Reviewing the Existing Methodologies and Tools of Cloud Forensics: Challenges and Solutions

Khalid A Alattas[1]

Department of Computer Science and Artificial Intelligence, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia.

kaalattas@uj.edu.sa

Magdy Bayoumi[2]

Department of Electrical and Computer Engineering, University of Louisiana at Lafayette, Lafayette, LA 70503, USA.

magdy.bayoumi@louisiana.edu

ABSTRACT

Cloud computing is relatively a new technological advancement which has speedily become part of the important technological improvements for computer science. Cloud computing as technological advancement has significantly grown in the recent past. It is currently cheaper hence affordable as the cloud platforms stabilize. Most of the businesses and organizations have successfully migrated their systems to accommodate cloud infrastructure hence obtaining benefits that foster technology and economy. There has been reluctance due to security issues and loss of control because of infrastructures and data that could be controlled by third parties. Cloud forensic which is a result of the cloud computing has come up due to the ever-increasing criminals who take advantage of the technological progress to steal data and information from the cloud, cause a denial of service and provoke increased economic impacts on the organization. The digital forensics has had challenges and solutions to its methodologies and tools used because they must grow in complexity to measure up to the standards of the criminals. This paper shall focus on the existing methodologies and cloud forensic tools, including their challenges and solutions that have been developed.

Key words: Cloud forensics methodologies, digital forensic methodologies, cloud infrastructure, cloud forensics, forensic investigation, forensic challenges

1. INTRODUCTION

Cloud computing is an essential component of information technology that has received much popularity in recent years and has continued to rise. Currently, cloud computing is an important technology that is useful in engaging the customers and most enterprises are now investing in cloud services, soft wares and hardware that support the cloud services and enhance its implementation and management within the organization [1].

On a daily basis, several organization and institutions are transferring their services to cloud platforms. Many companies have considered the adoption of cloud technology. However, the core challenge that acts as an obstacle to the adoption is the security concern that has increasingly caused digital crimes on the cloud environments [2]. Regardless of the positive side of the speedy cloud computing advancements that many users enjoy, the cloud services have also caused increased the number of users who perform malicious operations in the cloud environments. Cloud services involve the transmission of information and exchange of money hence attracting criminals who seek to profit themselves. According to a survey done by Cloud Security Alliance, up to 24.6 per cent of the companies would willingly pay criminals a ransom to release their data or prevent cyber-attacks [1].

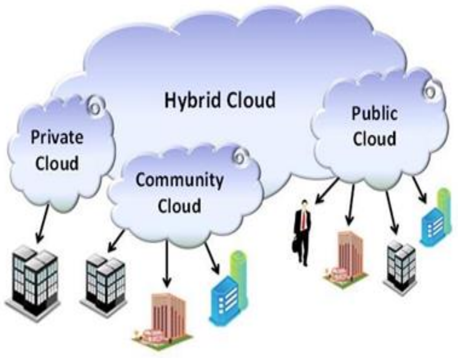


Figure 1: Cloud computing models

Cyber-crime has become a major concern among the cloud service providers, law enforcers and users. The security mechanisms, regulations and policies have been developed to help in the protection of the users and the data [3].

Forensics refers to an act that is applied when investigating, identifying and acquiring evidence that would become admissible in a court of law. This process is important in the searching, forensic imaging, and digital media analysis to help in producing the report. The acquisition of digital evidence from a cloud environment is limited due to the cloud infrastructure and resources that are directly owned and provided by cloud service providers. The users have restricted access to the forensic data, and also they lack knowledge of the location in which data is stored [1]. Cloud service providers intentionally hide the physical location where data is actually stored, and they avoid the exposure of the tools and services that help in acquiring the cloud evidence. This means that the investigators must conduct a forensics investigation on the digital media which are the cloud computers to help in identification, preservation, collection and analysis of every evidentiary for an accurate result of the content to be presented to the court of law for prosecution. This form is referred to as cloud forensics [2].

