



Cloud Computing: Issues Regarding Security, Applications and Mobile Cloud Computing

Smita Parte, Noumita Dehariya

Assistant Professor (CSE) TIT College,
Bhopal, M.P., India

Abstract: Cloud computing is the use of computing resources that are delivered as a service over a network. Today, cloud computing generates a lot of solutions. Now a days there are many innovations coming every day in the mobile applications in order to serve end users in best possible ways as well as use of cloud computing is an also increase with mobile applications which is called as mobile cloud computing. The mobile cloud computing is uses the services of cloud into environment of mobile applications for overcoming the many issues such as bandwidth, battery life, most importantly storage, security etc. As this is our review paper, during this paper we present first survey over the mobile cloud computing systems. It is very promising area. Businesses World sees it's potential but there are also many issues like security trust, expectations, regulations, and performance. Cloud computing offers attractive financial and technological advantages but some of them has not been fully evaluated with respect to security. Security is considered one of the most critical aspects in cloud computing due to the sensitivity and importance of data stored in the cloud.

Keyword: Denial of Service (DoS) attacks, Intrusion Detection Systems (IDSs), Antivirus (AV), and Email Security.

I. INTRODUCTION

As a introduction, the mechanism of cloud computing delivers the facility of sharing the resources, accessing the shared resources, providing the web based infrastructure for information storage from any place in the world. The services offered by cloud are completely on demand services. Cloud computing solves the many issues of storing and monitoring of data for many business companies. The end user of cloud computing is not aware about the physical location of resources used [1]. In addition to this cloud, computing provides the facilities of designing, building, deploying and then managing their own applications remotely without need of any extra software or hardware. Following best examples of real time cloud service providers:

Elastic Computing Cloud (EC2): This is the cloud framework of Amazon. This provides the computational services that allow peoples to use CPU cycles without buying more computers.

Simple Storage Service (S3): Amazon also provides this service. Nirvanix Company which allowing organizations to store data as well as documents without adding a single on-site server. Therefore, with such benefits the cloud computing is increasingly used by many business companies as well as individuals [2]. The use of cloud computing increasing day by day, the end users and the service providers are able to utilize the cloud resources with less cost and easily without owning all the resource needed. However, the services of cloud computing is having many problems associated with it. The most common is security. Since from last few years, the problems like security, authentication, privacy preservation, access control etc studied more by various researchers [3]. The cloud services later introduced in mobile technologies as well which is called as mobile cloud computing. The user authentication in the mobile cloud computing environment, especially the more important to them and high level of security certification is required.

CLOUD computing” implies access to isolated computing services suggested by third parties via a TCP/IP connection to the public internet. It is internet based development and use of computer technology. Public cloud, Private cloud and Hybrid cloud, which combine both public and private clouds are types of cloud computing.

- **Public cloud:** Public cloud provides scalable, dynamically provisioned, virtualized recourses available over the internet from an offsite third party provider. Think Grid is a company that provides multi tenant architecture for supplying services such as Hosted Desktops. Other popular cloud vendors include Salesforce.com, Amazon EC2 and Flexi Scale.
- **Private cloud:** It is providing hosted services on the private networks. This type of cloud is used by large companies and allows their corporate network and data center administrators to effectively become in house service providers.
- **Hybrid cloud:** It combines resources from both internal and external providers and so it becomes the most popular choice for enterprises. It is comprise of two or more than two clouds. There are three service models in cloud computing as Software as -a-Service (SaaS), Platform as a-Service (PaaS) and Infrastructure as -a-Service (IaaS).

II. REVIEW OF CLOUD COMPUTING FRAMEWORK

Data centers layer: This layer provides the hardware facility and infrastructure for clouds. In data center layer, a number of servers are linked with high speed networks to provide services for customers

Service Oriented Cloud Computing Architecture Infrastructure As a service (annual): Annual data center built on top of the layer. Annual storage, hardware, servers and enables the provision of networking components. Client usually pays a per use basis. Thus, customers pay a cost based. Infrastructure can be expanded or shrunk dynamically as needed examples of annual Amazon EC2 (elastic cloud computing) and S3 (simple storage service).

Platform -as-a-service (PaaS): PaaS, testing and deployment of custom applications for an advanced integrated environment. Google App engine, Microsoft Azure, Amazon Simple storage service map is example of PaaS.

Software as a Service (SaaS): SaaS supports a software distribution with specific requirements. In this layer, the users can access an application and information remotely via the Internet and pay only for that they use. Sales force is one of the pioneers in providing this service model. Cloud computing is known to be a promising solution for mobile computing due to many reasons (e.g., mobility, communication, and portability [13]).

Infrastructure as a Service (IaaS): Mobile Cloud Computing at its simplest refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device.

III. ISSUES REGARDING CLOUD SECURITY

Cloud computing provides tremendous advantages to organizations of all sizes. For small businesses, cloud computing permits time constrained IT groups to work additional with efficiency. For big enterprises, the cloud provides the flexibility to proportion or right down .To respond quickly to dynamical market conditions. Businesses of all sizes will leverage the cloud to extend innovation and collaboration.

