Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Some Forensic & Security Issues of Cloud Computing

Ashish Badiye*, Neeti Kapoor
Assistant Professor,
Institute of Forensic Science,
RTMNU, Nagpur, INDIA

Pooja Shelke
Assistant Professor,
G H Raisoni College of Engineering
Nagpur, INDIA

Abstract - The field of cloud computing is still in its early years as far as implementation and usage, partly because it is heavily promoted by technology advancement and is so high resource dependent that researches in academic institutions have not had many opportunities to analyze and experiment with it. However, cloud computing arises from the IT technicians aspiration to add another layer of unification in processing information. At the moment, a general understanding of cloud computing refers to the following concepts:

- ***network computing,***
- ***utility computing,***
- ***software as a service,***
- ***storage in the cloud***
- ***Virtualization.***

These refer to a client using a provider's service remotely, also known as in the cloud. Even if there is an existent debate on whether those concepts should be separated and deal with individually, the general agreement is that all those terms could be summarized by the cloud computing umbrella. Cloud Computing is one of the hottest topic discussed today in the field of IT giving many future oriented technological and economical opportunities. Many customers remain hesitant to move their business IT infrastructure completely to this virtual place. Given its recent development and insufficiency of academic published work, many discussions on the topic of cloud security have surfaced from engineers in companies that provide the aforementioned services. This paper introduces the current state of cloud computing, with its development challenges, academic circles and industry research efforts. Further, it describes cloud computing security problems and benefits and showcases a model of secure architecture for cloud computing performance.

Keywords: cloud computing secure architecture, cloud forensics, cloud modeling, security issu

I. Introduction

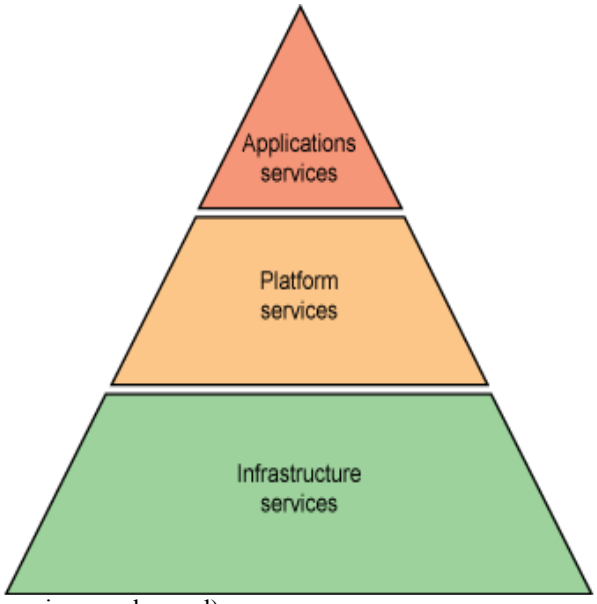
Cloud computing is a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software and that's the specialty of CC. It is a computing in which scalable and often virtualized resources are provided as a service over the Internet. Cloud Computing is an Internet-based development. The cheaper and more powerful processors, together with the "software as a service" (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. Meanwhile, the increasing network bandwidth and reliable yet flexible network connections make it even possible that clients can now subscribe high quality services from data and software that reside solely on remote data centers. Although envisioned as a promising service platform for the Internet, this new data storage pattern in "Cloud" brings about many challenging design issues which have intense influence on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that of data integrity authentication at entrusted servers. For example, the storage service provider, which experiences complicated failures occasionally, may decide to hide the data errors from the clients for the benefit of their own. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client.[1] Cloud Computing is a model that focuses on sharing data and computations over a scalable network of nodes. Examples of such nodes include end user computers, data centers, and Cloud Services. We term such a network of nodes as a Cloud.[1] The concept based on 3 services; Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as well as Web 2.0 and other recent innovative technology trends which rely over the Internet for fulfilling the computing needs of the users.

SaaS: The cloud user, dependent on their contracted services with the cloud vendor will only control certain configuration parameters, whilst the cloud vendor maintains control over applications and infrastructure.