The core objective of this research paper is providing an expounded literature review on the currently existing methodologies, the tools dealing or possibly assisting cloud forensic processes. This research analytically reviews the cloud forensics that exists with their challenges and solutions. It explores the tools and methodologies founded on a detailed review of the concerned areas, every work that has been done in digital forensic and cloud forensic methodologies. The research provides the future work that will essentially be done and the tools that must be implemented to help in the cyber-crime investigation process in a cloud-based environment. This research paper has been structured into sections. There will be a section of literature review based on related work on cloud computing, the digital and cloud forensic, the existing methodologies in the digital and cloud forensics. Secondly, there shall be a proposed model of the solution to the challenges using various solutions that best suit the identified challenges. Finally, we shall have the closing section, which will provide the conclusion, future work and any recommendations for the reviews and identified challenges on how to mitigate them [1] [3].

2. LITERATURE REVIEW

A. *Digital and cloud forensics*

Cloud computing is provided by the CSP who supply the services to the organization at a fee. CSP maintains the computing infrastructure needed to provide various services which deliver the cloud services to the users via the internet [6]. The cloud computing works with resources and not platforms, software or equipment as remote service. The cloud services can have their models which are software as a service, platform as a service or infrastructure as a service. The various models of deployment include private cloud, public cloud, hybrid cloud and community cloud [1].

Digital forensics helps in dealing with the digital evidence that has been seized in a crime scene. The vital component of digital forensics is the digital forensics which maintains the digital evidence integrity and that of the chain of custody as well. Breaking the chain of custody means that the pieces of evidence have been compromised [3].

Cloud forensics is part of the digital forensics. It explains the importance of performing digital investigations founded in forensics procedures and principles. The crime investigators in any cloud environment must deal with many issues when compared to digital forensic experts.

The process of identifying pieces of evidence in a cloud environment is a hard process because of the diverse deployments and models that are applicable and often limit the seizing proves of the computer devices that contain the evidence. The diverse cloud forensic methods have been innovated and used in cloud deployment and service models [1] [4] [2].

When internal hosting of the private cloud takes place, the forensic investigations is almost compared to the traditional way of performing forensic investigation, but if hosted externally, the process of forensic investigation processes will depend on the cloud service providers and the signed contract [5].

B. Current methodologies

Since 1999, there have been diverse methods and frameworks that have been developed concerning how to conduct accurate forensic digital investigations which include diverse stages and phases. The forensic computing has a process which involves the identification, preservation, analysis and presentation of the digital evidence in a way that is accepted legally [5].

In the year 2001, the United States department of justice developed an electronic crime scene investigation guide for responses. This was designed to help the law enforcing officers and other responders of crime scenes to become responsible by preserving, recognizing, collecting and protecting the digital evidence collected from the crime scene. Abstract Digital Forensic was a model which consisted of nine stages of collecting and preserving the digital evidence. In the year 2003, IDIP was developed, which was an integrated process of performing digital investigation. It was introduced to assist in physical investigations of the crime scenes. Enhanced IDIP model provided a way of separating the primary and secondary investigations in a crime scene as well as depicting the stages that iterate instead of linear [6].

Among the latest models include Cloud forensic process of 2012, which focused on the evidence's admissibility and competence as well as ensuring that the digital evidence has been kept into consideration of the human factors. The Advanced data Acquisition Model of 2013 assisted digital forensic experts in presenting the process of evidence in a court of law. The integrated digital forensic process model of 2013 was an important merger of the existing models of forensic investigation, whereby it consisted of the process that enhances evidence sourcing and protection.

Finally, in 2015, the Open Cloud Forensics model was proposed. This is a forensic process consisting of stages which include preservation stage, identification stage, collection stage, organization stage, presentation stage and finally the verification stage. The stages have unique functionalities [4].

C. Comparison framework

This is an important framework that will help in creating the map of the stages of the diverse methodologies. The comparison framework goals include merging similar stages of the framework that has been proposed and secondly assign the limitations to the various stages of the diverse comparison frameworks.

