iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5459

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

A TPA-Authentication Scheme for Public Cloud using Kerberos Protocol

Kirti Rathore[1], Sumit Nigam[2]
[1]*Research Scholar-MTECH SIMS-Indore*
[2]*Assistant Professor-CSE SIMS-Indore*

Abstract: ***Cloud computing is the new generation technology provides the way of sharing of resources, memory, software anything in the form of service using internet. Security is an important and unique phenomenon gives safe and isolated environment. Security model and principles are defined to implement security features with any applications. Confidentiality, authentication and integrity are primary principles for trust establishment. Existing work only concentrates on integrity concept and does not imposes for authentication or access control. A Kerberos based strong authentication scheme has been generated using third party auditing concept to improve the strength of authentication as well as trust on CSP. This work will implement security service architecture to create Kerberos environment and also establish communication between Kerberos and CSP. The complete work will be implemented using Java technology and Open Stack serve for public cloud environment.***
Keywords: Cloud computing, TPA, Kerberos, CSP

I. INTRODUCTION

Cloud computing is the delivery of computing services—servers, storage, databases, networking, software, analytics and more—over the Internet ("the cloud"). Companies offering these computing services are called cloud providers and typically charge for cloud computing services based on usage, similar to how you are billed for water or electricity at home. We are probably using cloud computing right now, even if we don't realize it. If we use an online service to send email, edit documents, watch movies or TV, listen to music, play games or store pictures and other files, it is likely that cloud computing is making it all possible behind the scenes. The first cloud computing services are barely a decade old, but already a variety of organizations—from tiny startups to global corporations, government agencies to non-profits—are embracing the technology for all sorts of reasons. Here are a few of the things we can do with the cloud:

A. Create new apps and services
B. Store, back up and recover data
C. Host websites and blogs
D. Stream audio and video
E. Deliver software on demand
F. Analyze data for patterns and make predictions.

G. Benefits of Cloud Computing
1) Cost
2) Speed
3) Global scale
4) Productivity
5) Performance
6) Reliability

H. Types of Cloud Services
1) IaaS
2) PaaS
3) SaaS

Most cloud computing services fall into three broad categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (Saas). These are sometimes called the cloud computing stack, because they build on top of one another. Knowing what they are and how they are different makes it easier to accomplish your business goals.

I. Infrastructure-As-A-Service (Iaas)

The most basic category of cloud computing services. With IaaS, you rent IT infrastructure—servers and virtual machines (VMs), storage, networks, operating systems—from a cloud provider on a pay-as-you-go basis.

J. Platform As A Service (Paas)

Platform-as-a-service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivering and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and databases needed for development.

K. Software As A Service (Saas)

Software-as-a-service (SaaS) is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet or PC.

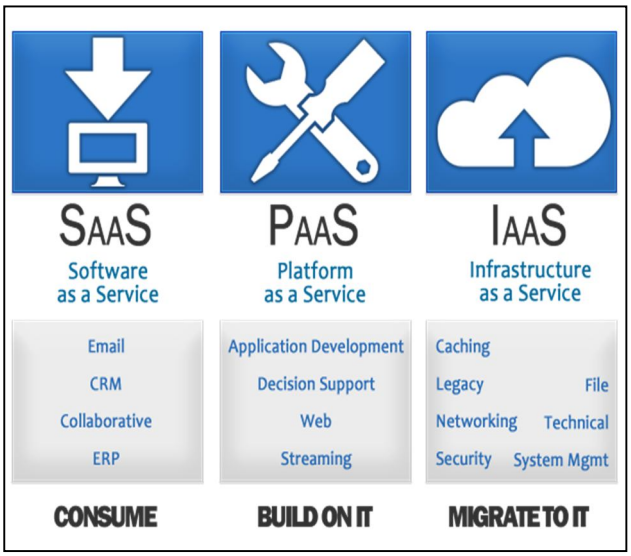


Figure 1: Cloud Computing Services

L. Types of Cloud Deployments

There are three different ways to deploy cloud computing resources: public cloud, private cloud and hybrid cloud.

1) *Public Cloud:* Public clouds are owned and operated by a third-party cloud service provider, which deliver their computing resources like servers and storage over the Internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software and other supporting infrastructure is owned and managed by the cloud provider. You access these services and manage your account using a web browser.
2) *Private Cloud:* A private cloud refers to cloud computing resources used exclusively by a single business or organization. A private cloud can be physically located on the company's on-site datacenter. Some companies also pay third-party service providers to host their private cloud. A private cloud is one in which the services and infrastructure are maintained on a private network.
3) *Hybrid Cloud:* Hybrid clouds combine public and private clouds, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, hybrid cloud gives businesses greater flexibility and more deployment options.

