Authenticated Key Exchange Protocols for Parallel Network File Systems

C.INDUMATHI[1] S.MEEN[2] R.RAJPRIYA[3] N.POORNIMA[4] K.SUVITHA[5]

[1](B.E (CSE), Kongunadu College of Engg & Tech, Trichy, India, kkmailit@gmail.com)
[2](Principal, Kongunadu College of Engg & Tech, Trichy, India)

***ABSTRACT**:* In this paper, we propose a variety of authenticated key exchange protocols that are designed to address the issues. We show that our protocols are capable of reducing 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 secure, while the other is fully forward secure. Third, we have designed a protocol which not only provides forward secrecy, but is also escrow-free.

KEYWORDS:

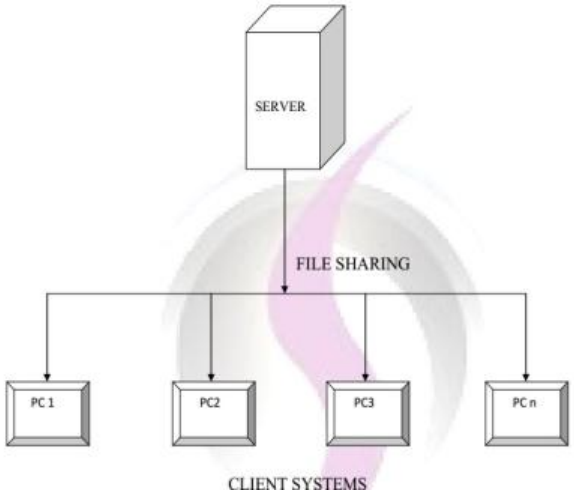
INTRODUCTION

In this work, we 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 accessing multiple remote and distributed storage devices 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.

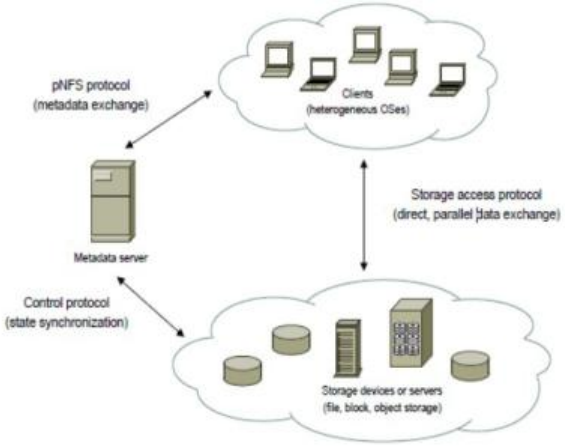
EXISTING SYSTEM

Key establishment for secure many-to-many communications. The proliferation of large-scale distributed file systems supporting parallel access to multiple storage devices. Parallel Network File System (pNFS) makes use of Kerberos to establish parallel session keys between clients and storage devices.



PROPOSED SYSTEM

Variety of authenticated key exchange protocols that are designed to address the existing issues. Protocols are capable of reducing the workload of the metadata server and concurrently supporting forward secrecy and escrow-freeness. Metadata server executing our protocols has much lower workload than that of the Kerberos-based approach.

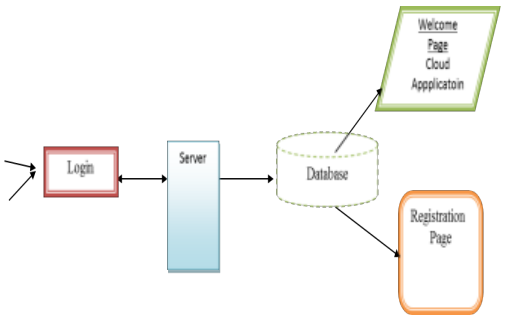


MODULES

- User Interface Design
- Parallel sessions
- Authenticated key exchange
- Forward secrecy
- Un Authorized Access
- Server Authentication

USER INTERFACE DESIGN MODULE

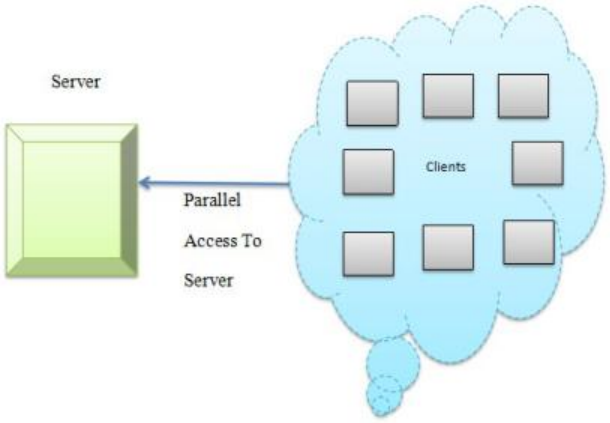
The important role for the Network user is to move login window to cloud user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not. If we enter any invalid username or password we 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. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and sever authentication.



