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

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

Security for cloud computing data using a security cloud as a Third party auditor (TPA): A Survey

Ankit R. Mune[1], P. R. Pardhi[2]

M Tech Scholar, Department of Computer Science, RCOEM, Nagpur, India [1]

Professor, Department of Computer Science, RCOEM, Nagpur, India [2]

Abstract: Cloud computing is considered next generation architecture of IT Enterprise for computing. Cloud is nothing but the internet. Last 10 year ago peoples store their Credential data in data centre with firewall and used various security techniques used for protect the data but day by day the peoples data is increase and storing space is not enough for data storage since the data is stored anywhere across the global, the client organization have less control over the stored data. To build the trust for the growth of cloud computing the cloud providers must protect the user data from unauthorized access. For this one technique could be encrypting data on client side before store but in this technique burden for client is too much increase just like encrypting and decrypting data. Another techniques could be security services like computing hash, encryption/decryption service if provide for same cloud storage provider. We provide two cloud one for encryption and decryption namely Trusted third party which will provide security services and second one is for only storage. The software is only responsible for Encryption/decryption, computing/verifying Hash of data and does not store any data in trusted third party that is security cloud.

Keywords: Cloud computing, Encryption/decryption service (TPA), Hash service for Data verification and integrity check.

I. INTRODUCTION

In recent years, cloud computing fig 1 has become a hot topic in the global technology industry. The initiatives include Google's research project for building an infrastructure to support research needs of top-tier American universities. Weiss noted that cloud computing services include several existing computing technologies, such as service-oriented utility computing, grid computing with large amount of computing resources, and that using data centers for data storage services[1].

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centres into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centres[2]

Prior to the development of the concept of cloud computing Fig 1 critical industrial data was stored internally on storage media, protected by security measures including firewalls to prevent external access to the data and including organizational regulations to prohibit unauthorized internal access. In the cloud computing environment, storage service providers must have in place data security practices to ensure that their clients' data is safe from unauthorized access and disclosure. More importantly, the regulations and measures for preventing privileged users such as system administrators from unauthorized access must be rigorously established and implemented.[1]

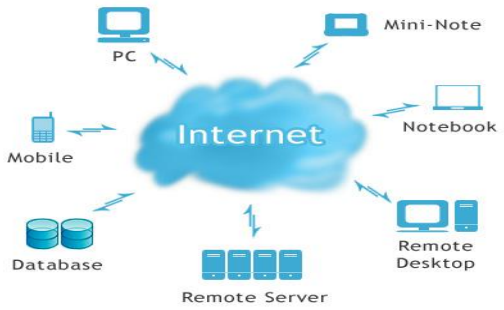


Fig.1 Cloud computing

A Simple approach for system to protect user data is that data of user is encrypted before it stored. In a cloud computing environment, a user's data can also be stored following additional encryption, but if the storage and encryption of a given user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and authorized staff) can use their decryption keys and internal access privileges to access user data. From the user's perspective, this could put his stored data at risk of unauthorized disclosure.[1]

Creating user trust through the protection of user's data content is the key to the widespread acceptance of the cloud computing. This study proposes a model for cloud computing based on the concept of using a separate encryption and decryption service [1] that is called Third

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

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

party auditor fig 2. In the model, data storage and decryption of user data are provided separately by two different service providers. In addition, those working with the data storage system will have no access to decrypted user data, and those working with user data encryption and decryption will delete all encrypted and decrypted user data after transferring the encrypted data to the system of the data storage service provider.[1][5]

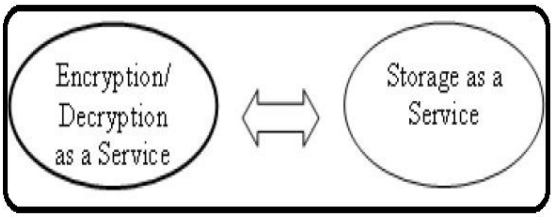


Fig. 2 Both Cloud services

Under this model the data storage cloud system provider is authorized to store the user's encrypted data, but does not have access to the Decryption Key. Thus, the storage system can only retrieve encrypted user data, but is unable to decrypt it. The cloud computing system responsible for encrypting user data has authority over all encryption keys required for data encryption but, given that the encryption provider does not store the user's data, Given that encryption is an independent cloud computing service which is a TPA, a unique feature of the model is that different services are provided by multiple operators. For example, the "Encryption as a Service "provider and the "Storage as a Service" provider cooperate to provide a Cloud Storage System with effective data protection refer fig. 2

II. CLOUD COMPUTING

The term cloud has been used historically as a metaphor for the Internet. This usage was originally derived from its common depiction in network diagrams as an outline of a cloud, used to represent the transport of data across carrier backbones (which owned the cloud) to an endpoint location on the other side of the cloud. This concept dates back as early as 1961,when Professor John McCarthy suggested that computer time-sharing technology might lead to a future where computing power and even specific applications might be sold through a utility-type business model. This idea became very popular in the late 1960s, but by the mid-1970s the idea faded away when it became clear that the IT-related technologies of the day were unable to sustain such a futuristic computing model. However, since the turn of the millennium, the concept has been revitalized. It was during this time of revitalization that the term cloud computing began to emerge in technology circles.[8]

