Vandana Publications

Volume-4, Issue-1, February-2014, ISSN No.: 2250-0758

International Journal of Engineering and Management Research

Available at: www.ijemr.net

Page Number: 190-193

A Study on Security Challenges, Threats and Vulnerabilities in Cloud Computing

P. Madhubala[1], Dr.R.Thangaraj[2]

[1] Research Department of Computer Science, Mother Theresa Women's University, Kodaikanal, TN, INDIA

[2] Department of CSE , Bannari Amman Institute of Technology, Sathiyamangalam, TN, INDIA.

ABSTRACT

Cloud computing has recently evolved as a new paradigm for hosting and delivering services over the internet. It moves the application software and data to be centralized to large centers where the pool of data and information is maintained by the cloud providers. Also cloud services are simpler to acquire and scale up and down. Cloud computing security is the key driving force for information security in the software industry. Even though cloud computing is efficient and promising, there are many challenges for data security as the cloud user does not know the location of the data.. There are challenges faced by both the cloud providers and consumers. Cloud providers must ensure that consumer's data is protected. Consumers must have confidence that the integrity, confidentiality, privacy, availability, identity and access management of their data is guaranteed. It is important to understand the levels at which there can be security vulnerabilities. In our opinion virtual infrastructure, storage and data access vulnerabilities are the foremost challenges. The objective of this article is to provide an analysis of the security and privacy challenges significant to cloud computing

Keywords—**Security, SLA-Service Level Agreement, VM-based malware brute force.**

I. INTRODUCTION

The Cloud Computing Model is a new paradigm that was developed to provide economic resource utilization over the Internet. Companies such as Google, Microsoft, IBM, Amazon and Yahoo are providing Cloud Services to end-users as well as entire organizations. Cloud Computing is a method of computing in which users can increase or decrease their computing resources. These resources are generally virtualized and provided as a service over the internet. End-users simply consume these services and pay on usage basis or subscription basis.

1.1 Deployment Models of Cloud:

There are three famous deployment models of cloud computing as described below:

Public: In public cloud (also known as external cloud), the services are provided by a third party via Internet, and they are available and are for commercial purposes.

Private: In private cloud, the cloud consists of hosting private applications and services for private use only (private networks).

Hybrid: In hybrid cloud, the cloud is a combination of public and private cloud. This is the suitable option for those who want to invest minimally in infrastructure and data storage with more security.

1.2 Service models of cloud

As well as by deployment models, cloud computing provisioning is categorized as follows: according to the service models used to provide capability to the outsourcing user.

The following are common cloud computing service models:

With Infrastructure as a Service (IaaS) the cloud provisions such basic IT infrastructure as storage, network and computing capacity.

With Platform as a Service (PaaS) the cloud provisions higher infrastructure-level services for the consumer. In both a RunTime Environment (RTE) and an Integrated Development Environment (IDE) the cloud enables users to configure differentiated applications for their own individual needs.

With Software as a Service (SaaS) software is provided as an integrated service network based on the cloud infrastructure. Consequently users save the costs of hardware, software licenses and maintenance of the IT.

With Something-as-a-service (XaaS) there are many variants:

Infrastructure-as-a-Service - Virtual resources, such as servers, hard drives, storage, data bases and IP addresses

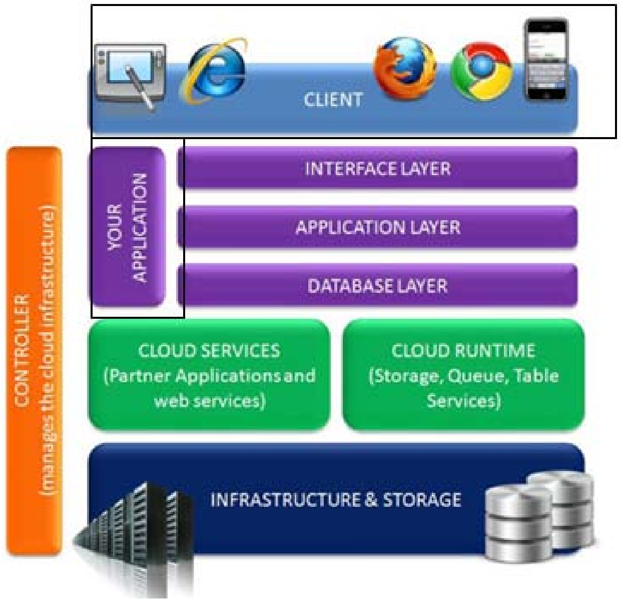
Platform-as-a-Service - Deployment and configurations

Software-as-a-Service - Software modules or components.

