www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-2, April 2018
Review Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

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

Received: 20/Mar/2018, Revised:06 /Mar/2018, Accepted: 18/Apr/2018, Published: 30/Apr/2018

***Abstract*—** We are aware that Cloud Computing evolves as a transformative and potentially helpful field for future generations 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 the cloud, recovering of evidence 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 with the Cloud Forensics area.

***Keywords*—** Digital Forensics; Cloud Computing; Security; 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 to 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 an integrated 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 the court of law. Hence, proper selection of tools and frameworks is required for the investigation process over the cloud to keep it in pace with the advanced and continuously changing computer technologies [1].

The organization of the paper is in the following manner: Section I contains an introduction to Cloud Forensics. Section II contains the related work of various authors in the field of Cloud Forensics. Section III contains the need and requirement of Cloud Forensics. Section IV contains a brief overview of its process. Section V explains the current challenges in the field of Cloud Forensics, Section VI describes the logging measures available in the respective domain of Cloud Forensics, Section VII explain the forensic tools available for investigation process and Section VIII concludes the research work with the future perspectives and open areas.

II. RELATED WORK

Research identifying works associated with Cloud Forensics have been proposed by several authors. Authors Saad Alqahtany, Nathan Clarke, Steven Furnell, and Christoph Reich highlights the open problems and the technological advancements required in the investigation process over cloud [2]. Authors Deoyani Shirkhedkar and Sulabha Patil focus on the importance of digital forensics techniques and methodologies for solving crime-related cases over cloud environment [3]. Authors B. Sumitra, C. R. Pethuru, and M. Misbahuddin explain several authentications, privacy and security-related concerns with context to Cloud Computing [4]. Authors Stavros Simou, Christos Kalloniatis, Evangelia Kavakli and Stefanos Gritzalis emphasizes the vitality of Cloud Forensics in today's real world scenario [5]. Authors Keyun Ruan, Joe Carthy, Tahar Kechadi, and Mark Crosbie brings out some of the key challenges faced as a part of investigation procedures in Cloud Forensics [6]. Author Raffael Marty highlights the importance of logs extraction and methods for the same in the forensics process involved over cloud [7]. Authors Deevi Radha Rani and G. Geethakumari give an overview of some of the forensic tools that are helpful in the recovering of evidence over cloud environment and hence useful in Cloud Forensics domain [8]. By analyzing the above research works by several

authors, we inferred that there is a need for awareness regarding Cloud Forensics field among people. As with the continuous increase in enterprises and organizations shifting towards the cloud, Cloud Forensics will play a key role in resolving issues and evidence recovery owing to certain security breaches and malware attacks over the cloud domain.

III. 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 a set of tools that help 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 domain that deals with the same aspects on account of several security threats and concerns over cloud environment [9].

Table 1 gives an insight of the threats prevailing to the cloud services consumers which have been categorized as per the security model of three of the main principles which are Confidentiality, Integrity, and Availability (CIA) and the significance of the same to all of the delivery models of Cloud Computing services.

Table 1. Cloud Security Concerns

Concern	Description
Issue : Confidentiality	
Internal User: • CSP's malevolent intent • Customer's malicious intent • 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: • SaaS : customers and the respective administrators • PaaS : Developers of applications and the environment managers involved in testing • IaaS : Platform Consultants from third-party.
External User or attacker's threats: • An Attack on software of cloud infrastructure remotely. • An Attack on software of cloud applications remotely. • Attacks on both software and hardware remotely against cloud user organizations.	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 include cloud 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: • It includes security access rights failure among multiple domains. • 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: • It includes security perimeters defined incorrectly. • Improper configuration of VM's and hypervisors.	If the resources are segregated, there could be a potential threat to the data integrity in cases of platforms or environment like SaaS which are providing cloud hosting.
User Access: • 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: • Includes any defective application or faulty infrastructural components.	With an increase in the customer's data, the data threat to its quality degradation increases. Moreover, any wrongly configured application or component that may be used by other users of cloud can also significantly affect data correctness for the users sharing the cloud infrastructure.
Issue: Availability	
Change management: • Includes penetration testing measures which may impact other cloud customers • 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: • Affects services over network bandwidth.	Denial Of Service threats, generally known as external threats are affecting public cloud services. However, all cloud service models can be impacted as hardware and application components causing the denial of