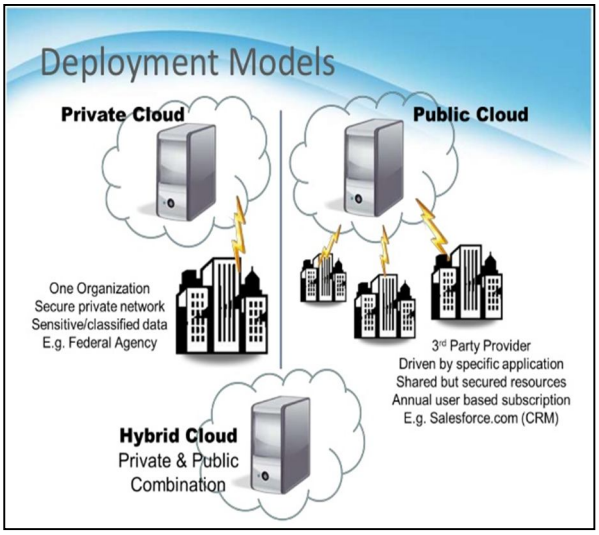


Figure 2: Deployment Models of Cloud Computing

II. RELATED WORK

Security in cloud computing is one of the major areas of research. Many researchers have investigated on cloud security.

Salah H. Abbdal et. al. explore that cloud computing is a novel paradigm in information technology. This approach involves methods that forward services to users on demand via pay-as-you-go. Cloud computing can reduce computation and communication costs, and this advantage has resulted in the influx of cloud computing users. Cloud storage, which allows users to remotely outsource their data to the cloud, is considered a major cloud computing service. However, this form of storage introduces new security challenges, such as unreliable service providers. Data storage correctness is another challenge that should be addressed before this modern storage model can be extensively applied. Most proposed schemes for data integrity verification use a third party auditor, specifically a single third party auditor. However, a single third party auditor may become a bottleneck in the overall system operation and may degrade system performance because thousands of users may delegate their tasks to a single third party auditor. In this paper, they propose a new scheme for securing data integrity via a multiple third party auditors based mutual authentication to overcome the aforementioned limitations and ensure high-level security. They suggest a remote data storage correctness checking scheme based on homomorphic linear authentication and an elliptic curve digital signature algorithm to support public verifiability. Their proposed scheme uses a Merkle hash tree at the cloud server to store data, thereby enabling rapid data access. Finally, our proposed scheme identifies misbehaving servers and verifies data storage correctness.

A block representation of proposed solution is shown below;

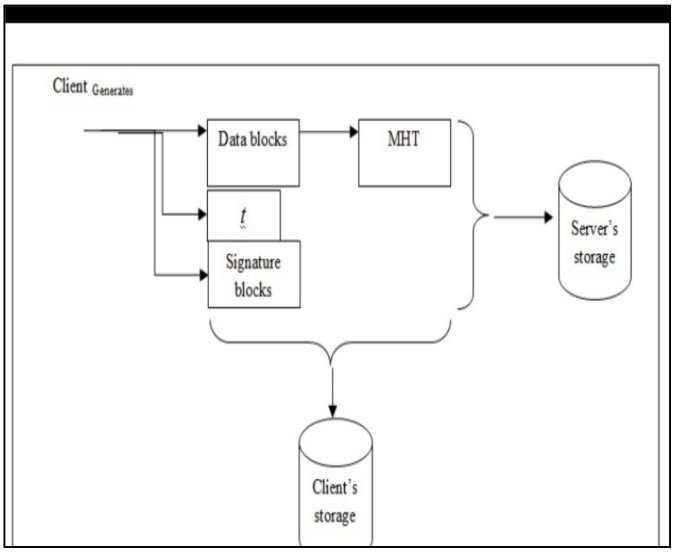


Figure 3: Block Representation of Proposed Solution

Amit Joshi et. al. proposed an scheme to enhance the cloud security techniques through randomized motion evolved as a paradigm to concatenate with the hierarchical key based security. The 4 specific objectives for this research work includes Comparative Analysis of Security techniques for Secure cloud data and identifying major barriers for cloud security, propose a security technique for security in private Cloud Environment with changing facets, analysing and proposing a model for security with comparison with grids and their success rate.

