ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 7, July 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Cloud Computing and Its Security Issues

Akanksha Dubey
B.E, Department of Information Technology,
MAEER's MIT College of Engineering, Kothrud,
Savitribai Phule Pune University, Pune, India

Abstract: ***Cloud computing, which is often referred to as "the cloud," is the delivery of everything from applications to information centers (on-demand computing resources) over the web on a pay-per-use basis. Cloud computing permits the consumers and businesses to make use of applications without actually installing and then access their personal files at any workstation having internet access. Much more efficient computing can be done using this technology of cloud computing by centralizing the data storage, its processing and the bandwidth. The various advantages of cloud includes the creation and storage of data at some remote servers, which in turn utilizes the client resource to the most minimum level. However, this advantage contains the drawback of privacy vulnerabilities and data security. This research paper discusses the challenges and security issues involved in cloud storage.***

Keywords: Cloud computing, data security, cloud data storage, cloud deployment models, cloud security challenges, cloud security issues.

I. INTRODUCTION

One of the important topics in the IT sector today is cloud computing. Its main model of computing as a resource has changed the scenario of computing as we are familiar with, and its promises have enthralled businesses and individuals alike which include, greater reliability, increased flexibility, decreased costs and massive scalability. Cloud computing, as described by NIST, is basically a model for enabling convenient, always-on, on-demand network access to a shared pool of computing resources, for example, applications, storage, services, etc., that can be released and provisioned rapidly with minimal effort in management or interaction with service provider[8]. It is one of the new models of providing the computing resources that utilizes the existing technologies. A datacenter is the core of cloud computing that makes use of virtualization to separate the instances of applications or the services that are being hosted on the "cloud". The cloud users are provided with the ability to rent a computing resource at a rate that is dependent on the datacenter services being requested. This data needs to be protected not only during its transmission but also when it is stored in storage at the service provider's end. In order to carry out this, various service providers provide different levels of privacy and security for the stored data based on the their available resources like data availability claims, business priorities, bandwidth, cost of operations and so on[6].

A very simple instance of cloud computing is, Gmail, Yahoo email, Hotmail etc. All that is needed is an internet connection and its ready to start sending the emails. The email management software and the server are all on the cloud and it is completely managed by the provider of the cloud service such as Yahoo, Google. The consumer can use the software and enjoy benefits from it. The analogy is, '***If you need eggs, would you buy a hen?'***

II. CLOUD SERVICE MODELS

A. ***Infrastructure as a service (IaaS):*** This service provides the companies with computing resources on a pay-per-use basis. These resources include networking, servers, data center space and storage. There are various issues in IaaS:

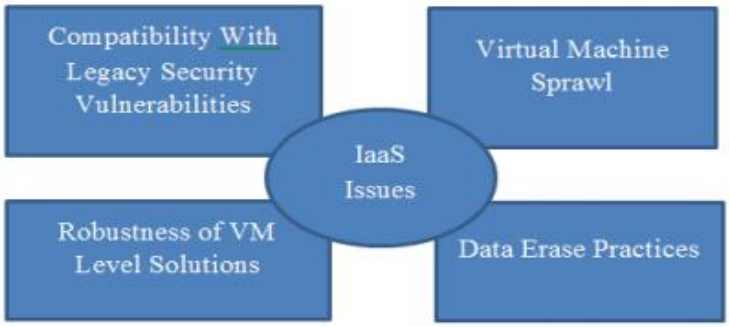

Fig1. IaaS Issues

B. ***Platform as a service (PaaS):*** This service provides an environment that is cloud-based having everything that is required to maintain the entire lifecycle of building and delivering cloud applications, without actually having to bear with the cost and the complexity of buying and managing the required hardwares and softwares. The different issues in PaaS are:

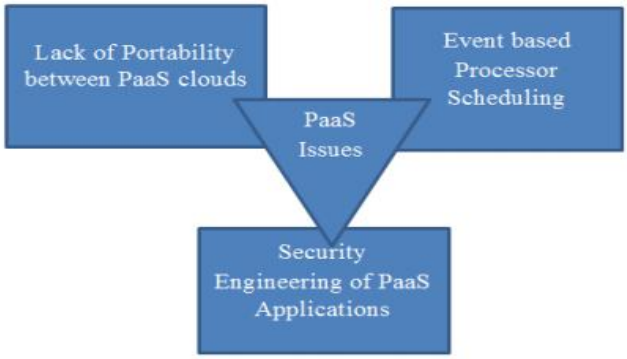

Fig2. PaaS Issues

C. ***Software as a service (SaaS):*** The cloud-based applications (SaaS) run on remote computers in the "cloud" which are owned and also operated by others who connect to users' workstation through the Internet and, mostly, a web browser.

