International Journal of Advanced Scientific Technologies, Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) Volume.3,Special Issue.1,March.2017

A Study of Security and Privacy Attacks in Cloud Computing Environment

Mrs.K.Santhi Sri
Associate Professor
Vignan's University

Mrs. PRSM Lakshmi
Assistant Professor
Vignan's University

Mr. M.V.Bhujanga Rao
Assistant Professor
R.V.R&J.C. College of Engineering

Abstract— Cloud computing refers to providing different computing services on-demand and pay per use basis through Internet. Cloud Computing has gained acceptance for execution in different organizations. This emerging technology has several issues like security, performance and accessibility Different dimensions included related to multi-tenant nature, architecture, scalability and elasticity. This study paper provides complete knowledge about security problem in cloud. It also includes approaches related to data encryption and message authentication.

Index Terms— cloud computing, decryption, encryption, concurrent access, message signing and verification, data confidentiality, message authentication, cloud security

I. INTRODUCTION

Cloud Computing is continuously rising and showing consistent growth in the field of computing. Cloud computing (so-called, cloud) represents one of the outstanding shifts in information technology which can enhance collaboration, quickness, scaling and availability, and provide the potential for cost reduction through optimized and accomplished computing [11,12]. Cloud computing is rising from recent advances in technologies such as hardware virtualization, Web services, distributed computing, utility computing and system automation. With virtualization, one or more physical servers can be configured and partitioned into multiple independent "effective" servers, all functioning independently and appearing to the user to be a single physical device. Such virtual servers are in spirit disassociated from their physical server, and with this added elasticity, they can be moved around and scaled up or down on the fly without affecting the end user. The difference with cloud computing is that the computing process may run on one or many connected computers at the same time, utilizing the concept of virtualization.

The Cloud however is inclined to many privacy and security attacks. The biggest problem hindering the progress and the wide adoption of the Cloud is the privacy and security issues associated with it. Clearly, many privacy and security attacks occur from within the Cloud provider themselves as they usually have direct access to stored data and steal the data to sell to third parties in order to gain profit. The main aim of the paper is to finds out the problem related with cloud security. Paper extracts the issues and focuses on data security and privacy during communication on the clouds.

II. SECURITY ISSUE WITH CLOUD MODEL

In the given state, a constant research effort in the area of cloud storage and cloud computing security will help achieve the balance between economic probability, simplicity of deployment and a suitable collection of security considerations for each cloud service (CS) client.
In a public cloud enabling a shared multi-tenant environment, as the number of users increase, security risks get more intensify and diverse. It is necessary to identify the attack surfaces which are horizontal to security attacks and mechanisms ensuring successful client-side and server-side protection [8]. Because of the miscellaneous security issues in a public cloud, adopting a private cloud solution is more secure with an option to move to a public cloud in future, if needed[2]. Based on the deployment model of cloud, security issues are classified as:

A. Issues with Public Cloud

In a public cloud, there exist many clients on a shared platform and communications security is provided by the service provider. A few of the key security issues in a public cloud include:

• In case of a public cloud, the same communications is shared between multiple tenants and the chances of data leakage between these tenants are very high. However, most of the service providers run a multitenant infrastructure. Proper investigations at the time of

choosing the service provider must be done in order to avoid any such risk [11,12].

• The three basic necessities of security: confidentiality, integrity and availability are required to protect data throughout its lifecycle. Data must be protected during the various stages of creation, sharing, archiving, processing etc. However, situations become more difficult in case of a public cloud where we do not have any control over the service provider's security practices [6].

Even though data is stored outside the limits of the client organization in a public cloud, we cannot reject the possibility of an insider attack originating from service provider's end. Moving the data to a cloud computing environment expands the circle of insiders to the service provider's staff and subcontractors[18]. An access control policy based on the inputs from the client and provider to prevent insider attacks has been proposed in [7]. Policy enforcement implemented at the nodes and the data-centers can prevent a system administrator from carrying out any cruel action. The three major steps to achieve this are: defining a policy, propagating the policy by means of a secure policy propagation element and enforcing it through a policy enforcement element.

The Guidelines on Security and Privacy in Public Cloud Computing published by NIST offer a summary of the security, privacy and availability risks of cloud computing [8]. The NIST procedure identify, among other points, the following risks related to the use of cloud computing by organizations:

• **Trust**: Through the use of cloud computing and CS the organization relinquishes control over significant parts of aspects of security and privacy. As a result of this, the organization makes a commitment and places trust into the control mechanisms and processes engaged by the cloud provider. One risk is the possible for insider access to the information, provoking both intentional incidents leading to loss or corruption of data, or unplanned errors, leading to considerable unavailability of the CS. Another risk is the potential lack of clarity over data ownership, especially in border cases such as transaction data generated through the use of CS.

