iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 Issue: I Month of publication: January 2014

DOI:

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

A Survey on Current Cloud Computing Trends and Related Security Issues

Rachna Jain[1], Reena Singh[2]

Assistant Professor[12]

Dept. of Computer Science

Bharati Vidyapeeth College of engineering

Delhi, India

ABSTRACT
Cloud Computing is an emerging technology which provides services on the basis of as you pay as you go. It provides resources (e.g. CPU and storage) as general utilities that can be leased and released by users through the internet in an on-demand fashion. But deploying cloud computing in an enterprise infrastructure brings significant security concerns. Though cloud computing have an economical computation over the current infrastructure, but implementation of cloud computing in an enterprise requires proper planning and understanding of emerging risks, threats, vulnerabilities, and possible countermeasures. In this paper, we have discussed the architecture and business model of cloud computing along with the security issues related to its implementation. We presented the security issues by considering both's (User & Providers) point of view. We also focused lights on the techniques presented by the researcher to provide security in cloud computing environment.

Keywords: Cloud Computing, Security Threat, Services

I. INTRODUCTION

With the rapid development of processing and storage technologiesand the success of the Internet, computing resources have become cheaper, more powerful and moreubiquitously available than ever before. This technological trend has enabled the realization of a new computing model called cloud computing, in which resources (e.g., CPU and storage) are provided as general utilities that can be leased and released by users through the Internet in an on-demand fashion.

With the help of the right tools and technologies, any business can address the risk and budgeting complexity often associated with cloud computing.

Businesses are unquestionably excited about cloud computing, they're also more than a little concerned about security. Companies love the cloud's efficiency and flexibility , but worry about confidential information falling into the wrong hands. "That's their biggest fear,You don't hear about an outage at a company on the evening news, but you hear about security breaches." Some 66 percent of

IT decision makers cite security concerns as a barrier to implementing a cloud computing strategy, and 56 percent say they won't fully embrace the cloud until they're more confident in cloud service providers' ability to meet their compliance requirements, according to a 2013 IDG Enterprise cloud computing research study.

II. ARCHITECTURE

When talking about a cloud computing system, it's helpful to divide it into two sections: the front end and the back end. They connect to each other through a network, usually the Internet. The front end is the side the computer user, or client, sees. The back end is the "cloud" section of the system.

The front end includes the client's computer (or computer network) and the application required to access the cloud computing system. Not all cloud computing systems have the same user interface. Services like Web-based e-mail programs leverage existing Web browsers like Internet Explorer or Firefox. Other systems have unique applications that provide network access to clients.

On the back end of the system are the various computers, servers and data storage systems that create the "cloud" of computing services. In theory, a cloud computing system could include practically any computer program you can imagine, from data processing to video games. Usually, each application will have its own dedicated server.

A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware. Middleware allows networked computers to communicate with each other. Most of the time, servers don't run at full capacity. That means there's unused processing power going to waste. It's possible to fool a physical server into thinking it's actually multiple servers, each running with its own independent operating system. The technique is called server virtualization. By maximizing the output of individual servers, server virtualization reduces the need for more physical machines.

This section describes the architectural, business and various operation models of cloud computing.

A layered model of cloud computing:

Generally speaking, the architecture of a cloud computing environment can be divided into 4 layers: the hardware/datacenter layer, the infrastructure layer, the platform layer and the application layer, as shown in Fig.. We describe each of them in detail:
The hardware layer: This layer is responsible for managing the physical resources of the cloud, including physical servers, routers, switches, power and cooling systems.In practice, the hardware layer is typically implemented in data centers. A data center usually contains thousands of servers that are organized in racks and interconnected through switches, routers or other fabrics. Typical issues at hardware layer include hardware configuration, faulttolerance,traffic management, power and cooling resource management.

The infrastructure layer:

Also known as the virtualizationlayer, the infrastructure layer creates a pool of storage and computing resources by partitioning the physical resources using virtualization technologies such as Xen , KVM and VMware . The infrastructure layer is an essential component of cloud computing, since many key features, such as dynamic resource assignment, are only made available through virtualization technologies.

