ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

A Review on Cloud Computing Vulnerabilities

Ms. Sugandha Nandedkar, Ms.Sangeeta Kakarwal

Asst.Prof., Department of Computer Science and Engineering, DIEMS /Dr. BAMU, Aurangabad, MH, India.

Prof. and HOD, Department of Information Technology,PESCOE/Dr. BAMU, Aurangabad, MH. India.

Abstract: Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing provides significant cost effective IT resources as cost on demand IT based on the actual usage of the customer. Despite of this cloud computing also causes significant changes in the vulnerability factor. Thus moving to a cloud infrastructure, it might change the attackers' access level and motivation, as well as the effort and risk—a fact that must be considered as future work. But, for supporting a cloud-specific risk assessment, it seems most profitable to start by examining the exact nature of cloud-specific vulnerabilities.

This paper focuses more on cloud-specific vulnerabilities. As well as puts some of the corrective measures we can follow to safely handle it.

Keywords: Cloud Computing, Disaster Recovery, Security, Vulnerability

I. INTRODUCTION

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services -- such as servers, storage and applications -- are delivered to an organization's computers and devices through the Internet [1].

In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system'sinterface software**,** which can be as simple as a Web browser, and the cloud's network takes care of the rest.The simplest example of CC is an e-mail account with a web-based e-mail service like Hotmail, Yahoo! Mail or GmailHere instead of running an e-mail program on your computer, you log in to a web e-mail account remotely. The software and storage for your account doesn't exist on your computer -- it's on the service's computer cloud [2].

Clouds are of two types: 1) Community cloud 2) Public Cloud

Community Cloud: Community cloud shares infrastructure between several organizations from a specific community with common concerns, whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than that of a private) to realize its cost saving potential.

Public Cloud: A public cloud is established where several organizations have similar requirements and seek to share infrastructure so as to appliance. In addition, it can be economically attractive as the resources (storage, workstations) utilized and shared in the community are already exploited.

This is the cloud computing model where service providers make their computing resources available online for the public. It allows the users to access various important resources on cloud, such as:Software, Applications or Stored data. The prime benefits of using public cloud is that the users are emancipated from performing certain important tasks on their computing machines that they cannot get away with otherwise, these include:Installation of resources, their configuration; and Storage.

Two BIG terms for cloud: 1) Disaster Recovery 2)Security

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

A. *Disaster Recovery*

Cloud Computing is an ideal solution for disaster recovery. As with any Disaster Recovery solution for a business we should have both an onsite and offsite backup. Even we can maintain redundant copies of data. Most of the companies that are providing Cloud Computing solutions, will in most cases have at least 3 data-center sites that are farmed out so the data is not 100% at one site location but instead mirrored to 2 other sites for redundancy and then those sites are individually backed up.

B. *Security*

Looking at the security issue related to cloud computing, the biggest question most have with Cloud Computing is will it be Safe? Unfortunately answer is "No". Reason why is everything that Cloud Computing is based on is mechanical, although it seems virtual. The Safety of the data is only as Safe as the will and determination of the individual that wants to have at it [1], [2], [3].

II.CLOUD SPECIFIC VULNERABILITIES

According to the Open Group's risk taxonomy, vulnerability is the probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force.Cloud computing causes significant changes in the vulnerability factor. Of course, moving to a cloud infrastructure might change the attackers' access level and motivation, as well as the effort and risk—a fact that must be considered as future work. But, for supporting a cloud-specific risk assessment, it seems most profitable to start by examining the exact nature of cloud-specific vulnerabilities.

A vulnerability is cloud specific if it

- — is intrinsic to or prevalent in a core cloud computing technology,
- — has its root cause in one of NIST's essential cloud characteristics,
- — is caused when cloud innovations make tried-and-tested security controls difficult or impossible to implement, or
- — is prevalent in established state-of-the-art cloud offerings.

We now examine each of these four indicators.

A. *Essential Cloud Characteristic Vulnerabilities*

NIST describes five essential cloud characteristics:on-demand self-service, ubiquitous network access, resource pooling, rapid elasticity, and measured service [3].

Following are examples of vulnerabilities with root causes in one or more of these characteristics:

- Unauthorized access to management interface.
- Internet protocol vulnerabilities.
- Data recovery vulnerability.
- Metering and billing evasion.

Thus, we can leverage NIST's well-founded definition of cloud computing in reasoning about cloud computing issues. The Prevalent Vulnerabilities is in State-of-the-Art Cloud Offerings. If a vulnerability prevalent in state-of-the-art cloud offerings, it must be regarded as cloud-specific. E.g. injection vulnerabilities, weak authentication schemes, command injection, cross-site scripting, etc.