• Affects application, data and network DNS.	services can be introduced by internal and external threat agents. Hence these; denial of service threats greatly affect cloud customers.
Physical disruption: • Includes cloud provider's IT services disruption by means of physical access • Includes cloud customer's IT services disruption by means of physical access. • Includes services of third-party WAN provider's disruption.	Physical disruption threat can be easily applicable to cloud user infrastructure in the case where the working is remote or the office environments are less secured.
Weak Recovery procedures: • 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.

IV. 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 evidence in the cloud environment at several areas including logical, physical etc such as client side, server side etc.
- Collection & Preservation process involves collecting evidence and preserving it so as to maintain its integrity through measures like duplicity of evidence 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 evidence obtained.
- Presentation process involving a properly documented report that needs to be shown in court of law based on the analysis of recovered evidence [10].

V. 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 the system and the log files becomes difficult because the client access is restricted to a very little domain i.e. either to the predefined 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 are responsible for intentionally hiding the details.
- **Physical Inaccessibility:** Cloud forensics involves data being stored in distributed forms, so the possibility of seizing the hardware containing data becomes very difficult. Also, determining the location of data is difficult on account of the distribution of hardware devices geographically.
- **Volatile Data:** There may be a loss of evidence 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 is completed, the attacker can take advantage of the same by shutting the VM which leads to absolute eradication of continuously changing or 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, specifically in SaaS, there is an inherent dependency 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 significant. As far as this challenge is concerned, it affects all stages of forensics such as identification, preservation, and collection.
- **Service Level Agreements (SLA):** SLA's are one of the important aspects of 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 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 the 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.

- **User's Incompetent Skills**: There may be many clients or users involved in the cloud environment that may not be technically skilled like the administrators. As a result, there may be unawareness regarding forgeries and crimes related with cyber world among these users. In such cases, the absence of proper periodic reviews can affect the user's cloud because of such suspicious activities. As a result, forensic process becomes more time-consuming and gets affected.

- **Other Challenges:** These include lacking proper certified, automated and tested tools and frameworks, imaging of complete physical media, integration of a large number of evidence, different time zones evidence, location issues as data may be stored at different geographical locations, more expenses as compared to traditional forensics, security concerns with remote access from any compromised machine, improper collaboration of the service provider with forensic investigator, security principles being compromised etc [11,12].

VI. 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 behaviours. Certain challenges related to 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 centres 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 to 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 [13, 14].

VII. CLOUD FORENSICS TOOLS

Some of the tools used for investigations over cloud environment include EnCase, Forensic Tool Kit, F-Response Tool, Belkasoft Evidence Centre, Oxygen Forensic Extractor etc. On base 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 used in case of IaaS. It helps in determining different logs such as firewall logs, API logs, virtual disks logs etc. Its main components include virtual disk image, API requests logs and firewall logs of OpenStack. The main advantage of this tool is that it helps the forensic investigators in extracting data from the Cloud of OpenStack without any requirement of interaction with the service provider. Its advantage includes support provided to a large number of users at a time. On the other hand, it is useful mainly at IaaS layer as this layer provides more control to the users of cloud. For other layers PaaS and SaaS, developments still need to be performed in the OpenStack framework.

- **UFED Cloud Analyzer**: This tool is very useful in case of extracting data from social media platforms like Facebook, Twitter etc. It 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 [15].

