# Cloud Forensics: An overall research perspective

M.Patidar[1*], P. Bansal[2]

[1*]Department of Information Technology, Institute of Engineering & Technology, Davv, Indore, India
[2] Department of Information Technology, Institute of Engineering & Technology, Davv, Indore, India

e-mail: madhurpatidar15@gmail.com, pratosh@hotmail.com

**Corresponding Author: madhurpatidar15@gmail.com, Tel.: +91-98930-54954*

***Abstract—*** We are aware that Cloud Computing, is a transformative and promising field for next generation computing on account of its several economic benefits in every domain including commercial, public, governmental, organizational etc. However on account of increase in the digital crimes and a number of security threats over the cloud environment, works related with investigations over cloud, recovering of evidences and systematic forensics methodologies need to be focused upon. Cloud Forensics is a relevant field that works on all of these issues. This paper gives an overall research perspective of Cloud Forensics including its overview, need, process, challenges, logging measures and forensic tools. With the help of certain forensic tools, cloud investigation processes have been eased. On the other hand, there are certain challenges encountered in the cloud forensics domain. The paper also gives an insight regarding the broad future scope and areas associated in the field of Cloud Forensics.

***Keywords—*** Cloud Computing; Security; Digital Forensics; Cloud Forensics, Logs, Digital Investigation.

## I. INTRODUCTION

Cloud Forensics refers to that area of cloud computing in which the research is mainly done focusing on the ways on revealing how a digital crime might have happened over the cloud. For example, determining the causes behind different kinds of attacks like ddos etc happening over the cloud. Although cloud computing technology is increasingly being adopted by organizations, still there are concerns related with the security and increasing crimes over the cloud. Hence, the use of cloud forensics plays a significant role over here. It can be referred to as a cross discipline of cloud computing mechanisms and digital forensics procedures. Certain investigations are being performed over the cloud to comply with the digital forensics procedures of identification, preservation, collection and analysis of evidentiary data to make it presentable in court of law. Hence, proper selection of tools and frameworks is required for the investigation process over cloud to keep it in pace with the advanced and continuously changing computer technologies [1].

The paper is organized in the following manner: Section I gives an introduction to the field of Cloud Forensics. Section II highlights the need of cloud forensics. Section III gives a brief overview of its process. Section IV explains the current challenges in the field of Cloud Forensics, Section V gives a view of logging measures available, Section VI gives an insight of the forensic tools available for investigation process and finally Section VII marks the end of the paper with the conclusion and future work to be carried out.

## II. NEED OF CLOUD FORENSICS

On account of several security threats that may affect cloud networks, there is an essential requirement for certain measures to overcome the same. As digital forensics is a continuously growing field providing set of tools that helps in reconstructing certain events in the transactions and gives accurate information provable in the court of law, the same can be applied over the cloud to achieve productive results. Cloud Forensics is the area that deals with the same [2].

Table 1 gives an overview of the threats for the cloud services consumers which have been categorized as per the confidentiality, integrity and availability (CIA) security model and the relevance of the same to all of the delivery models of cloud services [3].

Table 1. Cloud Security Threats

| Threat | Description |
|---|---|
| **Issue : Confidentiality** | |
| **Internal User Threats:**<br>• CSP's malicious intent<br>• Customer's malicious intent<br>• Malicious intentions of third party users in support of either of them. | Insider's threat can be greater as compared to others as multiple internal users can be introduced through each of the delivery models. At different layers; it can be summarized as:<br>• SaaS : customers and the respective administrators<br>• PaaS : Developers of applications and the environment managers involved in testing<br>• IaaS : Platform Consultants from third party. |
| **External User or attacker's threats:**<br>• Attack on software of cloud infrastructure remotely.<br>• Attack on software of | These threats can be perceived to be applicable more towards the public clouds or the Internet. However all kinds of cloud models are affected by the same. For example, Private clouds where the endpoints of the users are being targeted. Real time examples of those affected includes cloud |

