International Journal of Digital Contents and Applications for Smart Devices
Vol. 6, No. 1 (2019), pp.1-6
http://dx.doi.org/10.21742/ijdcasd.2019.6.1.01

Cloud Computing for Analysis on Digital Forensics Challenges

Divya Vadlamudi

Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
divya.movva@kluniversity.in

Abstract

In the trendy life, there's a speedy increase within the usage of the technology. One reason of increasing the technology is usage of cloud. The mobile devices or any other technological devices mainly depend on cloud. The cloud can be accessible from anywhere. Cloud rhetorical method had introduced to assist the investigators to search out the proof once the criminal attacks the cloud and to take care of the integrity and security for the information keep within the cloud. The increasing within the criminal attacks in cloud, created the investigators to search out the most recent ways for the rhetorical investigation method. equally within the same means the criminals additionally discover new ways that to cover the supply of evidences. This causes harm to the investigation method and is named anti-forensics. to cover the sources anti-forensic techniques area unit used and analysis should be done against the anti-forensics techniques in cloud surroundings. during this paper we have a tendency to targeted chiefly on careful study on numerous challenges in cloud rhetorical and anti-forensic techniques.

Keywords: *Anti-forensics; Cloud computing; Cloud forensic; Cloud forensic challenges and Cloud forensic solutions.*

1. Introduction

In today's world computer is the main part of our life because we are doing many tasks that are impossible by the man to do within the few seconds. Computers can perform any task within the few seconds and it can give the required output in few milliseconds. The computers are equipped with the many resources that can be used by the criminals also.[1]

Computer users are increasing in the same way the criminals are increasing to destroy the data or to hide the data required by the users. According to the court of law the eye witness and digital evidences are same and there must be digital evidences when the criminal attacks on any of the computer in the wrong way. So it is very crucial to the investigators and the criminals to handle the digital evidences. When the investigators found the digital evidences of that attack then the criminals gives us counter attack of hiding the source of evidence or destroying the source of evidence.

In the cloud computing the digital forensics and opposed –forensics square measure the most half and therefore the current analysis goes on anti-forensics in cloud computing. Cloud provides United States the infrastructure with within the low value and it will be exploited by the criminals. primarily the criminals within the cloud to destroy the information or misuse the

Article history:
Received (May 13, 2019), Review Result (July 19, 2019), Accepted (September 25, 2019)

Print ISSN: 2205-8532, eISSN: 2207-4058 IJDCASD

information. When the criminals attacks the cloud surroundings then the evidences will be found in VM and cloud service supplier.

Mainly the cloud service supplier desires to confirm the user privacy and if any of the criminal attacked the various cloud information then the criminal evidences should be notable by CSP[1][2].Digital forensics is finding the evidences against the criminal event. once this digital forensics is applied within the cloud surroundings then it's known as as cloud forensics. Anti-forensics is AN attack consists of techniques and ways to destroy the supply of proofs or hide the supply of evidence [3].if the criminals use this anti-forensic techniques to cover the supply then it's terribly tough for the investigators to seek out the proof for the criminal attack. the most important usage of anti-forensic techniques is to cover the proof. primarily the cloud investigators use the anti-forensic techniques to supply the trait and consistency to the cloud [4]. Anti-forensics is incredibly necessary issue within the cloud [5].

2. CLOUD COMPUTING TECHNIQUES IN ANTI - FORENSIC

- Evidence Destruction
- Obfuscation
- Data Hiding
- Compromise integrity of evidence
- Circumvent VM Isolation

2.1 Cloud computing in Evidence destruction

When the VM is running or VM terminates then the proof is destructed. The log files of VM square measure deleted once the VM terminates. once the VM is running knowledge the info the information} files is deleted and deleting data within the VM is additionally is done. proof destruction results in VM termination and proof deletion.

2.2 Obfuscation

This technique is used to modify the logs inside VM and changing/updating the file timestamps in the volume file. Obfuscation leads to scramble the file timestamps, file header modification and alter log files.

2.3 Data hiding

Here we tend to stumble upon facet channel attacks and covert channel attacks. These attacks square measure wont to destroy the communication gap between the VM’s and destroy the vital info that VM doesn’t recognize. this will even be achieved through facet channel attack. The CSP uses completely different ways to cover {the info the knowledge the data} however the attackers will move that information from one VM to a different VM through these facet channel or covert channel by victimization some security mechanisms.

2.4 Compromise integrity of evidence

This task mainly depends upon the investigators and CSP. The evidence that cannot be handled by any of the attackers and that cannot be modified. CSP must ensure that the evidence cannot be destroyed or modified by the attacker.

2.5 Circumvent VM isolation

These can be achieved through side channel or covert channel attacks. The major usage of the cloud is because of main feature it gives us, called multi tenancy. Due to this the side channel attacks are mainly considered. Attackers may identify that the VM's are side by side then they break the communication between them and destroy the confidential information or steal the important information [10].

