JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 8, 2020

A STUDY OF USING AUTHENTICATED KEY EXCHANGE PROTOCOLS TO BOOST THE EFFICIENCY OF PARALLEL NETWORK FILE SYSTEM

M. Narendra[1], Dr.S. Suresh Raja[2]

1Research Scholar, Dept. of Computer Science & Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal-Indore Road, Madhya Pradesh, India.
2Research Guide, Dept. of Computer Science & Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Bhopal Indore Road, Madhya Pradesh, India.

Received: 11.03.2020 Revised: 12.04.2020 Accepted: 28.05.2020

ABSTRACT: Our work bases on current Internet standards for such document systems, for instance the equal Network File System (pNFS), which uses Kerberos to set up equal session keys among customer and limit gadgets. In this day and age, distributed computing is the creating technology. There exist some security dangers and troubles in getting to resemble network records right now virtual technology. To defeat this, simultaneous access and client verification is utilized for the resistance reason. This paper depends on Kerberos convention utilizing visual cryptographic in cloud. Kerberos is one of the most mainstream validation convention utilized in networks.

KEYWORDS: Authenticated, Exchange, Network, pNFS, Kerberos.

 DOI: http://dx.doi.org/10.31838/jcr.07.08.360

I. INTRODUCTION

At the point when the network association is accessible, the distributed computing model permits access to information and PC assets from anyplace. Distributed computing offers a common pool of assets including information extra room, networks ,PC preparing power , and specific corporate and client applications. The highlights of distributed computing remember for request self-administration, network get to broadcasting, pooling of asset, versatility and estimated administration. Cloud administrations are regularly made accessible by means of a private cloud, network cloud, open cloud or crossover cloud. Cloud administrations are well known on the grounds that they can decrease the expense and multifaceted nature of working PCs and networks. While there are benefits, there are protection and security concerns as well. Information going over the web and is put away in remote areas. Furthermore, cloud offers types of assistance to different clients all the while. This may offer ascent to a few potential assaults.

Kerberos is a validation convention right now Center (KDC) issues ticket encoded with client's secret key. There are three principle parts of Kerberos convention:

1) **Client:** Customers are the clients which demand the specialist co-op for administration from the particular application servers.
2) **Key Distribution Centre (KDC):** The KDC gives confirmation administrations and key appropriation usefulness. It contains client's and administration's mystery key. It comprises of two parts:

a) **Authentication server (AS):** The AS verifies the clients. On the off chance that another client registers with the AS, it gives the client ID and mystery secret word to the client. The database contains the username and relating passwords. The AS confirms the client, gives a session key and sends a pass to the customer.

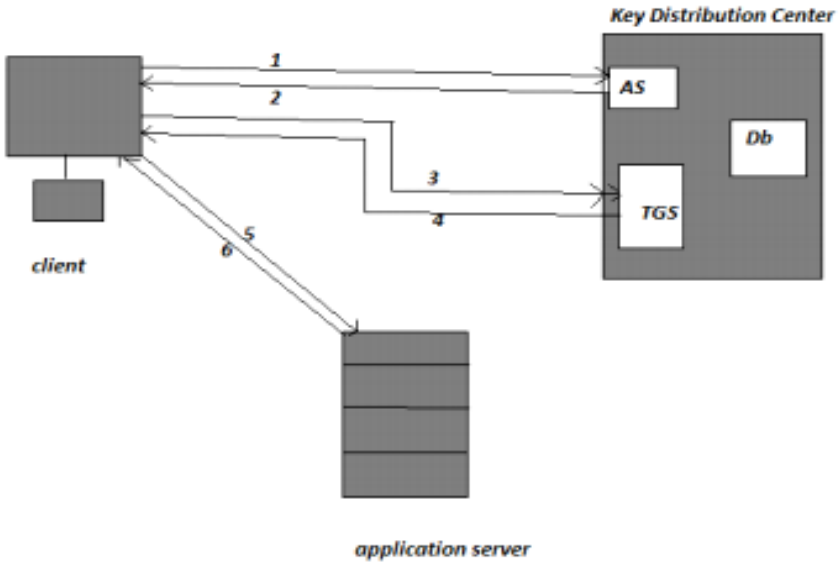
b) **Ticket Granting Service (TGS):** The TGS issues a pass to the client for building up session with the application server. It gives session key among client and application server. Client confirms its ID only once with AS and can contact TGS on various occasions to get tickets for various application servers.

c) **Application server:** The application server provides services for the requested user. Kerberos authentication process takes place as follows:

ISSN- 2394-5125 VOL 7, ISSUE 8, 2020

Step1: Customer demands administration by sending its client's ID together with the ID of Ticket Granting Service (TGS) to the Authentication Server (AS).

Step2: AS reacts with the ticket that is encoded with a key got from client's secret phrase. Customer decodes the approaching message and if the secret phrase is right, the ticket is effectively recuperated.



Step3: Customer demands Service Granting Ticket (SGT) by transmitting a message to the TGS containing the client's ID, administration ID and TGT.

Step4: TGS decodes approaching ticket and checks the ID. It checks to ensure that the lifetime has not lapsed. At that point it contrasts client ID and network address and the approaching data to confirm the client. In the event that fruitful, TGS issues a Service Granting Ticket (SGT) by utilizing which client is permitted to get to the server.

Step5: Subsequent to getting SGT from TGS, customer sends this ticket alongside client ID to the server so as to get to a help. The server confirms the ticket and verifies the client.

Step6: At long last, a server opens the discussion with customer and performs invert verification subsequent to confirming client data effectively.

The current system will depicts that confirmed key trade convention for simultaneous access network document system this is accomplished by three way validation right off the bat decreasing the outstanding task at hand of metadata server and furthermore giving forward mystery finally thirdly giving e scrow freeness. It ways to deal with improve the exhibition and adaptability of the system and equal secure session among customer and specialist co-op. It gives escrow freeness and defeats the forward mystery issue. It ways to deal with upgrade the security and security assault by mix of visual cryptography and computerized envelope in the Kerberos verification convention by this common confirmation accomplished thusly it tackles the key dissemination and clock synchronization issues and improves the effectiveness. This is finished with AES (propelled encryption standard) calculation and ECC calculation and for equal network document system actualizing the key administration in huge scale disseminated system by setting up the lightweight key administration strategy. This system present record system security engineering (FSSA) for key administration issue and for improving the security.

II. LITERATURE REVIEW

S. Sathya, M. Ranjith Kumar, K. Madheswaran(2017)the key establishment for secure many-to-various interchanges is critical nowadays. The issue is pushed by the increase of colossal scale flowed record systems supporting equal access to various stockpiling gadgets. Right now, of affirmed key exchange a convention that is planned to address the issues. This shows these conventions are fit for reducing the extraordinary weight of the metadata server and all the while supporting forward riddle and escrow-freeness. This requires only a little division of extended calculation overhead at the customer. This proposed three confirmed key exchange

conventions for equal network record system (pNFS). The conventions offer three connecting with focal points over the current Kerberos-based convention.

Hoon Wei Lim and Guomin Yang (2015)we study the issue of key establishment for secure many-to-various interchanges. The issue is moved by the augmentation of huge scale spread record systems supporting equal access to different stockpiling gadgets. Our work revolves around the present Internet standard for such record systems, i.e., equal Network File System (pNFS), which uses Kerberos to set up equal session keys among customers and capacity gadgets. Our review of the current Kerberos-based convention shows that it has different requirements: (I) a metadata server empowering key exchange between the customers and the capacity gadgets has significant extraordinary job needing to be done that confines the flexibility of the convention; (ii) the convention doesn't give forward secret; (iii) the metadata server makes itself all the session keys that are used between the customers and capacity gadgets, and this inherently prompts key escrow. Right now, propose a grouping of affirmed key exchange conventions that are planned to address the above issues.

D.K.S. MANIPRABHA, M. KRISHNA SATYA VARMA (2016) the key age secure for some to-various between correspondence is prolifed in perspective on spread of huge passed on document systems and is moved by supporting equal access to a couple of capacity gadgets. This proposes a grouping of affirmed key exchange conventions that are planned to address the issues we are looking with Kerberos based convention. We show that our conventions are fit for reducing up to generally half of the remarkable job needing to be done of the metadata server and all the while supporting forward secret and escrow-freeness. This requires only a little division of extended calculation overhead at the customer. We proposed three affirmed key exchange conventions for equal network record system. Our conventions offer three drawing in focal points over the current Kerberos-based convention.

Anupama T, Refeeda K (2015)the rule issue is persuaded by the development of colossal scale flowed record systems supporting equal access to various stockpiling gadgets. The system work revolves around the present Internet standard for such record systems, i.e., equal Network File System (pNFS), which uses Kerberos to set up equal session keys among customers and capacity gadgets. Our overview of the current Kerberos-based convention shows that it has different imprisonments: (I) a metadata server empowering key exchange between the customers and the capacity gadgets has considerable extraordinary job needing to be done that constrains the adaptability of the convention; (ii) the convention doesn't give forward riddle; (iii) the metadata server makes itself all the session keys that are used between the customers and capacity gadgets, and this normally prompts key escrow.

V. Prathyusha, AaruniGiriraj, Dr. Ramakrishna (2016)right now read the key establishment for secure many-to-various correspondences. The essential issue is inspired by the quick augmentation of gigantic scale flowed document systems supporting equal access to various stockpiling gadgets. Our examination of the current Kerberos convention shows that it has different obstructions: (I) a metadata server giving key exchange among the customers and the capacity gadgets has considerable residual job needing to be done that confines the versatility of the convention; (ii) the convention can't give forward riddle; (iii) the metadata server makes all the session keys for confirming correspondence among customers and capacity gadgets, and this inadvertently prompts key escrow.

III. PROPOSED SYSTEM

The primary point is to decrease the remaining task at hand of metadata server and to give solid validation Here, different customers web administration can get to the application server at the same time. By and large, metadata server is utilized to produce all the administration tickets and session keys between customer web administration and cloud server by setting substantial remaining task at hand on it. In our answers, customer web administration first pre-figures some key materials and advances them to metadata server and issues the comparing verification tokens. For each solicitation to get to at least one application servers at a particular time, customer web administration registers a session key from the pre-processed material. In this manner, the outstanding task at hand of creating session key by metadata server is decreased.

The altered adaptation of Kerberos permits the customers to create its own session keys. The key material is utilized to produce session keys. To address key escrow while accomplishing forward mystery, visual cryptographic system is fused into Kerberos-based pNFS. The improved Kerberos-based pNFS is as per the following:

Step 1: In the initial step, the customer sends its client ID, succession number (SN) and its mystery portions of picture to the AS.

ISSN- 2394-5125 VOL 7, ISSUE 8, 2020

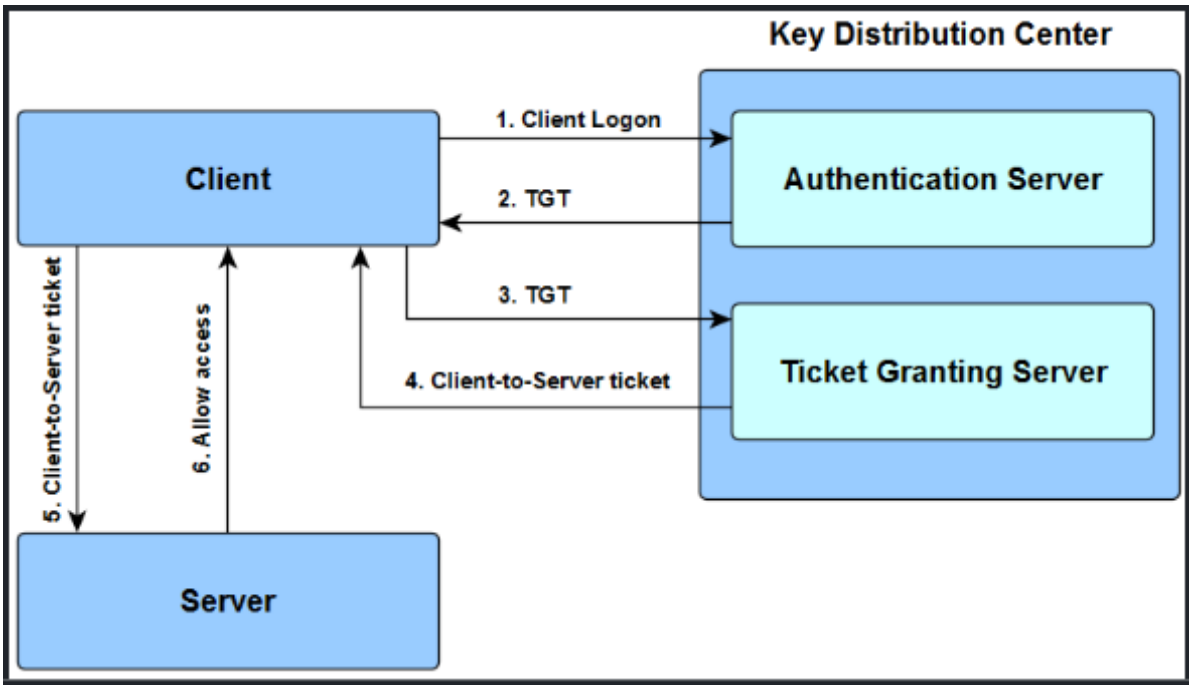
Step 2: At KDC, the AS contains the mystery portion of picture. The mystery share sent by the customer is stacked onto the mystery share by the AS. This creates a processed picture. The processed picture is contrasted and the first picture present in the database of KDC. In the event that it is equivalent, the AS produces a Ticket Granting Ticket (TGT). The TGT alongside session key, username, secret key and timestamp structures parcel 1. The parcel 1 is scrambled utilizing One Time Password (OTP), which is symmetric encryption. This One Time Password is encoded utilizing the open key of the customer. This structures the bundle 2. At that point, both these bundles are sent to the customer.

Step 3: Subsequent to getting the bundles, customer decodes the parcel 2 by utilizing its private key. Along these lines, the One Time Password (OTP) is extricated. Utilizing OTP, the session key and TGT is recouped. The customer keeps the session key with itself and sends TGT to the TGS.

Step 4: TGS, present in KDC, confirms the TGT with the assistance of database. At that point, it sends Service Granting Ticket (SGT)to the customer, which contains the mystery session key utilized for correspondence with the cloud specialist co-op.

Step 5: At that point, the customer sends mystery session key (which has been shared between the customer and metadata server) to the cloud server.

Step 6: At long last, the cloud server reacts the customer by sending the affirmation for the mentioned administration.



The accompanying chart speaks to the security be accomplished by Kerberos in cloud administrations.

Algorithm

- In initial step customer send client subtleties to the server for session foundation and access.
- In second step solicitation will reach to KDC.
- Thirdly, TGS in KDC will produce the pass to ticket will be create pass to customers.
- Fourth step customer will decode and send session key to server for session foundation and access to it.
- Last advance cloud server will react to mentioned customer for get to.

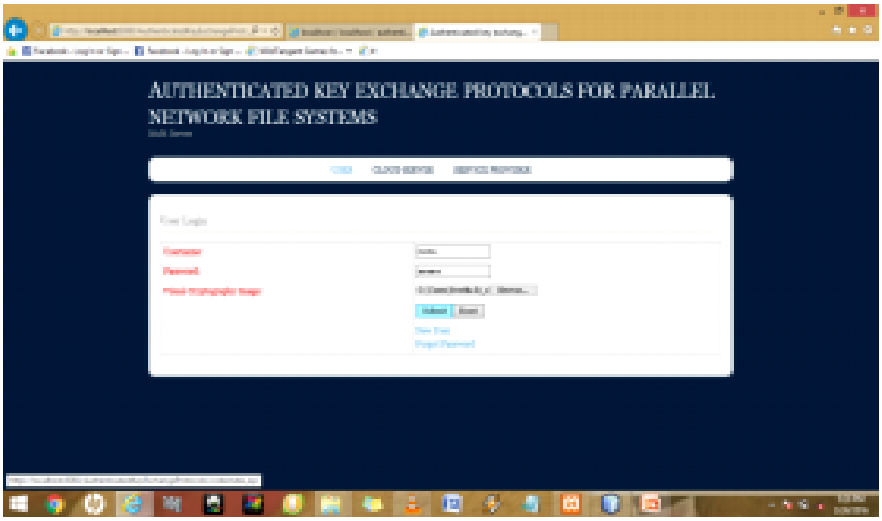
IV. ANALYSIS & RESULT

Key Generation and Encryption

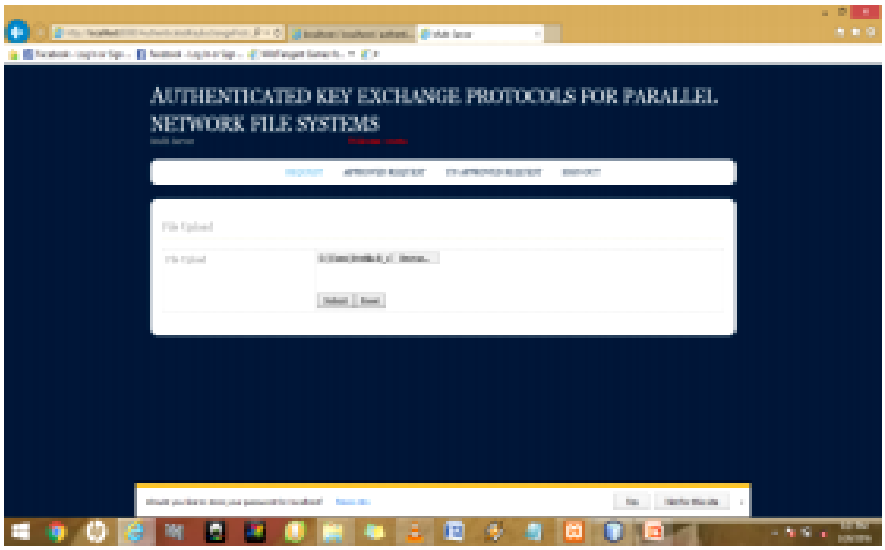
ISSN- 2394-5125 VOL 7, ISSUE 8, 2020

a) Secret key Authentication: The mystery key put together by the sender to the confided in focus (TC), at that point the TC will confirm the mystery key and validate to the individual sender and gets the session key from TC, else TC doesn't permit the client transmission.

b) Encryption The message is scrambled utilizing got session key and annexes the qubit with that encoded message, at that point transmits the entire data to the comparing recipient.

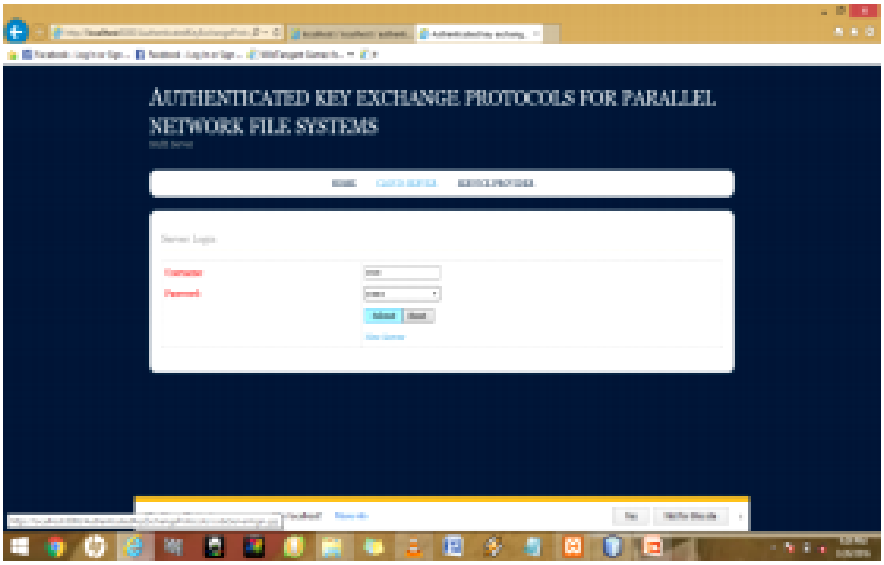


Authentication Service

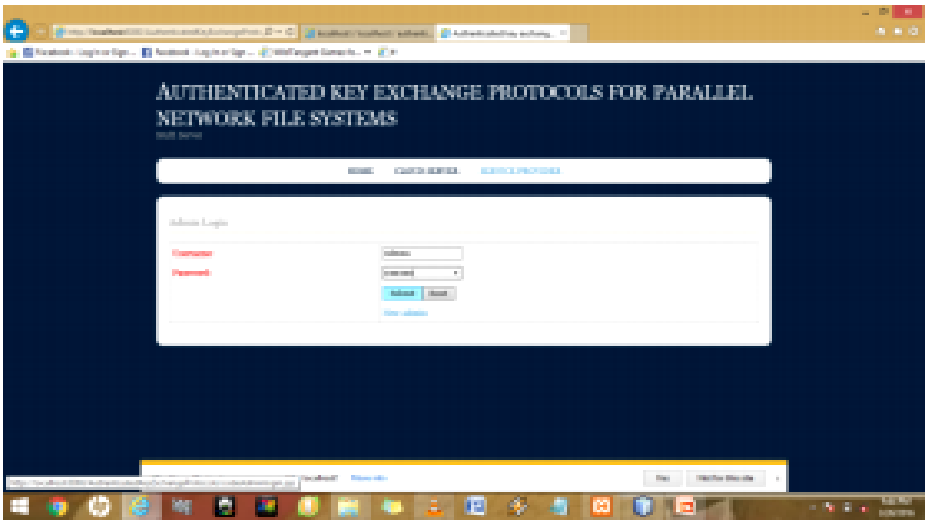


Session Access

ISSN- 2394-5125 VOL 7, ISSUE 8, 2020



Cloud Server Access



Cloud Server Maintenance

Figure 4: Key Generation and Encryption

Verification and Decryption

a) Mystery key Authentication: It gets the encoded message with hashed session key and qubit, at that point confirms the qubit with TC and produces the ace key and inverts the hash, the session key and furthermore switch hash the session key from sender at that point think about the session key which improve the key verification.

b) Decoding at that point at last unscramble the message utilizing session key and demonstrate it to the client.

ISSN- 2394-5125 VOL 7, ISSUE 8, 2020

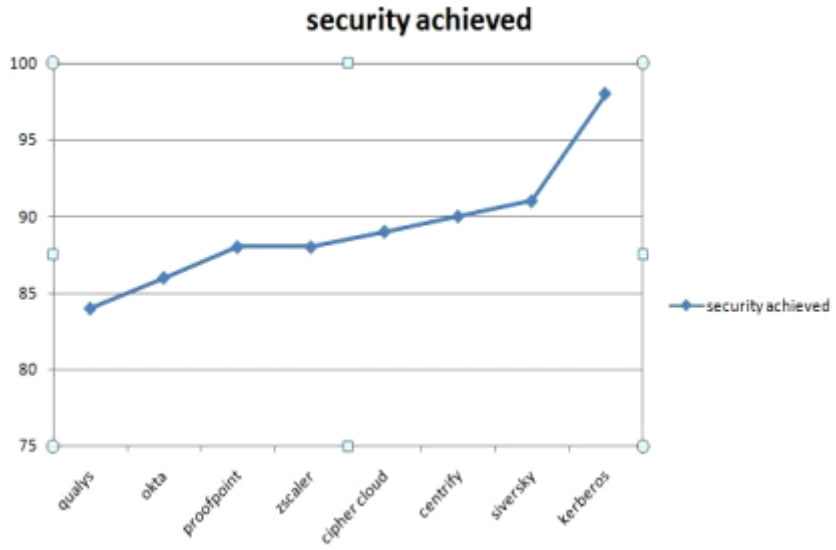


Figure 3: Comparisons – Security Levels

V. CONCLUSION

Right now, are joining the system of Visual cryptography and computerized envelope into Kerberos-based pNFS convention? Visual cryptography includes an additional layer of security in Kerberos, which goes about as a pre-verification. Less calculation multifaceted nature, high security, decoding process requires no specialized information are a portion of the anticipating highlights of Visual cryptography. For the safe trade of the session key between the customer web administration and KDC, we utilize the possibility of Digital Envelope. By utilizing this procedure, the fast bit of leeway of private key calculation is joined with the key administration favorable position of open key calculation. This takes care of the issue of key appropriation and secret phrase speculating assault. Here, we utilize equal Network File System idea, where various customers can get to the cloud server at the same time. We ruminate this work as an inventive advance towards the further improvement of Kerberos validation convention.