| | |
|---|---|
| cloud applications remotely.<br>• Attacks on both software and hardware remotely against cloud user organizations. | providers having huge data stores containing sensitive government properties information or any other personal information with an attempt to retrieve data. Other examples include attacks by the dedicated attackers, known to be supply chain attacks, social engineering attacks etc. |
| **Data leakage:**<br>• It includes security access rights failure among multiple domains.<br>• Any physical transportation system failure used for back up purposes. | The data leakage threats can be caused amongst organizations that use same cloud providers and can be caused due to errors by humans or hardware faults leading to compromise of information. |
| **Issue: Integrity** | |
| **Data Segregation:**<br>• It includes security perimeters defined incorrectly.<br>• Improper configuration of VM's and hypervisors. | If the resources are segregated, there could be a threat to the integrity of data in case of cloud hosting environments such as SaaS. |
| **User Access:**<br>• Includes poor identification and lack of access management processes. | If there tends to be poor access management or control processes, it causes many threat probabilities. For example, if any cloud organization's ex- employee maintains some kind of remote access to the cloud services, there may be chances of any purposeful damage to the data. |
| **Data Quality:**<br>• Includes any defective application or faulty infrastructural components. | With increase in the customer's data, the data threat to its quality degradation increases. Moreover any wrongly configured application or component that may be required by another cloud user can potentially affect data integrity for the users sharing the cloud infrastructure. |
| **Issue: Availability** | |
| **Change management:**<br>• Includes penetration testing measures which may impact other cloud customers<br>• Also any infrastructural changes with respect to cloud providers, third party systems impacting customers. | Change management is an important responsibility of the cloud providers and hence can introduce negative effects among cloud delivery models. Changes in existing cloud services including hardware and software can be responsible for it. |
| **Denial Of Service Threat:**<br>• Affects services over network bandwidth.<br>• Affects application, data and network DNS. | Denial Of Service threats are generally external threats affecting public cloud services. However all cloud service models can be impacted as hardware and application components causing denial of services can be introduced by internal and external threat agents. Hence these ;denial of service threats greatly affect cloud customers. |
| **Physical disruption:**<br>• Includes cloud provider's IT services disruption by means of physical access<br>• Includes cloud customer's IT services disruption by means of physical access.<br>• Includes services of third party WAN providers disruption. | Physical disruption threat can be easily applicable on cloud user infrastructure in the case where the working is remote or the office environments are less secured. |
| **Weak Recovery procedures:**<br>• Lack of proper mechanisms for disaster recovery and business continuity. | In order to implement proper recovery measures, in house systems along with business continuity measures adopted by third party cloud service providers must be taken care. In case of improper testing of these procedures, recovery time impact can be significant. |

## III. PROCESS OF CLOUD FORENSICS

After considering the reasons behind applying forensics, types of services and technology type of cloud to be used, the process of cloud forensics can be summarized as follows:

- Identification process involves determining the sources of evidences in the cloud environment at various physical and logical areas such as client side, server side etc.

- Collection & Preservation process involves collecting evidences and preserving it so as to maintain its integrity through measures like duplicity of evidences etc. Also, evidence's chain of custody maintenance is being focused upon.

- Examination process that involves usage of certain tools to extract relevant information from the evidences obtained.

- Presentation process involving a proper documented report to be presented in the court of law based on the evidence analysis [4].

## IV. CHALLENGES IN CLOUD FORENSICS

Cloud Forensics as a domain has a number of challenges. Some of the important ones can be illustrated as below:

- **Forensic data collection:** In SaaS, checking the status of system and the log files becomes difficult because the client access is restricted to a very little domain i.e. either to the pre defined interface or the API's. This is not the case with IaaS where the involvement of VM's is there that acts like an actual machine. Moreover, from the CSP's side also there are not any services for logs gathering and in some cases they hide the details intentionally.

- **Physical Inaccessibility:** In cloud forensics, the data being stored in distributed forms, so the possibility of seizing the hardware containing data becomes very difficult. Also, determining location of data is difficult on account of distribution of hardware devices geographically.

- **Volatile Data:** There may be loss of evidences such as temporary files, processes, entries of registries etc once the VM is turned off. So in any case of attacks by adversaries, after the attack being completed, the attacker can take advantage of the same by shutting down the VM instance which leads to a complete eradication of volatile data. So this is again one of the most important challenges for cloud forensics.

- **Dependency on CSP's:** In all the three models of cloud, especially in SaaS, we need to depend on the cloud providers for the identification, preservation and collection of the evidences helpful in reaching to the causes behind the crimes. Also there is some linking of CSP's with other CSP's for use of certain services. Hence, to perform the investigation efficiently, the chain of custody has to be considered significantly. As far as this challenge is concerned, it affects all stages for forensics such as identification, preservation and collection.

- **Service Level Agreements (SLA):** SLA's are one of the important aspects between a provider and a customer. Surprisingly, many important concerns regarding forensics investigations are not included in the same. The reasons may be due to lacking of CSP transparencies, boundaries of trust, less awareness regarding customers, neglecting international regulations etc. From the CSP's side there is no transparency on account of reasons like less knowledge regarding investigation of crimes and may be the techniques followed by them are inappropriate in context to cloud environments. Also it becomes difficult for the customer to rectify if the CSP's are adhering to their agreement. For e.g.- deletion of all data of customer after the expiration of the contract.

- **Evidence Segregation:** As we know, in a cloud environment, a single physical machine allows different virtual instances running over it which are isolated through virtualization. The customer instances do not have access to the physical disk devices rather can access only virtualized disks. So the challenge here includes CSP's to keep apart the resources among the tenants sharing the infrastructure during the investigation purposes so as to maintain the security principles such as confidentiality [5, 6].

## V. LOGGING IN CLOUD FORENSICS

Log collection and management is an important aspect and is very crucial for supporting forensic analysis processes and detecting any kind of suspicious behaviors. Certain challenges related with logging analysis in cloud forensics include logs decentralization, logs volatility, non existence and accessibility issues concerned with logs and lastly lack of any critical or productive information in the logs obtained. Investigation over cloud may be difficult due to the fact that logs and data may be spread over constantly changing data centers and hosts. The log records must contain certain essential fields such as session Id, timestamp, severity etc. At different layers, we can propose logging in the following manner.

