Indian Journal of Science and Technology, *Vol 10(18), DOI: 10.17485/ijst/2017/v10i18/112116, May 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Emphasizing on Various Security Issues in Cloud Forensic Framework

Pranay Chauhan and Pratosh Bansal

Department of Information Technology, Institute of Engineering and Technology, Devi Ahilya Vishwavidyalaya, Indore – 452017, Madhya Pradesh, India; pranaychauhan1985@gmail.com, pratosh@hotmail.com

Abstract

Objectives: To provide a competent secure framework for the cloud forensics system with enhancement of security in various phases of forensics investigation method. **Methods/Statistical analysis**: The various issues has been raised in above study about existing cloud forensics framework as security concern has been discussed during the evidence identification and collection, during acquisition, during preservation and during analysis and reporting. The study unveils about the requirement of various security parameters during the entire chain of custody in cloud system. **Findings:** The major finding is related to security concern in various phases. Coming towards the initial stage of identification and collection, it is not easy to execute these tasks. Since cloud data is stored in multiple data center and using conventional method for identification of evidence is a tedious job. Because of cloud distributing nature it is not easy to collect all evidence from these servers, as thousands of servers are running globally across data center and securing this evidence is the major task. After that level key challenges is locations of data centers and data acquisition from a large data set. The remote location of data centers and client machine may require stateless communication. Predictable time duration for data acquisition from remote data centers in comparison with local computer demoralize the investigation process and make it overwhelming for a moment of time. Furthermore, erroneous evidence acquisition not only wastes investigation effort but may lead the complete investigation into the wrong manner. After that concern is about log file format, analyzing logs is challenge due to unification issue. Also at time of reporting main challenge occur for choosing the right court of law; Cross boarder verification is a big issue during investigation, and then exchanging data between two countries needs more privacy. **Application/Improvements:** Strong secrecy for evidence identification and collection, with enhanced privacy level and improved chain of custody method. Recovery of data in cloud can be faster, which will help in disaster recovery also due to a unified format. And finally appropriate secure integrated framework may lead to resolve cases quickly.

Keywords: Data Acquisition, Data Centre, Hashing Algorithm, Log Analysis, Uni Log Format

1. Introduction

Cloud Computing is a technique to enhance the scale of uses and performance by sharing resources and services. It has changed the operational and behavioral model of organization to enhance efficiency and availability of resources. It attempts to resolve the major issues of traditional system as cost, storage and security through multi-task resource pooling, elasticity, and high-speed networks[1].

As the superior performance of cloud computing technology, it is accepted by multiple organizations to get easy and effortless functioning with very low cost. They are using cloud platform for better services and applications in various dimensions. It's over whelming performance not only attracting organizations and researchers for enlargement and development of business but also get attention in attacker's world. Attackers may attempt to compromise its security services to degrade system performance, compromise confidential information, illegal activities or immoral happenings. Vulnerabilities into conventional system invite various security attacks from adversary to compromise trusted nodes or information. A heavy risk

**Author for correspondence*

phenomenon requires enhancement in existing security policies for cloud computing environment. Computer forensic is a standard process to investigate and collect strong digital evidences from computing devices or digital media.

It toughly used in legal practices or crime investigation. Any information or raw facts stored or transmitted from digital approach may consider as digital evidence. Furthermore, digital evidence may use in authentication process or security management for proof of originality in physical or digital context[2,3].

Although a lot of work has been involved in cloud computing to enhance its security potential, the still possibility of enhancement has been anticipated. Similarly computer forensic may introduce a new dimension in cloud computing environment to double the prospective of cloud security policies and performance of cloud-based applications[3]. Cloud forensic is a novel measurement in cloud security which is the combination of computer forensic and cloud computing. Conventional forensic approaches provoked to do an offline investigation. Furthermore, they are not well-suited for online investigation.

Multiple storage locations and resource pooling generate enormous demand for digital verification which can be achieved through cloud forensic. This explores several dimensions for evidence collection and acquisition. Although, large data set creates a combustive environment for cloud forensic and generate vast hurdles in collection and acquisition process but also give multiple points for security measurement Optimization in cloud forensic effort not only helps to reduce security overhead but also leads to enhance system performance[2–4].

2. Problem Domain

The major purpose of use of cloud computing is resource sharing. Resources may be hardware, software, application as well as a platform. The consumer can access various resources i.e. Software, platform and storage as a service through public networks. Resource pooling and remote access make it cost effective technology. Furthermore, preplan of resource sharing reduces investment cost which leads to reducing cost of application implementation and deployment.

