Security Challenges in Cloud

Sonal Shukla
Computer Science
Maharishi Arvind College of Engg. and Reaserch Center
Jaipur, India
Sona.shukla91@gmail.com

Surrendra Yadav
Computer Science
Maharishi Arvind College of Engg. and Reaserch Center
Jaipur, India
syadav66@yahoo.in

Bhramdutt Bohra
Computer Science
Maharishi Arvind College of Engg. and Reaserch Center
Jaipur, India
brahmdutt.bohra@gmail.com

***Abstract*— Cloud Computing is a term which allows user to access the set applications to perform a group of functions or tasks on the internet enabled devices. The cloud has been divided into three types: private, public and hybrid which are briefly described in this paper. SaaS, IaaS and PaaS are the services of the cloud. Cloud is generally provided by the third party, thus it faces few security challenges which are required to be resolved. In this paper we have discussed those issues and also the security architecture needed for the same.**

Keywords—Cloud Computing; Security; data privacy; SaaS ;PaaS ;IaaS; architecture .

I. INTRODUCTION

Cloud computing is a term used for providing the services hosted over the Internet. The term cloud computing simply referred to as "cloud" which provides resources on demand for data applications - everything starting from application to data stores over the Internet in a mode of pay for usage basis [1]. Cloud computing is simply accessing the services through Internet including storage, applications and servers making use of remote services of another company for a fee. The store and access data or programs virtually is also provided to a company by the use of cloud computing.

Cloud computing has influenced many aspects of computing which has emerged as a new technology in globalized era. Also users can move their data over the internet and are able to access them on the "on-demand" basis. Moving the data outside the organization and access them over the internet makes data vulnerable and owner's side losses of control of that data. Data on cloud servers can be easily accessed instead of the data stored on your local disk to both computing providers and law enforcement agencies. The "Cloud Computing" term is used for accessing the data over the net by using the on demand model.

Cloud computing is also related technologies like grid computing, virtualization, autonomic computing and utility computing. Cloud computing is a general computational resources which are coordinated to achieve the objective that is similar to grid computing in one aspect, but it is a step forward to better resource utilization and dynamic resource provisioning to leverage virtualization technology. Cloud computing uses on-demand resource provisioning and utility-based pricing, for being a realization of utility computing. Cloud computing shares the characteristics of other computing technologies to other technologies, but new safety issues arise at the same time [2].

II. WHAT IS CLOUD COMPUTING

Cloud computing, a driving force of demand from its audiences operating system, client-server architecture, and browser to rethink their understanding that whether there be any future of computing as a information system which can be easy as well as innovative. while reducing overall client-side needs and complexity, cloud computing have leveraged user with hardware requirements. Cloud computing is often represented by flow charts and diagrams used was inspired by the cloud symbol used on internet. A separate migration clouds on the remote server accessible via a network, bookmarks, photos, music files and personal data, including, maintaining a growing number of 'bit by bit' with end users in recent years is taking place. Cloud computing virtualization technology is strong; In fact, the technology dates back to the 1967, but for decades the only mainframe systems [3] but was available.

A. Types of Clouds:

There are basically three types of clouds: Public, private and hybrid. Through a public cloud, a provider through the

978-1-4673-7910-6/15/$31.00 ©2015 IEEE

Internet can offer services to anyone, including storage and application. They may be provided either freely or charged on the basis of pay-per-usage method.

1) Public Cloud:

The costs of applications provided, hardware used and bandwith are borne by providers in public cloud services, thus, it is easy to install and are less expensive. They are scalable and users can only take advantage of those services. Public clouds ownership and operation is done by the companies to provide fast access to resources for computing to an individuals or companies, which are easily affordable. By using public cloud services, users don't have to buy supporting infrastructure, software or hardware which is mainly owned and managed by the providers.

2) Private Cloud:

A private cloud or corporate cloud also known as the internal cloud, offers IT services which is provided for a limited number of end users protected via a firewall. Private cloud is generally used in businesses that want to have more control over their corresponding data. As far as the community is concerned, the requirements are similar to the one or more than one organization sharing same resources. A single company own and operate the private cloud who wants to controls the customization process of the automated services and virtualized resources. These are then further used by the various constituent groups and business lines. Private clouds takes advantage of many of cloud's efficiencies by providing more control over resources and over steering clear of multi-tenancy [1].

