*International Journal of Computer Trends and Technology (IJCTT) – volume 23 Number 4–May 2015*

# Distributed Security on Cloud: Mobile Cloud Operating System

Manish Tewari[#1], Anuj Kumar Yadav[*2]

[#1] *Department of Information Technology, D.I.T University, Dehradun, Uttarakhand 2480001, India*

[*2] *Department of Computer Science and Engineering, D.I.T University, Dehradun, Uttarakhand 248001, India*

***Abstract*— We all were concern about security for cloud. Everyone is running on security algorithms like encryption decryption and all, but they were many approaches which is far better than the security algorithms. First we have to implement security part. As we all known cloud popularities is increasing day by day so everyone thinking whether our data is safe or not, as data is the most important for any person. With the help of this method your data is safe. The method is like this data is divided into small segments and store in all different cloud related with each other and that cloud will store data into different servers and those server will save data into different database and those database will store data into different disk. Like this our data is stored in different parts. As security for all cloud and all server is different, so hacker can't access the d ata from all the servers. As data is not stored in one server. Only a partial data is stored.**

***Keywords*— Distributed Security on Cloud, *Mobile Cloud Operating System*..**

## I. INTRODUCTION

A Cloud can be of two types private or public. Public Cloud sells services to anyone to the Internet. (Amazon Web Services is one of the largest public Cloud providers.) A private Cloud is a network on a data center that provides hosting services to a limited people who want's that services. When a service provider uses technology of public Cloud resources for creating their private Cloud, then it is called as a virtual private Cloud. Whether it is Private or public, goal of Cloud computing is to provide services as easy, flexibility, scalable to access computing resources for IT services.

Infrastructure-as-a-Service Amazon Web Services presents the customer with virtual server and storage and application program interfaces (APIs) so that customer can start, stop, access and configure to their own virtual servers and storage. Model allows a company to pay only for the capacity as they needed, and bring more whenever they required. Because this pay what you use model just like the way electricity, fuel and water consumption, it's referred like utility computing.

Platform-as-a-service Cloud likes a set of software development tools hosted on the service provider's infrastructure part. Developers can create their own applications on the service provider's platform over the Internet. PaaS providers use Application Programing Interfaces (APIs), website portals or gateway these software installed on the customer's computer for their own use. Force and Google Apps are examples of PaaS. Developers need to know that current technology, no standards for interoperability or data portability to the Cloud. Some service providers will not allow software which created by their user to be moved off the provider's platforms.

Software-as-a-service Cloud model, the providers supplies the hardware infrastructure, software product and interacts with the customers through a front-end web portal. Services can be any type from email to inventory control and database processing. Service provider for hosts both the application and data, the user is freely to use the service from anywhere which they like.

Security is the set of under control-based technologies and policies designed to be set and compliance rules and protect the information, applications of data and infrastructure resources associated with Cloud computing. Cloud's very nature as a sharing of resource, identity management, privacy and control access are of particular concern. Organizations which uses Cloud computing and Cloud providers for data operations, security in these and vulnerable areas have become a very much important for organizations contacting with a Cloud computing service provider. Cloud computing security should look on the security controls to the Cloud provider will incorporate to keep on maintain the customer data security, privacy and compliance providing with necessary regulations. Processes likely include a business continuity and data backup plan and restore in the case of a Cloud security breach.

Cyber infrastructure makes applications dramatically easier to deploy and developed, thus expanding the feasible scope of applications possible within organizational constraints, budgets and shifting the scientist's and engineer's effort away from information technology development and concentrating it on scientific and research in engineering. Cyber infrastructure also increases efficiency, quality, and reliability by commonalities capturing among application needs, facilitates the efficient sharing of services and equipment's.

As most of the resource deliveries are through remote connection, non-protected APIs, (APIs and PaaS services are one of the easiest attack vector). Attack methods such as fraud,

phishing, and exploitation vulnerabilities of software still achieve results. Passwords and credentials are often reused, amplifies the impact of such kind of attacks. Attacker gains access to your credentials, can have eavesdrop on your activities and transactions statements, manipulate data, return false information, and redirect your clients to illegal and untrusted sites. Your account or service images may become a new target for the attacker. They can have enough power of your reputation to do any subsequent attacks..