III.ARCHITECTURAL COMPONENTS AND VULNERABILITIES

Cloud service models are commonly divided into SaaS, PaaS, and IaaS, and each model influences the vulnerabilities exhibited by a given cloud infrastructure [1]. It's helpful to add more structure to the service model stacks: Figure shows a cloud reference architecture that makes the most important security-relevant cloud components explicit and provides an abstract overview of cloud computing for security issue analysis. We map cloud-specific vulnerabilities to components of this reference architecture, which gives us an overview of which vulnerabilities might be relevant for a given cloud service[4].

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

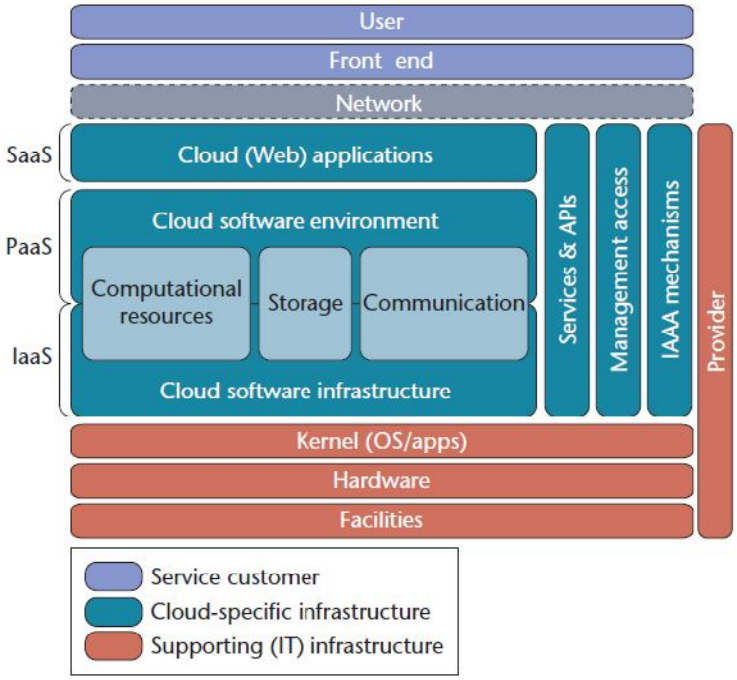

Fig.1. Cloud Reference Architecture

A. Cloud Software Infrastructure and Environment

The cloud software infrastructure layer provides an abstraction level for basic IT resources that are offered as services to higher layers: computational resources (usually VMEs), storage, and (network) communication. Theseservices can be used individually, as is typically the case with storage services, but they're often bundled such that servers are delivered with certain network connectivity and (often) access to storage. This bundle, with or without storage, is usually referred to as IaaS.

The cloud software environment layer provides services at the application platform level: a development and runtime environment for services and applications written in one or more supported languages; storage services (a database interface rather than file share); and communication infrastructure, such as Microsoft's Azure service bus [5].

Vulnerabilities in both the infrastructure and environment layers are usually specific to one of the three resource types provided by these two layers. However, cross-tenant access vulnerabilities are relevant for all three resource types.

B. Computational Resources

A highly relevant set of computational resource vulnerabilities concerns how virtual machine images are handled: the only feasible way of providing nearly identical server images—thus providing on-demand service for virtual servers—is by cloning template images.

Vulnerable virtual machine template images cause OS or application vulnerabilities to spread over many systemsData leakage by virtual machine replication is a vulnerability that's also rooted in the use of cloning for providing on-demand service. Cloning leads to data leakage problems regarding machine secrets: certain elements of an OS—such as host keys and cryptographic salt values—are meant to be private to a single host. Cloning can violate this privacy assumption. Again, the emerging marketplace for virtual machine images, as in Amazon EC2, leads to a related problem: users can provide template images for other users by turning a running image into a template. Depending on

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

how the image was used before creating a template from it, it could contain data that the user doesn't wish to make public.

C. Storage

In addition to data recovery vulnerability due to resource pooling and elasticity, there's a related control challenge in media sanitization, which is often hard or impossible to implement in a cloud context. Because cryptography is frequently used to overcome storage-related vulnerabilities, this core technology's vulnerabilities—insecure or obsolete cryptography and poor key management—play a special role for cloud storage.

