Journal of Computer and Communications, 2016, 4, 63-69
Published Online August 2016 in SciRes. http://www.scirp.org/journal/jcc
http://dx.doi.org/10.4236/jcc.2016.410007

Scientific Research Publishing

Forensics Issues in Cloud Computing

Aqil Burney[1], Muhammad Asif[1,2], Zain Abbas[3]

[1]Department of ASRM, College of Computer Science and Information Systems, IoBM, Karachi, Pakistan
[2]Department of Computer Science & Information Technology, NEDUET, Karachi, Pakistan
[3]Department of Computer Science (UBIT), University of Karachi, Karachi, Pakistan
Email: aqil.burney@iobm.edu.pk, asifashrafiubit@hotmail.com, zain@uok.edu.pk

Received 20 June 2016; accepted 19 August 2016; published 22 August 2016

Copyright © 2016 by authors and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

Cloud computing is an emerging technology that is being widely adopted throughout the world due to its ease-of-use. Organizations of all types can use it without pre-requisites such as IT infrastructure, technical skills, managerial overload, storage capacity, processing power, and data recovery or privacy setup. It can be availed by all clients as per their needs, expectations and budget. However, cloud computing introduces new kinds of security vulnerabilities that need to be addressed. Traditional "Computer Forensics" deals with detection, preemption and prevention of IT triggered frauds and crimes but it lacks the ability to deal with cybercrimes pertaining to cloud computing environment. In this paper, we focus on forensics issues in cloud computing, assess limitations of forensic team and present the obstacles faced during investigation.

Keywords

Computer Forensics, Cloud Computing, Cybercrimes, Cloud Security, Cloud Service Provider

1. Introduction

With the evolution of internet in 1990's, many changes have been witnessed by the computing world, from uni-processing environment to parallel processing, distributed computing, grid computing, ubiquitous computing, pervasive computing and now cloud computing [1]. It allows businesses to scale up and down their resources based on their needs [2]. Using cloud computing, users can store their data remotely and enjoy on-demand seamless application access without having to invest in hardware infrastructure or software management [3]. Thus, it shields the user from facing difficulties of traditional computing such as establishment of infrastructures, software licensing, and hiring of technical staff etc.

In this document, we have analyzed the limitations that Computer Forensics has in "Cloud Computing" and the need to address them for successful implementation of Computer Forensics for detection and prevention of fraudulent acts and cybercrimes. The objectives of this research is to analyze the processes, procedures, metho-

How to cite this paper: Burney, A., Asif, M. and Abbas, Z. (2016) Forensics Issues in Cloud Computing. *Journal of Computer and Communications*, **4**, 63-69. http://dx.doi.org/10.4236/jcc.2016.410007

dologies, tools and techniques of Computer Forensics and its usages in Cloud Computing for tracking digital evidences, frauds and cybercrimes, as this technology is evolving and spreading its roots throughout the world and utilizing the capability of internet for the great achievements. Cloud Computing is a diverse, flexible, cost-effective, and proven delivery platform for providing IT services to customers as well as businesses over the Internet [4]. However, it possesses an added risk because of outsourcing of essential services to a third party [5]. This is another area to be taken care of. Moreover, every technology has its merits and demerits but the important thing is the optimum utilization of merits while limiting the demerits. Thus, the main purpose of this discussion is to overcome the weaknesses in cloud computing and identify solutions that can be helpful in betterment of technology.

We have performed a substantive analysis on processes, procedures and techniques limitations of Computer Forensics in Cloud Computing and described the processes and set of rules of Computer Forensics that are being applied throughout the process of Computer Forensics. The process has critical approach that can be legally proceeded in civil court for prosecution. If predefined processes and techniques are inadequate for finding and collecting digital evidences, then successful implementation and execution of Computer Forensics in Cloud Computing will not be feasible and it will not be able to deliver the desired results.

The rest of the paper is organized as follows. Section 2 defines Computer Forensics. Section 3 outlines Cloud technology at length. Section 4 highlights main security aspects in cloud. Section 5 lists the issues and constraints whereas recommendation and conclusion follow.

