International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

Survey on Security Attacks and Solutions in Cloud Infrastructure

Shilpa D[1] , Nagashree C[2] , Divya C[3], Spurthi G S[4]

Assistant Professor, Department of Computer Science and Engineering, SVIT, Bangalore, India[1]
Assistant Professor, Department of Computer Science and Engineering, SVIT, Bangalore, India[2]
Assistant Professor, Department of Computer Science and Engineering, SVIT, Bangalore, India[3]
Assistant Professor, Department of Information Science and Engineering, SVIT, Bangalore, India[4]

Abstract: Cloud Computing is a booming internet driven technology, which renders a pool of resources such as network, storage, and applications on- demand basis. The cloud Services must be highly secured so that it increases the adoption of cloud for enterprise business management. The cloud services are shared by multitenant using internet channel which is a vulnerable to attacks. Cloud computing is exposed to many threats. In this paper we discuss some of the common attacks and their solution.

Keywords: Rapid Provisioning, Security, Denial of Service, Access Controls, virtualization.

I. INTRODUCTION

Cloud computing is an internet driven technology, which helps enterprises to improve their business. The cloud is a pool of hardware (e.g. network, storage etc) and software resources (e.g.: applications). The resources are virtualized and automated so that they can be easily accessible. Resources are allocated to the end user as "pay as you use" model. The properties of cloud such as rapid provisioning, pay as you go, scalability (scale in/out), reliability, virtualization and broad network access has made enterprises to adapt the cloud. The cloud computing technology also helps enterprises to reduce their infrastructure cost and operational cost. The resources that are required for day to day operation of an industry can be accessed by end users whenever and wherever they are needed. The end users are charged only for the resources that are used. This kind of dynamic allocation or on demand allocation of resources is very useful for industries which have dynamic infrastructure, where the resources are needed only for certain duration of time.

II. DIFFERENT CLOUD SERVICE MODELS

A. Software As A Service (SAAS)

The cloud service provider provides their end users with the capability to deploy their applications on cloud infrastructure. The cloud service provider licenses the applications to its end users based on pay as you use model or at no charge. SAAS was deployed for sales service force automation and customer relationship management. In addition to this SAAS is also extended for many business management such as human resource management, billing, financial management solutions[1].

B. Platform As A Service (PAAS)

Cloud Service Provider (CSP) rents hardware, operating system, storage, network capacity over the internet to the end users to build their application on top of platform.
PAAS provides a development and deployment middleware layer[1]. The virtualized servers can be used to test the new application. With the PAAS OS features can be changed and upgraded frequently. Industries instead of maintaining multiple hardware facilities that often suffer from incompatible issues, can adapt PAAS that would provide a better solution to get rid of incompatible issues.

C. Infrastructure As A Service (IAAS)

The hardware resources such as servers, network and storage are virtualized and provisioned to the customers based on their application. Gartner's Cloud IAAS research guides on sourcing, infrastructure, best practices, hybrid cloud, security and risk management, and regional market evolution. The customers can use API (Application Program Interface) to start a service, to communicate with network elements (such as hosts, switches and routers) and add new devices. The user does not have control of the underlying hardware in the cloud instead they can only manage the OS, storage and delivered applications [1].

In cloud computing services survey done by IDC IT group in 2009 over 87% of those survey cited security as the number one issue preventing adoption of cloud. A popular photo sharing site Instagram, the developer of instagram deployed the entire service using rented instances on amazon popular EC2 cloud computing. Public key cryptography and presence of secret keys in hardware that instagram doesn't control [2]. Most of the users are unaware of the multitenancy because cloud fully isolates individual customers into separate VM's so a VM should prevent unauthorised user from hacking the sensitive data.

Privacy and security are considered as two major obstacles for adoption of cloud by enterprises [6]. Figure 1 shows the cloud service models. When we move down the stack that contains IAAS, PAAS, SAAS there are more security issues that are to be addressed. To overcome the obstacles and increase the adoption of cloud for enterprises recently developed on cryptographic techniques can be used. The security issues in cloud differ from one service model to another model[3].

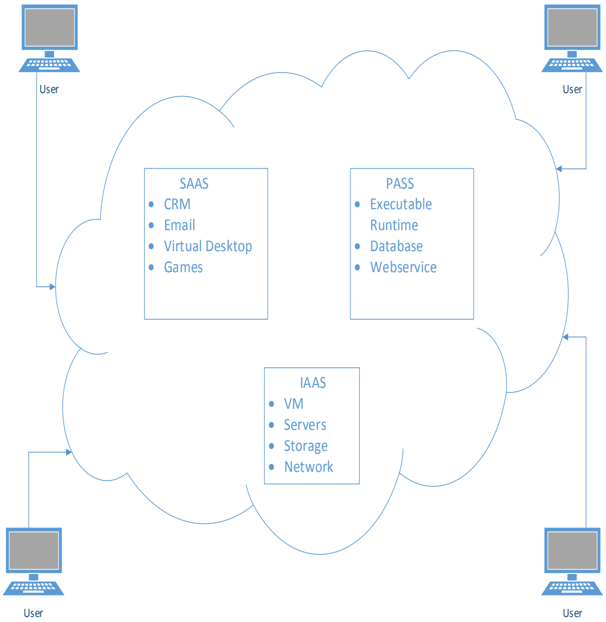

Fig 1: Cloud service model

III. FRAMEWORK FOR ANALYSING SECURITY IN CLOUD

The security services in cloud should provide the following attributes:

- Confidentiality: Customer's private data must be secured. The access of data should be restricted to a cloud service provider.

- Integrity: The customer data must not be tampered by cloud service provider or unauthorized user.

- Availability: Data must be available to authorized users whenever and wherever they are needed.

- Reliability: Back up for customer data must be provided.

- Efficient retrieval: The time for data retrieval must be less.

- Data sharing: The customers can share their data with trusted parties.

The five functional subsystems defined by IBM are:

A. Audit and compliance

The enterprises that uses IT solutions should be supported with audit functionality. The audit responsibilities must be clearly outlined in contracts and SLA's between organization and cloud service provider. To fulfill the audit regulations, an organization sets its own security policies and implements them using appropriate infrastructure. The audit and compliance addresses data captures analyses, reports, and archives and retrieves records and events. There is no standard framework or API are available for integration of multiple audit system. There is no specific model that delineates the audit responsibilities between CSP and consumer[4].

B. Access control

Cloud offers multitenancy so that access management in cloud is one of the critical issues. The access control can be done by authentication, authorization and federated sign on. The Cloud Service Authority (CSA) suggests the use of user centric authentication method such as open ID, it reduces the complexity and allows for reuse resources must be controlled based on user profile and policy information. If an organization uses the services provided by multiple CSP, it encounters a problem of authenticating multiple times during a single session for different cloud services. The multiple sign on problem can be solved using federated identity problem [4].

C. Flow control

Information flow control deals with security of data integration between CSP and consumer. The flow control includes secure flow of data through different phases of data life cycle (creation, storage, use and share, archive, destroy). Cloud services are shared by multiple consumers via internet, which is an uncontrollable and unsecure medium. The credential management should be in place at multiple levels of network stack. At application layer use of application specific encryption techniques to ensure adequate security for data. In transport layer the use of cryptographic protocols such as SSL and TLS. At network layer use of protocols such as VPN and tunneling tends to provide better security [5].

D. Identity and credential management

In cloud computing credential management includes provisioning, deprovisioning, management of identity objects. It also includes ability to define a trusted third party broker to accept users credentials (e.g.: username, password) and return a signed token to authorized users to access resources. The federated identity management allows an organization to rapidly manage access to multiple cloud services from a repository. Currently CSP's have custom connectors for communication of identity and access control objects, but they increase the complexity of management and are not flexible, dynamic and scalable. By using a brokered trusted identity federated services as a business agreement between CSP and consumers can reduce complexity and establish a trust with multiple different types of services can be done using a single trust broker [5].

E. Solution integrity

In the world of cloud computing solution integrity refers to ensure dependable and correct operation of cloud system in meeting compliances and technical standards. The data in a cloud must be protected cryptographically and physically preventing intrusions, failures and service outages. To provide a better fault tolerance for customers, CSP should ascertain the disaster recovery and continuity plane of its customers [5].

IV. SECURITY CHALLENGES

Cloud is facing challenges such as:

- Administrative access to server and applications*:* In cloud computing access to resources is via internet, which has more exposure to risks ,so it is necessary to restrict administrative access and to maintain visibility of changes in system control.
- Dynamic VM*:* VM's are dynamic. They can quickly rollback to previous instances, cloned and moved between different physical servers. This dynamic nature and potential for VM makes it difficult to achieve and maintain consistent security. Vulnerabilities are configuration errors can be disseminated. It is also difficult to maintain auditabilty and security of VM.

- Vulnerability exploits and VM to VM Attacks*:* Cloud computing servers use the same operating systems. The ability for an attacker or hacker to remotely exploit vulnerabilities in these systems and applications is a critical threat to virtualized cloud computing environments. Also the co-location of multiple virtual machines increases the attack surface and risk of VM-to-VM compromise.

- Data Integrity*:* Data Breaches are occurring due to hacking and intrusion, dedicated resources are required to be secured. The cloud Environment partially or fully shared is more exposed to risk. Enterprise needs confidence and auditable proof that cloud resources are not being forged nor compromised. OS application files and activities need to be monitored.

