COMPARATIVE STUDY OF RESILIENT AUTHENTICATED KEY EXCHANGES AND SECURITY ISSUES IN CLOUD COMPUTING ENVIRONMENT

Dr. A.R. Jayasudha

Associate Professor
Hindusthan college of Engineering and Technology, Coimbatore

***Abstract*: Computing services are provided as utility services through internet based on the consumers' demand and need and are privileged to pay as per their use. Cloud Computing enables the end users to access a pool of storage, servers, services and applications virtually. Virtual access as against physical saves a lot of time and cost. The pay-as-you go model provides many benefits to industries such as health care, banking and educational institutions. Cloud provides resources such as storage space, bandwidth, processing power etc. Wholesome data are stored in data centers of the cloud service providers. Data centers of Amazon, Google, and Microsoft are on internet, there by very limited control over data. This would lead to data breach, insecure interface, data attacks etc. This paper lists out various cloud models, its security risks that are prevalent in the cloud industry. It also analyses the challenges and provides best practices for improvising cloud security.**

Keywords: Security, Cloud Security, Cloud Service Provider, Cloud Services, Data Security

1. INTRODUCTION

On demand computing resources and services are provided through a distributed architecture which provides scalability and centralizes all resources. More similar to internet service providers, cloud service providers provide cloud services to their customers. Cloud resources such as networks, servers, storage and applications are provided through a convenient cloud model based on demand. These resources are provided with very less effort and communication and interaction. Three types of services Software as a Service, Platform as a service and Infrastructure as a service are provided. Cloud computing follows a pay-as-you use model which enables many organizations to move towards cloud paradigm. Organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers [2]. Usage of cloud computing resources ensures reduction in management and operation cost. Companies like Microsoft, Amazon, Google, and Salesforce.com are the leading cloud service providers. Reduction in management and operation cost enables and enhances the percentage of startups to take up entrepreneurship as infrastructure cost is greatly depreciating. Physical Machines in the form of virtual machines, storage facilities are dynamically allotted to users based on their requirement and demand. In depth exploration and exploitation of the technology has raised the level of business and transactions. Paradigms of cloud does not require prior expertise to control the cloud infrastructures. Cloud computing providers deliver common online business applications which are accessed from servers. [5]

II. CLOUD COMPUTING COMPONENTS

A. Cloud Computing models

In general, cloud services are divided into three categories, Saas, Paas and Iaas.

Software as a Service: It is a process through which the application service provider provides many applications via internet. This enables the clients to skip installation of any cumbersome software and saves time and money spent on maintenance of hardware and software. Servers, Operating system software, databases, data center space are provided by the cloud vendor and processes such as upgrades, backups are also managed by vendors. It is a full service on demand.

Platform as a Service: It is a service in which computing platform is provided as a service without need to download or spend on maintenance of softwares. Cloud applications are integrated and implemented with the high level infrastructure. Without management of infrastructure the client operates and controls deployed applications.

Infrastructure as a service: Virtualization enables execution of services by sharing hardware resources. Resources such as network, storage are made available for applications and operating systems. On demand, infrastructure are provided as services that uses suitable interfaces for interaction with hosts, switches and routers.

III. KEY SECURITY ISSUES

There are three segments in cloud computing such as applications, platforms and infrastructure. These segment provide different services and offer different products. Cloud Computing involves numerous security issues as it encompasses technologies including networks, databases, virtualization, scheduling of resources, load balancing and control of concurrent tasks. The security issues of these technologies are applicable to cloud resources and technologies also. The interconnection of systems in the cloud need to be

secure and in the similar way physical machine mapping to the virtual machine need to follow secure procedures. Data sharing involves encrypting the data as well as enforcing proper policies.

As all information and data are absolutely under the control of cloud service providers, security has become a major concern and obstacle for adoption of cloud. Cloud security guidance and recommendations are published by CSA[1], ENISA[3] and NIST[6]. These provide security guidance for cloud usage. Cloud security threats need to be properly addressed and handled, failing which would produce devastating results.

Data Loss or Leakage: There are a few reasons that lead to data loss or leakage such as, operation failures, improper use of encryption and software keys, insufficient authorization and authentication controls to sensitive data.

Account Hijacking: One of the major threats of cloud is account or service hacking. Account hijacking is mostly done using stolen credentials. Stolen credentials lets the unauthorized user to have access to significant areas of cloud services. This leads to compromise of integrity and confidentiality of data. In the case of lost credentials or stolen credentials, Single Sign on proves even more hazardous.

Cryptography techniques and Management of Keys: Cryptography techniques provides data protection and Key management controls access to protected data. Conversion of plain text to cipher text is recommended during data storage, during data transit and during backup of data. Encryption of archival data would safeguard data from malicious cloud service providers. Management of key need to be perfectly handled, improper ways of key management would compromise on all security aspects of encrypted data. Identity management is a critical factor to avoid account and service hijacking. Sharing of credentials are strictly prohibited across all types of cloud services.