3. PERON AND LEGARY'S APPROACH IN ANTI-FORENSICS

They both divide the anti-forensics in four categories as destroy, hide, manipulate the evidence

Destroying the evidences:

Attacker's main aim is to destroy the evidence of the investigation process and makes it unavailable. They destroy the evidence by using software and this software can be used as an evidence for the investigators.

Hiding evidences :

Removing the evidence from visibility but not destroying it completely. Placing files in unusual places where the investigator cannot find and such hiding software may generate an evidence for investigator. Example, FIST (File system Insertion and Subversion Technique).

Eliminating evidence sources:

Here the problem is eliminating the source of the evidence. Destroying the evidence is as simple as applying wax before committing the crime. For example criminals apply the wax in order not to catch by police man. By the time when the criminal holds the gun with waxed hand, investigators think that it was a planned murder. In the same way these applications are used in the digital world.

Counterfeiting evidence:

Creating a fake version of evidence which appears to be something else.

4. CLOUD FORENSIC CHALLENGES

In these the cloud rhetorical challenges are bestowed and every one can have the particular stage. There are four stages bestowed within the cloud rhetorical method they're 1) Identification 2) Preservation Collection 3) Examination and analysis 4) Presentation.

4.1 Identification

Identification is that the primary stage; the elemental purpose is to find all doable sources that contain the effective proof within the cloud surroundings, keeping in mind the tip goal to demonstrate that the assault occurred. Investigators need to discover which kind of hardware and software had used. They additionally need to recognize the area and the cloud service provider. An investigators group ought to be shaped with the unique abilities in cloud, comprehensive of legitimate guides, talented experts and law officers. Every action that are made by the criminal and the systems and strategies used to attack are recorded and exhibit in a reported shape. As we need to go for the further procedure of investigation this stage is essential, because next following stages depend upon the proof that is delivered in the identification stage. In this they need to demonstrate that how they will move for the further investigation process and it must be reported.

4.2 Preservation-collection

Subsequent to distinctive the confirmation, the gathering and protection of the proof from the realm within the cloud. Investigators ought to be confine and save the proof to stay the employment of .These embody well trained people, apparatuses needed for the actual cloud data extraction and methodologies square measure used. The important issue is to stay up the chain of custody for the proof, legitimacy to the proof and trait for the computerized sway show within the court of law. The proof got to be all around recorded and supply integrity for any longer future changes within the proof.

4.3 Examination-analysis

Analysis includes, ready workers and specialist technicians got to examine each one of the data to find proof. Thus on come in a rhetorical examination, investigators got to acquire Associate in nursing abnormal state review of the landscape and form a system; typically, deferrals might happen once surprising nevertheless preventable problems square measure older. Examiners ought to survey beforehand older cases and getting ready set ups to find styles that may facilitate to scale back preservation-collection stage are going to be used as contribution to the examination-analysis stage. Technicians concerned in analysis section ought to be ready to affect responsibility and expertness, once analyzing information will expose another user’s sensitive information thanks to multi occupancy atmosphere in cloud.

4.4 Presentation

Presentation stage is that the last stage and manages the presentation of the proof in an officer room. a awfully a lot of archived report with discoveries should be delivered utilizing master declaration on the analysis of the proof. Specialists with individual information of the strategies that make the reports got to be picked. They got to be came upon to travel up against the jury World Health Organization desires learning of cloud computing. Proof should be introduced during a manner that the jury can see all the specialized points of interest since cloud computing is extremely troublesome to know for typical net purchasers to induce it. The enforced reports aboard of the Data, as an example, reasonably incidence, listed off records, which’s dependable, what the results were, and delicate components of discoveries are going to be incorporated into the reports and displayed.

5. FORENSIC SOLUTIONS

5.1 Access to evidence in logs

Primary issue within cloud forensics is that the recognition as well as accumulation within log since make unclear infrastructure. Several scientists’ area unit returns up with their higher solution. Individual amongst them is zawoad et al. WHO bestowed rhetorical investigation, it permits the CSP's to store the log documents of VM and provides access to the cloud rhetorical investigators.

5.2 Volatile data

Conquer within difficulty of explosive knowledge, elective thanks toward contend with quiet securing. Zawoad projected 2 conceivable strategies for the continual synchronization. CSP’s will provide purchasers, and CSPs will coordinate save the knowledge.

5.3 Client side identification

To identify proof on customer's facet, Damshenas et al. Counseled coming up with ANd death penalty an application to log all potential confirmation on the customer' machine. In any case, they did not offer any approach regarding the applying and also the methodology.

5.4 Dependence on CSP- trust

In cloud the purchasers primarily depend upon the CSP's, that affects the association between them. The shortage of transparency and trust between CSP’s and customers could be a drawback that Haeberlen [6] was restrained considering the countable cloud. He recommended a basic primitive called AUDIT that a responsible cloud may offer. The thought is that the cloud records its activities in alter obvious log, purchasers can review the log and check for deficiencies, and finally they'll utilize log to form prove that a blame has (or not) occurred. At the purpose once AN authority identifies blame, it will get confirmation of the blame which will be verified freely by a third-party.