The platform layer:

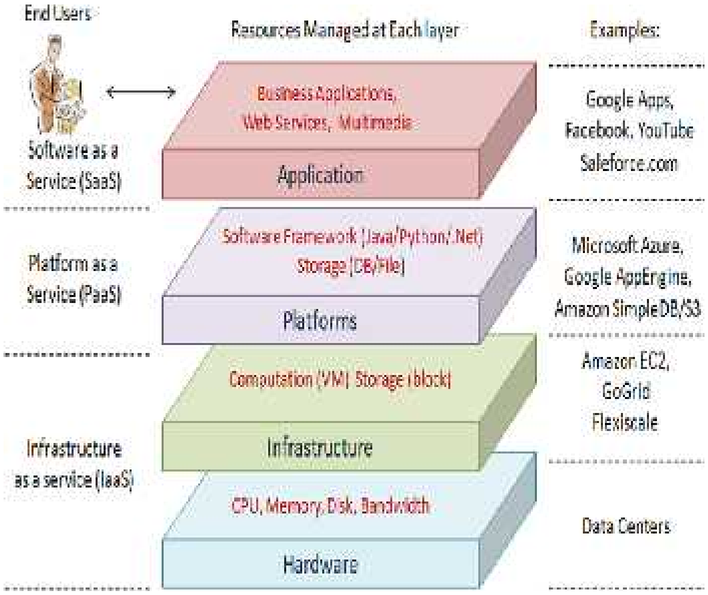
Built on top of the infrastructure layer, the platform layer consists of operating systems and application frameworks. The purpose of the platform layer is to minimize the burden of deploying applications directly into VM containers. For example, Google

App Engine operates at the platform layer to provide API support for implementing storage, database and business logic of typical web applications.

The application layer:

At the highest level of the hierarchy,the application layer consists of the actual cloud applications.Different from traditional applications, cloud applications can leverage the automatic-scaling feature to achieve better performance, availability and lower operating cost.Compared to traditional service hosting environments such as dedicated server farms, the architecture of cloud computing is more modular.

Each layer is loosely coupled with the layers above and below, allowing each layer to evolve separately. This is similar to the design of the OSI model for network protocols. The architectural modularity allows cloud computing to support a wide range of application requirements while reducing management and maintenance overhead.


End Users
Resources Managed at Each layer
Examples:
Business Applications, Web Services, Multimedia
Application
Google Apps, Facebook, YouTube Saleforce.com
Software as a Service (SaaS)
Software Framework (Java/Python/.Net) Storage (DB/File)
Platforms
Microsoft Azure, Google AppEngine, Amazon SimpleDB/S3
Platform as a Service (PaaS)
Computation (VM) Storage (block)
Infrastructure
Amazon EC2, GoGrid Flexiscale
Infrastructure as a service (IaaS)
CPU, Memory, Disk, Bandwidth
Hardware
Data Centers

III. BUSINESS MODEL

Cloud computing employs a service-driven business model.In other words, hardware and platform-level resources are provided as services on an on-demand basis. Conceptually, every layer of the architecture described in the previous section can be implemented as a service to the layer above.
Conversely, every layer can be perceived as a customer of the layer below. However, in practice, clouds offer services that can be grouped into three categories: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

Infrastructure as a Service:

IaaS refers to on-demand provisioning of infrastructural resources, usually in terms of VMs. The cloud owner who offers IaaS is called an IaaS provider. Examples of IaaS providers include Amazon EC2 , GoGrid and Flexiscale .

Platform as a Service:

PaaS refers to providing platformlayer resources, including operating system support and software development frameworks. Examples of PaaS providers include Google App Engine , Microsoft Windows Azure and Force.com .

Software as a Service:

SaaS refers to providing on-demand applications over the Internet. Examples of SaaS providers include Salesforce.com , Rackspace and SAP Business by Design .

The business model of cloud computing is depicted by Fig. . According to the layered architecture of cloud computing, it is entirely possible that a PaaS provider runs its cloud on top of an IaaS provider's cloud. However, in the current practice, IaaS and PaaS providers are often parts of the same organization (e.g., Google and Salesforce). This is why PaaS and IaaS providers are often called the *infrastructure provider.*.

