ISSN: 0976-3104
SPECIAL ISSUE: Emerging Technologies in Networking and Security (ETNS)
Chandravathi et al.

ARTICLE OPEN ACCESS

IMPLEMENTATION OF KERBEROS BASED AUTHENTICATED KEY EXCHANGE PROTOCOL FOR PARALLEL NETWORK FILE SYSTEMS IN CLOUD

C. Chandravathi[1], K. Somasundaram[2*], Ramesh Kandasamy[3], J. Velmurugan[1]

[1] *Department of Information Technology, Vel Tech High Tech Dr.RR Dr.SK Engineering College, Chennai, TN, INDIA*

[2] *Department of Computer Science and Engg, Aarupadai Veedu Institute of Technology, Chennai, TN, INDIA*

[3] *Department of Information Technology, Nandha Engineering College, Erode, TN, INDIA*

ABSTRACT

Aims: *In today's world, cloud computing is the developing technology. There exists some security risks and difficulties in accessing parallel network files in this type of virtual technology. To overcome this, concurrent access and user authentication is used for the defense purpose. This paper is based on kerberos protocol using visual cryptographic in cloud. Kerberos is one of the most popular authentication protocol used in networks* ***Materials and methods:*** *This protocol uses a trusted third party for authentication .Our work also focuses onto parallel Network File System(pNFS) and using kerberos to provide parallel session keys between client web service and cloud web service* ***Results:*** *Using visual cryptographic , the image is uploaded as an authentication services which is verified by the server and session key along with username and password is encrypted in the form of an image to reduce the impact of security risks.* ***Conclusion:*** *Thus, our proposed scheme will provide the kerberos protocol robust, secure, and escrow-free and provides full forward secrecy.*

Published on: 18th– August-2016

KEY WORDS

Cloud Computing, Kerberos, Parallel Network File System, Visual Cryptography

***Corresponding author:** **Email:** soms72@yahoo.com; **Tel.:** +91 9443467264 **Fax:** +91-44-2836 0198

INTRODUCTION

Cloud computing is the transfer of computing services which is done over the internet. Cloud service allows using software and hardware by individuals and business that are managed by third parties at secluded locations. Examples of cloud services include online storage, social networking sites, webmail, and online business applications. When the network connection is available, the cloud computing model allows access to data and computer resources from anywhere. Cloud computing offers a shared pool of resources ,including data storage space , networks ,computer processing power , and specialized corporate and user applications. The features of cloud computing include on-demand self- service, network access broadcasting, pooling of resource, elasticity and measured service. Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud. Cloud services are popular because they can reduce the cost and complexity of operating computers and networks [1]. While there are benefits, there are privacy and security concerns too. Data travelling over the internet and is stored in remote locations. In addition, cloud provides services to multiple customers simultaneously. This may give rise to several possible attacks [2].

Kerberos is an authentication protocol in this key Distribution Center (KDC) issues ticket encrypted with user's password. There are three main components of kerberos protocol:

1) Client: Clients are the users which request the service provider for service from the specific application servers.

2) Key Distribution Centre (KDC): The KDC provides authentication services and key distribution functionality. It contains user's and service's secret key. It consists of two components:

THE IIOAB JOURNAL
ISSN: 0976-3104

a) Authentication server (AS): The AS authenticates the users. If a new user registers with the AS, it provides the user ID and secret password to the user. The database contains the username and corresponding passwords. The AS verifies the user, issues a session key and sends a ticket to the client.
b) Ticket Granting Service (TGS): The TGS issues a ticket to the user for establishing session with the application server. It provides session key between user and application server. User verifies its ID just once with AS and can contact TGS multiple times to get tickets for different application servers.
3) Application server: The application server provides services for the requested user.
Kerberos authentication process takes place as follows:

Step1: Client requests service by sending its user's ID together with the ID of Ticket Granting Service (TGS) to the Authentication Server (AS).

Step2: AS responds with the ticket that is encrypted with a key derived from user's password. Client decrypts the incoming message and if the password is correct, the ticket is successfully recovered.

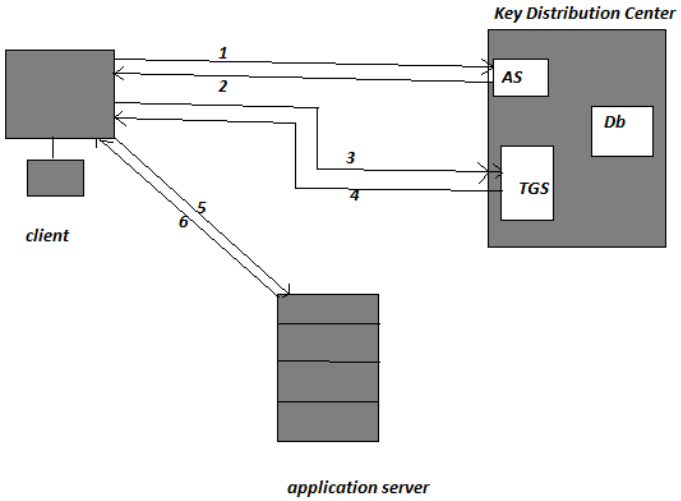


Fig.1. Kerberos architecture

Step3: Client requests Service Granting Ticket (SGT) by transmitting a message to the TGS containing the user's ID, service ID and TGT.

Step4: TGS decrypts incoming ticket and verifies the ID. It checks to make sure that the lifetime has not expired. Then it compares user ID and network address with the incoming information to authenticate the user. If 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 sends this ticket along with user ID to the server in order to access a service. The server verifies the ticket and authenticates the user.

Step6: Finally, server opens the conversation with client and perform reverse authentication after verifying user information successfully.

In this work, the problem of many-to-many communications in large scale network file systems (NFSs) that support parallel access to multiple storage devices is investigated. Parallel Network File System (pNFS) is a communication model where there is large number of clients accessing multiple remote and distributed storage devices in parallel. Here, key materials are exchanged and parallel secure sessions between clients and the storage devices in the pNFS are established [3].

Security issues in cloud

Attacks are the most important problem in cloud services.
1) Replay Attack: Getting the data in advance and then replaying it after some time produces unauthorized effect. To avoid replay attack, Kerberos uses timestamp mechanism. This requires synchronization of clocks. When the

THE IIOAB JOURNAL
ISSN: 0976-3104

user's request is authenticated within stipulated time, the attackers monitor it and replay the information within that time and timestamp mechanism would become waste.

2) Dictionary Attack: The secret key generated from user's password may be vulnerable to dictionary attack, if the password is not strong.

3) Key Storage Problem: As symmetric key algorithm is used for encryption and decryption in kerberos, a secret key need to be shared 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 which is designed to act as KDC may be modelled by the attackers in such a way that it contains built-in listeners. Then, the attackers can fool the users by installing malware. This listens to the users operations including password. Thus, the attackers can directly attack KDC, and masquerade as KDC to complete the man in the middle attack [4].

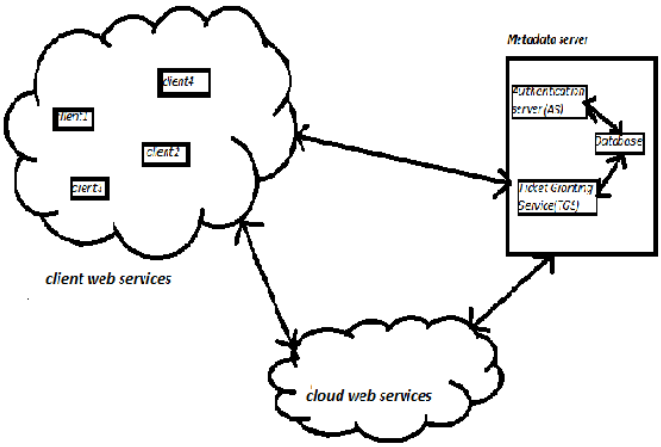


Fig. 2. Concept of parallel Network File System (pNFS)

5) Authentication Forward Problem: In Kerberos 5 a new feature called authentication forwarding is added.When a client is granted access to a server, it can let this server act as a client to apply for a other server. This leads to springboard attack. There is no such problem in Kerberos 4, as it does not support authentication forwarding.

6) Unauthorized Database Access: Kerberos database contains all the user credentials. It must be secured very carefully, otherwise the database may be compromised by the attacker and he/she can easily access the credentials such as usernames and passwords of the clients.

7) Single Point of 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 clock synchronization. For communication, the system clock of client must be synchronized with the server clock. If the client clocks are not synchronized with the Kerberos server clock, the authentication becomes unsuccessful.

9) Digital Signature: Kerberos verifies only the identities of the user and performs the exchange of keys, but it cannot fulfil the purpose of digital signature. Thus, it cannot provide the undisputable mechanism.

EXISTING SYSTEM

The existing system will describes that authenticated key exchange protocol for concurrent access network file system this is achieved by three way authentication firstly reducing the workload of metadata server. and secondly providing forward secrecy at last thirdly providing escrow freeness [4]. It approaches to enhance the

THE IIOAB JOURNAL
ISSN: 0976-3104

performance and scalability of the system and parallel secure session between client and service provider. It provides escrow freeness and overcomes the forward secrecy issue.

Likewise 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. And data security is provided by cloud service provider by implementation of kerberos authentication service. This is done with DES (data encryption standard) algorithm. It ensure the authenticated user to gain access. Basically this system implement the Kerberos authentication service in cloud service provider .therefore existing another service two factor authentication for secure communication one factor as secret share and another one for client private key [5]. It approaches to enhance the security and security attack by combination of visual cryptography and digital envelope in the Kerberos authentication protocol by this mutual authentication achieved therefore it solves the key distribution and clock synchronization issues and improves the efficiency. This is done with AES (advanced encryption standard) algorithm and ECC algorithm. and for parallel network file system implementing 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 [6].

PROPOSED SYSTEM

In our proposed scheme, the main aim is to reduce the workload of metadata server and to provide strong authentication Here, multiple clients web service can access the application server simultaneously. In general, metadata server is used to generate all the service tickets and session keys between client web service and cloud server by placing heavy workload on it. In our solutions, client web service first pre-computes some key materials and forwards them to metadata server and 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 beginning of the pre-defined validity period. For each request to access one or more application servers at a specific time, client web service computes a session key from the pre-computed material. Thus, the workload of generating session key by metadata server is reduced.

The modified version of 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 and visual cryptographic image for enhancement to security layer. Two shares of images is maintained in both client and server , visual cryptography images to be kept with the client web service and the another one and the original image is to be kept with the KDC. The improved kerberos-based pNFS is as follows:

Step 1: In the first step, the client sends its user ID, sequence number (SN) and its secret shares of image to the AS.
Step 2: At KDC, the AS contains the secret share of image. The secret share sent by the client is stacked onto the secret share by the AS. This generates a computed image. The computed image is compared with the original image present in the database of KDC. If it is equal, the AS generates a Ticket Granting Ticket (TGT). The TGT along with session key, username, password and timestamp forms packet 1. The packet 1 is encrypted using One Time Password (OTP), which is symmetric encryption. This One Time Password is encrypted using the public key of the client. This forms the packet 2. Then, both these packets are sent to the client.
Step 3: After receiving the packets, client decrypts the packet 2 by using its private key. Thus, the One Time Password (OTP) is extracted. Using OTP, the session key and TGT is recovered. The client keeps the session key with itself and sends TGT to the TGS.
Step 4: TGS, present in KDC, verifies the TGT with the help of database. Then, it sends Service Granting Ticket (SGT)to the client, which contains the secret session key used for communication with the cloud service provider.
Step 5: Then, the client sends secret session key (which has been shared between the client and metadata server) to the cloud server.
Step 6: Finally, the cloud server responds the client by sending the acknowledgement for the requested service.

THE IIOAB JOURNAL
ISSN: 0976-3104

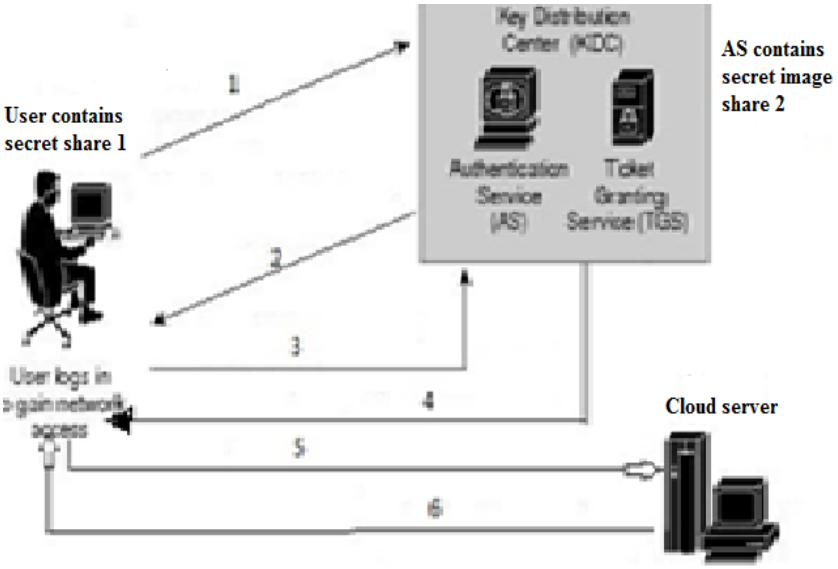


Fig. 3. Kerberos-based pNFS using visual cryptography

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

Algorithm:

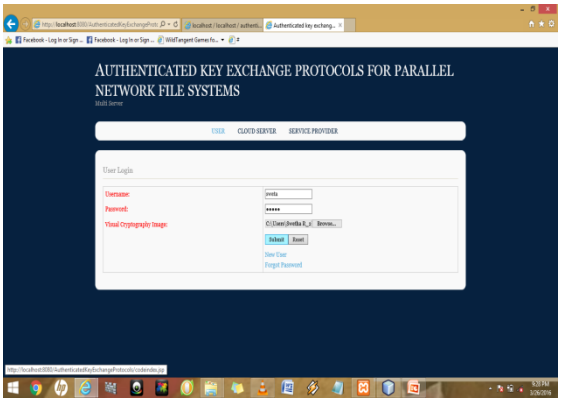
- In first step client send user details to the server for session establishment and access.
- In second step request will reach to KDC
- Thirdly, TGS in KDC will generate the ticket to ticket will be generate ticket to clients.
- Fourth step client will decrypt and send session key to server for session establishment and access to it.
- Final step cloud server will respond to requested client for access.

RESULTS

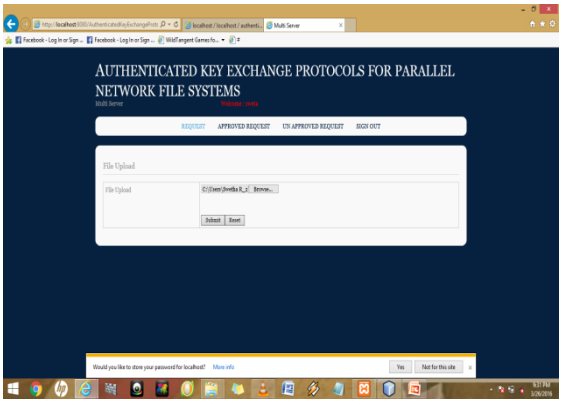
Key generation and encryption

a) Secret key Authentication: The secret key submitted by the sender to the trusted center (TC), then the TC will verify the secret key and authenticate to the respective sender and gets the session key from TC, else TC doesn't allow the user transmission.

b) Encryption The message is encrypted using received session key and appends the qubit with that encrypted message, then transmits the whole information to the corresponding receiver.

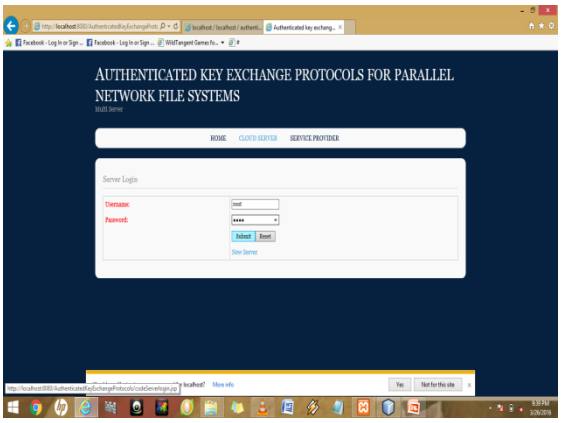


a) Authentication service:

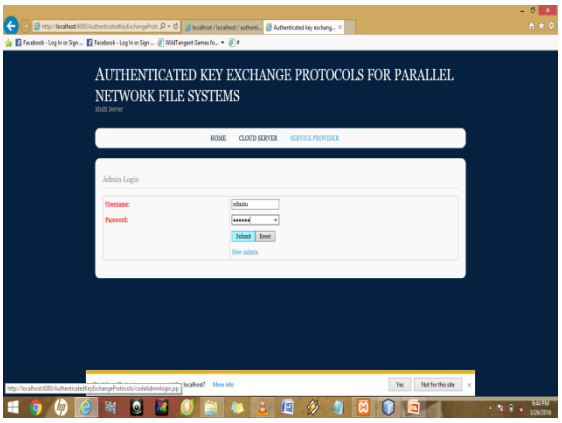


b) Session access:

THE IIOAB JOURNAL
ISSN: 0976-3104



c) Cloud server access:



d) Cloud server maintenance:

Fig: 4. Key generation and encryption

Verification and decryption

a) Secret key Authentication: It receives the encrypted message with hashed session key and qubit, then verifies the qubit with TC and generates the master key and reverses the hash, the session key and also reverse hash the session key from sender then compare the session key which improve the key authentication.
b) Decryption then finally decrypt the message using session key and show it to the user.

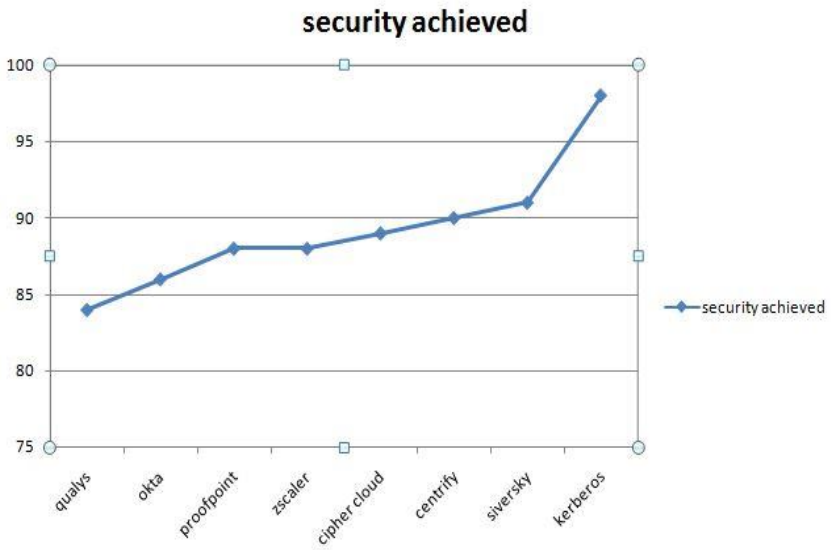


Fig: 5. Comparison – Security Levels

CONCLUSION

In this paper, we are incorporating the technique of Visual cryptography and digital envelope into Kerberos-based pNFS protocol. Visual cryptography adds an extra layer of security in Kerberos, which acts as a pre-authentication. Less computation intricacy, high security, decryption process requires no technical knowledge are some of the projecting features of Visual cryptography. For the secure exchange of the session key between the client web service and KDC, we use the idea of Digital Envelope. By using this technique, the high speed advantage of private key algorithm is combined with the key management advantage of public key algorithm.

THE IIOAB JOURNAL
ISSN: 0976-3104

This solves the problem of key distribution and password guessing attack. Here, we use parallel Network File System concept, where multiple clients can access the cloud server simultaneously. We ruminate this work as an innovative step towards the further improvement of Kerberos authentication protocol.

.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

None.

REFERENCES

[1] Hoon Wei Lim and GuominYang,[2015]. Authenticated Key Exchange Protocols for Parallel Network File Systems. *IEEE Transactions on Parallel and Distributed Systems* 27(1): 92-105.

[2] Mehdi Hojabri and K. venkat rao, [2013]. Innovation in cloud computing: Implementation of Kerberos version5in cloud computing in order to enhance the security issues. *International Conference on Information Communication and Embedded Systems*:452-456.

[3] Abhishek Thorat, MaheshMore, Ganesh, Thombare, Vikram Takalkar, Manisha N.Galphade, [2015]. An Anti-phishing Framework using Visual Cryptography. *International Journal of Advanced Research in Computer and Communication Engineering* 4(2): 332-334.

[4] S. Khandelwal, Pariza Kambo, [2015]. Two Factor Authentication Using Visual cryptography and Digital Envelope in Kerberos. *International Conference on Electrical, Electronics, Signals, Communication and Optimization*: 1-6.

[5] Hoon wei lim . Key management for large scale storage distributed Storage Systems. *SPA Sophia anti polis research, France.*

[6] Dr.G.Ananda Rao et al., [2011]. Three Party Authentication Key Distributed Protocols Using Implicit and Explicit Quantum Cryptography. *Indian Journal of Computer Science and Engineering* 2(2): 143-145.