Cloud Security Using Authentication And File Base Encryption

Fadadu Chirag[#1], Shrikanth Venkatesh[#2], Trivedi Harshal[#3]

[#1#2] Information Technology Department,

Parul Institute of Engineering & Technology, Vadodara, Gujarat, India.

[#3] Computer Engineering Department

Vinus International College of Technology, Gandhinagar, Gujarat, India.

Abstract:-Nowadays cloud computing word become famous in IT field, where user can store their data online and access any time and any where according to their requirement. World's giant companies Amazon, Google and Microsoft provide cloud services to their customers. Although there are many advantages of cloud computing but some business-critical applications, especially large enterprises, still less trusted on cloud and wouldn't move their data on cloud because of security concerns. However, privacy and security issues become strong barrier for user to accept cloud computing system. This paper briefly introduced about cloud computing and its key terms. In particularly, we intend to discuss cloud security requirement and data privacy issues. We proposed encryption technique like SHA encryption algorithm to provide data privacy and security in the cloud. Also provide some authentication for storage data within cloud.

***Keyword*: Cloud Security, Authentication, Encryption.**

I. INTRODUCTION

Cloud Computing means "internet computing", internet is seen as collection of clouds and cloud computing enables consumers to access resources online from anywhere any time without worrying about physical/technical issues of resources. User only need high speed internet to enjoying cloud services. Google apps and yahoo mail are best example of cloud computing services. Cloud computing is a new computing model that will interconnect the large-scale computing resources to effectively integrate, and to computing resources as a service to users. Users can use the broadband network at any time on demand access to virtual computers and storage systems, without the need to consider the complexities of the underlying implementation and management, greatly reducing the difficulty and hardware to achieve the user's investment. Cloud computing effectively the actual separation of physical and virtual services, a variety of business services reduced costs, improved utilization of network resources[1].

Cloud computing is widely used concept. Nowadays many organizations especially small as well as medium business enterprise get benefit by moving their data and applications in to the cloud. The adoption of cloud computing may increases Efficiency and Effectiveness in developing and deployment. Cloud Computing also help to save the cost in purchasing and maintaining the infrastructure. Cloud computing is cheaper than other computing services ,less maintenance cost, only involves application charges which is used by user.

Once creation of a cloud, Deployment of cloud computing differs with according to user requirements and their need. The principal service models being deployed are:

Software as a Service (SaaS): Software‘s are provided as a service to the consumers according to their requirement, enables consumers to use the services that are hosted on the cloud server.

Platform as a Service (PaaS): Clients are provided platforms access, which enables them to put their own customized software‘s and other applications on the clouds.

Infrastructure as a Service (IaaS): Rent processing, storage, network capacity, and other basic computing resources are granted, enables consumers to manage the operating systems, applications, storage, and network connectivity[2].

However there are still exit many problems in cloud computing today, according to recent survey some problems like data privacy, security and data integrity are primary concern for user to accept cloud computing technology.

Although cloud computing service providers touted the security and reliability of their services, actual deployment of cloud computing services is not as safe and reliable as they claim. In 2009, the major cloud computing vendors successively appeared several accidents. Amazon's Simple Storage Service was interrupted twice in February and July 2009. This accident resulted in some network sites relying on a single type of storage service were forced to a standstill. In March 2009, security vulnerabilities in Google Docs even led to serious leakage of user private information. Google Gmail also appeared a global failure up to 4 hours [3].

Our authentication and encryption technique are help to more secure user data within a cloud so user can trust on their data security. In authentication technique we provide secure authentication of user data like first user login cloud with user name and password .Once user access application or store their data on cloud again we provide file authentication like file delete, modify, copy or any other access can’t be done

Without user permission(another user id or password). This type of authentication help user for more security of data.

Our proposed encryption algorithm provide user side file encryption in that when user upload file at that time file is encrypt and then store in to the cloud. We except that our encryption algorithm provide more security of user data. Without worrying about security issue more and more user can move their data on cloud and enjoying cloud storage service.

II. RELATED WORK

There are various encryption algorithms used in cloud computing for user data privacy and security. One of technique of user data security is TPA (Third Party Auditor) between client and cloud service provider, which acts as external auditor to audit the user outsource data. This scheme provides secure and efficient dynamic operations (data update, delete and append) on data blocks stored in the cloud [4]. But what happen when data is transfer from user to cloud, there is no mechanism for security between user and cloud.

Another technique IBE is a form of public key cryptography in which a third party server uses a simple identifier, such as an e-mail address, to generate a public key that can be used for encrypting and decrypting electronic messages. Compared with typical public key cryptography, this greatly reduces the complexity of the encryption process for both users and administrators [5].

Suppose a user wants to login to a secured cloud system. To login into a system we must provide a correct combination of user name and password and it should be matched with the combination stored in the database whether in plaintext form or in encrypted form. For a secured login user provide login credentials and then to authenticate the user system encrypts the provided password up to the number of times defined to the system [6]. Above technique is only for secure user id and password but this technique is not use in user data which is stored by user in to the cloud. So our proposed algorithms provide encryption of user data by performing encryption technique and transfer user data in encrypted form from user to cloud.

There are various authentication technique used in cloud computing nowadays like multi dimensional password, user identity and all other technique. We provide some file authentications that improves more security of user data. Some authentication techniques like file can't delete , copy or modify by any third party even administrator.

