Volume 2, Issue 10, October 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Issues and Security Algorithms in Cloud Computing

K.S.Suresh M.Tech[#1]
Asst. Professor
Department of CSE, MLRIT
Dundigal, Hyderabad, A.P

Prof K.V.Prasad [#2]
Principal
Gayatri institute of Engineering and Technology
JangareddyGudem, A.P.

ABSTRACT: Cloud Computing is the use of activity of using Computer hardware and software. Cloud Computing is a set of IT Services that are provided to a customer over a network and these services are delivered by third party provider who owns the infrastructure. It is often provided "as a service" over the Internet, typically in the form of infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS).This paper describes about the different security algorithms , security issues and security attacks in cloud computing.

Keywords: Cloud computing, Infrastructure, Service, Security Attacks, Security Algorithms.

1. INTRODUCTION

Cloud computing is a technology that keep up data and its application by using internet and central remote servers [1]. Cloud computing can be considered a new computing paradigm with implications for greater flexibility and availability at lower cost. Because of this, cloud computing has been receiving a good deal of attention lately. The four deployment models operated by cloud computing are the: Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud as shown in Fig 1.Each model has its own features and especial characteristics that suits to the cloud users' particular reasons in embracing cloud computing.

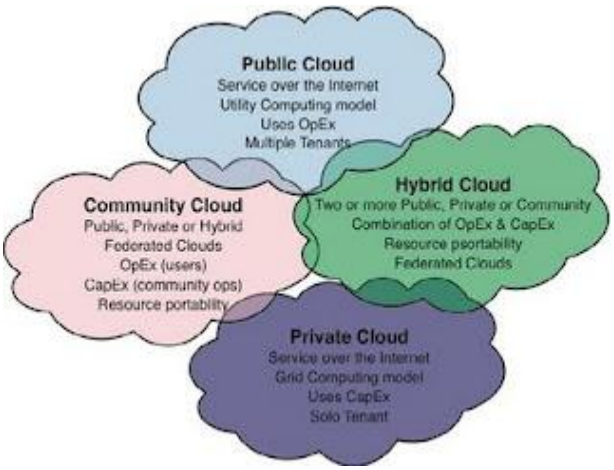

Fig :1Deployment models operated by CloudComputing

Private cloud -- The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud -- The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud -- The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services and the comparison of private and public cloud as shown in fig2.

Hybrid cloud -- The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

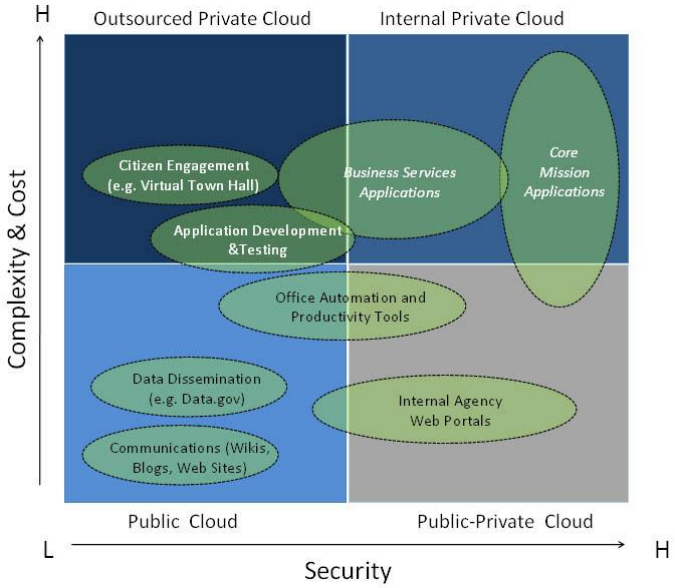

Fig 2 :Comparision of Security and complexity between Private and Public cloud.

2. Security issues associated with the cloud

There are number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS) via the cloud) and security issues faced by their customers[2] .In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information[3].

2.1 Security issues faced by cloud providers

2.1.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

Characteristics and components of IaaS include:

Utility computing service and billing model.
Automation of administrative tasks.
Dynamic scaling.
Desktop virtualization.
Policy-based services.
Internet connectivity.

2.1.2 Platform as a Service (PaaS)

Platform as a Service (PaaS) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Platform as a Service (PaaS) is an outgrowth of Software as a Service (SaaS), a software distribution model in which hosted software applications are made available to customers over the Internet. PaaS has several advantages for developers. With PaaS, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than

maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts.

2.1.3 Software as a Service (SaaS)

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support Web services and service-oriented architecture (SOA) mature and new developmental approaches, such as Ajax, become popular. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world.SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for SaaS. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for SaaS distribution.

