National Conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

Decentralized Access Control Using LDAP (Lightweight Directory Access Protocol)

Dr. Yuvaraju B.N [1], Parikshith K*[2]

[1]Professor, Computer Science & Engineering, The National Institute of Engineering (NIE), Mysuru, Karnataka, India

[2] Computer Science & Engineering, The National Institute of Engineering (NIE), Mysuru, Karnataka, India

ABSTRACT

Lightweight Directory Access Protocol (LDAP) provides the need of high level security through single sign-in and centralized user management at server with a facility of decentralized access control. LDAP protocol offers security services and integrated directory with an ability of storing user management information in a directory. Through which at the same time the user can determine which application and service to be accessed from server and also the user privileges. Here in this paper, we explain authentication mechanism for web server application by using LDAP method. We also show the result and performance analyses on the access speed in using LDAP method.

I. INTRODUCTION

Advance of Internet technology has brought about very positive impact in all sectors. One of which is web-based application, which is required by government institutions, private sectors and education sectors. In line with the trend of using web applications on business activity, and security level, user's identification requirement became main concerns. Client server applications on web server has been started to be used widely and growing fast.

Data confidentiality of client is more important in any sector of work, where in user authentication became more and more important. Access to web applications which is connected to LAN or single host will attract other parties who have no access to the network and application. Therefore, mechanism to identify user who have privilege to access the application is needed. This is to be added by providing the username and password for login process, so only right user can access the application which is in the network. It is also known as the user authentication, which is done with the help of lightweight directory access protocol (LDAP).

Authentication process for web-based application is needed, in order to enable this each member to register or they need to be added. The objective of this process is to store user information and to collect information for database server. Usually, each web server applications have their own database table of login credentials. This matter became a must if the web application needs a login process for accessing the application pages.

However, in the modern era number of web server application is growing, each application will need to authenticate user or member. Therefore the user will have a lot of username and password to remember, this will complicate the user to remember all of it. For the simplification purpose, the authentication method for user by using Lightweight Directory Access Protocol (LDAP) was introduced in 1993 [1].

This method accommodates the need of high level of security, single sign-on, and centralized user management which offers services of security and integrated directory especially with ability of storing and managing user information in a directory.

With this authentication method by using LDAP, each web-based application can be united using single identification of user information stored in the directory of LDAP server. The user can accessed every application easily without having to remember more than one username or password as well as privilege to users according to the existing information on the LDAP server.

II. HISTORY OF LDAP

International Telecommunication Union (ITU) and International Organization for Standardization (ISO) in year 1990 released a standard for directory service called X-500. The main feature for X-500 is to build a global distributed system which offers an access to information comprehensively to the directory. X-500 defines Directory Access Protocol (DAP) used by client to access the directory. The implementation of X-500 as service protocol was too heavy for desktop at that time. In the year 1993, Michgan University with the help of ISODE Consorsium designed and built a protocol which can work on TCP/IP. The result is **Lightweight Directory Access Protocol (LDAP).**

LDAP is a client-server protocol which works on TCP/IP to access and manage data on the directory. This method accommodates the need for high level of security, single sign-on, and centralized user management which offer service of security and integrated directory especially with the capability to store and manage user information in a directory. Here at the same time the user can determine application, service and server which need to be accessed, and the privilege of that user.

III. LDAP DIRECTORY ADVANTAGE

There are many advantages for directory service, such as [2]:

- Make network administration easier: Central management of people information
- Central management of computer and machine configuration Central management of user accounts
- Reduced support costs from centralized management
- Unify access to network resources: Uniform naming convention; Potential for single login to network resources
- Provide single destination for users to search for information: Contact information
- Central location of network resources
- Help streamline business processes
- Provide repository and look up for application and service data

Compare with standard database, LDAP directory has some advantages, such as flexibility, scalability, heterogeneity, replication facility, distributed data management support, query optimization, and maintainability.

IV. SYSTEM ARCHITECTURE DESIGN

Design of system architecture includes client computer and server. In designing, web application is store in server and LDAP server directory, which store user account information with relevant attributes. Client computer is connected with servers. The authentication mechanism that is located at web login form determines what credential is being used by user. This can be LDAP credential or database web server credential. Figure below illustrates the system architecture Client can use computer with different operating system or specification such as Windows, UNIX, or Linux. **Secure Socket Layer (SSL)** protocol is a protocol which describes how a client-server based application can work over a secure channel and also can be processed quickly.

