Security issues occur in Cloud Computing and there Solutions

Karamjit Singh
Department of CSE
PEC University
Chandigarh, India
11421karam@gmail.com

Isha Kharbanda
National institute of electronics and information technology
New Delhi India
Ishakharbanda2@gmail.com

Navdeep Kaur
Department of CSE
PEC University,
Chandigarh, India
aulakh83@gmail.com

***Abstract* - Cloud computing is a recent advancement wherein IT infrastructure and applications are provided as "services" to end-users under a usage-based payment model. Many organizations, such as Google, Amazon, IBM and many others, accelerate their paces in developing Cloud computing systems and providing services to user with best affords but there phases many difficulties regarding security problem and users also afraid toward security of own data i.e. whether cloud providers able to maintain data integrity ,confidentiality as well as authentication.**

To resolve the security issues in cloud computing, this paper presents various solutions for different issues.

Keywords: Cloud Computing, Cloud Security, IaaS, Public Key Cryptography, Digital Signature.

I. INTRODUCTION

Cloud computing provides computation, software applications, data access, data management and storage resources without requiring cloud users to know the location and other details of the computing infrastructure. Cloud computing providers offer their services according to three fundamental models: Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

Software as a service, Leverages the Cloud in software architecture, Eliminates the need to install and run the application on the customer's own computer.

Platform as Service, Delivers a computing platform and/or solution stack as a service, Facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers.
Infrastructure as Service, In the "cloud", all data processing tasks are handled by a large number of distributed computers, end-users get access to the computer and storage systems through network on their demand.

Public Key Cryptography (PKI): Fundamental or core, security services associated with a PKI.
PKI is generally considered to be associated with three primary services:

- Authentication is the assurance to one entity that another entity is who he, she, or it claims to be.
- Integrity is the assurance to an entity that data has not been altered (intentionally or unintentionally) between "there" and "here" or between "then" and "now." Data integrity is the assurance of no alteration: The data (either in transit or in storage) has not been undetectably altered. Clearly, such assurance is essential in any kind of business or electronic commerce environment
- Confidentiality is the assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.

Digital certificate is a digital form of identification, much like a passport or driver's license. A digital certificate is a digital credential that provides information about the identity of an entity as well as other supporting information. Digital certificates provide support for public key cryptography, because digital certificates contain the public key of the entity identified in the certificate.
Public Key Cryptography and Digital Signatures: The relationship of a public key to a user's private key allows a recipient to authenticate and validate a sender's message. Digital certificates provide support to public key cryptography by providing a reliable means to distribute and access public keys. When a user is signing a message, the user provides the private key that is associated with the public key available on the digital certificate. In turn, when the recipient is validating a digital signature on a message.

II. ISSUES IN CLOUD COMPUTING

Various issues occur in cloud computing regarding data security as following:-

How cloud provider will provides authentication and integrity over user's data.

How cloud provider able to protect stored users data in cloud storage servers form attackers. And how to protect private data from access of hackers whose aim is to hack the servers for access over private data.

How cloud users able to change cloud provider and transfer stored data from one cloud provider to another, example: Suppose users 'A' cloud provider is Google and after some years user A is not comfortable with Google cloud provider and want to shift to Amazon (another cloud provider) then how user A is able to shifting data which stored at Google cloud provider to Amazon.

Above described issues cause major problems in Cloud Computing regarding storage and security of data. These some security related issues will cause fear in mind of user that is cloud provider will able to handle data properly and in secure manner. If cloud provider will not be able to handle data secure then, this will make effect on users by losing trust on cloud provider.

In next section, Solution of all mentioned issues which cause storage and security of data relates problem.

III. DIFFERENT SOLUTIONS FOR SOLVING DIFFERENT ISSUES

To resolve problem regarding authentication and integrity in cloud computing over users data implement Public key cryptography over cloud is best answer.

When transmission of data occurs between users and cloud then a lot of problems occurs due to an attackers or unauthorized users access.

To solve data security related problems cloud provider must use the public key cryptography concepts.

To achieve authentication over data, cloud providers enable user's authentication via assigning blocking window through which users must pass by giving username/password after that if user pass authentication then he/she can access data.

Another problem related to data integrity security, if during transmission attacker changes information i.e. integrity problem, then how user as well as cloud provider will detect change in information.

To resolve this problem cloud provider must implement concept of public key cryptography that is Digital Signature [6].

When users send data over cloud and extract data from cloud then must use digital signature over data.

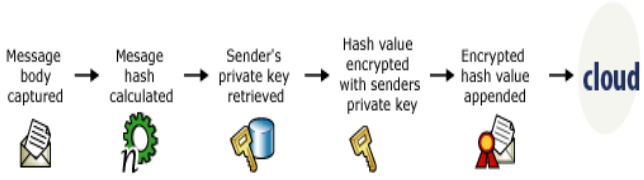

Fig 1. Process to achieve data integrity

Suppose a user 'A' want to store data on cloud by achieving data integrity. To achieve data integrity during transmission of data, user first calculate hash value of message then user will retrieve own private key and encrypt hash value which was calculate from message and after that encrypted hash value will append with message and send to cloud.

When any attacker will make changes in data during transmission then on cloud side when cloud provider will calculate hash over data/message then calculated hash by cloud will not match with appended hash then automatically cloud will not accept that data and will send query for retransmission of previous data. Same procedure will be held on when user will extract data from cloud. In this case cloud will send data to user by calculating hash and encrypt it with private key of cloud provider and user will match appended hash with message and users' calculated hash. By this method both users and cloud provider will able to detect whether data integrity is lose or not.

Second issue, how cloud provider able to protect stored users data in cloud storage servers form attackers.