IV. PROBLEM STATEMENT

Amazon S3, Mosco Cloud Files are providing Cloud services as Software as service. Standard techniques such as encryption, one time password, digital certificates are adopted for authentication purposes[6]. Though there are number of techniques, all methods are independent and does not guarantee a higher level of security against attacks. Extensive study was made on cryptographic primitives such as encryption, signature and pseudo-random function. Authenticated Key exchange protocols form a central component in many network standards such as IPSec, SSL, SSH etc. Communication channel over a public network is more prone to be attacked by malicious attacker. Thereby it becomes insecure for message transmission. A cryptographically strong encryption key is agreed between two communicating entities that was enabled by authenticated key exchange. Message authenticity and data confidentiality is maintained using the agreed strong encrypted keys. In authentic key exchange protocol, each client holds a static long – term public key and a corresponding long-term secret key. Similarly, for individual sessions, each client generates their secret key and exchanges the corresponding public key. A Key exchange protocol that has been proven secure would be completely insecure to the prevailing leakage attacks.

Limitations in existing Key Exchange Models

The existing leakage resilient authenticated key exchange models fail to fully capture general leakage attacks due to many reasons. The authenticated key exchange model security feature demands that the session key should not be distinguishable from the randomly chosen key even if sensitive information is been obtained. Partial information about session key could be obtained by encoding the available information in to the leakage function. In the existing models, the adversary is not allowed to make any leakage query during the challenge session. Earlier proposed notions [8, 11] have already captured some leakage attacks, it focuses only on partial leakage of the long-term secret key. It is to be notes that the partial leakage is independent from the secret key reveal queries. There are potential weakness of the randomness that are caused due to poor implementation of the pseudo-random number generations.

Modelling Leakage Resilient KE Model

Leakage Resilient Key exchange model captures challenge dependent leakage on both the long-term secret key and the secret key. This would happen due to poor random implementations.

This model addresses the limitations of the previous leakage-resilient models by allowing long term leakage queries before and after the challenge session. This model requires the adversary to commit a set of leakage functions before it obtains all the inputs instead of asking the adversary to specify the leakage functions before the system set up. Once the adversary obtains all the inputs, leakage functions specified in the committed set can be used to learn partial information of the last unknown secret.

Challenge Dependent KE Model

Side-channel attacks against KE protocols are captured using challenge dependent KE model. This model captures long term and secret key leakage and permits the adversary to issue queries for leakage after the activation of the challenge session.

Send (A,B,message) – Send message to party A on behalf of party B and obtain A's response for the message.

EstablishParty(pid**) –** Register a long term public key on behalf of party id.

LongTermReveal(pid) – Query the long term secret key of honest party id.

SessionkeyReveal(sid) – Query the session key of the completed session sid.

SecretKeyReveal(sid) – Query the secret key of session sid.

Constraints on Leakage function

Several constraints on the leakage function to prevent adversary from breaking the authenticated key exchange model. The leakage function f1 and f2 need to produce the output size lesser than long term key and secret key. Another restriction is related to the challenge dependent leakage security of Key exchange protocols. The adversary is not allowed to adaptively issue leakage query after it obtains other information for session key computation.

REFERENCES

[1] CSA (Cloud Security Allicance), "Security guidance for criti al areas of focus in cloud computing V2.1", Deceber 2009.

[2] A. Kundu, C.D. Banerjee, P.saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICTT, Vol.4, No. 5 pp.143-152, 2010.

[3] ENISA (Europeran Netowrk and Information Security Agency), "Cloud Computing: Benefits, Risks and Recommendations for Information Security", November 2009.

[4] CSA, "Top threats to Cloud Computing V1.0" Marc 2010.

[5] Lizhe Wang, Jie Tao, Kunze , Castellanos A.C,. Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp.825-830, Dalian, Cine Sep.2008, ISBN:978-0-7695-3352-0.

[6] P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm", Information Technology Laboratory, NIST.

[7] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Version 15", Information Technology Laboratory, NIST (National Institute of Standards and Technology), October 2009. Availableahttp://csrc.nist.gov/groups/SNS/cloud-computing/.

[8]. Alwen, J., Dodis, Y., Wichs, D.: Leakage-resilient public-key cryptography in the bounded-retrieval model. In: CRYPTO. pp. 36–54 (2009)

[9] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[11] Cremers, C.: Examining indistinguishability-based security models for key exchange protocols: the case of ck, ck-hmqv, and eck. In: ASIACCS, 2011. pp. 80–91 (2011)

[12] Ronald L. Krutz, Russell Dean Vines "Cloud SecurityA Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc.,2010