PaaS: The cloud seller controls the cloud infrastructure and runtime environments when the cloud user controls the application.

IaaS: Although a cloud user will have control over their servers with the installed Operating System & Applications with this the cloud offering the cloud vendors will still controls the virtualization infrastructure and at least parts of the network infrastructure.

***Cloud Architecture**



• Application Services (services on demand)
– Gmail, Google Calender
• Platform Services (resources on demand)
– Google Appengine
• Infrastructure as services (physical assets as services)
– IBM Blue house, VMWare, Amazon EC2, Microsoft Azure Platform, Sun Parascale etc.

II. Deployment Models In Cloud Computing

Private Cloud- This is referred as cloud for individuals, where everything is with you only the control and ownership. The infrastructure is operated exclusively by the organization who is actual owner of that cloud. The owner has managerial control, and includes only that same organization's data. In this model the access control is with the user or owner.

Community Cloud- This is shared amongst several organizations, either because of a common organizational goal, or in order to pool IT resources. Community clouds may be located within one or more of the community organization's premises, and will be administered by the community. It is like a group of people with the same interest and fulfilling their requirements with a common source.

Public Cloud- This will usually be owned by a provider organization, which will maintain the cloud facilities in one or more corporate data centers. The administrative control of the cloud resources will therefore reside with the provider, rather than the user.

Hybrid Cloud- This is a composition of two or more of the above deployment models. Hybrid clouds can be used to provide load-balancing to multiple Clouds.[2]

III. Advantages Of Cloud Computing

Vast Range: Obviously, the biggest facility that cloud computing provides is access to a variety of applications. More importantly, user has neither to install software for this nor face any storage problems.

Flexibility: One of the major benefits of cloud computing is that there is no limitation of place and medium. We can reach our applications and data anywhere in the world, on any system.

Cost-effective: Cloud computing services are easily affordable. User needs not expend on hardware and software systems.

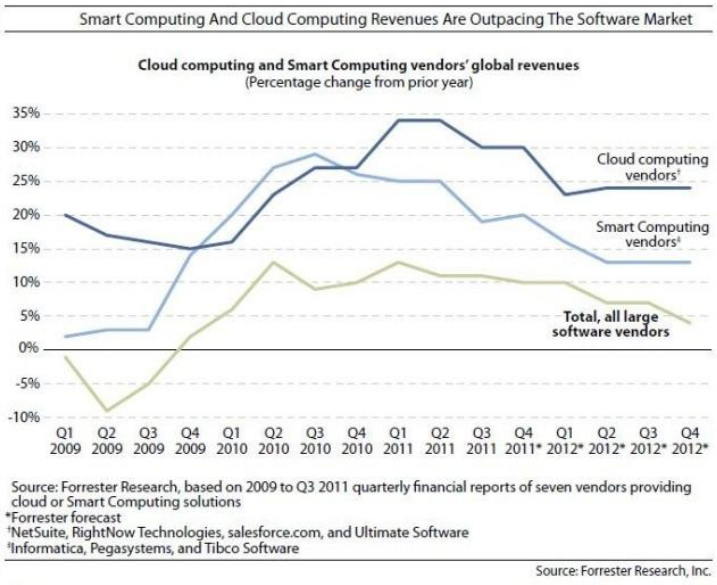
Synchronization and Integrity: Business people can share their data or documents on internet and at one place. They are independent of carrying any specific hardware or software with them. [3 - 4]

IV. Disadvantage Of Cloud Computing

Dependency: Among certain limitations of **cloud computing** is users' dependency on the provider. **Risk and Insecurity:** Cloud **computing** services mean taking services from remote servers. User doesn't have control over their software. Also, there is always insecurity regarding stored documents. Nothing can be recreated if their servers go out of service.

Migration Problems: In case the user has to switch to some other provider, there are migration issues. It's not easy to transfer huge data from one provider to the other. [3]

*** Growth analysis of cloud computing**



***Growth of Cloud Computing Vs Smart Computing**

The inflexion point of Smart Computing will happen when analytics, BI and awareness-based technologies including RFID can be used to make customer experiences consistently positive and drive cultural change throughout a business to centre on customers' expectations. In 2012, financial services, professional services, and manufacturing will be the three industries that dominate software purchases.

