Security issues and challenges in cloud

K.Surya, M.Nivedithaa, S.Uma, C.Valliyammai,
Department of Computer Technology,
Madras Institute of Technology,
Chennai, India.

Abstract- **Cloud computing is emerging as a rapid growing technology in the IT industry. As a large amount of information on individuals and companies are placed in cloud, there is an ultimate need to ensure the safety of the cloud environment. The main issues concerned with cloud are security, privacy, reliability, legal issues, open standard, compliance, freedom, long term viability etc. The various security issues associated with cloud computing include privileged access, regulatory compliance, data location, data segregation, recovery, investigative support, data availability. The main requirements to ensure security in cloud are authorizing and authenticating users, data confidentiality, non-repudiation, availability. In this paper, security issues and challenges in various types and layers of cloud are discussed.**

Keywords- Cloud computing; Infrastructure as a Service (IaaS; Software as a service (SaaS); Platform as a Service (PaaS).

I. SECURITY ISSUES IN VARIOUS TYPES OF CLOUD

A. Private Cloud:

The private cloud is made accessible only by a specified customer and it is managed either by the organization or a third party service provider. Private cloud maximizes and optimizes the utilization of existing-in house resources. It is chosen as there are lesser security concerns over data privacy and data transfer. Only authorized persons within the organization has access to the private cloud and the data stored in it.

B. Public Cloud:

A public cloud is one in which the service providers makes the resources such as data storage centers, server, network devices etc. available to the public users over the internet [5].

The shared multi-client feature of public clouds adds security risks such as unauthorized access of data by other clients using the same hardware. Also, because the environment is shared by multiple users, resource contention issues arises whenever one of the users using the hardware consumes a large amount of resources either due to need or due to attacks. The data stored in a public cloud is at risk if it is not encrypted or if proper access control mechanisms are not used. Also, when data is moved or deleted by provider or user, the data remains may be exposed to unauthorized users.

In a public cloud model, infrastructure security is provided by the Cloud Service Provider (CSP). The CSP must have strong security and be clear regarding security issues and procedures for solving them. However, the CSP should also not be fully trusted. The security status of the CSP should be periodically checked.

In order to ensure security of data in public cloud, all the network traffic must be encrypted. The data stored in the cloud must also be encrypted by the owner or the service provider. A monitoring and logging process must be enforced to validate the security status of the vendor.

C. Hybrid Cloud:

Hybrid Cloud [1] is a private or public cloud which is linked to other deployment models such that the data transfer between these doesn't affect each other and these models are centrally managed and restricted by a secure network. Infrastructure of this deployment model is managed by both the organization and third party provider [3]. Hence it is trusted as well as untrusted.

A lack of data redundancy can cause serious effects mainly when it is stored in a single data center. To solve this, redundant copies of data are distributed among different data centers. Maintaining compliance is difficult with hybrid cloud. Data moving between clouds should be protected. The public cloud provider can meet expectations detailed in service-level agreement (SLA) but not the private cloud. Hybrid cloud is a complex system where the

978-1-4673-6126-2/13/$31.00

administrators have limited experience in managing risks and that creates risk. Security controls such as authorization, authentication and identity management should be implemented in both public cloud provider and private cloud.

The major concern in hybrid cloud is violation of confidentiality and integrity of data [7]. A company's information or data stored in cloud can be exposed intentionally or accidentally. Such actions result in damage to goodwill or financial status of a company. Encryption is a most popular technique for addressing the threats based on confidentiality and integrity issues. Companies need to encrypt their data and communications in order to protect themselves from malicious attackers present in the internet. All the data present in the cloud will be in encrypted format and it requires key from the corresponding companies to decrypt the data.

II. SECURITY ISSUES IN DIFFERENT LAYERS OF CLOUD

A. Hardware Layer:

Hardware layer is the server layer. It represents the physical hardware that constitutes the cloud. Generally, cloud providers do not tell about the physical devices used to provide services. Hardware resources are quite expensive and are not fault tolerant. Also, a large number of attacks can be done on the server by malicious users which cause serious problems such as data loss etc. The various attacks are described below.

a) Denial of Service Attacks:

A DoS attack denies occurs when a user sends too many invalid requests to the server. It occurs when the service is flooded by large number of requests. This can be overcome by having an Intrusion Detection System (IDS) [12]. Each cloud has an IDS. When a specific cloud gets attacked, the co-operative IDS alert all the systems. By the mechanism of voting, a decision is made such that the performance is not tampered with.

b) Cookie Poisoning:

It occurs when the contents of cookie is modified to gain unauthorized access to an application or a web page. It can be prevented from happening by having regular cleaning up of cookies and encrypting the cookie data.

c) Distributed Denial of Service Attacks:

DDoS is an enhanced version of DoS. It happens in a distributed environment. In this case, the amount of data that is made accessible by the public is under the sole control of the attacker [12]. It can be avoided by having an extensive modification of the underlying network. But these modifications are costly. A logic based on providing a transparent transport layer was proposed by [13] through which protocols such as HTTP, SMTP can penetrate. Another method is to have an IDS.

