

<http://ansinet.com/itj>

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSI*net*

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

A Scheme for the Identity Authentication of College Social Network Management

¹Xu Dawei, ²Wen Hui, ²Nie Peiyao, ²Sun Mei and ²Dong Zhiguo

¹School of Computer Science and Technology, Shandong University of Finance and Economics,
Shandong Provincial Key Laboratory of Digital Media Technology, Jinan, Shandong, 250014, China

²School of public Management, Shandong University of Finance and Economics, Jinan,
Shandong, 50014, China

Abstract: Network management is the necessary means to ensure that large-scale heterogeneous network running smoothly, the core idea of College social network management based LDAP is to use LDAP to store and access the network management data and implement the user authentication system who based the core of directory and conduct unified identity authentication on campus, to improve the ability of network management, to improve the application efficiency of the digital campus greatly.

Key words: LDAP, network management, information model, college social network

INTRODUCTION

The way of modern life gradually incline to the Internet, social Networking Services which as a new thing, has changed people's habit of connecting with each other and becoming a convenient way to establish and maintain social relationship and get especially the favour of contemporary college students. World has be changed by social networking, the campus users have also been changed by social networking. With the constant improvement of the university year after year and the broaden of online users and the increase of depth of participation it is imperative to create a campus social networking system to meet network users (Chen, 2010; Xiong, 2006).

ZhongWei has referred to build campus network system which adopts the distributed technology in the context of "Design of campus social contact network". The system should be based on personal real information, based on social network, based campus network as a platform, realize campus specific application. With the traditional public social networking services (such as renren, weibo, etc.) than reflects the following characteristics: (1) Real name: Campus network is relatively close to the real-name system, online identity is consistent, the introduction of the unified identity authentication make the every campus user has a unique status in the network. (2) Extensibility: With the existing campus applications such as mail system, certification system closely integrated, realize data integration and sharing information. (3) practical. (4) Security: Campus

network follow strict certification system for each specific application permissions for the proper, efficient and flexible system, different users have different basic permissions, according to actual circumstances at the same time, establish additional permissions and temporary permissions system. Through multi-level access authentication mechanism, protect the safety of key data fully. (5) interactivity: Everyone involved (Zhong *et al.*, 2012; Yuan and Zhang, 2007).

Campus social network can be considered in a foundation platform of informationization application for online campus, based on the above series of child application and we focused on identity authentication in the network management (Peng and Mao, 2004).

Due to the different requirements of each system, different characteristics, using the applications and information systems of colleges and universities become complex and diverse. Development language of various system applications, system architecture, data storage, management methods are vary. The data storage of user information are different which makes it very difficult to share user data between different systems.

Due to the rapid development of microelectronics technology and LSI technology, the storage capacity is not the "bottleneck" of the data storage but the new "bottleneck" is transferred to the method of data storage, data storage can be divided into three, namely: Independent files, the relational database and specialized storage. Independent files are mainly used in small programs scattered field, simple operation but the data storage performance is low; relational database approach

play a major role in very large network information processing systems with the requirements of reliability and integrality but its fine performance is the expense of a lot of system resources, the model of large-scale relational database is based on the same principle; specialized data storage is used in specific application areas it is can be flexible based on the actual storage requirements and specific storage, LDAP is a typical representative which is widely applied in the Internet.

LDAP is Lightweight Directory Access Protocol, based on the x.500 agreement but simplify a lot and can be customized according to demand. It uses a tree-structured organization, implements the storage of the data structure specified. It is a standard cross-platform protocol which can be applied to a variety of system platforms and has become an important network management tools and methods gradually. LDAP and relational database is the concept of two different levels, the latter solves the storage mode while the former is the storage mode and the access protocol. LDAP is the same level of the query language SQL of relational database, is a more abstract concept. LDAP is fit for the information storage as the data reading require from multiple places and these data do not need to be updated frequently. It is often used to store the information of user account and address list and so on.

LDAP: LDAP (Lightweight Directory Access Protocol), different with X.500, LDAP can support TCP/IP protocol which is obligatory application on the Internet. It is composed of four basic model which describes the directory storage, access control and operation processing of the directory data completely (Comer and Stevens, 1998).

Information model: The basic unit of information stored in the directory is the directory entry (entry). Each directory entry contains a set of attributes used to store certificate information, each attribute has a type and one or more values □□, the values □□ of the attribute value depends on the attribute type. Each attribute, an attribute grammar, is used to determine the type of the attribute values □□ and the characteristics of attribute values □□ during the directory operation.