1.3 Basic Cloud Architecture

To understand the architecture in the most basic sense, the entire setup is divided into two parts.

Front End - This is the part visible to the user. The client computer and the applications needed to access the cloud are in this part of the architecture.


CLIENT
YOUR APPLICATION
INTERFACE LAYER
APPLICATION LAYER
DATABASE LAYER
CONTROLLER (manages the cloud infrastructure)
CLOUD SERVICES (Partner Applications and web services)
CLOUD RUNTIME (Storage, Queue, Table Services)
INFRASTRUCTURE & STORAGE

Back End - The Cloud Service Layer is responsible for the services that the cloud actually provides.

The Cloud Runtime Layer consists of the various technologies used to implement the cloud. The Cloud Runtime Layer manages the requests and monitors the amount of resources used by each user. The actual application or services being used by the user is executed by using the Interface, Application and Database Layers in conjunction with each other. All the layers and the interfaces between them are monitored by a Cloud Controller that controls the entire cloud and its functions.

1.4 Characteristics of cloud computing.

The following characteristics summarize the essentials of the technology of cloud computing:

- **On-Demand-** The resources are available to the user as and when he needs it. The availability of resources should be controllable by the Resource Provider.
- **Scalable-** The user must be able to increase or decrease the resources as needed. The Resource Provider must be able to support the variable resource demand.
- **Reliability-** Since the user depends on the service provider completely, the services must be reliable.
- **Utility-Based Subscription-** The user should only be asked to pay for the services he uses and the amount of resource usage without any extra charges.
- **Maintenance-** The user is not responsible for upgrading and maintaining the applications on the cloud. Thus, it becomes easy to maintain cloud applications as changes only need to be made on the cloud and not on individual units.
- **Access Independence-** Since the application and all the data are on the cloud, the user can access the application from anywhere and from any device.
- **Multi-Tenancy-** Allows the sharing of resources and costs of the entire set-up amongst a large number of users that use the same resources for various services.
- **Resource Pooling -** All the resources (such as storage, processing, etc.) of the service provider are pooled together to provide varied services to the users using dynamic scalability.

1.5 Applications of cloud computing

The Cloud Computing technology becomes ideal in the following three cases of workloads:

- **Unpredictable User Estimate** – The salability offered by Clouds becomes ideal in situations where users cannot be estimated at the time of creation.
- **Cyclical**– Applications with fluctuations in usage can benefit from the metered services provided by the pay-as-you-go model of cloud computing.
- **Parallelized-** Applications (such as Big Data analytics) work better with parallel scaling across servers as compared to scaling to one large server.

1.6 Example of cloud computing

A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. Users do not need software or a server to use these e-mail services. All a consumer would need is an internet connection for sending or receiving emails. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo, Google etc.

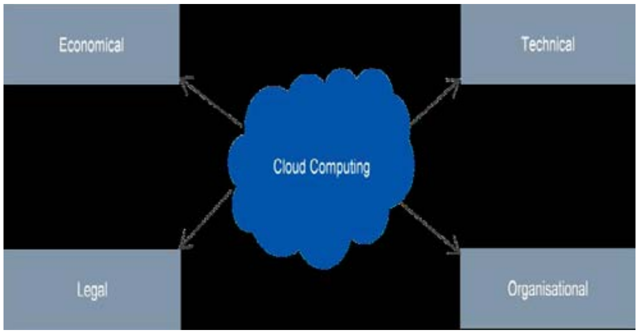
II. SECURITY IN CLOUD

2.1 Traditional Security

Security concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company. Another argument, made by the Jericho Forum [16], is: "It could be easier to lock down information if it's administered by a third party rather than in-house, if companies are worried about insider threats. In addition, it may be easier to enforce security via contracts with online services providers than via internal controls”.

