A Secure Key for Cloud using Threshold Cryptography in Kerberos

Shubha Bharill, T. Hamsapriya, Praveen Lalwani
Department of Computer Science and Engineering
Oriental Institute of Science and Technology
Bhopal, M.P., India

ABSTRACT

In IT industry now a days there is a need for several new resources and storage requirement for terabyte of data generated every day. Cloud Computing is a solution for this in a cost effective manner. Cloud Computing provides on demand resources as services to client. Cloud is highly scalable, flexible and platform in dependable. Although it is benefiting the clients in several ways but as data is stored remotely it has many security loopholes like attacks, data loss, other authentication and security issues. In this paper an authentication model is proposed for cloud computing based on Kerberos protocol using threshold cryptography to provide more security and to increase the availability of key. This model can also benefit by filtering the unauthorized access and to reduce the burden of computation and memory usage of cloud provider against authentication checks for each client. It acts as a third party between cloud server and clients to allow authorized and secure access to cloud services. In this paper we will take a review of related work for cloud security issues and attacks. In next section we will discuss the proposed architecture and its working. Next we will see how it can provide better security and availability to key used for authentication.

General Terms

Authentication, Security.

Keywords

Cloud Computing, Kerberos, Threshold Cryptography, Security, Authentication.

1. INTRODUCTION

IT-related capabilities are provided as services to multiple external customer through Cloud Computing using internet technology. The use of the Internet and new technologies nowadays, for business and for the current users, is already part of everyday life. It allows users to consume services without knowledge and control technology and infrastructure supporting them. To days' businesses are very complicated, whenever there is a new requirement we need to purchase new hardware, software licenses etc. organizations also need experts to install, configure, test and run them. Cloud computing reduces this entire burden as organizations need not to own all these resources. Resources are owned by the third party cloud provider. The basic idea behind this is reusability of IT resources. Services are provided as utility in cloud computing so user only pay according to the type and amount of service they used. Beside all the advantages of cloud since it is a distributed and shared environment there are several issues related to its security. One of them is Authentication that must be solved in Cloud computing environment as soon as possible. Therefore, we wishes to propose protocol that can solve suitable user and services certification in cloud computing environment. In this paper we proposed a novel authentication protocol that is based on Kerberos [1].

The Kerberos protocol is designed to provide reliable authentication over open and insecure networks where communications between the hosts belonging to it may be intercepted. Kerberos is a computer network authentication protocol which works on the basis of 'ticket' to allow nodes communicating over a non secure network to prove there identity to one another in a secure manner. It is beneficial because it provides mutual authentication- both the user and the server verify each other's identity. Because of some limitations of Kerberos it is restricted by some well known organizations. When the Kerberos server is down due to any physical or environmental attack, no one can log-in. This can be resolved by using multiple server instead of single server. Another limitation with Kerberos is Kerberos assumes that each user is trusted but is using an un-trusted host on an un-trusted network. Its primary goal is to prevent unencrypted passwords from being sent across that network. However, if anyone else than the proper user has access to the one host that issues tickets used for authentication called the key distribution center (KDC) the entire Kerberos authentication system is at risk. Since all authentication is controlled by centralized KDS, compromise of this authentication infrastructure will allow an attacker to impersonate any user. This will reduce the security of Kerberos authentication model. For avoiding these all limitations we are providing a new approach for more secure Kerberos authentication model.

By using Shamir's Secret Sharing algorithm with Kerberos these limitations can be removed. Shamir's Secret Sharing is an algorithm in cryptography where a secret is breaked into parts, distributing each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret. Considering on all participants to combine together the secret might be impractical, and therefore the threshold Cryptography scheme is used where any k of n parts are sufficient to reconstruct the original secret. Due to some limitations of Kerberos we are using a Threshold cryptography algorithm to avoid single point of failure. The combination of these two algorithms will give a more secure authentication system.

The rest of the paper is organized as follows: In Section 2 we present the related work based on review of previous work. Section 3 discusses the proposed work which contents Kerberos and Threshold Cryptography Algorithm. Conclusion and Future Work is presented in section 4.

