International Journal on Applications in Information and Communication Engineering
Volume 8 : Issue 1 : June 2022, pp 24 – 28 www.aetsjournal.com ISSN (Online) : 2394 - 6237

AUTHENTICATED KEY EXCHANGE PROTOCOLS FOR PARALLEL NETWORK FILE SYSTEM

VIDHYA . M , K. RENUKA

Abstract— This Project entitled **"Authenticated Key Exchange Protocols for Parallel Network File System"** as Front End: PHP, Back End: MYSQL. The problem is inspired by the proliferation of large-scale distributed file systems supporting parallel access to multiple storage devices. A scalable file system that logically functions as a centralized file server but is physically distributed among a set of untrusted computers. Our work focuses on the current Internet standard for such file systems, i.e., parallel Network File System (pNFS), which makes use of Kerberos to establish parallel session keys between clients and storage devices. Our review of the existing Kerberos-based protocol shows that it has a number of limitations: (i) a metadata server facilitating key exchange between the clients and the storage devices has a heavy workload that restricts the scalability of the protocol; (ii) the protocol does not provide forward secrecy; (iii) the metadata server generates itself all the session keys that are used between the clients and storage devices, and this inherently leads to key escrow. In this paper, we propose a variety of authenticated key exchange protocols that are designed to address the above 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**..**

***Keywords*—**Protocols, Distributed File System, Parallel Network File System, Kerberos.

I. INTRODUCTION

Authentication and key establishment are fundamental steps in setting up secure communications. Authentication is concerned with knowing that the correct parties are communicating; the key establishment is concerned with obtaining good cryptographic keys to protect the communications, particularly to provide confidentiality and integrity of the data communicated. Because the modern world increasingly relies on digital networks, the security of communications is a critical element in the functioning of society today and will become only more important in the future. Authentication and key establishment typically occur at the start of a communications session, which we often call simply a session. Authentication allows those parties active in the session to learn the identity of other parties in the session. Key establishment is used to set up a session key, used to subsequently protect the data communicated during the session with the help of whatever cryptographic mechanisms are chosen.

Vidhya M, Student, B.Sc Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India – 641021, (e-mail: vidhya.manickam20@gmail.com).

Mrs.K.Renuka, Head of the Department, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India – 641021,
(e-mail: hod.csc@rathinam.in).

II. SYSTEM STUDY

A. Existing System:

Independent of the development of cluster and high-performance computing, the emergence of clouds and the map-reduce programming model has resulted in file systems such as the Hadoop Distributed File system (HDFS) Amazon S3 file system, and cloud store.

Disadvantages:

- The current focuses on interopibility, instead of efficiency and scalability, of Various mechanisms to provide basic security.
- Moreover, key establishment between a client and multiple storage devices.

B. Proposed System:

In this work, we investigate the problem of securing many to many communications in the large-scale network file system that supports parallel access to multiple storage devices.

Advantages:

The proposed system achieves the following three:

- Scalability - the metadata server facilitating access requests from client to Multiple storage devices.
- Forward Secrecy - the protocol should guarantee the security of past session keys.
- Escrow free - the metadata server should not learn any information about any keys.

III. PROPOSED WORK

A. Module Description:

1)Cloud Network Formation:

Parallel secure sessions between the customers and the capacity gadgets in the parallel Network File System (pNFS) The present Internet standard—in a productive and versatile way. This is like the circumstance that once the foe bargains the long haul mystery key, it can take in all the subsequence sessions. In the event that a legitimate customer and a genuine stockpiling gadget finish coordinating sessions, they register a similar session key. Second, two of our conventions give forward mystery: one is somewhat forward secure regarding various sessions inside a day and age.

2)Authenticated key exchange:

Our essential objective in this work is to plan proficient and secure validated key trade conventions that meet particular necessities of pNFS. The principle after effects of this paper is three new provably secure confirmed key trade conventions. Portray our outline objectives and give some instinct of an assortment of pNFS verified key exchange6 (pNFS-AKE) conventions that we consider in this work.

3)Forward secrecy:

The convention should ensure the security of past session keys when the long-haul mystery key of a customer or a capacity gadget is bargained. Be that as it may, the convention does not give any forward mystery. To address key escrow while accomplishing forward mystery at the same time, we fuse a Diffie-Hellman enter understanding strategy into Kerberos-like pNFS-AKE-I.