• **Data protection**: From the CS customer viewpoint, there are fewer mechanisms for data protection when data is created through CS or maintained in cloud storage. Two aspects of data protection are considered, namely data accessibility and data access control. The first aspect depends on the migration and backup capabilities offered by the type of the CS chosen by the client. The second aspect is less trivial, due to the specifics of the shared multi-tenant environment in which CS are deployed.

• **Governance**: Due to their wide availability and in many cases high degree of usability, CS (especially on the SaaS level) can easily bypass the security, privacy and software use policies adopt by the organization. While ensure that systems are safe and risk is manage is likely (although not trivial) in the case of in-house system deployments, that is far further tricky in the case of cloud services.

B. Issues with Private Cloud

In a private cloud, clientele have total power over the network. Private cloud provides the plasticity to the customer to execute any traditional network perimeter security practice. Although the security architecture is more reliable in a private cloud, yet there are issues/risks that need to be considered: A few of the key security issues in a private cloud include:

• In a private cloud, users are facilitated with an option to be able to manage portions of the cloud, and access to the infrastructure is provide through a web interface or an HTTP end point. There are two ways of implementing a web-interface, either by writing a whole application stack or by using a standard applicative stack, to build up the web limit using common languages such as Java, PHP, and Python etc. As part of broadcast process, Eucalyptus web interface has been found to have a bug, allowing any user to perform internal port scan or HTTP requests through the management node which he should not be tolerable to do. In the nutshell, interfaces need to be properly developed and standard web application sanctuary techniques need to be deployed to protect the diverse HTTP requests being performed [2].

• Virtualization techniques are quite in style in private clouds. In such a scenario, risks to the hypervisor should be carefully analyzed. There have been instances when a visitor in service system has been able to run processes on other guest VMs or host. In a virtual atmosphere it may happen that virtual machines are able to exchange a few words with all the VMs including the ones who they are not invented to. To ensure that they only communicate with the ones which they are supposed to, proper authentication and encryption techniques such as IPsec [IP level Security] etc. should be implement [9].

Private clouds are considered safer in similarity to public clouds; still they have multiple issues which if unattended may lead to major defense loopholes. Hybrid cloud model is a combination of both public and private cloud and hence the sanctuaries issues discuss with respect to both are applicable in case of hybrid cloud.

Cloud Service Security

Based on Cloud Service Model, safekeeping issue can be categorize [2]. It can be categorized into network level,

user verification level, data level, and generic issues. Each cloud service model comprises its own inherent security flaws; however, they also share some test that affects all of them. Before analyzing security challenges in Cloud compute, we need to understand the relationships and dependencies between these cloud service models. PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and Sass services, but also it may be true on the other way around.

Security Issues with SaaS

SaaS provides application services on demand such as email, conferencing software, and big business application such as ERP, CRM, and SCM [9]. SaaS users have less control over security among the three fundamental delivery models in the cloud. The adoption of SaaS applications may raise some security concerns.

Data Security: Data security is a common concern for any technology, but it becomes a major face up to when SaaS users have to rely on their providers for proper security. Data security includes the definite gearshift and technology used to enforce information authority. This has been broken out into three sections to cover detection of data migration to cloud, protecting data in transit to the cloud and between different providers and protecting data once it's within the cloud. The SaaS provider is the one responsible for the security of the data while is being processed and store[10]. In SaaS, organizational data is often process in plaintext and stored in the cloud. in addition, data backup is a critical aspect in order to smooth the progress of recovery in case of disaster, but it introduces security concerns as well . Also cloud providers can subcontract other services such as backup from third-party examine providers, which may raise concerns. besides, most compliance values do not predict compliance with regulations in a world of Cloud Computing. In SaaS model, the process of compliance is composite because data is to be found in the provider's datacenters, which may introduce regulatory acquiescence issues such as data space to yourself segregation, and security, that must be]enforced by the provider.

Application Security: Since applications are typically delivered via the Internet through a Web browser. However, flaws in web applications may create vulnerabilities for the SaaS applications. Security challenge in SaaS applications are not different from any web application technology, but traditional security solutions do not effectively protect it from attacks, so new approaches are obligatory Attackers have been using the web to cooperation user's computers and carry out malevolent actions such as steal sensitive data [2]. The Open Web Application Security Project (OWASP) has identified the ten most critical web applications security threats. There are more security issues, but it is a good start for securing web applications.

Multi-Tenancy: The impact of multi-tenancy is visibility of residual statistics or trace of operations by other user or tenant. In this case, multiple consumers with same or different organization use same funds or applications. Information security is one of the prime factors for this phase. Since data from multiple tenants is likely to be stored in the same database, the risk of data leakage between these tenants is high. Security policy are needed to make certain that customer's data are kept separate from other customers [7].

