International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-4, Issue-1, January 2016

An Authentication Scheme Based On Multiple Trusted Third Party

Atul Kumar, Dr. U.C. Jaiswal

***Abstract*— Cloud computing is a contemporary and modern technology in the field of distributed computing that provides web oriented services. The practice of using remote servers through network, hosted on the global server to store data, manage data, and process data, rather than a local client server or a personal computer. The customer used dynamically scalable resources and cloud provides economically service to a large extent. However security issue is obvious in some of the area in cloud computing environment where security can break by some techniques such as storage data, user authentication and data during transmission etc. In cloud computing environment, the user can access services through some authentication parameters which are provided by the cloud provider or third party. Third party is single independent security service providers which work as arbitrator between cloud provider and users. They can leak the credentials parameter to the unauthorized user. In this paper, we provide a framework for user authentication using decentralization of third party stored information.**

***Index Terms*— Cloud Manager, Cloud Server, User, Security, Authentication Scheme**

I. INTRODUCTION

Cloud computing technology is an innovative technology that is doing computing at extent level data. In cloud computing, we do not need to buy the hardware and software; in fact we only pay for use of it. That causes, we need less money to use of that service.

Cloud computing provides internet based service on a utility basis to the business process. The multitenant (consumers) share a pool resources and service hence security is the major concern in cloud environment. That's why we need a proper mechanism to ensure security of authentication and on data [7]. One side ,if we need to provide guarantees secure enough to user then processing become slow and user may inconvenient to use .Other side ,if we need to provide less guarantees secure to user the processing become faster but security risk is high. Hence we required to proper balanced mechanism between security and processing time.

The five essential characteristic of cloud computing is given following [8]:

1. On demand self service: The cloud computing server provides resources to the tenant according to whatever they required through online control panel.

2. Broad network access: All cloud resources are store over the internet and user can access through different device such as mobile smart phones, laptops, office computers and tablets. This mobility of devices is particularly attractive for businesses.

3. Resource pooling: In cloud environment, multiple customer access computing resources in pool based model without knowing the location of their stored data.

4. Rapid elasticity: Computing resources on server can be scaled as per the customer requirement.

5. Measured service: Easily measure the services provided for customers in the shared pooled resources by cloud infrastructure mechanism.

Atul Kumar is currently pursuing masters degree program in Computer Science Engineering from MMMUT. Gorakhpur, India

Dr.U.C. Jaiswal is currently Associate Professor in Department of Computer Science Engineering in MMMUT. Gorakhpur, India

II. LITERATURE REVIEW

Security in cloud computing**:**

The fastest growing of cloud computing market has lead malicious user to revise attacks technique in order to cope with the feature of cloud infrastructure. Users will not compromise their privacy so cloud service providers must be ensuring that the customer's information is safe.

Cloud computing consists of platforms, applications and infrastructure section. Each section performs different task and offers different services and products for individuals and businesses around the world. The business application includes Web Services, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Managed Service Providers (MSP), Utility Computing, Internet Integration and Service Commerce. There are numerous security issues for cloud computing as it [9]

Service delivery and data availability: Network reliability is a main goal for cloud computing and cloud service because a cloud is provide service over public network (Internet).This network may be break[2] .we need to ensure internet backbone network connectivity .A few computer manufactures and storage service providers ensure that data continue to be available at a requirement level of performance in situation of ranging from normal disastrous .Data availability is achieved through data redundancy involving where the data is stored and how it can be reach.

Confidentiality and privacy: Confidentiality related to the treatment of information that an individual person has disclosed in a relationship trust, with the full expectation that it will not be divulged to other without permission in way that are inconsistent with the understand of the original data disclosure[4]. Privacy is the control on the extent, temporal order and circumstances of sharing oneself (physically, behaviorally, and intellectually) with other.

Disaster recovery and business continuity: users and service providers should get the insurance that the cloud service persist in case of the occurrence of security incident and disasters .The recovery procedures should also be clearly defined in order to reduced the downtime length.