The implementation of the comparisons framework considers the limitations of the stages of the models that were previously proposed and used. Some could be detailed while others are complicated with a big number of processes that help in implementing the omitted vital aspects that have been oversimplified. The comparison framework helps in merging similar stages and provide similar results to one stage [7].

Identification being the initial stage is unique and often helps in identifying every possible evidence. It also helps in the preservation and constitution of the collected data that must be simultaneously preserved well. The comparison framework helps in the analysis and association of the cloud forensics challenges that are derived dependent on the suggestions and the limitations of the crime scene. The framework has four steps;

Identification. This is the initial stage and helps in that identification of every possible source that is suspected of containing potential pieces of evidence in the cloud environments.

Preservation. This is important for the collected data. After the identification of the potential evidence, the process of collecting and acquiring evidence from the crime scene must be preserved. There is a need for the investigators to collect, isolate and preserve the pieces of evidence from access by other people.

Examination; the process of evidence analysis includes the investigators extracting data from the previous stages and inspecting the vast amount of data that have been identified in the crime scene. While performing the analysis, data significance is key in order to transform them into evidence that is admissible in a court of law hence the need for professionalism and responsibility.

Presentation. This is the last stage and involves evidence presentation obtained to a court of law. This uses a properly written report in which the findings needs to be provided by means of testimonies on the analyzed evidence [1].

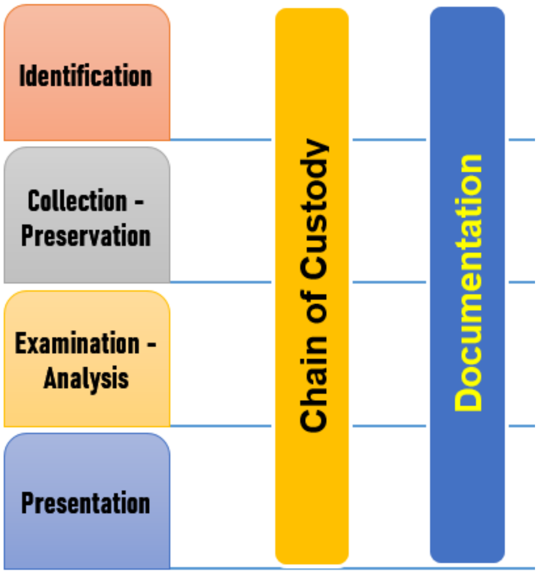
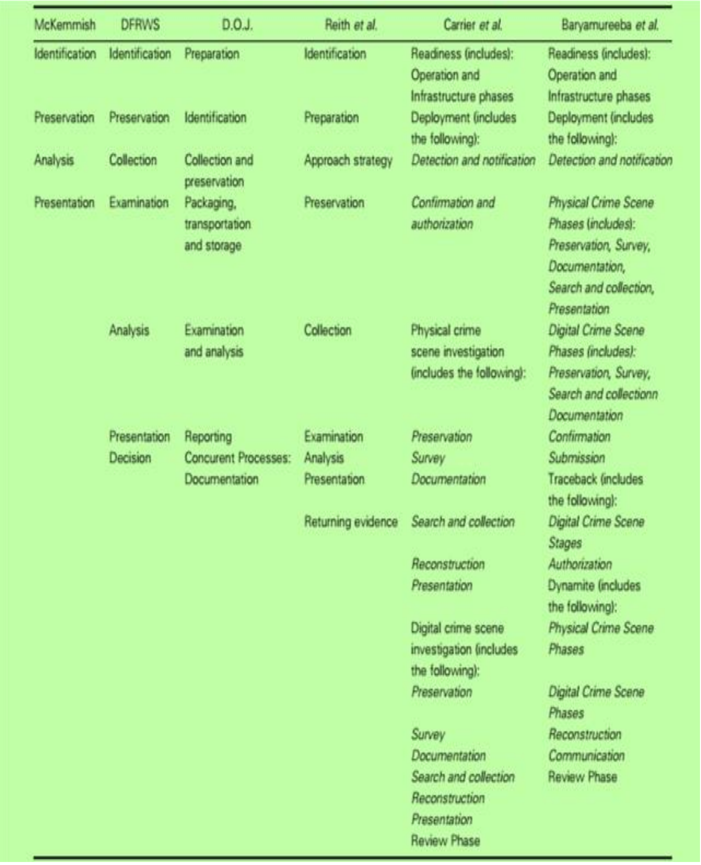


Figure 2: Stages of a model.



