International Journal of Engineering & Technology, 7 (2.7) (2018) 1072-1075

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Analysis on digital forensics challenges and anti-forensics techniques in cloud computing

Divya Vadlamudi [1] *, Dr. K. Thirupathi Rao [2], Pellakuri Vidyullatha [1], B. RajasekharReddy [3]

[1] Assistant Professor, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
[2] Professor, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
[3] Student, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
**Corresponding author E-mail: divya.movva@kluniversity.in*

Abstract

In the modern life, there is a rapid increase in 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 forensic process had introduced to help the investigators to find the evidence when the criminal attacks the cloud and to maintain the integrity and security for the data stored in the cloud. The increasing in the criminal attacks in cloud, made the investigators to find the latest methods for the forensic investigation process. Similarly in the same way the criminals also discover new ways to hide the source of evidences. This causes damage to the investigation process and is called anti-forensics. To hide the sources anti-forensic techniques are used and research must be done against the anti-forensics techniques in cloud environment. In this paper we focused mainly on detailed study on various challenges in cloud forensic 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.

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 anti –forensics are the main part and the present research is going on anti-forensics in cloud computing. Cloud gives us the infrastructure with in the low cost and it can be misused by the criminals. Mainly the criminals in the cloud to destroy the data or misuse the data [1].when the criminals attacks the cloud environment then the evidences can be found in VM and cloud service provider.

Mainly the cloud service provider wants to ensure the user privacy and if any of the criminal attacked the respective cloud data then the criminal evidences must be known by CSP [2] [3]. Digital forensics is finding the evidences against the criminal event. When this digital forensics is applied in the cloud environment then it is called as cloud forensics. Anti-forensics is an attack consists of techniques and methods to destroy the source of evidences or hide the source of evidence [4]. If the criminals use this anti-forensic techniques to hide the source then it is very difficult for the investigators to find the evidence for the criminal attack. The major usage of anti-forensic techniques is to hide the evidence. Mainly the cloud investigators use the anti-forensic techniques to provide the trustworthiness and consistency to the cloud [5]. Anti-forensics is very important issue in the cloud [6] [7].

2. Anti-forensic techniques in cloud computing

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

2.1. Evidence destruction in cloud computing

When the VM is running or VM terminates then the evidence can be destructed. The log files of VM are deleted when the VM terminates. When the VM is running the data files can be deleted and deleting data inside the VM is also can be done. Evidence destruction leads to VM termination and evidence 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.

Copyright © 2018 Divya Vadlamudi et. al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2.3. Data hiding

Here we come across side channel attacks and covert channel attacks. These attacks are used to destroy the communication gap between the VM's and destroy the important information which VM doesn't know. This can also be achieved through side channel attack. The CSP uses different methods to hide the information but the attackers can move that information from one VM to another VM through these side channel or covert channel by using 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 [8], [20].

3. Peron and legary's approach in anti-forensics

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

3.1. 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.

3.2. 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).

3.3. 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.

3.4. Counterfeiting evidence

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

4. Cloud forensic challenges

In these, the cloud forensic challenges will be presented and each one will have the specific stage. There are four stages presented in the cloud forensic process they are 1) identification 2) collection and preservation 3) Examination and analysis 4) presentation.

4.1. Identification

Identification is the primary stage; the fundamental point is to locate all possible sources that contain the effective evidence in the cloud surroundings, keeping in mind the end 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 distinguishing the confirmation, the collection and protection of the evidence from the area in the cloud. Investigators should be confine and save the evidence to keep the utilization of digital device or by copying the digital evidence. In this collection-preservation particular resources will be utilized. These include well trained individuals, apparatuses required for the particular cloud information extraction and methodologies are used. The critical issue is to keep up the chain of custody for the evidence, legitimacy to the proof and trustworthiness for the computerized prove to display in the court of law. The evidence ought to be all around recorded and provide integrity for any further future changes in the proof.

