DEVELOPMENT OF A DISTRIBUTED FILE SHARING SYSTEM IN AN ENTERPRISE USING ACCESS CONTROL MECHANISM

I. J MGBEAFULIKE(1) **M.K OKPARA(2)**

[1]Department of Computer Science, Chukwuemeka Odumegwu University, Uli
[2]Department of Computer Science, Abia State Polytechnic, Aba

ABSTRACT
With the increasing usage of online file sharing platform, the security of these currently provided services becomes a list topic among the users. Files are more easily to be shared however their confidentiality is also dropped. Some file sharing platform allows users to download files without the need to input any password. The aim of this research is to design and implement a distributed file sharing and access control system that will provide users with an online storage and sharing platform and at the same time, with sufficient security means. The methodology used in developing the system is Structured System Analysis and Design Methodology (SSADM) because it divides the system into phases. The system was developed using PHP Scripting Language as the server side language and MySQL as the Database for the system. With this system, users can access their files in the server securely and concurrently. Sharing file is also protected by access control. Security, user – friendly and cross platform are the main purpose of the new system.

Keywords: Distributed File Sharing, Access Control System,Security, confidentiality

1. INTRODUCTION

Since Information Technology (IT) is hosting their services, applications and data on cloud, it is growing fast regarding the privacy of a sensitive data being compromised. Before uploading and sharing data on cloud, level – managed access/security must be applied. Online sharing of files is practice of sharing of file to different users across the internet. Common file sharing form include File Transfer Protocol (FTP) model and peer –to – peer (P2P) file sharing network. File transfer protocol is used for exchanging files over any network that supports the TCP/IP protocol (such as the Internet or an intranet). Peer – to – Peer network is a type of network in which each workstation has equivalent capabilities and responsibilities.

With the emergence of cloud computing as one of the promising technologies that has shifted the computing model from traditional computing into the new era of cloud computing. Information and communication technology (ICT) has change the way organizations and individuals used to perform their daily work flow and business organization. Cloud storage systems have been the source of attraction for the online users so as to have easy access anytime and everywhere. Many online service providers have thieved to serve many organization and individual users as well as business people to have their data on cloud with a more reliability and security.

This paper is concerned with solving the problems of unauthorized access to shared file by users in distributed environment, lack of multi – level managed access control in accessing the share file and lack of control over the place where data needed to be stored in distributed environment. The objective of this paper is to develop a software system that will restrict

unauthorized access to data files on systems and to develop a multi – level managed security using authentication service.

2. LITERATURE REVIEW

Network file sharing is an area that has attracted a lot of attention given the need for information exchange(Clarke, 1999). The explosion in the growth of the Internet over the past several years, and the projections that the growth will continue at a similar pace, makes file sharing an even more important issue. There are however a number of problems in the already existing sharing mechanisms.

2.1 File Sharing

It is described as the 'practice of sharing or offering access to digital information or resources, including documents, multimedia (audio/video), graphics, computer programs, images and e-books. It is the private or public distribution of data or resources in a network with different levels of sharing privileges', Margaret (2009).

The most common technique for file storage, distribution and transmission includes: Removable storage device, centralized file sharing hosting server installations on network, World – Wide – Web oriented hyperlinked document and distributed peer-to- peer network

2.2 Methods of File Sharing

i. File Transfer Protocol (FTP): File Transfer Protocol (FTP) is a central computer called the *FTP server* holds all the files to be shared, while remote computers running *FTP client* software can log in to the server to obtain copies.

ii. Peer to Peer File Sharing (P2P): Peer-to-Peer (P2P) file sharing allows users to directly access download and edit files. It is also refers to as a network that allows computer software and hardware to function without the need for special server devices. (Maguire 2003).

iii. Electronic mail (Email): It is information stored on a computer that is exchanged between two users over telecommunications.

iv. Online Sharing Services: Numerous Web services built for personal and/or community file sharing exist on the Internet including well-known options like Box and Dropbox.

2.3 File Sharing Security

Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services(Yu et al., 2010). Information security is much more than just protecting digital information sharing, it means "protecting information and information systems from unauthorized access use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability" (Sattarova and Kim, 2007). Security is critical for enterprises and organizations of all sizes and in all industries.

2.4 Goal of Information Security

The goal of information security is divided into three(Krishnan et al., 2007):

i. Confidentiality: The confidentiality aspect refers to limiting the disclosure and access of information to only the people who are authorized and preventing those not authorized from accessing it.

ii. Integrity: Integrity aims at maintaining and assuring the accuracy, consistency of data and trustworthy manner over the period in which it will be existent.
iii. Availability: The concept of availability refers to the up time maintenance of all resources and hardware. This means that all the hardware and resources one have are functional all the time.