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

IV. TYPES OF CLOUD

There are many issues to consider when moving an enterprise application to the cloud environment. For example,some service providers are mostly interested in lowering operation cost, while others may prefer high reliability and security.Accordingly, there are different types of clouds, each with its own benefits and drawbacks:

Public Cloud

Public cloud (also referred to as 'external' cloud) describes the conventional meaning of cloud computing: scalable, dynamically provisioned, often virtualised resources available over the Internet from an off-site third-party provider, which divides up resources and bills its customers on a 'utility' basis.
An example is ThinkGrid, a company that provides a multi-tenant architecture for supplying services such as Hosted Desktops, Software as a Service and Platform as a Service. Other popular cloud vendors include Salesforce.com, Amazon EC2 and Flexiscale.

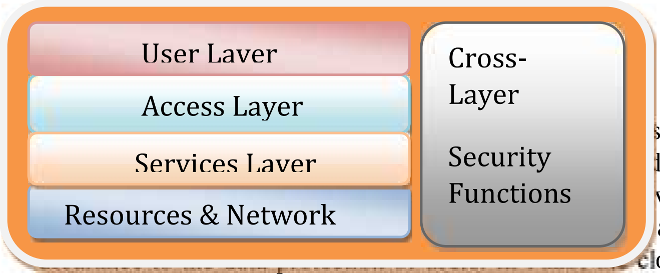
Private Cloud

Private cloud (also referred to as 'corporate' or 'internal' cloud) is a term used to denote a proprietary computing architecture providing hosted services on private networks. This type of cloud computing is generally used by large companies and allows their corporate network and data centre administrators to effectively become in-house 'service providers' catering to 'customers' within the corporation. However, it negates many of the benefits of cloud computing, as organisations still need to purchase, set up and manage their own clouds.

Hybrid Cloud

It has been suggested that a hybrid cloud environment combining resources from both internal and external providers will become the most popular choice for enterprises. For example, a company could choose to use a public cloud service for general computing, but store its business-critical data within its own data centre. This may be because larger organisations are likely to have already invested heavily in the infrastructure required to provide resources in-house or they may be concerned about the security of public clouds .

V. SECURITY CHALLENGES IN CLOUD COMPUTING ENVIRONMENT



s in
ding
vily
any
cloud providers offer some controls to the users building applications on their platform, without ensuring them the threats with network or intrusion prevention. While with IaaS, the developers have a better control over the application. This addresses proper security and compliance. Hence in cloud computing, security threats can occur at both the ends, for Cloud Service Users as well as for Cloud Service providers[1]:

VI. THREATS FOR CLOUD SERVICE USERS

Responsibility Ambiguity:

The lack of a clear definition of responsibility among cloud service users and Providers may evoke conceptual conflicts. Moreover, any contractual inconsistency of provided services could induce anomaly, or incidents.

Loss of Governance & Trust:

For an enterprise, migrating a part of its own IT system to a cloud infrastructure implies to partially give control to the cloud service providers. The cloud service users have no abilities to evaluate security implementation level achieved by the provider. Such a lack of sharing security level in view of cloud service provider will become a serious security threat in use of cloud services for cloud service users.

Service Provider Lock-in:

A consequence of the loss of governance could be a lack of freedom regarding how to replace a cloud provider by another.

Unsecure Cloud Service User access:

As most of the resource deliveries are through remote connection, non-protected APIs attack methods such as phishing, fraud, and exploitation of software vulnerabilities could take place. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.

Lack of Information/Asset Management:

When applying to use Cloud Computing Services, the cloud service user will have serious concerns on lack of information/asset management by cloud service providers such as location of sensitive asset/information, lack of physical control for data storage, reliability of data backup (data retention issues), countermeasures for BCP and Disaster Recovery and so on. Furthermore, the cloud service users also have important concerns on exposure of data to foreign government and on compliance with privacy law such as EU data protection directive.

Data loss and leakage:

The loss of encryption key or privileged access code will bring serious problems to the cloud service users. Accordingly, lack of cryptographic management information such as encryption keys, authentication codes and access privilege will heavily lead sensitive damages on data loss and unexpected leakage to outside.

VII. THREATS FOR CLOUD SERVICE PROVIDERS

Responsibility Ambiguity: When dealing with third parties. The cloud service provider is somehow a cloud service user. Ambiguity of such user roles and responsibilities definition related to data ownership, access control, infrastructure maintenance, etc, may induce business or legal dissention.

Protection Inconsistency: Due to the decentralized architecture of a cloud infrastructure, its protection mechanisms are likely to be inconsistent among distributed security modules. Hence, there may be a case that, an access denied by one module may be granted by another. A threat of such type may be profited by a potential attacker which compromises both the confidentiality and integrity.

Evolutional Risks: One conceptual improvement of cloud computing is to postpone some choices from the design phase to the execution phase. This means, some dependent software components of a system may be selected and implemented at the time of system execution. But, conventional risk assessment methodology can no longer match such an evolution. Hence, a system which is assessed as secure during the design phase may exploit vulnerabilities during its execution due to the newly implemented software components.

Business Discontinuity: The whole cloud infrastructure together with its business workflows thus relies on a large set of services, ranging from hardware to application. Hence, the discontinuity of service delivery, such as black out or delay, may bring out a severe impact related to the availability.

Supplier Lock-in: The platform of a service provider is built by some hardware and software components by suppliers. Some supplier-dependent modules or workflows are implemented for integration or functionality extension. However, due to the lack of standard APIs, the portability to migrate to another supplier is not obvious.

License Risks: Software licenses are usually based on the number of installations, or the numbers of users. Although, created virtual machines will be used only a few times, the provider may have to acquire from more licenses than really needed at a given time. The lack of a “clouded” license management scheme which allows to pay only for used licenses may cause software use conflicts.

Bylaw Conflict: Depending on the bylaw of hosting country, data may be protected by different applicable jurisdiction. An international cloud service provider may commit bylaws of its local data centers which is a legal threat to be taken into account.

Bad Integration: Migration of a part of an IT infrastructure to an external cloud service provider requires deep changes in the infrastructure design. A bad integration caused by incompatible interfaces or inconsistent policy enforcement may evoke both functional and non-functional impacts.

Unsecure Administration API: Non-protected APIs, mostly administration APIs becomes a target of choice for attackers. This is not specific to cloud environment. However, the service-oriented approach makes APIs a basic building block for a cloud infrastructure. Their protection becomes a main concern of the cloud security.

Shared Environment & Data Unreliability: Cloud resources are virtualized, different cloud service users share the same infrastructure. Any unauthorized and violent access to cloud service user's sensitive data may compromise both the integrity and confidentiality.

Service Unavailability: Due to the service-oriented design principle, service delivery may be impacted while the cloud infrastructure in not available. A typical Denial of Service attack on one service may clog the whole cloud system.

VIII. TECHNIQUES FOR PROVIDING CLOUD COMPUTING SECURITY

Apart from various ups and downs in cloud security environment, there is a continuous growth in security management and in security mechanisms This section provides a review of techniques which can be used to provide security in Cloud computing environment

Techniques used for Data Leakage Protection: Rafael Moreno et al. [2] suggested that cloud platforms should provide new services for collecting context information and to perform analysis and manage data privacy in order to support applications requesting the information. On the other hand, Danny Harnik et al. [3] said that deduplication. (the term de-duplication means storing only a single copy of redundant data and providing just a link to this copy rather than storing actual copies of this data) with allowing a limitation on number of user uploads per time window can help in protecting data. Ji Hu Klein [14] gave a benchmark to secure data-in-transit in the cloud.

Technique for Preventing Malicious Attacks: Farzad Sabahi [4] with the help of an access control mechanism tool has shown how to control unauthorized user in accessing secured data. He showed malicious attacks by the unauthorized users on the victim’s IP address and physical server. Peter Mell [5], explained that to defend against malicious cloud users IAAS can be used as one of the models that exposes challenges with using virtualization as a frontier security protection.

Technique for handling Backup and Storage: Acc. To the studies of Intel IT center[6], problem with backup and storage increases with increase in server virtualization. So, data De-duplication can be one of the alternatives for this problem. On contrast, Danny hamrik et al.[3], have shown the de-duplication in cloud storage is carried with the misuse of data backup , as backup data is generally in unencrypted form.

Technique for Managing Shared Technological issues: Perez R et al. [8] discussed that in spite of several advantages, hypervisors have exhibited flaws that have permitted guest operating systems to expand inapt levels of control or authority on the original platform. Hence it can certainly lead to security issues on the cloud. Lori M. Kaufman [11] has shown the implementation of Infrastructure as a Service by the customer in order to facilitate the infrastructure or hardware usage.

Technique for preventing Service Hijacking: As discussed by Rajnish Choubey et al.[7], account hijacking is one of the severe threats. As no native API’s are used for registering various cloud services the chances of hijacking ones account increases considerably.

Technique for handling VM Hopping: In the conclusion K. Owens [9] and A. Jasti et al. [10] mentioned that with VM hopping, an attacker on one VM gains rights to use another victim VM. After gaining rights attacker can check the victim VM's resource procedure, can alter its configurations and can even delete stored data, thus, putting it in danger the VM's confidentiality, integrity, and availability. This attack can only take place if two VMs are operating on the same host, and the attacker recognizes the victim's VM's IP address. Although IaaS and PaaS users have partial authority, Thomas Ristenpart et al. [12] have shown that on the basis of various tricks and combinational inputs, an attacker can get hold of or decide the IP address using benchmark customer capabilities.

Technique for handling VM Dos: As discussed by Jianyong Chen [13], even Cloud computing environment is in the clutches of DoS attack, but having service providers place sufficient configurations to put an upper limit on the resources owed to the VMs decreases their probability. Moreover, it is wise to have the Service Level Agreement (SLA). As it legally identifies responsibilities of the service provider and the user.

IX CONCLUSION

Cloud Computing is a combination of several key technologies that have evolved and matured over the years. Though cloud computing has a perspective for cost saving to an enterprise but the security risks are also colossal. Hence, enterprise looking into cloud computing technology should religiously analyze the security risks prior to its implementation.

REFERENCES

[1] Kangchan Lee, " Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012.

[2] Rafael Moreno-Vozmediano, Rubén S. Montero, and Ignacio M. Llorente, "Key Challenges in Cloud Computing to Enable the Future Internet of Services", IEEE, Digital Object Indentifier 10.1109/MIC.2012.69.

[3] Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg, "Side Channels in Cloud Services: Deduplication in Cloud Storage", 540-7993/10, IEEE, 2010, pp: 40 – 47.

[4] Farzad Sabahi, "Cloud Computing Security Threats and Responses", 978-1-61284-486-2, IEEE, 2011, pp: 245 – 249.

[5] Peter Mell, "What's Special about Cloud Security?" , IEEE, IT Pro July/August 2012, pp: 6 – 8.

[6] Intel IT Center, "Preparing your Virtualized Data Center for the Cloud", pp: 1 – 20.

[7] Rajnish Choubey, Rajshree Dubey, Joy Bhattacharjee, "A Survey on Cloud Computing Security, Challenges and Threats", International Journal on Computer Science and Engineering, ISSN: 0975-3397, Vol. 3 No. 3 March 2011, pp: 1227 – 1231.

[8] Perez R, van Doorn L, Sailer R. "Virtualization and hardware-based security". IEEE Security and Privacy 2008;6(5):24–31.

[9] K. Owens, "Securing Virtual Computer Infrastructure in the Cloud," white paper, Savvis Communications Corp., 2009.

[10] A. Jasti et al., "Security in Multi-Tenancy Cloud," Proc. IEEE Int'l Carnahan Conf. Security Technology (ICCST 10), IEEE Press, 2010, pp. 35–41.

[11] Lori M. Kaufman, Bruce Potter, "Monitoring Cloud Computing by Layer, Part 1", 1540-7993/11, IEEE, pp: 66 – 68.

[12 Thomas Ristenpart et al., "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. 16th ACM Conf. Computer and Communications Security (CCS09), ACM Press, 2009, pp. 199–212.

[13] Jianyong Chen, Yang Wang, Xiaomin Wang, "On demand security architecture for Cloud Computing, IEEE 2011, pp: 1 – 12.

[14] Ji Hu Klein, "A Benchmark of transparent data encryption for migration of web application in cloud", Eighth IEEEInternational Conference on Dependable, Autonomic and Secure Computing, 2009, pages 735 – 740, Chengdu.

[15] John Viega, "Cloud Computing and the Common Man", IEEE, 0018-9162/09, pp: 106 – 108.