2. Computer Forensics

Computer Forensics is the science of identifying, extracting preserving, and presenting the digital evidence stored in digital devices that can be legally admissible in court for any cybercrime or fraudulent [6]. In other words, finding out facts, records, and digital trails can be legally admissible in the court for criminal prosecution [7]. Digital information is fragile in that it can be easily modified, duplicated, or destroyed etc. In the course of the investigation it should be assured that digital evidence is not modified without appropriate authorization [8].

Computer forensics has had major impact in detecting and preventing frauds as well as potential business losses that can deface an organization of its reputation. The basic process of computer forensics is based on the following steps:

- Identifying,
- Preserving,
- Recovering,
- Analysis,
- Presenting.

Above mentioned set of process deals in computer forensics for detection and prevention of frauds and cybercrime, now our main concern is efficient utilization of these processes in cloud forensics for achieving desired objectives of detection and prevention of frauds and cybercrimes.

3. Cloud Technology

Cloud is a network of processing elements or servers that has infrastructure to provide processing and storage facilities to clients throughout the world over the internet. The technology is spreading instantly in all domains. For instance, common users are utilizing public cloud services in the form of Google® Drive, Dropbox®, One-Drive® and Media Fire® for data storage [7]. Similarly, commercial level cloud technology is also boosting itself. Many small, medium to large organizations are utilizing private cloud services for their businesses. Rather than investing huge amount for finance to develop infrastructures, platforms, software applications and operating systems; they obtain all these as well as get administrative and management services in the form of web apps from cloud service providers in private manner. Community Cloud is another service in which group of organizations uses cloud facility. Hybrid cloud has both public as well as private cloud facilities. For secure computing it utilizes the private cloud environment whereas noncritical activities and operations are done on public cloud [7].

3.1. Cloud Service Provider (CSP)

In cloud computing environment several challenges may exist in cloud computing forensics. Cloud Service Pro-

vider is an entity that provides services to its clients including infrastructure, OS licensing, application interfaces, data storage, processing power, backups and other necessary supporting tools for cloud computing [6]. Cloud Computing supports the virtualization where hardware and configurations are provided as per requirement of the client and its budget.

3.2. Cloud Infrastructure Models

Cloud Service Providers are providing different services according to their contractual agreements and they follow different infrastructure models as per their policies due to that cloud computing forensics varies according CSP policies and SLA (Service Level Agreement) [6].

3.3. Deployment Models

Cloud computing has different deployment models as mentioned below:

- Public Cloud,
- Private Cloud,
- Community Cloud,
- Hybrid Cloud.

Deployment models vary as per requirement of clients. Public cloud can be efficient for general public having general needs; Private cloud deployment model can be efficient for commercial clients according to their specific needs and businesses. Community cloud can be helpful for those organizations those are having similar objectives in their businesses and hybrid cloud is effective in condition when client has general objectives that can be utilized on public cloud as well as specific objectives that can be achieved on private cloud as shown in **Figure 1**.

3.4. Service Models

Three service models are provided to the client by Cloud Service Provider in which

- IaaS (Infrastructure as a Service),
- SaaS (Software as a Service),
- PaaS (Platform as a Service).

IaaS provides access to physical machines, virtual machines and virtual data stores. SaaS provides access to software applications. PaaS Provides access to runtime environment for software applications, software development and software deployment tools [6].

4. Forensics in Cloud Computing

As a client of a Cloud Service Provider we must have following concerns about our data and crucial services.

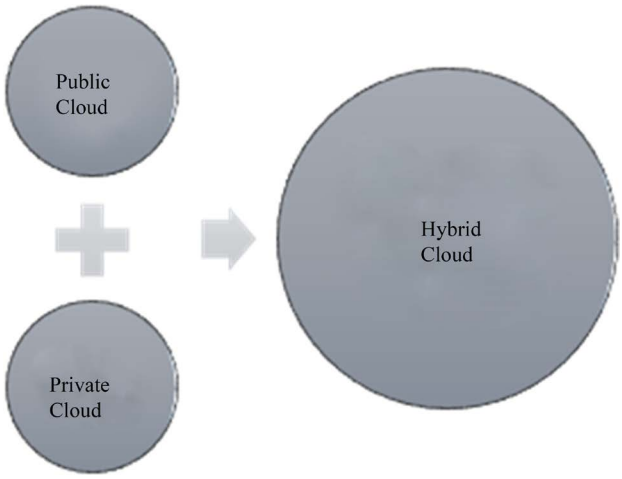

Figure 1. Hybrid Cloud.