2. RELATED WORK

Title of the Paper	Concept	Future Work	Year of Publication	Conference/Journal Name
[1] Innovation in Cloud Computing: Implementation of Kerberos version5 in cloud computing in order to enhance the security issues	Investigate a problem of data security in cloud service provider and also proposed an effective and flexible distributed scheme with explicit dynamic data support, including Kerberos authentication service and third party to authenticate the user in the cloud server and vice-versa.	Kerberos is a complex and not a fully trustworthy algorithm so in future, work should done to make Kerberos more secure.	2013	IEEE, International Conference on Information Communication and Embedded System (ICICES)
[2] A Secure Authentication Protocol for Cloud Services	Implemented a new approach for authentication to user using Authentication Server and Cloud service provider server and compare it with Kerberos and PKI.	Proposed approach is a logical vantage approach so they will compare characteristics of other various systems with the proposal system on open cloud computing environment hereafter.	2011	Journal Of Advanced Information Technology And Convergence
[3] Composing Kerberos and Multimedia Internet Keying (MIKEY) for Authenticated Transport of Group Keys	Proposed two approach, Kerberos and MIKEY to provide authenticated transport of group keys in environments that deploy Kerberos for authentication.	By integrating proposed work with concrete applications that leverage group communication a deeper study on GPSK bounded with Kerberos to make the overall system more efficient.	2013	IEEE, Transactions on Parallel and Distributed Systems
[4] Ensure Data Security in Cloud Storage	Present a framework to ensure data security in cloud storage system using SLA a common standard between user and provider.	By using federated identity management, unique identity and hierarchical identity based cryptography (HIBC), the key distribution and mutual authentication can be simplified.	2011	IEEE, International Conference on Network Computing and Information Security
[5] Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing	Designed and proposed a privacy enhanced and trust-aware IdM architecture compliance with SAMLv2/ID-FF standards to provide an efficient identity management and access control, as well as dynamic, autonomic, and user-centric system for better scalability in cloud computing services.	Validate the optimal values of the parameters of the reputation model and evaluate the performance of the system experimentally through simulations using OMNeT++.	2012	IEEE, Transaction on Consumer Electronics
[6] Ensuring Data Storage Security in Cloud Computing through two way Handshake based on Token Management	Proposed a method to ensure the user's data in the cloud by utilizing the homomorphic token with distributed verification of erasure- coded data so that one can achieve the identification of misbehaving server.	Data Storage Security in Cloud Computing is still in its infancy now and research problems are yet to be identified.	2010	IEEE, International Conference on Advances in Recent Technologies in Communication and Computing
[7] Authentication Using Graphical Password in Cloud	Proposed a graphical password authentication system that can resist against common attacks and improve security issues in cloud computing and compared the proposed scheme with previous researches.	Security can be provide to the Transmission channel for secure transmission of data.	2012	IEEE, 15th International Symposium on Wireless Personal Multimedia Communications.

Title of the Paper	Concept	Future Work	Year of Publication	Conference/Journal Name
[8] An Efficient Schema Shared Approach for Cloud based Multitenant Database with Authentication & Authorization Framework	Shared database shared schema approach has been proposed using Kerberos that offers large no. of tenants per database server as the single database serves the database requirements of multiple Institutions.	It can be implemented where SaaS cloud services are to be delivered between multiple clients (Institutions) with authentication	2011	IEEE, International Conference on P2P, Parallel, Grid, Cloud and Internet Computing
[9] Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures	PasS a set of security protocols for ensuring the privacy and legal compliance of customer data in cloud computing architectures is proposed for the secure processing, storage and auditing of users' confidential data by leveraging the tamper-proof capabilities of cryptographic coprocessors.	Consider a variety of design choices including those that do not rely on the presence of a trusted third-party, investigate alternative key management and distribution mechanisms, research the development of standard patterns to systematically support the software division process, and provide detailed analysis and evaluation of the system implementation.	2009	Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing
[10] Privacy Preserving Access Control with Authentication for Securing Data in Clouds	Proposed a new privacy preserving authenticated access control scheme for securing data in clouds in which the cloud verifies the authenticity of the user without knowing the user's identity before storing information and added feature of access control in which only valid users are able to decrypt the stored information.	One limitation is that the cloud knows the access policy for each record stored in the cloud. It protect the privacy of user attributes as well.	2012	12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing
[11] SecCloud: Bridging Secure Storage and Computation in Cloud	Proposed SecCloud, a novel auditing scheme to secure cloud computing based on probabilistic sampling technique as well as designated verifier technique to consider secure data storage, computation and privacy preserving together.	To improve the efficiency of the algorithm the designated verifiers can concurrently handle multiple sessions from different users' verifying requests.	2010	IEEE, 30th International Conference on Distributed Computing Systems
[12] Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments	Proposed a comprehensive security framework for cloud computing environments. We present the security framework and discuss existing solutions, some approaches to deal with security challenges.	Need to provide security mechanisms to ensure that Cloud Computing benefits are fully realized	2010	34th Annual IEEE Computer Software and Applications Conference Workshops
[13] Secure Key Distribution for the Smart Grid	Proposed a scheme for a smart grid using a trusted third party which not only has no issue on key revocation, but also the third party can be easily identical in case power outages occur**.**	Other algorithms can be used in place of trusted third party.	2012	IEEE, Transactions On Smart Grid,
[14] Secure Locking For Un-trusted Clouds	Identified new attacks that an un-trusted cloud provider can launch via control of the locking mechanism, and proposed an extension to existing locking scheme.	Vector clocks can be explored to replace the centralized time server.	2011	IEEE, 4th International Conference on Cloud Computing

