A Survey on Kerberos Based Parallel Network File System using Visual Cryptography in Cloud Computing

J.Velmurugan[1] A.Jayanthi[2] E.Ajitha[3] D.Anuja[4] R.Swetha[5]
[1,2,3]Assistant Professor [4,5]Student
[1,2,3,4,5]Department of Information Technology Engineering
[1,2,3,4,5]Vel Tech Hightech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai - Avadi

Abstract— In today's world, cloud computing is the developing technology. There exist some security risks in this type of virtual technology. To overcome this, user authentication is used for the defense purpose. This paper gives an outline of kerberos protocol using visual cryptography in cloud. Kerberos is one of the most popular authentication protocol used in networks. This protocol uses a trusted third party for authentication .Our work also focuses onto parallel Network File System(PNFS) which makes practise of kerberos to offer parallel session keys between client web service and cloud web service .Using visual cryptographic , the session key along with username and password is encrypted in the form of an image to reduce the impact of security risks .Thus, our proposed outline makes the kerberos protocol vigorous, protected, escrow-free and provides full forward secrecy.

Key words: cloud computing, kerberos, parallel network file system, visual cryptography

I. INTRODUCTION

Cloud computing is the transfer of computing facility over the internet. Cloud service allows the usage of software and hardware by individuals and business, that are managed by third parties at secluded positions. On the availability of network connection, the cloud computing model allows access to data and computer resources. Cloud computing offers a common pool of resources ,including data storage space ,networks ,computer processing power , and dedicated corporate and user applications. The features of cloud computing are on-demand service, resource pooling, rapid elasticity and measured service. The services offered by cloud are made available through a private cloud, community cloud ,public cloud or hybrid cloud. Cloud services are popular because of low cost and complexity of owing and operating computers and networks. Along with benefits, there are some privacy and security concerns too. Cloud provides services to multiple customers simultaneously. This may give rise to several possible attacks.

Kerberos is a authentication protocol in which Key Distribution Center(KDC) issues a ticket in an encrypted form. The three main components of kerberos protocol are as follows:

1) Client: Clients are the one who requests the services from the application servers.
2) Key Distribution Centre(KDC):The KDC offers authentication service and key distribution functionality. It contains the secret key required for establishing the communication. It has 2 components:

– Authentication server (AS): The authentication process is done by AS. If any new user registers with the AS by providing the user ID and secret password which is already present in the database. The AS verifies the username and password and issues the session key and sends a ticket to the client.
– Ticket Granting Service (TGS): The application server establishes the session by getting the ticket from TGS. A session key is provided between user and application server. User checks its ID once with AS and contacts TGS multiple times to get tickets for different servers.

3) Application server: The application server provides services based on the user's request.

Kerberos authentication process has the following steps:
Step1: Client sends request for service by giving their ID together with the ID of Ticket Granting Service (TGS) to the Authentication Server (AS).
Step2: AS replies with the ticket that is encrypted with a key derived from user's password. Client decrypts the message and if the password is correct, the ticket is successfully recovered.

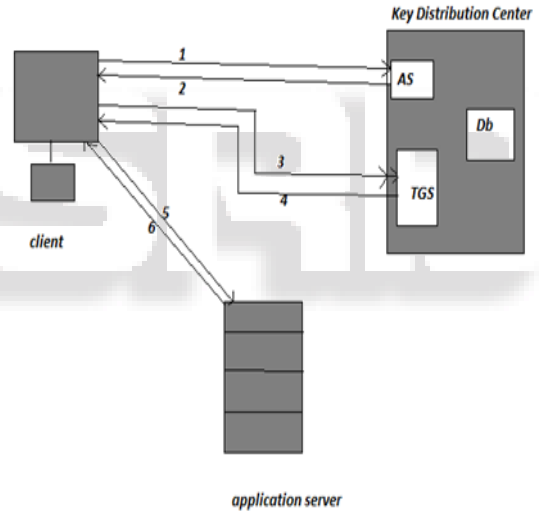

Fig. 1: Kerberos architecture

Step3: Client requests for the Service Granting Ticket (SGT).This is done by transmitting a message to the TGS containing the user's ID, service ID and TGT.
Step4: TGS decrypts the ticket from the user and verifies the ID. It checks to make sure that the lifetime has not expired. Then, it relates user ID and network address with the received information to authenticate the user. If this becomes successful, TGS issues a Service Granting Ticket (SGT) by using which user is allowed to access the server.
Step5: After getting SGT from TGS, client forwards this ticket along with user ID to the server in order to use a service. The server verifies this ticket and authenticates the user.
Step6: Finally, server opens the conversation with client and perform inverse authentication after successfully verifying the user information.
In this work, the problem of simultaneous many communications in large scale network file systems (NFSs) that support parallel access to multiple servers is investigated.

Parallel Network File System (PNFS) is a communicational model, where there are large number of clients accessing multiple remote and distributed storage devices in parallel. Here, key materials are exchanged and parallel secure sessions is established between clients and the servers in the PNFS.

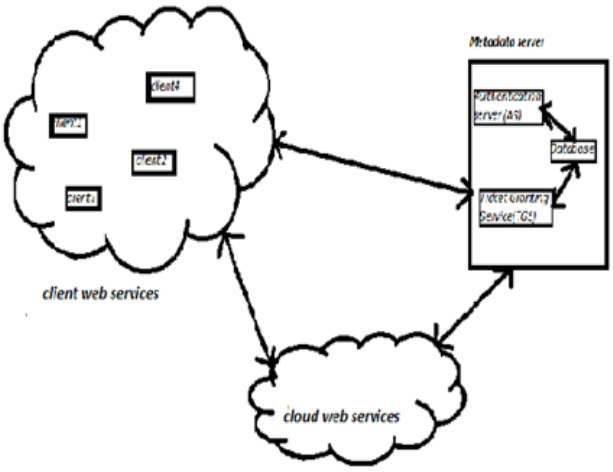

Fig. 2: Concept of parallel Network File System (PNFS)

II. SECURITY ISSUES IN CLOUD:

Attacks are the most important problem in cloud services.

1) Attack due to replay: Getting the data in progress and then replaying it later produces unauthorized effect. To avoid this type of attack, Kerberos uses timestamp mechanism. This requires synchronization of clocks. When the user's request is authenticated within required time, the attackers observers it and repeats the information within that time and timestamp mechanism would become useless.
2) Attack of password: The secret key generated from user's password may be vulnerable to dictionary attack, if the password is not strong.
3) Problem due to key storage: As symmetric key algorithm is used for encryption and decryption, a secret key need to be pooled between clients and KDC, between AS and KDC, between KDC and distant KDC. This makes key management and maintenance, a tedious problem.
4) Malware Attack: The system that is designed to act as KDC may be modelled by the attackers in such a way that it comprises built-in listeners. Then, the attackers can fool the users by installing malware. This listens to the users actions including password. Thus, the attackers can easily attack KDC, and masquerade as KDC to complete the man- in- the- middle- attack.
5) Authentication Problem: In Kerberos 5 a new characteristics called authentication forwarding is added. When a client is granted access to a server, it lets this server to act as a client for another server. This points to springboard attack. There is no such problem in Kerberos 4, as it does not support authentication forwarding.
6) Unauthorize Access of Database: The database of Kerberos contains all the user credentials. It must be secured very carefully, otherwise the database may be conceded by the attacker and the attacker can easily access the important things such as usernames and passwords of the clients.
7) Single Point Failure: KDC must be available continuously for Kerberos protocol. If the KDC is down, the system may undergo single point of failure. This may be solved by using multiple KDC in Kerberos protocol.
8) Clock Synchronization: Use of timestamps generates the problem of synchronization of clocks. For communication, the system clock of client must be synchronized with the server clock. If the synchronization of client clocks does not take place, the authentication becomes unsuccessful.
9) Digital Signature in kerberos: The verification of the essentials of the user and the exchange of keys is done by kerberos, but it cannot fulfill the purpose of digital signature. Thus, it cannot offer the undisputable tool.

III. EXISTING SYSTEM:

Paper[1] describes that authenticated key exchange protocol for concurrent access network file system. This is achieved by three way authentication. First, reducing the workload of metadata server. Second, providing forward secrecy. At last, providing escrow freeness. It approaches to boost the performance and scalability of the scheme and parallel secure session between client and service provider. It provides escrow freeness and overcomes the forward seceracy issue.

Paper[2] describes the methodology of preserving the confidential information by image share security with the help visual cryptography whereas it provides high degree of correlation. This paper prevents from phishing attack and also identify whether it is an authentic user.

Paper [3] describes that data security in cloud service provider by application of kerberos authentication service. This is done with DES (data encryption standard) algorithm. It ensures the authenticated user to gain access. Basically, this system implements the Kerberos authentication service in cloud service provider

Paper[4] describes the two factor authentication for secure communication-One factor as secret share and another factor for client private key. It approaches to enhance the security and security attack by combination of visual cryptography algorithm and digital envelope technique in the Kerberos authentication protocol. By this, mutual authentication achieved. Therefore, it solves the distribution of keys and synchronization of clock issues and improves the effectiveness. This is done with AES (advanced encryption standard) algorithm and ECC algorithm.

Paper[5] describes the key management in large scale distributed system by establishing the lightweight key management technique. This system introduce file system security architecture(FSSA) for key management problem and for improving the security.

IV. PROPOSED SYSTEM:

In our proposed scheme, the main aim is to reduce the load of key distribution server and to provide strong authentication. Here, multiple clients web service can access the application server simultaneously. In general, key distribution server is used to create all the service tickets and session keys between client web service and cloud server by placing heavy load on it. In our solutions, client web service first computes some key materials and forwards them to key distribution server, which in response, issues the corresponding authentication

tokens. It is not necessary that client web service must compute the key materials before each access request. Instead, this is at the done at the start of the pre-defined validity period. For each request to access one or more application servers at a stipulated time, client web service calculates a session key from the pre-computed material. Thus, the load of producing session key by metadata server is reduced.

The modified kerberos allows the clients to generate its own session keys. The key material is used to generate session keys. To address key escrow while achieving forward secrecy, visual cryptographic technique is incorporated into kerberos-based PNFS. In visual cryptography, the session key along with username and password is encrypted in the form of an image. Two shares of images are produced, out of which one share of image is to be retained with the client web service and the other share and the original image is to be saved with the KDC. The modified kerberos-based PNFS is as follows:

Step 1: In the first step, the client sends its user name, password and secret image to the AS.

Step 2: In the KDC, the secret image is encrypted in any format which is not even known to the client. The AS generates the ticket and sends it to the client along with the username and password.

Step 3: After receiving the tickets, client verifies it whether the ticket belongs to it or not. If the verification is successful, client sends this ticket to the TGS for getting the session key.

Step 4: TGS, present in KDC, verifies the TGT(ticket generated from AS) with the help of database. Then, it sends Service Granting Ticket (SGT)to the client, which contains the secret session key used for exchange of information with the cloud service provider.

Step 5: Then, the client forwards secret session key (which has been shared between the client and key distribution server) to the cloud server.

Step 6: At the last, the cloud server responds the client by sending the acknowledgement for the requested service. Then, the file can be uploaded by the client in the server.

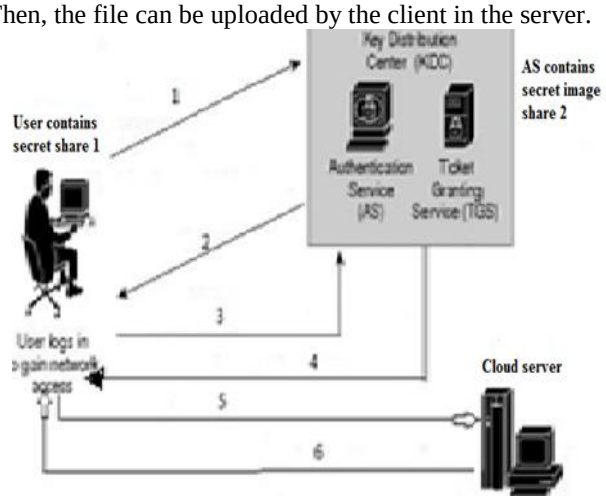

Fig. 3: Kerberos-based pNFS using visual cryptography

The following graph represents the security be achieved by Kerberos in cloud services.

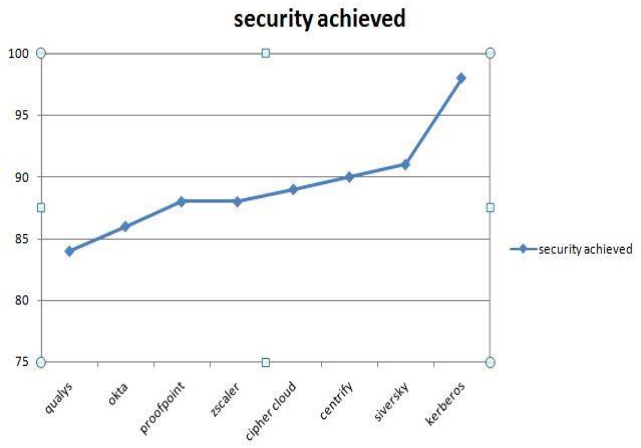

Fig. 4:

V. CONCLUSION

In this paper, we are including the technique of Visual cryptography into Kerberos-based PNFS protocol. Visual cryptography is a pre-authentication technique used in kerberos. This provides more security for the user. Less computation intricacy and high security are some of the projecting features of Visual cryptography technique. The client generates its own session key by selecting some random key from the available ones. This prevents the attackers from hacking the session. This selection of random key is known only to the server. Here, we use parallel Network File System concept, where multiple clients can access the cloud server simultaneously. We ruminate this work as a inventive step towards the further development of Kerberos authentication protocol.

REFERENCES

[1] "Authenticated Key Exchange Protocol for Parallel Network File System", Hoon Wei Lim, Guomin Yang, Parallel and Distributed Systems volume:27, issue :1,2016.

[2] "Innovation in cloud computing: Implementation of kerberos version5in cloud computing inorder to enhance security issues", Hojabri, M. , Rao ,K.V. Information Communication and Embedded Systems (ICICES), Pages: 452 - 456,2013.

[3] "An Anti-phishing Framework using Visual Cryptography", Abhishek Thorat, Mahesh More, Ganesh Thombre,International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 2, 2015.

[4] "Two factor Authentication using Visual Cyptography and Digital Envelope in Kerberos", Khandewal, N.S., Kamboj.P lectrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 ,Pages: 1 - 6.

[5] "key management for large scale storage distributed Storage Systems" , .Hoon wei lim ,SPA Sophia antipolis research, france.

[6] "An extended review on visual cryptography schemes", Ramya.J, Parvathavarthini.B, Control, Instrumentation Communication and Computational Technologies (ICCICCT), Pages: 223 - 228, 2014.

[7] "Kerberos based authentication protocol with improved identity protection in 3G Network" A.P. Shrestha, K.J. Park, J.S. Park, D.Y. Choi, and S.J. Han, EEE Pacific Asia Conference on circuits, 2010, pp. 771-774.
[8] "An improved kerberos protocol based on Diffie-Hellman-DSA key exchange", Z. Hu, Y. Zhu and L. Ma, IEEE International Conference on Natural Language Processing, 2012, pp. 400-404.
[9] "Security analysis and improvement for Kerberos based on dynamic password and Diffie-Hellman algorithm" .C. Wang and C. Feng,IEEE 4th International Conference on Emerging Intelligent Data and WebTechnologies, 2013, pp. 256-260.
[10] "Kerberos based secure communication in wireless sensor network" , K. jain, U. Bahuguna, and N. Bishti,Conference on Advances in Communication and Control System (CAC2S), 2013, pp. 622-625.