III. Cloud Deployment Models

A. ***Public Cloud:*** A public cloud is set up where various organizations have same requirements and look forward to share infrastructure. This is the type of cloud computing model where the service providers make available online for public their computing resources. It permits the users to access several types of important resources on the cloud, such as: Software, Stored data or Applications. One of the major benefits of public cloud deployment is that the users are freed from performing some important jobs on their machines that they cannot escape otherwise, which include: the installation of resources, their configurations and their storage. Examples of public cloud are: Microsoft, Google, Amazon. There are various benefits of public cloud model as shown:

Fig3. Benefits of Public cloud

B. ***Private Cloud:*** This type of an infrastructure is operated solely for a single organization, which is either managed internally or by some third party, and hosted either internally or externally. These clouds can take the advantage of the cloud's efficiencies, at the same time providing more control of required resources and also steering clear of multi-tenancy. There are benefits of the internal cloud model. Diagram given below shows a few of these benefits:

Fig4. Benefits of Private cloud

C. ***Hybrid Cloud:*** A private cloud foundation when integrated with the strategic combination and use of the public cloud services is known as hybrid cloud. The reality is that a private cloud cannot survive in isolation from the rest of the company's resources and also the public cloud. Most of the companies having private clouds evolves to manage the workloads across various data centers, private and public clouds, thus creating the hybrid clouds. Some benefits of hybrid cloud are as shown in the diagram below:

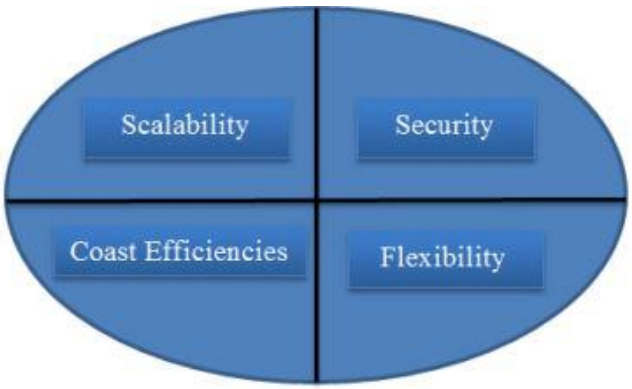

Fig5. Benefits of Hybrid cloud

IV. SECURITY ARCHITECTURE

The security in the cloud computing environment is a worrisome issue since the devices used by the customers to provide them services do not belong to these users. The customers have no control over, nor any kind of knowledge of, what could happen to their data when used over cloud services. This is a huge concern in situations when the users have personal and valuable data which is stored in a cloud computing service. These customers will not compromise their privacy and hence service providers must make sure that the customers' data is kept safe. However, this is becoming challenging since as the security developments are made, there is always someone to figure a way out to disable the security and then take advantage of the user data [2].

Service Provider Layer: Some of the important components of this layer are SLA Monitor, Resource Provisioning, Metering, Scheduler, Accounting, Load Balancer and Policy Management. The security issues related to this layer are Identity, Data transmission, Infrastructure, Privacy, Audit, People and Identity, and Compliance, Binding Issues and Cloud integrity.

Virtual Machine Layer: Some important components of this layer creates a number of virtual machines and the operating systems and their monitoring. The various security issues related to this layer are Access management, VM Sprawl, Infrastructure, VM Escape, Separation between Customers, Regularity issues, Cloud legal and Identity.

Data Center (Infrastructure)Layer: Some of the important components contains the CPU's, Servers, storage and memory and is denoted as Infrastructure-as-a-Service (IaaS). The security issues in this layer are: Physical Security: Network and Server, and secure data at rest.

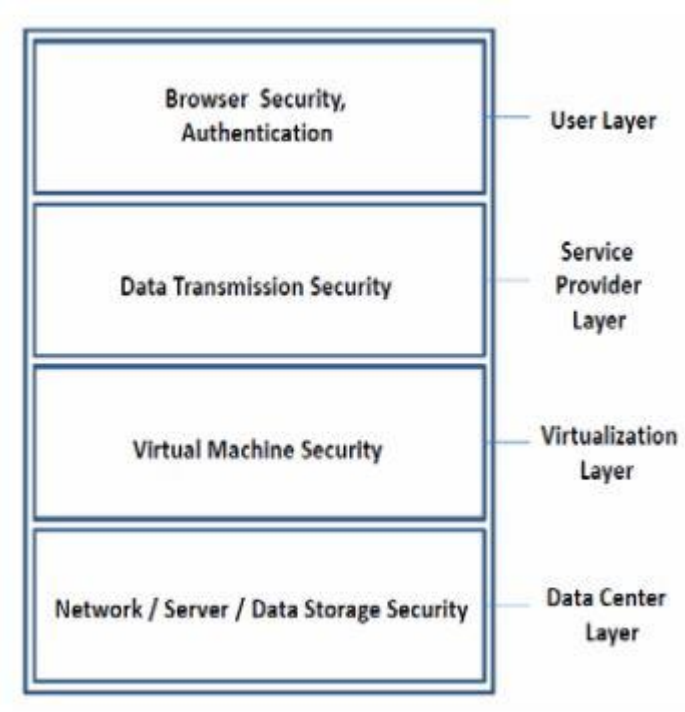

Fig6. Security Architecture of cloud computing

V. SECURITY CHALLENGES IN CLOUD

The key security challenges in cloud computing are explained as follows:

1) **Policy Integration:** Many cloud providers like Amazon, Google are accessed by the end users. There should be minimum amount of disagreements between their policies since they use their own approaches and policies.