The study observed that fame of cloud computing not only attract enterprise and consumer for better performance but also getting attention in the illegal world. Attackers or criminals are trying to explore system vulnerabilities and deploy security threats to compromise resources or services from public networks. The various security issues in the conventional system are identified which may affect the privacy and integrity of information. It gives an opportunity to attackers for breaking authentication and verification process in service access. Illegal and unauthorized access can become a lead for immoral or criminal activity. The complete study explores the need to revised security policy for cloud computing. It also demands to develop an exclusive policy for dynamic nature cloud environment[5].

Although, there are so many reasons to adopt cloud computing, but other side few issues may put into the backseat. These barriers not only degrade its performance but may compromise the trust of a user on service providers. The study observed that uncertainty on backup and data recovery, time synchronization, resource pooling, optimization of uses, national and international level legal issues and security requirement desire extra concern and enrichment to improve performance. Here, security is a major concern of user and service provider, because risk and trust can't consider as insubstantial activity[6].

Security concerns related to huge data storage at remote places, data transmission from public and private networks, dependencies on other networks and data centers, heterogeneous and distributed resource arrangement, integration of various service models and on demand service allocation. Here, conventional security techniques for confidentiality, authentication and integrity can't effectively integrate on various levels of a cloud environment. Subsequently, remote data centers and public network require extra concern for same[7].

To get the power of computer forensic in cloud computing, researchers added forensic policy with cloud security services to enhance the security level. This phenomenon is known as cloud forensic. The basic steps which encompass during cloud forensic are identical to digital forensic i.e. evidence identification, evidence collection, acquisition, preservation and then analysis. Whereas conventional cloud forensic framework consists four/five phases for investigation and security measurement. It may elaborate as follows: Table 1 and Table 2 demonstrate various phases during cloud forensic investigation[3,8,9].

Coming towards the initial stage of identification and collection, it is not easy to perform these tasks. Since cloud data is stored in multiple data center and using

conventional method for identification of evidence is a tedious job. Because of cloud distributing nature it is not easy to collect all evidence from these servers, as thousands of servers are running globally across data center. It also affects the chain of custody method during an investigation and securing this evidence is the major task[2].

Table 1. Existing framework for cloud forensic[9]

	MCKEMMISH	NIST	B.MARTINI
Step 1	Identification	Collection	Evidence Source identification and preservation
Step 2	Preservation	Examination	Collection
Step3	Analysis	Analysis	Examination and Analysis
Step4	Presentation	Reporting	Reporting and presentation

Table 2. Study of various forensic issues and proposed mechanism

S. No.	Investigated Cloud Forensic Issues	Proposed Mechanism
1	Security of data and vulnerability	Enhanced level of security, CSP based trust factor
2	Privacy and virtualization issues	Discuss about their pro and cons
3	Multiple issues	Cybercrime Forensic Framework
4	Discuss data center framework with secrecy issues	Data center adoption system
5	Privacy issues during forensic steps.	Imaging concept, multimodal system and data reconstruction
6	Compare issues of NIST and Mc Keemish framework	Refinement of forensic framework
7	Discuss issues in cloud security Model and forensic framework	Monitoring and cloud trust model
8	Multiple challenges during forensic steps	Forensic architecture
9	Challenges during forensic steps and client server system	Client and server forensic setup
10	Challenges during evidence collection, preservation and acquisition phase	Various aspects in network, storage and virtualization

Security concern during evidence identification and collection: In the cloud, evidences may execute at numerous points. Some imperative places may be as follows;

- Firewall log file from client and server systems.
- Storage media, backup and recovery nodes.
- Transmission medium during communication.
- System logs files, data files, temp files and buffer memory and much more.

Above modes are primary places for evidence identification which may expand according to the deployment of cloud structure. Major challenges with the above modes are they are required to freeze from before evidence collection. Work identify that updates on above modes will be excluded from verification process. It gives a static verification process up to level. Moreover, a reliability of information from evidence collection platform and modes is also the big question.

Investigation process is a linear approach where digital evidence is primary input for further process. Thus wrong or altered digital evidence may mislead the complete investigation into the wrong way. Integrity management on evidence modes is the big challenge and need to be improved. While identifying the right evidence is another important concern. The complete study strongly demands to develop exclusive accurate evidence identification and integrity approach for primary evidence modes in cloud environment. The following aspects are used to congregate identified evidence[10].

- Generation of evidence.
- Storage of evidence.
- Transmission of evidence.
- Electronic evidence collection.
- Evidence deletion, their backup and so on,

These evidence tactics get a compromise by the hateful action; due to which privacy get to negotiate. Though, faulty and false evidence can disturb the entire investigation procedure[10].