***Risk in Cloud Company**

Cloud computing has "exclusive attributes that require risk measurement in areas such as data integrity, recovery and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance and auditing," Gartner says. (Compare security products.)Customers must demand transparency, avoiding vendors that refuse to provide detailed information on security programs. Ask questions related to the qualifications of policy makers, architects, coders and operators; risk-control processes and technical mechanisms; and the level of testing that's been done to verify that service and control processes are functioning as intended, and that vendors can identify unexpected vulnerabilities.

Cloud computing is fraught with security risks, according to analyst firm Gartner. Smart customers will consider getting a security assessment from a impartial third party before committing to a cloud seller, Gartner says in a June report titled "Assessing the Security Risks of Cloud Computing."[5]

V. Security Issues

Here are seven of the specific security issues Gartner says customers should raise with vendors before selecting a cloud vendor. [5]

Privileged user access

Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. "Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access," Gartner says. [5]

Regulatory compliance

Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions," according to Gartner. [5]

Data location

When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises. [5]

Data segregation
Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says. [5]

Recovery
Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a failure. "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."

Investigative support
Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then our only safe assumption is that investigation and discovery requests will be impossible."

Long-term viability
Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. "Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application," Gartner says [5].

VI. Challenges

In order to establish a forensic capability for cloud organizations we are facing enormous challenges. International cyber law and policies must progress to help resolve the issues surrounding multi-jurisdiction investigations.

Challenges in elastic, static and live forensics
The production of endpoints, especially mobile endpoints, is a challenge for data discovery and evidence collection. The impact of crimes and the workload of investigation can be exacerbated in cloud computing simply because of the sheer number of resources connected to the Cloud. Time synchronization is crucial to the audit logs that are used as source of evidence in the investigation. Accurate time synchronization has been always an issue in network forensics, and is made all the more challenging in a cloud environment as timestamps must be synchronized across multiple physical machines spread in multiple geographical regions, between cloud infrastructure and remote web clients including numerous end points. In AWS (Amazon Web Service) the right to alter or delete the original snapshot is explicitly reserved for the AWS account that created the volume. When item and attribute data are deleted within a domain, removal of the mapping within the domain starts immediately, and is also generally complete within seconds. Once the mapping is removed, there is no remote access to the deleted data.

Challenges in evidence segregation
Customer instances have no access to raw disk devices, but instead are presented with virtualized disks. On the physical level system audit logs of shared resources and other forensic data are shared among multiple tenants. Currently, the provisioning and de-provisioning technologies still need to be much improved in the Cloud (CSA, 2009), and it remains a challenge for the CSP and law enforcement to keep the same segregating in the whole process of investigation without breaching the confidentiality of other tenants sharing the same infrastructure and ensure the admissibility of the evidence. Another issue is that the easy-to-use feature of cloud models results in a weak registration system, facilitating anonymity that is easy to be abused and making it easier for cloud criminals to conceal their identities and harder for investigators to identify and trace suspects as well as segregate evidence. Moreover, encryption is used in the Cloud to separate data hosting of the CSPs and data usage of the cloud customers and most of the major CSPs encourage customers to encrypt their sensitive data before uploading to the Cloud if encryption is not provided by the CSP by default (Amazon, 2010; Force.com, 2010; Google, 2010). Unencrypted data in the Cloud can be considered lost from a strict security perspective. A chain of separation is required to segregate key management from the CSP hosting the data and needs to be standardized in contract language. [6]

Challenges in virtualized environments
Cloud computing claims to provide data and compute redundancy by replicating and distributing resources. However in reality most CSPs implement instances of a cloud computer environment in a virtualized environment. Instances of servers run as virtual machines, monitored and provisioned by a hypervisor. The hypervisor in a Cloud is analogous to a kernel in the traditional operating system. Attackers will aim to focus their attacks against the hypervisor; compromise of the hypervisor amplifies any attack as many compute resources rely on its security. For law enforcement and cloud investigators, however, there is a huge lack of policies, procedures and techniques on hypervisor level to facilitate investigation. Furthermore, the distributed nature of cloud computing forces a stronger international collaboration

between law enforcement and industry, in cases such as confiscating "a Cloud" since the agency of single nation cannot manage it when the physical servers are spread across different countries.