Benefits of the SaaS model include:
easier administration
automatic updates and patch management
compatibility: All users will have the same version of software.
easier collaboration, for the same reason
global accessibility.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service[4]. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured[5]. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist[6].

Dimensions of cloud security

Correct security controls should be implemented according to asset, threat, and vulnerability risk assessment matrices[7]. While cloud security concerns can be grouped into any number of dimensions (Gartner names seven[8] while the Cloud Security Alliance identifies fourteen areas of concern[9]) these dimensions have been aggregated into three general areas: Security and Privacy, Compliance, and Legal or Contractual Issues[10].

3. Security Concerns

1. **Data?** The main thing that is where the data is because the data is in cloud so the cloud provider should agree to provide security to the data of our customers.
2. **Access**? And second thing that who has access to the data that is at cloud. If anyone using the cloud needs to look at who is managing their data and what types of controls are applied.
3. **Training to Employees?** Train the employees because the employees need to know how to access the data maintaining security.
4. **Data Classification?** Because there is data of different user so the question is “Is Data Classified”
5 **service level agreement (SLA) ?** The SLA serves as a contracted level of guaranteed
service between the cloud provider and the customer that specifies what level of services will be provided.
6. **What happens if there is a security breach?** If a security incident occurs, what support will you receive from the cloud provider? While many providers promote their services as being unhackable, cloudbased services are an attractive target to hackers.

4. SecurityAlgorithms

RSA- is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission.
MD5- (Message-Digest algorithm 5), a widely used cryptographic hash function with a 128-bit hash value, processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks . the message is padded so that its length is divisible by 512.

In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message.

AES- In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively [11].

AES algorithm ensures that the hash code is encrypted in a highly secure manner. AES has a fixed block size of 128 bits and uses a key size of 128 in this paper. Its algorithm is as follows:

1. Key Expansion
2. Initial Round
3. Add Round Key
4. Rounds
5. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
6. Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
7. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column
8. Add Round Key—each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
9. Final Round (no Mix Columns)
10. Sub Bytes
11. Shift Rows
12. Add Round Key

Encryption- converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plain text .

Security Attacks

cloud computing systems are providing awide variety of services and interfaces to enable vendors to rent out spaces on their physical machines at an hourly rate for a tidy profit.

Threats

Extortionists : Using DDoS attack to exhaust server resources
Competitors : Using known vulnerabilities to interrupt services

Distributed Denial of Service (DDoS) attack, which means many nodes systems attacking one node allat the same time with a flood of messages

The DDos Attack Tools

Complex: Agobot,Mstream,Trinoo
Simple: Extensible Markup Language (XML) based Denial of Service (X-DoS)
Hypertext Transfer Protocol (HTTP) based Denial of Service (H-DoS)

X-DoS:

Coercive Parsing attack
Open xml tags
Exhaust CPU usage

H-DoS:

Using HTTP Flooder

starts up 1500 threads
send randomized HTTP requests to the victim web server
exhaust victim's communication channels

Cloud TraceBack, CTB

service-oriented traceback architecture
to defend against X-DoS attacks the area of cloud computing.

H-DoS attack

affected Iran
using the attack as an example of bringing down a cloud system
train our back propagation neural network called Cloud Protector

Cloud Protector

Backpropagationneuralnetwork

5. Conclusion

Cloud computing is revolutionizing how information technology resources and services are used and managed, but the revolution always comes with new problem

In the future, we will extend our research by providing implementations and producing results to justify our concepts of security for cloud computing.

References

[1] Priyanka Arora, Arun Singh, Himanshu Tyagi "Analysis of performance by using security algorithm on cloud network" in international conference on Emerging trends in engineering and management (ICETM2012), 23-24 june, 2012.

[2] ""Swamp Computing" a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25.

[3]""Thunderclouds: Managing SOA-Cloud Risk", Philip Wik". Service Technology Magazine. 2011-10. Retrieved 2011-21-21.

[4] Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concerns". Technet Magazine, Microsoft. Retrieved 12 February 2012.

[5] Hickey, Kathleen. "Dark Cloud: Study finds security risks in virtualization". Government Security News. Retrieved 12 February 2012.

[6]Winkler, Vic (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham, MA USA: Elsevier. pp. 59. ISBN Securing the Cloud Cloud Computer Security Techniques and Tactics.

[7] "4 Cloud Computing Security Policies You Must Know". CloudComputingSec. 2011. Retrieved 2011-12-13.

[8] "Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07-02. Retrieved 2010-01-25.

[9] "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. 2011. Retrieved 2011-05-04.

[10] "Cloud Security Front and Center". Forrester Research. 2009-11-18. Retrieved 2010-01-25.

[11] M. Sudha , Dr.Bandaru Rama Krishna Rao , M. Monica "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment," in International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010.

