IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 12, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912007 |

Cloud Forensics and its Dimensions

Dr. Kalyan Bamane [1], Aniket Gulwade [2]

Assistant Professor, Dept. of I.T., DYPCOE Akurdi, SPPU University, Pune (MH)- India[1]

Software Engineer, Trimble Inc, Pune (MH)- India[2]

ABSTRACT: Distributed computing takes a shot at the wide system, which spreads around the world. Consequently, Cloud Forensics can be seen as a subset of Network Forensics. The center system still stays as the digital legal examination of the system. Be that as it may, when the information is erased, it turns into the essential wellspring of proof in advanced crime scene investigation. In Cloud Forensics, it will be a test to recoup the erased information, distinguish information proprietor, and utilize that information for occasion remaking. The cloud specialist co-ops (CSPs) and the clients presently can't seem to actualize cloud legal capacities which will bolster the examination in the event that if any assault has occurred or information robbery happens. This execution requires fundamental comprehension of cloud legal sciences specialized issues, difficulties, devices and innovations. The CSP's must establish methods, define, implement and establish the support using the forensic capabilities for investigation of the cybercrime, the three dimensions of the cloud forensics includes the cloud based technological dimension, cloud sourced organizational dimension and legal complexity based jurisdictional dimension.

KEYWORDS: cloud computing system (CCS); Cyber forensics; Cloud Forensic Techniques; Cloud Computing ecosystem

I. INTRODUCTION

In cloud computing system (CCS), has the three provision models have three confronts exclusive to cloud forensics. Each service facility form level for CCS shares inequitable liability with the CSP. This association grounds sole confronts when conducting cloud cyber forensics inspections, as any catastrophe can thwart proof from being tolerable in a patio of ruling. Due to hybrid CCS multi-tenancy servers, data is residing in the multiple data centers set in various countries jurisdiction this poses the legal jurisdictional challenges. As may CSP's may not always operate in the favor of users for conducting forensic investigation, as it consume time, money, computing resources for issues which bothers them least. In cyber cloud computing systems the users are victims of the cybercrime over Internet, as cloud is Internet based computing engine. Cyber forensics is still evolving, it is right time to implement it for investigating the criminal activities over cloud, which assists users to pay their attention in fighting and thwarting the criminal and illegal activities committed over the cloud, which cause the harm to users computing resources and his business, due to increasing in the cloud security risks are expanding in day-by-day exponentially at infinite speed.

II. RELATED WORK

This section describes few of the available cloud forensics process and tools. The paper "A Comparative Analysis of Cloud Forensic Techniques in IaaS " by Palash Santra, Asmita Roy and Koushik Majumder presented the cloud forensic process presented in figure 2. The paper "An Analytical Comparative Approach of Cloud Forensic Tools during Cyber Attacks in Cloud", SocProS 2017, Volume 2, presents the cloud forensics steps presented in figure 1