2.1 Security Concern During Data Acquisition

This is next level process during cloud forensic. Main challenges in cloud forensic are locations of data centers and data acquisition from a large data set. The remote location of data centers and client machine may require stateless communication. Expected time duration for

data acquisition from remote data centers in comparison with local computer demoralize the investigation process and make it overwhelming for a moment of time. Subsequently, data acquisition from large data set not only increase investigation overhead at data servers but may reduce the accuracy of evidence acquisition. The complete phenomena make this level too much overhead creator for a server as well as client side. Furthermore, erroneous evidence acquisition not only wastes investigation effort but may lead the complete investigation into the wrong manner [5,11,12].

The complete study explores the need to develop exclusive service for data acquisition from the large data set. Conventional mechanisms are based on simple data selection and fetching mechanism. Knowledge-based data acquisition is required to overcome fetching effort and improve accuracy with privacy. Knowledge management mechanism may help to reduce the searching scope and safe acquisition time duration. Besides dependency on cloud providers is there for legal processes, cooperation is also required from these providers during safe acquisition process[13].

Cloud execution has multiple layers of abstraction, from hardware to virtualization. Virtualization is another aspect during the acquisition phase, because virtual instances get demolished, after a short interval of time. So to collect these instances and freezing them for long duration is another critical task, many flaws interrupt virtual machine analyzing[14]. In the meantime, the protection of evidence is essential because formerly encrypted data may also be insecure. And it might disrupt investigation outcomes.

2.2 Security Concern During Preservation

Preservation of evidences against the tampering or deleting digital evidences plays crucial role in cloud forensic investigation process. A lot of work has been done in this field; still live vs. Dead investigation issue is seeking big attention. Due to dynamic nature of cloud computing environment live investigation is too much hectic job. Subsequently, in live investigation updates after freeze event is still big issue. It required more preservation of data[13,15]. In dead investigation machine is in halt state and investigation is performed, so investigating in live state is complex and critical and it required proper preservation mechanism. Currently, authentication is maintained by one way hash function: such as MD5 (message digests) which will provide unique hash of file or a complete disk image and it is not strong enough[3,8,16]. Multi factor authentication is required, in order to ensure the primitiveness and integrity of data, and strong encryption mechanism needs to be developed for better confidentially[4,10,17].

All though in analysis and resulting phase several logs collected from different layers of cloud, then centralizing them is another big concern. Because these decentralized logs are spread in multiple tiers of cloud[18,19]. It became difficult for investigator to perform examination from various ends since cloud do not provide access to everyone. Major concern arises during: how system log files, data files, buffer data and deleted files can be beneficial for investigation. However lack of tools in investigation may negatively distress the analysis phase. It also causes incomplete evaluation, and may affect the valid report generation[20,21].

2.3 Security Concern During Analysis and Reporting

Again severe facts, where multiple logs file are evaluated. Concern is about log file format, analyzing logs is challenge due to unification issue; some data can be loss due to this UN unification format[9]. And it make inconsistency between cloud service providers, that how to gather log data. So a uni-log format is required to perform appropriate analysis which will support faster investigation[19,22,23]. Well along a secured frame is needed to protect these uni-logs against much vulnerability[17, 24,25].

During reporting, main challenge occur for choosing the right court of law; since in conventional forensic investigation court of law can easily be decide on crime committed country. But in cloud it is not easily decidable due to cloud multiple locations and remote resources. Cross boarder is a big issue during forensic investigation, and then exchanging data between two countries again-haveprivacyconcern[10,26].

Furthermore, the overhead of security strategies may create an awkward and complex environment for cloud computing. Cloud forensic may not only add a new dimension to cloud security but will also create enhance toughness for security threats and simplify chain of custody. The complete work observes that proposed solution will help to enhance security policy in cloud forensic.

3. Proposed Solution

Cloud forensic provides new dimensions in cloud computing environment to maintain security with structured

fashion. It paired potential of convention security mechanism by intersecting its strength with computer forensic. Cloud forensic not only help to exchange security measurement or digital investigation but also help to maintain the trust of a user. Compromising single bit data may become a crucial reason to loss user's trust from the organization. Thus any organization can't take a risk with user trust and always try to maintain their data safe and secure. Although a lot of research work is undergoing in this field still a scope of improvement is possible. Most of the Solutions are based on static evidence investigation and offline mode. It may achieve requirement of security measurement but Cannot be accurate for the current situation. Figure 1 shows the proposed methodology.

Within evidence identification and collection process, identifying accurate evidence and its integrity is a major concern and still need to be improved. Integrity management of evidence modes and platform not only help to identify actual proofs but also improve system accuracy and performance. Various integrity algorithms such as MD5 or SHA-1 are in practice.