III. LAYERS OF CLOUDS

A. Infrastructure-as-a-Service(IaaS)—the Infrastructure services layer:

In the case of IaaS, servers, network devices, and storage disks are made available to organizations as services on a need-to basis. Virtualization (a software technology that uses a physical resource such as a server and divides it up into virtual resources called Virtual Machines—VMs), allows IaaS providers to offer almost unlimited instances of servers to clients, while making cost-effective use of the hosting hardware. Companies can use IaaS to build new versions of applications or environments without having to invest in physical IT assets. Increasingly, organizations are using IaaS to host their websites, monitor their traffic and keep them running 24x7, without hogging up internal IT resources. IaaS is particularly beneficial for micro-, small and medium-sized businesses that can access server and storage systems, which they would otherwise have to purchase. Microsoft has been offering IaaS services, either through its own infrastructure or that of its partners.[9]

B. Platform-as-a-Service (PaaS)—the Platform layer:

This layer provides a platform for creating applications. PaaS solutions are essentially development platforms for which the development tool itself is hosted in the Cloud and accessed through a browser. With PaaS, developers can build Web applications without installing any tools on their computers and then deploy those applications without any specialized systems administration skills. Today, PaaS is being delivered like a utility say, water or electricity over the Internet, with ISVs and corporate IT departments, paying according to usage. Owing to PaaS, there has been a jump in the number of people who can develop, maintain and deploy web-based applications without requiring specialized expertise. An example of PaaS is Microsoft's Azure, which the company is providing as a cutting-edge cloud-based platform on which applications can be built.[9]

Fig. 3 Layers of clouds

C. Software-as-a-Service (SaaS)—the Application layer:

This layer includes applications that run off the Cloud and are available to Web users or enterprises on a pay-as-you-go, anytime-anywhere basis. Microsoft's Online Services are an example of SaaS for the enterprise. The Cloud, apart from its different layers, is also visible through three variants. There are the public Clouds for instance, a deployment option for enterprises where the infrastructure services are provided by a hosting partner. It is this third party vendor that hosts and manages these offerings. The other version is the private Cloud, where it is deployed within the enterprise and managed and maintained by the

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

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

organization itself. A private cloud is a collection of virtualized infrastructure fabrics that are coupled with automated management. It is deeply integrated with the application platform and identity, protection and access technologies to create an internal service-oriented environment for enterprises. Although the private cloud does not offer the Capex to Opex advantage, with the hypervisor capability becoming integral to the operating system (e.g. Hyper-v within Windows Server 2008 R2), it is becoming increasingly affordable for enterprises. A more recent, architecturally new concept in Cloud computing is the hybrid Cloud, which is a blend of the public and private Cloud. The hybrid Cloud, created by the enterprise, can leverage the benefits provided by both public and private Clouds. However, issues related to the sharing of responsibilities between the enterprise and the third party vendor and governing such a Cloud, make it a slightly complex deployment option.[9]

IV. DEPLOYMENT MODES IN CLOUD

There are four types of cloud available in cloud computing i.e. private cloud, public cloud, hybrid cloud and community cloud.

A) Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units).[10] It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.[6]

B) Public cloud: The cloud infrastructure is provisioned for open use by the general public. [10] It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider [6].

C) Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations) [6]. It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

D) Hybrid cloud: Hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that will be unique entities, but bound together by standardized technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds) [6],[10].

V. PROBLEM STATEMENT FOR SYSTEM

The user is always concern about data security, data integrity, and sharing data with specific band of men and women must be addressed. You will find multiple means of achieving this, example encrypting data on client machine and then storing to cloud storage server, computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific people. Therefore it becomes more tedious for client to keep these information and share such information, more over in the event the device which stores such information is lost or stolen it pose a threat to the total data. Another way could be same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, but since administrative can have use of both services for maintenance, the security service provided by the cloud storage provider, the information might be compromised. Therefore mentioned approaches burdens the client by which makes it additionally accountable for securing it data before storing it to the cloud storage.

VI. RELATED WORKS OF CLOUD TPA

In recent year cloud is very good for storing data. But also some problem are very effective in that to destroy the security. Now a days on clouds various attacks are coming for destroy the security mechanism of cloud computing. Form that many of design some system for protect data on cloud but this all are fail because of their various small drawbacks. In previous systems Scenario is First when user want to store data on the Cloud at that time. User was send the confidential data to TPA then TPA will encrypt the data by using algorithms and then it will send the data to Cloud service provider for storage. As from above approach data was stored in CSP in encrypted format but the drawbacks for the system is that when data was go to TPA, TPA will encrypt the data and send but not delete from there database means TPA can see the User data so the system is fail.

VII. PROPOSE APPROACH FOR SYSTEM

In our propose approach we remove the drawbacks of previous approach such as, Three different network entities can be identified as follows

A) User: User is an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations. Also he is totally responsible for storage data.

