ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 3, Issue 2 (Apr. - Jun. 2015)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)

Nested Testimony Model to Access Cloud Data

[I]Avinash Kumar, [II]S. Aravinth Kumar, [III]Akhil Kumar Tripathi
[I,III]M.Tech, Dept. of SCSE, Galgotias University, Greater Noida, India
[II]Asst. Professor, Dept. of SCSE, Galgotias University, Greater Noida, India

Abstract
In the era of Internet, we are continuously relying on online file storage system to back up our data. As we are demanding more online storage, we are also inviting some security breaches. This online storage has emerged as a Utility Computing known as the Cloud Computing. This is a concept of remote access of the system which consequently results in the least use of Client's resource for computation or storage. There are various algorithms and methods available for securing data over the cloud. In this paper, I seek to explain the current research associated to data security like integrity and confidentiality. Precisely, the paper focuses on securing client in the cloud Services.

Keywords
Kerberos; RSA; Hybrid Implementation.

I. Introduction

Cloud is widely used current generation technology. The term cloud has been used historically as a metaphor for the Internet [1]. The cloud sees no borders and thus has made the word a much smaller place. It has pervaded in the field of computations. Globalization of computing assets is the most precious gift the cloud has given in the technological field till date. It is an internet based service where QoS (Quality of Service) is a vital entity to be delivered to the Cloud User. Like Grid Computing, The cloud has one most salient feature that is "On Demand" or "Pay-per-Use" [1].

A. Cloud Based Offerings:

SaaS (Software-as-a-Service): SaaS is one of the services of cloud that help user to access applications using web-browsers. Its emphasis is on the End-Users rather than Managed Services. This results an axiom which depicts SaaS as a paradigm where data is stored in a remote system or server and it is accessed via internet. The data is cached on client system like desktop, notebook, mobile phones, etc.

CaaS (Communication-as-a-Service): CaaS is an outsourced business concept which provides solution for communication enterprise. This service of cloud is liable for managing hardware and software needed to deliver Voiceover IP Services, Instant Messaging, and Video Conferencing capabilities to their customers [1]. It helps to selectively deploy communication features and services on pay-as-you-go basis to the users.

IaaS (Infrastructure-as-a-Service): It deals with the delivery of computing infrastructure as a service. It acts by platform virtualization environment as a service. It delivers service on predefined, standardized infrastructure which is specifically optimised for the applications of the customer. The user of IaaS can access the application on custom based.

MaaS (Monitoring-as-a-Service): MaaS is an outsourced service for security. It anchorage the business platform that uses internet. By the influence of online storage of data, the MaaS has evolved as one of the most important Service to protect user form cyber threat and ensure confidentiality, reliability and availability of IT assets. Various companies and organisations use this service to monitor server logs, security domains and many other important informative data to ensure integrity of these systems.

PaaS (platform-as-a-Service): PaaS is the outsourced delivery of platform as a service. It is used for developing and running customised web-applications. PaaS is protuberance of SaaS service offering. It supports the cycle for developing applications without software downloads or installation for end users.

B. Cloud composition

Cloud computing typically uses hardware and software as a computing resource for delivering various services over internet [2]. Cloud is used as a remote storage and as backup for various data and information that can be retrieved in future.

C. Examples of Cloud Computing

Amazon, G Space, Google Cloud, AT&T, Salesforce.com, Hadoop, GoGrid, Microsoft (Azure), NetSute, Rackspace Cloud, Enomaly, RightScale.

The storage of data over cloud comes at greater risks. Confidentiality, Integrity, Write-Serializability and Read Freshness are the most important desirable properties of Cloud Service. There are many reasons for the security breach in the cloud service, like bugs in the system, crashes of the OS, operator errors, system's misconfiguration. The other reason could be the disloyalty of employee of the Cloud Service provider.

II. Discussion

A. Problem Statement

The cloud Service provider focuses on two main challenges while dealing with their customers. The one regarding confidentiality and reliability of the data and other regarding access of the service.

B. Techniques

a) Encryption: The use of encryption algorithms to hide the important data using the Encryption Key
b) Authentication Process: The implementation of creating Username and Password for the User.
c) Authorization Practice: The log containing the information of the User who can access the data stored on the cloud.

C. Methodology Proposed

a) Kerberos: Mutual Authentication Process.
b) RSA: Ron Rivest, Adi Shamir and Leonard Adleman.
c) Hybrid Implementation.

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

1) Kerberos Mutual Authentication Process Implementation
Kerberos is an authentication protocol over network. It is a mutual authentication process which involves both Client and Server. It provides strong authentication process using secret key cryptography. It uses session key which helps encrypted data stream over IP network for each user [2]. A new user on the network needs to create its profile using attributes like user_id and hashed password will be saved on the database. Each user has its own id and password in the system.

Steps for Kerberos Implementations [2]:
Log on to workstation.
Send the request for ticket granting ticket to the AS.
AS verifies user's access right in database, create ticket-granting ticket and session key. Results are encrypted using key derived from user password.
User will send the request cloud service granting ticket to TGS.
TGS will send the Ticket+session key to the user.
Workstation sends ticket and authenticator to cloud server provider.
Server verifies ticket and authenticator match, then grant access to service.
However Kerberos alone might not be able to secure the authentication process properly. We might use RSA for encryption of session key used in the Kerberos encryption technique. The RSA is an asymmetric key based technique which uses two types of keys, the Public Key and the Private Key.