Following are some major issues of cloud computing while its implementation.

a) Privacy: It related to storing and securing data, and monitoring the use of the cloud by the service providers. In the context privacy occur according to the cloud deployment model [3]. Privacy in Cloud computing include following issues:

- ❖ Unauthorized Secondary Usage
- ❖ Lack of User Control
- ❖ Data Proliferation and Trans border Data Flow
- ❖ Dynamic Provisioning

b) Security: Cloud vendors are being facing issues in confidentiality, integrity and availability in data security. Cloud is expected to offer the capabilities like encryption strategies to ensure safe data storage environment, strict access control, secure and stable backup of user data

Some security issues in cloud computing is as follows:

- ❖ Access
- ❖ Availability and backup
- ❖ Control over data life cycle
- ❖ Multitenancy
- ❖ Audit

c) Trust: Trust revolves around ‘assurance’ and confidence that people, data, entities, information or processes will function or behave in expected ways. At a deeper level, trust might be regarded as a consequence of progress towards security or privacy objectives [5]. Trust between the Service provider and the customer is one of the main issues in cloud computing. There is no way for the customer to be sure whether the management of the Service is trustworthy, and whether there is any risk of insider attacks. This is a major issue and has received strong attention by companies [9]. The only legal document between the customer and service provider is the Service Level Agreement (SLA). This document contains all the agreements between the customer and the service provider; it contains what the service provider is doing and is willing to do [10].

IV. TAXONOMY OF SECURITY ASPECTS IN CLOUD COMPUTING

The taxonomy contains four classes as application and platform, administration, infrastructure, and compliance

- **Administration:** The administration of cloud services presents one of the main challenges from a security perspective. This is still given too little support by cloud providers, let alone tools available to cloud users. These are still under development and aim at enabling cloud service users to manage their rented cloud services in an integrated and efficient way.
- **Application and platform:** The key risks affecting the application and platform part of the cloud taxonomy are those which can arise during the development and use of cloud services and which may have their origins both in the infrastructure and in the application provided as a service as well as the associated platform.
- **Infrastructure:** The infrastructure area of the taxonomy concerns the threats to the security of services on the infrastructure layer. The infrastructure layer is divided into the four areas of physical security, host, virtualization and network which constitute the core components of the cloud infrastructure.
- **Compliance:** The domain compliance brings together all the regulatory issues which may impact the protection goals. Important security guidelines, certificates and standards which a cloud vendor ought to have are also

discussed in the context of governance. In general it is the case that compliance monitoring procedures for Internet based services such as cloud services must be extended if they are about to cover applications, users and activities in cloud computing systems effectively.

V. SECURITY CONCERNS

To provide effective security for a cloud environment, both the cloud provider and consumer must partner to provide solutions to the following security concerns:

- **Governance and Enterprise Risk Management:** The ability of an organization to govern and measure enterprise risk that is introduced by cloud computing. This concern includes items such as legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault.
- **Compliance and Audit:** Maintaining and proving compliance when using cloud computing. Issues involve evaluating how cloud computing affects compliance with internal security policies, and also various compliance requirements.
- **Application Security:** Securing application software that is running on or being developed in the cloud. This concern includes items such as whether it is appropriate to migrate or design an application to run in the cloud.
- **Encryption and Key Management:** Identifying proper encryption usage and scalable key management. This concern addresses access controls of both accesses to resources and for protecting data.
- **Identity and Access Management:** Managing identities and leveraging directory services to provide access control. The focus is on issues that are encountered when extending an organization's identity into the cloud.

VI. EXISTING CLOUD SOLUTIONS

Due to a general lack of interoperability standards, and the lack of sufficient market pressure for these standards, transitioning between cloud providers may be a painful manual process.

•All Types of solutions for Cloud:

- i. Substituting cloud providers is in virtually all cases a negative business transaction for at least one party, which can cause an unexpected negative reaction from the legacy cloud provider.
- ii. Understand the size of data sets hosted at a cloud provider. The sheer size of data may cause an interruption of service during a transition, or a longer transition period than anticipated. Many customers have found that using a courier to ship hard drives is faster than electronic transmission for large data sets.
- iii. Document the security architecture and configuration of individual component security controls so they can be used to support internal audits, as well as to facilitate migration to new providers.

•For IaaS Cloud Solutions:

- i. Understand how virtual machine images can be captured and ported to new cloud providers, who may use different virtualization technologies.
- ii. Identify and eliminate (or at least document) any provider specific extensions to the virtual machine environment.
- iii. Understand what practices are in place to make sure appropriate deprovisioning of VM images occurs after an application is ported from the cloud provider.
- iv. Understand the practices used for decommissioning of disks and storage devices.
- v. Understand hardware/platform based dependencies that need to be identified before migration of the application/data.
- vi. Ask for access to system logs, traces, and access and billing records from the legacy cloud provider.
- vii. Identify options to resume or extend service with the legacy cloud provider in part or in whole if new service proves to be inferior.
- viii. Determine if there are any management level functions, interfaces, or APIs being used that are incompatible with or unimplemented by the new provider.

