ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 2, February 2016

An Improved Authenticated Key Exchange Protocols to Enhance the Security for Parallel Network File System

[1]Bercelin Raj P, [2]Mr.G.Ashwin, [3]Dr.A.Lenin Fred.

[1]PG Scholar, [2]Assistant Professor, [3]Professor, Computer Science & Engineering,
Mar Ephraem College of Engineering & Technology,
Elavuvilai, Marthandam, India

***Abstract*— This proposes a variety of authenticated key exchange protocols that are designed to address the issues. We show that our protocols are capable of reducing up to approximately 54% of the workload of the metadata server and concurrently supporting forward secrecy and escrow-freeness. All this requires only a small fraction of increased computation overhead at the client. We proposed three authenticated key exchange protocols for parallel network file system (pNFS). Our protocols offer three appealing advantages over the existing Kerberos-based pNFS protocol. First, the metadata server executing our protocols has much lower workload than that of the Kerberos-based approach. Second, two our protocols provide forward secrecy: one is partially forward securing (with respect to multiple sessions within a time period), while the other is fully forward secure (with respect to a session). Third, we have designed a protocol which not only provides forward secrecy, but is also escrow-free.**

***Index Terms*—Authenticated key, Exchange Protocols, pNFS, Kerberos-based approach.**

I. INTRODUCTION

In this work investigate the problem of secure many to many communications in large-scale network file systems that support parallel access to multiple storage devices. That is, we consider a communication model where there are a large number of clients (potentially hundreds or thousands) accessing multiple remote and distributed storage devices (which also may scale up to hundreds or thousands) in parallel. Particularly, we focus on how to exchange key materials and establish parallel secure sessions between the clients and the storage devices in the parallel Network File System (pNFS) the current Internet standard in an efficient and scalable manner. The development of pNFS is driven by Panasas, Netapp, Sun, EMC, IBM, and UMich/CITI, and thus it shares many common features and is compatible with many existing commercial/proprietary network file systems.

A. Networking Basic

Networking is the practice of linking multiple computing devices together in order to share resources. These resources can be printers, CDs, files, or even electronic communications such as e-mails and instant messages. These networks can be created using several different methods, such as cables, telephone lines, satellites, radio waves, and infrared beams. Without the ability to network, businesses, government agencies, and schools would be unable to operate as efficiently as they do today. The ability for an office or school to connect dozens of computers to a single printer is a seemingly simple, yet extremely useful capability. Perhaps even more valuable is the ability to access the same data files from various computers throughout a building. This is incredibly useful for companies that may have files that require access by multiple employees daily. By utilizing networking, those same files could be made available to several employees on separate computers simultaneously, improving efficiency.

B. The Ins And Outs of Networking

When it comes to networking, there are two essential pieces of equipment that enable numerous devices to be connected: routers and switches

C. Switches

Switches are used in order to connect many devices on the same network. These devices are generally within the same building, such as an office building or school and could consist of various computers, printers, and other gadgets. The switch acts as a controller, allowing the connected objects to share information with one another. This not only increases productivity and efficiency, but also saves money.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 2, February 2016

D. Routers

In addition to switches, networks generally employ routers as well. These essential tools connect different networks to each other through the internet in order to allow for data exchange between networks. Whereas the switch can be considered a controller, a router should be considered more of a dispatcher, packaging digital information and choosing the best route for it to travel. Routers can feature several other functions, including firewalls and virtual private networks (VPNs) that enhance the security of the data being sent over the internet.

E. Network Types

There are countless types of networks available, especially as networking technologies continue to advance. Two of the most commonly employed networks are LAN and WAN.

F. Local Area Network (LAN):

These networks are used to connect devices over relatively short distances, such as within a building, school, or home. LANs generally employ Ethernet cables as a means of connecting the various gadgets within the network.

• Wide Area Network (WAN): These networks are used to connect devices over much larger distances than LANs. A WAN is established by using routers to connect various LANs and are generally not owned by a single person or organization. The internet is one massive WAN that spans the entire planet.

• Other Network Types: Various other types of networks exist, including wireless local area networks (WLANs) that are LANs based on wireless network technology and metropolitan area networks (MANs) that cover larger areas than LANs but smaller areas than WANs. These MANs generally span a city and are owned and operated by a government or corporation.

G. Network Topology

Not to be confused with network type, network topology refers to the virtual layout of the devices within a network and can refer to five distinct categories:

• Bus: This topology utilizes a common backbone, generally a single cable, to connect all the devices on a network.

• Ring: Found in some offices and schools, ring topologies give each device two neighbors for communication purposes. All data travels in a ring, and a failure of that ring can bring down the whole network.

• Star: Found in many homes, a central connection known as a "hub" is connected to all the objects on the network. This hub could be a router or a switch.

• Tree: A hybrid bus/star network, several star hubs are connected to the core cable of a bus in order to vastly increase the number of computers able to connect to the network.

• Mesh: The mesh topology employs the concept of routing, in which each piece of data sent on the network has multiple paths it can take instead of one fixed route. The internet is a perfect example of this topology.

H. Computer Network Definition

A computer network is a collection of computers and other devices that are able to communicate with each other and share data. These devices include computers, printers, tablets, phones, and many other electronics.