This problem can be protected by applying strong barrier over cloud storage servers i.e. apply firewall over servers and intrusion detection system to detect unconscious activity from the side of unauthorized servers and attackers. User's separation access over servers, this can be done by applying separation of stored data over servers according to users requirement.

There will be two cases: first when users want to store data over server for its own use only and second if users want to store data over cloud which can be access by other authorized user. These both type of users data will store on separate servers and these servers will not have any connection.

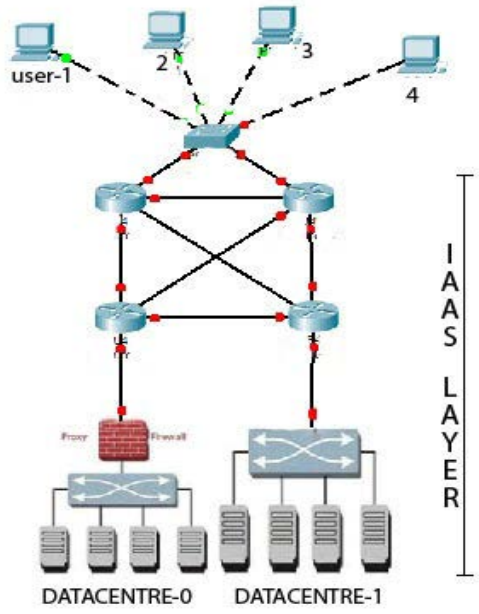

Fig. 2 Architecture to secure user's private data at IAAS

When user want to store data over cloud for its own use only, then connection from outside to cloud servers will not be directly with cloud data server, there must be placement of a proxy firewall to avoid direct connections with internal servers of cloud on which private data of users will store. This will hide ip addresses of internal servers by which servers can be protected from hackers. By this way cloud provider can protect user's private data.
Let us suppose there are four users form which user-1 and user-3 want to store data with more privacy and for their own user only then those users' data will be stored in datacenter-0 and other user whose data will not be much more private and access by other authenticated users will be stored in datacenter-1.

TABLE 1- Cost of cloud storage as per security requirement:

User ID	Data Centre	Cloudlets (Task)	Time	Debt.
1	0	1	160	45.6

2	1	1	160	35.6
3	0	2	160	91.2
4	1	2	160	71.2

To achieve more security, users must have to pay more in above example user-1 and user-3 will pay more than others. Increment in investment to achieve security will be depends upon cost per storage and access time over resources.

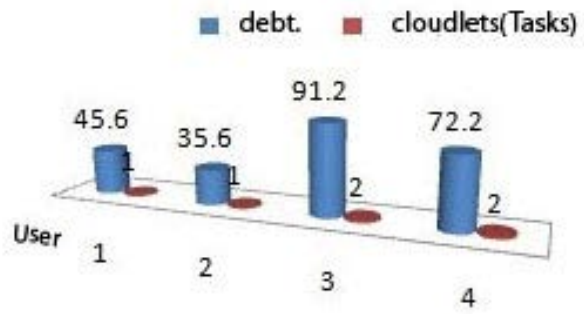

Fig 3: Chat between Users, Debt. And Cloudlet (task)

Third issue in cloud computing, how cloud users able to change cloud provider and transfer stored data from one cloud provider to another.

This problem can be solving by only when cloud providers will ready to maintaining trust relationship between different cloud providers. An entity (cloud provider) can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects [1]. When cloud provider will maintain trust relationship between each other then users will be able to transfer data from one cloud provider to other.

IV. CONCLUSIONS

This Paper represents different security issues which are occur in cloud computing and provide solutions how to make data secure from unauthorized users and to check data integrity during transmission of data from cloud to users and vice versa and how to secure private data over Server. This paper represent with the help public key cryptography, Digital Signature and better network design, we can protect user's private data and enable users to change cloud provider with transferring data form one cloud to another.

REFERENCES

[1] Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition By Carlisle Adams, Steve Lloyd.
[2] B. Hayes, "Cloud computing," *Communications of the ACM*, vol. 51, no. 7, pp. 9–11, 2008.
[3] Sahai and B. Waters, "Fuzzy identity-based encryption," *Advances in Cryptology-EUROCRYPT 2005*, pp. 457–473, 2005.
[4] Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems Harley Kozushko Thursday, September 11, 2003 Independent Study.
[5] Liazhu Dai and QinZhou, A PKI-based Mechanism for Secure and Efficient Access to Outsourced Data, 201O International Conference on Networking and Digital Society 640-643
[6] William Stallings: Cryptography and Network Security [book style].
[7] CloudSim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms by Rodrigo N. Calheiros1, Rajiv Ranjan, Anton Beloglazov1, César A. F. De Rose3, and Rajkumar Buyya.

AUTHORS PROFILE

I am Karamjit Singh. I had done my bechlor degree from Beant collage of engg and technology,gurdaspur in Computer Science and Engg. and Master of Engg. from PEC Univeersity, Chandigarh,India in department of CSE with Specialization in Information Security. My fields of interest are in Cloud Computing ,Cloud Security, Network Security and Public Key Infrastructure.

I am Isha Kharbanda.I had recieved bechlor degree as well as Master degree in Computer Application from Punjab Technical University, Jalandhar. I had also done B-Level from national institute of electronics and information technology,Delhi,India.My fields of interest are in Cloud Computing ,Cloud Security, Computer Network and DBMS.

Navdeep Kaur received bachelor from Lala Lajpat Rai Institute of Engineering and Technology,India and M.E from ThaperUniversity Patiala, India. My research interests include network security and privacy, and cloud computing security, DBMS.