Volume 8, No. 2, March 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Cloud Computing Application: Its Security Issues and Challenges Faced During Cloud Forensics and Investigation

Osama Chaudhary
Department of CSE, SEST
JamiaHamdard, New Delhi, India
dipsite.osama@gmail.com

Arfiya S Siddique
Department of CSE, SEST
JamiaHamdard, New Delhi, India
arfiyaa@gmail.com

Abstract: Cloud computing is evolving web based technology. Which provide various service to physical IT infrastructure which is managed and hosted by third party. Features due to which cloud find its application in E-learning, cloud based ERP and E-governance are flexibility, availability, scalability, efficiency and reliability. As large number of computing technology is involved in cloud computing it is an object of security issues. In this research, we have discussed about basics of cloud computing, features, models, application, security issue, basics of digital forensics and cloud forensic as well as the challenges faced during the cloud investigation.

Keywords :Cloud computing, E-governance, cloud ERP, E-learning, Forensic, Cloud Forensics

I. INTRODUCTION

Cloud computing has revolutionized the digital world. It has completely changed the face of physical computer, software used and database storage. According to the official NIST definition, "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[1]. Another definition by Open Cloud Manifesto Consortium defines the key aspects of cloud computing as:
“the ability to scale and provision computing power dynamically in a cost-efficient way and the ability of the consumer (end user, organization, or IT staff) to make the most of that power without having to manage the underlying complexity of the technology. (The Open Cloud Manifesto Consortium, 2009)”[2]
With this we conclude that this practice of shared data resources has made cloud computing to act as a catalyst for ubiquitous computing. It has change the traditional approach of IT world.

Characteristics

The features of cloud computing that have changed the face of physical computing and has

urged traditional vendors to move to the cloud technology have been listed in this section.

- Resource pooling
- On demand service
- Scalability
- Virtualization
- Reliability
- Maintainability
- High performance
- Customizable
- Location independent
- Multitenancy
- Efficient resource utilization
- Cost pay-as-use

II. WHY CLOUD COMPUTING

In this section, we have analyzed what is making cloud rapid inroads.

Reduced labor cost

The research shows that cloud reduce labor cost by 50% in monitoring and maintenance, which fetch significant profit to business.[8]

Enhances utilization rate

Cloud enhance the utilization rate of various component through virtualization (para virtualization, partial virtualization or full virtualization). Upto 50% in full virtualization.

Reduces completion time

Location independent availability of resources reduces completion time from weeks to minutes

Reduced project cost

The Saas based on pay as you go model significantly cuts the project cost and reduces the cost of purchasing software license and software.

III. MODELS

To further sophisticate the approach of computing, cloud has different models according to the cloud environment, ownership, size and access required by the client.

Public cloud:

application and storage for public over the internet. E.g Amazon EC2, IBM’s Blue Cloud and Google App Engine service platform.

Private cloud:

service and infrastructure are dedicated to particular organization. It is more secure and expensive than public cloud.

Hybrid cloud:

combination of both public and private cloud. Use of private cloud in public cloud with set boundaries.

Community cloud:

Organization belonging to same community share computing infrastructure.

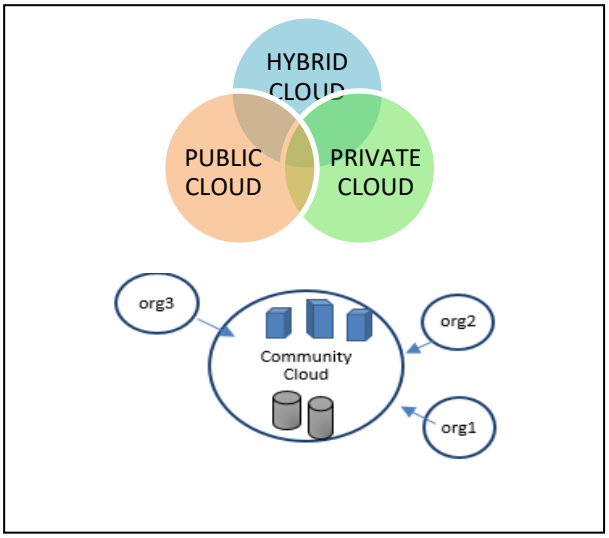

Figure 1: Different Cloud Models

IV. SERVICE MODELS

Saas

Software as a service referred as "on demand service" in which organization need not to install and run application on their computer, third party provider makes the application available to customer by hosting over the internet