- Data Integrity,
- Data Confidentiality,
- Data Availability,
- Service Availability.

If all relevant things are working fine, then we are availing a better service but everything will be at stake if someone like a hacker or a malicious person compromises data integrity, confidentiality or availability. In case of such an untoward incident, the role of forensics teams is to investigate, report and curb the crime. New challenges exist in Cloud Forensics for prevention and detection of frauds and cybercrime. Its exponential growth and usage has introduced a set of challenges that need to be mitigated in order to assure cloud computing security and maintaining high level of trust amongst the users (clients).

4.1. Variations in Investigation

Investigation in cloud computing varies as per service models that is being provided to the client accordingly. If IaaS is compared with SaaS and PaaS, it is more affable and a computer forensics team can found it more affable during investigation. A computer forensics team can get instance access to log history of the compromised system in SaaS and PaaS service models whereas in IaaS model the image of Virtual Machine can get for investigation [6].

4.2. Physical Devices Accessibility

In cloud computing a cloud forensic team can get access to the physical devices if the deployment model is private cloud; assistance and access is provided by the CSP but if the deployment model is public cloud then access may not be granted as per requirement of the investigation team [6].

4.3. CSP Collaboration

If a client's cloud is compromised, then a request is generated for cloud forensic to CSP which then relies on the cooperation of CSP. In case the CSP intends to provide physical and logical access to the investigation team for tracing the trails of fraud, crime or forgery, the investigation may be successful but if CSP isn't collaborating, forensics investigation will yield nothing [8].

4.4. Conducive Laws

In case CSP is not intending to cooperate with cloud forensic team as per requirements, then the team has to rely on laws and legal procedures that can be useful for getting desired permissions and access to physical and logical system of client's cloud [6].

4.5. Client's Site Compromised

In cloud computing this is not necessary that a user of cloud is a techy savvy who is aware of all aspects of social engineering (Hacking phases) that are used to exploit client's cloud in terms of data theft, unauthorized changes in data and issues of data integrity and confidentiality. As a result, it increases the chances of exploitation of a victim and client's system can be easily compromised by the social engineering tactics [9]. Exploitation techniques may use malicious JavaScript® or malicious browser extensions. Similarly, some malicious program may be installed on client's browser or operating system that can steal cookies or session id, or log the keys. Rapid use of different devices (*i.e.* PCs, Laptops, Smart phones, Tablets and different PDAs) to access cloud service from random places can also make forensic procedure more complex and difficult to extract vital information from heterogeneous environments that can be useful in legal procedures [10].

4.6. CSP's Site Compromised

If a CSP is not providing access and assistance to the investigation team as per requirement of contractual agreement, then it would lead to the suspicion that the cloud has been compromised from CSP site due lack of physical and logical security policies, or procedures for protecting data, and ensuring data confidentiality and data integrity. There may also be a possibility that acts of some malicious employee at CSP site has disrupted

client [3].

4.7. Issues of Intense Seizing of Physical Devices

First step in computer forensics is to seize physical devices at the scene due to lack of intense accessibility to the physical devices at CSP site [10]. If this is not done, there are chances of lost critical evidences that could have proven to be vital in computer forensics. In case of cloud, data is not necessarily available at a single location and may reside at different geographical locations; that makes seizing of physical devices impossible in cloud forensics [8].

4.8. Issues of Recovering of Volatile Data

In some cases, a malicious program exploits the system through execution in RAM or processors Registers. Being volatile part of memory, it's easier to wipe them out completely from these devices by simply switching OFF and ON or rebooting the [10].