Title of the Paper	Concept	Future Work	Year of Publication	Conference/Journal Name
[15] Security Threats in Cloud Computing	Identified the most vulnerable security threats in cloud computing, which will enable both end users and purveyors to know about the key security threats associated with cloud computing**.**	Work should perform on security standards for secure cloud computing.	2011	IEEE, 6th International Conference on Internet technology and Secure Transaction.
[16] Securing User Authentication using Single Sign-On in Cloud Computing	Designed and implemented an optimized infrastructure for secure authentication and authorization in Cloud Environment using SSO (Single Sign-On) for authenticate once and gain access of multiple resources to reduce number of login and password in heterogeneous environment and to gain balance in Security, Efficiency and Usability.	Cloud server can activate and decamp resources as needed, dynamically update infrastructure elements, and shift workloads to improve efficiency without having to worry about creating new infrastructures. If the number of SSO users increases, this feature will be fruitful.	2011	IEEE, International Conference On Current Trends In Technology

3. PROPOSED WORK

The main focus of this model is to authenticate a client before accessing service. Merely username and passwords checking is not enough for a cloud computing like distributed and shared environment. Kerberos is an authentication protocol for network and also provides single sign-on facility to clients. Kerberos was developed in the mid of 1980's at MIT. It is upgraded to different versions since it comes to action. Currently Kerberos version 5 is in use. The main entities used are key distribution centre (KDC), authentication server (AS) and ticket-granting server(TGS). Control node at cloud acts as interface between cloud and client. Control node receives the requests from clients and must check each client for identification.

Cloud Server or Control node must have the ability to check the identities and authenticity of the clients before granting access to subscribe services [13]. Task for each client/server interaction, server can be required to undertake this .but in a loud computing like open and shared environment , this places substantial burden on each server. By using Kerberos, Authentication Server (AS) does this work on behalf of Cloud Server, who knows the password of all users and stores them in a centralized database. AS then interacts with the Ticket Granting Server (TGS) that grant a master ticket to the clients to access all the subscribed cloud services for a session. In cloud system a client has to login every time, whenever he/she wants to access services for a session even if he/she is using same service further. This unnecessary login of an authorized client waste a lot of time .To reduce this drawback we proposed a scheme in which the client can have access to subscribed services for the entire session. One full session can be of 8, 9 or more hours. By this it minimize the number of times that a client has to logon. Suppose every ticket is once usable. If the user wants to access the same or different services at the server at different times after once logon, re-login is required for every attempt. This situation can be improved by making the ticket reusable.

3.1 Problem Identification

There have been a lot of work already done to provide security to data stored at cloud but In nearly survey done about cloud computing the primary reason provide for not adopting is security reason. Security is still a main reason for not completely believing in cloud. There may be various possible attacks on data like Physical and Environmental attacks. It may destroy data stored at server side. Although data scattered on various server so it is possible to reconstruct data again but what if the encryption key has lost due to these attacks? Then there is no possibility to decrypt data. This is serious problem. Second problem is ,Security to data stored is provided through an encryption algorithm, but what if encryption key is known by third party or unauthorized user?