Challenges in internal staffing

Today most cloud organizations are dealing with investigations with traditional network forensic tools and staffing, or are simply neglecting the issue. The major challenge in establishing a cloud forensic organizational structure is the lack of forensic expertise and relevant legal experience. The deep-rooted reasons for this challenge, which is also a challenge for the whole discipline of digital forensics, are firstly, the relative slow progress of forensic research compare to the rapidly evolving technology and secondly, the slow progress of relevant laws and international regulations. With only a decade of research and development, the discipline of digital forensics is still in its infancy, new forensic research areas in non-standard systems (Beebe, 2009), such as cloud computing, need to be explored, techniques need to be developed, regulations need to catch up, law advisors need to be trained, staff need to be equipped with new knowledge and skills to deal with the new grounds for cyber crimes created by the rapid rise of new models such as cloud computing.

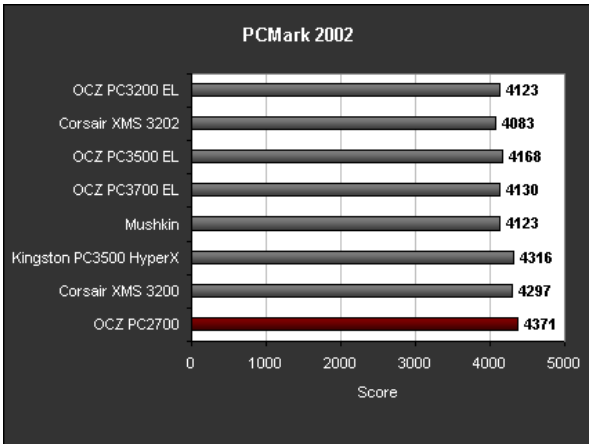
VI. Investigation Procedures On A Cloud Environment

1. Client Analysis

It is like a post-mortem of client machine and consists of primary steps of investigation procedure. Firstly the power is cut which leads to freezing of persistent data in its current state. This maintains the integrity of the evidence which is one of the important aspect of IT security. Thereby creating mirror image of the data and analyzing it. While examining the investigator has to concentrate on online services used by the client like browser history, web mail, cache files, log files, cookies so on. This gives vital information about the client and the machine and may focus the mind of investigator towards CSP's.

2. Client-Ram Forensics

This is the live analysis of data on client machine and it is very rich data when it comes to cloud computing.



This is the data which is not included or available with dead forensics; live analysis can capture this data. It may include analysis of RAM, chatting sessions, various encrypted files, passwords, currently running services and processes and network traffic analysis. Analysis of this data requires specialist technicians which is generally not possible for the law enforcement people. Technical attendant reduces the amount of machines seized and the data to be analyzed further in the forensic lab. This can help in cracking the case much faster than the traditional way.

3. Analysis of Cloud Service Provider

Investigation of server is the most difficult task to be done by the investigator. It is because investigator is not aware of what type of data and records are held by the CSP's. In case of organization services (private cloud) used by the employee there are more chances of co-operation from the CSP's. There are chances of less security measures taken by the service provider regarding the safety of data of an organization. This may also because of cost implications in storing log of all data for a period of time. If we think about public cloud the case gets worst.

4. Network Traffic Analysis

Network is one more and valuable source of data between client and CSP's communication. Traffic relevance, data integrity, and packet capture rate are primary concerns when positioning an NFAT (Network Forensic Analysis Tool) on a network. Before placing a NFAT, the traffic of interest should be identified. A good NFAT must be able to capture and store the packets form a highly saturated network this is the area where some NAFT fails. Network filter can also be used by the investigator to divert the traffic which is of no use.