D. Communication

The most prominent example of a cloud communications service is the networking provided for VMEs in an IaaS environment. Because of resource pooling, several customers are likely to share certain network infrastructure components: vulnerabilities of shared network infrastructure components, such as vulnerabilities in a DNS server, Dynamic Host Configuration Protocol, and IP protocol vulnerabilities, might enable network-based cross-tenant attacks in an IaaS infrastructure [2].

E. Cloud Web Applications

A Web application uses browser technology as the front end for user interaction. With the increased uptake of browser-based computing technologies such as JavaScript, Java, Flash, and Silverlight, a Web cloud application falls into two parts: an application component operated somewhere in the cloud, and a browser component running within the user's browser.

In the future, developers will increasingly use technologies such as Google Gears to permit offline usage of a Web application's browser component for use cases that don't require constant access to remote data.

F. Services and APIs

It might seem obvious that all layers of the cloud infrastructure offer services, but for examining cloud infrastructure security, it's worthwhile to explicitly think about all of the infrastructure's service and application programming interfaces. Most services are likely Web services, which share many vulnerabilities with Web applications. Indeed, the Web application layer might be realized completely by one or more Web services such that the application URL would only give the user a browser component. Thus the supporting services and API functions share many vulnerabilities with the Web applications layer [5].

G. Management Access

NIST's definition of cloud computing states that one of cloud services' central characteristics is that they can be rapidly provisioned and released with minimal management effort or service provider interaction.Consequently, a common element of each cloud service is a management interface—which leads directly to the vulnerability concerning unauthorized access to the management interface.

H. Identity, Authentication, Authorization, and Auditing Mechanisms

All cloud servicesrequire mechanisms for identity management, authentication, authorization, and auditing (IAAA). To a certain extent, parts of these mechanisms might be factored out as a stand-alone IAAA service to be used by other services. Two IAAA elements that must be part of each service implementation are execution of adequate authorization checks and cloud infrastructure auditing.

Most vulnerabilities associated with the IAAA component must be regarded as cloud-specific because they're prevalent in state-of-the-art cloud offerings. Example of weak user authentication mechanisms:

Denial of service by account lockout, Weak credential-reset mechanisms, Insufficient or faulty authorization checks, Coarse authorization control, Insufficient logging and monitoring possibilities.

I. Provider

Vulnerabilities that are relevant for all cloud computing components typically concern the provider—or rather users' inability to control cloud infrastructure as they do their own infrastructure. Among the control challenges are

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering,

Ahmednagar, Maharastra, India

insufficient security audit possibilities, and the fact that certification schemes and security metrics aren't adopted to cloud computing. Further, standard security controls regarding audit, certification, and continuous security monitoring can't be implemented effectively.

IV.CONCLUSION

Cloud computing is in constant development; as the field matures, additional cloud-specific vulnerabilities certainly will emerge, while others will become less of an issue. Using a precise definition of what constitutes a vulnerability and the four indicators of cloud-specific vulnerabilities we identify here offers a precision and clarity level often lacking in current discourse about cloud computing security.

Control challenges typically highlight situations inwhich otherwise successful security controls are ineffective in a cloud setting. Thus, these challenges are of special interest for further cloud computing security research. Indeed, many current efforts—such as the development of security metrics and certification schemes, and the move toward full-featured virtualized network components—directly address control challenges by enabling the use of such tried-and-tested controls for cloud computing.

Above paper discusses the different vulnerability issues related to cloud computing. Despite of the different security constrains imposed by the service provider of the cloud, the author wants to put some basic suggestions here: always store the data in encrypted form only. Also you can put some your own integrity constraints to your data.

REFERENCES

1] George Reese, *Cloud Application Architecture Building Application and Infrastructure in the Cloud,* 1ST ed., O'REILLY Publications, 2010.
2] Anthony T. Velte, Cloud Computing a Practical Approach, 1st ed., Tata Mcgraw Hill Publications, 2009.
3] Bernd Grobauer, Tobias Walloschek, and ElmarStöcker, "Understanding Cloud Computing Vulnerabilities", copublished by the IEEE Computer and Reliability Societies 1540-7993/2011 IEEE March/April 2011.
4] KwangMongSim, "Agent-Based Cloud Computing", in IEEE Transactions on Services Computing, Vol. 5, No. 4, October-December 2012.
5] QiangDuan, Yuhong Yan, and Athanasios V. Vasilakos, "A Survey on Service-OrientedNetwork Virtualization Toward Convergence ofNetworking and Cloud Computing", IEEE Transactions on Network and Service Management, Vol. 9, No. 4, December 2012.