I. Computer Networking Essentials

Both traditional and modern forms of computer networking aim to provide users with the ability to share data amongst multiple gadgets, whether they be in the same building or across the globe. Traditional computer networking relied on Ethernet and fiber optic cables to connect various devices on a network. More modern technology has emerged that allows for wireless connections between electronics. These technologies include Wi-Fi and Bluetooth compatible devices. It is very helpful to understand the role that each of these technologies plays in computer networking.

• **Wide Area Interconnects:** Networks that must support large volumes of devices simultaneously, such as satellites or cellular networks are considered wide area interconnects. They are generally expensive to build and run more slowly than others due to the large area and high volume of users.

• **Long Distance Interconnects:** These include cables such as Ethernet and fiber optics. They support a very large amount of data and serve many clients who share common hardware.

• **Short Distance Interconnects:** These technologies are much newer than other the others and include tools such as Bluetooth. These interconnects are highly optimized for low-cost and also low power usage. Bluetooth is used in many mobile devices, laptop computers, and speakers in order to enable the transfer of data. Popular information sent over Bluetooth includes music, phone calls, and contact information. The market for Bluetooth technology is growing at a rapid pace to include many other items such as remote controlled helicopters and cars, home security systems, and fitness gear. Because it is rather affordable for the connectivity it supplies, Bluetooth technology is finding its way into countless niches.

J. Computer Networking

The Server

In information technology, a server is considered any instance of an application that can receive and serve the

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 2, February 2016

requests of other programs. Usually these applications are run on computers dedicated to acting solely as servers so that the heavy burden of fulfilling requests from other devices on the network does not overwhelm the computers. Running servers on dedicated computers is also a safety measure, helping to keep the server from being attacked. The computers dedicated to acting as servers usually include faster CPUs, bigger hard drives, better RAM, and multiple power sources. These enhancements allow the server to handle the immense workload and also give it reliability in the event of unfortunate events.

K. *Peer – To - Peer Networks*

A Peer-to-Peer network, or P2P network, is one in which multiple computers are connected without linking through a separate computer that acts as a server. These connections can vary based on how many computers are being linked together. Two computers can be linked via a USB drive to allow for the transfer of files. Multiple computers in an office can be connected directly to each other via traditional copper wiring instead of through a server computer. The fundamental basis for P2P networks is that individual permissions must be set for each computer on the network. For instance, if one computer (A) is connected to a printer and another computer (B) on the network wishes to use the printer, then A would first have to grant B permission.

L. *Network Security*

Network Security is an organization's strategy and provisions for ensuring the security of its assets and of all network traffic. Network security is manifested in an implementation of security policy, hardware, and software. For the purposes of this discussion, the following approach is adopted in an effort to view network security in its entirety:

- Policy
- Enforcement
- Auditing
- Policy

The IT Security Policy is the principle document for network security. Its goal is to outline the rules for ensuring the security of organizational assets. Employees today utilize several tools and applications to conduct business productively. Policy that is driven from the organization's culture supports these routines and focuses on the safe enablement of these tools to its employees. The enforcement and auditing procedures for any regulatory compliance an organization is required to meet must be mapped out in the policy as well.

M. *Enforcement*

Most definitions of network security are narrowed to the enforcement mechanism. Enforcement concerns analyzing all network traffic flows and should aim to preserve the confidentiality, integrity, and availability of all systems and information on the network. These three principles compose the CIA triad:

Confidentiality - involves the protection of assets from unauthorized entities

Integrity - ensuring the modification of assets is handled in a specified and authorized manner

Availability - a state of the system in which authorized users have continuous access to said assets.

Strong enforcement strives to provide CIA to network traffic flows. This begins with a classification of traffic flows by application, user, and content. As the vehicle for content, all applications must first be identified by the firewall regardless of port, protocol, evasive tactic, or SSL. Proper application identification allows for full visibility of the content it carries. Policy management can be simplified by identifying applications and mapping their use to a user identity while inspecting the content at all times for the preservation of CIA.

The concept of defense in depth is observed as a best practice in network security, prescribing for the network to be secured in layers. These layers apply an assortment of security controls to sift out threats trying to enter the network:

- Access control
- Identification
- Authentication
- Malware detection
- Encryption
- File type filtering
- URL filtering
- Content filtering

These layers are built through the deployment of firewalls, intrusion prevention systems (IPS), and antivirus components. Among the components for enforcement, the firewall (an access control mechanism) is the foundation of network security.

N. *Auditing*

The auditing process of network security requires checking back on enforcement measures to determine how well they have aligned with the security policy. Auditing encourages continuous improvement by requiring organizations to reflect on the implementation of their policy on a consistent basis. This gives organizations the opportunity to adjust their policy and enforcement strategy in areas of evolving need.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 2, February 2016

O. Scope of the Project

A variety of authenticated key exchange protocols that are designed to address the issues. Metadata server executing our protocols has much lower workload than that of the Kerberos-based approach.

