Impact of database security in Cloud Computing

J.Srinivasan
Assistant Professor,(CSE)
Adhiparasakthi College Of Arts & Science
Kalavai,Vellore-632506
srikeerthana2003@gmail.com

D.Ranjith
MPhil-Research Scholar (CSE)
Adhiparasakthi College of Arts & Science ,
Kalavai,Vellore-632506
ranjithdesigan@gmail.com

ABSTRACT

The aim of this paper is to get an overview of the database services available in cloud computing environment, analyses the security risks combination and propose the possible counter measures to minimize the risks. And also analyzes the cloud database service providers namely; Amazon and Xeround, RackSpace2. The reason behind choosing these are providers is because they are currently amongst the leading cloud database providers the relational cloud databases which make the separation. The focus that examines has been to provide an overview of their database services as well as the available security measurements. It has been appended at the end of the report to help with technical configurations of database migration and connecting applications to the databases for the mentioned cloud database providers.

Keywords

Amazon, Xeround, RackSapce2, Cloud Computing, Cloud Database Service, Security risks

1. INTRODUCTION

What are the security risks present for implementing a database system in the cloud? What can be done to improve the confidentiality, integrity and availability of a database system in the cloud? This paper intends to answer these questions by analyzing the security risks present for a database system in the cloud and the counter measures that eliminates or at least mitigates these risks.

2. METHODOLOGY

The different cloud-based sequence models, along private, public or hybrid cloud, carry with them a extent of challenges, and security responsibilities to all. The cloud service model that an organization wants to implement influences security design and implementation. We will discuss about this three cloud computing service models. The Models are DAAS-Data as a Service, IAAS- Infrastructure as a Service and NAAS-Network as a Service.

3. Cloud Computing service Delivery Models

The three main-cloud service delivery models are: Data as a Service (DaaS), Infrastructure as a Service (IaaS) and Network as a Service (NaaS).

3.1 Data as a Service

It is a cousin of software as a service [1]. DaaS is based on the idea that the product, data in this case, can be determining on demand [2] to the user regardless of geographic or organizational separation of provider and consumer. Additionally, the appearance of service-oriented architecture has rendered the actual platform on which the data resides also irrelevant [3]. This growth has enabled the recent emergence of the relatively new concept of DaaS. Data provided as a service was at first primarily used in web mashups, but now is living increasingly employed both commercially and, lesser commonly, within organizations like as the UN [4].

Traditionally, most enterprises have used data stored in a self-hold repository, for which software was specifically established to access and present the data in a human-readable form. One result of this paradigm is the gathering of both the data and the software needed to interpret it into only one package, sold as a consumer product. As the number of bundled software/data packages proliferated and required interaction among each other, another layer of interface was mandatory. These interfaces, altogether known as enterprise application integration, often tended to encourage vendor lock-in, as it is usually simple to integrate applications that are built upon the same foundation technology [5].

The result of the combined software/data consumer package and required EAI middleware has been an increased amount of software for organizations to manage and maintain easily for the use of particular data. In addition to normal costs, a

cascading amount of software updates are required as the format of the data changes. The reality of this situation contributes to the attractiveness of DaaS to data consumers because it allows for the separation of data cost and usage from that of a specific.

3.2 Infrastructure as a Service

This is the base layer of the cloud stack. Its work for a foundation for the another two layers, for their execution. The keyword after this stack is Virtualization**.** Amazon Elastic Compute is a good example of an IaaS. In Amazon Elastic Compute Cloud your application will be executed on a virtual computer it may also called as instance. You have your choice of virtual computer, definition that you can select a configuration of CPU, memory and storage that is optimum for your application. The IaaS supplies the whole cloud infrastructure i.e.:. hardware (loading items), switches,router,servers, firewalls, storage and other network equipment. The consumer buys these resources for his needed basis. One more feature I liked about Amazon Elastic Compute, which is perhaps supplies by other IaaS providers as well, is Elastic Load Balancing. This attribute can auto-deliver an application's incoming traffic across multiple Amazon EC2 instances (virtual computers).The Amazon EC2 SLA (Service Level Agreement) guarantees 99.95% availability of the service within a region over a trailing 365 day period.

3.3 Network as a Service

To design for open stack. This will be another big break through in terms of virtualizing the network infrastructure in the cloud. The key features consist of compute for interconnecting two VM instances to different virtual networks, network services insertion and request "adaptive" network resources. Open Stack: NaaS will contribute network resources required to interconnect Open Stack zones and network resources required to support new services like virtual private cloud. According to Seeking[8] Alpha and offering Cisco, there are still various open questions to compare, but in the future, this Network as a Service would be elaborate to hold SLA, Network level QoS and other network based auditing/analyzing services, beyond assign services like interconnecting two VM instances or providing resources required to interconnect Open Stack "Zones" or geographically dispersed computer/storage resources.[9].

4. CLOUD DEPLOYMENTS MODELS

Cloud computing is composed of four deployment models, namely: private cloud, public cloud, community cloud, and hybrid cloud as discussed briefly below

4.1 Private cloud

In a private cloud model, the infrastructure is provisioned for exclusive use by a single organization. [3] The underlying infrastructure can be on or off premise and the management and operational tasks can be carried by the organization itself, a cloud service provider or a combination of both. Private clouds are the only option when it comes to protecting highly sensitive data.

4.2 Public cloud

In public cloud model, the cloud infrastructure is available for open use by everyone including general public or a large industry groups. [11] The entire underlying infrastructure is built and managed by the cloud provider and the consumers only require internet access in order to utilize the available services. Public clouds are not very secure and as a result they are not recommended to be used for any type of sensitive data at all.

4.3 Community cloud

In community cloud model, the cloud infrastructure is used exclusively by a community of users that have the same requirements and concerns (security needs, law compliance and policy considerations). The underlying infrastructure can be managed and owned jointly by the members of the community or a cloud provider can be chosen for the management and operational tasks. This model has the security benefits similar to private cloud but is more cost efficient than owning an on-premise private cloud.

4.4 Hybrid cloud

A hybrid cloud is formed when two or more distinct cloud infrastructures are used together. For example when a private cloud and community cloud is used together, or when public and private cloud infrastructures are used together then the solution is known as the hybrid cloud. Hybrid clouds are usually used when there are different security requirements for different sets of data. For instance, highly sensitive data can be kept in a private cloud while less sensitive data can be uploaded to a public cloud.

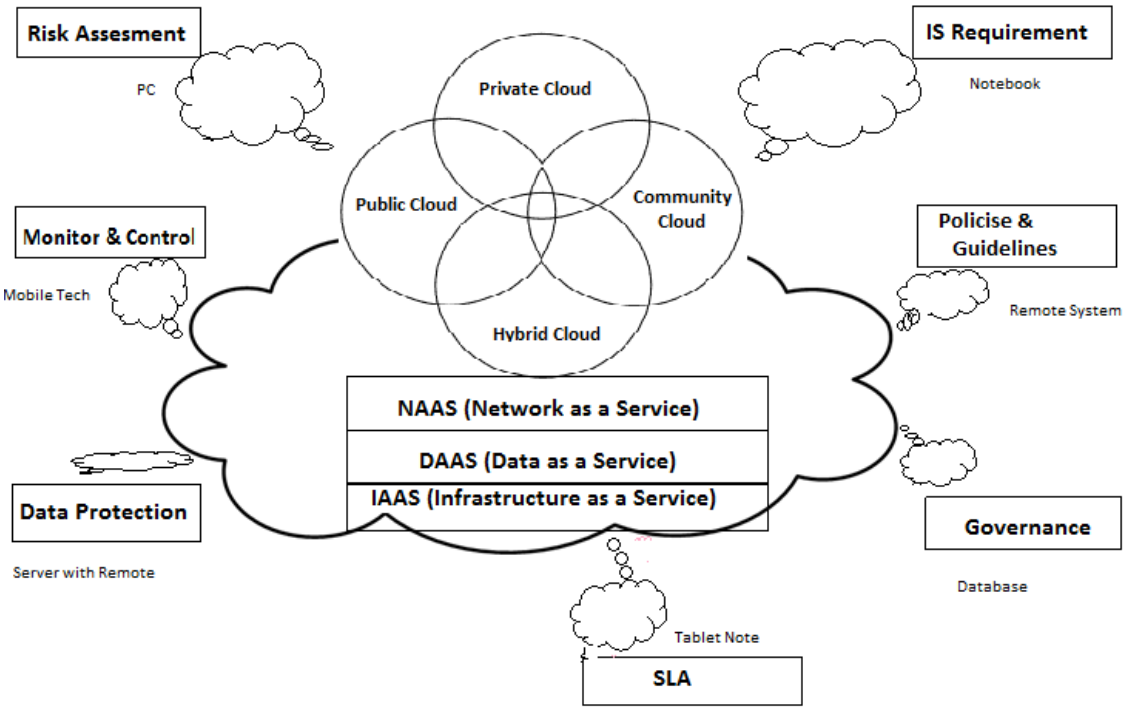

Fig 1: Cloud Deploy Models

5. CLOUD COMPUTING ADVANTAGES

Cloud computing proposes numerous advantages to both individuals and organizations. The main advantages and driving factors behind cloud computing is the fact that it is economically very favorable. It allows consumers to access a huge range of applications and services without downloading or installing anything. The underlying infrastructure and network is managed and operated by an external provider, and the consumers get rid of maintaining servers, training IT employees as well as purchasing software licenses which results in an overall minimization of monetary costs in training, power consumption, infrastructure maintenance and storage space. Thus users will be able to access data wherever they are without being dependent to a specific location. Cloud computing is also considered quite safe in terms of redundancy.

5.1 Services of Cloud

The services are now offering a new service besides the traditional services (DaaS, IaaS and Naas) known as Database as a service which is essentially an on-demand database accessible to the consumers from the cloud over the Internet. In the multi-instance model each consumer is provisioned with a unique DBMS running on a dedicated virtual machine belonging only to a specific customer. This feature enables consumers to have better control over administrative and other security related tasks such as role definition and user authorization. On the other hand, the multi-tenant model uses a tagging method and provides a predefined database environment that is shared by many consumers.

5.2 Security Issue

Volatide databases into cloud environment brings a number of security concerns that organizations have to take into consideration as the ultimate responsibility for data security assurance is with organizations and not with providers. When internal databases with sensitive data are migrated to the cloud, users need to be assured that proper database security measurements are in place that encompasses data confidentiality, integrity, and availability. The main aspects of database security in the cloud are that data must be secured during at rest, in transit, and in use, and access to the data must be controlled

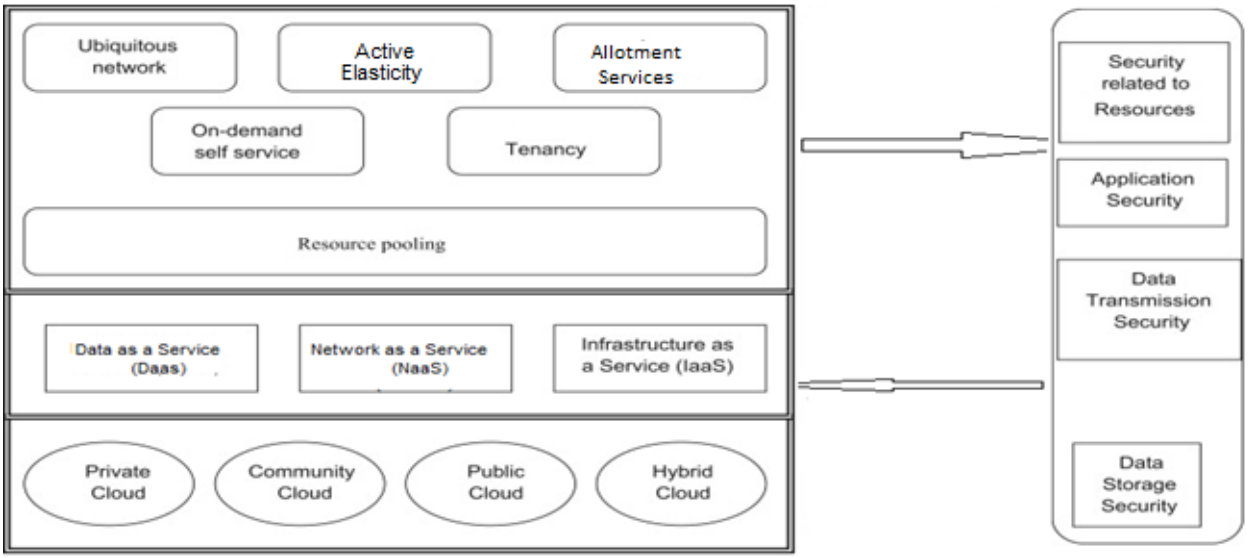

Fig: 2 Cloud Architecture for Data Storage Security

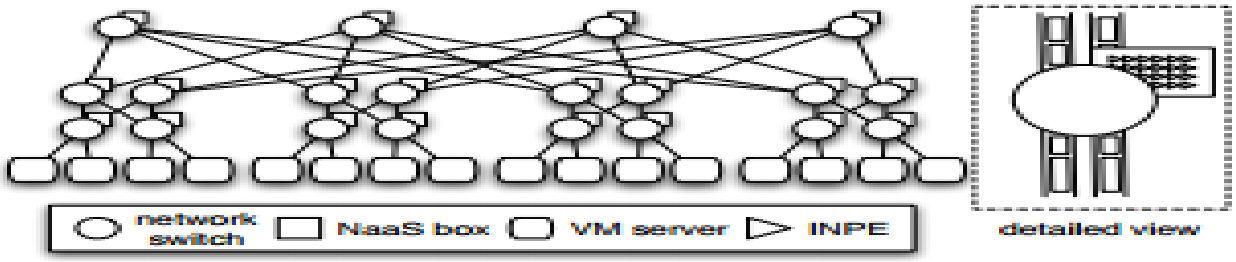

Fig 3: NAAS Architecture

6. OVER COME MODELS OF SECURITY THREATS

The chief concern in cloud environments is to provide security around multi-tenancy and isolation, giving customers more comfort besides "trust us" ideas of clouds. there has been survey works reported that classifies security threats in cloud based on the nature of the service delivery models of cloud computing system. The identified threats and countermeasures are:

- Failures in Provider Security
- Attacks by other Consumer
- Accessibility and Authenticity Issues
- Authorization and Regulatory Issues
- Consumer Security Systems which Interacting the provider

6.1 Failure in Provider Security

The overcome threats that Provider controls the networks & Servers, etc. Consumer should trust provider's security, Failures may Corrupt CIA principles. The Countermeasures are Check and monitor the provider's security and External verification may suffice for SMB, provider security may exceed customer security.

6.2 Attacks by other Customers

The overcome threats are Provider the resources shared with untreated parties the Examples is CPU, storage, network. Consumer's data and applications should be separated. Failures will violate CIA principles. The Countermeasures are Hypervisors for compute separation MPLS, VPNs, VLANs, firewalls for network separation Cryptography and Application layer scattered.

6.3 Availability and Reliability Issues

The Overcome threats are Complexity increases chance of failure, Clouds are prominent attack targets, and Internet reliability is spotty. Gathered the resources may provide attack vectors but cloud provides focus on availability. The Countermeasures are Evaluate provider measure to make secured the availability, Monitor availability carefully Plan for downtime use public clouds for less fundamental applications.

6.4 Legal and Regulatory Issues

The Overcome threats are Laws and regulations will prevent cloud computing, Requirements to retain control Certification requirements that not met by the provider. The Countermeasures are evaluate legal issues and requires provider compliance with laws and regulations, Restrict geography as needed.

6.5 Integrating Provider and Customer Security Systems

The Overcome threats are Divide the provider and consumer security systems, Fired employees retains access to cloud is behavior in cloud not reported to customer. The Countermeasures is at least, integrate analyze the management consistent access control and worthier the integrate monitoring and notifications

7. CONCLUSION & FUTURE WORK

In an emerging discipline, like cloud computing, security needs to be analyzed more frequently. With advancement in cloud technologies and increasing number of cloud users, data security dimensions will continuously increase. Optimal cloud security practices should include encryption of sensitive data used by cloud-based virtual machines, centralized key management that allows the user (and not the cloud provider) to control cloud data; and ensuring that cloud data is accessible according to established enterprise policies.

To address the security threats and issues relevant to cloud computing and virtualization, this paper outlines recommended security best practices in virtual and cloud environments. For virtualized environments, private cloud, portions of hybrid clouds, and public Infrastructures as a service (IaaS) deployments, the enterprise, not the service provider, needs to assume responsibility for security.

8. ACKNOWLEGEMENT

At this moment I take the opportunity to thank my parents and my dear friends who provided me full support, and encouraged me to complete the work.

9. REFERENCE

[1] Buyya Rajkumar, Broberg James & Goscinski, , 2011 *Cloud Computing Principles and Paradigms*, John Wiley & Sons, Inc., Hoboken, New Jersey USA ISBN: 978 0 470 88799 8

[2] NIST, *the NIST definition of cloud computing*, September2012,http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf,

[3] Cloud Security Alliance, 2011 *Security guidance for critical areas of focus in cloud computing V3.0*, ,

[4] Danielson, Krissi (2008-03-26) 2010 august. "Distinguishing Cloud Computing from Utility Computing". Retrieved.

[5]. Keep an eye on cloud computing, Amy Schurr, Network World, 2008-07-08, ,Sep 2009citing the Gartner report, "Cloud Computing Confusion Leads to Opportunity". Retrieved

[6]. B. Rochwerger, J. Caceres, R.S. Montero, D. Breitgand, E. Elmroth, A. Galis, E. Levy, I.M. Llorente, K. Nagin, Y. Wolfsthal, E. Elmroth, J. Caceres, M. Ben-Yehuda, W. Emmerich, F. Galan.2009 "The RESERVOIR Model and Architecture for Open Federated Cloud Computing", IBM Journal of Research and Development, Vol. 53, No. 4

[7]. IEEE International Conference on Cloud Computing (CLOUD).Thecloudcomputing.org. http://www.thecloudcomputing.org. Retrieved 2010-08-22.

[8]. WETHERALL, D.1999 Active Network Vision and Reality: Lessons from a Capsule-Based System. In SOSP

[9].YU, Y., GUNDA, P. K., AND ISARD, M. Distributed Aggregation for Data-Parallel Computing: 2009 Interfaces and Implementations. In SOSP.