2.5 Types of Security

i. Communication Security: It is the discipline of preventing unauthorized interceptors from accessing telecommunication in an intelligible form, while still delivering content to the intended recipient.
ii. Perimeter Security: The perimeter security is concerned with protecting the data while it is being stored. This is to ensure the safeguarding of the approach ways to an organization facility.
iii. Insider Security: It is preventing unauthorized employee/contractor etc. to access organizational files. They can become a threat to the organization. It is concerned with preventing attacks performed inside the perimeter of the trusted internal network.

2.6 Access Control

Vincent et al; (2006), access control system is concerned with determining the allowed activities of legitimate users mediating every attempt by a user to access a resource in the system. Qing-hai and Yang (2011) indicate that access control is an important measure in providing protection for the system's resources; and it is considered the most important security mechanism in a computer system; and one of the most important measures to achieving confidentiality and integrity of data. The objectives of access control system are described in terms of protecting resources against inappropriate or undesired user access.

2.7 Access Control Component

i. **Identification**: Stewart et al. (2008) defined identification as the process by which a subject professes an identity and accountability is initiated. The identification process is established when a user provides a user-name, a log-on ID, a personal identification number (PIN), or smart card for the access control to be effective.
ii. **Authentication**: Identification requires authentication. Authentication involves validating a password linked to a username. Authentication is about providing a private piece of information that is known solely by a certain subject (Harris 2002).
iii. **Authorization:** Harris (2002) defined authorization as a process of assigning authenticated subjects access and the right to carry out specific operations, depending upon their preconfigured access rights and permissions outlined in access criteria.

3. PROPOSED SYSTEM

The proposed system is a web based system that uses Access level control based on security access grouping. The security access grouping is defined and classified based on level and function of a staff in the organization. The classification is as follow;

i. **Level 1 (Strategic Level):** They are the one that one that examine where the organization is now, decide where it is going and how it will get there.
ii. **Level 2 (Tactical Level):** They help middle manager allocate resources and establishing controls to implement the level 1 plans of the organization.
iii. **Level 3 (Operational Level):** This level carry out day – to – day activities in the

organization. They carry out the operating plan, procedures, schedule, policies specifications and cost developed by the level 1.

3.1 System Implementation

The system to achieve this objective was developed using PHP server side scripting language (Hypertext Preprocessor), HTML (HyperText Markup Language) and MySQL (Structured Query Language) database servers were used as they are already widely used by developer and as such have a lot of documentation online which will help the researcher easily find research material that will make it easy to implement and run the software application.

3.2 Methodology

The methodology used in this work is Object-Oriented Analysis and Design Methodology (OOADM). OOADM models the "real-world" requirements, independent of the implementation environment. The design applies object-oriented concepts to develop and communicate the architecture and details of how to meet requirements.

3.3 Architecture of The System

In figure 3.1, client requests a file/document from the server. The server then checks from the database whether the file is present or not, if the file is found then it is transferred from server to the client who requested the file. Clients can also upload, download and edit documents on the server. The file server manages the file operations and is shared by each client's PC attached to them and the client process/scan table, application program (user interface, database processing and generate queries), handle integrity and security, full DBMS.

