Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.576 – 581

SAFEGUARD ACCESS TO METASERVER IMPLEMENTED IN PARALLEL NETWORK WITH KEY VERIFICATION

S.PRIYANKA[1], G.SANGEETHA[2], R.SANGEETHA[3], S.SUBASH PRABHU[4]

[1] sspriyankasundarraj@gmail.com, [2] sangeethagopal76@gmail.com

[1, 2, 3] UG Scholar, [4] Asst. Professor/CSE

[1,2,3,4] P.S.R.RENGASAMY COLLEGE OF ENGINEERING FOR WOMEN

ABSTRACT: To propose a range of valid key interchange protocols that are designed to provide forward secrecy in parallel network. To establish proper secure many-many communication between the clients and storage devices. The session keys are generated for accessing the data. This security mechanism is applied for each time access a data in the server. The propose application is capable of decrease the amount of work in the metadata server and concurrently supporting forward secrecy. It is also support escrow freeness. Parallel network file system which makes use of fault tolerant striping protocol launch parallel session key between client and storage device.

Keywords- Session Key, Parallel Network FileSyetem, Forward Secrecy.

I. INTRODUCTION

A Network Security is a specialized field in Computer Networking that involves securing a computer network infrastructure. It also involves authorization of access to data in a Network.Involing large number of client and server services that allow on organization that focus great performance and consistently. Greatest I/O bandwidth is accomplish through parallel access to multiple storage devices with in huge compute cluster. The data defeat is secure through data mirroring using Fault tolerant striping protocol. To prove high performance in General Parallel File

System .Our primary goal is to provide security to Meta server data in parallel network file system. The key verification technique is applied accessing files in many-many communication process. The session keys are used to download the data. A Session key is an encryption and decryption key that is randomly generated to ensure the security of communications session between a user and another computer or between two computers. Session keys are also known as the same key is used for both encryption and decryption. The focus how to session key exchange between clients and metaserver in the parallel network file system .the fault tolerant striping protocol used as the following properties:

A) Scalability-It is provide well scalability, to escape the bottleneck problem and also support a more number of clients in parallel.
B) Forward Secrecy-the secure communication protocol are used to maintain a forward secrecy. They not used in long term secret key between clients and metaserver.
The next one is an,
C) Escrow Freeness- the server generate key between one clients to another client. But server should not study about key.

The outcome of this paper is achieved by the above three properties.

II. SYSTEM DESCRIPTON

The Network structure is define as the single file system usual sustained in Internet Engineering Task Force. In network file system is an important aspect is a performance. The Proposed system will produce high performance, because used in different types keys.NFS most new version is the, in more story by the parallel network file system. To use in different clients and one server is called as metaserver. A Metaserver is considered an intermediate providing for dispersed web resources. It is used to collect data from various web services, web pages, databases, other online resources, repositories and then present the combined results to the client using a standard web protocol. The metadata server is also generates key. The NFS will not performed in read and write operation in puffs, but puffs through action between clients and storage devices. PNFS contain protocol as,

i) The protocols to transfer the data between client and metadata server.

ii) Access the data by the client according to storage devices.

iii) The protocol coordinate state between the server and storage devices.

These are advantages of PNFS.

III. SECURITY DELIBERATION

The Network structure is dedicated on simplicity and efficiency and were designed on intranet and internet[1]. The later versions of network structure is only improve the access and performance, in which time the security is a greater apprehension. In later version will occur more

number of security issues. But in this version to control the security issues by using high performance and parallel applications. The key exchange is a monotonous one, but important aspect of security of the system. The network structure will be included in network file system. The network file system is support the end-to-end communication, where a client through mutually authenticates to a Network File System server. Moreover, deliberation should be given to the reliability and secrecy of Network File System applications and answers. PNFSis similarly to the Network File System. The PNFS is communication between client and metadata server are authentic and secure .Otherwise, the environment on the communication between client and storage devices.

IV. RELATED WORK

The large number key scheme has been proposed. In existing system, used in large number clients and one server.in proposed system used also large number clients and one type of metaserver.in previous system define a large scale distributed system[2]. Large scale distributed means more number of including them. The existing system both metaserver and storage devices are trusted entities, no implicit trust on the clients. The storage devices are access in [3].They used only company and college area. The key verification technique is applied accessing files in many-many communication process. The whole process is a client should enter the details into the server, server should accept the client, server accept the all clients because only occur in authorized clients.

The client should share the information to the other clients. At the time server should generate the one time password key [4]. Next step, the client upload the file to metaserver. Then other clients download the files, the server should generate key and send into a client's mail, the clients can pass the key in server, then server lead file into the clients.so, in this process no occur in unauthorized, then also generate authentication. The related work is more dependent in existing system. It is called as proposed system [5].

V. IMPLEMENTATION

The vital of this proposed work is to provide security to Meta server data in parallel network file system. The key verification technique is applied accessing files in many-many communication process [6]. This paper is authenticated as key generation scheme are high security by using authentication process. The proposed system used as the Fault Tolerant striping protocol. It is define as If look at the words fault and tolerance, can define the fault as a malfunction from normal behaviour and tolerance as the capacity for enduring or putting up with something [7]. The fault tolerance refers to a system's ability to deal with malfunctions. The mainly used in Internet environment. This risk widely extent in the internet [8]. This risk occur in security attack, to solve in this problem in security mechanism. The server generate key, the key range in 32bit[9].The Security mechanism is used to detect, prevent or recover from a security attacks. The mechanisms are divided into those that implemented in a exact protocol sheet and those that are not exact to any particular protocol sheet or security service [10].