## II. Literature Survey

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

### *A. Distributed Cloud OS*

A distributed operating systems control program running on a set of computers that are interconnected by an internet network. This control program unifies the different computers into a single integrated compute and storage resource. Depends upon on the facilities it provides, a distributed operating system is classified as general purpose, real time, or embedded. The need for distributed operating system stems from rapid changes in the hardware environment in many organizations. Hardware prices have fallen rapidly in the last decade, resulting rapid increase of workstation, personal computers, data and compute servers, and networks. This rapid increase has underlined the need for efficient and transparent management of these physically distributed resources.

**C**loud is a distributed operating system that integrates a set of nodes into a conceptually centralized system. System is composed of compute servers, data servers, and user workstation. A compute server is a machine that is available for use as a computational engine. A data server is a machine that functions as a repository for long-lived (that is, persistent) data. A user workstation is a machine that provides a programing environment for developing applications and an interface with the compute and data servers for executing those applications on the servers. Note that when a disk is associated with a compute server, it can also act as a data server for other operating system that runs on top of a native operating system that runs on top of a native kernel called Ra (after the Egyptian sun god). It currently runs on Sun-3/50 and Sun-3/60 computers and cooperates with Sun SPARCstation's (running UNIX) that provides user interfaces. Clouds are a general-purpose operating system. That it is intended to support all types of languages and application distributed or not.

### *B. Cloud Computing:*

It is not easy to defined cloud computing. Many definitions evolve, which share the same common denominator: which is the Internet we use. Cloud computing is another way to use the Internet services in our daily life from a single machine, all the tools installed on computers. It is also the ability to use shared computing resources with local servers handling applications. With cloud computing users do not worry about the location and the storage of their data. Starting using their services anywhere and at any time. The main part of this technology is virtualization (Hypervisor) and virtual world.

Virtualization provides a means to separate the physical hardware and the operating system and applications by simulating software. The software called hypervisor is uploaded inside the computer. Software can also upload the files that define a virtual computer, into a virtual machine. Virtual appliance is an application that is grouped together with all the components that it needs in order to run with an operating system. The computers virtualization and operating systems hides the physical characteristics of computers from the users. Hypervisor is a part of virtualization, allows many virtual operating systems to run on the same physical machine altogether.

In the same server system hardware, one can be able to install many instances of the virtual servers, which can be connected together via the virtual switch. The architecture which allows the creation of a virtual data center with the same functionalities as a real rack system environment. The redundancy of this system allows the applications to be available to the users at any time and everywhere.

.

## III. Problem Statement

Cloud computing has created a fundamental shift in how information technology infrastructure is managed and run, changed both the business and technology sides of IT. But, as with any major change in history, there are many supporters and sceptics for useful help. Transferring enterprise IT to the cloud is a complex task that includes both technical and organizational challenges. A new paradigm that doesn't have a clear one-sentence definition; it includes multiple factors; so that they can transformation to a cloud-based process may seem confusing. Complexity paired with uncertainty creates a number of organizational cloud-adoption barriers.
Those barriers represent business part, technical and organizational challenges. The importance of organizational challenges is difficult to filter, but such challenges can be critical in the decision-making process. Cloud must be prepared to face substantial resistance, as employees inside organizations might be reluctant to embrace cloud-transformation and make this crucial technology shift.

### *A. Data Security*

Data security is by far the most challenging barrier to cloud must adopt. Data is one of the most important corporate

world, and companies want to know about their data is in safe hand. Companies feel confident and relax when they store data internally because they have full control. Although no such guaranty that data is better protected internally comparing to public cloud. Such kind of possibility that data could be even safer in the public cloud because public cloud providers may poses higher level of data security expertise comparing to their customers.

When stored at public cloud, data can be compromised at several different data-lifecycle stages: during transfer from the internal company network to the public cloud, data is stored in the public cloud, during restoring the processes and data backup. Few questions to ask in order to ensure data security in a public cloud

- Who has been accessing the data? What will be the access-control policies? Do I have full visibility into information regarding these access-control policies?
- Whether it is encrypted data during transfer from the internal network to the public cloud? What is the encryption algorithm? Can data be encrypted when stored in the cloud? Who holds the encryption keys?
- If a cloud provider is not supposed to have access to the data, encryption keys should be held only by the company who owns the data part. Some of the company standards mandate full data encryption doesn't permit cloud providers to hold encryption keys.
- What will be the disaster-recovery process? Can cloud provider replicate data across multiple datacentres? Are these datacentres located in different geographical locations?
- If data is stored in only one datacentre and the cloud provider doesn't have the capability to replicate it at other datacentres, must be raised.
- How the data-backup process hold. Who has right to access the backup data? Where is the backup data stored?
- What is the recovery process in data? How much time data recovery takes?
- What is the investigation process in security breach? Cloud provider has security-breach investigation capabilities or not?