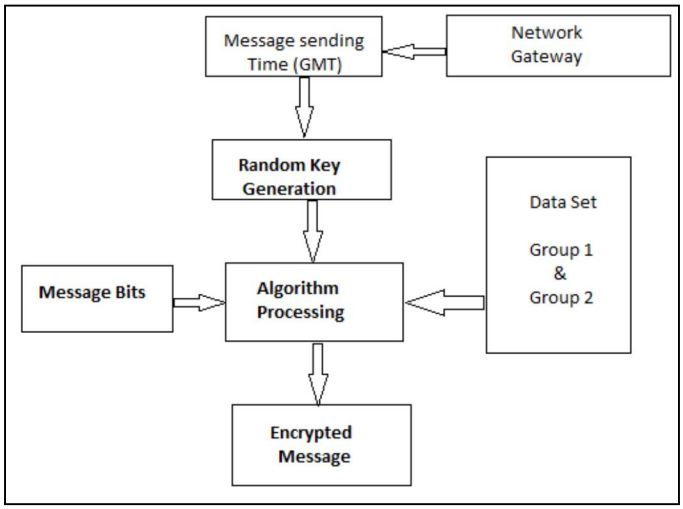


Figure 4: Block Representation of Joshi Scheme

Mehdi Hojabri[] proposed an scheme based on Kerberos for third party authenticator. In cloud data storage system, users store their data in the cloud and for accessing must refer to cloud server provider. Thus the correctness of the user being refer to the distributed cloud server must be guaranteed because the data stored in the cloud may be frequently, updated with user including, insertion, deletion, modification, appending, reordering, etc. To ensure this updating is under correctness user is important so in this paper we introduce one model based on kerberos. In this model each user for gain the cloud server must be register and authentication with third party. After added the requirement information into the data base it can get some qualification. After getting the qualification it should refer to the Kerberos authentication service and do this scenario:

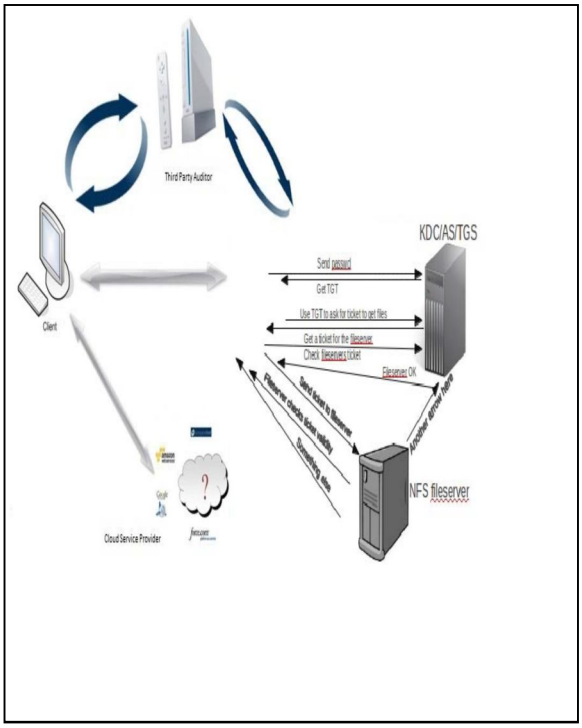


Figure 5: Kerberos based authentication scheme

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

III. KERBEROS AUTHENTICATION SCHEME

Kerberos is an authentication protocol which is used to authenticate users in the distributed environment. Using Kerberos authentication protocol, a client can authenticate itself to multiple servers using its password which is also known as the long term secret key. Client receives Ticket-Granting-Ticket (TGT) from the Authentication Server (AS) and this ticket can be used for multiple services that a client needed. Therefore, client stores this Ticket-Granting-Ticket in its database. Then, it requests for Service-Granting-Ticket and stores it in its database.

An advantage of storing Service-Granting-Ticket in database is that client will not have to re-enter password every time when he has to access the application server such as email server. A Kerberos environment consists of Key Distribution Center (KDC), a number of clients and Application Servers. Key Distribution Center (KDC) consists of authentication server (AS) and Ticket Granting Server (TGS). An AS issues Ticket-Granting-Tickets to the user after the verification and TGS issues Service-Granting-Tickets to the user.

If a client wishes to authenticate herself to application server, then Kerberos will perform this task in three phases as:

Whenever a user logs on to a workstation, the client process running in the workstation sends a message to the Authentication Server.

Authentication Server checks in the database whether username and password are correct. If all is correct, then Authentication Server (AS) sends a Ticket-Granting-Ticket to the user and also a session key so that user can communicate with the server.