Data transmission: Some encryption technique is used for secure data transmission. To provide the protection for data only goes where the consumer are want by using authentication and integrity and also ensure that it is not modified in transmission. Now days, SSL/TLS protocol are used for data transmission. Fully homomorphism encryption scheme is used for encrypting the transmitting data in which allow data to be processed without decrypt the data [3]. To provide confidentiality and integrity data in transmission, the cloud provider need to check some access control like authorization, authentication, auditing, and ensuring the availability of the Internet-facing instances at cloud provider.
Virtual machine security: The whole idea of cloud computing depend upon the one key that is called virtualization. Virtualization is defined as the different instances running on the same physical machine are isolated from each other. Virtual machines are dynamic means it can quickly be reverted to previous instances, paused and restarted easily [2]. They can move between the physical servers. This dynamic nature of virtual machine make it difficult to achieve maintain consistent security, configuration error may be occurred and it is difficult to maintain an audit ability record of the security state of the virtual machine at any given point of time. Virtualization fall in mainly two categories, one is full virtualization and second is Para virtualization. In full virtualization, entire hardware architecture of machine is replicated virtually and in Para virtualization, an operating system is changed so that it can be run at same time with other different operating systems. Virtual Machine Monitor (VMM) is software layer that hiding the physical resources and operation used by the multiple virtual machines.
Network security: Networks are found many type i.e. shared and non shared network, public and private network and small area and large area size network and each of them have number of threats to deal with [4]. Some type of problem is associated with that like DNS attacks, Sniffer attacks, issue of reused IP address, etc. Domain name system (DNS) server performs an operation that translated of a domain name to an IP address. Since domain name much easier to remember than IP address of server.
Data security: Secure storage of data at the server is most challenge because many tools are available which find the actual location of vital data .That causes we required most secure encryption technique for storing data [10] .Homomorphism technique is an advance technique to use. In order to assure the information security and data integrity, Hypertext Transfer Protocol (HTTP) and Secure Shell (SSH) are the most common adoption.
Data integrity: Data integrity can be preserved by database constraints and transactions management. Transactions should be follow ACID (atomicity, consistency, isolation and durability) properties to ensure the data integrity.
Data Segregation: Data in cloud environment are typically shared by different user. This structure is not sufficient for preserving data segregation via single encryption applies on data. Some time user not wants to encrypt the data for storage. Because some time encryption leads destruction and corruption of data.
Security Policy and Compliance: Ancient cloud providers are subjected to external audits and security certifications. If cloud providers not follow that security policy then it leads to decrease the customer trust. An organization implements the Audit and compliance of the customers to the internal and external processes that may fallow the requirements classification.
Trusted Third Party:
Trusted third party (TTP) service between cloud server and users, to lead the establishment of the necessary trust level and provides noble solution to preserve the confidentiality, integrity and authenticity of data in communication [6]. A trusted third party is an intermediate entity which provide intersection between two parties who trusted by both of the parties. All the critical transaction communication between the parties is monitored by the trusted third party efficiently.TTP is common in any number of commercial transaction and in cryptographic digital transaction as well as cryptographic protocols. Third parties, such as banks and certificated authorities are used in the electronic transfer of secure data. The third party uses cryptography and security measure to attest the identity of the sender, the security of data during transmission and to verify delivery to intended recipient. The scope of TTP provides end to end secure connection between parties. As describe by castell, "A third party is an impartial organization delivering business confidence through commercial and technical security feature, to an electronic transaction [1].

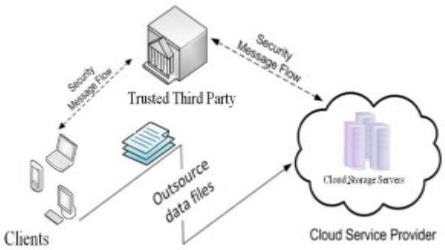

Fig.1. Network architecture for cloud data storage

There are three entities in this architecture: cloud uses, cloud servers and trusted third party.

Problem with existing model trusted third party.

1. The first problem is that the trusted third party can read all the authenticated attribute of the user and message which communicate between them. Third party may be disclosed to unauthorized users.
2. Second problem is that when the TTP leaves the corporate it must hire a new TTP and start up the process on from the bottom up. Otherwise the outgoing TTP can get access to all sensitive materials.
3. It may be corporate entity. This can share important data to other cloud service providers.
4. Many employee worked with single third party organization may be they leak sensitive data to unauthorized user.

III. PROPOSED FRAMEWORK

Client/user stored his data over the internet (cloud servers).we considered the confidentiality and integrity issue of the cloud environment and provides a solution to these issues by proposing a noble algorithm that checks authenticity in distributed scheme.

