PNFS PROTOCOLS USING AUTHENTICATION FOR EFFICIENT AND SECURE KEY EXCHANGE

[1] Nasleena p.n, [2] Mable Jose
[1] Student, [2] Assistant professor
[1]Computer science,
[1] St. Joseph's College , Thrissur, India

Abstract : ***In parallel network file systems the key exchange using for the secure communication. the multiple storage devices are access parallel .Earlier used Kerberos based protocols. But it has some limitations. to avoid these limitations here introduce the new protocols that is PNFS protocol. the advantages of these protocols is scalability to reduce the workload of metadata server. Meta data server generates the session keys. provide forward secrecy for the long term secret key produce of clients or storage devices .and also provide the key escrow freeness in between the clients and storage devices.***

IndexTerms - parallel networks, scalability, forward secrecy , escrow freeness, secret key.

I. INTRODUCTION

In many to many communications of large scale network systems that support parallel access to multiple storage devices .that is large number of clients access multiple storage devices in parallel. so the main purpose of this proposed system is to define the key exchange and establish parallel secure sessions between clients and storage devices in parallel network file system. and also using the three protocols for improve the performance than kerberos based protocol. the protocols used for efficient and secure key exchange and that reduce the workload of meta data server .the computational overhead of clients and storage devices at a reasonably low level. PNFS protocols allow direct and concurrent access to multiple storage devices to improve the performance and scalability .the PNFS file system has two parts. Meta data processing and data processing. the three protocols PNFS protocol that transfer the file meta data between the metadata server and client node. The storage access protocol using client access the data from the associated storage devices according to corresponding meta data .the control protocol using the synchronizes state between meta data server and storage devices.

II.EXISTING SYSTEM

For secure key exchange using the Kerberos-based protocol but that has some limitations[1]. the meta data server generates the session keys that are used between client and storage devices .meta data server has heavy work load. some of the earliest work in securing large-scale distributed file systems, for example have already employed Kerberos for performing authentication and enforcing access control[1].

III.PROPOSED SYSTEM

In this paper the three protocols provide the advantages are scalability, forward secrecy, and escrow free. The meta data server provide the secret key to the client when they are in authenticated user. and also a session key pass. Client using file transfer in parallel file system. session keys give the meta data server for the communication established client and storage devices. Mainly focus on how to exchange key materials and establish parallel secure sessions between the clients and the storage devices in parallel Network File System(PNFS)the current Internet standard ,in an efficient and scalable manner[2]. 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 subsequences session **,** second , two our protocols provide forward secrecy: one is partially forward securing with respect to multiple sessions within a time period[4].