Same copy of session key is also included in the ticket that AU issues to the client. Ticket-Granting-Ticket and session key are encrypted using a key generated from the user password. Because message sent by the AU to client is encrypted using key generated from user password, only authorized user reads the

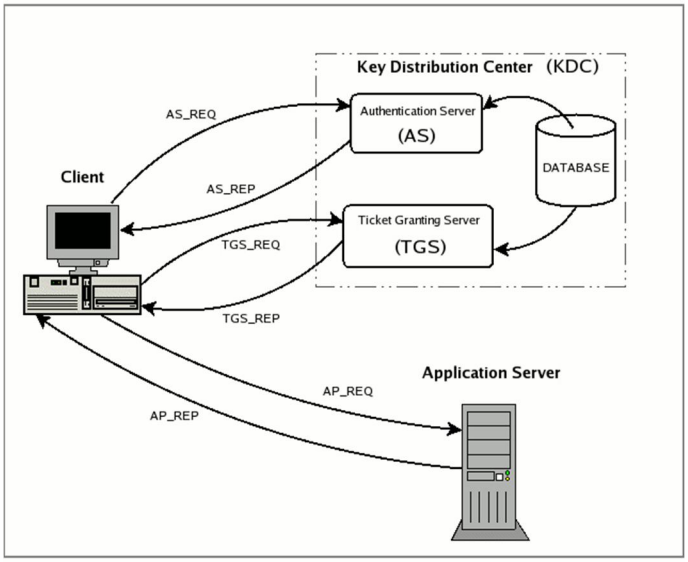


Figure 6: Kerberos Architecture

A. *Limitations*

1) Kerberos assumes that each user is trusted but is using an untrusted host on an untrusted network.
2) Relocation of password can be dangerous in Kerberos.
3) For an application to use Kerberos, its source must be modified to make the appropriate calls into the Kerberos libraries.
4) Kerberos is an all-or-nothing solution. If Kerberos is used on the network, any unencrypted passwords transferred to a non-Kerberos aware service are at risk.

IV. PROBLEM STATEMENT

Cloud computing is the fastest horizontal and vertical growing area in terms of its users and number of services it offers. These services and users data will always be stored at some different location where the user loss controls over it. Gaining control and making the data secure will affects the performance and other applications of cloud providers. Thus, some mechanism needs to be defined which works as a balance between both provider and client. The mechanism should be capable of providing the required

security to the user by applying some encryption schemes and generating the key from the user's end which keeps the control of data to user always.

Authentication is the process which allows a sender and receiver of information to validate each other. If the sender and receiver of information cannot properly authenticate each other, there is no trust in the activities or information provided by either party. Authentication can involve highly complex and secure methods or can be very simple which completely depends on risk and asset value of data. Simple authentication is one of the major reason for security theft and most vulnerable source for attackers. SomeWeak Authentication" (WA) means cryptographic authentication between previously unknown parties without relying on trusted third parties. In some applications, imperfect security may be sufficient but still they may be on risk. Enhancement in the risk and asset value generates need to analyse attack probabilities and economic impacts. These factors can be taken in account in protocol design. So, authentication plays very important role in account safety.

Existing works only concentrate on data integrity and verifiability concept and does not use any specific logic for strong authentication. They only user userid-password scheme for authentication purpose, which is cannot be consider as trusted way for proofing. Subsequently, Existing authentication mechanism eighth involved local level security or third party based on cryptography This work observes that Kerberos can be good opportunity to enhance the level of authentication with maintaining proper third party audit. This work demand to generate such kind of authentication mechanism based on Kerberos for cloud computing.