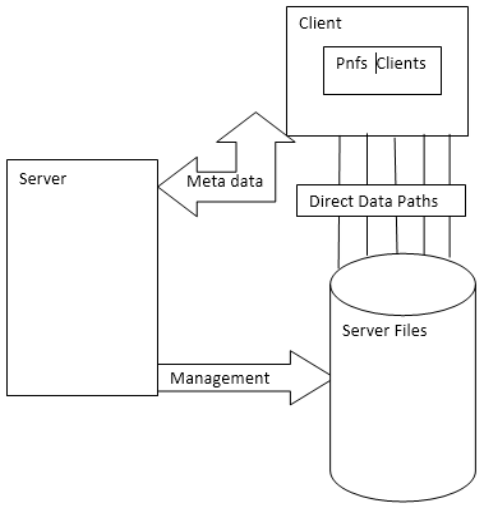

Fig1.Architecture Diagram

The metadata is intermediated between client and server. The clients maintain a parallel network file.MetaServer manages the server files. Clients access the server files through direct data paths.

A. CLIENT AUTHENTICATION

In this module each new client must be created their own profile to access the Meta server**.** In registration process authentication information is provided to each user. Using this authentication only they log on to the application and access it. The information provided to each user must be unique and confidentially maintained.

B. SERVER VERIFICATION

In this module, a server verified client information and accepted. Then only the clients access the application. In every time when the client access the application a new one time password key is generated and send to their mail id. Using this key only the client access the server and go further process. This authentication process is verified each time. Server monitor all clients file details and data sharing information also.

C. DATA SHARING

In this module an authorized client upload their data to the Meta server. This information access by many other clients in secure manner. A client uploads file information such as file type, file name to the server. Clients send a message notification to other clients about their data sharing details.

D. KEY GENERATION

In this module clients access the Meta server data in secure manner. First client search data from the server based on the category. All file information is shown such as file name, file type and client details who upload data to the server. The client access files using a key only. When the client request a key for accessing the file, a unique is generated and sends it to their mail id.

E. DATA ACCESS

In this module a client access the files from the server using a key. Clients get a key from their mail id each time accessing the file. The key is verified then only the client able to download the file securely. This key generation and verification mechanism is applied for all files in each time access. The server is accessed data in client, by using the server files. The several clients can access the data in parallel network. The existing system will used as the key sharing midpoint, but proposed system. The key sharing midpoint is an important one.

VI. KEY SHARING MIDPOINT

The existing system will used as the key sharing midpoint, but proposed system not used in the key sharing midpoint, because one time password can be generated in very time.so,no used in key sharing midpoint. They only symmetric key are used. The key sharing midpoint is used in network infrastructure. The message can be sent in ticket format. In this method, the security can be week.

A) OUTLINE OF OUR PROTOCOL

Our goals are secure data transfer between client and metadata server by using variety of authenticated keys. To focus the parallel network file system to establish between client and storage device through a metadata server. They include many-to-many communications, it is also extended by the multi-user setting. In our solutions, to improve on efficiency and capability with esteem to the metadata server. Our goal is to decrease the workload of the server, because use keys. On other hand, the upstairs of the client and storage device will be very low. Another goal is to produce the high forward secrecy and escrow-freeness. In existing system, the metadata server is generate the key, but proposed system, metadata server do not study about key, so complicity will not occur.

B) KEY STOWING

Note that the key stowing necessities for Fault Tolerant striping protocol and all our labeled protocols are crudely similar from the client's viewpoint. The key stowing necessities for each storage device is larger in puffs. The storage device can be store the key items for one client in their internal state. Fault Tolerant Striping Protocol can be maintain the client key information.

VII. PERFORMANCE

The proposed system became provide the high security. The two type of keys can be used. One key is used to client transfer the message from other client. Another key is used to one client is Upload the data to another client, the another client is download the data by using key. The key is used in one time. Next time the client enter, they used different kinds of key. So the system is highly protected. It is also maintain a forward secrecy and escrow freeness. To avoid the collusion. These are the advantages of proposed system. The key verification technique is applied

to accessing the files in a many-many communication process. To provide a data secrecy assignment.

VIII. CONCLUSION

To suggested variety of authenticated key exchange protocols for network structure. The protocol named as fault tolerant striping protocol. It should be occur in three advantages, i) it also provide the better scalability.ii.)The protocols are produce forward secrecy.iii) Escrow-free – the metadata server should not learn any information about any session key used by the client and the storage device, provided there is no complicity among them. The week password is used to develop a key that encrypts and transmitted between client and key sharing midpoint. The key sharing midpoint to transmit the message in metadata server.

REFERENCES

[1] Hoon Wei Lim Guomin Yang, Authenticated Key Exchange Protocol for Parallel Network File System, Vol 27, no 1, 2015.

[2] M. Armbrust, A. Fox, R. Griffith, Single Password of Many to Many communication, pages 50-55, April 1998.

[3] J.H. Howard, M.L. Kazar, Capacity and Performance in distributed file. Page 52-81, Feb 2004.

[4]M. Bellare, D. Point cheva, Key Exchange secure between metaserver and client, pages 140-156.Nov 2008.

[5] J. Linn, Secure Data Beach Security, The Internet Task Force Engineering in version 2,RFC 2473,Jan 2012.

[6] J. Dean and S. Ghemawat. Map Reduce: Simplified data processing on large clusters. Pages 137–150. USENIX Association, Dec 2004.

[7] M. Eisler. XDR: External data representation standard, STD 67, RFC 4506, May 2006.

[8] J. Linn. The Kerberos version 5 GSS-API mechanism. *(IETF)*, RFC 1964, Jun 1996.

[9] J. Linn. Generic security service application program interface version 2, update 1.RFC 2743, Jan 2000.

[10] D. Mazieres, M. Kaminsky, M.F. Kaashoek, and E. Witchel. Separating key management from file system security. In pages 124– 139. ACM Press, Dec 1999.