Algorithm:

Step1: consumer sends a request for login to the cloud server without cookies.

Step2: Cloud server redirect message to the cloud manager and cloud manager split and redirect message to different TTP servers.

Step3: First TTP server sends a request to user for give <username>.

Step4: User enters <username> send to first TTP. Then second TTP send request to provide <password>.

Step5: Then each attribute of data<username> and <password> received by the cloud Manager (for validation and verification of username and password)

Step6: Cloud manager responds with "Primary key and cookies". Then user redirect with cookies to cloud server.

Step7: In last phase cloud server request object to the user.

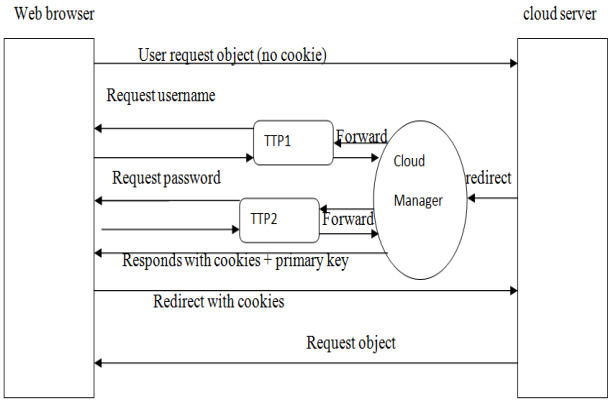

Fig2. Communication steps required in proposed framework

IV. SECURITY ANALYSIS:

In this paper since we are using a multiple trusted third party servers and we are storing the one parameter of credential at each server, compromising one of them TTP servers will not disclose the security. Second things we use a cloud manager for the matching of their username and password for a particular user. If any TTP is compromising by any outsider attacker then the probability of success is less than or equal to 0.5.We create a link to username and password for reducing the user overhead in deciding the authorization by cloud manager.

V. CONCLUSION

In this paper, we justified that decentralized TTP is an appropriate cryptographic primitive for secure data upload in clouds authentication scheme. We proposed a simple framework to simultaneously achieve security and performance in company oriented cloud storage applications from spoofing. We proposed a new authentication scheme secure in the standard model. Our scheme has balanced complexity in terms of computation and communication time.

ACKNOWLEDGMENT

This paper is made possible through the support and institutional facilities provided by the Department of Computer Science & Engineering MMMUT, Gorakhpur. We convey our sincere thanks to other M. Tech scholars for their rigorous brainstorming sessions to shape up this research paper.

REFERENCES

[1] Ashish sing and Kakali Chatterjee "A Secure Multi-Tier Authentication Scheme in Cloud Computing Environment" International Conference on Circuit, Power and Computing Technologies: 2015

[2] Diogo A. B. Fernandes ,Liliana F. B. Soares and João V. Gomes in"Security issues in cloud environments: a survey" 2013 Springer-Verlag Berlin Heidelberg..

[3] Dr.R.S.Shaji and X.P.Ajitha Baby Fathima in" A Multi Server Storage Authentication System for Cloud Computing" ©2014 IEEE

[4] Aeri Lee in "Authentication scheme for smart learning system in the cloud computing environment" © 2015 Springer-Verlag France.E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," *IEEE Trans. Antennas Propagat.*, to be published.

[5] Shuai Han and Jianchuan Xing in"ensuring data storage security through a novel third party auditor scheme in cloud computing" ©2011 IEEE

[6] Changyou Guo and Xuefeng Zheng" The Research of Data Security Mechanism Based on Cloud Computing" SERSC © 2015.

[7] Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy" Cloud Computing: Security Issues and Research Challenges" IRACST ,Vol. 1, No. 2, December 2011.

[8]] S. Srinivasan" Cloud Computing Basics" Springer New York Heidelberg Dordrecht London.

[9] Pate S, Tambay T (2011) Securing the Cloud-Using encryption and key management to solve today's cloud security challenges. Storage Networking IndustryAssociation2011.Source:http://www.snia.org/sites/default/education/tutorials/2011/spring/security/PateTambay_Securing_the_Cloud_Key_Mgt.pdf. Accessed on Dec.2015

[10] Jaidhar, c.d." Enhanced mutual authentication scheme for cloud architecture" Advance computing conference ,2013 IEEE 3rd international doi:10.1109/iadcc.2013.6514197