P. System Requirements

HARDWARE		SOFTWARE	
Processor	Pentium IV 2.6GHz,Intel Core 2 Duo	Front End	J2EE
RAM	512 MB DD-RAM	Back End	MY SQL 5.5
MONITOR	15'' Color	Operating System	Windows 7
Hard Disk	40GB	IDE	Eclipse

II. SYSTEM DESIGN

A. Proposed System Model

a. Diffie-Hellman Key Agreement

Diffie-Hellman key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming.

Phase I - For each validity period v:

(1) $S_i \rightarrow M: \ ID_{S_i}, \mathcal{E}(K_{MS_i}; g^{s_i})$

(2) $C \rightarrow M: \ ID_C, \mathcal{E}(K_{CM}; g^c)$

(3) $M \rightarrow C: \ \mathcal{E}(K_{CM}; g^{s_1}, \ldots, g^{s_N}),$
$\tau(K_{MS_1}; ID_C, ID_{S_1}, v, g^c, g^{s_1}), \ldots, \tau(K_{MS_N}; ID_C, ID_{S_N}, v, g^c, g^{s_N})$

Phase II - For each access request at time t:

(1) $C \rightarrow M: \ ID_C, ID_{S_1}, \ldots, ID_{S_n}$

(2) $M \rightarrow C: \ \sigma_1, \ldots, \sigma_n$

(3) $C \rightarrow S_i: \ \sigma_i, g^c, \tau(K_{MS_i}; ID_C, ID_{S_i}, v, g^c, g^{s_i}), \mathcal{E}(sk_i^0; ID_C, t)$

(4) $S_i \rightarrow C: \ \mathcal{E}(sk_i^0; t+1)$

Specification of pNFS-AKE-II (with partial forward secrecy and escrow-free).

b. Advantages of Proposed System

We have designed a protocol which not only provides forward secrecy, but is also escrow-free.the metadata server executing our protocols has much lower workload than that of the Kerberos-based approach.

B. System Architecture

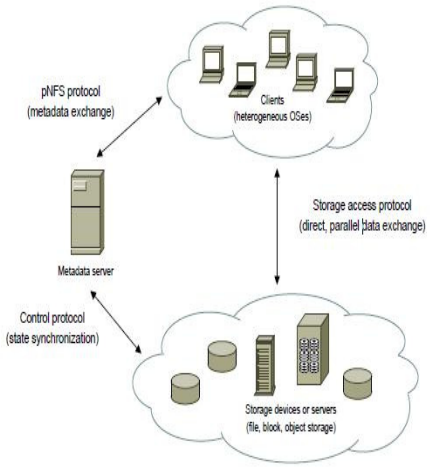


Fig 3.1: System Architecture

C. Module Description

a. User Interface Design

This is the first module of our project. The important role for the Network user is to move login window to cloud user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user name and valid password).

If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user.

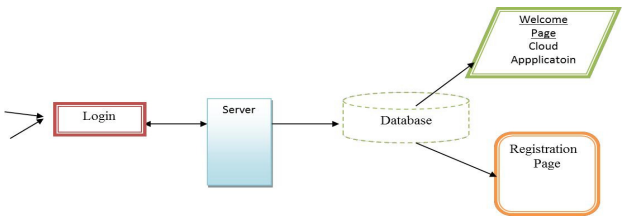


Fig 3.2: User Interface Design

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 2, February 2016

b. Parallel Sessions.

Parallel secure sessions between the clients and the storage devices in the parallel Network File System (pNFS). The current Internet standard—in an efficient and scalable manner. This is similar to the situation that once the adversary compromises the long-term secret key, it can learn all the subsequence sessions. If an honest client and an honest storage device complete matching sessions, they compute the same session key. Second, two our protocols provide forward secrecy: one is partially forward securing with respect to multiple sessions within a time period.

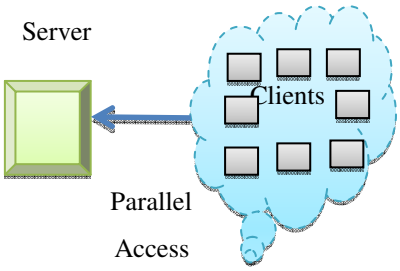
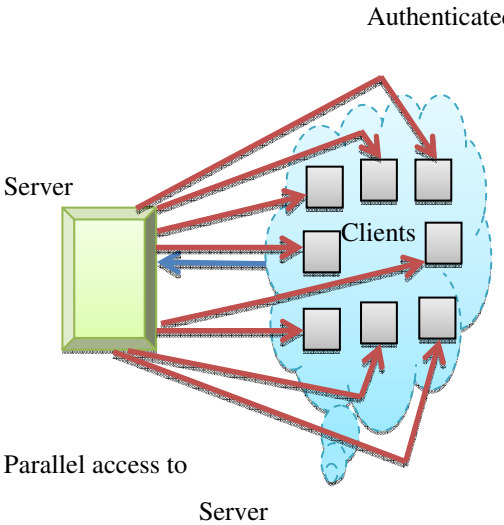


Fig 3.3: Parallel Sessions

c. Authenticated Key Exchange

Our primary goal in this work is to design efficient and secure authenticated key exchange protocols that meet specific requirements of pNFS. The main results of this paper are three new provably secure authenticated key exchange protocols. We describe our design goals and give some intuition of a variety of pNFS authenticated key exchange (pNFS-AKE) protocols that we consider in this work.