PARALLEL SESSIONS

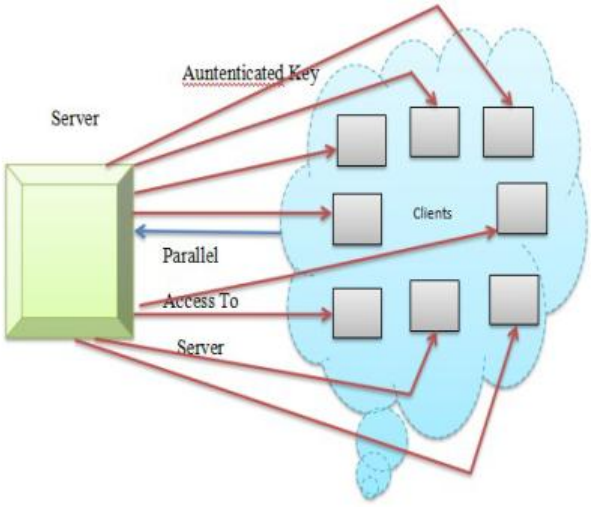
Parallel secure sessions between the clients and the storage devices in the parallel Network File System (pNFS). The current Internet standard-in an efficient and scalable manner. This is similar to the situation that once the adversary compromises the long-term secret key,

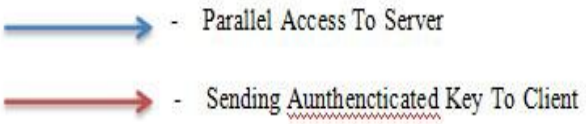
it can learn all the subsequence sessions. If an honest client and an honest storage device complete matching sessions, they compute the same session key. Second, two our protocols provide forward secrecy: one is partially forward secure with respect to multiple sessions within a time period.



AUTHENTICATED KEY EXCHANGE MODULE

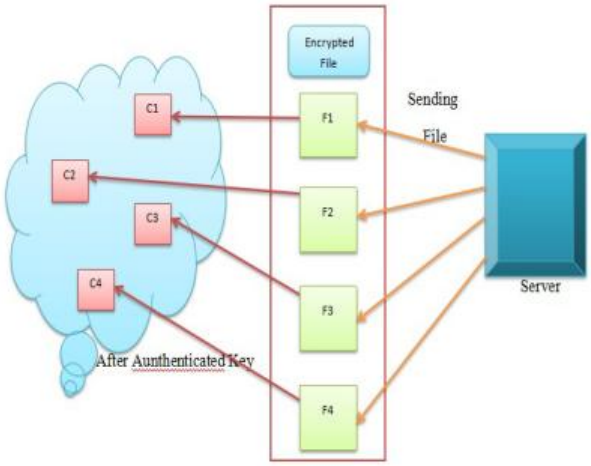
Our primary goal in this work is to design efficient and secure authenticated key exchange protocols that meet specific requirements of pNFS.The main results of this paper are three new provably secure authenticated key exchange protocols.We describe our design goals and give some intuition of a variety of pNFS authenticated key exchange6 (pNFS-AKE) protocols that we consider in this work.





FORWARD SECRECY MODULE

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, by trading efficiency over security.

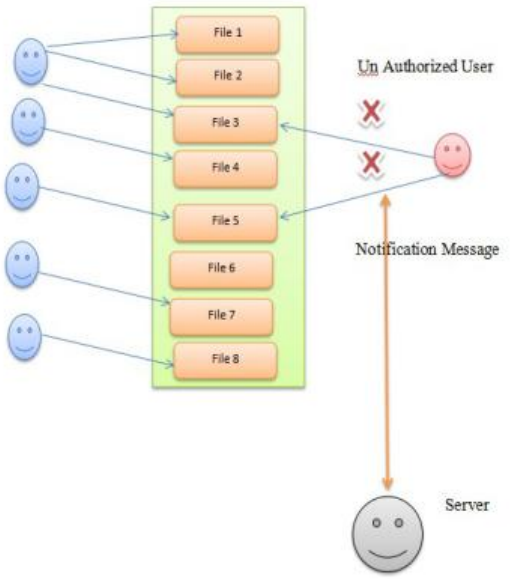


UN AUTHORIZED ACCESS

In this module the unauthorized user i.e., the users who are not having permission to access other information. The user who uses the network in a wrong manner may block by the server when the server gets a notification message that someone is accessing in unauthorized access. Once the Unauthorized

user blocked by the server cannot be undone ever.