The most popular packet-collection software available today is tcpdump **(www.tcpdump.org/tcpdump.man.html)**. It is available to the root user on most UNIX platforms as well as under Windows. It has little disadvantage regarding storage management, it keeps on storing the data and record on the disk

and this may sometimes lead to memory crash, so the investigator has to be attentive. One more point of concern is handling of encrypted data. Due to security issues a CSP can use network security protocols such as SSL.

5. API Analysis

An API (Application program interface) is the set of commands used by end clients to interact with the cloud service. This is not practiced by all CSP. The API commands are not standardize. If the end user is accessing cloud, then the API will include commands to start, stop and restart the machine. The APIs are created by the CSP.

6. Validation of Data

Software hashing tools are commonly used in conventional investigations to validate the on-going integrity of data used as evidence. A hash function is an algorithm for converting arbitrary length data strings into fixed length hash values, typically a few hundred bytes in length. Hash functions are designed so that any change in the input data should (with high probability) produce a different output hash value.

VII. Conclusion

This paper has considered number of impacts of cloud computing on digital forensic investigations. It has focused on technical and legal difficulties faced by a forensic investigator during investigation in virtual environment. If we see current scenario of the world, more businesses and organizations will be moving their data to cloud environments in near future. Development in the IT sector will create new complexities for the Crime investigators in accessing, retrieving and acquisition of evidential data. With the emerging technology there will be growth in cyber crime and the demand to conduct forensic investigation on cloud will increase.

Such investigations may face lack of guidance, tools and techniques to retrieve evidence in a forensically sound manner. There is also the need for sound laws regarding clouds including data retention and privacy. Current available laws should be re-examined because of the need to precede ahead and combating criminals.

References

[1] V. Vinaya, P. Sumathi, "Implementation of Effective Third Party Auditing for Data Security in Cloud", *International Journal of Advanced Research in Computer Science and Software Engineering (I.J.A.R.C.S.S.E)*, Volume 3, Issue 5, May 2013

[2] .https://www.ibm.com/developerworks/communiy

[3] *http://djacademy.ac.in/TechFreaks/cloud.html*

[4] *http://www.cloudstoragecenters.com/advantages-and-disadvantages-of-cloud-computing-system/*

[5] Jon Brodkin "Gartner: Seven cloud-computing security risks Data integrity, recovery, privacy and regulatory compliance are key issues to consider", July02, 2008

[6] Keyun Ruan, Joe Carthy, Prof. Tahar Kechadi, Mark Crosbie, "Cloud forensics: An overview", http://www.scribd.com/doc/134477529/Cloud-Forensics

[7] Casey, E. Handbook of Computer Crime Investigation, Academic Press. Boston. 2002

[8] W.Kruse, J. Heiser, "Computer Forensics: Incident Response Essentials", Addison Wesley. New York. 2002

[9] R. Richardson, CSI Computer Crime and Security Survey, 2008

[10] http://www.gocsi.com/forms/csi_survey.jhtml (March/April 2009)

[11] M.K Rogers, K. Seigfried, "The Future of Computer Forensics: A Needs Analysis Survey. Computers & Security" Volume 23 (1), 2004. pp. 12-16.

[12] George Grispos, William Bradley Glisson, Tim Store, "Calm before the Storm: The Emerging Challenges of Cloud Computing in Digital Forensics" 2011

[13] Stephen Biggs, Stilianos Vidalis, "Cloud Computing Storms" *International Journal of Intelligent Computing Research (IJICR)*, Volume 1, Issue 1/2,June 2010.

[14] Vicka Corey, Charles Peterman, Sybil Shearin, Michael S. Greenberg, & James Van Bokkelen, "Network Forensics Analysis, IEEE INTERNET COMPUTING' Nov-Dec 2002.

[15] Ricci S.C. Ieong, Forza "Digital forensics investigation framework that incorporate legal issues" (www.elsevier.com/locate/di.in)

[16] Information Technology Act, 2000; amended by IT(amendment) Act, 2008

[17] Pooja Shelke, Ashish Badiye, "Biometric for Enhancement of Security Standard"Vol-2, Issue-9,sep 2012