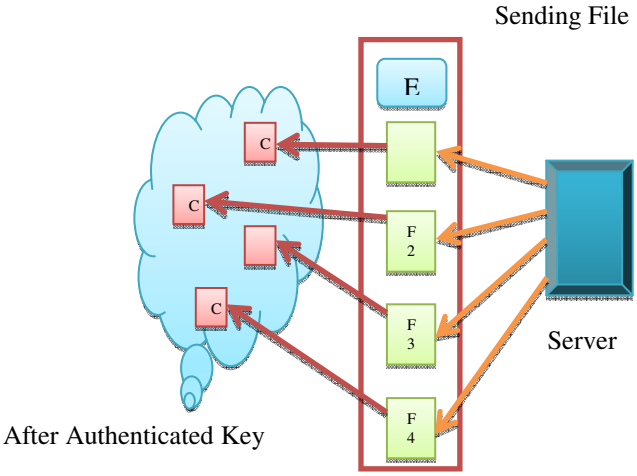

- Parallel Access to Server


- Sending Authenticated Key to Client

Fig 3.4: Authenticated Key Exchange

d. Forward secrecy

The protocol should guarantee the security of past session keys when the long-term secret key of a client or a storage device is compromised. However, the protocol does not provide any forward secrecy. To address key escrow while achieving forward secrecy simultaneously, we incorporate a Diffie- Hellman key agreement technique into Kerberos-like pNFS-AKE-I. However, note that we achieve only partial forward secrecy (with respect to v), by trading efficiency over security.



c1, c2, c3, c4 - Clients.

F1, f2, f3, f4 – Encrypted Files.

Fig 3.5: Forward secrecy

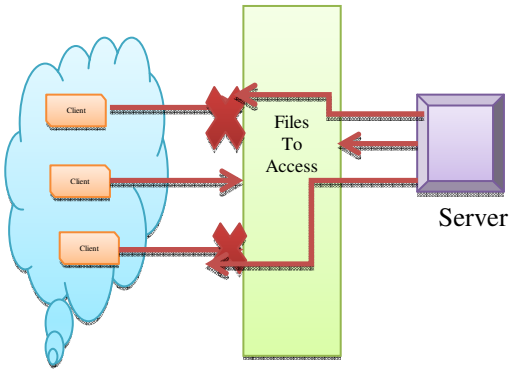
e. Server Authentication

Accept &Allow user file

The admin can accept the new user request and also block the users. The users can upload the file to Network. And the admin can allow the files to Network then only the file can store the cloud. If the file uploaded by the user is not permitted from the Server means the file cannot be uploaded by the Client.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 2, February 2016



- Server Removing Unauthorized Access

Fig 3.6: Server Authentication

D. Input Expected Output

- Parallel Session

  Input : Client access the Network for data

  Output: Server takes the IP Address of client to send Authenticated key.

- Authenticated Key Exchange

  Input : Client must enter Authenticated Key to access Files.

  Output: Data will receive to client.

- Forward Secrecy

  Input : At the time of downloading the file will encrypt for Privacy

  Output: Authenticated Key change encrypts data to Original File.

- Client Uploading and Downloading

  Input : Client can Upload and Download file with server permission.

  Output: If the Authenticated Key is correct he ca

- Server Authentication

  Input : when unauthorized User access the details

  Output: User can Block the user.

E. Use Case Diagram

The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted. In the Diagram we show how number of Clients accessing Server Parallel and Server producing Authenticated Key to Client and after exchange of authenticated key they can able to access data from the server by only key access during the time of downloading the file will be in encrypt from when the key is given it will decrypt into original form. A Server can add a new client and he can able to Block the existing client.

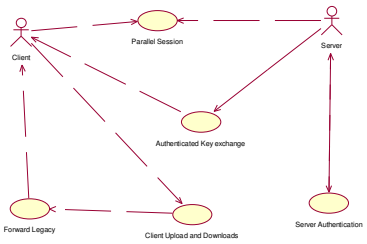


Fig 3.7: Use Case Diagram

F. Class Diagram

The class diagram is the main building block of object oriented modeling. It is used both for general conceptual modeling of the systematic of the application, and for detailed modeling translating the models into code. In the Diagram we show how number of Clients accessing Server Parallel and Server producing Authenticated Key to Client and after exchange of authenticated key they can able to access data from the server by only key access during the time of downloading the file will be in encrypt from when the key is given it will decrypt into original form. A Server can add a new client and he can able to Block the existing client.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 2, February 2016

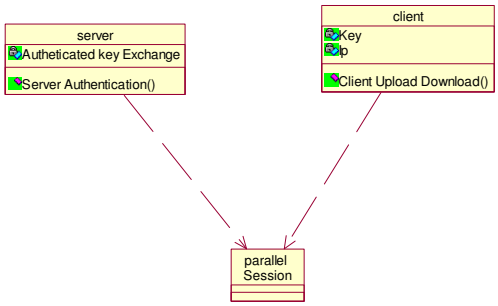


Fig 3.8: Class Diagram

G. Object Diagram

Object diagram we are telling about the flow of objects how the process is running. In the above digram tells about the flow of objects between the classes.In the Diagram we show how number of Clients accessing Server Parallel and Server producing Authenticated Key to Client and after exchange of authenticated key they can able to access data from the server by only key access during the time of downloading the file will be in encrypt from when the key is given it will decrypt into original form. A Server can add a new client and he can able to Block the existing client.