IV.SYSTEM ARCHITECTURE

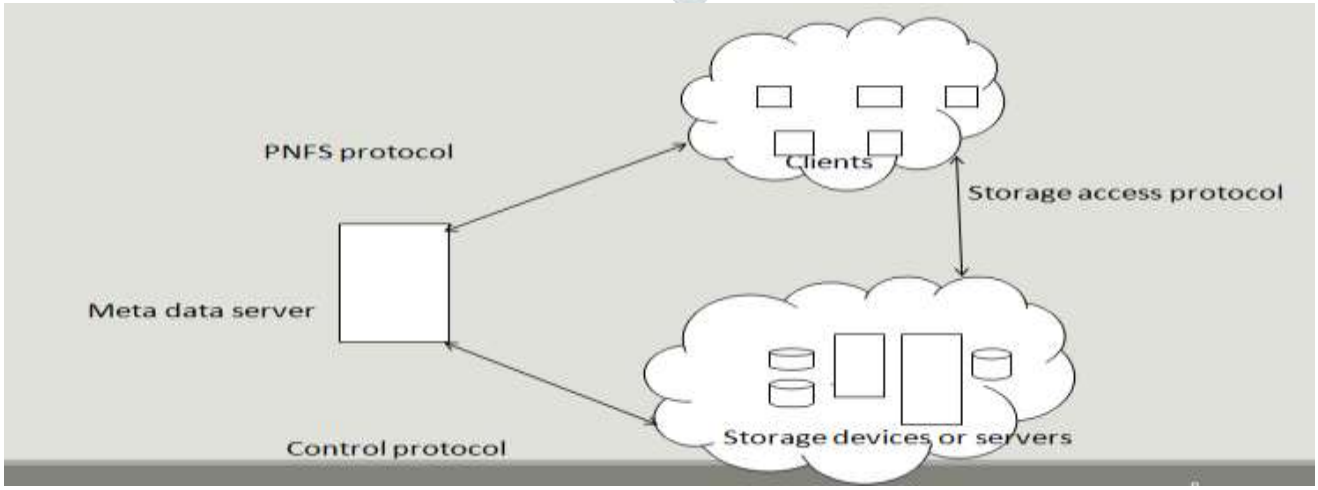

fig 1:conceptual model of PNFS protocols

The figure shows the conceptual model of PNFS protocols. the three protocols provides the communication make possible more secure and authentic in parallel network file systems clients, meta data server and storage devices are connected through the protocols.

V.METHODOLOGY

In this paper using Kerberos based PNFS protocol .server and client communication for file transfer. The meta data server pass the session keys and also provide the secret key. Meta data plays a vital role in managing the client operation[3]. It generates one-Time Password(OTP)to authenticated the user access[3].