McKemmish	DFRWS	D.O.J.	Reith *et al.*	Carrier *et al.*	Baryamureeba *et al.*
Identification	Identification	Preparation	Identification	Readiness (includes): Operation and Infrastructure phases	Readiness (includes): Operation and Infrastructure phases
Preservation	Preservation	Identification	Preparation	Deployment (includes the following):	Deployment (includes the following):
Analysis	Collection	Collection and preservation	Approach strategy	*Detection and notification*	*Detection and notification*
Presentation	Examination	Packaging, transportation and storage	Preservation	*Confirmation and authorization*	*Physical Crime Scene Phases (includes): Preservation, Survey, Documentation, Search and collection, Presentation*
	Analysis	Examination and analysis	Collection	Physical crime scene investigation (includes the following):	*Digital Crime Scene Phases (includes): Preservation, Survey, Search and collectionn Documentation*
	Presentation Decision	Reporting Concurent Processes: Documentation	Examination Analysis Presentation	*Preservation* *Survey* *Documentation*	*Confirmation* *Submission* Traceback (includes the following):
			Returning evidence	*Search and collection*	*Digital Crime Scene Stages*
				Reconstruction *Presentation*	*Authorization* Dynamite (includes the following):
				Digital crime scene investigation (includes the following):	*Physical Crime Scene Phases*
				Preservation	*Digital Crime Scene Phases*
				Survey *Documentation* *Search and collection* *Reconstruction* *Presentation* Review Phase	*Reconstruction* *Communication* Review Phase

Figure 3: Digital and cloud forensics methodologies.

3. METHODOLOGIES AND FRAMEWORKS DISCUSSION

A big number of models use four stages as part of their framework. Some of the activities on the models are not wholly drawn on the comparison framework but have been combined into a single stage. Examining the methodologies' complexity needs conventional complexity indicators that are based on the number of stages that have been introduced and the number of phases on all the stages per the methodologies. After that, the analysis is performed [2] [8].

The results of the complexity analysis show that cloud forensics is much demanding when compared to digital forensics because of the introduced new frameworks and methodologies on the cloud investigation process for the purpose of preserving the evidence and maintaining the chain of custody in every stage of the investigation [1].

Several models are currently dedicated to digital forensics and do not consider the cloud environment features. Five models of the cloud forensic purposes have been developed, but as of now, only two are completed. There have been few authors who have attempted to come up with new models to help in conducting digital forensic investigations in an environment of cloud computing.

Finally, the preservation of the different activities in the cloud forensics framework, which runs alongside other processes could be different because evidence preservation is a vital investigation step which must be well-handled for presentation in a court. The process of documenting could be considered an activity due to the reason that it's done all through the investigation. These activities, chain of custody included needs to be applied in the process of digital investigation [1] [5].

A. *Cloud forensic challenges*

The cloud forensics challenges are categorized according to the process stages that they fall under. It is evident that many challenges apply to the public cloud, whereas fewer ones have private cloud applicability.

i. *Identification stage.*

Access to the pieces of evidence in logs.

Logs are important in the investigation process. Access to log files means that one can identify incidents which is important for the investigators. Logs collection in cloud environments is hard because cloud services are multi-tenant where the same processing systems process user requests from many sources. Most of the cloud service providers never provide access to logs by not gathering them or intentionally hiding them [1].

Volatile data. Data that has been stored in virtual machines instances in IAAS models of service might often be lost when the virtual machines are rebooted or shut down. This means that important evidence may be lost like the registry entries, temporary internet files and the processes [1] [7].

ii. Preservation- collection stage

Integrity and stability of the evidence caused by the multi-tenancy of the data as well as their privacy. The preservation of the integrity and evidence's stability is vital during the cloud investigation process of the SaaS, PaaS and IaaS. Data must be preserved to enhance the acquisition of evidence without violation of any law [1].