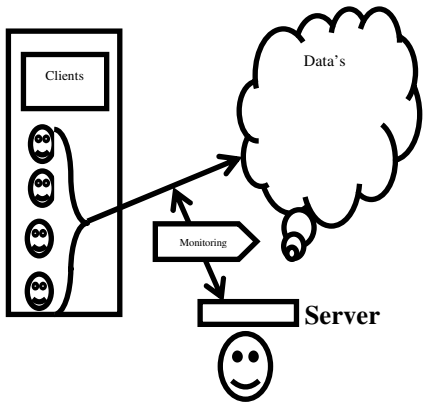


Fig 3.9: Object Diagram

H. State Diagram

State diagrams require that the system described is composed of a finite number of states; sometimes, this is indeed the case, while at other times this is a reasonable abstraction. Many forms of state diagrams exist, which differ slightly and have different semantics. In the Diagram we show how number of Clients accessing Server Parallel and Server producing Authenticated Key to Client and after exchange of authenticated key they can able to access data from the server by only key access during the time of downloading the file will be in encrypt from when the key is given it will decrypt into original form. A Server can add a new client and he can able to Block the existing client.

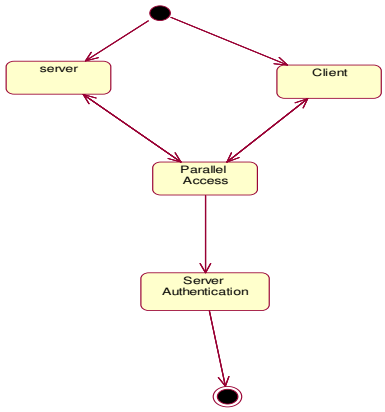


Fig 3.10: State Diagram

I. Activity Diagram

In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control. In the Diagram we show how number of Clients accessing Server Parallel and Server producing Authenticated Key to Client and after exchange of authenticated key they can able to access data from the server by only key access during the time of downloading the file will be in encrypt from when the key is given it will decrypt into original form. A Server can add a new client and he can able to Block the existing client.

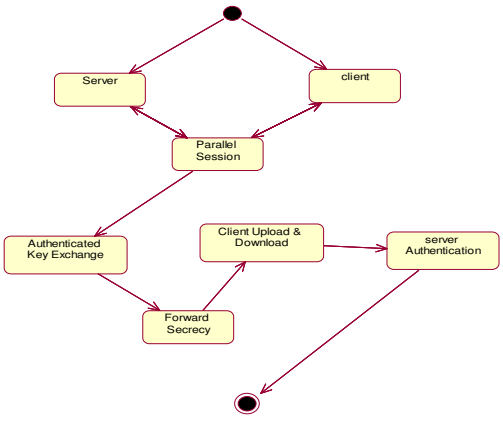


Fig 3.11: Activity Diagram

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 2, February 2016

J. Sequence Diagram

In our sequence diagram specifying processes operate with one another and in order. In our sequence diagram first get Authenticated key to get access Network. In the Diagram we show how number of Clients accessing Server Parallel and Server producing Authenticated Key to Client and after exchange of authenticated key they can able to access data from the server by only key aceess during the time of downloading the file will be in encrypt from when the key is given it will decrypt into original form. A Server can add a new client and he can able to Block the existing client.

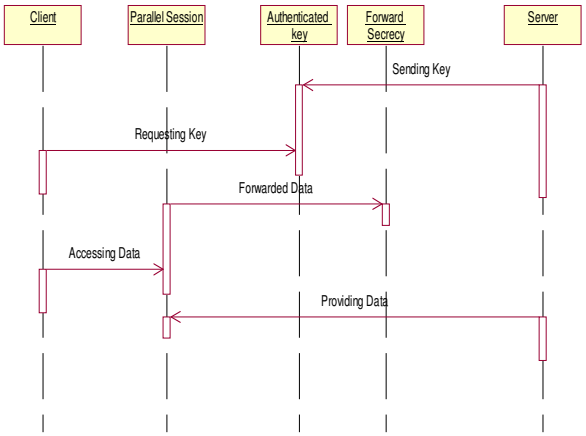


Fig 3.12: Sequenec Diagram

K. Collaboration Diagram

A collaboration diagram describes interactions among objects in terms of sequenced messages. Collaboration diagrams represent a combination of information taken from class, sequence, and use case diagrams describing both the static structure and dynamic behavior of a system. In the Diagram we show how number of Clients accessing Server Parallel and Server producing Authenticated Key to Client and after exchange of authenticated key they can able to access data from the server by only key access during the time of downloading the file will be in encrypt from when the key is given it will decrypt into original form. A Server can add a new client and he can able to Block the existing client.