VI. REFERENCES

[1] S. Sathya, M. Ranjith Kumar, K. Madheswaran, Parallel network file systems using authenticated key exchange protocols, *Journal of Applied and Advanced Research* 2017.

[2] Hoon Wei Lim Guomin Yang, ―Authenticated Key Exchange Protocols for Parallel Network File Systems‖, IEEE Transactions on Parallel and Distributed Systems in 2015. D.K.S. Maniprabha, M. Krishna Satya Varma, *Enhanced Authenticated Key Exchange in Parallel Network File Systems for Security*, ISSN 2319-8885 Vol.05,Issue.30 September-2016, Pages:6388-6391

[3] Anupama T, Refeeda K, Cloud And Parallel Network File System Using Authenticated Key Exchange Protocols, International Journal of Science and Research (IJSR),2015

[4] V. Prathyusha, AaruniGiriraj, Dr. Ramakrishna, Exchange Protocols on Network File Systems Using Parallel Sessions Authenticated & Improved Keys, Volume: 2 | Issue: 09 | September 2016 | ISSN: 2455-3778.

[5] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A view of cloud computing. Communications of the ACM, 53(4):50–58. ACM Press, Apr 2010.

[6] H.W. Lim. Key management for large-scale distributed storage systems. *In Proceedings of the 6th European Public Key Infrastructure Workshop (EuroPKI)*, pages 99–113. Springer LNCS 6391, Sep 2010.

[7] S. Langella, S. Hastings, S. Oster, T. Pan, A. Sharma, J. Permar, D. Ervin, B.B. Cambazoglu, T.M. Kurc¸, and J.H. Saltz. Model formulation: Sharing data and analytical resources securely in a biomedical research grid environment. *Journal of the American Medical Informatics Association (JAMIA)*, 15(3): 363–373. BMJ, May 2008.

[8] P. Mell and T. Grance. The NIST definition of cloud computing. National Institute of Standards and Technology (NIST), Special Publication 800-145, August 2011,

[9] O. O'Malley, K. Zhang, S. Radia, R. Marti, and C. Harrell. Hadoop security design. Yahoo!, Oct 2009. https://issues.apache.org/jira/secure/ attachment/12428537/security-design.pdf.

[10] S. Parker. De-risking drug discovery with the use of cloud computing. *ISGTW*, Jun 18, 2012. http://www.isgtw.org.

[11] Rosenthal, P. Mork, M.H. Li, J. Stanford, D. Koester, and P. Reynolds. Cloud computing: A new business paradigm for biomedical information sharing. *Journal of Biomedical Informatics (JBI)*, 43(2): 342–353. Elsevier, Apr 2010.

[12] S. Shepler, M. Eisler, and D. Noveck. Networks file system (NFS) version 4 minor version 1 protocol. *The Internet Engineering Task Force (IETF), RFC* 5661, Jan 2010.

[13] O. Tatebe, K. Hiraga, and N. Soda. Gfarmgrid file system. *New Generation Computing (NGC)*, 28(3): 257–275. Springer, Jul 2010.

[14] R. Thurlow. RPC: Remote procedure call protocol specification version 2. *The Internet Engineering Task Force (IETF)*, RFC 5531, May 2009.

[15] B. Welch, M. Unangst, Z. Abbasi, G.A. Gibson, B. Mueller, J. Small, J. Zelenka, and B. Zhou. Scalable performance of the Panasas parallel file system. *In Proceedings of the 6th USENIX Conference on File and Storage Technologies (FAST)*, pages 17–33. USENIX Association, Feb 2008.

[16] Kesavan, S., Saravana Kumar, E., Kumar, A., Vengatesan, K: An investigation on adaptive HTTP media streaming Quality-of-Experience (QoE) and agility using cloud media services; *International Journal of Computers and Applications.*