Chain of custody. A vital part of the process of presenting evidence in the court is ensuring that the evidence's chain of custody being presented has been maintained during and after the investigation process [3] [2].

iii. Examination, the analysis stage

Lacking forensic tools. The process of analyzing data in the cloud environments need appropriate forensic tools. Several cloud investigation tools have been made and introduced for digital forensic investigations. There are currently no tools made to specifically help in cloud investigations [9].

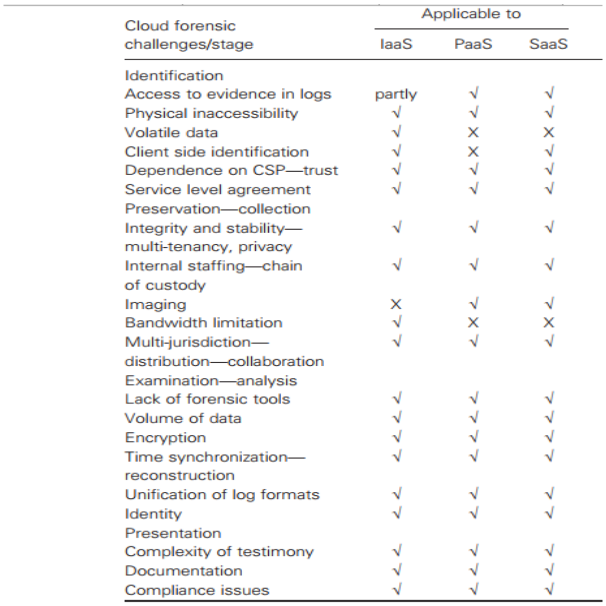
Volume of data. The data amount stored by the cloud service providers in their data centres is vast, and it increases daily. Vast data amount often produces many problems during the search for relevant digital evidence [1].

iv. Presentation stage

Complexity of testimony. Every technical acquisition information is doubtful to be easily accepted by the court of law, whereby the judge involves people with less understanding of the computer systems. The processes and every followed step by the investigator need to be thoroughly clarified. This means that the preparation of the report must be simple, clear and understandable to everyone.

Documentation.

It is challenging to convince the judge that the acquired evidence in the investigation process has been properly documented and that there are no modifications that have been made to the evidence in the stages previously followed.



Cloud forensic challenges/stage	Applicable to		
	IaaS	PaaS	SaaS
Identification			
Access to evidence in logs	partly	√	√
Physical inaccessibility	√	√	√
Volatile data	√	×	×
Client side identification	√	×	√
Dependence on CSP—trust	√	√	√
Service level agreement	√	√	√
Preservation—collection			
Integrity and stability—multi-tenancy, privacy	√	√	√
Internal staffing—chain of custody	√	√	√
Imaging	×	√	√
Bandwidth limitation	√	×	×
Multi-jurisdiction—distribution—collaboration	√	√	√
Examination—analysis			
Lack of forensic tools	√	√	√
Volume of data	√	√	√
Encryption	√	√	√
Time synchronization—reconstruction	√	√	√
Unification of log formats	√	√	√
Identity	√	√	√
Presentation			
Complexity of testimony	√	√	√
Documentation	√	√	√
Compliance issues	√	√	√

Figure 4: Cloud forensic challenges overview

B. Challenges analysis.

The challenges that are fund in the cloud computing environments cannot be categorized into specific stages. Organizations and companies like brokers, banks and hospitals do not transition easily to the cloud environment due to trustworthy issues, data retention concerns as well as the laws and regulations.

In cloud forensics field, the vital task is to access logs which are evidence. Winning any investigation needs access logs presentation in a court, meaning that logs are powerful. Limited access and being controlled in the cloud will make it hard to obtain evidence before a court of law.