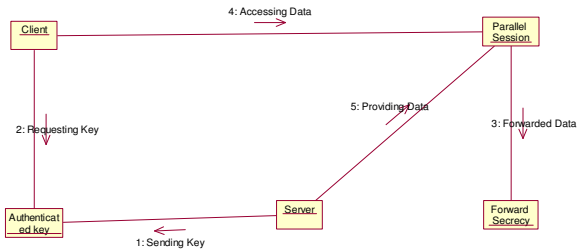


Fig 3.13: Collaboration Diagram

L. Data Flow Diagram

It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel. In the DFDs the level zero process is based on the login validations. What is the cloud user contained constraints send to the cloud provider

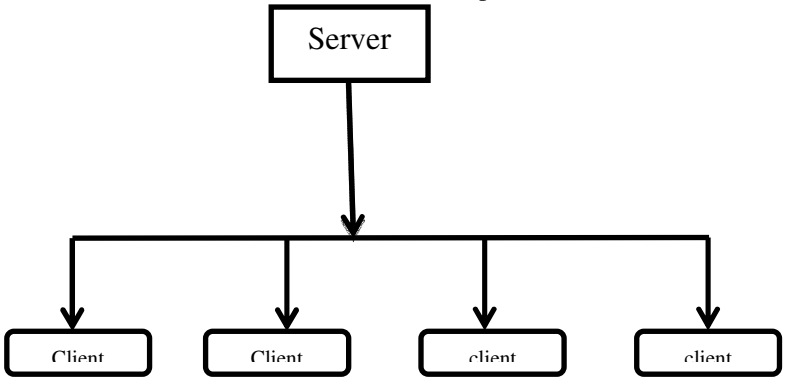


Fig 3.14: Data Flow Diagram

M. E-R Diagram

Entity-Relationship Model (ERM) is an abstract and conceptual representation of data. Entity-relationship modeling is a database modeling method, used to produce a type of conceptual schema or semantic data model of a system, often a relational database. In the Diagram we show how number of Clients accessing Server Parallel and Server producing Authenticated Key to Client and after exchange of authenticated key they can able to access data from the server by only key access during the time of downloading the file will be in encrypt from when the key is given it will decrypt into original form. A Server can add a new client and he can able to Block the existing client.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 2, February 2016

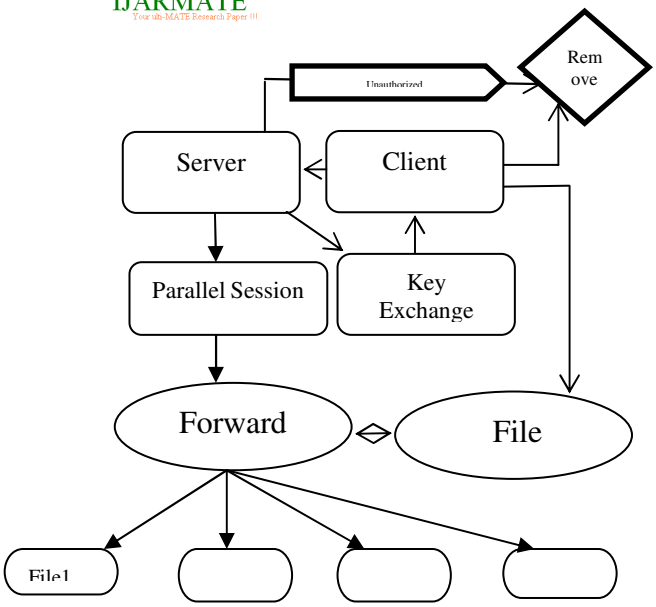


Fig 3.15: E-R Diagram

N. *Component Diagram*

In the Unified Modeling Language, a component diagram depicts how components are wired together to form larger components and they are used to illustrate the structure of arbitrarily complex systems. In the Diagram we show how number of Clients accessing Server Parallel and Server producing Authenticated Key to Client and after exchange of authenticated key they can able to access data from the server by only key access during the time of downloading the file will be in encrypt from when the key is given it will decrypt into original form. A Server can add a new client and he can able to Block the existing client.

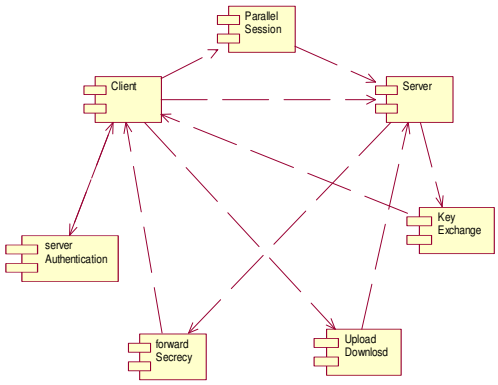


Fig 3.16: Component Diagram

III. RESULT & ANALYSIS

A. *Registration*

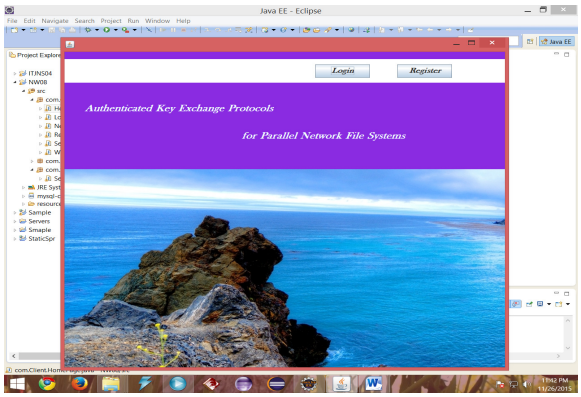


Fig 4.1: Registration

The models of registration forms are as follows:-

The steps in the registration process is displayed in three images below.