4.9. Issues of Data Integrity & Confidentiality

In cloud computing, there exist possibility of compromised data integrity & confidentiality at CSP site (Data leakages, Data alteration, Data delectation and unwanted Data restoration) [9]. Thus, the evidences provided to cloud forensic team by CSP cannot be trustworthy. This can cause investigation team on some false lead or track that cannot be fruitful for forensics.

4.10. Issues of Locations

As client of cloud computing one isn't actually sure about the data storage as it may reside at different geographical locations. There is a possibility that CSP is just pretending the storage of data at some location where laws aren't applicable for getting intense access to the physical devices but in reality it is not there so it introduces new issues during the cloud forensics processes. For instance, if a client is from Pakistan and data actually resides in Israel then access to the data becomes more difficult due to bilateral relations of the countries.

4.11. Lack of Automated Tools

Traditional software tools of computer forensics are inadequate in cloud computing forensics due to inaccessibility of the physical devices. They become inadequate during cloud digital investigation and not feasible for gathering of digital evidences, so they are not viable for cloud computing forensics.

4.12. Cloud Forensic Expenses

Overall cloud forensics cost is more than the cost of traditional forensics with lesser achievements as it minimizes the chances of detection of frauds or criminal acts due to its constraints.

4.13. Issues of Incompetence Skills of Client

A client or a user of cloud may not have technical skills like a DBA or Network Administrator. This lack of skills introduces new potential issues in cloud computing. There are possibilities that frauds, forgeries or cybercrimes have already occurred but users of cloud are not aware of these issues because no periodically reviews are performed for prevention and detection of malicious acts that can exploit the cloud of a client. Thus, delaying in reviews introduces more forensics issues as timely actions reduce the risks of greater disasters that can collapse the business entity and can be a cause of business loss.

4.14. Remote Access Place Security

Cloud service can be accessible from anywhere in the world through internet so a user of cloud service accesses that service from a compromised system it poses a potential threat to security of entire cloud service. For instance, a machine that is already compromised through malware, spyware, backdoors and key logger can be used for frauds and crimes by exploiting credentials of a legitimate user.

5. Issues in Cloud Forensics

Forensics issues in cloud computing elevate the challenges that need to be mitigated to make cloud computing more reliable, safe, and secure. Cloud computing is just boosting itself by introducing attractive features, services and lesser cost to its clients but at the same time have many potential risks such as data integrity, data confidentiality, not having precise knowledge where exactly data is physically stored, legality issues, and existence of regularity bodies. Forensics cost increases in cloud computing as compared to traditional forensics, volatile data recovery issues, difficulties in identification that either Cloud Service Provider site is compromised or Client site compromised, less chances of intense seizing of physical devices of compromised cloud and contractual agreement restrict the forensics team regarding SLA (Service Level Agreement) that constraints the overall functionalities of investigation team. Giant organizations might afford the forensics cost but for the small companies it is sometimes impossible to afford it. Main constraints faced are summarized below:

- Forensics team has to perform its task in limited domain.
- Personnel resource allocation is a challenge at different geographical locations.
- Different legalities issues in different countries.
- High cost of forensics.
- Ineffectiveness of traditional forensics tools.

6. Recommendations and Future Work

In this research we focused on forensics issues in cloud computing that are being faced by digital investigation teams. These should be mitigated in a better way for enhancing the overall functionalities in cloud computing. The main areas of future development may focus on the following:

- Research & Development in software tools that can enhance the process of evidence gathering in cloud computing.
- Make standards for Cloud Service Providers that ensures physical access to compromised systems without any SLA (Service Level Agreement).
- Make standards for periodically reviewing the cloud system for early detection and prevention of fraudulent acts and cybercrime.
- Further new processes and techniques can be introduced in cloud forensics.
- Make an autonomous body that ensures that provided information regarding data storage at physical location is in compliance.
- Make a regularity body that ensures legal prosecution will be admissible at CSP even if it doesn't follow its policies as per contractual agreement with the client.
- Creation of centralized regularity body will be highly effective and increase the overall performance and effectiveness of forensics teams that can address those issues those are still creating hurdles and great challenges in the way.