The LDAP standard specification defines a large number of objects, as well as attribute type, who are divided into different modes according with certain standards and principles. User can customize their own models to adapt to the description and storage of specific data, the fundamental task of mode customizing is to define new objects and attributes for entries to be able to use the content outsided of the system.

Naming model: The LDAP naming model is used for the definition of how directory is to identify and organize. The directory entries are organized into a tree structure which is called the directory information tree. Directory entry is organized on their Distinguished Name (DN) in the directory information tree, the distinguished name of a directory entry is accurately identified and unique. The DN of an LDAP entry is composed of two parts, the RDN and record the location of LDAP directory. DN is a group of ordered sequence of the relative distinguished name of directory entry through which from the root of the information tree, untill to the directory.

LDAP directory store data by tree hierarchy. The DN of the LDAP directory record is used to read a single record and back to the top of the tree. As the primary key of directory entry in the catalog, DN which is an ordered set of RDN sequence, the user can arbitrarily access any entry in the tree with the DN.

Functional model: The LDAP functional model is a subset of the functional model of X.500. LDAP supports the following operations: "search", "add", "delete", "modify", "modify RDN", "bind", "unbind", "abandon" operation. "Search" operation contains the parameters of the basic object, scope and filter. The basic object and scope is used to determine which part of the query tree to query, the filter is used to point out the directory entry that meet the query in the selected range. Query time and the size limit of the number of queries of LDAP are directly included in the query request, query results are returned to the client once.

LDAP use three operating of "add value", "delete value" "instead of value" to simplify the "modify" operation. When a attribute value which is nonexistent is added, the operation automatically creates this attribute. When the last value of an attribute will to be deleted by the request, then the entire attribute will be deleted automatically. The operation "bind" is a subset of operation function "bind" of the X.500 which allows only simple authentication methods, such as passwords. The operations of "unbind", "abandon", "modify RDN", "add", "delete" are the same to other LDAP operations.

Security model: Security problem is crucial in the network it is no exception in the directory service. According to different application needs, the LDAP server's authentication mechanism is divided into three types: No authentication, basic authentication and SASL (Simple Authentication and Security Layer) authentication. LDAP allows you to use the ACI (generally known as the ACL or Access Control List) to control the permissions of read and write on the data by need. ACI can control the access

of data based on who has access to data, what data has access to, where the data exists as well as other. These are completed by the LDAP directory server, so the client application do not worry whether or not to carry out safety inspection on.

Compare of traditional databas: A major development goals of the university network management system is to strengthen the mutual openness, not only customers program (with full privileges) be allowed access any data in any network management system but also data switching can be completed flexibility directly between network management system according to the need. It is easily to achieve these goals by the technology of LDAP data access and directory storage.

In addition to network management based on LDAP compensate for the deficiencies of the storage method of the traditional database it can play a greater role in the Internet environment by the following advantages.

Control of access rights based entry: This control is access rights of customers based on the smallest unit of data storage it can greatly improve the security level of the system.

LDAP encryption transfer of information: An effective means to prevent unauthorized users tapping information. Support multi-valued attributes: Allows certain attribute of the entry take multiple values at the same time which

not only facilitate the query of the entry but also can reduce the storage of redundant entries (Mitchell *et al.*, 1997).

Framework of social network management based on LDAP: The social network management based LDAP is mainly achieve a user authentication system with the core of directory which support traditional network management protocol based on the integration of the LDAP. when users need to access applications, user name and password are submitted to the directory service system. It is compared with the data of directory database to determine the user's identity. As the architecture framework of the system shown in Fig. 1.

The major performance improvements of the management structure based LDAP directory technology are:

- The storage strategy combining with relational database storage can meet a variety of requirements of data storage. Data is in high frequency changes you can use traditional database to store and relatively static data you can use the LDAP directory to store

Support different customer access. Local customers access to the application scheduler through the GUI interface and to be provided the required data by the latter; network customers access to the LDAP directory