4.3. Examination-analysis

Analysis includes the extraction of information from the past stage and the assessment of the huge amount of information identified. Prepared staff and specialist technicians ought to inspect every one of the information to discover evidence. So as to go into a forensic examination, investigators ought to acquire an abnormal state review of the landscape and shape a system; generally, deferrals may happen when unexpected yet preventable issues are experienced. Examiners should survey beforehand experienced cases and preparing plans to discover designs that can help to reduce the time of examination and build up their action plan. The discoveries from the preservation-collection stage will be utilized as contribution to the examination-analysis stage. Technicians involved in analysis phase should be prepared to deal with responsibility and professionalism, once analyzing data can expose another user's sensitive data due to multi tenancy environment in cloud.

4.4. Presentation

Presentation stage is the last stage and manages the presentation of the evidence in an official courtroom. A very much archived report with discoveries must be delivered utilizing master declaration on the analysis of the evidence. Specialists with individual knowledge of the methods that create the reports ought to be picked. They ought to be set up to go up against the jury who needs learning of cloud computing. Proof must be introduced in a way that the jury will see all the specialized points of interest since cloud computing is very difficult to understand for conventional Internet clients to get it. The implemented reports alongside the supporting materials concerning the chain of custody of the evidence ought to be submitted to the courtroom. Data, for example, kind of occurrence, traded off records, which's dependable, what the results were, and subtle elements of discoveries will be incorporated into the reports and displayed.

5. Forensic solutions

5.1. Access to evidence in logs

The primary issue in cloud forensics is the identification and accumulation of logs from cloud infrastructure. Many scientists are come up with their better solutions. One of them is zawoad et al [9]. Who presented secure-logging-as-a-service strategy for cloud forensic investigation, it permits the CSP's to store the log documents of VM and give access to the cloud forensic investigators.

5.2. Volatile data

To conquer the issue of volatile data, live investigation has been utilized as an elective way to deal with dead securing. Zawoad [10] proposed two conceivable methods for the continuous synchronization. CSP's can give a continuous synchronization API to clients, and CSPs can coordinate the synchronization mechanism with each VM and save the information inside their infrastructure.

5.3. Client side identification

To identify evidence on customer's side, Damshenas et al [11]. Recommended planning and executing an application to log all potential confirmation on the customer' machine. In any case, they didn't give any approach about the application and the method.

5.4. Dependence on CSP- trust

In cloud the clients mainly rely upon the CSP's, which affects the connection between them. . The lack of transparency and trust between CSP's and customers is an issue that Haeberlen [12] was dealt with considering the countable cloud. He recommended a basic primitive called AUDIT that a responsible cloud could provide. The thought is that the cloud records its activities in alter obvious log, clients can review the log and check for deficiencies, and finally they can utilize log to build prove that a blame has (or not) occurred. At the point when an evaluator identifies blame, it can get confirmation of the blame that can be verified freely by a third-party.

5.5. Internal staffing- chain of custody

It is difficult to find the perfect individuals to function as a group with a specific end goal to be associated with a cloud investigation. Ruan et al [13]. Proposed a solution that includes interior staffing, CSP-customer colloboration and external assistance with specific roles. People of the group must be prepared on, law directions, new approaches, specific technologies, specialized tools and strategies. As indicated by Chen et al.,[14] an investigator ought to have the perfectness in forensic skills such as programming, organizing, co-working, conveying and consulting with CSP's and understanding laws and directions.

5.6. Forensic tools

The majority of the researchers recognize that tools should be produced to identify, gather, and break down forensic data. Juels et al. [15] created PORs instrument for semi-trusted online files, which ensure the protection and the trustworthiness of files. In IaaS, Dykstra et al. [16] prescribed the suitable scientific device for securing cloud-based information. This is a web-based point and snap interface to manage and maintain the infrastructure. They concluded that it offers the most appealing parity of speed and control with trust option.

5.7. Volume of data

An answer for the challenge is to use the public cloud to store the evidence, yet this technique emerges new issues from a lawful and specialized point of view [17]. The other solution is the espousal of triaging procedures, however first, an evaluation on the influence of the different triage forms on real world devices and information should be conducted [18]. They likewise express that data mining gives a potential answer for understanding the large volume of data as long as it is used as an insight and learning instrument. New methods should be come into action to allow only little recovery of data, and they should be in according to accepted forensic principles.