3) Hybrid Cloud:

A hybrid cloud is the combination of the two or more than two clouds. A hybrid cloud makes the use of public cloud services along with the private cloud foundation. A private cloud can't exist in isolation from public cloud and the company's IT resources. Many of the companies will be able to manage workloads in between data centers with private clouds; this generated the need of hybrid clouds- combination of public and private clouds [1].

B. Different Cloud Services

The three prominent types of cloud computing services are Infrastructure-as-a-Service (IaaS) is a area where companies having large cloud computing services provides virtual infrastructure; Platform-as-a-Service (PaaS) offers the company, freedom to built their own custom applications which can be used by all of its entire workforce and Software-as-a-Service (SaaS) is a area which requires a company to subscribe to its services and access services using the Internet.

1) Software-as-a-Service (SaaS):

SaaS Application Service Provider (SP) on the Internet offer various software applications which can be described as a process. Installation and operation of the application on the client computer to get rid of and also to eliminate the heavy burden of software maintenance causes; Continuous operation, security and support. SaaS provider inadvertently IT infrastructure (servers, software, operating systems, databases, data center space, network access, power and cooling, etc.) and implementing procedures and takes responsibility for managing the entire solution to run and manage necessary (infrastructure etc. patches / updates, application patches / updates, backups,). SaaS on demand as a service offering provides a complete application. Examples of SaaS are: LinkedIn, Salesforce and Workday etc.

2) Platform as a Service (PaaS):

"Any software download or installation, end users or administrators as a service without. It provides the computing platform and solution stack. In order to implement an infrastructure with a high level of integration provides test and cloud applications. Users (networks, servers, operating systems and storage), including infrastructure management, but he probably controls deployed applications and their settings. Examples of PaaS includes: Google Apps (mostly known), Appscale, FlexiScale and Windows Azure etc.

3) Infrastructure as a Service (IaaS):

IaaS uses virtualization technology through which the implementation of services reflects the sharing of hardware resources. The main objective of such applications and the operating system more accessible server, network and storage resources is to make it as. Therefore, infrastructure and hosts, switches and routers to communicate with the application programming interface (API) using the on-demand services, and a simple and transparent manner that provides the ability to add new equipment. The customer usually pays per use. Examples of IaaS includes: Amazon Web Service, Bluelock, and At&t etc[4].

III. CLOUD ARCHITECTURE

Front-end and Back-end: are the sections divided into two in the cloud computing architecture. They have a network, usually connected to each other via the Internet. Front end in this architecture refers to client side i.e. is the computer user or end user. Back-end system refers to the "cloud" section. A central server is used to ensure that everything runs smoothly, it monitors traffic and customer demand. It has a set of rules called protocols and middleware software (a special software) [5]. Infrastructure, platform, and application are the 3 layers of Cloud architecture.

These three development provision in the cloud layers of hardware and software resources with virtualization and standardization are implemented [6]. The infrastructure layer is develop with virtualized calculations, storage and network support. The outline of these hardware needs is meant to offer the facilities demanded by users. Internal, automated provisioning of resources is realized by virtualization and then infrastructure management process is optimized. The platform layer provides general-purpose and is for the iterative use of the set of software resources. At this layer, user gets the environment to develop their applications, to monitor the execution results and performance and also to text the

operation flows. The users are assured with scalability, dependability, and security protection at this platform.