While the strength of such algorithms depends on upon the size of the key input. It not only maintains the privacy of content but also provide correct direction for further process. So using the improved algorithm will perk up security. After that, data acquisition level is suffering data fetching from the remote data center and searching digital evidence from the large data set.

Mapping of various data centers into a particular manner and simplifying large data set according to knowledge map may help to overcome the acquisition overhead. Here, inverted hash-based system can be used for mapping purpose and help to generate light process low overhead security policy.

Preservation of evidence against the tampering or deleting digital evidence is mandatory. The conventional system mainly emphasizes over offline evidence collection and preservation. Live evidence collection and preservation will improve system efficiency and accuracy of security measurement. Protective data will also boost privacy level in a live acquisition, as well as cloud service utilization.

Depth level defense mechanism can be used for high-level protection, where virtual instance will help to overcome various vulnerabilities. Better defense mechanism will also help in transferring evidence remotely.

While during analysis and reporting, uni log format is required to perform appropriate analysis. After that, there is a need to dissolve multiple formats and develop unified log maintenance format to maintain consistency and similar attribute culture in forensic evidence. The unified format will not only help to develop similar log maintenance pattern but will also overcome the problem of mismanagement in log maintenance.

Along this protected frame is needed to defend these uni-logs against various threats. Better cloud monitoring can be performed due to these unified formats. Thus it also helps service providers for better cloud migration. The complete study concludes that little bit enhancement into cloud forensic steps may lead to giving big impact on system performance. It will not only improve safety factor but also improve the investigation state from offline mode to online state. Issues during troubleshooting and recovery can also be overwhelmed.

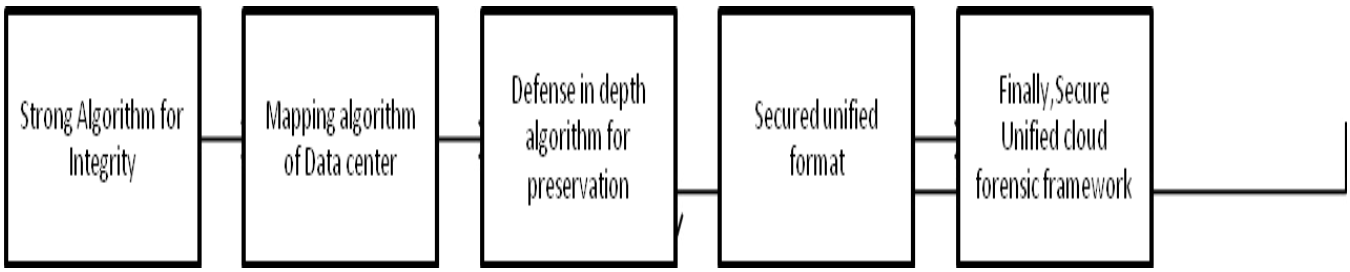

Figure 1. Projected methodology.

Step by step execution of projected methodology

1. Strong algorithm for integrity is required
2. Mapping algorithm for data centre (for various log collections)
3. Strong algorithm is needed for preservation
4. Unified format need to developed
5.At last secured framework will help in better security

4. Expected Outcome of the Proposed Work

The outcomes are quite clear and precise. The proposed system will enhance security performance of the system.

a) Strong secrecy for evidence identification and collection.
b) Secure mapping of large data sets from the data centre to perform the fast acquisition.
c) Enhanced privacy level and improved chain of custody method.
d) Fast troubleshooting.
e) Recovery of data in the cloud can be faster, due to a unified format.
f) Appropriate secure integrated framework may lead to resolve cases quickly

5. Conclusion

A study of existing system discusses, about the various security concern in the framework. A lot of issues are there during evidence identification, acquisition, preservation and analysis. While inaccurate evidence identification can mislead the entire process, while acquisition and preserving evidence from the data center is another big concern. During analysis, the uniqueness of log format is another vital concern. Our proposed methodology is just a small pace to minimize issues at some level.