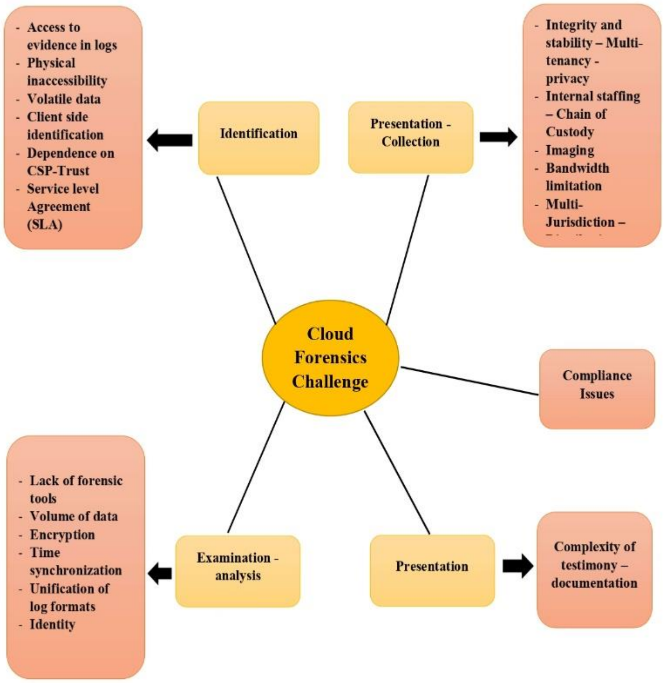

- Access to evidence in logs
- Physical inaccessibility
- Volatile data
- Client side identification
- Dependence on CSP-Trust
- Service level Agreement (SLA)
Identification
Presentation - Collection
- Integrity and stability – Multi-tenancy - privacy
- Internal staffing – Chain of Custody
- Imaging
- Bandwidth limitation
- Multi-Jurisdiction –
Cloud Forensics Challenge
Compliance Issues
- Lack of forensic tools
- Volume of data
- Encryption
- Time synchronization
- Unification of log formats
- Identity
Examination - analysis
Presentation
Complexity of testimony – documentation

Figure 5: Cloud forensic challenges

C. Cloud Forensic Solutions

Here, the possible solutions are provided to address the challenges that have been identified and analyzed. The identified solution is presented based on their stage.

i. Identification stage.

Access to evidence in logs.

Secure-logging-as-a-service refers to a cloud forensic mechanism which permits the cloud service provider to store the virtual machine's logs and make them accessible to the forensic investigators while still ensuring the confidentiality of the cloud users and information hence preservation [1]. Also, the log-based model has been proposed to help in reducing forensic complexity for the non-repudiation of the cloud user's behaviours with this model. The user keeps another log synchronously and locally so that it may help in checking SaaS activities without the CSP's interference [3] [10].

Volatile data.

Overcoming these problems will require live investigation as another approach is used for dead acquisition. Such an approach assists the investigators to collect the data. Else, they may be lost if the computer is shut down. Preventing loss of volatile data will include frequently synchronizing data between the virtual machine and the persisting storage, which is non-cloud-based [1].

ii. Preservation- collection stage

Integrity and stability of the evidence caused by the privacy of the data and multi-tenancy nature of the data. Integrity validation will need digital signatures on the evidence being collected. The digital signatures must be generated and checked. Alternatively, the role-based scheme will allow for the access control based on the roles to be enforced for the data that are encrypted and stored on the public cloud.

Chain of custody. The most effective solution is internal staffing whereby the CSP customer collaboration and assistance with specified roles from the external are trained, new laws are established, specialized tools and new methodologies are established. Ensuring chain of custody needs qualified experts in forensic investigations. Finally, an organization's policies and SLAs that are legally binding need to be documented, communicated and collaborated in regards to forensic activities [1].

iii. Examination, the analysis stage

Lacking forensic tools. There is a need for tools that will identify, collect and analyses the data. PORs tool guarantees privacy and files integrity. En-Case and Accessdata FTK tools are important in the acquisition of evidence and ensure trust which is needed.