Security protocol such as SSL offers a facility to encrypt data, server authentication, message integrity and also choice for client authentication over TCP/IP connection on transport layer. Application layer protocol usually works over SSL/other which include HTTPS or even Lightweight Directory Access Protocol (LDAP).

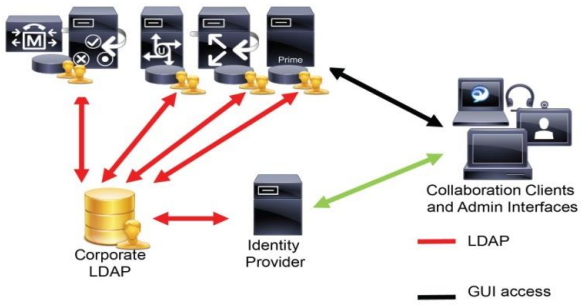

Figure 1. System Architecture Design

The client-server authentication implementation of LDAP uses three basic components, which are hardware, software and programming code. The LDAP client computer with standard specification and any operating system (windows, unix, linux). The web based application and all computers should be connected to the internet via Network Interface Card (NIC) as communication interface between client and server.

V. AUTHENTICATION & AUTHORIZATION MECHANISM

Networked applications and web server application frequently use LDAP to support authentication. In the simplest form, they present the username and password supplied by the user in an LDAP Bind operation. If the Bind succeeds, this proves that the password is correct.To access the LDAP service, the client must first authenticate them self to access service. It must tell the LDAP server who is going to access the data so that the server can decide what can be seen and done by the client. If the client authentication is successfully to the LDAP server, then the server will check the authority of the client for the request. This process is called access control.

There are mainly three kind of authentication process using LDAP method.

- ***Anonymous***

A client that sends a LDAP request without doing a "bind" is treated as an anonymous client. That client can view the directory and is treated like a guest who is unable to modify data in the server.

- **Simple Authentication**

This authentication mechanism consists of sending the LDAP server the fully qualified Domain Name of the client (user) and the client's clear-text password. This mechanism has security problems because the password can be read from the network.

- ***Simple Authentication and Security Layer (SASL)***

To avoid exposing the password we can implement this way, you can use the simple authentication mechanism within an encrypted channel (such as SSL), provided that this is supported by the LDAP server. Simple Authentication and Security Layer (SASL) specifies a challenge-response protocol in which data is exchanged between the client and the server for the purposes of authentication and establishment of a security layer on which they carry out subsequent communication. By using SASL, LDAP can support any type of authentication agreed upon by the LDAP client and server.

LDAP server can also authenticate users from other services (ie: Send mail, Login, Ftp, etc.). This is accomplished by migrating specific user information to LDAP server and using a mechanism called Pluggable Authentication Module (PAM).

Authorization can be more complex. This is the job of working out what the user is permitted to do once they proved their identity. Most applications define a set of roles, each with permission to do certain things, and assign users to some roles. This can be represented using multi-valued attributes in the LDAP directory.

In web application, several access levels will be implemented for read-only access to public data, read-only access to data in certain defined categories. Author access to create new content, editor access to modify content created by author, and for manager to set access permissions for others and all.

VI. PERFORMANCE ANALYSES OF AUTHENTICATION MECHANISM USING LDAP

This part of the paper will describe and analyze the performance LDAP authentication method [3]. We tested using different user ID and different distance between the client's computers to the server device. The data collection has been done as follows:

Performance evaluation tools (Ethereal) view Ethereal is used to measure the performance of the system in which the traffic is analyzed on both sending and receiving direction. The information obtained consists of time between first packets an last packet, average packet size, average packets/sec, average Mbit/sec. The following are several graphics which show the performance of the authentication system using LDAP method based on varying the user ID and distance of the user from the server.