- **SaaS**: In this, an agent should be used by the consumer for sending the commands over SaaS which will process them and send responses back in form of logs. The agent may also provide its own logs along with that. The summary of the same will also be recorded such as timestamps and ids. For the authentication and verification of logs, we can apply certain HASH algorithms.
- **PaaS**: At this layer, the third party shall receive a log module from CSP's. The third party can also create customized modules for logs and then can further perform the forensic investigation processes.
- **IaaS**: For this layer, VM's are the only important sources for logs retrieval and investigations. Outside VM's, there is a little scope for logging procedures.

There are different categorizations in the context of logging processes such as:

- **Business**: It includes logs relevant to business. Examples include monitoring SLA's, identifying currently used features etc.

- **Operational**: It includes any kind of errors, critical conditions related to system and applications.
- **Security**: It relates with the security related concerns such as authentication, authorization etc. For the logging process of the same, certain security tools will prove beneficial.
- **Compliance**: It is concerned with the logging in context to regulatory and compliance issues [7,8,and 9].

## VI. CLOUD FORENSICS TOOLS

Some of the tools used for investigations over cloud environment include EnCase, Forensic Tool Kit, F-Response Tool, Belkasoft Evidence Center, Oxygen Forensic Extractor etc [10]. On based of research, following two tools have been found popular and most effective for investigations based on cloud forensics.

- **Forensics OpenStack tools** (**FROST)**: It is an OpenStack cloud platform. Mainly useful in case of IaaS. Helps in determining different logs such as firewall logs, API logs, virtual disks logs etc.

- **UFED Cloud Analyzer**: This tool is very useful in case of extracting data from social media platforms like Facebook, Twitter etc. Helps in providing storage for files and also other means that helps in fastening the investigation process. Other features of the tool include extraction based on specific entities such as usernames, preservation of the data extracted etc [11].

## VII. CONCLUSION AND FUTURE SCOPE

Cloud Forensics is a continuously growing field and will keep on growing, keeping in view the rapid pace of technology development. As discussed in section IV, there are certain challenges in the field of cloud forensics that needs to be worked upon. The paper highlighted an overall research perspective for the current and most evolving field i.e. Cloud Forensics. Developments in the fields will definitely ease the process for the investigators and security professionals.

In future, we plan to explore and focus on certain open areas to be focused upon. Some of them include the following points:

- Cross border issues need to be overcome.
- Difficulties in context to logging of data mainly reviewing, correlation and policy monitoring.
- Proper control over cloud data, dependencies on cloud service provider and certain legal issues.

## REFERENCES

[1] S. Alqahtany, N. Clarke, S. Furnell, and C. Reich. "*Cloud forensics: a review of challenges, solutions and open problems*." In Cloud Computing (ICCC), 2015 International Conference on pp. **1-9**. IEEE, **2015**.

[2] D. Shirkhedkari, and S. Patil. "*Design of digital forensic technique for cloud computing*." International Journal of Advance Research in Computer Science and Management Studies 2, no. 6 (**2014**).

[3] J. Sen, "*Security and privacy issues in cloud computing*." Architectures and Protocols for Secure Information Technology Infrastructures (**2013**): **1-45**.

[4] S. Simou, C. Kalloniatis, E. Kavakli, and S. Gritzalis. "*Cloud forensics: identifying the major issues and challenges*." in International Conference on Advanced Information Systems Engineering, pp. **271-284**. Springer, **Cham**, **2014**.

[5] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie. "*Cloud forensics*." in IFIP International Conference on Digital Forensics, pp. **35-46**. Springer **Berlin Heidelberg**, **2011**.

[6] D.Lillis, B. Becker, T. O'Sullivan, and M. Scanlon. "*Current Challenges and Future Research Areas for Digital Forensic Investigation*." arXiv preprint arXiv:**1604.03850** (**2016**).

[7] T. Sang, "*A log based approach to make digital forensics easier on cloud computing*." in Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on, pp. **91-94**. IEEE, **2013**.

[8] R. Marty, "*Cloud application logging for forensics*." in Proceedings of the 2011 ACM Symposium on Applied Computing, pp. **178-184**. ACM, **2011**.

[9] S.Thorpe, T. Grandison, and I. Ray. "*Cloud Computing Log Evidence Forensic Examination Analysis*." in Proceedings of the 2nd International Conference on CyberCrime, Security and Digital Forensics, **2012**.

[10] D.R. Rani, and G. Geethakumari. "*A meta-analysis of cloud forensic frameworks and tools*." in Power, Control, Communication and Computational Technologies for Sustainable Growth (PCCCTSG), 2015 Conference on pp. **294-298**. IEEE, **2015**.

[11] S. Naaz and F.A. Siddiqui. "*Comparative Study of Cloud Forensics Tools*." Communications on Applied Electronics (CAE) ISSN: **2394-4714**.