B) Third Party Auditor (TPA) or security cloud: TPA is an entity, which has expertise and capabilities for Encryption and decryption Service. When client want to store data at the cloud storage at that time TPA (encryption/decryption service) Encrypt the data and return back to user for storage purpose.

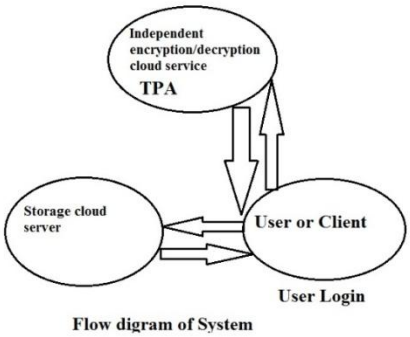
C) Cloud Storage Server (CSS): CSS is an entity which is totally responsible for storage the data. After encrypting your data if you want to store the data on cloud Storage server[7].

In the whole scenario When we user want to store confidential data to cloud for storage. But now a days peoples do not trust on cloud for storage because for leakage of data from cloud. For that we make a system for

secure data storage in cloud. For remove the drawbacks for previous model we design this security services when data is encrypted at that nobody can intact the data. This scenario has been divided in two parts

A) Data upload scenario:

First end user login with his user name and password if he is authenticate user at that time by using deffie hellman[4],[5] key is exchange for that session and user calculate the SHA value for the data for integrity purpose user will calculate the SHA value by using SHA-512 After that user select which data(any file) is to be store on cloud side now user encrypt the data by using DH keys and send to the security cloud(TPA).Now TPA will decrypt data by using DH keys and Encrypt by using AES algorithm[3] and stored the Master key of AES for that user for decryption process and TPA will send Data to the user for store to the storage cloud side and also TPA(security cloud) will delete data from TPA side only stored master key of AES of each user.



Flow digram of System

Fig.4 Flow diagram of system

B) Data Download scenario:

Data download scenario is reversed scenario of data upload scenario when user want his data from storage cloud at that time he request to storage cloud for data back once he will get data from storage cloud he want to access the data but the data is in encrypted form for the data decryption process we will have to send data to security cloud. When we send the encrypted data to security cloud it will decrypt the data by using AES [3] Master Key which will be stored in the Security cloud. Again for security purpose TPA will encrypt the data by using DH [4],[5] keys and send to user. At last user will decrypt the data by using DH[4]keys. For check the data integrity User will check the data by using the SHA-512 and he will match the Previous SHA value with this. If the SHA value match your data integrity is good means nobody Hack your data in security cloud as well as Storage cloud.

VIII. CONCLUSION

In this paper, a survey of TPA in cloud computing for secure the data is presented. Cloud computing include three types of service: infrastructure, platform and software. In which we presented a two cloud system security cloud system for encryption and decryption and storage cloud system for data storage. TPA (security cloud) is a very good system for cloud security system use for to encrypt and decrypt the data of user's and another cloud service which is only use for to store the encrypted data. When we use two different cloud system for whole process so there is no chances to leak or hack our data. Hence we provide two different cloud system for user's data so this system is beneficial than the previous one.

ACKNOWLEDGMENT

I express my sincere gratitude to Dr. M. B. Chandak, Head Department of CSE, for his valuable guidance and advice. Also I would like to thanks to my guide Prof. P .R. Pardhi and the faculty members for their continuous support and encouragement.

REFERENCES

[1] Jing-Jang Hwang, Hung-Kai Chuang,Yi-Chang Hsu, Chien-Hsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," Proceedings of the 2011 International Conference on Information Science and Application, April 2011.

[2] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou," Ensuring Data Storage Security in Cloud Computing"

[3] Avi Kak Lecture 8: AES: The Advanced Encryption Standard Lecture Notes on "Computer and Network Security"

[4] Dieter Gollmann (2006). Computer Security Second Edition West Sussex, England: John Wiley & Sons,Ltd.

[5] Williamson, August 10, 1976. Diffie, W.; Hellman, M. (1976). "New directions in cryptography"(http://www-ee.stanford.edu/%7Ehellman/publications/24.pdf). IEEE Transactions on Information Theory 22 (6):644–654. doi:10.1109/TIT.1976.1055638 (http://dx.doi.org/10.1109%2FTIT.1976.1055638).

[6] Bhavna Makhija, VinitKumar Gupta, Indrajit Rajput,"Enhanced Data Security in Cloud Computing with Third Party Auditor" proceeding of the , February 2013 International Journal of Advanced Research in Computer Science and Software Engineering.

[7] Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Wenjing Lou, Senior Member, IEEE, and Jin Li" Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing"

[8] John W. Rittinghouse,James F. Ransome © 2010 by Taylor and Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informa business" Cloud Computing Implementation, Management, and Security"

[9] http://www.microsoft.com/india/msindia/perspective/interfaces_cloud_three_layers.aspx

[10] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou,‖ Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing‖ in IEEE INFOCOM 2010, San Diego, CA, March 2010.

[11] Ashish Bhagat,Ravi Kant Sahu "Using Third Party Auditor for Cloud Data Security: A Review" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 3, March 2011