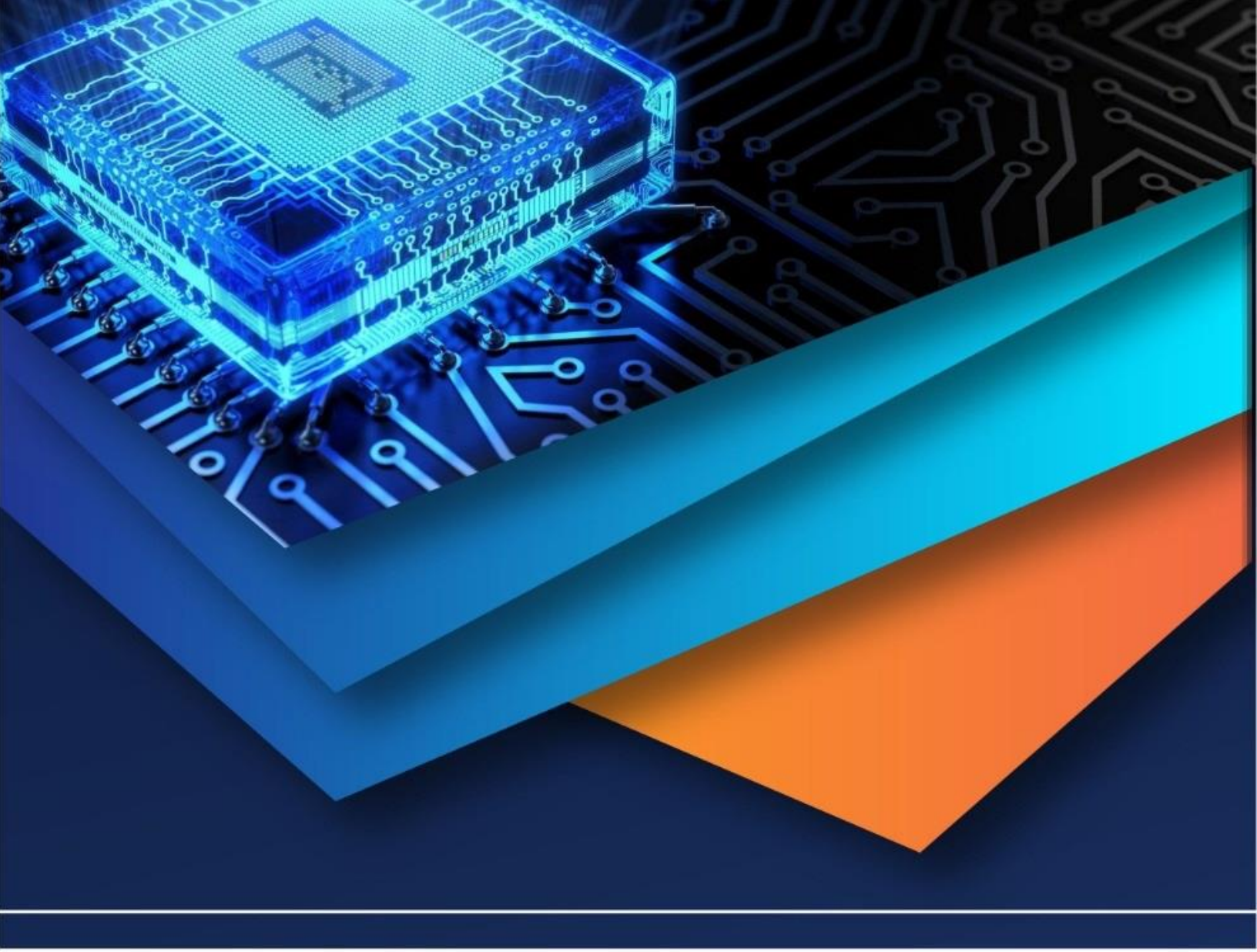
V. SOLUTION DOMAIN

The study of existing cloud computing policy and authentication scheme observe that there is strong need to enhance the level of cloud computing authentication scheme for safe and secure communication. Third party auditor and Kerberos also suffer with some lack of interest. This solution proposed a technique to proposed an hybrid scheme for authentication purpose in cloud computing. Here, AS and TGS has been used as the component of KDS server Thus, in this work a TPA-HE policy based work is proposed to provide higher security with less concern management. It focuses on features of cloud computing models for all kinds of applications and data on the cloud platform which have no fixed infrastructure and security boundaries. The main design goal is to help the data owner to achieve fine-grained access control on files stored in Cloud Servers. Specifically, the work will enable the data owner to enforce a unique access structure on each user, which precisely designates the set of files that the user is allowed to access. Also to prevent Cloud Servers from being able to learn both the data file contents and user access privilege information used to generate key along with the fastest access of secured data by using homomorphic encryption. The work will also consider the event of a security breach, which overcomes from data isolation issues. The work also analyzed the existing service delivery models of cloud computing and identifies that the resources of cloud services based on may be owned by multiple providers. Thus the work also proposes a novel security model with enhanced mechanism. In addition, the proposed scheme should be able to achieve security goals like user accountability and support basic operations such as user grant and revocation as a general one-to-many communication system would require.

VI. CONCLUSION

The complete study concludes that there is strong need to improve the level of authentication to enhance the level of security. Kerberos can be a good approach to integrate authentication with ticket granting approach. Proposed solution would help to improve the level of authentication in cloud computing. Future expectation of this paper is the implementation of proposed solution and evaluation on basis of computation time and relevant factors.

REFERENCES



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY