Volume 5, Issue 6, June 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure Key for Authentication and Secret Sharing in Cloud Computing

[1]Dr. Santosh Lomte, [2]Shraddha Dudhani

[1]Principle, Everest Education Trust College of Engineering and Technology, Aurangabad, Maharashtra, India
[2]Department of MCA, Dr.D.Y.Patil Institute of Management and Research, Pimpri, Pune, Maharashtra, India

Abstract: Now a days the cloud computing is emerging and versatile technology. The requirement of IT industry is to storage terabyte data generated by every day. For storage IT requires many of hardware, software and network infrastructures. Cloud computing solve this problem in cost effective manner. It has completely changed the scenario not only IT Industry but some other sectors like education, healthcare sector. It has capability to provide servers for wide range of resources from research to E commerce. Cloud computing is growing very fast because of their features like resource capability, network infrastructure, storage capability, cost effective, quick access of information. On other side all data is virtual and cloud is as open services and they are using public network for their application and services, which in turn has question on security issues like authentication data loss. In this paper authentication model is proposed using Kerberos technique and threshold cryptography

Key words: security, Kerberos, authentication

I. INTRODUCTION

Cloud computing is one of the robust and dominant technology in present scenario .it offers services in least cost manner. Than traditional approach .user can easily uses all services of cloud and share their data. The standard services offer by cloud computing is like cloud storage, i cloud, Google drive.

Cloud provide best feature but everything is through internet so that there are chance of hacking of data.

we know there are many security issues in cloud computing like network and data security are the broad areas .In data security there are many issues like access control, data integrity, data Confidentiality, data, data integrity data location, data availability authentication. All the security issues are sensitive but most important and skepticism subject is data authentication. Authentication mechanism helps to establish proof of identities. The authentication mechanism process ensures that the origin of electronic message or document is correctly identified. For data authentication login and password is mandatory provided by cloud service provider the authentication mechanism may be applied in both domain and workgroup. Once password is hacked by the hacker authentication is lost and attacks on available data which can be modified, deleted. Therefore we try to propose new model that can solve problem of authentication so that authorized user can get all services provided by cloud provider .in this paper we are proposing new security mechanism based on Kerberos protocol and threshold cryptography Many real life systems use an authentication protocol called Kerberos.

II. RELATED WORK

Authentication process provides password and login. But on public network the password is easily hacked by the hacker so that there are many mechanism are used like key infrastructure where we are commonly used symmetric and asymmetric algorithm .one of the more popular algorithm in asymmetric is RSA. It uses with Kerberos authentication protocol. RSA is very strong protocol but there is some disadvantage of this method generating keys over head of keys. Symmetric protocol is also used for secure authentication. Best algorithm of symmetric scheme is Diffie Hellman algorithm but again there are some disadvantage of this scheme is key exchange problem. So public key infrastructure having some disadvantage. Authentication Using Graphical Password in Cloud is also one method it resist to common attacks and improve security in cloud computing. Securing user authentication using single sign in on cloud .it is one of the optimized solution it reduces number of password and login. But again there is disadvantage multiple user can not be involved secure locking for untrusted clouds mechanism.

There is some disadvantage of public key infrastructure. So there is another concept called secret sharing scheme. In which secret is divided in to the parts and distribute among trusted dealer.

When someone else wants secret again combine all parts of secret and reconstruct original one

This secret solves the problem of key exchange

III. PROPOSED WORK

The authentication is the process to authenticate client before enter in cloud it is not just putting password and login. Authentication is most sensible issues in cloud for the same Kerberos is authentication protocol used in cloud was developed by MIT Labs in 1980. It is the protocol that works with four parties

1. Client station
2. authentication server
3. Ticket granting server
4. Server offers services

Kerberos is mainly works on ‘Ticket’ to communicate with other user communicate over non secure data.

IV. PROBLEM STATEMENT

As security is sensitive issue in cloud computing .the data are coming from cloud using public network (internet) there are chances to hack the data. There have been lot of work done on security issues and challenges but still there is not 100% full proof solution. There are many physical and some other attack on data that destroy data on server. one solution for that is scattered the data on more than one server instead of one server .but this not solve problem completely because data stored in encrypted mode using encryption key .the attackers attack on key and may be hack the data.

V. PROBLEM SOLUTION

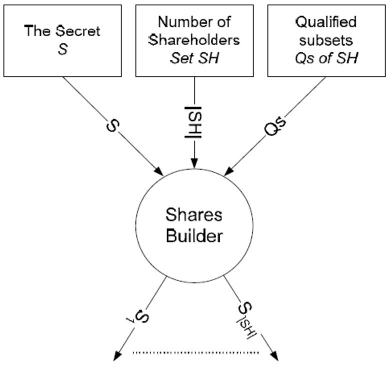
Attackers attack on data that is placed on same server. So that solution is do multiple copies of same data and data is placed on multiple servers. But data is encrypted by encrypted key. Attackers may be attack on key so that data is revealed to the attackers. The solution of this problem is instead of putting multiple copies of data on different server we are applying Shamir’s secret sharing on key. The encrypted key is divided into number of parts and stored them on different server. But again if attackers attacks on one of the server that part of the key is lost but still we can reconstruct the key using Shamir’s threshold scheme which uses threshold value it is applied on the key. The most famous perfect secret sharing scheme is the (k, n)-threshold scheme first proposed by Shamir in 1979 and hereafter referred to as a Shamir threshold scheme A key can be reconstructed again with minimum number of secret that are on different server there is no problem if attackers attack on one server

The reaming server can reconstruct key. This Shamir’s scheme overcome problem of key exchange .Shamir’s scheme uses lag ranges of polynomial to divide the key in number of pieces

Secret sharing refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own. More formally, in a secret sharing scheme there are one dealer and n players. The dealer gives a secret to the players, but only when specific conditions are fulfilled. The dealer accomplishes this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of fewer than t players can. Such a system is called a (k, n)-threshold scheme (sometimes it is written as an (k-n) threshold scheme).

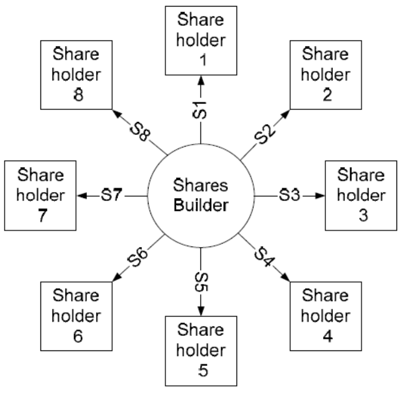
Phases of Secret Sharing

1. Shares building phase.

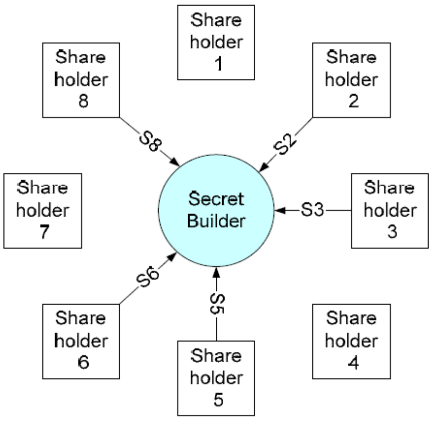


In this phase share builder gentates secrect ,genrate shares holder and assigien threshold valu on secrect

2. Shares distribution phase.



3. Secret reconstruction phase.



. The idea behind this construction is simple and elegant. A Shamir (k, n)-threshold scheme is defined over Zp. Each participant Pi is associated with a unique non-zero xi (which is not secret). If the secret is s, the dealer randomly chooses a polynomial f(x) of degree at most k − 1 defined over Zp such that f(0) = s. The dealer then securely issues participant Pi with share f(xi). The Shamir scheme has perfect privacy since knowledge of k − 1 share does not leak any information about the secret s. It also has recoverability since any k participants can interpolate their shares to recover the polynomial f(x) and hence the secrets.

VI. WORKING MODEL

As propose work is based on Kerberos authentication model. It has following steps

1. Authentication server:

Whenever a cloud wants to access a service from cloud server it requires a Kerberos 'Ticket' before it will honor 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.