6. References

1. Pennypritzer. NIST cloud computing forensic science challenges. NIST Publication; 2014. p. 1–51.
2. Shah J, Malik LG. Cloud forensic issues and challenges. International Conference On Emerging Trends In Engineering and Technology; 2013. p. 138–9.
3. Reilly D, Wren C, Berry T. Cloud computing pros and cons for computer forensic investigations. International Journal multimedia and Image Processing. 2011; 1(1):26–34.
4. Sharevski F. Digital forensic investigation in cloud computing environment: impact on privacy. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE); 2013 Nov 21–22. p. 1–6. Crossref.
5. Ahmed S, Raja YMA. Tackling cloud security issues and forensic model. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) 7th International Symposium on High-capacity Optical Networks and Enabling Technologies; 2010 Dec 19–21. p. 190–5.
6. Cloud Security Alliances. Cloud adoption in financial sector. CSA Publication; 2015. p. 1–13.
7. Chi J, Duan Y, Zhang T, Fan J. Study on the security models and strategies of cloud computing. Procedia Engineering, Elsevier, ScienceDirect. 2011; 23:586–93. Crossref.
8. Martini B, Choo KKR. Cloud storage forensic own cloud as a case study. Digital Investigation, Elsevier, ScienceDirect. 2013 Dec; 10(4):287–99.
9. Martini B, Choo KKP. An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, Elsevier, ScienceDirect. 2012 Nov; 9(2):71–80. Crossref.
10. Cloud Security Alliance. Mapping the forensic standard ISO/IEC 27037 to cloud computing. CSA Publication; 2015. p. 1–31.
11. Damshenas M, Dehghantanha A, Mahmoud R, Shamusddin SB. Forensic investigation challenges in cloud computing environments. In the Proceedings of the Institute of Electrical and Electronics Engineers (IEEE) International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec); 2012 Jun 26–28. p. 190–4.
12. Chen L, Xu L, Yuan X, Shashidhar N. Digital forensic in social network and the cloud. Institute of Electrical and Electronics Engineers (IEEE) International workshop on Sensor Peer to Peer Network and social network; 2015 Mar. p. 1132–7.
13. Lei Y, Cui Y. Research on live forensic in cloud environment. Second International symposium on computer communication control and automation. Atlantis press; 2013 Nov. p. 231–4. Crossref.
14. Poore J, Flores JC, Atkison T. Evolution of digital forensic in virtualization by using virtual machine introspection. In the Proceedings of the 51st Association for Computing Machinery (ACM) Southeast Conference, Savannah, Georgia; 2013 Apr 4–6.
15. Wang Y, Clee H. Research on some relevant problems in computer forensics. Second International Conference on Computer Science and Electronic Engineering Atlantis Press Paris France; 2013 Jan. p. 1564–71. Crossref.
16. Chen Y. Paxon V, Katz RH. What's new about cloud computing security. Technical report on Electrical Engineering and Computer Science. California: University of California at Berkeley; 2010 Jan 20.
17. Bakshi K. Consideration for cloud data center framework architecture and adoption. Institute of Electrical and Electronics Engineers (IEEE) Aerospace Conference (IEEEAC); 2011 Mar 5–12. p. 1–7.
18. James JI, Shosha AF, Gladyshev P. Digital forensic investigation and cloud computing. Cybercrime and Cloud Forensic: Application for Investigation processes; 2012 Dec. p. 1–41.

19. Zhang Y, Lin Y. Research on the key technology of secure computer forensic. Institute of Electrical and Electronics Engineers (IEEE) 3rd International conference symposium on Intelligent Information Technology and Security Informatics; 2010 Apr 2–4. p. 649–52. Crossref.
20. Yan C. Cybercrime forensic system in cloud computing. Institute of Electrical and Electronics Engineers (IEEE) International Conference on Image Analysis and Signal Processing; 2011 Oct 21–23. p. 612–5.
21. Wazid M, Katal A, Goudar RH, Rao S. Hacktivism trends digital forensic tools and challenges: a survey. Institute of Electrical and Electronics Engineers (IEEE) conference on Information and Communication Technologies; 2013 Apr 11–12. p. 138–44.
22. Cohen F, Ruan K. Challenges to digital forensic evidences in the cloud. Cybercrime and cloud Forensics Application for Investigation Process; 2012 Jan. p. 2–7.
23. Chen G, Du Y, Qin P, Du J. Suggestion to digital forensic in cloud computing ERA. In the Proceeding of Institute of Electrical and Electronics Engineers (IEEE) 3rd International Conference on Network Infrastructure and Digital Content; 2012 Sep 21–23. p. 540–54. Crossref.
24. Aminnezhad A, Dehantanha A, Taufik M , Damshenas M. Cloud forensic issues and opportunities. International Journal of Information Processing and Management. 2013 Jun; 4(4):76–85.
25. Damshenas M, Dehghantanha A, Mahmoud R, Shamuddin SB. Cloud computing and conflicts with digital forensic investigation. International Journal of Digital Content Technology and its Application. 2013 May; 7(9):543–53.
26. Shah V, Bansal P. CDCD-5 an improved mobile forensics model. International Journal of Computer Science and Information Technology and Security. 2012 Aug; 2(4):739–41.