Paas

Set of tools and services designed to make coding and deploying those applications quickly and efficiently

Iaas

Is the hardware and software that powers server, storage, network, operating system? It basically provides the infrastructure requirement of the organization.[7]

Service Models	Services Provided	Service Providers
Saas	Gmail, google doc, finance	Salesforce, google apps
Paas	Java2 runtime, developer tools, middleware	Window azure, google app engine
Iaas	Server, storage, processing power, networking	Amazon web service, Dropbox, Akamai

V. APPLICATION OF CLOUD COMPUTING

In this section we have discuss major application of cloud computing.[5][6]

Application	Services Provided	Service Providers
e-learning	Email, simulation tools, file broadcasting, shared interaction	Talent MS, Docebo SaaS LMS, Litmos LMS, WizIQ's LMS, Mindflash Online training LMS,
Cloud ERP	Supply chain vendor, Project & HR, customer relationship management, Finance and count	Oracle JD Edward, NetSuite, Epicor, Plex,
e-governance cloud	Complaint resolution system, employee management system, e-police, e-court, payment & tax system, transportation management system	Bharat Sanchar Nigam Ltd, Hewlett Packard Enterprise India Ltd, IBM India Pvt. Ltd, Tata Communications Ltd and Sify Technologies Ltd.

VI. ISSUES WITH CLOUD SECURITY

As cloud computing combines number of computing concepts and parameters such as network, application, host, privacy and legal aspect, service provider terms, client networks etc. securing all the parameters of cloud computing becomes a robust job. [12]

Cloud security in different cloud service models [11]

Services	User control over security	Issues
Saas	Very low	Security issues and bugs

	control	in application provided by third party, issue with security policies, issue related to multitenancy database, security challenges of data encryption & data backup
Paas	Partial control	Insecure third party web services, security of web hosted development tool and third party server
Iaas	Full control	Data Leakage Protection, End to End Logging and reporting, Infrastructure Hardening, infrastructure shared with vulnerable application

Cloud security in different cloud models

Model	Maintained by	Security level
Public	Cloud service provider	Low
Private	Single organization	High
Community	Several organization and service providers	High
Hybrid	Organization	Medium

VII. DIGITAL FORENSICS

Digital Forensic is the science of evidence recovery and investigation in crimes which involves digital devices. It has evolved over the years as the number of digital devices involved in crimes has increased.

Cloud Forensics

Cloud forensics, as the name suggest can be called as the subset of digital forensics (network forensics primarily). As cloud computing is the collection of network resources (e.g network, server, application and storage) so basically its forensic analysis of network.

Dimension of cloud forensics

- Data Collection
- Evidence Segregation
- Virtualized Environment
- Preservation of Evidence
- Reporting and Documentation

VIII. CHALLENGES IN CLOUD FORENSICS

As we have discussed various application in section [3] and security challenges in section [4]. These security issues lead to various cloud breach which paves the way too many cybercrimes. In this section, we discuss about the challenges face during cloud forensic investigation.

Traditional computer forensics involves:

- Collection of media at the crime scene or location where the media was seized
- preservation of that media
- validation
- analysis
- interpretation
- documentation