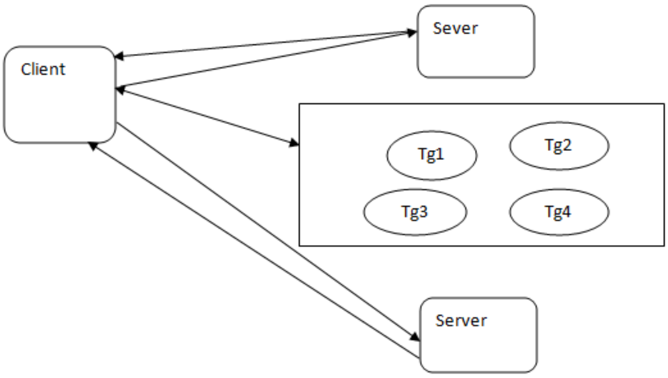
To get ticket client first request authentication from authentication from the Authentication Server (AS). The AS creates a "session key" (which is also an encryption key) basing on client's password and a random value that represents the demanded service. The session key is adequately a "Ticket Granting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

2. Ticket Granting Ticket:

Tickets Granting Ticket performs 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

In this phase the threshold security algorithm is used in Kerberos instead of only single ticket generating generate multiple ticket by TGS (n TGS) out of that some of them (k) are used to decrypt the master key where (k<n).client sends a request to k number of TGS .If k number of TGS reply then client obtain master key for using services of clients or otherwise it will try for new subset of TGS

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...



The Kerberos authentication model it can provide authentication to the client so that authenticate client can be used all services of cloud. Along with secret scheme is used for the data security it is reduced problem of key exchange and Also the availability of secure key is increased. In traditional approach, 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 approach multi authenticity is provided to the key it means until 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 data can not reveal to some unknown person

VII. CONCLUSION

In this paper we have discussed about the need of authentication in cloud computing .it is narrative approach of authentication by Kerberos and threshold cryptography so that encryption technique is more robust. There have lot of work done already on security issues and challenges but still there are loop holes. This work of fiction is unique approach because propose scheme minimizes the problem of exchange of key that are generally occurs in symmetric and asymmetric key cryptography.

VIII. FUTURE WORK

We have discussed novel approach for security of authentication but threshold cryptography divide secret and store in different server. That means server is trusted entities but some authorized user itself changes the key structure that is stored as part of secret on server then next time some authorized user uses that secret to part reconstructed .but that key cannot be formed because one or more part of secret are not original secret that are involved to reconstruct key. We can enhance this work for identification and detection of cheater among share holder that holds the part of secret

REFERENCES

[1] N.Hemalatha ,A.Jenis,A.Cecil,L.Arockiam “Encryption Technique and Security Issues in Cloud Computing “International Journal of Computer Application volume 96-No-16 June 2014

[2] S.Srinivsan “Is Realistic In Cloud Computing?” International Information Management association ,Inc 2013

[3] Rajarshi Roy ‘security in Cloud Computing ‘International Journal of Computer Application volume 96 –No-15,June 2014

[4] Donald ,A.Cecil,S.ArulOliandL.Arockiam ‘ Mobile Security Issues and Challenges’ perspective International Journal of Electronics and Information 2013

[5] Prof. DivyakantMeva, Dr. C. K. Kumbharana ‘Issues and Challenges of Security in Cloud Computing Environment’ International Journal of Advanced Networking Applications ISSN No. : 0975-029

[6] Masudur Rahman, Wah Man Cheung ‘A Novel Cloud Computing Security Model to Detect and Prevent DoS and DDoS Attack’ International Journal of Advanced Computer Science and Applications,Vol. 5, No. 6, 2014

[7] M.Muthumani, Mrs.M.Kavitha, , Dr.S.Karthik ‘Survey on Improved Security in Public Cloud ‘International Journal of Advanced Research in Computer Science Volume 5, No. 8, Nov-Dec 2014

[8] Mladen A. Vouk ‘Cloud Computing – Issues,Research and Implementations’ Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[9] Allen Oommen Joseph , Jaspher W. Kathrine and RohitVijayan ‘Cloud Security Mechanisms for Data Protection: A Survey’ International Journal of Multimedia and Ubiquitous Engineering Vol.9, No.9 (2014), pp.81-90

[10] Heng He, Ruixuan Li, , Xinhua Dong, and Zhao Zhang, ’Efficient and Fine-Grained Data Access Control Mechanism for P2P storage cloud’ IEEE Transactions on Cloud Computing, Vol.2, no.4, October-December 2014.

[11] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and MircoMarchetti ‘Scalable Architecture for Multi-User Encrypted SQL Operations on Cloud Database Services’, IEEE Transactions on Cloud computing, vol.2, no.4, October-December 2014.