2.2 Current Security Challenges

Hackers and worms can attack a system and create devastation within a few hours. Time, cost, innovation are great benefits of cloud computing but still there are significant security concerns of cloud computing that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. For all the benefits that cloud computing promises, it also poses a number of challenges for providers and consumers, chiefly of a technical, legal, economic and organizational nature. The main hurdles to be negotiated lie in sufficient utilization of the IT capacities, contractual complexities, regulations on data access, the concentration of data and the fact that the user is tied to one cloud provider.



Major security issues related to those faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers are discussed below:

Availability - There are currently two major threats in this regard. First is network-based attacks; second is availability of the Cloud Service Provider itself.
Access to data - Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been entrusted with approved access to the cloud. Anyone using the cloud needs to look at who is managing their data and what types of controls are applied to these individuals.
Authentication & Authorization--Every organization has its own way to manage authentication and authorization. Every organization must determine if its current authentication system could also work in a secure and reliable way for users in a cloud environment. Apart from that, there is no way to insure authentication of cloud services.
Confidentiality – Management of Security Keys is a complex and difficult task for both the individual customers and for Cloud Service Providers.
Identification of Data - organizations located in different geographical regions have different requirements and controls placed on data access. Because the data is in the cloud, one may not realize that the data must reside in a physical location. The cloud provider should provide the level of security required for different customers and their needs.
Legal Issues - Providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country.
Service Level Agreement (SLA) terms - The SLA serves as a contractual level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided.
Security Violation - Many encryption algorithms provide insufficient security.

2.3 New challenge in Mobile Cloud Applications:

A challenge specific to Mobile Cloud Computing is Task partitioning at design time and at run time (offloading) of an application – deciding what goes on the mobile and what goes on the cloud.

2.4 Future Challenges

- Runtime monitoring of the cloud provider’s performance such as SLA’s and network conditions.
- Privacy and security beyond authentication and authorization.
- Legal challenges posed by the fact that issues pertaining to liability, responsibility and contractual obligation can often only be examined legally on a case by case basis. Such examination must, for example, take into account that cloud users are, in turn, liable to their customers in the event of the cloud vendor‘s failure to provide the proper service.

2.5 Future research priorities

In our opinion the following areas of cloud services should be focused toward research to face the security challenges described.

- Make legacy provisioning and billing systems more flexible. The lack of flexibility in the provisioning and deployment of services is not compatible with cloud environment.
- Implement automatic deployment and provisioning of cloud solutions.
- Improve the following security characteristics:
  - “Shared” accreditation
  - Validation of customer applications
  - Integrating Software as a Service
  - Accessing federated and shared services
  - Varying interpretations of security guidelines

III. THREATS AND VULNERABILITIES

3.1Attacks targeting multi-tenancy environment

By identifying the target VMs (Virtual Machines), attackers can potentially monitor the cache in order to steal data hosted on the same physical machine (Hardesty 2009). Such an attack is also known as a side-channel attack

3.2 Data availability

A major risk to business continuity in the cloud computing environment is loss of internet connectivity (that could occur in a range of circumstances such as natural disasters) as businesses are dependent on the internet access to their corporate information. In addition, if vulnerability is identified in a particular service provided by the cloud service provider, the business may have to terminate all access to the cloud service provider until they can be assured that the vulnerability has been rectified.

3.4 VM-based malware

Vulnerabilities in VMs can be exploited by malicious code (malware) such as VM-based rootkits designed to infect both client and server machines in cloud services. Rootkits are locking technologies usually employed by other malware programs to abuse compromised systems by hiding files, registry keys and other operating system objects from diagnostic, antivirus and security programs. For example, in April 2009, a security researcher pointed out how a critical vulnerability in VMware’s VM display function could be exploited to run malware, which allows an attacker 'to read and write memory on the "host" operating system [OS]' (Keizer 2009: np).