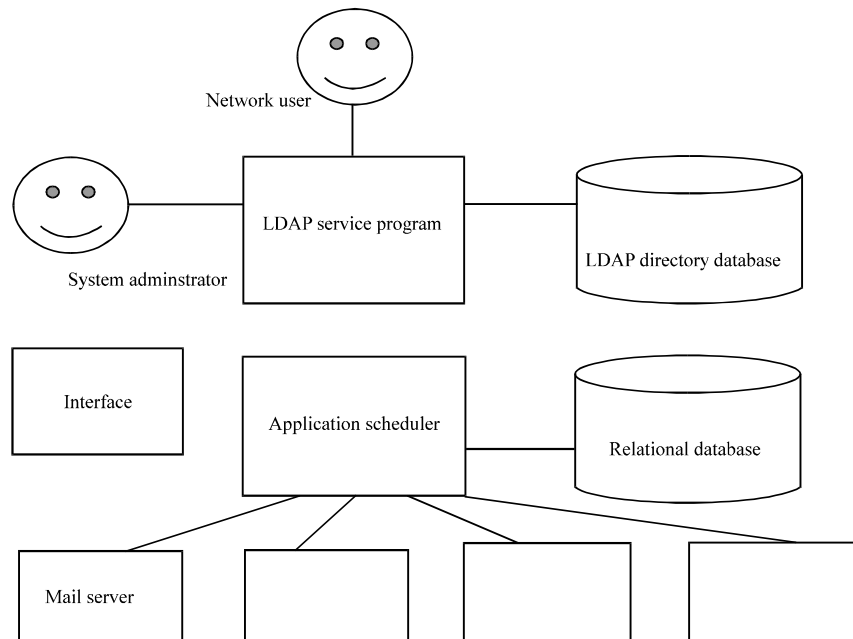


Fig. 1: Network management framework based LDAP

data directly by standard LDAP protocol it does not require of the participation of the application scheduler, so as to reduce the processing burden of the network management system.

Increase the data reliability. The core data can be stored in LDAP directories and relational databases in different formats, A single storage system failure will not result in the paralysis of network management system.

Access performance of LDAP directory data is good. The system can store the LDAP directory data in different physical host easily in order to achieve the purpose of load sharing which improves data access performance.

Security. Database and LDAP directory, the library has its own safety control mechanisms to protect the data stored, especially the access control and encrypted transmission based on LDAP entries which makes data security can be guaranteed in the open Internet environment.

Building the LDAP information model: The LDAP information model is a prerequisite to determine data storage of network management its construction involves two steps:

- Create an LDAP directory tree. Each legitimate user corresponds to a node in the LDAP directory information tree it is decided that the attribute of the node and the Organizing nodes into a directory information tree. Determine each node what attribute should have which is the objectives and key of the design of directory

Expression of entry information. LDAP server provides a series of standard object definitions and data attributes definitions but they do not fully meet the needs of the user management; the objects and attributes are customized for the specific requirements of management which has become an essential task to properly express the directory information.

According to the characteristics of the LDAP, combining with the situation of school, user information contains unit, name, number, user name, password is stored by LDAP in the design of the system. we need to organize and classify the data according to those types of information. There are two main problems in the design of organizational structure:

- Different administrative departments, different units, different departments in school, each department includes personnel with administrative privileges, then build an administrators group in each department or build a group of the administrator

alone to manage them centralized and then assign the personnel to the appropriate unit

- From the basic system structure, each faculty has a different category of persons (such as teacher, undergraduate, graduate, etc.), then build the group according to the category of persons first, then assign the personnel to departments; or group according to department first, then build each their own group in accordance with the category of persons

This is the problem of the attributes of the account, type design and group design. During the design of the account attributes, the primary consideration should be to meet the general management and maintenance functions and then consider the question of the property classification. The classification of the account can be defined based on the identity of school personnel, such as the teacher, student and network student and so on the ways of classification to be organized. This classification allows management of daily work and system management to be consistent, easy to use and different types of users can be provided for different front-end applications. Accounts are stored in different containers of staff (OU) based on account type.

In order to solve the problem of cross-licensing of different types, you can introduce the concept of the group. The use of the group can be more flexible than the management in accordance with the user types. A variety of groups can be defined in accordance with the application needs, the authorization of the application modules should be divided more detailed and this group of authorized users is the mixing of many types of users, different types of users can be in the same group according to the permissions. Group is stored by the way of "group" in an LDAP design. the LDAP directory structure of the storage of system account information as shown in Fig 2.