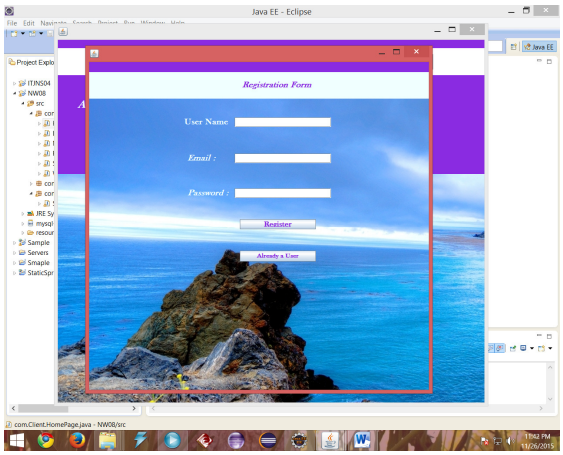


Fig 4.2: Registration Form

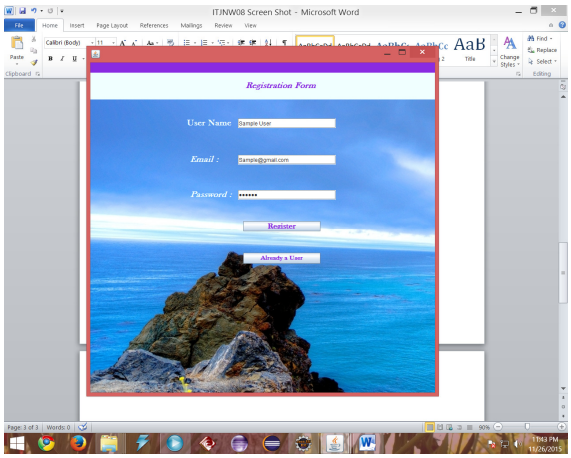


Fig 4.3: Registration Form II

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE
Your uth-MATE Research Paper !!!

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 2, February 2016

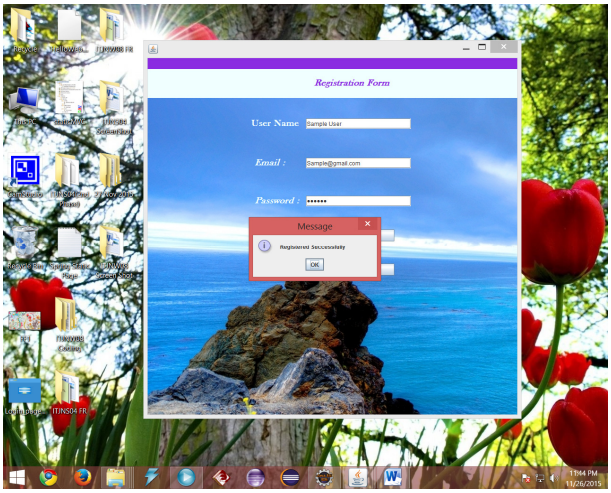


Fig 4.4: Registration Form III

B. Login

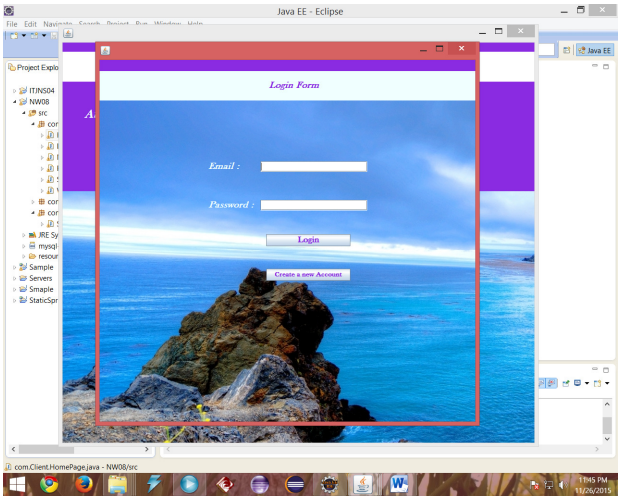


Fig 4.5: Login Page

C. Parallel Sessions

Parallel secure sessions between the clients and the storage devices in the parallel Network File System (pNFS). The current Internet standard—in an efficient and scalable manner. This is similar to the situation that once the adversary compromises the long-term secret key, it can learn all the subsequence sessions. If an honest client and an honest storage device complete matching sessions, they compute the same session key. Second, two our protocols provide forward secrecy: one is partially forward securing with respect to multiple sessions within a time period.

i. Networks Users(Parallel Sessions)

