An Integrated Research Analysis of Cloud Forensics for Secured Computing Environment

[1]N.Jaswanth
Department of CSE,
Sree Vidyanikethan Engg College,
Tirupati.AP,INDIA

[2]J.Durga
Assistant Professor,
Department of CSE,
Sree Vidyanikethan Engg College,
Tirupati.AP,INDIA

ABSTRACT:

Cloud Forensics under Cloud computing an on-demand paradigm becoming a well transformative technology in the computing now a day's grabbing important attention towards pursuing in-depth analysis of security issues, migrations from disasters, outages experienced by many CSP today in cloud environment. In spite of better understanding about the domain this paper shows updated current emerging significances, challenges, opportunities, case studies and various tools used in cloud forensics and in addition discuss valuable research issues and directions in cloud forensics that adds accountability and trust in cloud technology.

Key words**: Cloud Computing, Cloud forensics, challenges, CSP, research issues**

I. INTRODUCTION:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. (NIST) [1]. Gartner research estimates show us that by 2015 20% of non IT companies will be CSP. Various studies tells worldwide cloud service market hits $150.1 billion by 2013 and also size of average digital forensics cases growing 35% per year [2], As its emerging technology Cloud computing is said to be a game changing technologies in the recent history of computing. Unfortunately, due to its young age, cloud companies don't have yet any process that allows for a set procedure on how to investigate or go about cloud issues. Lack of this absence, they have no means of ensuring the robustness and suitability of cloud services when it comes to supporting investigations of criminal activity. Today many people, companies consider, understands cloud forensics in various perceptions that might lead to wrong side of coin some times. In general Cloud forensics is the application of digital forensics in cloud computing as a subset of network forensics. Basically, it is a cross-discipline between cloud computing and digital forensics. "Digital Forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data.” NIST [3]. Cloud computing, in turn, is based on broad network access, and thus follow the main principles found in the network forensic process with some techniques particularly tailored for the cloud computing environment. “The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and preservation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”.The computer crime will be extended to cloud crime, which is basically any crime that involves cloud computing in the sense that cloud can be the subject, object, or tool related to the crimes.

II. SIGNIFICANCE:

Digital Forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data. Its sometimes considered as a cross discipline of cloud computing and digital forensics. The value of the global cyber security market is expected to reach $120 billion by 2017, driven by changing threats and technologies, according to a recent report. According to a report by CA Technologies' internet security business unit, 'Crimeware-as-a-Service' is now an emerging trend, with almost all Trojans (96%) now developed as a result of this tactic.[4] It claimed that cyber criminals are also increasingly reliant on cloud-based web services and applications, such as Google Apps, Flickr and Microsoft Office Live, as well as real-time mobile web services to target general users. This section gives us in detail regarding significance in cloud forensics:

Most of prior surveys show that sequence of acceptance regarding cloud forensics significance is “it’s a part of cloud security”. “It requires more funding for its further R&D process for making cloud technology more transformative”, “lack of proper knowledge and lack of proper applying strategies”,”Lack of proper forensic expertise practices”. Coming to real scenario under significance we must consider it in terms of security, SLA, internal collaborations… etc.

Cloud Forensics has numerous uses [5], such as:

Investigation

- On cloud crime and policy violations in multi-tenant and multi-jurisdictional environments
- On suspect transactions, operations, and systems in the cloud for incident response
- Event reconstructions in the cloud

Troubleshooting

- Finding data and hosts physically and virtually in cloud environments
- Determining the root cause for both trends and isolated incidents, as well as developing new strategies that will help prevent similar events from happening in the future
- Tracing and monitoring an event, as well as assessing the current state of said event

Log Monitoring

Collection, analysis, and correlation of log entries across multiple systems hosted in the cloud, including but not limited to: audit assists, due diligence, and regulatory compliance

Data and System Recovery: Recovery of data in the cloud, whether it's been accidentally or intentionally modified or deleted

- Decrypting encrypted data in the cloud if the encryption key is already lost
- Recovery and repair of systems damaged accidentally or intentionally
- Acquisition of data from cloud systems that are being redeployed, retired or in need of sanitation

Due Diligence/Regulatory Compliance

Assist organizations in exercising due diligence as well as in complying with requirements related to the protection of sensitive information, maintenance of certain records needed for audit, and notification of parties concerned when confidential information is exposed or compromised.

III. CHALLENGES:

Today, the challenges are discussed in general where we need to focus on critical challenges [6] to overcome hidden security issues. For instance, the legal dimension currently has no agreements among cloud organizations when it comes to collaborative investigation, and majority of SLAs have no terms and conditions present when it comes to segregation of responsibilities between the cloud service provider and customer. Policies and Cyber laws from different regions must also do their part in order to resolve conflicts and issues arising from multi-jurisdiction investigations.

➢ Data collection:

Decreased access to forensic data means cloud customers generally have little or no control or even knowledge of the physical locations of their data. In fact, they may only be able to specify location at a high level of abstraction, typically as an object or container. CSPs intentionally hide data location from customers to facilitate data movement and replication.

➢ Live Forensics:

The proliferation of endpoints, especially mobile endpoints, is a challenge for data discovery and evidence collection. Because of the large number of resources connected to the cloud, the impact of a crime and the workload of an investigation can be massive. The use of disparate log formats is already a challenge in traditional network forensics. The challenge is exacerbated in the cloud due to the sheer volume of data logs and the prevalence of proprietary log formats. The challenges are to recover the deleted data, identify the ownership of the deleted data, and use the deleted data for event reconstruction in the cloud.

➢ Evidence Segregation:

It is a challenge for CSPs and law enforcement agencies to segregate resources during investigations without breaching the confidentiality of other tenants that share the infrastructure. Another issue is that the easy-to-use feature of cloud models contributes to a weak registration system. This facilitates anonymity, which makes it easier for criminals to conceal their identities and harder for investigators to identify and trace suspects.

➢ Virtualised Environments:

Hypervisors are prime targets or attack, but there is an alarming lack of policies, procedures and techniques for forensic investigations of hypervisors. Data mirroring over multiple machines in different jurisdictions and the lack of transparent, real-time information about data locations introduces difficulties in forensic investigations. Investigators may unknowingly violate laws and regulations because they do not have clear information about data storage jurisdictions.

- External dependency chains:

cloud forensic investigation thus requires investigations of each individual link in the dependency chain. An interruption or even a lack of coordination between the parties involved can lead to problems.

- Service Level Agreements:

Today maximum SLAs omit important terms regarding forensic investigation. This is due to low customer awareness, limited CSP transparency the lack of international regulation. Most cloud customers are unaware of the issues that may arise in a cloud forensic investigation and significance.

IV. CASE STUDIES:

This section discusses the most occurred recent outages [7] and disasters by CSP in cloud technology:

Amazon EC2 cloud service fueled play station network attack:

Hackers posed the normal business and signed up for legitimate server rental through EC2 service. Its not clear till now how hackers used EC2 to put the attack out.

- Microsoft's windows live hotmail:

Its Outage started on dec 30, 2011, it persisted till jan 2 2011. Almost 17,000 hotmail users inboxes got deleted.

- Amazon web services:

Suffered sweeping outages and service interruptions for customers. EBS services under amazon got stuck in Re-mirroring storm.

- Jive software: Several hundred jive software users wikis went down in January a cloud outage prompted by data center glitch.
- Google App Engine:

It didn't knock everything but affected most of its apps, websites.

V. TOOLS IN CLOUD FORENSICS:

OWADE Cloud Forensics tool: OWADE decrypts and geolocates the historical WiFi data stored by Windows, providing a list of wifi points the computer has accessed (including the locations of the access points to within500 feet) and when each point was last accessed. OWADE [8] is even able to partially recover the users data even when the user has utilized the browsers private mode. OWADE is written in Python, runs on Linux, and only uses GPL libraries and software (John the ripper, dd rescue). Its cryptographic engine is the first to fully re-implement the Windows DPAPI without using any windows dll files and is able to decrypt the Windows Credential store. Its registry analyzer is able to reconstruct the computer environment (hardware, network, user) almost perfectly and extract software information that allows OWADE to perform a vulnerability analysis post-mortem and to detect pirated software.

OWADE extracts software information from the registry for two purposes:

1. Finding potential vulnerabilities: OWADE is able to infer the list of potential vulnerability that affected the computer post-mortem by correlating the list of software installed on the machine and their version with a known list of vulnerabilities (CVE).

2. OWADE also compare the list of installed software with a list of known anti-virus and anti-malware to understand if the computer was protected.

Detecting Pirated software OWADE extract the installed software version serials to compare it with a list of serial number that are known to be pirated.

ISSUES:

1. Acquisition of data is more difficult.
2. Cooperation from cloud providers is paramount.
3. Cloud data may lack key forensic attributes.
4. Current forensic tools are unprepared to process cloud data.
5. Chain of custody is more complex.

RESEARCH DIRECTIONS: The research directions can be focused more on:

- FaaS (Forensics as a Service) [9]
- Internal Collaborations.
- Policies and mechanisms
- Laws & Approaches
- Architectures & new Investigating tools [10]

VI. CONCLUSION:

In this paper we discussed in detail regarding cloud computing, cloud forensics, its importance and critical areas not only under security considering all other aspects under cloud forensics investigation. We focused more on the current challenges, case studies and the recent current directions need to concentrate. As services like SaaS, PaaS, Iaas under cloud technology, FaaS (Forensics as a Service) must be included in mandatory sense in order to overcome the digital threats and issues causing critical troubles to customers in cloud technology. Future work can be focused on the innovative frame works, strategies that suggests the companies under cloud computing for better and secured services for their customers.

REFERENCES:

[1]http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2]http://www.rcfl.gov/downloads/documents/RCFL_Nat_Annual07.pdf

[3]http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

[4] http://www.cloudforensicsresearch.org

[5]http://cloudtimes.org/2012/11/05/the-basics-of-cloud-forensics.

[6]http://www.dcs.gla.ac.uk/~grisposg/Papers/calm.pdf

[7]http://www.crn.com/slideshows/cloud/240144284/the-10-biggest-cloud-outages-of-2012.htm

[8] http://cdn.ly.tl/talks/owade-paper.pdf

[9]http://www.dfinews.com/articles/2012/05/cloud-forensics-service-fraas

[10]http://www.igi-lobal.com/book/cybercrime-cloud-forensics/69206 . Cybercrime and Cloud Forensics: Applications for Investigation Process.