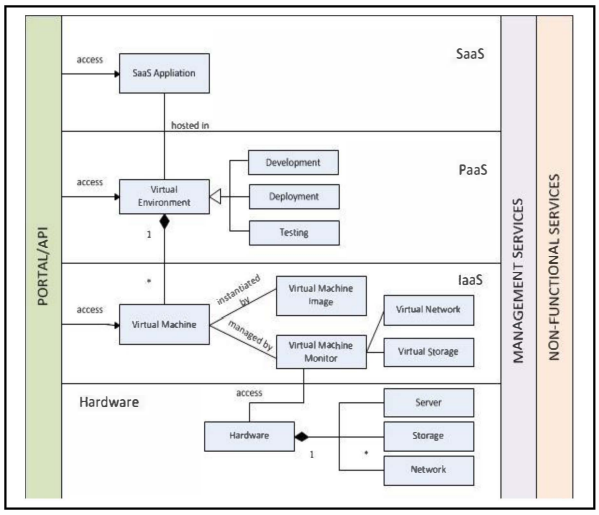

Fig.1. Cloud Architecture

Usually, the virtualized cloud acts as a "system middleware" between the infrastructure and application layers in the cloud architecture. The combination of all needed software modules application layer is formed for SaaS applications. Daily management work in offices, such as information retrieval, document, processing, and calendar and authentication services, etc is included in this layer. Most important concerns with cloud storage of data are that of data integrity verification at the servers which cannot be believed. For example, sometimes service provider, may experiences Byzantine failures [7].

IV. Cloud Specific Security Challenges

In conventional communication systems is applied to cloud security concerns, the use of cloud computing is possible or easier to carry out attacks that introduces new attack vectors [8]. In a traditional deployment model (on-premise application), the delicate data of companies or organization continues to reside within the boundaries of institute and is subject to its logical, physical and access control policies and personnel security. Unlike in SaaS model, the organizations vulnerable data is resided away from the boundaries of organization or we can say that it is stored at the end of the SaaS vendor side. Therefore, the providers of SaaS must involve extra security measures to their system to ensure data security in the storage area and prevent an act of breaking due to security issues. In order to secure the IaaS layer, two fields are introduced, namely the virtual and physical environment. There are several security requirements which are required to be included in the previous virtual level, which involves holding back the secure communication medium, access of data, virtual protection of data and data encryption techniques [9].

In Cloud Computing, existing vulnerabilities, associated attacks, and threats arises numerous security issues. The weak points in the Cloud's security architecture used by an adversary via important techniques to access to the internet and other resources can be defined as vulnerabilities [10]. Making cloud computing secure has been the main aspect of emphasis of cloud computing security. Most of these factors are not distinctive to the cloud rather it is stored, regardless of where the data is vulnerable to attack. Hence it can be said that all the topics of computing security including design of security architectures, the minimizing of attack surfaces, enforcement of access control, and protection from malware come under this broad category of cloud computing security. Still, some of the aspects in the cloud computing security are as follows:

1. Since cloud is a shared resource, the ones sharing it may be the attackers and hence known as tenants.

2. Cloud-based data is widely accessible over internet by protocols and APIs which are not secure in the public networks.

3. Due to incorrect modification by cloud providers or accidental omission, sometimes there could be a loss in cloud data.

4. Cloud data can be accessed quite easily by the provider of the cloud [10].

In this epoch of cloud, the cloud provider mostly will be processing the data as the data processor, say, by stockpiling on the platform. The responsibilities of cloud provider include providing operating system, premises security and infrastructure and network security which depend on the kind of cloud taken into account. On the other hand, the cloud customer will be the one processing the cloud data for its own intentions thusly the data controller has a certain set of responsibilities including controlling the infrastructure virtually and security of application. The service model utilized also becomes a criterion. Before the data is transmitted or stored, it must necessarily be encrypted to secure it from various attacks thus maintaining its integrity which can be done by using algorithms such as DES, 3DES, blowfish, AES, etc in cloud computing [11].

V. Secured Architecture for Cloud

The information security and protection on cloud is an essential issue, turning into the greatest boundary of distributed computing improvement. Business continuity and privacy of data are both huge items for acquiescence; what implementations are put forward by provider of mechanisms is also a matter to ponder upon [12].

Cloud service provider should provide the details of the security architecture that might either help or obstruct security management according to the standard of organizations, say, the isolation between tenants should be disclosed which is generally guaranteed by the architecture of virtualization. The

capability and the level of security vary from provider to provider. This often results in the unavailability of the security mechanism such as key management and data encryption.