5.5 Internal staffing- chain of custody

It is troublesome to search out with a selected finish goal to be related to a cloud investigation. Ruan et al [7]. Projected an answer that features interior folks of the cluster should be ready on, law directions, new approaches, specific technologies, specialized tools and techniques. As indicated by Chen et al.,[8] AN investigator have to be compelled to have the perfectness in rhetorical skills like programming, organizing, co-working, transfer and consulting with CSP’s and understanding laws and directions.

5.6 Forensic tools

The majority of the researchers acknowledge that tools ought to be created to spot, gather, and break down rhetorical knowledge. Juels et al. [9] created PORs instrument for semi-trusted on-line files that make sure the protection and also the trait. The prescribed the scientific mechanism for securing info. It can be often a web-based purpose to snap also maintain the communications. They all over offer with foremost appealing parity of velocity and management with hope choice.

5.7 Volume of data

An answer for the general community cloud near store up the proof, nonetheless this method emerges innovative problems commencing a lawful and specialized purpose of read. The opposite resolution is that the espousal of triaging procedures, New strategies ought to be inherit action to permit solely very little recovery of knowledge, and that they ought to be in consistent with accepted rhetorical principles.

5.8 complexity of testimony

Orton in counseled that folks with individual learning of the techniques in cloud sociology ought to exhibit the proof and to possess the capability to seem and disclose the method wont to extract knowledge. The individual ought to be ready to portray the vital to explain the method.

5.9 Documentation

As indicated by Wolthusen should be exhibited during a method inform doable gaps within the knowledge sets, vulnerabilities regarding the linguistics and interpretation {of knowledge of knowledge of information} and limitation of the gathering mechanisms along with the particular data. The documentation ought to embrace all the members concerned in knowing that the proof modified and proof occurred through hashes.

6. CONCLUSION AND FUTURE WORK

Anti-forensics is the major problem in the current generation and it is mainly observed in the cloud. The cloud infrastructure and architecture cannot be understood by many members, so it is difficult to address the anti-forensics in the cloud environment. Many methodologies and researchers proposed different cloud forensic challenges and solutions to the challenges but increase in the security concern in the cloud did not come down. Many customers use the cloud because of its characteristics but have many security breaches. Computer code important to contemporary web user United Nations agency be extraordinarily alert of their security and privacy once mistreatment on-line service that helps in securing the evidence from getting tampered.

References

[1] Mell, P. and Grance, T., **(2010)**. The NIST definition of cloud computing. *Communications of the ACM*, *53*(6), p.50.

[2] Kent, K., Chevalier, S., Grance, T. and Dang, H., **(2006)**. “Guide to integrating forensic techniques into incident response”. *NIST Special Publication*, *10*, pp.800-806.

[3] Kessler, G.C., **(2007)**, March. “Anti-forensics and the digital investigator”. In *Australian Digital Forensics Conference* (p. 1). DOI: 10.4225/75/57ad39ee7ff25

[4] Dahbur, K. and Mohammad, B., **(2011)**, April. “The anti-forensics challenge”. In *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications* (pp. 14). ACM. DOI: 10.1145/1980822.1980836

[5] Kebande, V. and Venter, H.S., **(2015)**, July. “A functional architecture for cloud forensic readiness large-scale potential digital evidence analysis”. In *European Conference on Cyber Warfare and Security* (pp. 373). Academic Conferences International Limited.

[6] Haeberlen, A., **(2010)**. “A case for the accountable cloud”. *ACM SIGOPS Operating Systems Review*, *44*(2), pp.52-57.DOI: 10.1145/1773912.1773926

[7] Ruan, K., “Designing a forensic-enabling cloud ecosystem”. *Cybercrime and cloud forensics*, pp.331-344. **(2012)**. DOI: 10.4018/978-1-4666-6539-2.ch026

[8] Chen, G., Du, Y., Qin, P. and Du, J., September. “Suggestions to digital forensics in Cloud computing ERA”. In *Network Infrastructure and Digital Content (IC-NIDC), 2012 3rd IEEE International Conference on* (pp. 540-544). IEEE. **(2012)** DOI: 10.1109/ICNIDC.2012.6418812

[9] Juels, A. and Kaliski Jr, B.S.,. “PORs: Proofs of irretrievability for large files”. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp.584-597). **(2007)** Acm. DOI: 10.1145/1315245.1315317

[10] Rani, D.R. and Kumari, G.G., **(2016)**, April. “A framework for detecting anti-forensics in cloud environment”. In Computing, Communication and Automation (ICCCA), 2016 International Conference on (pp. 1277-1280). IEEE.DOI: 10.1109/CCAA.2016.7813913