Access Control: Accessing applications over the internet via web browser makes access from any network device easier, as well as public computer and mobile devices. However, it also exposes the service to bonus security risks. The Cloud Security consortium has released a document that describes the current state of mobile computing and the top threats in this area such as information burglary mobile malware, insecure networks (WiFi), vulnerabilities found in the device OS and official applications, self-doubting marketplaces, and proximity-based hacking.

Security Issues with PaaS

PaaS cloud (public or private) offers an integrated milieu to design, develop, test, deploy, and support custom applications developed in the language the platform supports. PaaS application security comprises two software layers: Security of the PaaS platform itself (i.e., runtime engine), and Security of customer applications deployed on a PaaS platform. PaaS providers are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications.

Mashes combine more than one source element into a single integrated unit. Thus, PaaS models also inherit security issues related to mashes such as data and network security. Also, PaaS users have to depend on in cooperation the security of web-hosted development tools and third-party services.

Access Control: In the PaaS delivery model, the CSP is responsible for managing access control to the network, servers, and application platform infrastructure. However, the customer is responsible for access control to the applications deployed on a PaaS platform. Access control to applications manifests as end user access management, which includes provisioning and authentication of users.

C. Security Issues with IaaS

With IaaS, cloud users have better control over the security compared to the other models as long as there is

no security hole in the virtual machine monitor. They control the software running in their virtual machines, and they are accountable to configure security policies correctly. However, the fundamental compute, network, and storage infrastructure is controlled by cloud providers. IaaS provides a pool of resources such as servers, storage, networks, and other computing resources in the form of virtualized systems, which are accessed through the Internet. IaaS providers must undertake a substantial effort to secure their systems in order to minimize these threats that result from creation, communication, monitoring, modification, and mobility. Unlike PaaS and SaaS, IaaS customers are primarily responsible for securing the hosts provisioned in the cloud. Some of the new host security threats in the public IaaS include:

• Attacking unpatched, vulnerable services listening on standard ports (e.g., FTP, NetBIOS, SSH)

• Hijacking accounts that are not appropriately secured (i.e., weak or no passwords for standard accounts)

• Stealing keys used to access and manage hosts (e.g., SSH private keys)

• Deploying Trojans embedded in the software component in the VM or within the VM image (the OS) itself

• Attacking systems that are not properly secured by host firewalls

III CONCLUSION

Security concern has become the biggest complexity to adoption of cloud because all information and data are completely under the control of cloud service providers. In the cloud, data and services are not restricted within a single organization's edge. This vitality and fluidity of data introduces more risk and complicates the problem of access control. Therefore, compared with the traditional models, in cloud computing model ensuring confidentiality and integrity of the end-user's' data is far more challenging. Security issues can be categorized into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues.

REFERENCES

[1] Shyam Nandan Kumar, "Cryptography during Data Sharing and Accessing Over Cloud." International Transaction of Electrical and Computer Engineers System, vol. 3, no. 1 (2015): 12-18.

[2] Shyam Nandan Kumar, "DecenCrypto Cloud: Decentralized Cryptography Technique for Secure Communication over the Clouds." Journal of Computer Sciences and Applications, vol. 3, no. 3 (2015): 73-78.

[3] Shyam Nandan Kumar, "Review on Network Security and Cryptography." International Transaction of Electrical andComputer Engineers System, vol. 3, no. 1 (2015): 1-11.

[4] Shyam Nandan Kumar, "World towards Advance Web Mining: A Review." American Journal of Systems and Software, vol. 3, no. 2 (2015): 44-61.

[5] Omar, M.N, Salleh, M., and Bakhtiari, M., "Biometric encryption to enhance confidentiality in Cloud computing", International Symposium on Biometrics and Security Technologies (ISBAST), 2014, IEEE, pp. 45-50, Kuala Lumpur.

[6] Chandar, P.P., Mutkuraman, D. and Rathinrai, M., "Hierarchical attribute based proxy re-encryption access control in cloud computing", International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2014, IEEE, pp. 1565-1570, Nagercoil.

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption", in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 3494. Springer, pp. 457-473, 2005.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89-98.

[9] B. Waters, "Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization,"in Public Key Cryptography (PKC '11), pp. 53-70, Springer, Berlin, Germany, 2011.

[10] Wenyi Liu, Uluagac, A.S. and Beyah, R., "MACA: A privacy-preserving multi-factor cloud authentication system utilizing big data", IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2014, pp. 518-523, Toronto, ON.

[11] Jen Ho Yang and Pei Yu Lin, "An ID-Based User Authentication Scheme for Cloud Computing", Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014, IEEE, pp. 98-101, Kitakyushu.

[12] Jia-Lun Tsai and Nai-Wei Lo, "A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services", Systems Journal, IEEE (Volume: 9, Issue: 3), pp. 805-815, 21 May 2015.