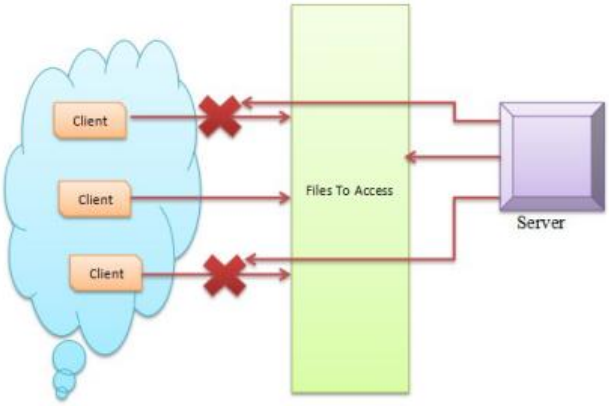
Authorized



SERVER AUTHENTICATION MODULE

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.



- Server Removing Unauthorized Access

ALGORITHM

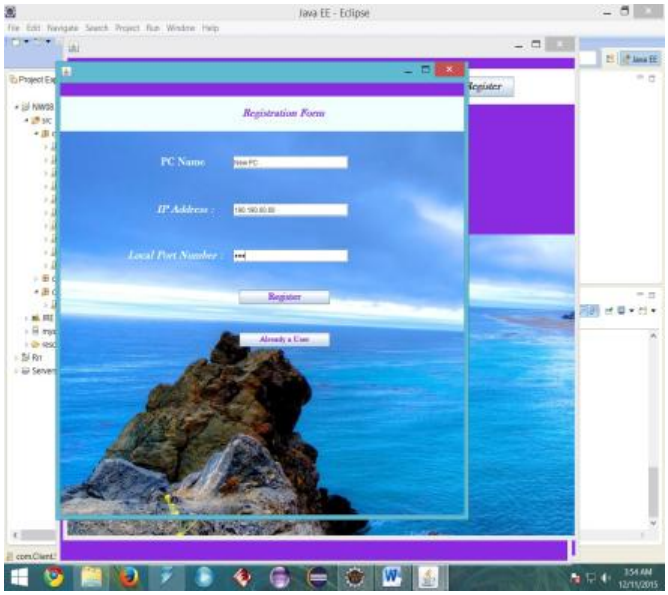
Diffie-Hellman key agreement:

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.

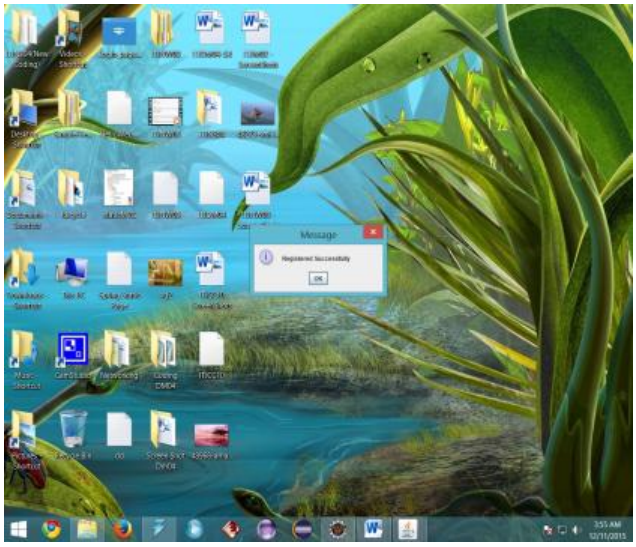
FUTURE ENHANCEMENT:

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.

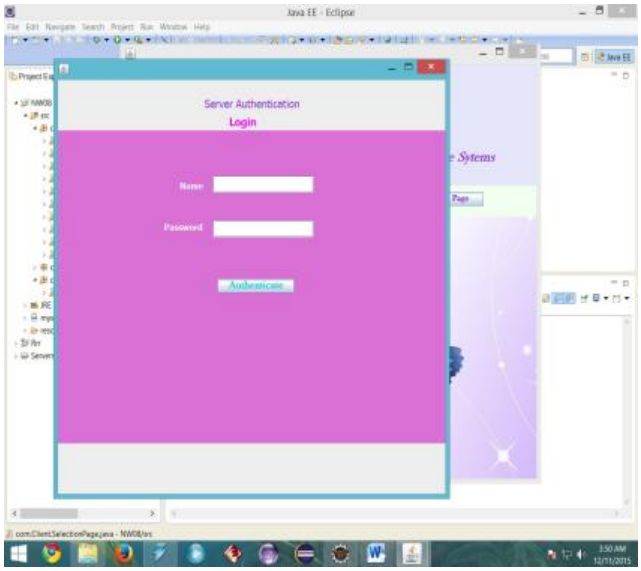
User interface module:



TO IDENTIFY SERVER RESPONSE:



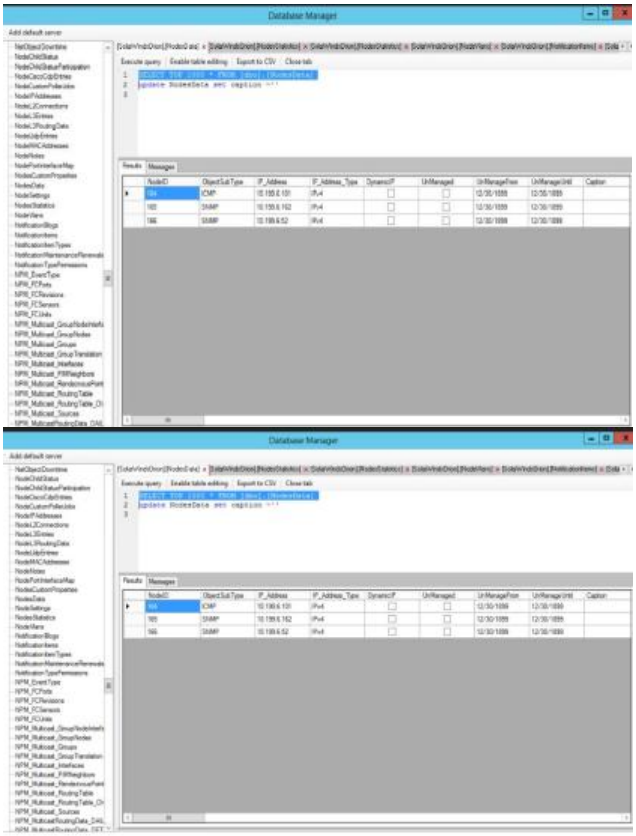
SERVER AUTHENTICATION LOGIN:



TABLES CREATIONS

Table definitions must have a valid locator. The locator describes the real-world object that the table definition was derived from. A locator is created automatically when you import the table definition from a data source, or you can specify a locator in the Table Definition Properties window.

TABLE FORMAT FOR KEY EXCHANGE:



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

secure (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.

REFERENCES

[1] A. Zouaq and R. Nkambou, "Evaluating the Generation of Domain Ontologies in the Knowledge Puzzle Project," IEEE Trans. Knowledge and Data Eng., vol. 21, no. 11, pp. 1559-1572, Nov. 2009.

[2] A. Maedche and S. Staab, "Ontology Learning for the Semantic Web," IEEE Intelligent Systems, vol. 16, no. 2, pp. 72-79, Mar. 2001.

[3] P. Velardi, R. Navigli, A. Cucchiarello, and F. Neri, "Evaluation of Onto Learn, a Methodology for Automatic Learning of Domain Ontology's," Ontology Learning from Text: Methods, Applications, and Evaluation, P. Buitelaar, P. Cimiano, and B. Magnini, eds., pp. 92-106, IOS Press, 2005..

[4] A. Conde, M. Larran˜ aga, I. Calvo, J.A. Elorriaga, and A. Arruarte, "Automating the Authoring of Learning Material in Computer Engineering Education," Proc. 42nd IEEE Frontiers in Education Conf. (FIE '12), pp. 1376-1381, 2012.

[5] "Constraint Grammar: Language-Independent System for Parsing Unrestricted Text," Natural Language Processing, F.Karlsson, A. Voutilainen, and J. Heikkila, eds., no. 4, Mouton de Gruyter, 1995.

[6] T. Leidig, "L3-Towards an Open Learning Environment," ACM J. Educational Resources in Computing, vol. 1, no. 1, pp. 5-11, 2001.

[7] P. Vossen, "Extending, Trimming and Fusing WordNet for Technical Documents," Proc. Second Meeting of the North Am. Chapter of the Assoc. for Computational Linguistics (NAACL '01), 2001 .

[8] K. Verbert, D. Ga_sevi_c, J. Jovanovi_c, and E. Duval, "Ontology- Based Learning abContent Repurposing," Proc. 14th Int'l Conf. World Wide Web (WWW '05), pp. 1140-1141, 2005.

[9] M. Larran˜aga, I. Niebla, U. Ruedat, J.A. Elorriaga, and A.Arruarte, "Towards Collaborative Domain Module Authoring," Proc. Seventh IEEE Int'l Conf. Advanced Learning Technologies (ICALT '07), pp. 814-818, July 2007.

[10] K. Cardinaels, M. Meire, and E. Duval, "Automating Metadata Generation: The Simple Indexing Interface," Proc. 14th Int'l Conf. World Wide Web (WWW '05), 2005.