Figure 1 Cloud forensic steps

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912007 |

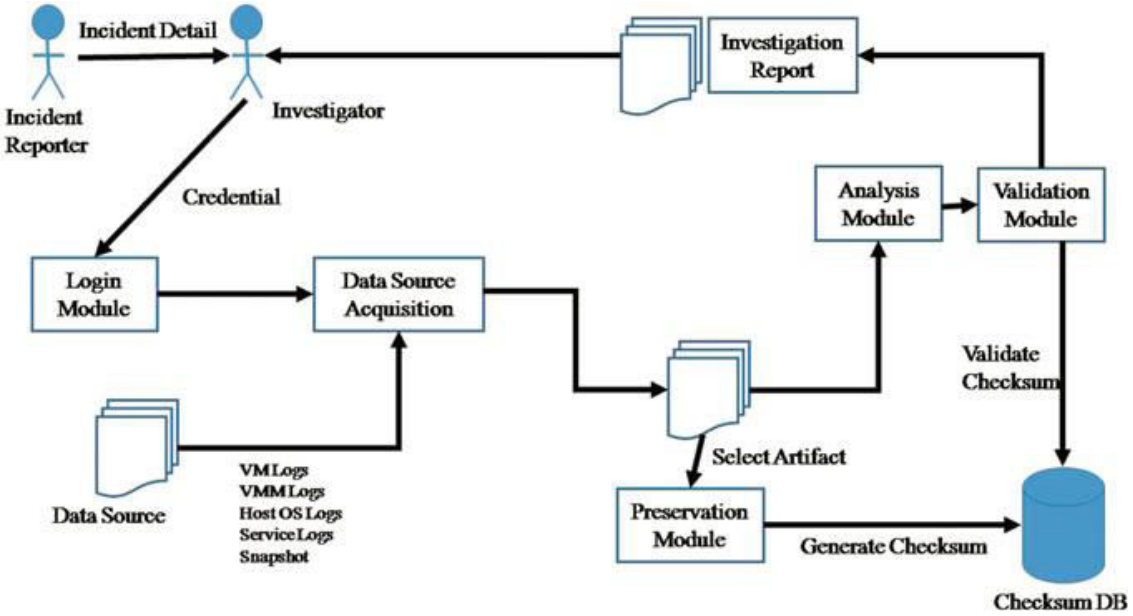

Figure 2 Cloud forensic process

The authors also present the list of popularly available tools some of them are Digital forensics frameworks, Open computer forensics architecture, CAINE, X-Ways forensics, SANS investigative forensics toolkit (SIFT), Encase, Registry recon, Sleuth Kit (+Autopsy), Libforensics, Volatility, Windows SCOPE, Corner's toolkit, Oxygen forensic suite, Bulk extractor, Xplico, Mandiant Redline, Computer online forensic evidence extractor (COFEE), P2eXplorer, PlainSigh, XRY, HELIX3, Cellebrite UFED, FTK imager, DEFT, and Bulk extractor. Forensic tools summary presented in table 1.6. The FROST and UFED analyzer has also been discussed.[7]

Table 1 forensics tools in 2019 for cloud applications

Sl.No.	Tools	Description and Applications
1.	SANS SIFT	The SANS Investigative Forensic Toolkit (SIFT) is an Ubuntu-based Live CD which includes all the tools you need to conduct an in-depth forensic or incident response investigation.
2.	ProDiscover Forensic	ProDiscover Forensic is a powerful computer security tool that enables computer professionals to locate all of the data on a computer disk and at the same time protect evidence and create quality evidentiary reports for use in legal proceedings.
3.	Volatility Framework	The Volatility Framework was released publicly at the BlackHat and based on years of published academic research into advanced memory analysis and forensics.
4.	The Sleuth Kit (+Autopsy)	The Sleuth Kit is a collection of command line tools that allows us to analyze disk images and recover files from them. It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.
5.	CAINE	CAINE (Computer Aided Investigative Environment) is a Linux Live CD that contains a wealth of digital forensic tools. It provides updated and optimized environment to conduct a forensic analysis and Semi-automatic report generator.
6.	X-Ways Forensics	X-Ways Forensics is an advanced work environment for computer forensic examiners. X-Ways Forensics is efficient to use, not a resource-hungry, often runs faster, finds deleted files and offers many features that the others lack. X-Ways Forensics is fully portable, runs off a USB stick on any given Windows system without installation.
7.	Xplico	Xplico is a network forensics analysis tool, which is software that reconstructs the contents of acquisitions performed with a packet sniffer such as Wireshark, tcpdump, and Netsniffing. Xplico is able to extract and reconstruct all the Web pages and contents like images, files, cookies, and so on.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912007 |

III. CLOUD FORENSIC DIMENSIONS

A. Cloud based technological dimension –

The Cloud based technological dimension insists the tools to execute the cyber forensic research investigations in Cloud Computing ecosystem. The methods includes the data gathering, assimilation, live forensics, documentation of the media, proof substantiation and segregation, in virtual and physical environment with hands-on measures. Data assimilation includes gathering data, naming and labeling the data, and documenting it.