5.8. Complexity of testimony

Orton in [18] recommended that people with individual learning of the techniques in cloud criminology should exhibit the proof and to have the capacity to appear and disclose the process used to extract data. The individual should be able to portray the testing results and most important to describe the logic behind the process.

5.9. Documentation

The documentation of the investigation as indicated by Wolthusen [19] must be exhibited in a way pointing possible gaps in the data sets, vulnerabilities about the semantics and interpretation of data and limitation of the collection mechanisms along side the actual data. The documentation should include all the members involved in investigation, the steps taken for knowing that the evidence has not been changed 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. Designing and developing trustworthy software and services is of vital importance for modern Internet users who are extremely aware about their security and privacy when using online services. Thus, the design and implementation of cloud services that can assist investigators conducting cyber-crime investigations in a more efficient way raises users' trustworthiness and system's security as well. For implementing cloud-forensic software and services, first, we need to understand the main requirements that need to be fulfilled in such systems. This review moves towards this direction by identifying the respective efforts from the investigation side in order to understand what investigators demand during a forensic process and which are the present efforts already conducted in the cloud which helps in securing the evidence from getting tamper ed.

References

[1] Malik, R., Shashidhar, N. and Chen, L., 2015, January. Analysis of Evidence in Cloud Storage Client Applications on the Windows Platform. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 3). The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

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

[3] Kent, K., Chevalier, S., Grance, T. and Dang, H., 2006. Guide to integrating forensic techniques into incident response. *NIST Special Publication*, *10*, pp.800-86.

[4] Kessler, G.C., 2007, March. Anti-forensics and the digital investigator. In *Australian Digital Forensics Conference* (p. 1).

[5] 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* (p. 14). ACM.

[6] 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* (p. 373). Academic Conferences International Limited.

[7] Al Fahdi, M., Clarke, N.L. and Furnell, S.M., 2013, August. Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. In *Information Security for South Africa, 2013* (pp. 1-8). IEEE.

[8] Liu, F., Ren, L. and Bai, H., 2014. Mitigating Cross-VM Side Channel Attack on Multiple Tenants Cloud Platform. *JCP*, *9*(4), pp.1005-1013.

[9] Zawoad, S., Dutta, A.K. and Hasan, R., 2013, May. SecLaaS: secure logging-as-a-service for cloud forensics. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security* (pp. 219-230). ACM.

[10] Zawoad, S. and Hasan, R., 2013. Cloud forensics: a meta-study of challenges, approaches, and open problems. *arXiv preprint arXiv:1302.6312*.

[11] Damshenas, M., Dehghantanha, A., Mahmoud, R. and bin Shamsuddin, S., 2012, June. Forensics investigation challenges in cloud computing environments. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on* (pp. 190-194). IEEE.

[12] Haeberlen, A., 2010. A case for the accountable cloud. *ACM SIGOPS Operating Systems Review*, *44*(2), pp.52-57.

[13] Ruan, K., 2012. Designing a forensic-enabling cloud ecosystem. *Cybercrime and cloud forensics*, pp.331-344.

[14] Chen, G., Du, Y., Qin, P. and Du, J., 2012, 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.

[15] Juels, A. and Kaliski Jr, B.S., 2007, October. PORs: Proofs of retrievability for large files. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 584-597). Acm.

[16] Dykstra, J. and Sherman, A.T., 2012. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, *9*, pp.S90-S98.

[17] Grispos, G., Storer, T. and Glisson, W.B., 2013. Calm before the storm: the challenges of cloud. *Emerging digital forensics applications for crime detection, prevention, and security*, *4*(1), pp.28-48.

[18] Orton, I., Alva, A. and Endicott-Popovsky, B., 2012. Legal process and requirements for cloud forensic investigations. *Cybercrime and Cloud Forensics: Applications for Investigation Processes*, pp.186-229.

[19] Wolthusen, S.D., 2009, September. Overcast: Forensic discovery in cloud environments. In IT Security Incident Management and IT Forensics, 2009. IMF'09. Fifth International Conference on (pp. 3-9). IEEE.

[20] 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.