3.2 Problem Solution

First problem can be solved if the encryption key is divided into multiple parts and these parts may be stored at different servers, so if any server which is having a part of key has stopped due to any problem, other parts of key are still secure and can be used for decryption.

By providing multi party authentication to the secure data, problem of security can be solved. Multiparty authentication is a process of authenticating by not only a single user but there are more than one authenticator are required to access a service. This can be achieved by using threshold cryptography in Kerberos.

3.3 Kerberos

Here Kerberos is used for providing authentication for a client who want to access the applications stored at server side. Some another reasons for using Kerberos is, in Kerberos user password never travel over the network, never stored in any form on the client machine and it never be stored in unencrypted form and mutual authentication. Awareness of authenticity of user and server to each other is known as Mutual authentication. Fig 3.1 shows main components of Kerberos and its transaction of messages between the component.

3.3.1 Authentication Sever (AS)

Authentication Server issues a ticket granting ticket to users. User sends their user name to server. Server responds with TGT encrypted with user’s password. User enters password on client-if correct the TGT is successfully decrypted.

3.3.2 Ticket Granting Sever (TGS)

Logically different from the AS but may reside on the same server. User contacts when a network service is desired. Service ticket request is encrypted with session key provided by the in the TGT, not user’s password.TGS authenticates tickets and issues a ticket for the resources as well as the encryption key to use with communication with the service.

3.3.3 Network Sever

Client sends resource ticket and authenticator to the service encrypted with the client/server key. Server verifies both and issues a return message with a modified version of timestamp in the authenticator encrypted with client/service key. views message- if timestamp is modified correctly the service is genuine and ready to process request.

Since all authentication process is controlled by a centralized Key Distribution Centre, compromise of this authentication infrastructure will allow an attacker to impersonate any user by getting the knowledge about the key. So we use Threshold Cryptography algorithm to divide Ticket Granting Server into multiple parts to allow multiparty authentication, it means one cannot decrypt the key until the predefined numbers of parts of TGS are not available. Second reason for using Threshold Cryptography algorithm is to provide more availability to the TGS. In a traditional Kerberos authentication system if TGS got deactivated due to any reason, then all the system get affected and the whole procedure of authentication get shut down. To avoid this type of system failure in this paper we are proposing a Threshold Cryptography algorithm which will divide our TGS into n parts and at least k parts are need to make an useful information. Here k is always smaller than n.

3.4 Threshold Cryptography

Reason for using threshold cryptography is to provide more security to the key used by secret share scheme. In this scheme data D is divided into n pieces and knowledge of some pieces k is enables to derive secret data D. knowledge of any pieces k-1 makes secret data D completely undetermined. Such a scheme is called a (k, n) threshold scheme. This scheme is easily computable when it has necessary data available. This is a safe and convenience method to provide security to key.

Mathematical Derivation of Threshold Cryptography Algorithm:

Suppose using (*k*, *n*) threshold scheme to share our secret S. Choose at random k-1 coefficients and $a_0, a_1 \ldots\ldots\ldots\ldots a_{k-1}$. Let a_0 =S. Then we can build the polynomial to divide the key as:

(

$$\mathrm{q(x) = a_0 + a_1x + a_2x^2 + \cdots \ldots \ldots . + a_{k-1}x^{k-1}}$$

subset of k pairs, can find S using interpolation. The secret is a constant term a_0. For an Example:

S= 1234, n=6, k=3

Randomly two numbers: a_1=166, a_2=94 are used to produce the polynomial:

$$\mathrm{q(x) = 1234 + 166.x + 94.x^2}$$

Six points are obtained from the polynomial: (1, 1494); (2, 1942); (3, 2578); (4, 3402); (5, 4414); (6, 5614). So that each participant can get different single point (both x and q(x)).

To reconstruct the secret:

In order to reconstruct the secret S, *k* points will be enough. Let k=3 and consider (2, 1942); (4, 3402); (5, 4414). It is possible to construct q (x) by using Lagrange’s polynomial, and the value of S can also be derived. Let us consider (x0, y0) = (2, 1942); (x1, y1) = (4, 3402); (x2, y2) = (5, 4414).