The root of the directory information tree is a virtual root and has no real meaning, any node in the tree is an entry of directory information tree. root node following the establishment of staff container (OU), users are all stored in the container of personnel which can attain management and maintenance more flexible and efficient. Staff container is classified and organized in accordance with the user type earlier designed (Fig.2). The system uses the category attribute of persons to describe the relationship between staff and organizations it is easy to carry out a variety of management operations to the user. It is to use the attribute to save the subsidiary information of the user and user information itself is not dependent on their organizational structure (unit), operation of

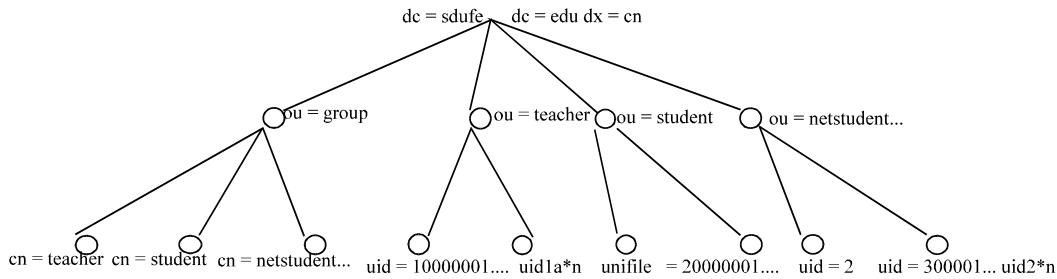


Fig. 2: Directory tree of the LDAP

organizational structure is very simple for unit adjustment of personnel. Storage of the group structure can be used this way: all groups have been established in the group container of the root directory, side by side with the staff container. Basic groups fixed is created in accordance with the personnel classification, name is consistent with personnel classification. Using Group can be very convenient for structural expansion, can add a new grouping in the case of increase of the category of personnel.

The system uses LDAP structure to store the account information and authentication information services. Account information of teacher is decided by the unified account establish by personnel system, account information of graduate student is decided by graduate student account system, the account information of the junior college students is decided by school system and the account information of online education student information is decided by the Networking Academy system. These four different data sources is called the basic information table together. LDAP use the way of data synchronized to attain account information, use the way of differences in the view to update the account information.

CONCLUSION

With the continuous development of the campus network, the progress and expansion of the application scope, more application server and more users are provide a unified directory service it is the more significant manifestation of this superiority of the directory service which is convenient to the user but also greatly reduces the difficulty of network management and improves the efficiency of information management. The Core idea of the social network management based LDAP is using LDAP technology to store and access the network management data which improve the quality of the network in terms of reliability, access speed, openness, cross-platform greatly which provide a strong technical support for modern network management going to a comprehensive open.

ACKNOWLEDGMENTS

This work was supported by MOE Project of Humanities and Social Sciences (Project No.10YJC880076, 12JD710120, 13JDSZ2084). This work was supported by the access of the Beijing Institute of Technology which supported by Shandong Provincial Department of Education, and this work was supported in part by Shandong Provincial Natural Science Foundation (ZR2011FL027), National Natural Science Foundation (61101162\61101085\60873041\61272091), Program of Integrating Informatization and Industrialization of Shandong Province (2012EIO20/ 2012EIO25) and Program for Scientific Research Innovation Team in Colleges and Universities of Shandong Province.

REFERENCES

Chen, Y., 2010. The campus SNS website construction and the future development of our country. Henan University Library, Zhengzhou, China.

Comer, D.E. and D.L. Stevens, 1998. Internetworking with TCP/IP ANSI C Version: Design Implementation and Internals. 3rd Edn., Prentice Hall, USA., ISBN: 9780139738432, Pages: 660.

Mitchell, J.C., V. Shmatikov and U. Stern, 1997. Finite-state analysis of SSL3.0. Computer Science Department Stanford University. [http:// www.cs.utexas.edu/~shmat/shmat_usenix98.pdf](http://www.cs.utexas.edu/~shmat/shmat_usenix98.pdf)

Peng, X.C. and X.D. Mao, 2004. Social network analysis of BBS group characteristics. Youth Res., 4: 39-44.

Xiong, X.Q., 2006. SNS: Reality return of network interpersonal communications. News Spread, 9: 23-25.

Yuan, L.Y. and R. Zhang, 2007. Real image of virtual network world-meaning analysis of the spread of campus SNS. Modern Commun. (J. Commun. Univ. China), 4: 152-153.

Zhong, W., Q.H. Yang and C.H.Q. Dai, 2012. Design of campus social contact network. J. Wuhan Univ., 12: 302-304.