2) **Authentication:** The data of the customers that is stored on the cloud is available throughout the internet to the unauthorized users. Therefore, the authenticated user and assistance on cloud must have interchangeable administration.

3) **Trust Management:** The trust management approaches must be developed and used in the cloud environment which should have trust negotiation factor among the users and the service providers.

4) **Access Control:** Cloud must have the right policies of access control so as to verify and promote only authenticated users. These services must be well planned, adjustable, and their allocation must be overseeing conveniently. Service Level Agreement (SLA) approach must be used between the parties involved in the cloud services.

5) **Service Management:** Different cloud providers such as Google, Amazon, comprise to build new services to meet the need of their customers.

VI. SECURITY ISSUES IN CLOUD

Data Locations: When the users use the cloud services, they probably will not know where their data will be hosted and in which geographical location their data will be stored in. Customers need to ask their service providers whether they will store

the complete data or alter the data for the storing purpose. Also on the basis of their customers will the service providers make fair accomplishments to follow the local privacy requirement [4].

Data Security: It is referred to as confidentiality, integrity and availability (CIA). These are the key issues for the cloud vendors. *Confidentiality* can be defined as the privacy of the data. Confidentiality is designed to avoid the sensitive information from getting accessed by unauthorized or wrong users. In this, it stores the encryption key data from an enterprise C, and stored in encrypted format at the enterprise D and this data must be kept secure from the enterprise D's employees. *Integrity* is described as the correctness of the data. *Availability* can be defined as data that is available on time or when required.

Trust Issue: Trust is also a chief issue in cloud computing environment. Trust can be between human to machine or machine to human or human to human. Trust revolves around confidence and assurance. In cloud computing, users store their data on cloud as there is trust between the parties involved in cloud. For example customers use Gmail server or Yahoo server as they trust on these providers.

Data Recovery: The process of restoring the data that has been lost or corrupted due to an accident is called is data recovery.

Network Security: Networks are of various types like public or private, shared and non-shared, small area or large area networks and each of these have a number of security problems to deal with [2]. The problems associated with network level security consists of the DNS attacks, issue of reused IP address, Sniffer attacks and so on.

VII. CONCLUSION

Cloud computing is the latest technology studied in recent years. There are various cloud platforms that are employed in many companies currently. There are numerous issues in cloud computing. Some examples of cloud computing issues are knowledge Confidentiality and measurability, ability, Service Level Agreement (SLA), knowledge Integrity, Performance. In this paper, we discussed the issues related to cloud computing which involves data location, security, storage, confidentiality, integrity and availability. Creating trust is one of the ways to overcome these security issues because it creates the relationship between entities quickly and safely. It is now known that cloud computing has bright future.

References

1. Sunita Sharma, Amit Chugh "SURVEY PAPER ON CLOUD STORAGE SECURITY", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 2, April 2013.
2. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy "Cloud Computing: Security Issues and Research Challenges", International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.
3. Palvinder Singh, Er. Anurag Jain "Survey Paper on Cloud Computing", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 3 Issue 4 April 2014.
4. Manpreet Kaur, Hardeep Singh "A REVIEW OF CLOUD COMPUTING SECURITY ISSUES", International Journal of Advances in Engineering & Technology, June, 2015.
5. Monjur Ahmed and Mohammad Ashraf Hossain "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.
6. Anup Mathew "Survey Paper on Security & Privacy Issues in Cloud Storage Systems", EECE 571B, TERM SURVEY PAPER, APRIL 2012.
7. Issa M. Khalil, Abdallah Khreishah and Muhammad Azeem "Cloud Computing Security: A Survey", www.mdpi.com/journal/computers 2014.
8. Uttam Thakore "Survey of Security Issues in Cloud Computing", University of Florida, Journal of Undergraduate Research.
9. Chandrahasan, R. Kalaichelvi, S. Shanmuga Priya, and L. Arockiam. "Research Challenges and Security Issues in Cloud Computing." International Journal of Computational Intelligence and Information Security 3.3 2012
10. Kant, Dr Chander, and Yogesh Sharma. "Enhanced Security Architecture for Cloud Data Security." International Journal of Advanced Research in Computer Science and Software Engineering 3.5 2013

