cloud Forensics: by NIST 2014a
"Cloud computing forensics science is the application of science 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 reconstructions of these events."

Cloud forensics has three dimensions in it which are-

- Technical Dimension
- Legal Dimension
- Organizational Dimension

Technical Dimension: In this dimension, some tools are used to perform cloud forensics in cloud computing. Some of the main tasks completed in this i.e. data collection, live forensics, proactive measures, virtualized environments etc. These tools are differing from each other in the terms of their deployment model and service model.

Legal Dimension: This is useful to ensure privacy of users that forensics procedure should not breach any law and regulations in the jurisdictions of data centers. A service level agreement (SLA) is the medium to ensure security of data between cloud service provider and consumer.

Organizational Dimension: There is cloud service provider and cloud service consumers both become parts. If cloud service provider is providing their services to users then investigations widens. Mainly three types of third parties are involved in this investigation process, these Ares-

- IT professionals
- Incident handlers
- Legal advisers

Cloud Forensics process model
To identify any evidence in the cloud environment as well as in digital environment, it is necessary to follow a step by step procedure to make it successful. There are various frameworks for digital forensics provided (Josiah Dykstra and Alan T. Sherman, 2011) to complete great forensics process. Generally these frameworks applicable under many circumstances so that they can be useful accordingly based on the requirements. Also these frameworks are technology independent.

Consider the "Guide to Integrating Forensic Technique into Incident Response" published by NIST (Kent et al. 2006). The NIST process, like many others, can be roughly summarized as follows:

- Collection
- Examination
- Analysis
- Reporting

In the collection phase data acquisition process involved. In the phase of the examination, all the data combined based on the interest or similarity. In analysis phase all the examined evidence should be analyzed based on the investigative questions. In the report, all the outputs and procedures to get this output should be described.

3. LITERATURE REVIEW

M. Edington Alex, R. Kishore et.al.[5], They highlighted some challenges which is faced by forensic investigator. In most of the research work investigators need to depend on CSP so there may be chance that CSP can alter data and this can affects complete investigation process. After obtaining permission from the international telecommunication union (ITU) they proposed a solution based on centralized forensic server and a forensic layer called forensic monitoring plane (FMP) implemented outside of the cloud premises for mitigate the dependency on CSP.

Aniello Castiglione, Giuseppe Cattaneo, Giancarlo De Maio, Alfredo De Santis and Gianluca Roscigno et.al.[6] To uncover the recent attacks they provide a novel methodology to collect network information from online services, such as web pages, chats, documents, photos and videos. On behalf of the investigator for collecting information they are based on TTP.For experimental evaluation of the methodology they used a proof –of – concept prototype, called LIENA. Through

this methodology the network packets and interpretation information is automatically collected from remote sources. A digital notary who acts as a third party is introduced in order to certify both the acquired.

Juan-Carlos Bennett and Mamadou H. Diallo [7] introduces a Forensic Pattern-Based Approach in 2018 which is a semiformal architecture with the help of object oriented approach amidst patterns. Followed NIST Forensics framework to collect, examine and analyze the evidence. They introduced Cloud evidence collector and cloud evidence analyzer to congregate more and better network evidence in minimum analysis time.

Simou et. al. [8] in 2018 provided a framework which represents a visionary model along set of forensic constraints to tracery a cloud forensics enables services. This model also helpful to complete forensic process in leading way so that developers can procreate cloud system to forensic enabled.

Palash Santra et. al. [9] provided A Comparative Study which shows awareness about log analysis over cloud forensics methods. Authors suggested Boolean and Euclidian cryptography methods to secure log data because log data is most important data to make successful process of cloud forensics. Also they suggest that if we can implement knowledge based system using fuzzy logic and data mining to prevent malicious activity in the cloud.

Sugandh Bhatia and Jyoteesh Malhotra [10] in 2018 introduced a trustworthy framework to ensure security, privacy in cloud computing technology so that organizations can embrace it. It publicizes all the information about technology to the technicians who involve in the organizations. With the help of this model, organization readiness can also forecast. A complete organization can be managed along with this model appliance.

Palash Santra et. al. [11] discusses detailed Comparative Analysis of Cloud Forensic Techniques in IaaS. In this paper author provided a parallel study based on different forensics methods that were proposed for Infrastructure as a service (IaaS) model. All the steps in cloud forensics model i.e. Evidence acquisition, collection, analysis, and presentation techniques has been appropriated to make this analysis in IaaS."

Ezz El-Din Hemdan and D. H. Manjaiah [12], proposed a Digital Forensic accession for probe of Cybercrimes in Private Cloud Environment. They conceived an experimental environment to introduce forensic process in private cloud. The most essential steps in cloud forensic process are Data acquisition and collection from the Virtual machines. They popularized live forensics and dead forensics approach to investigate virtual machines in private cloud environment.

Ahmed Nour Moussa, Norafida Ithnin and Anazida Zainal et.al.[13], For overcome the limitations of other research where system is implemented and controlled by the cloud service provider they proposed a conceptual bilateral cloud-forensic-as –a-service model. In this model consumer and service provider both can collect, verify the equality of the forensic analysis process and with this mean they also can resolve disputes that emerges from independently collected results. The success of this model depends on two factors: The quality of the forensic data that is collected by the consumer and also depends on comparison and conflict resolution protocol (CCRP) to enable mutual agreed outcomes.

4. CHALLENGES IN CLOUD FORESNSICS

There are some challenges in cloud forensics (Stavros Simou et.al. ,2016), which are-

- There are various challenges to collect logs in forensics environment because sometime CSP hides log details and most of the time does not provide log services.
- Data inaccessibility is also a big challenge, because data stored at various locations.
- In all the service models, investigator needs to depend on CSP to identify, preserve and collect evidence.
- Integrity of the collected evidence and chain of custody is the important part in cloud forensics process should be maintained to present evidence in admissible form in the court.
- Multi jurisdiction distribution is also a big challenge because data is distributed at geographical level.
- Strong encryption methods are needed to store evidence in secure format.
- Evidence should be documented properly without any changes from the beginning stage.

5. RECENT SOLUTIONS AND COMPETITATIVESS ANALYSIS

Cloud Computing technology is based on service models and deployment models, it is very difficult to perform digital forensics procedure in this environment. Multi tenancy, location transparency, dependency on CSP are the major challenges in cloud computing. A technology was introduced called "hypervisors" to manage and create virtual machines. Integrity and data segregation are two most integral part in the process of cloud forensics.

An object oriented pattern based approach [7] dependent on semi formal architecture was introduced. This architecture can be understood with the help of abstraction of patterns. All the possible attacks in cloud environment according to type of system were considered. A proper framework with UML object oriented models were presented in front of cloud

Table 1.0 Comparative study of the recent cloud forensics solutions.

Forensics Methods	Problem Identified	Benefits	Limitations
FROST (Dykstra et. al. , 2013)	It is useful to reduce dependency on cloud service provider	• It is very useful to forensic acquisition as it supports Infrastructure-as-a-Service (IaaS). • There is no dependency on cloud services provider as the tools are user-driven. • It is also beneficial for real-time monitoring, metrics, or auditing.	It is only beneficial for acquisition phase.
A framework to collect CSP independence forensics data (M. Edington Alex et.al. , 2017)	Investigator needs to depend on CSP to collect forensics data.	All the necessary information about fraudulent activities can be collected by FMP as it is validated with DDoS.	This model is not tested with entire cloud environment.
LINEA (Aniello Castiglione et. al., 2017)	Because of volatility in the cloud system, it is difficult to collect network evidence.	• A methodology is suggested to collect network evidence. • Evidence collection makes by online services. • It is beneficial for both expert and non-expert analysts. • It is useful to recognize recent attacks.	It uses only one IP address to each CollectorVM.
A SEMI-FORMAL MODELING APPROACH (Benneet et. al., 2018)	Due to the complexity of cloud system and limited access of cloud infrastructure makes it difficult to Collect forensic information in the UCaaS network infrastructure.	• This framework was useful to make forensics techniques in UC based technology. • To enhance security this is very useful model. • To collect forensics data a systematic approachis provided by this model. • The main key benefit of this approach is it can be reused in investigation process because it is based on patterns. • With the help of this approach malwares can be detected.	• This model has Limited forensics patterns. • The pattern evaluation is done informally and restricted within few architects.
A generic methodology to build cloud forensic-enabled services (CFeS) (Simou et. al., 2018)	There was a gap in the field of cloud forensics as there was no methodology to cloud forensics enabled services.	• This model is an integrated model based on cloud services characteristics with the cloud investigation to help engineers to invent cloud forensics enabled	• This is limited to an organization that offers services only in private deployment model. Also there is no third party dependency.

		services. • Forensics constraints were introduced to design cloud forensics services. • This model can represented to complete picture of cloud services of any organization.	• Different jurisdiction not able to solve by this framework.
Log-Based Cloud Forensic Techniques (Palash Santra et. al., 2018)	To identify all the To understand all log based activities.	• With the help of log records, attacks can be identified. • Log management process is also described.	• Dumped log record security is very difficult. • There is no method to preserve Pre-forensic and post-forensic data for forensic presentation
CSPCR: Cloud Security, Privacy and Compliance Readiness (Sugandh Bhatia and Jyoteesh Malhotra, 2018)	There were many models for self evaluation of any organizations but they were not satisfactory for improvement of the system.	• This model is used to create awareness about hazards in cloud. • This is useful to achieve high level security as it contains hexagonal security model. • The proposed framework is very useful to check the representation and efficiency of the technical personnel.	There is need of the trusted third party to represent the CSPCR assessment.
Cloud Forensic Techniques in IaaS (Palash Santra et. al., 2018)	To create awareness about all cloud forensics techniques in cloud forensics.	Data integrity to prevent evidence from tempering.	There is no specific algorithm to reduce search space and filtering.
Digital Forensic Approach for Investigation of Cybercrimes in Private Cloud Environment (Ezz El-Din Hemdan et. al, 2018)	It is analyzed that there were various security threats in the private cloud network.	This approach was very beneficial to collect digital evidence from virtual machines in private cloud.	This technique was only for private cloud.
CFaaS (Ahmed Nour Moussa et.al. ,2018)	There was no framework to collect and verify data at both consumer and provider side.	It is useful to collect and verify independent data at consumer and provider side to resolve potential disputes.	There is a limitation that consumer can't collect direct data from provide side.

evidence collector and cloud evidence analyzer patterns based approach to provide security and to collect evidence in cloud environment. This approach had a great feature "Reusability", so that investigator can use it multiple times in forensics process.

An integrated method invented [8] which is used to make Cloud services to Cloud Forensic enabled services with the set of forensic constraints and a conceptual model to express modeling language and to present a complete process. To aware software engineer about cloud forensics services this model was invented. This method combines the characteristics of cloud computing and cloud investigation process. This method was invented to help software engineer to create forensics enabled services.

A method that was inspired from VM introspection [9] was suggested so that all the snapshots of the VM can be stored in sequential manner. This method was beneficial for digital provenance, isolation of cloud instance, prevention of data corruption by third party so that integrity can be preserved.

A hybrid approach was suggested by authors [9] to examine different components in cloud environments to find illegal activities inside the cloud. Basically this approach was based on three techniques known as swap space analysis, conjunctive delivery model, terminated process based approach.

An acquisition and collection of any cybercrime in private cloud environment [12] is based on digital forensic approach. VMware used to build an experiment environment. Complete

procedure done in Private cloud network, this gives relaxation to examiner that the crime is committed in particular place. Investigation of virtual machines was done with live forensics and dead forensics procedures. When forensic procedure continue with the running virtual machine so that all the information or volatile data can be collected and analyze by forensic investigator on the other hand when forensic procedure is done in offline mode, it is categorized in dead forensics.Upper table shows comparative analysis of recent solutions in cloud forensics.

6. CONCLUSION

In this paper forensics methods are discussed to understand cloud forensics techniques. Advantages and disadvantages of the methods will be useful to make advance methods so that forensics procedure improved. Some methods are very useful to collect, analyze evidence in forensics environment, but also there are some limitations as well based on deployment model in cloud. In cloud forensics services are provided by virtual machines i.e. users can use services and after sometime when they released resources, these resources can be accepted by others. There is some live forensics and dead forensics procedures are used to collect evidence from virtual machines, but this approach was limited to only private cloud, some future research can be extend to collect data from virtual machines in public cloud.

7. REFERENCES

[1] Almulla, Sameera; Iraqi, Youssef; and Jones, Andrew 2014.A State-Of-The-Art Review of Cloud Forensics. *Journal of Digital Forensics, Security and Law*: Vol. 9:No. 4 , Article 2, DOI: https://doi.org/10.15394/jdfsl.2014.1190.

[2] https://en.wikipedia.org/wiki/Cloud_computing

[3] https://en.wikipedia.org/wiki/Digital_forensics

[4] https://www.techstagram.com/2013/03/20/cloud-forensics-importance/

[5] M.E. Alex, R. Kishore.2017.Forensics framework for cloud computing, Computers and Electrical Engineering.http://dx.doi.org/10.1016/j.compeleceng.2017.02.006.

[6] A. Castiglione, G. Cattaneo, G. De Maio, A. De Santis and G. Roscigno.2017.A Novel Methodology to Acquire Live Big Data Evidence from the Cloud.in *IEEE Transactions on Big Data*.

[7] doi: 10.1109/TBDATA.2017.2683521.

[8] Bennett, Juan-Carlos & H. Diallo, Mamadou. 2018.A Forensic Pattern-Based Approach for Investigations in Cloud System Environments. 1-8. 10.1109/CSNET.2018.8602908.

[9] Stavros Simou,Christos Kalloniatis,Stefanos Gritzalis,Va silios Katos.2018. A framework for designing cloud forensic-enabled services (CFeS).

[10] Santra P., Roy A., Majumder K.2018.A Comparative Analysis of Cloud Forensic Techniques in IaaS. In: Bhatia S., Mishra K., Tiwari S., Singh V. (eds) Advances in Computer and Computational Sciences. Advances in Intelligent Systems and Computing, vol 554. Springer, Singapore.

[11] Bhatia, Sugandh & Malhotra, Jyoteesh .2018.CSPCR: Cloud Security, Privacy and Compliance Readiness - A Trustworthy Framework. International Journal of Electrical and Computer Engineering. 8. 10.11591/ijece.v8i5.pp3756-3766, 2018.

[12] Santra P., Roy A., Majumder K.2018. A Comparative Analysis of Cloud Forensic Techniques in IaaS. In: Bhatia S., Mishra K., Tiwari S., Singh V. (eds) Advances in Computer and Computational Sciences. Advances in Intelligent Systems and Computing, vol 554. Springer, Singapore.

[13] Hemdan E.ED., Manjaiah D.H.2019. Digital Forensic Approach for Investigation of Cybercrimes in Private Cloud Environment. In: Sa P., Bakshi S., Hatzilygeroudis I., Sahoo M. (eds) Recent Findings in Intelligent Computing Techniques. Advances in Intelligent Systems and Computing, vol 707. Springer, Singapore.

[14] Moussa, A.N., Ithnin, N. & Zainal.2018.CFaaS: bilaterally agreed evidence collection. A. J Cloud Comp (2018) 7: 1. https://doi.org/10.1186/s13677-017-0102-3.

[15] Pichan, Ameer & Lazarescu, Mihai & Teng Soh, Sie.2015. Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigatio. 13. 10.1016/j.diin.2015.03.002.

[16] DykNetwork Forensicsstra, Josiah & Sherman, A.T.2011. Understanding Issues in cloud forensics: Two hypothetical case studies. Journal of . 3. 19-31.

[17] Simou, Stavros & Kalloniatis, Christos & Gritzalis, Stefanos & Mouratidis, Haris.2016. A survey on cloud forensics challenges and solutions. Security and Communication Networks"10.1002/sec.1688.

[18] Dykstra, Josiah & T. Sherman, Alan.2013. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. Digital Investigation. 10. S87–S95. 10.1016/j.diin.2013.06.010.

[19] K. R. Choo, C. Esposito and A. Castiglione.2017.Evidence and Forensics in the Cloud: Challenges and Future Research Directions. In *IEEE Cloud Computing*, vol. 4, no. 3, pp. 14-19, 2017.

[20] doi: 10.1109/MCC.2017.39.