CLOUD COMPUTING: STUDY OF SECURITY ISSUES AND RESEARCH CHALLENGES

Adnaan Arbaaz Ahmed, Dr.M.I.Thariq Hussan

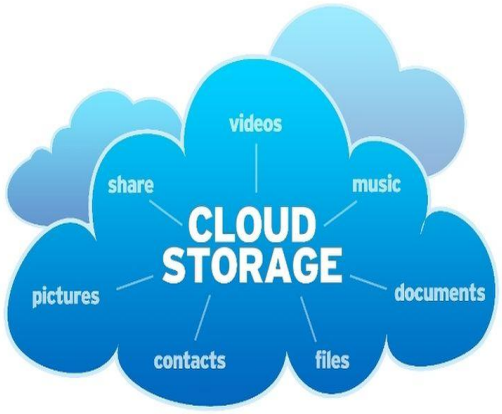
Abstract - Cloud computing is the practice of using a network of remote servers hosted on internet to store, manage and process data on demand and pay as per use. It provides access to a pool of shared resources instead of local servers or personal computers. As it do not acquire the things physically, it saves managing cost and time for organizations. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Microsoft etc. Cloud computing is an emerging domain and is acclaimed throughout the world. There are some security issues creeping in while using services over the cloud. This research paper presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure. This paper also analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate and boost up its usage. The main emphasis of our study based on existing literature and to understand the concept of multi-tenancy security issue.

Index Terms – Cloud, Multitenancy

Manuscript Received March, 2018.
Adnaan Arbaaz Ahmed, *B.Tech Scholar, Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad.*
Dr.M.I.Thariq Hussan, *Professor and Head, Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad.*

1. INTRODUCTION

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud Service Providers (CSP's) offer cloud platforms for their



customers to use and create their web services, much like Internet Service Providers (ISP's) offer costumers high speed broadband to access the internet. CSPs and ISPs both offer services. Cloud computing is a model that enables convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications that can be rapidly provisioned and released with minimal management effort or service provider's interaction.

Clouds are the new trend in the evolution of the distributed systems. Earlier to Cloud we used Grid. In Cloud Computing, the user does not require knowledge or expertise to control the infrastructure of clouds; it provides only abstraction. It can be utilized as a service of the Internet with high scalability, higher throughput,

quality of service and high computing power. Cloud computing providers deliver common online business applications which are accessed from servers through web browser.

Recent developments in the field of Cloud computing have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

- The transmission of personal sensitive data to the cloud server.
- The transmission of data from the cloud server to clients' computers.
- The storage of clients' personal data in cloud servers which are remote servers not owned by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one.

The aspects presented in this paper are organized with a view to discuss and indentify the approach to cloud computing as well as the security issues and concerns that must be taken into account in the deployment towards a cloud based computing infrastructure. Discussion on the technological concepts and approaches to cloud computing including the architectural illustration has been taken into consideration within the context of discussion in this paper. Security issues inherent in cloud computing approach have been discussed afterwards. The exploration in the technological and security concerns of cloud computing has led to the concluding realization on the overall aspects of cloud computing.

2. CLOUD COMPUTING ARCHITECTURE

2.1 SERVICE MODELS

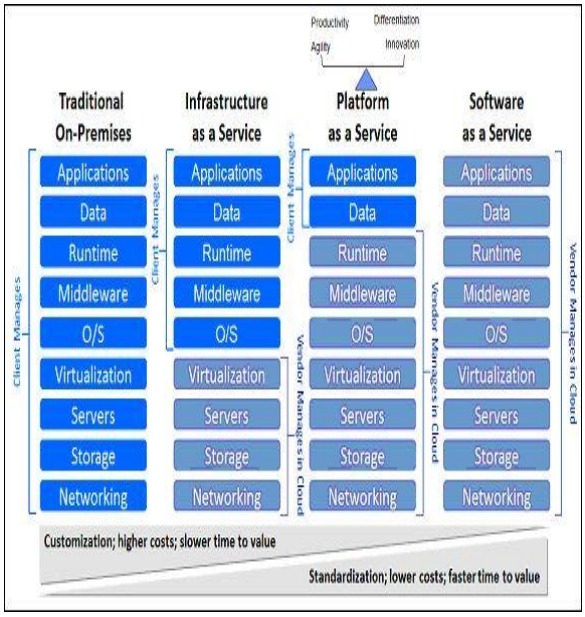
Broadly speaking cloud providers offer three types of services:

- Software as a Service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

Software as a Service (SaaS): It is also called a delivery model where the software and the data which is associated with is hosted over the cloud environment by third party called cloud service provider, just like your Gmail account, you use that application on someone else's system.