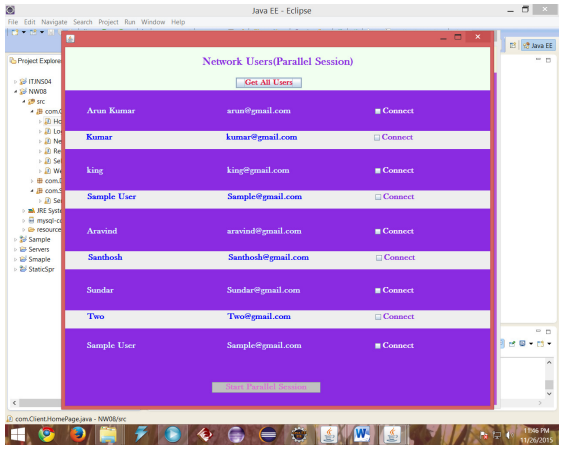


Fig 4.6: Network Users

ii. Selected Users.

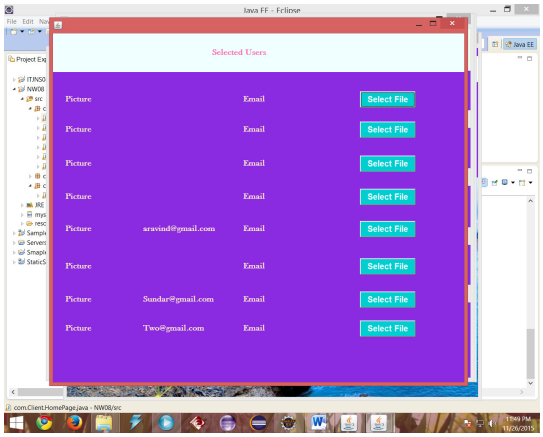


Fig 4.7: Selected Users

IV. Conclusion And Future Scope

A. Conclusion

We proposed three authenticated key exchange protocols for parallel network file system (pNFS). Our protocols offer three appealing advantages over the existing Kerberos-based pNFS protocol. First, the metadata server executing our protocols has much lower workload than that of the Kerberos-based approach. Second, two our protocols provide forward secrecy: one is partially forward securing (with respect to multiple sessions within a time period), while the other is fully forward secure (with respect to a session). Third, we have designed a protocol which not only provides forward secrecy, but is also escrow-free.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 2, February 2016

B. *Future Enhancement*

Authentication using Password authenticated key exchange using distributed server (PAKEUDE) is done where a cryptographic key - exchange of messages. Security analysis has shown that our protocol is secure against passive and active attacks in case that one of the two servers is compromised.

REFERENCES

[1] M. Abd-El-Malek, W.V. Courtright II, C. Cranor, G.R. Ganger, J. Hendricks, A.J. Klosterman, M.P. Mesnier, M. Prasad, B. Salmon, R.R. Sambasivan, S. Sinnamohideen, J.D. Strunk, E. Thereska, M. Wachs, and J.J. Wylie. Ursa Minor: Versatile cluster-based storage. In Proceedingsof the 4th USENIX Conference on File and Storage Technologies (FAST), pages 59–72. USENIX Association, Dec 2005.

[2] C. Adams. The simple public-key GSS-API mechanism (SPKM). The Internet Engineering Task Force (IETF), RFC 2025, Oct 1996.

[3] Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, and R. Wattenhofer. "FARSITE: Federated, available, and reliable storage for an incompletely trusted environment." In Proceedings of the 5th Symposium on OperatingSystem Design and Implementation (OSDI). USENIX Association, Dec 2002.

[4] M.K. Aguilera, M. Ji, M. Lillibridge, J. MacCormick, E. Oertli, D.G. Andersen, M. Burrows, T. Mann, and C.A. Thekkath. Blocklevel security for network-attached disks. In Proceedings of the 2nd International Conference on File and Storage Technologies (FAST). USENIX Association, Mar 2003.

[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] Amazon simple storage service (Amazon S3). http://aws.amazon.com/s3/.

[7] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In Advances in Cryptology– Proceedings of EUROCRYPT, pages 139–155. Springer LNCS 1807, May 2000.

[8] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Advances inCryptology – Proceedings of CRYPTO, pages 258–275. Springer LNCS 3621, Aug 2005

[9] B. Callaghan, B. Pawlowski, and P. Staubach. NFS version 3 protocol specification. The Internet Engineering Task Force (IETF), RFC 1813, Jun 1995.

AUTHORS BIOGRAPHY

P.Bercelin Raj was born on 1990. He attended an International Seminar at Agni college of Engineering & technology,Chennai on Digital Image Processing and its applications.. He has also attended an international conference at Panimalar College of Engineering and Technology,Chennai on the topic of Network Management. He has also attended an International Conference at Sri Sai Ram College of Engineering and technology chennai on the topic of Mobile Computing. Currently He is a PG Scholar at Mar Ephraem College of Engineering and Technology in the department of computer science and engineering. He had completed his UG at GKM College of Engineering and Technology Chennai in the department of Computer Science & Engineering. He had completed his diploma at Morning Star Polytechnic College,Chunkankadai. His area of interest is working on Networking and Mobile Computing.