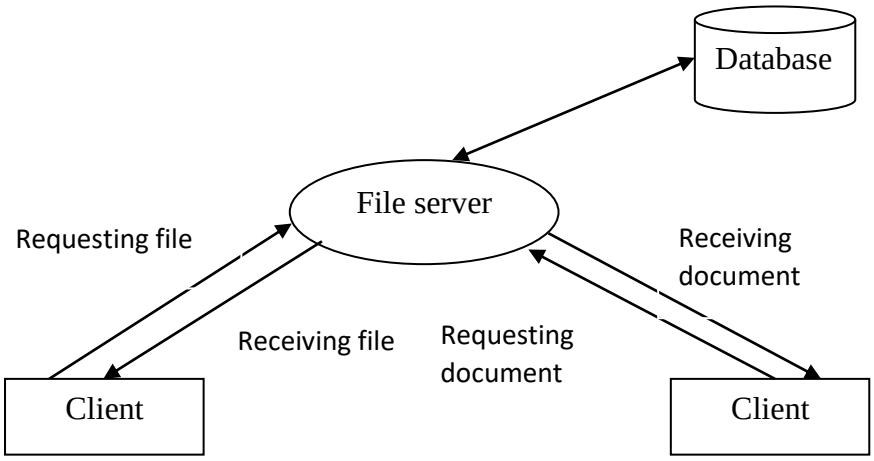

Figure 1: Architecture of the Proposed System

3.4 Sample Input Sample

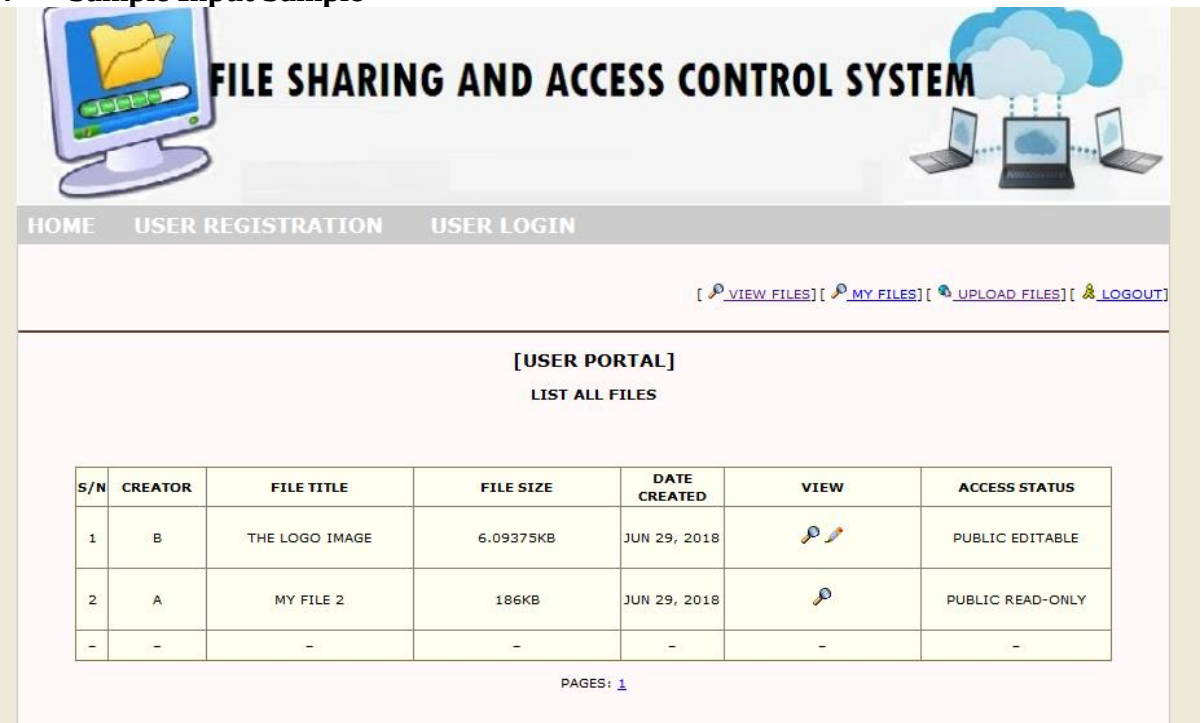

Figure 2: View All Files Module

3.5 Result

Enterprises have distributed offices and teams, which leads to scattered data and devices across the organization. A true enterprise file sharing system is capable of connecting millions of files with thousands of users, no matter what type of storage or access device. This paper focuses on development of distributed file sharing system in an enterprise where files can be easily access, upload, download and edit. The result shows.

4. DISCUSSION AND CONCLUSION

This research was aimed at improving on the current file distribution services by the design and implementation of a File Distribution System. One of the major contributions of this work is the implementation of security access grouping and classification based on level and function of a staff in the organization The principal target of the research was to create a file sharing service that is both efficient and easy to use, eliminating any unnecessary complicated process and focusing on the satisfaction of the users of the system.

REFERENCES

Clarke, I. (1999), A distributed decentralized information storage and retrieval system. unpublished dissertation, University of Edinburgh, 1999.

Harris, S. (2002). *Mike Meyers' Cissp(r) Certification Passport*. McGraw-Hill ProfMed/Tech, 2002.

Krishnan, Ramayya, Michael Smith, Zhulei Tang, and Rahul Telang (2007). "Digital Business Models for Peer-to-Peer Networks: Analysis and Economic Issue." Review of Network Economics 6, 194–213, 2007.

Maguire, James (2004). "Hitting P2P Users Where It Hurts." Wired, January 13, 2004. (www.wired.com/entertainment/music/news/2003/01/57112; accessed May 9, 2019.)

Margret Rouse (2009). The ultimate guide to cloud-based file sharing. whatis.com – TechTarget – whatis.com.

Qing-hai, B. and Ying, Z. (2011). Study on the access control model in informationsecurity. *IEEE*, pages 830–834.

Sattarova, F. Y. and Kim, T. (2007). IT Security Review: Privacy, Protection,Access Control, Assurance and System Security. *International Journal of Multimediaand Ubiquitous Engineering*, 2(2).

Stewart, J. M., Tittel, E., and Chapple, M. (2008). *CISSP: Certified InformationSystems Security Professional Study Guide*. SYBEX Inc., Alameda, CA, USA, 4th edition.

Vincent C.Hu, David F. Ferraiolo, Rick D. Kuhn (2006). "Assessment Of Access Control System. National Institute Of Standards And Technology, Gaithersburg

Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving secure, scalable and fine-grained data access control in cloud computing. In *INFOCOM, 2010 Proceedings IEEE* (pp. 1–9).