Lagrange’s polynomials can be computed as :

$$l_0 = \frac{x-x_1}{x_{0-x_1}}.\frac{x-x_2}{x_{0-x_2}} = \frac{x-4}{2-4}.\frac{x-5}{2-5} = \frac{1}{6}x^2 - 1\frac{1}{2}.x + 3\frac{1}{3}$$

$$l_1 = \frac{x-x_0}{x_{1-x_0}}.\frac{x-x_2}{x_{1-x_2}} = \frac{x-2}{4-2}.\frac{x-5}{4-5} = -\frac{1}{2}.x^2 + 3\frac{1}{2}.x - 5$$

$$l_2 = \frac{x-x_0}{x_{2-x_0}}.\frac{x-x_1}{x_{2-x_1}} = \frac{x-2}{5-2}.\frac{x-4}{5-4} = -\frac{1}{3}.x^2 - 2.x + 2\frac{2}{3}$$

$$f(x) = \sum_{j=0}^{2} y_{j.l_j}\ (x)$$

$$f(x) = 1942.\left(\frac{1}{6}x^2 - 1\frac{1}{2}x + 3\frac{1}{3}\right) + 3402.\left(-\frac{1}{2}x^2 + 3\frac{1}{2}x - 5\right) + 4414.\left(\frac{1}{3}x^2 - 2x + 2\frac{2}{3}\right)$$

$$= 1234 + 166.x + 94x^2$$

Remember that the secret is the free coefficient, which means that S=1234, and as it is similar to the equation 5.2.

3.5 Working Model

3.5.1 Initial Authentication to the client

Whenever a cloud wants to access a service from cloud server it requires a Kerberos ‘Ticket’ before it will honour client request. Only on the basis of that ticket the cloud server will grant access to all the subscribed service to client. This ticket proves client’s authentication to server. This removes overhead of cloud server for performing authentication checks and also saves cloud’s processing and memory.

To get ticket client first request authentication from authentication from the Authentication Server (AS). The AS creates a “session key” (which is also an encryption key) basing on client’s password and a random value that represents the demanded service. The session key is adequately a “Ticket Granting Ticket”, that will be used by the client to get master ticket to access services from the client server.

3.5.2 Ticket Granting Ticket (TGT)

Ticket Granting Ticket perform a ticket exchange to obtain service granting Ticket. Client next sends the Ticket Granting Ticket to a Ticket Granting Server (TGS). In traditional Kerberos Authentication Model there is only one TGS, so if the master key sent by TGS is known by someone, then one who is not authorized can use the services provided by the cloud server. It makes data unsafe.

To avoid this failure, a security algorithm known as Threshold Cryptography Algorithm, is applied at TGS. Through this algorithm instead of single TGS, multiple TGS (n) have been used where at-least k number of parts are needed to decrypt the master key (where k< n). Client sends a request for master key to k number of TGS. If k number of TGS reply ,then the client can get the required master key otherwise client will send the request to TGS[k+1] and wait for reply. This process will continue until at-least k no. of TGS will not reply. After getting the master key client can request the required service form the service provider. This whole procedure is illustrated in fig 1.

The server either rejects the ticket or accepts it and performs the service. The master key granted to client can only be decrypted by the cloud server with the secret key shared between the cloud server and TGS. Client or anybody else will never be able to decrypt the master ticket. Since the ticket client has received from the TGS is time-stamped , it allows client to make additional request using the same ticket within a certain time period (typically, 8 hours) without need to prove authentication again. As the ticket is valid for a limited instance of time, this makes fewer chances that anyone else will be able to use it later. A flow chart for understanding the working of new authentication model is describe in Fig 2.