Platform as a Service (PaaS): In this service, you can use Web-based tools to develop applications so they run on systems software which is provided by another company, like Google App Engine.

Infrastructure as a Service (IaaS): It provides services to the companies with computing resources including servers, networking, storage, and datacenter space on a pay-per-use basis.



2.2 Deployment models

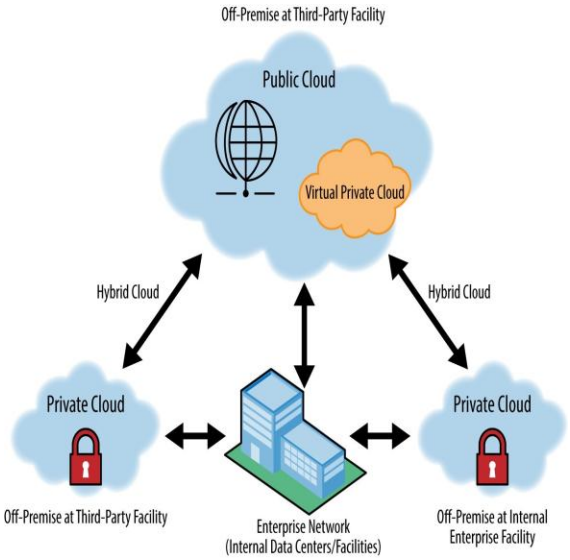
There are three Deployment Models and are described below:

- Public Model
- Private Model
- Hybrid Model

Public Model: This infrastructure is available to the general public. As the name suggests, public cloud is a model in which resources are generally available to everyone and anywhere.

Private Model: This model is developed for the private organizations like one house and an organization and they can use it for their own purpose. This kind of a service is not accessed by everyone.

Hybrid Model: Hybrid Clouds are combination of public and private cloud in a same network. This can be done if private cloud need some important services from the public cloud like Private cloud can store some information on their private cloud and we can use that information on public cloud.



3. SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing consists of applications, platforms and infrastructure segments. Every segment performs different operations and offers different products for businesses and individuals around the world. There are numerous security issues for cloud computing as it encompasses many technologies which includes networks, databases, operating systems, virtualization, resource scheduling, transaction management, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

• Access to Servers & Applications

• Data Transmission

• Virtual Machine Security

• Network Security

- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance

3.1 Data Transmission

It is the process of sending digital or analog data over a communication medium to one or more computing network. In Cloud environment most of the data is not encrypted in the processing time. To process data for any application that data must be unencrypted. In homomorphism encryption which allows the data to be processed without being decrypted. The attack is carried out when the attackers place themselves in the communications path between the users. Here there is the possibility that they can interrupt and change communications.

3.2 Virtual Machine Security

The term Virtual Machine (VM) describes sharing the resources of one single physical computer into various computers within itself. VM's provide agility, flexibility and scalability to the cloud resources by allowing the vendors to copy, move and manipulate their VM's. Keeping this in mind, malicious hackers are finding ways to get their hands on valuable data by manipulating safeguards and breaching the security layers of cloud environments. The cloud computing scenario is not as transparent as it claims to be. The service user has no idea about how the data is processed and stored and cannot directly control the flow of data storage and processing. Having VM's would indirectly allows anyone access to the host disk of the VM to take an illegal copy of the whole system.

3.3 Data Integrity

Corruption of data can happen at any level of storage. So Integrity monitoring is must in cloud storage. Data Integrity in a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation, durability). Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds, users may lose control of their data and rely on cloud operators to enforce access control.

3.4 Data Location

Cloud users are not aware of the exact location of the datacenter and also they don't have any control over the physical access to that data. Most of the cloud providers have datacenters around the world. In many countries certain types of data cannot leave the country because of potentially sensitive information. Next in the complexity chain there are distributed systems in which there are multiple databases and multiple applications.

Based on the study, we found that there are many issues in cloud computing but security is the major issue which is associated with cloud computing.

Top seven security issues in cloud computing environment as discovered by "Cloud Security Alliance" CSA are:

- Misuse and reprehensible use of Cloud Computing.
- Insecure API.
- Wicked Insiders.
- Shared Technology issues / multi-tenancy nature.
- Data Crash.
- Account, Service & Traffic Hijacking.
- Unidentified risk report.

3.5 Misuse and reprehensible Use of Cloud Computing

Hackers, spammers and other criminals take advantage of the suitable registration, simple

procedures and comparatively unspecified access to cloud services to launch various attacks such as key cracking, password etc.

3.6 Insecure Application Programming Interfaces (API)

Customers handle and interact with cloud services through API's. Providers must ensure that security is integrated into their service models, while users must be aware of security risks.

3.7 Wicked Insiders

Malicious insiders create a huge threat in cloud computing environment, since consumers do not have a clear sight of provider policies and procedures. Malicious insiders can gain unauthorized access into organization and their assets.

3.8 Shared Technology issues/multi-tenancy nature

This is basically based on shared infrastructure, which is not designed to accommodate a multi-tenant architecture.

3.9 Data Crash

Comprised data may include deleted or altered data without making a backup, unlinking a record from a huge environment, loss of an encoding key and illegal access of sensitive data.

3.10 Account, Service & Traffic Hijacking

Account or service hijacking is usually carried out with stolen credentials. Such attacks include phishing, fraud and exploitation of software vulnerabilities. Attackers can access critical areas of cloud computing services like confidentiality, integrity and availability of services.

3.11 Unidentified Risk Report

Cloud services means that organizations are less involved with software and hardware, so organizations should not be aware with these issues such as internal security, security compliance, auditing and logging may be overlooked.

4. RESEARCH CHALLENGES

Cloud computing research addresses the challenges of meeting the requirements of next generation private, public and hybrid cloud computing architectures and also the challenges of allowing applications and development platforms to take advantage of the benefits of cloud computing. Many existing issues have not been fully addressed, while new challenges keep emerging from industry applications. Some of the challenging research issues in cloud computing are given below.

• Service Level Agreements (SLA's)

• Cloud Data Management & Security

• Interoperability

• Multi-tenancy

• Server Consolidation

• Common Cloud Standards

• Platform Management

4.1 Service Level Agreements (SLA's)

Cloud is administrated by service level agreements that allow several instances of one application to be duplicated on multiple servers if need arises; dependent on a priority scheme, the cloud may minimize or shut down a lower level application. A big challenge for the cloud customers is to evaluate SLA's of cloud vendors. Most of the cloud vendors create SLA's to make a defensive shield against legal action while offering assurances to customers. So there are some issues such as data protection, outages and price structures that must be taken

into account by the customers before signing a contract with the vendor. And also is there any SLA associated with backup, archive, or preservation of data? If the service account becomes inactive then do they keep user data? If yes, then how long? So it's an important research area in cloud computing.

4.2 Cloud Data Management

Cloud data can be huge, unstructured and typically append only with rare updates. As service vendors don't have access to the physical security system of data centers, they must rely on the infrastructure provider to achieve full data security. In a virtualized environment like the clouds, VMs can dynamically migrate from one location to another; hence directly using remote attestation is not sufficient. In such case, it is critical to build trust mechanisms at every architectural layer of the cloud. Software frameworks such as **MapReduce** and its various implementations such as **Hadoop** are designed for distributed processing of data intensive tasks, these frameworks typically operate on Internet scale file system.

4.3 Interoperability

It is the ability of a computer system to run application programs from different vendors and to interact with other computers across LAN or WAN independent of their physical architecture and operating systems. Many public cloud networks are configured as closed systems and are not designed to interact with each other. To overcome this challenge, industry standards must be developed to help cloud service providers design interoperable platforms and enable data portability. Organizations need to automatically provision services, manage VM instances, and work with both cloud-based and enterprise-based applications using a single tool set that can function across existing programs and multiple cloud providers.

4.4 MULTI-TENANCY

Multi-tenancy is a major concern in cloud computing. Multi-tenancy occurs when multiple consumers uses the same cloud, same operating system, on the same hardware, with the same data-storage system to share the information and data or runs on a single server.

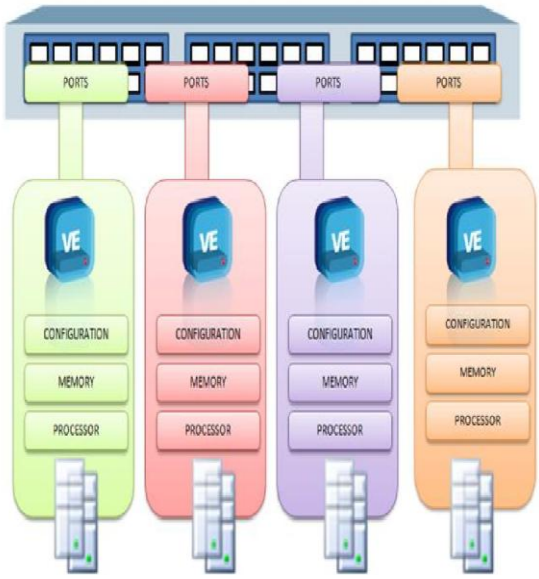
There are multiple types of cloud applications that users can access through the Internet, from small Internet based widgets to large enterprise software applications that have increased security requirements based on the type of data being stored on the software vendor's infrastructure. These application requests require multi-tenancy for many reasons, the most important is cost. Multiple customers accessing the same hardware, application servers, and databases may affect response times and performance for other customers. For application-layer multi-tenancy specifically, resources are shared at each infrastructure layer and have valid security and performance concerns. For example, multiple service requests accessing resources at the same time increase wait times but not necessarily CPU time, or the number of connections to an HTTP server has been exhausted, and the service must wait until it can use an available connection or in a worst-case scenario drops the service request.

4.4.1 Architecture

This architecture fully separates your information from other customer's information, while allowing us to roll out rapidly the latest functionality to each, all at once. This approach offers the most configurability and allows you to extract deep insight from your information

Oracle delivers a latest Multitenant architecture that allows a multitenant container database to grasp numerous pluggable databases. An

existing database can simply be adopted with no application changes necessary.



4.4.2 What Multi-Tenancy is Able To Do?

Simplify Data Mining: Instead of being composed from various sources, all the information for consumers is stored in a single database scheme.

Decreases expenditure: Multi-tenancy reduces the overhead by amortizing it over many users, like they can charge for the certified software because everyone can run it on a single system, so only single certify will need to purchase.

More elasticity: It provides the flexibility of importing and exporting your information

5. CONCLUSION AND FUTURE WORK

Cloud computing has enormous prospects, but with equal number of security threats. One of the biggest security worries with the cloud computing model is the multi-tenancy. In this paper, we first discussed various models of cloud computing, security issues and research challenges in cloud computing. Multi-tenancy is major issue for Cloud Computing Security. There are several other security challenges that include security aspects of network and virtualization.

The infinite possibilities of cloud computing cannot be unseen only for the security issues - the unending analysis and research for robust, regular and integrated security models for cloud computing might be the only path of inspiration.

Based on this fact that the impact of security issues in cloud computing can be decreased by multi-tenancy architecture. Regardless of the nature of security issues, it can be undoubtedly concluded that the deployment of any form of cloud computing should deal with the security concerns corresponding to those of the safety critical systems.

We believe that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques are needed to be radically tweaked to be able to work with the clouds architecture. We hope our work will provide a better understanding of the design challenges of cloud computing, and pave the path for further research in this area.

REFERENCES

[1] Abbadi, I.M. and Martin, A., "Trust in the Cloud", Information Security Technical Report, 16, 108-114, 2011.

[2] Casola, V., Cuomo, A., Rak, M. and Villano, U., "The Cloud Grid approach: Security analysis and performance evaluation", Future Generation Computer Systems, 29, 387-401, 2013.

[3] Zissis, D and Lekkas, D., "Addressing cloud computing security issues", Future Generation Computer Systems, 28, 583-592, 2012.

[4] Teneyuca, D, "Internet cloud security: The illusion of inclusion", Information Security Technical Report, 16, 102-107, 2011.

[5] R. L Grossman, "The Case for Cloud Computing", IT Professional, Vol. 11(2), 23-27, 2009.

[6] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O' Reilly Media, USA, 2009.

[7] Takeshi Takahashi, Gregory Blancy, Youki Kadobayashiy, Doudou Fally, Hiroaki Hazeyamay, Shinichiro Matsuo, "Enabling Secure Multitenancy in Cloud Computing: Challenges".

[8] Nagarjuna, Kalyan Srinivas, S.Sajida, Lokesh, "Security Techniques for Multitenancy Applications in Cloud", International Journal of Computer Science and Mobile Computing, Vol.2 Issue. 8, 248-251, 2013.