B. User login:

User Registration / Login:

After the registration, he will be issued with valid user id and password by the Administrator. The user can log in to the system with this User Id and Password. After successfully login into the system, the user moves to the instruction web page where A user's account allows a user to authenticate to a system and to be granted authorization to access resources provided by or connected to that system; however, authentication does not imply authorization. To log into an account, a user is typically required to authenticate oneself with a password or other credentials for the purposes of accounting, security, logging, and resource management. Once the user has logged on, the operating system will often use an identifier such as an integer to refer to them, rather than their username, through a process known as identity correlation.

C. User Privileges:

1) Offer Data

The client can share their information with another client in the same gathering the information will decipher by way of setting information.

2)Transfer Data

The client can transfer the document to the cloud. What's more, the Admin can enable the information to store in the cloud.

3)Download File

The client likewise downloads the cloud record by the conditions.

D. Server Authentication:

1) Acknowledge client

The administrator can acknowledge what the new client asks for and furthermore dark the clients.

2)Permit client document

The clients can transfer the document to the cloud. Furthermore, the administrator can enable the documents to the cloud then just the record can store in the cloud.

E. Software Description:

Front End: PHP

PHP stands for Hypertext Preprocessor. PHP scripts run inside Apache server or Microsoft IIS. PHP and Apache server are free. PHP code is very easy. PHP is the most used server side scripting language. PHP files contain PHP scripts and HTML. PHP files have the extension "php", "php3", "php4", or "phtml".

Generate dynamic web pages. PHP can display different content to different user or display different content at different times of the day Process the contents of HTML forms. We can use an PHP to retrieve and respond to the data entered into an HTML form. Can create database-driven web pages. An PHP can insert new data or retrieve existing data from a database such a MySQL.

PHP is a standard HTML file that is extended with additional features. Like a standard HTML file, PHP contains HTML tag that can be interpreted and displayed by a web browser. Anything we could normally place in an HTML file Java applets, Blinking text, server side scripts. We can place in PHP. However, PHP has three important features that make it unique. PHP contains server side scripts. PHP provides several built-in objects.

Back End: MYSQL

The MySQL server provides a database management system with querying and connectivity capabilities, as well as the ability to have excellent data structure and integration with many different platforms. It can handle large databases reliably and quickly in high-demanding production environments. The MySQL server also provides rich function such as its connectivity, speed, and security that make it suitable for accessing databases.

The MySQL server works in a client and server system. This system includes a multiple-threaded SQL server that supports varied backend, different client programs and libraries, administrative tools, and many application programming interfaces (API)s.

To get started, you must do the following:

1. Download MySQL Version 5.0.27.
2. Build and load the MySQL server.
3. Initialize the MySQL database.
4. Start the MySQL server.

F. System Testing:

System testing is the state of implementation, which is aimed at ensuring that the system works accurately and efficiently as expected before the live operation, commences. It certifies that the whole set of programs hangs together System testing requires a test plan, that consists of several key activities and steps for running the program, string, system, and user acceptance testing. The implementation of a new design package is important in adopting a successful new system.

Testing is an important stage in software development. The system test's implementation should be a confirmation that all is correct and an opportunity to show the users that the system works as they expected It accounts for the largest percentage of technical effort in the software development process.

The testing phase is the development phase that validates the code against the functional specifications. Testing is vital to the achievement of the system's goals. The objective of testing is to discover errors. To fulfill this objective a series of test steps such as the unit test, integration test, validation, and system test were planned and executed.

G. Unit Testing:

Unit testing is testing changes made in an existing or new program this test is carried out during the programming and each module is found to be working satisfactorily. For example in the registration form after entering all the fields we click the submit button. When submit button is clicked, all the data in the form are validated. Only after validation entries will be added to the database.

H. Validation Testing:

Software validation is achieved through a series of tests that demonstrate conformity with requirements. Thus the proposed system under

consideration has been tested by validation & found to be working satisfactorily.

I. Output Testing:

Ask the user about the format required by the tests and the output generated by the system under consideration. It can be done in two ways, one on screen and the other in printer format. The output format on the screen is found to be correct as the format designed n the system test.