V. SECURITY THREATS AND SOLUTIONS

Cloud environment is prone to security attacks. The current industry demands security as one of the critical factor. Figure 2 shows the various attacks cloud has to address.In this section we discuss about the various security attacks and solutions.

A. Denial of Service Attack (DOS)

In the cloud Environment, multitenant shares the resources. If a non legitimate user utilizes large amount of resources, all other legitimate users will experience decrease in performance [5]. The DOS attack occurs when an attacker overloads the server with request for resources. The cloud service provider such as Amazon divides the cloud in to availability zones[5]. Another defense of DOS is to monitor resource based on the network bandwidth and storage consumptions to charge the usage[6]. The HTTP, XML, Representational State Transfer (REST) are DOS attacks. The HTTP based Distributed DOS attacks and XML based Distributed DOS attacks are more critical. To encounter these attacks there exists a framework called cloud defender which has 5 phases 1) sensor filter 2) hop count filter 3) IP frequency divergence filter 4) puzzle resolver filter 5) double signature filter. The first four detects HTTP based DDOS attack and 5th filter detects the XML based attack[6].

B. Target shared memory attack

Attacker takes advantage of shared memory (cache or main memory) of both physical and virtual machines. This attack can lead to another attack such as side channel attack and malware injection attack. Intruder gains unauthorized access to the data which describes the structure of cloud such as number of process running, total count of users logged in a specific terms. The main aim is to incur virtual machine memory through malicious insider attack [7].

C. Malware Injection attack

The intruder creates his own virtual machine or malignant service implementation modules and adds them into existing infrastructure [5]. Cloud assumes it as new service implementation and redirects the request to malicious module. The intruder learns about user request, data, and access rights. Retrospective detection based on portable executable (PE) technique to detect malignant instance is used. Another defense mechanism known as cloud AV which has antivirus as a network service and N version protection provides better detection enhanced forensics capabilities, improves deploying ability and management. The hypervisor can be used for scheduling all service instances it can check integrity of instances from file allocation table (FAT) of the customers VM before servicing their requests.

D. Phishing attack

Phishing is a way of retrieving personal information from unsuspecting user through sending emails, webpage linker and instant message. These links appear to the authenticated but leads to fake access locations. Phishing attacks are of two types: 1) abuse behavior: an attacker hosts a phishing attack site in the cloud by using cloud services.2) hijack the accounts using social engineering technique. To avoid the phishing attacks access to sensitive data about the enterprise such has employee information (login details), financial records should be controlled. The employee passwords used to access the cloud should be strong and hard enough to guess. The authorized should be given information only on need to know basis. The use encryption also provides strong defense to phishing attacks [8].

E. Botnet attack (stepping stone attack)

In stepping stone attack the intruder tries to access the data by avoiding to reveal their identity and location to reduce detection. This is done by indirectly intruding in to target victims host by a series of other hosts (called stepping stone). Botnet attacker was seen in Amazon E22 cloud also using relay command through Google app engine. Stepping stone host is detected based on analysis of incoming and outgoing traffic through stepping stone host. such as packet content, timing network traffic. However the intruders introduce random delay, encrypted traffic to gain access. To defense this attack pebble scheme is introduced where it first identifies the cryptography keys used in botnet operator and then it traces back the bot master [9].

F. Audio Steganography Attack

Audio Steganography is known to be one of the critical attack to cloud storage systems. In audio steganography the users embed confidential information within the audio files. The user can send secret data through media files which appear to be a normal sound files. The intruder uses this methodology to gain access to cloud storage. StegAD(Steganography Active Defense) method is employed to overcome Audio Steganography Attack. The RS image gray scale stegno-analysis algorithm is used to scan the hiding place of audio files in cloud storage. After acquiring suspicious files, SADI (Steganography Audio Dynamical Interference) technique to interfere in all the possible places in those suspicious files. Interference) technique to interfere in all the possible places in those suspicious files [1].

G. *Flooding Request Attack*

When the Server is overloaded and reached the maximum threshold capacity it will distribute its job to a nearest Server. This sharing Approach makes the cloud faster. When the malicious has gained access to cloud, forged data can be easily created and send request to the Server. The Server checks the Authencity of these requests which consumes CPU Memory and engages IAAS to a great extent. While processing these non-legitimate requests, legitimate services can starve and as a result the server will be offload its services to another server[11]. The solution is to organize a set of servers and each server is assigned a specific type of job e.g. one group of server is assigned the work of memory management, another server storing files etc. These set of Servers will be interconnected themselves for message passing. so when a server is overloaded a new server in the set will be deployed which has complete records of the current states of the servers. Hypervisor is used for Scheduling among these fleets to check the authorization of request and prevent the servers from being overloaded with forged requests [12].