The data embraces hosted in infra of CSP and data hosted in consumer end. This data should be time stamped assimilated at regular time intervals with snapshots. The tools and techniques vary for each cloud service deployment and model utilized to consume the cloud service From literature survey and our own research it is revealed that the forensic evident data includes the objet d'art hosted on client user premises (on premise) and CSP side artifacts hosted in the CSP infra. The methods with relevant tools and techniques followed to incorporate and assimilate the forensic records fluctuate with the cloud service replica of data accountability. The data gathering progression must safeguard the data reliability, with clear cut definite duties segregation between the end-user and CSP. This should not overlap or breach the data retention policies, rules, regulations, standard procedures, data laws, in the influence followed everywhere the information is gathered, or the data secrecy, of erstwhile multilateral tenants, data availability is compromised with the resources shared. For instance in public cloud service offerings the CSP work of art may need the data isolation of the resident while this is not required in public clouds.Due to swift elasticity and suppleness of cloud services offered and consumed the cloud forensic equipment's have to be resilient whence the cloud service resources are offered and de-provisioned based on claim. In almost all cases involve extensively scaled static as well as online live forensic tools for data capturing (inclusive of the volatile data compilation), recovery of data, inspection of proof, analysis and validation of the proof by pooling of resources, and sharing the infra, The complete progression of isolating the proof in the bulky CCS includes the complete compartmentalization, consequently the forensic measures, technology and tools devised must group the forensic data among the multiparty tenants among the various cloud service deployment and model based offerings. In cloud virtualization hypervisors, Dockers container, and server-less computing systems enquiry measures are virtually non-existent. In cloud another facade is by the data loss and its control. The cyber forensic tools, techniques, and measures must be devised to locate the physically existing forensic records with precise time-stamped data with due concern in jurisdictional issues proactive channel be able to appreciably aid cloud forensic examination. Some instance include the safeguarding the storage snapshots captured regularly, tracking the certification of access controlling systems, in addition performing the object/data –level third party level auditing and certification of the all the logs/accesses.

B. Cloud sourced organizational dimension

The cloud based technological dimension, arises whence the multiparty multilateral parties like CSP's and cloud service consumers, tenants, third parties etc and cloud service end users are involved. The cloud forensic investigation amplifies when the CSP produces and offers their designed cloud services.The CSP must correspond with third-parties for their proficiency skill in the cyber forensic Investigation with expertise in computing system infra, storage and networks security, ethical hacking activities, cloud security architects may assists forensic investigators at the cybercrime medias and scenarios.

The scope of the forensic study amplify while a CSP offers a paid services to service consumers, various cloud entities involved in the process of the cloud cyber forensics investigation processDue to more chain of dependencies in cloud applications within one another CSP and other hybrid cloud offerings due to dynamically changing cloud business. In this situation the cloud cyber digital forensic investigation is carried on each chain links of dependencies. The disruption of responsibilities co-ordination of the link, or corruption in the dependency chain amongst the involved multi-parties gives rise to serious disaster problems.

Cloud computing organizational policies, regulations, standards, roles, responsibilities, principles, procedures, POC's, and SLA's helps to facilitate the collaboration and communications among the involved 3rd parties, multi-tenants and researchers. 3rd party's helps in auditing compliance to standards, of international organizations and bodies of certifications, provide the technical expertise to conduct the effective and efficient auditing forensic investigations. To institute the cloud effective forensic capability requires affording the internal staffing, multilateral provider-tenant-end user- consumer collaboration and external assistance fulfilling the below roles are:

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912007 |

Forensic Investigators: examiners are accountable for groping cyber-criminal activities like accusation of delinquency. The investigators need to work with legal experts and exterior legal agencies based on the investigation types, with ample proficiency they should have to investigate their own infra, and other 3rd party infra with the interactions during the forensic studies.

IT experts: IT experts include cloud computing system, Inter and Intra network admin's and security experts, team of ethical hackers, admin's, cloud security architects, and other supporting technological and support staff. These IT experts assist with their specialist knowledge in holding up of investigations, by the forensic investigators in establishing the cybercrime scenarios, Medias and they assists in data assimilation.

The incident handlers: in cloud ecosystems generally responds to data loss and leakage and break in the data confidentiality violation, data integrity breach, data authenticity loss, non-availability of data through denial of service, DDOS, malicious code injections, SQL type injections, data attacks, insider/outsider attacks. The security threats and havocs should be properly categorized at all levels and spot the appropriate and relevant handles at each level.