B. Virtualization Layer

The most common way to cause problems to a virtualized cloud is to attack a hypervisor, who monitors and controls all the virtual machines running on cloud. Attacks on hypervisor can be done through guest OS or host OS. Other attacks on hypervisor include virtual library checkout, migration attack and encryption attack.

a) Virtual Library Checkout:

A large company houses many virtual servers in its data center. This virtual library of servers consists of all the virtual machines (VMs) controlled by the company. Periodically, the workers or employees of the company make use the images of the VMs to do software upgrades and maintenance on their own machines. Since the worker' machines are not as secure as the company's data center, attackers could use one of the VMs on a worker machine and plant a malicious item in the VM image. When the worker puts the VM back into the company's data center, the malicious item migrates into the data center, helping the attacker access all the resources in the data center.

b) Migration Attack:

It is the attack on the network when a virtual machine is migrated from one location to another. Companies move virtual machines to various locations based on their use. The attackers can make use of the network vulnerability to access the virtual machines.

c) Encryption Attack:

It is an attack to extract unauthorized information from virtual machines by making use of the security problems in the virtualization software. It can be done by gaining session keys during virtual machine transfer. This attack is complex and generally not done.

C. Infrastructure Layer

Infrastructure of cloud includes servers, software, data-center space, network equipment, etc. An infrastructure provided as a service indicates the sharing of physical resources among many users [4]. The infrastructure or the resources can easily be

increased or replicated depending on the demand from the user who is charged based on their consumption.

With Infrastructure as a Service (IaaS), a user or developer has better control over the security as long as there is no problem with the virtualization manager [3]. A common problem with IaaS is that the reliability of the data stored in the hardware must be ensured. The owner must have full control over the data stored irrespective of its physical location. In a cloud offering IaaS, the service providers have to address physical, environmental and virtualization security while the consumers have to address the security controls related to operating systems, applications and data.

IaaS has many components. Integrating these components to make it work in a shared environment is itself a major challenge. Security issues associated with each and every component must be addressed. The various components are Service Legal Agreement (SLA), utility computing, Cloud software and platform virtualization.

Software Legal Agreement is like a bond between the client and the provider. SLA is the solution for guaranteeing quality of service in cloud. Web Service Legal Agreement (WSLA) was developed where the SLA tasks were handed over to a third party. Clients have to trust the provider's WSLA framework.

Utility computing bundles the resources such as storage, network equipment, etc. as payable services and hands it over to the clients. It reduces the total cost and also supports scalability in terms of users or resources. One main challenge is to manage the utility of the resources. For example, the second level providers may use the resources of higher level providers. So there can be multiple levels of utility. Second challenge is to resist the attackers who try to use the services without paying accordingly. Both the provider and user have to cooperate in order to avoid such attackers.

Web Service security is a standard security extension in SOAP. It defines a security header which determines how XML signature and encryption are applied to messages. The client's browser must be a security enhanced one.

Virtualization techniques must be applied so that none could access others' disks, memory, or applications in the same host. Strong isolation must be maintained. A compulsory access control mechanism must be maintained from a client's side along with optional encryption of data. Solutions from a provider's side may include establishing a Virtual Private Network, applying encryption techniques, designing proper techniques for virtual machine management. Computer hardware must also be protected by storing it in highly secured locked rooms with monitoring appliances. Other solutions include managing multi-party accessibility to encrypted data, creating transparent cryptographic file systems and using a self-encrypting enterprise tape.

A security model for IaaS (SMI) has been proposed [2]. It consists of three sides- the IaaS components, security model, restriction level. The security model side has three entities- Secure Configuration policy (SCP) for each layer, Secure Resources Management Policy (SRMP) that controls management policies and Security Policy Monitoring and Auditing (SPMA) which monitors the system. The restriction policy indicates the level of restriction of the security models. The restriction varies from loose to tight depending on the provider and clients.

D. Platform Layer:

Here, the cloud providers deliver platforms, tools and other business services that enables customer to develop, deploy and manage their own application without installing any platform or tools in their local machine [8].

SOA related security issues – The PaaS model inherits the properties of Service-oriented Architecture (SOA). This means that the security issues are common for both SOA and PaaS. These includes DoS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks [9, 10]. The solution for the above issues may be Mutual authentication, authorization and WS-Security standards.

API Security –PaaS offers APIs like business functions, security function, application functions, etc. These functions come under the deliver management functions. These APIs need to be enforced with security standards like OAuth [11], to have authentication and authorization consistent over the calls made to the APIs.