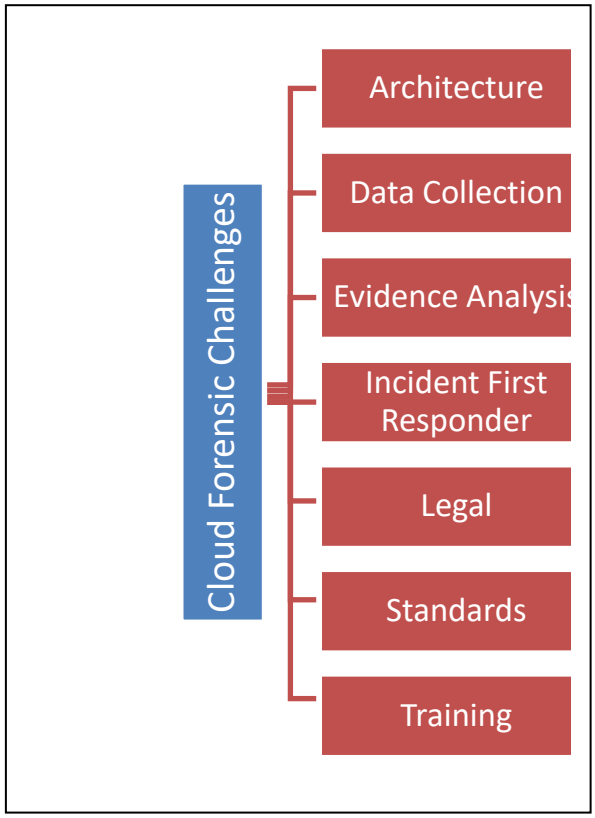

Figure 2: Cloud Forensic Challenges

In traditional Forensic investigation investigator usually have control over the evidence collection however in cloud computing investigation evidence are not physically accessible. Further the analysis of available artifacts and logs becomes challenging for the investigator. The forensic challenges faced during investigation of cloud computing are related to control of the evidence, including collection, preservation and

validation. With cloud computing, investigation agency does not have physical control of the media nor the network on which it exists. Comparative Study of Cloud Forensics tools has been done in [13].

CHALLENGES	ABOUT
Data Gathering	Most crucial step of investigation. It becomes to set boundaries of evidence collection over cloud. Huge data is stored over cloud
Identifying the evidence	To identify where exactly the evidence resides is a challenge
Legal	e.g., jurisdictions, laws, service level agreement. Identifying issues of jurisdiction. Lack of international communication and support
Standards	e.g standard operating procedures, testing, validation. Lacks of proper practice and standards
Training	Lack of proper forensic training and investigation knowledge

IX. CONCLUSION

As we have discussed various application in section [3] and security challenges in section [4]. These security issues lead to various cloud breach which paves the way for many cybercrimes. In this section, we discuss about the challenges faced during cloud forensic investigation.

The Cloud face of IT industry in terms of application, concept, cost, security and availability is undoubtedly commendable.

Various service model and types of cloud makes cloud computing effective, categorical service, geological load balancing, improved performance and service.

Cloud application reduces the cost, enhances business outcomes and significantly improves performance.

Cloud Forensic is challenging and is pushing the boundaries of digital forensics. Cloud forensics brings many technological, legal, geographical and organizational challenges.

X. REFERENCES

[1] NIST Cloud Computing 11 Forensic Science Challenges, Draft NISTIR

[2] Quoted under report, “The Open Cloud Manifesto Consortium: A call to action for the worldwide cloud community”, Draft 1.0.7, 2008

[3] Nitin Kumar, Shrawan Kumar Kushwaha and Asim Kumar, “Cloud Computing Services and its Application” ISSN 2231-1297, Volume 4, Number 1 (2014)

[4] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, “An analysis of security issues for cloud computing”, Journal of Internet Services and Applications 2013

[5] Quoted under cloud ERP service provider, http://www.enterpriseappstoday.com/erp/11-cloud-erp-software-options-1.html

[6] Jon Brodkin “Gartner: Seven cloud-computing security risks Data integrity, recovery, privacy and regulatory compliance are key issues to consider”, July 02, 2008

[7] 8006 Ahmed E. Youseef “Exploring cloud computing services and applications” vol. 3 no. 6 July 2012.

[8] H. Guo et al. “Forensic investigations in cloud environments”, in Computer Science and Information Processing (CSIP), 2012 International Conference on. IEEE, 2012.

[9] Dominik Birk, “Technical Challenges of Forensic Investigations in Cloud Computing Environments, in Workshop on Cryptography and Security in Clouds”, January 12, 2011.

[10] Ragib Hasan, “Security and Privacy in Cloud Computing”.

[11] Pearson, S. and AzzedineBenameur, “Privacy, Security and Trust Issues Arising from Cloud Computing” IEEE Second International Conference Cloud Computing Technology and Science (CloudCom), Nov 30-Dec 3, 2010.

[12] Osama Chaudhary, Cloud Forensic and Challenges, Blog Published by digital4n6journal.com, 8 Feb 2017.

[13] Sameena Naaz, Faizan Ahmad Siddiqui, “Comparative Study of Cloud Forensics Tools”, Communications on Applied Electronics (CAE) ISSN: 2394-4714, Foundation of Computer Science FCS, New York, USA Volume 5 – No.3, June 2016, page 24-30.