7. Conclusions

This research paper dealt with issues related to forensics in cloud computing. They pose a real challenge during digital crime investigation in cloud environment. Real issues that were being faced by investigators were highlighted and some recommendations were put forth to improve the reliability of information systems that use cloud services. This will ensure timely tracking of frauds and cybercrimes, reduce the risks of business loss, reduce data leakages, and provide smarter ways of recovering the lost data.

The aim of this research is to ensure that identifying, preserving, recovering, analyzing and reporting the digital facts and evidences are performed in an efficient manner. This will yield evidence admissible in the court for proving that a crime has occurred.

References

[1] Jadeja, Y. and Modi, K. (2012) Cloud Computing-Concepts, Architecture and Challenges. 2012 *International Conference on Computing, Electronics and Electrical Technologies* (*ICCEET*), Kumaracoil, 21-22 March 2012, 877-880. http://dx.doi.org/10.1109/icceet.2012.6203873

[2] Xiao, Z., Song, W. and Chen, Q. (2013) Dynamic Resource Allocation Using Virtual Machines for Cloud Computing

Environment. *IEEE Transactions on Parallel and Distributed Systems*, **24**, 1107-1117. http://dx.doi.org/10.1109/TPDS.2012.283

[3] Wang, C., Wang, Q., Ren, K., Cao, N. and Lou, W. (2012) Toward Secure and Dependable Storage Services in Cloud Computing. *IEEE Transactions on Services Computing*, **5**, 220-232. http://dx.doi.org/10.1109/TSC.2011.24

[4] Hashizume, K., Rosado, D.G., Fernández-Medina, E. and Fernandez, E.B. (2013) An Analysis of Security Issues for Cloud Computing. *Journal of Internet Services and Applications*, **4**, 1. http://dx.doi.org/10.1186/1869-0238-4-5

[5] Armbrust, M., Fox, A., Griffith, R., *et al.* (2009) Above the Clouds: A Berkeley View of Cloud Computing.

[6] Rani, D.R. and Geethakumari, G. (2015) An Efficient Approach to Forensic Investigation in Cloud Using VM Snapshots. 2015 *International Conference on Pervasive Computing* (*ICPC*), Pune, 8-10 January 2015, 1-5. http://dx.doi.org/10.1109/pervasive.2015.7087206

[7] Morioka, E. and Sharbaf, M.S. (2015) Cloud Computing: Digital Forensic Solutions. 2015 12*th International Conference on Information Technology-New Generations* (*ITNG*), Las Vegas, 13-15 April 2015, 589-594.

[8] Sindhu, K.K. and Meshram, B.B. (2012) Digital Forensic Investigation Tools and Procedures. I*nternational Journal of Computer Network and Information Security*, **4**, 39. http://dx.doi.org/10.5815/ijcnis.2012.04.05

[9] Fernandes, D.A., Soares, L.F., Gomes, J.V., Freire, M.M. and Inácio, P.R. (2014) Security Issues in Cloud Environments: A Survey. *International Journal of Information Security*, **13**, 113-170. http://dx.doi.org/10.1007/s10207-013-0208-7

[10] Damshenas, M., Dehghantanha, A., Mahmoud, R. and bin Shamsuddin, S. (2012) Forensics Investigation Challenges in Cloud Computing Environments. 2012 *International Conference on Cyber Security, Cyber Warfare and Digital Forensic* (*CyberSec*), Kuala Lumpur, 26-28 June 2012, 190-194.


Scientific Research Publishing

Submit or recommend next manuscript to SCIRP and we will provide best service for you:

Accepting pre-submission inquiries through Email, Facebook, LinkedIn, Twitter, etc.
A wide selection of journals (inclusive of 9 subjects, more than 200 journals)
Providing 24-hour high-quality service
User-friendly online submission system
Fair and swift peer-review system
Efficient typesetting and proofreading procedure
Display of the result of downloads and visits, as well as the number of cited articles
Maximum dissemination of your research work

Submit your manuscript at: http://papersubmission.scirp.org/