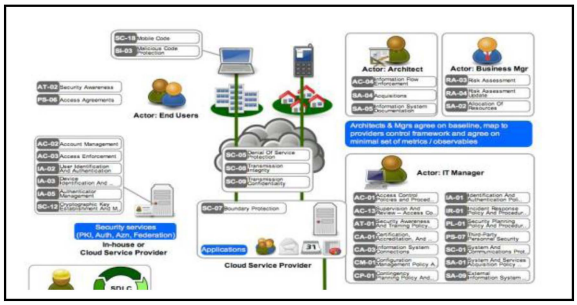

Fig.2. Secure Cloud Architecture

For example: for encrypting security artifacts and keys, AES 128 bit encryption services are included to key management services. For such kind of critical services, one should have full faith on the internal security services. For these applications which depend on the internal services, "hybrid cloud" architecture is the best solution one could suggest. Another solution is Single Sign-On (SSO) [13]. Nowadays enterprises are taking the option of Single Sign-On (SSO) technology into consideration to inscribe the password explosion as they assist in cutting down the application passwords and diverse networks to one. The remedy of utilization of SSO by organizations was suggested for implementing strong authentication and security management. A single login can enable a wholesome environment of cloud computing to cloud users in order to access diverse applications under a strict authentication [14]. A part of security architecture published by open security group of architecture is as follows.

The pattern above in the figure depicts the actors i.e. architects, business manager, end user etc. that are in continuous interaction with the systems i.e. applications organized on the cloud, end point, data security services and protecting the actors and systems controls [15].

VI. Conclusion

Could computing is no doubt today's need. It allows user to store their data on the more protected and managed way, even the globalization of many organization is dependent on the cloud computing. But instead of all its positive points, it also has some flaws in the security department which needs to be managed. The challenges faced by the cloud in the area of security are discussed in the paper. It also described the small part of the secure architecture of cloud and basic idea of single sign-on technology.

REFERENCES

[1] http://www.ibm.com/cloud-computing/in/en/what-is-cloud-computing.html

[2] Navdeep Aggarwal, Parshant Tyagi, Bhanu P. Dubey and Emmanuel S. Pilli, "Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review", International Journal of Computer Applications (0975 – 8887), 5/1/2013

[3] Dimitrios Zissis, Dimitrios Lekkas, "Addressing cloud computing security issues", www.elsevier.com/locate/fgcs, 2012.

[4] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges", (IJCSITS), Dec, 2011

[1] Pankaj Sareen, "Cloud Computing: Types, Architecture, Applications, Concerns, Virtualization and Role of IT Governance in Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, March, 2013

[2] Kai Hwang, Geoffrey Fox and Jack Dongarra, " Book: Distributed Computing: Clusters, Grids and Clouds", Chapter 7, Cloud Architecture and Datacenter Design pp. 57

[3] Qian Wang, Cong Wang, Jin Li, Kui Ren, and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing".

[4] Rashmi, Dr.G.Sahoo, Dr.S.Mehfuz, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions", International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.4, Aug-13.

[5] Osama Harfoushi, Bader Alfawwaz, Nazeeh A. Ghatasheh, Ruba Obiedat, Mua'ad M. Abu-Faraj and Hossam Faris,"Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review",(http://www.scirp.org/journal/cn) http://dx.doi.org/10.4236/cn.2014.61003, Feb-14.

[6] Mark D. Ryan, "Cloud computing security: the scientifc challenge, and a survey of solutions", Jan-13.

[7] Leena Khanna and Prof. Anant Jaiswal, "Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them", Volume 3, Issue 3, IJARCSSE, Mar-13.

[8] Huaglory Tianfield, "Security Issues In Cloud Computing", 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC'12), Seoul, Korea, Oct-12.

[9] Subra Kumaraswamy, "Introduction to Cloud Security Architecture from a Cloud Consumer's Perspective", http://www.infoq.com/articles/cloud-security-architecture-intro.

[10] Kashif Munir and Prof Dr. Sellapan Palaniappan, "SECURE CLOUD ARCHITECTURE", Advanced Computing: An International Journal (ACIJ), Vol.4, No.1, Jan-12.

[11] opensecurityarchitecturegroup.org.