Legal practitioner's needs to warrant and certify that no court of laws regulated rules are not violated during the forensic process investigational procedures executed. In addition the confidentiality of the customer's data other than the one victim is preserved. It is also the responsible of the cloud customer while sketching the S.L.A should envelop every bit of the legal jurisdiction of hosting the data. The legal advisors should responsibly correspond with the peripheral ruling enforcement bureau all over the forensic exploration.

C. Lawful complexity based jurisdictional facet

Performing forensic investigation activities in multi-lateral, multi tenancy, in multi-jurisdictional disputes is the top lawful concerns. In cloud forensics needs to devise the regulations, and agreements for storing the data. Maintaining the confidentiality of the co-customers using the same infra should be conserved. SLA should consists of the services type offered, technical support and restricted access granted to end user during the investigations, Trust boundaries establishment also it should clearly define the roles, duties, responsibilities of End user and CSP for carrying the forensic studies. Also define the techniques to carry out the forensic research in multilateral jurisdictional ecosystems devoid of infringing the local decree, customer data discretion, privacy preserving strategy.

An SLA should clearly define the terms, policies, guidelines that may guides the running forensic investigations, they are:

All the log details have service accessed details, techniques used etc, these details should be afford to investigation team by CSP at some point in the forensic investigations are carried out.

1. The trust boundaries, end users, service admin's roles and responsibilities amongst the CSP and service consumers must be clearly defined.
2. During the investigation, there should be no violations of rules and regulations must be permitted, and there should not be compromise on the service consumer data privacy should be permitted and it must be adhered in multi-controlled and multilateral environments. Section 1.4 describes the cloud forensic tools and technologies

IV. CONCLUSION AND FUTURE WORK

In this paper we discussed many security concerns, and issues of cloud services. We highlighted the Cyber forensic in cloud computing, cloud forensics and its dimensions, and Lawful complexity based jurisdictional facet. Also summarized the Cloud forensic process and tools, Issues and Challenges in Cloud forensics, Cloud Anti-forensics techniques in cloud computing. These issues have motivated us to look into Multi-stream and multisource logs approaches of forensic investigation of the cloud services.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 12, December 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0912007 |

REFERENCES

1. Almulla, S., Iraqi, Y. and Jones, A. (2013). Cloud forensics: A research perspective. In *9th International Conference on Innovations in Information Technology (IIT)*. Abu Dhabi: Ieee, pp.66–71.
2. Birk, D. (2011). Technical Challenges of Forensic Investigations in Cloud Computing Environments. , pp.1–6.
3. Grispos, G., Glisson, W. and Storer, T. (2011). Calm before the Storm: The Emerging Challenges of Cloud Computing in Digital Forensics. *dcs.gla.ac.uk*, pp.1–38. [online].
4. Guo, H., Jin, B. and Shang, T. (2012). Forensic Investigations in Cloud Environments. In *2012International Conference on Computer Science and Information Processing (CSIP)*. Xi'an,Shaanxi: Ieee, pp. 248–251.
5. IDC. (2010). *IDC eXchange » Blog Archive » New IDC IT Cloud Services Survey: Top Benefits and Challenges*. [online]. Available from: http://blogs.idc.com/ie/?p=730 [Accessed July 22,2013].
6. Josshua, G. (2012). Protection in the cloud: Risk management and insurance for cloud computing. *Internet Law*, 15(12).
7. Mell, P. and Grance, T. (2011). *The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technolog*. Gaithersburg, MD. [online]. Available from:
8. Ruan, K. et al. (2011). Cloud forensics : An overview. *IBM Ireland Ltd*, pp.1–16.
9. Ruan, K. and Carthy, J. (2012). Cloud Forensic Maturity Model. In *Digital Forensics and Cyber Crime*. Springer Berlin Heidelberg, pp. 22–41.
10. Trenwith, P.M. and Venter, H. (2013). Digital Forensic Readiness in the Cloud. In *Information Security for South Africa, 2013*. pp. 1–5.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details