VIII. CONCLUSION AND FUTURE SCOPE

Cloud Forensics is an emergent field and will keep on growing, keeping in view the rapid pace of technological development and involvement of Cloud Computing domain, plausibly one of the most discussed topics today. However, there are certain challenges in the field of cloud forensics that needs to be resolved upon. Applying the procedures of digital forensics for investigations over cloud will require an expertise in the respective domain along with the use of advanced technologies for evidence extraction. 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 work on some real world scenarios and analyze certain open areas in the respected field that needs to be focused upon. Some of these areas include the following:

- Cross-border issues related data storage over Cloud needs to be resolved as it poses certain difficulties for a Cloud Forensics Investigator.
- Difficulties in context to logging of data mainly extraction, reviewing, correlation, integrity maintenance, and policy monitoring so proper log management system need to be designed.
- Dependencies on Cloud Service Provider (CSP) need to be minimized on account of data privacy and leakage issues and therefore proper solutions need to be implemented for the same.
- As per the latest Cloud Security Report 2018, certain legal policies and compliance processes also hinders the Cloud Forensics investigation process and hence needs to be looked upon.
- Forensic tools that are technologically advanced properly tested and certified needs to be taken into consideration for the investigation processes.

ACKNOWLEDGMENT

The authors are sincerely thankful to their University for providing them the platform and necessary financial support for the purchase of some digital forensic tools that helped in research and testing works over the cloud environment.

REFERENCES

[1] A. Ghafarian, "*Forensics analysis of cloud computing services*." In IEEE Science and Information Conference (SAI), 2015, pp. 1335-1339, 2015.

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

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

[4] B. Sumitra, C. R. Pethuru, and M. Misbahuddin. "A survey of cloud authentication attacks and solution approaches." *International journal of innovative research in computer and communication engineering* 2, no. 10,pp. 6245-6253, 2014.

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

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

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

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

[9] S. Kathuria, "*A Survey on Security Provided by Multi-Clouds in Cloud Computing*" In International Journal of Scientific Research in Network Security and Communication, Vol.6, Issue.1, pp.23-27, 2018.

[10] E.Casey, "*Digital evidence and computer crime: Forensic science, computers, and the internet.*" ,USA, Academic press, Elsevier Inc Publication, pp 189-190, 2011.

[11] D.Lillis, Brett Becker, Tadhg O'Sullivan, and Mark Scanlon. "*Current challenges and future research areas for digital forensic investigation*." In Annual ADFSL Conference on Digital Forensics, Security and Law, 2016.

[12] A.Burney, M.Asif, and Z.Abbas. "*Forensics Issues in Cloud Computing*." In Journal of Computer and Communications 4, no. 10,2016.

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

[14] 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.

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

Authors Profile

Mr. Madhur Patidar has completed his Bachelor of Engineering (B.E.) in Information Technology from Institute of Engineering & Technology(IET), DAVV, Indore in the year 2013 and Master of Engineering (M.E.) in Information Technology with specialization in Information Security from the same college in the year 2017. He has an industrial experience of about 1.5 years and

has a teaching experience of about 2.5 years. Currently, he is working as an Assistant Professor in Medicaps University, Indore. He has presented one paper at an International Conference to be published in Springer. His main research work focuses on Cloud Computing, Digital Forensics, Cyber Security, Cloud Forensics etc.

Dr. Pratosh Bansal is currently a Professor in the Department of Information Technology of Institute of Engineering & Technology(IET), DAVV, Indore. He has more than 15 years of teaching experience and many students are currently pursuing Ph.D. under his guidance. He completed his graduation in Mechanical Engineering from Govt Engineering College, Jabalpur and completed M.Tech and Ph.D. in Computer Engineering. He handles various responsibilities at the university level and is the director of IQAC, Professor In-charge of Civil Engineering Department, Incubation Centre, CSI Student Chapter etc at IET DAVV, Indore. He has contributed many research papers at various journals and conferences. His area of interests includes E-Commerce, Cloud Computing, Digital Forensics, ERP, Green IT etc.