VI.IMPLEMENTATION

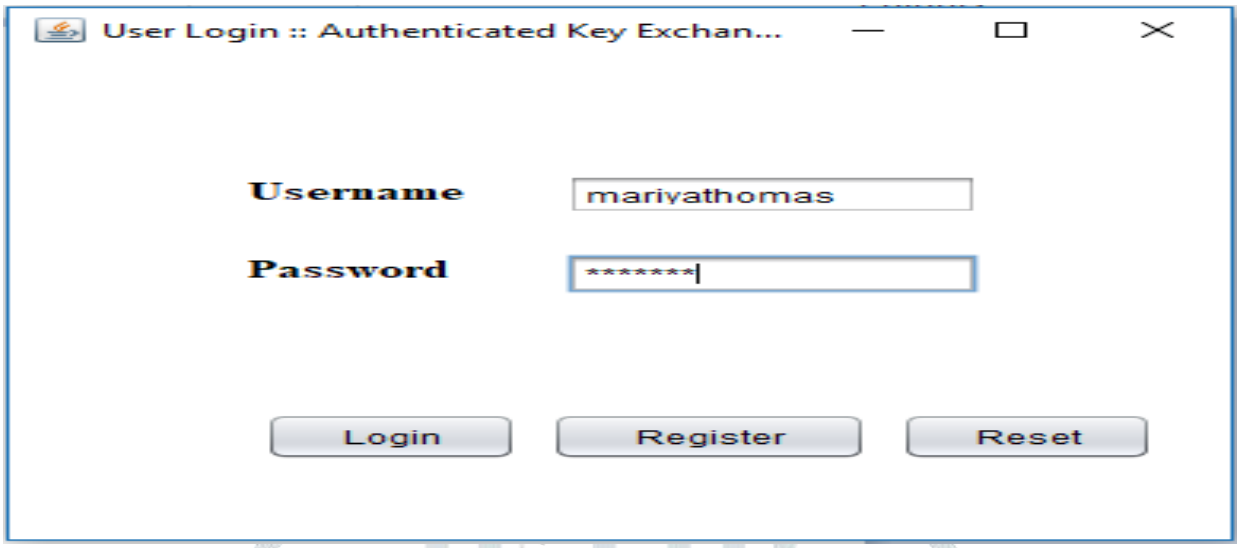

Fig 2:user login

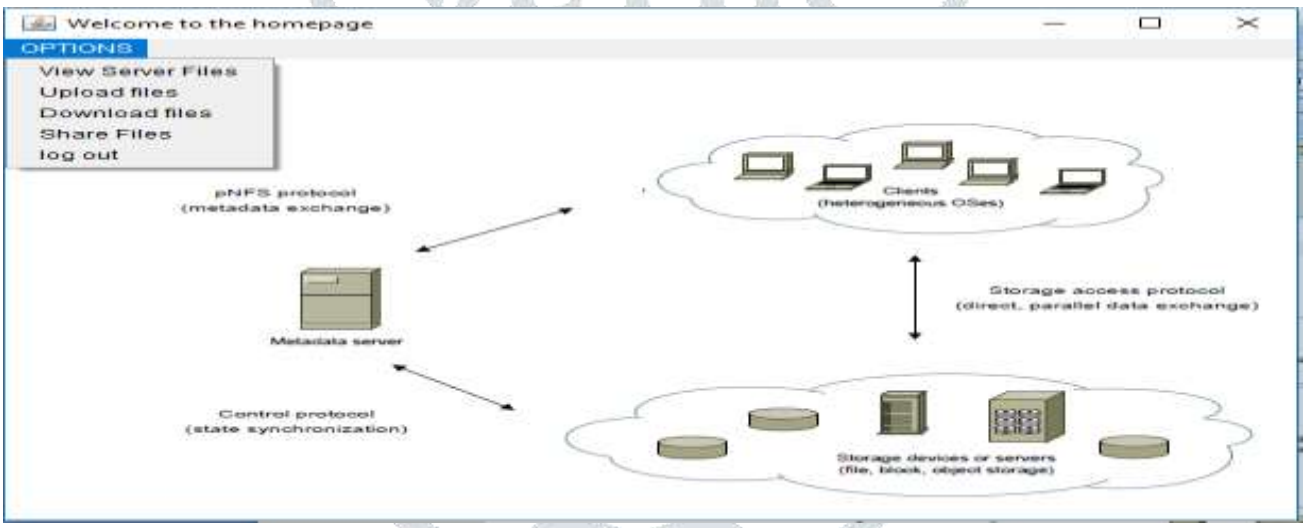

fig 3:user home page

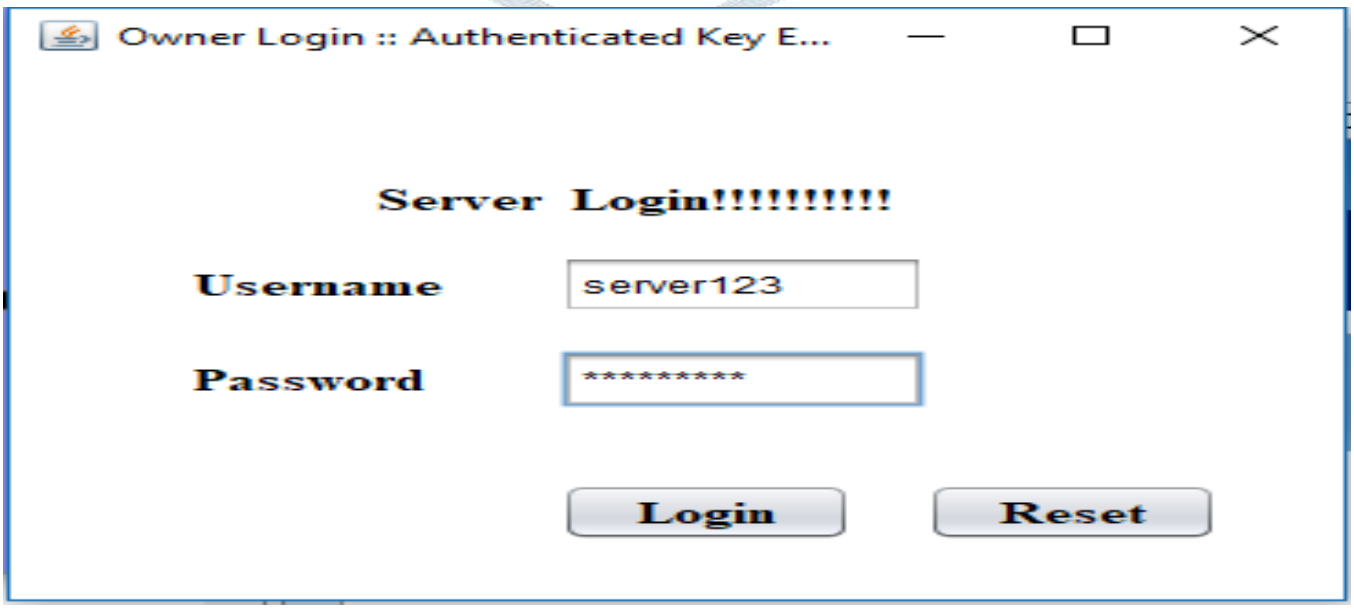

Fig 4:admin login

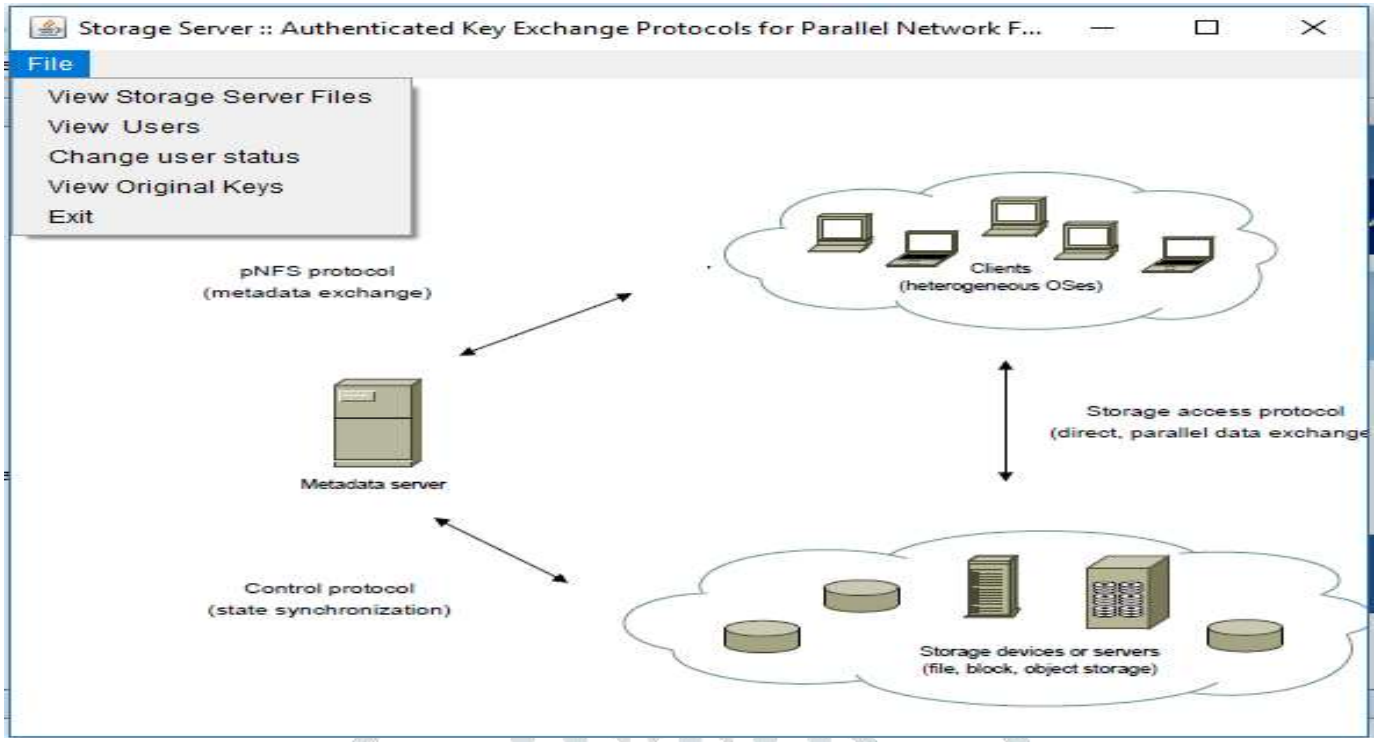

Fig 5:admin home page

VII.CONCLUSION

Proposed three authenticated key exchange protocols that overcome the limitations of Kerberos based protocol. that reduce the work load .provide forward secrecy with respect to multiple sessions and single session .and also the protocol provide escrow free.

VIII. ACKNOWLEDGEMENT

Fist and for most, I would like to thank GOD Almighty for his guidance and wisdom as I make the paper publication. and also I would like to thank my guide for her most support and encouragement for giving me this paper publication .finally I sincerely thank to my parents ,friends ,who provide the advice and support.

REFERENCES

[1] Hoon Wei Lim ,Guomin Yang :authenticated key exchange protocol for parallel network file system.
[2] LeMeniz Infotech:authenticated key exchange protocol for parallel network file systems.
[3] Singh Vikas J.,Shaikh faiz I.,Ahire Akash R.,Singh Vivekkumar R. :Parallel Network file system with Authenticated key exchange protocols
[4] Ganjali Lucky,K.Lakshmi.Anil Kumar:authenticated key exchange protocols for parallel network file systems,ijitech international journal of innovative technologies