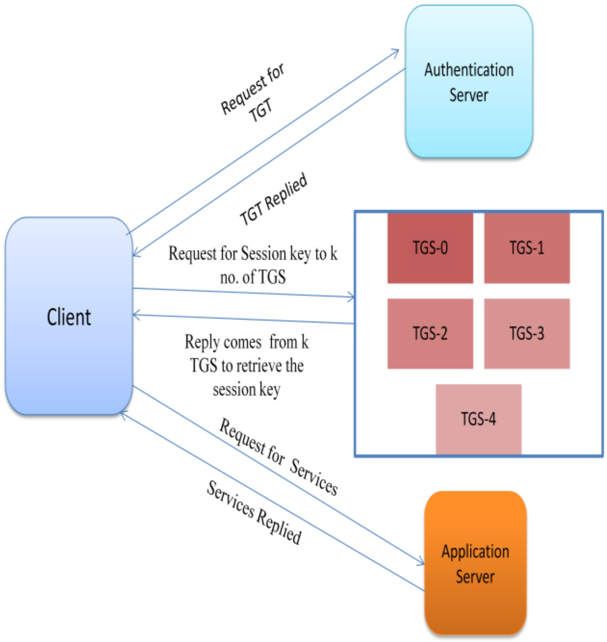

Fig. 1: Kerberos using Threshold Cryptography where n=5 and k=3

The control node at cloud receives the client request. It acts as the mediator between the data centre/cloud service provider and external user/brokers. It examines the service request, executes accounting and costing functions, keeps tracks of availability of Virtual Machines and their resources entitlements and also starts the execution of accepted service request on Virtual Machines those are allocated.

Kerberos Authentication model is itself responsible for providing authentication to the client, besides by using Threshold Cryptography in Kerberos Authentication model the security of the data stored at server side increseses at a high level. Also the availability of secure key is incresed. In traditional approch, key may be lost due to some environmental problems such storm, earthquake or any weather disaster or some other administrative problems such as leaving of an employ involved in a major project in the middle of the project. In our approch multy authenticity is provided to the key it means untill a particular number of parts are not presented no body can hack the key and in the second point of view if total no. of parts are not available and only pre specified no. of parts are available then also one can decrypt the data. This approch is usefull to provide more availability to the key. So that this is a more usefull and efficient approch for providing security and increse availability than previous one.

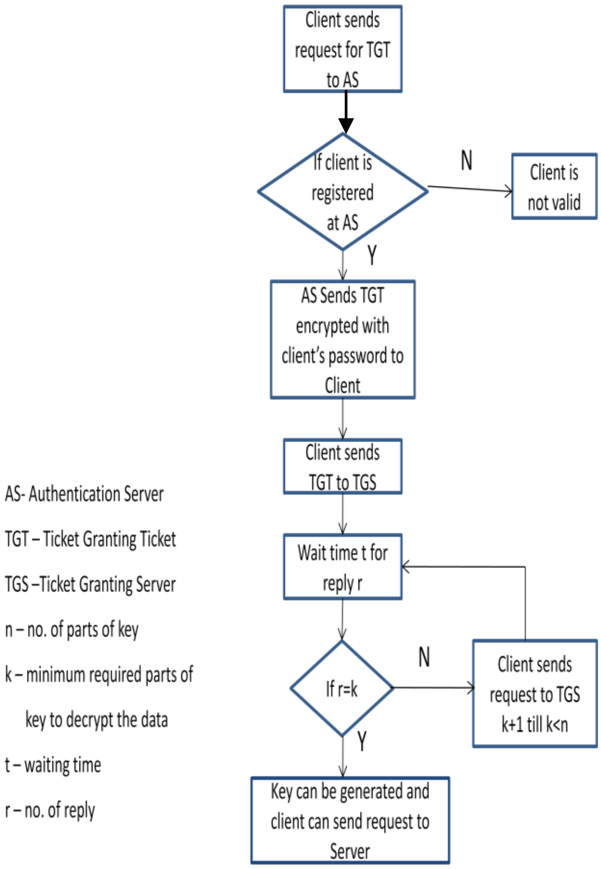
Client sends request for TGT to AS
If client is registered at AS
N
Client is not valid
Y
AS Sends TGT encrypted with client's password to Client
Client sends TGT to TGS
Wait time t for reply r
If r=k
N
Client sends request to TGS k+1 till k<n
Y
Key can be generated and client can send request to Server
AS- Authentication Server
TGT – Ticket Granting Ticket
TGS –Ticket Granting Server
n – no. of parts of key
k – minimum required parts of key to decrypt the data
t – waiting time
r – no. of reply

Fig 2: A flow chart for describing the new authentication algorithm

4. CONCLUSION

In this paper we discussed the need of authentication in cloud computing environment and a new approach for authentication. There have a lot of work already been done for providing security to clouds and also to provide authenticated user and services but in this paper a novel approach based on Kerberos authentication using threshold cryptography have given for a strong and more secure protocol. This approach is also useful for improving the availability of encryption key.