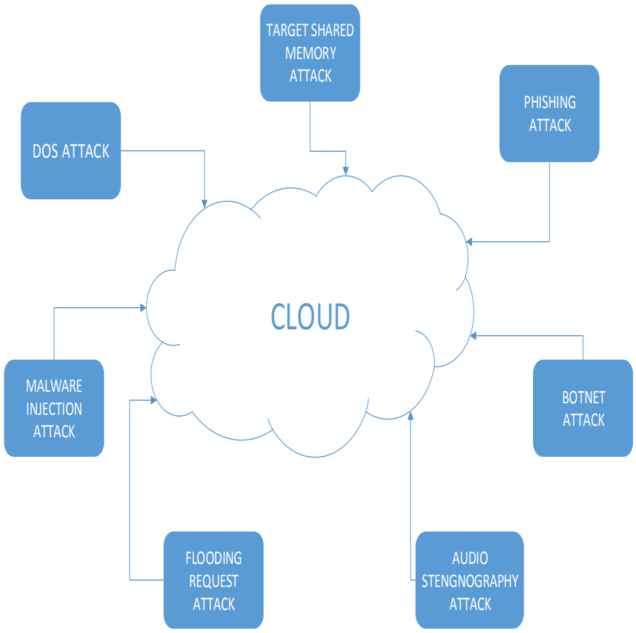

Fig 2: cloud attacks

VI. SOLUTION APPROACHES

In this section we summarize the solution approaches that can be used to defense the security attacks and improve the security of data.

- Intrusion Detection System (IDS): Attacks such as DOS, DDOS mainly target data confidentiality, integrity and availability.DOS, DDOS attacks are avoided by IDS and monitoring network traffic, log files and user behavior. IDS are of 2 types 1) host based IDS 2) network based IDS[13].
- Firewall: A bidirectional firewall can be deployed on individual virtual servers which can decrease attack surface and prevents the denial of service attacks [14].
- Integrity monitoring: Monitoring the integrity of data such as application, registry etc is required for detecting malignant users [15].
- Analysis of log: log files in the application are analyzed for detecting suspicious and collection of security related administrative activities and events in the data centre [15].

VII. CONCLUSION

In this paper we discuss an overview of cloud computing technology and framework for analyzing security issues. We also discuss about the attributes for security. We address the various security attacks and solutions to overcome security threats. We also deliberate about solution approaches to provide better security.

REFERENCES

[1] National Institute of Standards and Technology, NIST Definition of Cloud Computing, Sept 2011.

[2] Ramgovind, S.; Eloff, M.M.; Smith, E., "The management of security in Cloud computing," Information Security for South Africa, 2010 , vol., no., pp.1-7, 2-4 Aug. 2010.

[3] www.cloudreadyscurity.com

[4] IBM Corporation, Enterprise Security Architecture Using IBM Tivoli Security Solutions, Aug 2007.

[5] Karnwal, T.; Sivakumar, T.; Aghila, G, "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack". In Proceedings of the 2012 IEEE Students' Conference on

[6] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, 2009.

[7] Anil, S. L., & Thanka, R."A Survey on Security of Data outsourcing in Cloud". *International Journal of Scientific and Research Publications*, *Volume3*, 2013

[8] Arora, P., wadhawan, R. C., & ahuja, E. S. "Cloud computing security issues in infrastructure". *Ijarcss*, 2012..

[9] Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S," A Survey on Security Issues in Cloud Computing". *arxiv.org*, 2012.

[10] Deboosere, L., Vankeirsbilck, B., Simoens, P., De, F. T., Dhoedt, B., & Demeester, P, " Cloud-based desktop services for thin clients". In *IEEE Internet Computing, vol no. 16* (pp. 60-67), 2012.

[11] Dr.A.Venumadhav,"A Survey on Security of Data outsourcing in Cloud". *International Journal of Scientific and Research Publications, Volume 3*, 2013

[12] Green, M., "The Threat in the Cloud", *the IEEE Computer and Reliability Societies*, 2013.

[13] Jansen, W. a." Cloud Hooks: Security and Privacy Issues in Cloud Computing", *44th Hawaii*, 2011.

[14] Khalil, I. M., Khreishah, A., & Azeem, M". Cloud Computing Security", 2014.

[15] Yang, S, "Cloud computing security issues and mechanisms ". *Advanced Materials Research*, 2011.

BIOGRAPHIES

Shilpa D is working as Assistant Professor in Sai Vidya Institute of Technology, Bangalore. Her area of interest includes Computer Networks and Cloud Computing.

Nagashree C is working as Assistant Professor in Sai Vidya Institute of Technology. Her area of interest includes Cloud Computing and Computer Networks.

Divya C is working as Assistant Professor in Sai Vidya Institute of Technology, Bangalore. Her area of interest is cloud computing, Software engineering and Adhoc Networks.

Spurthi G S is working as Assistant Professor in Sai Vidya Institute of Technology. Her area of interest are Cloud Computing and Adhoc Networks.