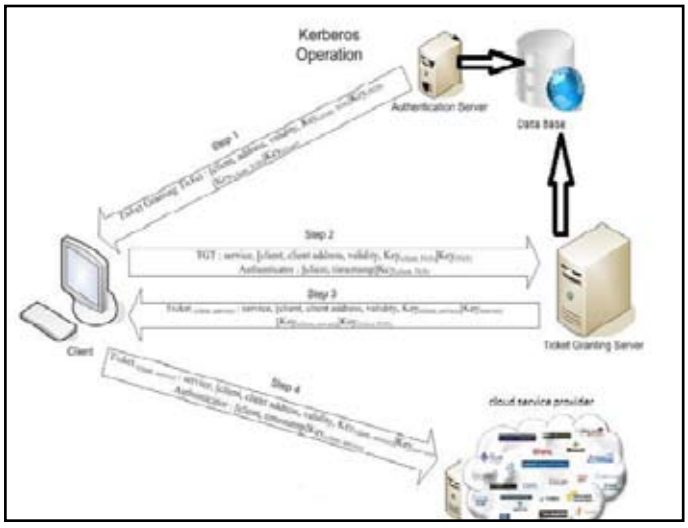

Fig. Kerberos Implementation in Cloud.

2) RSA
RSA uses concept of two keys known as public key and a private key. The public key is used for encryption. The information encrypted using the Public Key is being decrypted using the Private Key in reasonable time-period. The keys for the RSA algorithm are generated in the following manner:
Firstly, two different prime numbers, p and q are selected.
For security purposes, random selection of integer p and q is done, each integer having equal bit length. Prime integers can be efficiently found using a primality test [7].

a) Compute n = pq.
n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

b) Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n - (p + q - 1)$, where φ is Euler's totient function.

c) Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and φ(n) are coprime.

- *e* is released as the public key exponent.
- *e* having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65,537$. However, much smaller values of *e* (such as 3) have been shown to be less secure in some settings.

d) Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the multiplicative inverse of e (modulo φ(n)).

- This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$
- This is often computed using the extended Euclidean algorithm. Using the pseudocode in the Modular integers section, inputs a and n correspond to *e* and φ(n), respectively.
- d is kept as the private key exponent.

The public key consists of the modulus *n* and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.

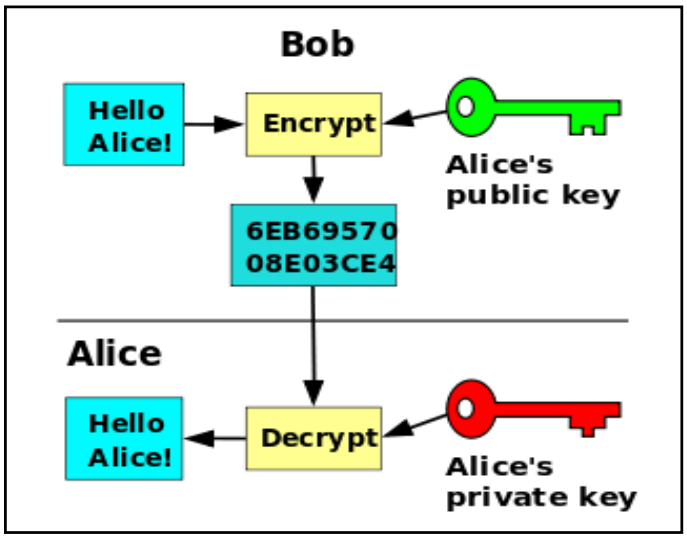

Fig: RSA

3) Hybrid Implementation
The RSA discussed above can be used to generate the session key of the Kerberos mutual authentication process. The session key can be obtained by the hacker to be used in the Cloud service but, the RSA will increase the time to the get the session key. Due this, the authentication time for cloud for the Kerberos will expire and hence the obtained session key will be of no use.

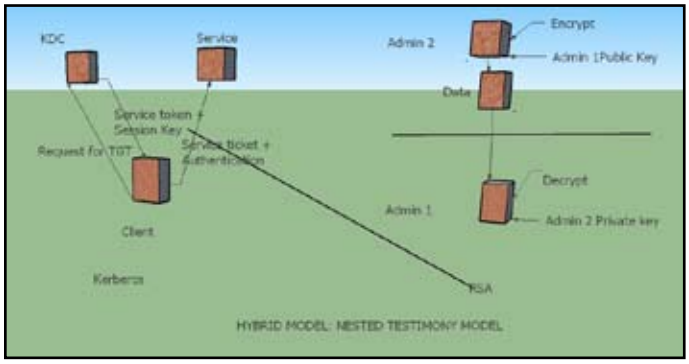

Fig: Hybrid Model

III. Conclusion

The proposed authentication methodologies which shows a hybrid implementation of symmetric and asymmetric key cryptography system is one of the solution for developing a complex system for the authentication process.

Reference

[1] *John W. Rittinghouse, James F. Ransome, "Cloud Computing Implementation, Management, and Security, CRC Press*

[2] *Sunita Sharma, Amit Chugh, "Survey Paper on Cloud Storage Security, " International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 2, April 2013*

[3] *Anup Mathew, "Survey Paper on Security & Privacy Issues in Cloud Storage Systems", EECE 571B, Term Survey Paper, April 2012*

[4] *Kalyani Kadam, Rahul Paikrao, Ambika Pawar, "Survey on Cloud Computing Security", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 12, December 2013)*

[5] *Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham "Security Issues for Cloud Computing," International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010*

[6] *Mladen A. Vouk," Cloud Computing – Issues, Research and Implementations," Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246 doi:10.2498/cit.1001391*

[7] *Rajan.S.Jamgekar, Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA," International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013.*