3.5 Launch pad for brute force and other attacks

There have also been suggestions that the virtualized infrastructure can be used as a launching pad for new attacks. A security consultant recently suggested that it may be possible to abuse cloud computing services to launch a brute force attack(a strategy used to break encrypted data by trying all possible decryption keys or password combinations) on various types of passwords. Using Amazon EC2 as an example, the consultant estimated that based on the 'hourly fees Amazon charges for its EC2 web service, it would cost more than [US]$1.5m to brute force a 12-characterpassword containing nothing more than lower-case letters a- z…[but] an 11-character code costs less than [US]$60,000 to crack, and a 10-letterphrase costs less than [US]$2,300' (Goodin2009: np).

Since the establishment of cloud computing the numerous cloud vulnerability incidents has risen considerably. For instance, the number of cloud vulnerability incidents more than doubled, increasing from 33 in 2009 to 91 in 2013. A total of 172 unique cloud computing outage incidents were uncovered, of which 129 (75%) declared their cause(s) while 43 (25%) did not. As cloud computing matures into mainstream computing, transparency in the disclosure of outages is imperative.

The investigation revealed that the top three threats were **"Insecure Interfaces & APIs"** (51 incidents; 29% of all threats), **"Data Loss & Leakage"** (43 incidents; 25%), and **"Hardware Failure"** (18 incidents; 10%). These three threats accounted for 64% of all cloud outage incidents. The investigation based its threat categories on the Cloud Security Alliance's Top Threats to Cloud Computing v 1.0 (CSA Top Threats) [2]. After a thorough review of reported incidents, 128 incidents were grouped into the 8 threats contained in the Top Threats Report while 44 incidents were unable to be categorized. Therefore, the authors propose five new categories to accommodate the remaining 44 incidents: Hardware Failure, Natural Disasters, Closure of Cloud Service, Cloud-related Malware and Inadequate Infrastructure Design and Planning.

CONCLUSION

In this paper we examined the basics of cloud computing, analyzed the security challenges, threats and vulnerabilities. In order for there to be wide acceptance of cloud computing there needs to be further analysis in the implementation and adaptation of the Cloud Technology. Thus, to maximize the benefits of this technology it becomes necessary to evaluate the existing implementations, because there may be loss of data and privacy. Researchers, Scholars and IT security professionals must come forward with practical achievements in security and privacy to users. Our study identifies top security concerns of cloud computing and its services.

ACKNOWLEDGEMENT

I would like to express my sense of gratitude to
DON BOSCO COLLEGE, Dharmapuri for their support and encouragement. And also I like to thank
MOTHER THERESA WOMEN'S UNIVERSITY, Kodaikanal for providing me the opportunity to carry out the research work in Cloud Computing. Finally I like to thank my Research Supervisor Dr.R.Thangaraj for his guidance and valuable suggestions.

REFERENCES

[1] AlZain, M.A., Pardede, E., Soh, B. & Thom, J.A. (2012). Cloud Computing Security: From Single to Multiclouds,45th Hawaii International Conference on SystemSciences. *IEEE ComputerSociety*, 5490-5499. from http://www.computer.org/plugins/d1/pdf/proceedings/hicss/2012/4525/00/4525f490.pdf.

[2] A Review of Trust Aspects in Cloud Computing Security International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.2, No.2, April 2013, pp. 116~122ISSN: 2089-

[3] Uma Somani, Kanika Lakhani and Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[4] Metri P. and Sarote G., "Privacy Issues and Challenges in cloud computing," International Journal of Advanced Engineering, Sciences and Technologies, vol. 5, no. 1, pp. 5-6, 2011.

[5] K. D. Bowers, A. Juels, and A. Oprea, "Proofs Of Retrievability: Theory and implementation," in Proc. Of ACM workshop on Cloud Computing security (CCSW"09), 2009; pp. 43-54.

[6] Kresimir Popovic and Zeljko Hocenski "Cloud computing security issues and challenges", MIPRO2010, May 24-28, 2010, Opatija, Croatia.

[7] Cong Wang, Qian Wang, and Kui Ren "Ensuring Data Sotrage Security in Cloud Computing" in IEEE 2009.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores" in CCS '007.

[9] Paul Zimski, "Cloud computing faces security strom" in 2009. Query Results by Exploring historical usage Data, ACM Trans. Inf. Syst., 24(1): 51-78, 2006.

[10] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/, D
December 2009.