III. PROBLEMS UNREVEALED

There are various encryption algorithms working on cloud for user data encryption. User data is stored in encrypted form in the cloud but when data is transfer from user side to cloud then data is not in encrypted form so our encryption algorithm provide user side data encryption and also provide encryption key to user so only user can access the data. When user want to retrieve their data file is pass through decryption algorithm.

There are many authentication to access the cloud but there are less authentication to the file so we provide file authentication from user side that file is only copy, delete or modify by user. Above parameter is not consider by cloud provider for user data security. This algorithm helps to improve user data security in to the cloud.

IV. PROPOSED ARCHITECTURE

User :

Users are the cloud users who are access the services of the cloud.

Encryption tool:

Encryption tool is used to encrypt the user file. When user want to store their file in to the cloud first file is upload by user then file is directly pass through encryption tool where file is encrypted and then go to virtual machines (VMs).

Cloud controller server:

The Cloud Controller Server (CLS) is the front end to the entire cloud infrastructure. CLS provides web service interface to the client tools on one side and interacts with the rest of the components of the eucalyptus infrastructure on the other side. CLS also provides a web interface to users for managing certain aspects of the cloud infrastructure.

Node controller server:

A node controller server (NCS) is a virtual extension (VT) server. Node controller server runs on each node and controls the life cycle of instances running on the node. The NCS interacts with the OS running on the node on one side and the cloud controller on the other side.

The figure given below shows the proposed model of cloud for user side file encryption.

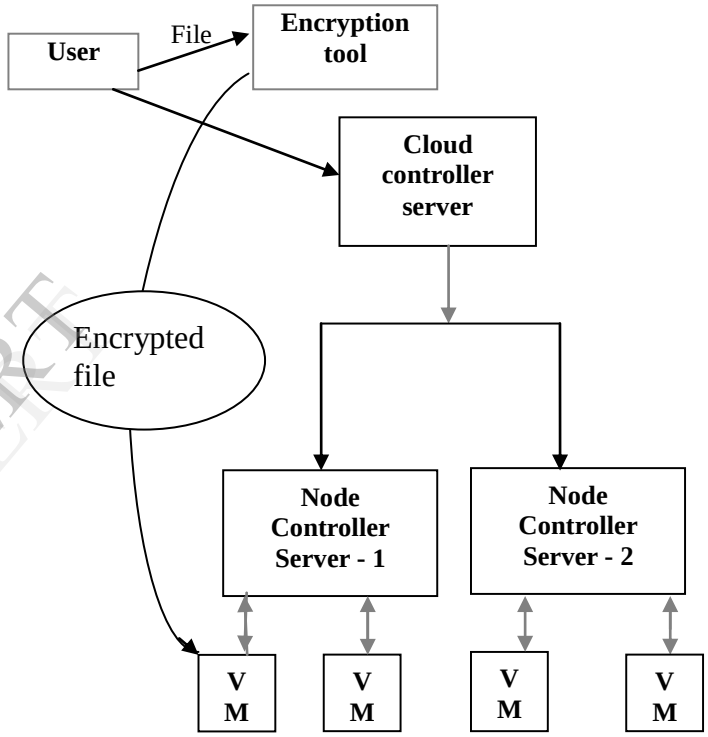

Fig 1: Proposed architecture for user side file encryption in cloud.

Virtual machines (VMs):

VMs are one kind of instances of the cloud. Separate instances are created for every user on demand of services. All the services are provided to users through VM instances. All instances are running on NCS [7].

V. APPROACH

In the above architecture shown in figure the cloud user would be accessing his services from the cloud controller server. If user want to store their data in to the cloud then file is directly go in to the encryption tool where our SHA algorithm perform encryption of user data and then file is transfer to the virtual machines. User data is stored in encrypted form in to the cloud. Our technique provides user data security when data is transfer from user to cloud. User have encryption key to access the data so no one can access the data without key. This technique is not consider by some cloud provider to secure user data when data is transfer from user to cloud.

VI. CONCLUSION

We have proposed a best technique for securing cloud by Data encryption algorithms i.e. SHA Algorithm. In this paper, we focused on data encryption from user side and provide authentication . We investigated that there are many algorithms provide data encryption when data is transfer from one cloud to another cloud and also provide encryption when data stored within cloud but there are few algorithms that provide user side encryption. Our algorithm(SHA) provides user side file encryption and provide more security of consumer data. This technique is help user to secure their data and improve cloud security.

REFRENCES

[1] Yubo Tan , Xinlei WangRashmi " Research of Cloud Computing Data Security Technology", IEEE 2012

[2] Farhan Bashir Shaikh , Sajjad Haider " Security Threats in Cloud Computing", 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates

[3] Deyan Chen, Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing ",2012 International Conference on Computer Science and Electronics Engineering.

[4] Balakarishnan.S, Saranya.G, Shobana.S, Karthikeyan.S "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", IJCST Vol. 2, Iss ue 2, June 2011.

[5] Simarjeet Kaur "Cryptography and Encryption In Cloud Computing", VSRD-IJCSIT, Vol. 2 (3), 2012, 242-249

[6] Sunita Rani, Ambrish Gangal "Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4302 - 4304

[7] Krimit Shukla, Harshal Trivedi , Parth Shah "Architecture for Securing Virtual Instance in Cloud", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4279 - 4282