•For PaaS Cloud Solutions:

- i. When possible, use platform components with a standard syntax, open APIs, and open standards.
- ii. Understand what tools are available for secure data transfer, backup, and restore.
- iii. Understand and document application components and modules specific to the PaaS provider, and develop application architecture with layers of abstraction to minimize direct access to proprietary modules.
- iv. Understand how base services like monitoring, logging, and auditing would transfer over to a new vendor.
- v. Understand control functions provided by the legacy cloud provider and how they would translate to the new provider.
- vi. When migrating to a new platform, understand the impacts on performance and availability of the application, and how these impacts will be measured.

•For SaaS Solutions:

- vii. Perform regular data extractions and backups to a format that is usable without the SaaS provider.
- viii. Understand whether metadata can be preserved and migrated.
- ix. Understand that any custom tools being implemented will have to be redeveloped, or the new vendor must provide those tools.

- x. Assure consistency of control effectiveness across old and new providers.
- xi. Assure the possibility of migration of backups and other copies of logs, access records, and any other pertinent information which may be required for legal and compliance reasons.
- xii. Understand management, monitoring, and reporting interfaces and their integration between environments.
- xiii. To find whether there is a provision for the new vendor to test and evaluate the applications before migration. Also, some researchers have suggested cloud based security solutions related to distributed denial of service (DDoS) attacks, intrusion detection systems (IDSs), antivirus (AV), and email security.

A) Intrusion Detection System (IDS)

The Architecture of IDS involves several IDS sensors distributed across the cloud and a central management unit. Each protected endpoint is monitored by a separate sensor. Each sensor reports alerts to the central management unit, which gathers all sensor alerts and processes them. The design can detect attacks using the correlated alerts from different IDS sensors [2].

B) Cloud Computing Security Overlay Network

Such overlay networks were first used in the deployment of the Internet over telephone networks. Security overlay network that offers an integrated set of security service. Security systems designed to protect any virtual or physical machine using an overlay network. The collaboration among all these security systems can provide a robust computing.

C) Distributed Denial of Service Attack (DDoS)

This attack is the form of attack that an attacker aims to prevent legitimate users from accessing information or services. The common type of this attack occurs when an attacker floods a network with excessive requests to the target server until the server is unable to provide services to normal users.

D) Email Security

McAfee Cloud Security helps organizations safely and confidently leverage secure cloud computing services and solutions. The Zscaler system [13] provides antispam services, among others, in the cloud. It uses a proxy to filter the network traffic into the cloud. McAfee SaaS Email Protection also provides a cloud based email antispam solution.

V. CONCLUSION

In this paper we have discussed security issues of cloud computing and also about mobile cloud computing. We have also explain some existing cloud security solutions by some researchers. There are many other challenges about security aspect of cloud computing. There are various solutions available for the challenges in cloud computing, stakeholders, vendors, enterprises and organizations have to think seriously about security aspect of cloud computing before adopting the cloud system.

REFERENCES

- [1] R. Kalaichelvi Chandrahasan., S. Shanmuga Priya and Dr. L. Arokiam., "Research Challenges and Security Issues in Cloud Computing", International Journal of Computational Intelligence and Information Security, March 2012, Vol. 3, No. 3
- [2] www.idc.com
- [3] Grobaur, B., Walloschek T., Stoker E., (2011). Understanding Cloud Computing Inerabilities. Security and Privacy. IEEE, Vol.9, pp 50.
- [4] Kresimir P., Zeljko H. (2010). Cloud Computing Security and Challenges. MIPRO 2010, May 24 28, 2010
- [5] Debabrata Nayak., Understanding the Security, Privacy and Trust Challenges of Cloud Computing. Retrieved from riverpublishers.com/journal/journal/RP_Journal_2245_1439_127.pdf
- [6] Heiser, Jay and Mark Nicolett: Assessing the security risks of cloud computing Technical Report G00157782, Gartner Research, June 2008.
- [7] www.cloud standards.org
- [8] Bardin, Jeff, Jon Callas, Shawn Chaput, Pam Fusco, Francoise Gilbert, Christofer ,Hoff, , Dennis Hurst, Subra Kumaraswamy, Liam Lynch, Scott Matsumoto, Brian Higgins, Jean Pawluk, George Reese, Jeff Reich, Jeffrey Ritter, Jeff Spivey, and John Viega: Security guidance for critical areas of focus in cloud computing . Technical report, Cloud Security Alliance, April 2009.
- [9] <http://www.cloud.competence.center.com/understanding/taxonomy/cloud-computing-security/>
- [10] Cloud Computing Security Issues and Solutions, Published by JoshuaKissoon on Sat, 03/23/2013