In future another framework can also be used to provide more security to cloud environment.

5. REFERENCE

[1] Mehdi Hojabri, K.venkat rao "Innovation in Cloud Computing: Implementation of Kerberos version5 in cloud computing in order to enhance the security issues" IEEE, International Conference on Information Communication and Embedded System(ICICES), 2013, pp 34-45.

[2] Jeong-Kyung Moon, Jin-Mook Kim and Hwang-Rae Kim, "A Secure Authentication Protocol for Cloud Services", Journal Of Advanced Information Technology And Convergence, 2012, pp 33-36.

[3] Jeffrey Lok Tin Woo, and Mahesh V., "Tripunitara Composing Kerberos and Multimedia Internet Keying (MIKEY) for Authenticated Transport of Group Keys" , IEEE, Transactions on Parallel and Distributed Systems, 2013, pp 1-11.

[4]] X. Zhang, H. Du, J. Chen, Y. Lin, L. Zeng "Ensure Data Security in Cloud Storage" International Conference on Network Computing and Information Security,2011, pp. 284-287.

[5] Rosa Sánchez, Florina Almenares, Patricia Arias, Daniel Díaz-Sánchez, Andrés Marí

n "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing", IEEE, Transaction on Consumer Electronics, 2012, pp 95-103.

[6] M. R. Tribhuwan, V. A. Bhuiyar, S. Pirzade "Ensuring Data Storage Security in Cloud Computing through Handshake based on Token Management" IEEE, International Conference on Advances in Recent Technologies in Communication and Computing,2010, pp. 386-389.

[7] Ming-Huang Guo, Horng-Twu Liaw, Li-Lin Hsiao, Chih-Yuan Huang, Chih-Ta Yen , "Authentication Using Graphical Password in Cloud", IEEE, 15th International Symposium on Wireless Personal Multimedia Communications, 2012, pp 177-181.

[8] Sanjeev Pippal, Vishu Sharma, Shakti Mishra, D.S.Kushwaha , "An Efficient Schema Shared Approach for Cloud based Multitenant Database with Authentication & Authorization Framework", 2011, IEEE, International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pp 213-218.

[9] W. Itani, A. Kayssi. A. Chehab "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures" Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing,2009, pp. 711-715

[10] Sushmita Ruj∗, Milos Stojmenovic†, Amiya Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2012, pp 556-563.

[11] Lifei Wei, Haojin Zhu, Zhenfu Cao, Weiwei Jia and Athanasios V. Vasilakos, "SecCloud: Bridging Secure Storage and Computation in Cloud", IEEE 30th International Conference on Distributed Computing Systems. 2010, pp 52-61.

[12] Hassan Takabi, James B. D. Joshi, Gail-Joon Ahn, "Secure Cloud: Towards a Comprehensive Security Framework for Cloud Computing Environments", 34th Annual IEEE Computer Software and Applications Conference Workshops,2010, pp 393-398.

[13] Jinyue Xia and Yongge Wang, "Secure Key Distribution for the Smart Grid", IEEE, Transactions On Smart Grid, 2012, pp 1437-1443.

[14] C.C. Tan, Q. Liu, and J. Wu, "Secure Locking For Untrusted Clouds" , 4th IEEE International Conference on Cloud Computing, 2011, pp. 131-138.

[15] Farhan Bashir Shaikh and Sajjad Haider, "Security Threats in Cloud Computing", Sixth IEEE International Conference on Internet Tehnology and Secure Transaction , pp 120-126.

[16] Ashish G. Revar, Madhuri D. Bhavsar, "Securing User Authentication using Single Sign-On in Cloud Computing", IEEE, International Conference On Current Trends In Technology, 2011, pp 1-4.

[17] Zubair Ahmad and Jamalul- Lail AbManan, "Trusted Computing based Open Environment User Authentication Model", 3rd IEEE, International Conference on Advanced Computer Theory and Engineering ,IEEE,2010,pp 487-491.

[18]www.wikipedia.com