This kind of question is forgotten, it must be very important – if data is compromised, the cloud service provider is the only source of information for any kind of investigation.

## IV. Research Methodology

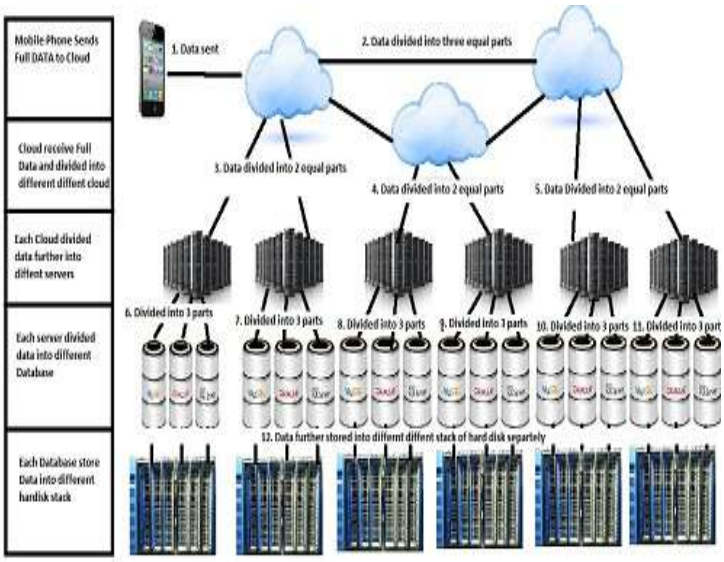


Fig. 1 Distributed Secuirty on Cloud Architecture

In Fig. 1 Distributed Security on Cloud Architecture is divided into five phase.

Phase1. Data is sending to cloud server from mobile phones, as mobile devices is connected directly with cloud.
Phase2. Cloud divides data among all cloud which is connected with each other.
Phase3. Now all clouds server further divides data into all servers which connected with them.
Phase4.Server further divides data and sends to all databases that connected with server.
Phase5. Now Database divides the data and store into all different drives.

This approach is very useful for security purpose. We know data is very important and hackers keep on attacking all the time, for security purpose this approach is apply. As we already know the data is not stored only in 1 server, data is divided into small segments and stored in many different clouds, many different virtualized servers and many different databases. So that hackers will never found where the actual real data is, they won't be able to found the complete data in one server.

## V. Conclusions

MCOS reserves data in simple and arranged manner. To get information from present mobile phones is very complex. If each mobile phone is connected to MCOS then data retention will be very easy. If each company connects their mobile phones to Cloud server then no terrorist can use their mobile phone for crime. Government will have full information of all

users as data of all mobile phones are available in Cloud server.

As data is the most important part in any device, to make data more secure I have implemented simple approach in a distributed manner. Rather than store data in 1 server, we divide the data and store in different server in different machines which is 1 more level of security. All servers have their own and different security programs for protecting their server. From this we have multi-level security which has come from all different servers and their respective clouds.

## REFERENCES


[1] Biao Song, Eui-Nam Huh Yuan Tian, "Towards the Development of Personal Cloud," in *IEEE*, 2011, p. 5.

[2] Partha Dasgupta, "The Clouds Distirbuted Operating System," , Georgia, 1991.

[3] Ditto, "Cyberinfrastructure," 2011.

[4] Kangchan Lee, "Security Threats in Cloud Computing Environments," vol. 6, 2012.

[5] Nahla Alwan, Ihsan Alshahib Lami Chigozirim Oriaku, "The Readiness of Mobile Operating Systems for Cloud Services," , 2012.

[6] B.-G. Chun and P. Maniatis., "Augmented smartphone applications through clone cloud execution," , 2009.