Volume of data. The suggested solution is the use of a public cloud which stores and provides evidence; however, the method has legal and technical issues. There is a need to develop new methods to deal with data volumes according to acceptable forensic principles [7].

iv. Presentation stage

Complexity of testimony. Using interactive presentations and virtualized environments will allow for data set exploration with a focus on the relevant data. Also, there is a need for the experts to present the evidence for a proper explanation of the investigation reports.

Documentation. There must be detailed documentation which provides the person involved in the investigation process, the precise steps taken while ensuring that the evidence is still intact. Every possible gap must be filled while uncertainties concerning the semantics and data interpretation and collection mechanisms limitation are done alongside actual data [2] [1].

4. CONCLUSION

Apart from the obvious merits, cloud computing complexity gives a place for malicious users to perform several criminal activities. The methodologies, the challenges and the solutions having been identified and proposed, it will help make the cloud computing environments more secure to the users and information.

The designs and development processes of trustworthy soft wares and services for the cloud environments will play a vital role in modern internet use, which is risks and needs deliberate protection of users and their data. The designing and implementation of the cloud services will assist in the investigation and conducting of cyber-crime investigations in more efficient ways which raise users' trustworthiness and security of the systems also.

5. FUTURE WORK

There is a need to continue with the research and to develop more helpful models that ensure that the security and privacy of data and users are always a priority which is met. The solution on how to deal with data volume needs to be researched and developed to enhance the security of the big data as well as ensuring that the users find it friendly to engage big data.

References

[1] C. K. S. G. Stavros Simou, "A survey on cloud forensics challenges and solutions," *SECURITY AND COMMUNICATION NETWORKS,* pp. 1-31, 2016.

[2] Jaber, A. N., Zolkipli, M. F., Shakir, H. A., & Jassim, M. R., "Host based intrusion detection and prevention model against DDoS attack in cloud computing," *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. Springer, Cham,* pp. 241-252, 2017, November.

[3] Jaber, A. N., & Rehman, S. U, "FCM–SVM based intrusion detection system for cloud computing environment," *Cluster Computing,* pp. 1-11, 2020.

[4] S. Alqahtany, "Cloud Forensics: A Review of Challenges, Solutions and Open Problems," *Centre for Security, Communications and Network Research,* 2015.

[5] C. K. E. K. S. G. Stavros Simou, "Cloud Forensics Solutions: A Review," *Cultural Informatics Laboratory, Department of Cultural Technology and Communication,* pp. 300-310, 2020.

[6] Hussein, M. K., Zainal, N. B., & Jaber, A. N, "Data security analysis for DDoS defense of cloud based networks," *In 2015 IEEE Student Conference on Research and Development (SCOReD). IEEE.,* pp. 305-310, 2015.

[7] V. Geetha, "About Cloud Forensics: Challenges and Solutions," *International Journal of Distributed and Cloud Computing,* pp. 1-8, 2015.

[8] A. M. Poorvi Jain, "Review of Cloud Forensics: Challenges, Solutions and Comparative Analysis," *International Journal of Computer Applications,* pp. 28-34, 2019.

[9] M. I. Martin Herman, "NIST Cloud Computing Forensic Science Challenges," *National Institute of Standards and Technology,* pp. 10-70, 2020.

[10] T. S. W. B. G. GEORGE GRISPOS, "Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics," *nternational Journal of Digital Crime and Forensics, ,* pp. 28-48, 2012.

[11] D. K. Gayatri Pandi, "CLOUD FORENSIC FRAMEWORKS, CHALLENGES, STATE OF ART AND FUTURE DIRECTIONS," *Journal of Emerging Technologies and Innovative Research,* pp. 712-719, 2018.

[12] Y. I. A. J. Sameera Almulla, "A STATE-OF-THE-ART REVIEW OF CLOUDFORENSICS," *The Journal of Digital*

Forensics, Security and Law , pp. 7-14, 2014.

[13] C. K. Stavros Simou, "Towards the Development of a Cloud ForensicsMethodology: A Conceptual Model," *International Publishing Switzerland* , pp. 470-481, 2015.