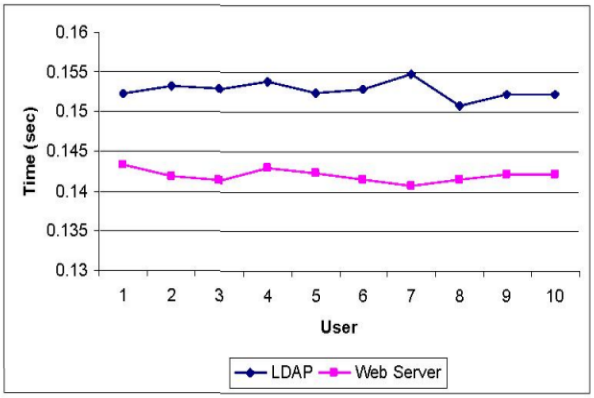

Figure 2. The average speed of access with LDAP and web server authentication

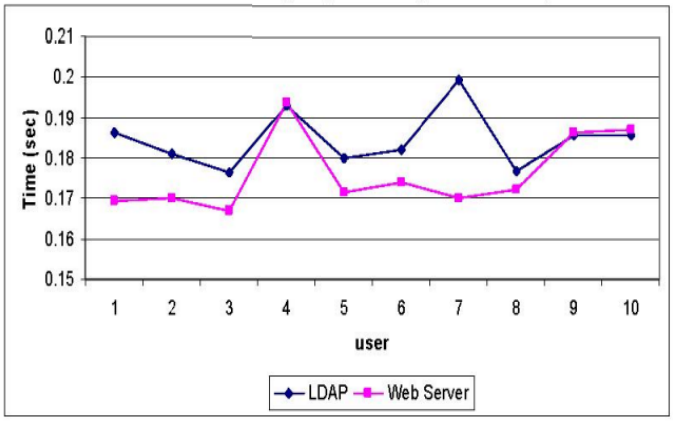

Figure 3. The time between first packet and the last packet with LDAP and web server authentication

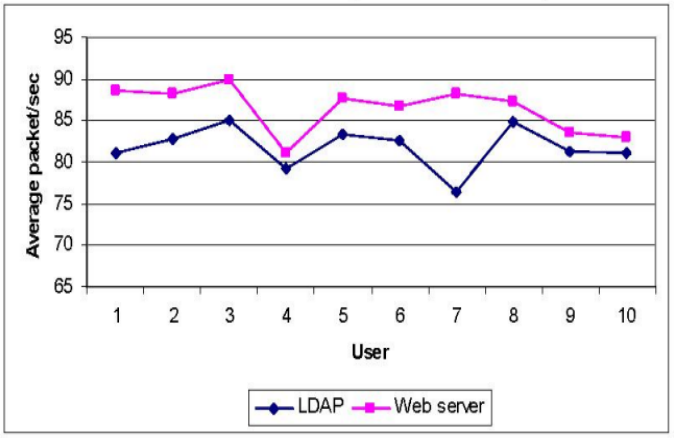

Figure 4. The average packet/sec with LDAP and web server authentication

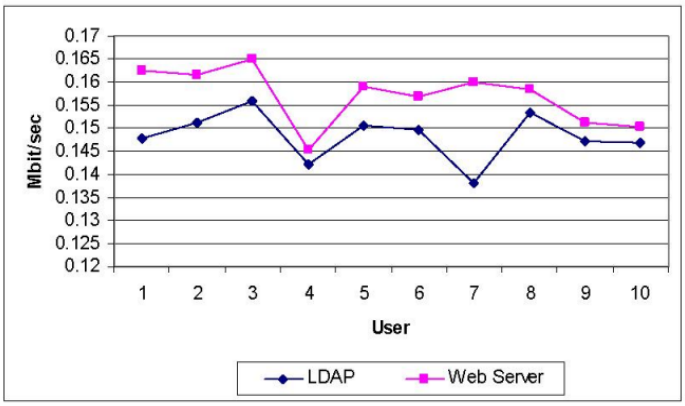

Figure 5. The network throughput with LDAP and web server authentication

The distance factor does not affect much the access speed when **decentralized** access method is used. The access speed is more affected by factor of real traffic condition on the network, such as the average packet/sec that is transmitted and also how much bandwidth can be used on the transmission process (network throughput).

VII. CONCLUSION

LDAP authentication method supports the single sign-in mechanism. This will allow many web server applications to be authenticated using the same credential of the user on a centralized LDAP server directory. Access speed is inversely related with the access time required, although the access time is inversely related with the average packet/sec and throughput value on the network. The performance of the LDAP authentication mechanism is based on the variation of different user or different location.

VIII. REFERENCES

1. Heinz Johner., Larry Brown., Franz- Stefan Hinner., Wolfgang Reis., Johan Westman., "Understanding LDAP", IBM Corporation, June 1998.
2. Hodges, J., "Introduction to Directories and LDAP", http://www.stanford.edu/-hodges/talks/mactivity.ldap.97/index2. html, accessed on April 2006.
3. Riri Fitri Sari, Syarif Hidayat (2006), Integrating Web Server Applications with LDAP Authentication: Case Study on Human Resources Information System of Ul