J. Testing Results:

All the tests should be traceable to customer requirements the focus of testing will shift progressively from programs Exhaustive testing is not possible To be more effective testing should be which has a probability of finding errors.

The following are the attributes of a good test

1. A good test has a probability of finding a errors.
2. A good test should be “best of breeds”.
3. A good test to be neither simple nor too complex.

K. System Implementation:

System Implementation is the stage in the project where the theoretical design is turned into a working system. The most crucial stage is achieving a successful new system and giving a user confidence in that the new system will work efficiently and effectively in the implementation stage.

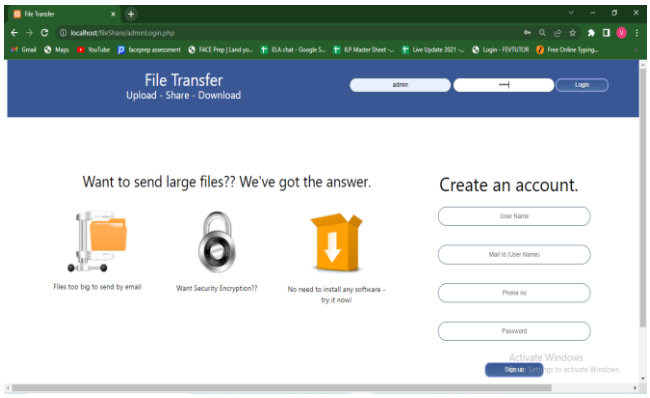
The stage consist of

1. Testing a developed program with sample data
2. Detection and correction of error
3. Creating whether the system meets a user requirements
4. Making necessary changes as desired by users.
5. Training user personal

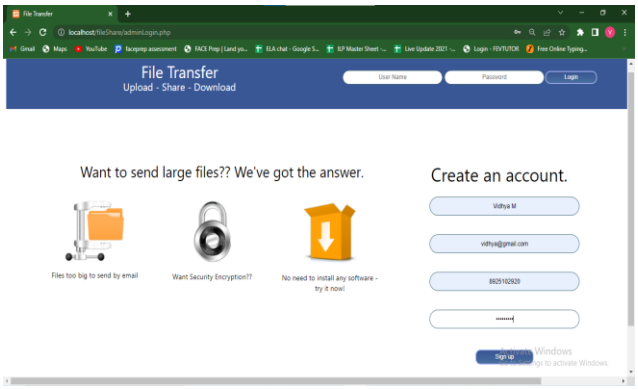
The implementation phase is less creative than system design. A system design may be dropped at any time prior to implementation, although it becomes more difficult when it goes to the design phase. The final report of the implementation phase includes procedural flowcharts, record layouts, and a workable plan for implementing the candidate system design into a operational design.PHP and MY SQL has offer very efficient yet a simple implementation technique for development of the project.