E. Software Layer:

In SaaS (Software as a Service) model [6], software is delivered or offered to customers as a service. Here data is stored outside enterprise at SaaS end. SaaS is a software application delivery model in which companies provides their application over the internet so that customers can access it. One benefit of this model is customers do not need to buy any

software licenses or any additional equipment for hosting the application but they pay for using the software application.

In SaaS, the client has to rely on the service provider for security related issues. SaaS vendor should check to ensure data security [3] and to prevent security breaches. This is done by using strong encryption techniques and fine-grained authorization control to access data. In cloud vendors such as Amazon, EC2, they use cryptographically strong Secure Shell (SSH) keys to gain access to data. Assessments like Cross-site scripting[XSS], Access control weaknesses, OS and SQL injection flaws, Cross-site request forgery[CSRF], Cookie manipulation, Hidden field manipulation, Insecure storage, Insecure configuration are used to validate and test data security.

Since all critical data are transferred over network, strong encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) are used for security. Assessments like Network penetration and packet analysis, Session management weaknesses, SSL trust configuration are used to test and validate the network security of SaaS vendor. SaaS model should provide reliability in terms of location of the data.

Data of different users may be stored in same location. Data of one user should not affect data of other user. Sometimes it may happen either by hacking or inserting a client code into SaaS. So the data of different users must be segregated at physical and application level. Assessments such as SQL injection flaws, Data validation, and insecure storage are used to test and validate data segregation of SaaS vendor.

Only Authenticated users are allowed to access data to which they have authorized access. SaaS vendor should backup sensitive information and should also encrypt them strongly to avoid leakage of sensitive information accidentally.

F. Network Layer:

a) DNS attack:

Sometimes, when a server is called by its name, the user is taken to some other cloud which might be evil. DNSSEC (Domain Name System Security Extensions) can reduce the effect of DNS attack.

b) Sniffer attack:

Sometimes, when a packet which is not encrypted goes over a network, it can be illegally read by unauthorized user. A sniffer program, through the NIC (Network interface Card), can be used to track all the data flowing in the network [12].

c) Issue of Reusing IP addresses:

As a user moves out of the network, the IP associated with the user gets assigned to some other user. But there is a time lag between these changes of IP address. During this time, with the IP in the DNS cache there is a chance to access the data of the original user.

III. CONCLUSION

Cloud computing is an emerging technology for the IT industries and Internet world with its great advantages and practical limitations. In this paper, we discussed the need for security in cloud and also the various issues and challenges in all layers of cloud technology. Typical secure cloud infrastructure is under research and the various solutions for providing integrated security model should come up to increase the potential users of the cloud.

IV. REFERNCES

[1] Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing", in Information Security for South Africa (ISSA), 2010.

[2] Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja, "Cloud Computing Security Issues in Infrastructure as a Service", in the International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 1, 2012.

[3] S. Subashini, V.Kavitha, "A survey on security issues in service delivery models of cloud computing", in the Journal of Network and Computer Applications, pp 1-11, Vol.34, No.1, 2011.

[4] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, Sugata Sanyal, "A Survey on Security Issues in Cloud Computing", 2011, http://arxiv.org/abs/1109.5388.

[5] Mohamed Al Morsy, John Grundy and Ingo Müller, "An Analysis of The Cloud Computing Security Problem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 2010.

[6] Tharam Dillon , Chen Wu and Elizabeth Chang, "Cloud Computing Issues and Challenges", in AMCHAM, 2012.

[7] Koushik Annapu reddy, "Security Challenges in Hybrid Cloud Infrastructures", in Seminar on Network Security, 2010.

[8] Mohamed Al Morsy, John Grundy and Ingo Müller, "An Analysis of The Cloud Computing Security Problem", in Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 2010.

[9] Meiko Jensen, JörgSchwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing". in IEEE ICCC, 2009, pp. 109-116.

[10] Z. Wenjun, "Integrated Security Framework for Secure Web Services", in IITSI 2010, pp. 178-183.

[11] B. Wang, Huang He, Yuan, Liu Xiao, Xi, Xu Jing, Min, "Open Identity Management Framework for SaaS Ecosystem", in ICEBE, 2009, pp. 512-517.

[12] R.Bhadauria, R.Chaki, N.Chaki, S.Sanyal, "A Survey on Security Issues in Cloud Computing", in arXiv, 2011.

[13] RuipingLua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network", IEEE Network, Vol. 25, No. 4, pp. 28-33, July-August, 2011.

[14] Sarvesh Kumar, Jahangeer Ali, Ashish Bhagat, Jinendran P.K "An Approach of Creating a Private Cloud for Universities and Security Issues in Private Cloud", in International Journal of Advanced Computing, ISSN:2051-0845, Vol.36, Issue.1,2013.