IV. EXPERIMENTAL RESULTS

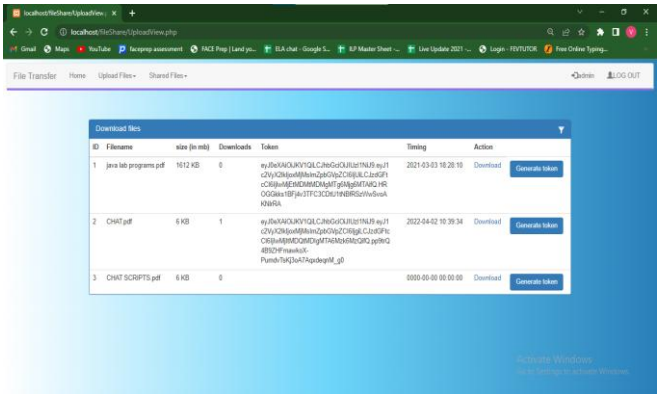
Admin Login



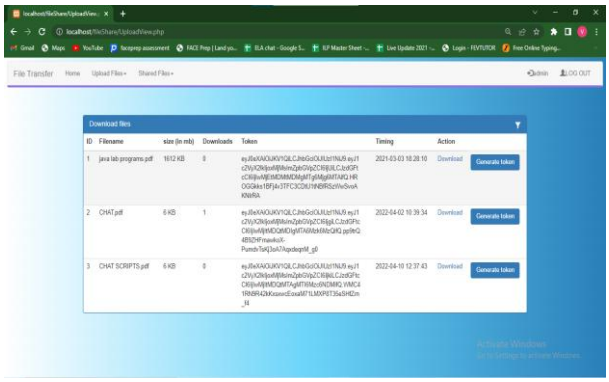
User Registration



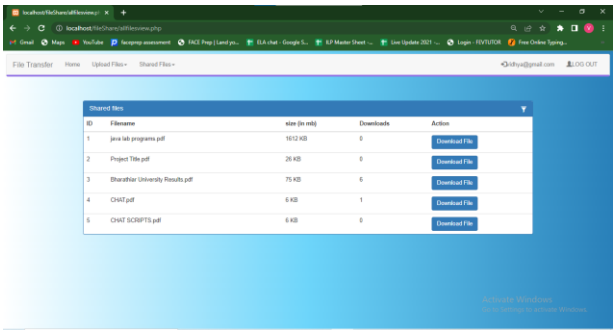
Upload Files View



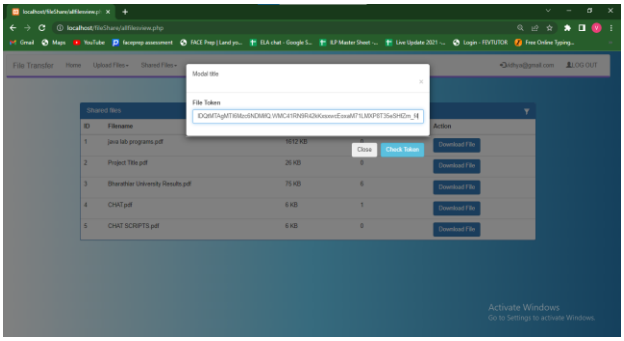
Generate Token



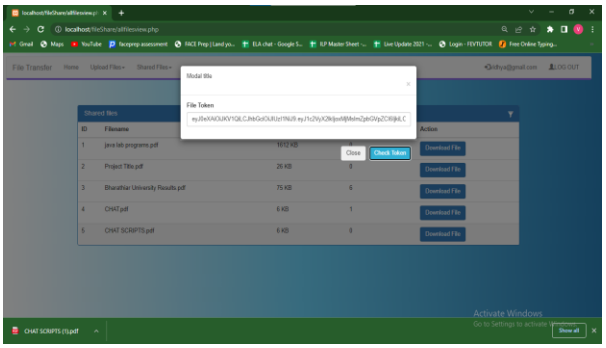
Shared Files View



File Token



File Downloaded



V. CONCLUSION

The "Authenticated Key Exchange Protocols for Parallel Network File System" has been developed to satisfy all proposed requirements. The process is maintained more simple and easy. The system is highly scalable and user-friendly. Almost all the system objectives have been met. The system has been tested under all criteria. The system minimizes the problem arising in the existing manual system and it eliminates the human errors to zero level. The design of the database is flexible ensuring that the system can be implemented. All phases of development were conceived using methodologies. Users with little training can get the required report. The software executes successfully by fulfilling the objectives of the project. Further extensions to this system can be made required with minor modifications.

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. In Future we enhance pNFSAKE- II with a key update technique based on any efficient one-way function, such as a keyed hash function. In Phase I, we require C and each Si to share some initial key material in the form of a Diffie-Hellman key.

REFERENCES

[1] S. Sathya, M. Ranjith Kumar, K. Madheswaran, "Parallel network file systems using authenticated key exchange protocols", June 2017.
[2] K. Chandra, Shaik Rehma Thunnisa Naga, "Authenticated Key Exchange Protocols for Parallel Network File Systems", March 2018.
[3] Raouf Boutaba, Nelson Fonseca, Dzmitry Kliazovich, Noura Limam, "Cloud Networking and Communications II", December 2015.
[4] Raouf Boutaba, Noura Limam, Stefano Secci, Tarik Taleb, "Communications and Networking in the Cloud", August 2014.
[5] Jiaqiu Wang and Zhongjie Wang, "A Survey on Personal Data Cloud",August 2014.