ENHANCEMENT OF LOGIN PROCESS MULTI-SERVER CONMMNICATION FOR MULTIMEDIA CONFERENCING SYSTEM (MCS) USING DISTRIBUTED LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

MOHAMMAD ABDELMO'TI ABU SALEH

UNIVERSITI SAINS MALAYSIA

2010

ENHANCEMENT OF LOGIN PROCESS MULTI-SERVER CONMMNICATION FOR MULTIMEDIA CONFERENCING SYSTEM (MCS) USING DISTRIBUTED LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

By

MOHAMMAD ABDELMO'TI ABU SALEH

Thesis submitted in fulfillment of the requirements for the degree of Master of Science

May 2010

DECLARATION

Name: MOHAMMAD ABDELMO'TI ABU SALEH

Matric No: PCOM0060/08

Faculty: SCHOOL OF COMPUTER SCIENCE

Thesis Title: ENHANCEMENT OF LOGIN PROCESS MULTI-SERVER CONMMNICATION FOR MULTIMEDIA CONFERENCING SYSTEM (MCS) USING DISTRIBUTED LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

I hereby declare that this thesis that I have submitted to School of Computer Science on 31/5/ 2010 is my own work. I have stated all references used for the completion of my thesis.

I agree to prepare electronic copies of the said thesis to the external examiner or internal examiner for the determination of amount of words used or to check on plagiarism should a request be made.

I make this declaration with the believe that what is stated in this declaration is true and the thesis as forwarded is free from plagiarism as provided under Rule 6 of the Universities and University Colleges (Amendment) Act 2008, Universiti Sains Malaysia (USM) Rules (Student Discipline) 1999.

I conscientiously believe and agree that the University can take disciplinary actions against me under Rule 48 of the Act should my thesis be found to be the work or ideas of other persons.

Student Signature: Date:

Acknowledgement of receipt by: Date:

ACKNOWLEDGMENT

I would like to take this chance to express my highest gratitude to all my family members for their spiritual support. Also, I would like to thank my friends and colleagues who have continuously encouraged me to pursue my studies.

Special thanks and gratitude's would go to my supervisor, Dr.Omar Amer Abouabdalla, the one who made me feel that science and creativity have neither borders nor limits.

My lovely university, Universiti Sains Malaysia (USM) has taken a place in my heart for the rest of my life. I guess that is because anyone who enters this university would leave it with tears. It makes you a different character, a person who loves science and a researcher who ought to create marvelous ideas that might help humanity to develop as much as it can.

Mohammad Abdelmo'ti Abu Saleh

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACL	Access Control List
AEID	Ancestor Entry Identifier
API	Application Programming Interface
CA	Certification Authority
CN	Common Name
DAP	Directory Access Protocol
DC	Document Conferencing
DEID	Descent Entry Identifier
DES	Data Encryption Standard
DIT	Director Information Tree
DN	Distinguished Name
DNS	Domain Name System
DSML	Directory Service Markup Language
EID	Entry Identifier
IDEA	International Data Encryption Algorithm
IETF	Internet Engineering Task Force
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
LDAP	Lightweight Directory Access Protocol
LDBP	Lightweight Directory Browsing Protocol
LDIF	LDAP Data Interchange Format
MCS	Multimedia Conferencing System
MD5	Message-Digest Algorithm 5

OIS	Open Systems Interconnection
PEID	Parent Entry Identifier
RC4	Rivest Cipher 4
RDB	Relational Database
RDN	Relative Distinguished Names
RFC	Request for Comment
RSW	Real Time Switch
SASL	Simple Authentication and Security Layer
SIP	Session Initiation Protocol
SLP	Service Location Protocol
SN	Surname
SSL	Secure Sockets Layer
SPML	Service Provisioning Markup Language
TCP/IP	Transmission Control Protocol/ Internet Protocol
UAC	User Agent Client
WAN	Wide Area Network
XED	XML Enabled Directory
XML	Extensible Markup Language

PENIGKATAN PROSES MENGELOG MASUK KOMUNIKASI PELBAGAI PELAYAN BAGI SISTEM SIDANG MULTIMEDIA (MCS) MENGGUNAKAN PROTOKOL CAPAIAN DIREKTORI RINGAN TERAGIH (LDAP)

ABSTRAK

Perkembangan pesat serta penyebaran yang meluas sistem sidang video dalam pelbagai bidang pengkomputeran adalah kerana keberkesanannya mewujudkan komunikasi dalam kalangan warga dunia dari serata pelusuk tempat. Satu daripada sistem ini yang begitu meluas digunakan di Malaysia ialah Sistem Sidang Multimedia (Multimedia Conferencing System, MCS). Dalam kes biasa, pengguna MCS perlu tahu alamat pelayan serta mempunyai akaun untuk mengelog masuk serta menggunakan sistem. Sekiranya pelayan tersebut rosak atau berada dalam keadaan luar-talian, pengguna perlu mempunyai suatu akaun lain bagi membolehkan mereka mengelog masuk pelayan yang lain. Tambahan pula, maklumat pengguna MCS (termasuk nama dan kata laluan) tidak begitu selamat kerana ia disimpan sebagai teks di dalam pelayan MCS. Oleh itu, kami mencadangkan suatu entiti baru yang ditambah pada sistem MCS, iaitu pelayan dan direktori LDAP. Melalui penggunaan pelayan LDAP terpusat bagi pelbagai pelayan MCS serta mengolah semula pelayan MCS untuk membolehkan komunikasi dengan LDAP, akan memudahkan pengguna mengelog masuk daripada mana-mana pelayan. di samping itu, pangkalan data pengguna yang tersimpan dalam pelayan LDAP dapat dicapai dengan selamat daripada mana-mana pelayan MCS lain. LDAP menyediakan lebih daripada keautentikan kepada pengguna. Pelayan MCS rekaan baru ini mampu mempercepatkan inivitasi dalam kalangan pengguna, yang membolehkan mereka

berhubungan satu dengan lain berdasarkan penggunaan kueri LDAP dan pelayan LDAP teragih untuk agihan beban di antara pelbagai pelayan LDAP. Pendekatan yang kami utarakan menunjukkan bahawa masa yang diperlukan untuk proses inivitasi adalah lebih cepat berbanding dengan sistem lama. Dapatan ini diperoleh hasil daripada tiga ujian yang dijalankan dalam tiga senario yang berbeza. Bagi ujian pertama, dapatan menunjukkan bahawa kelajuan adalah 17% lebih cepat apabila menggunakan MCS dengan Satu-LDAP daripada menggunakan MCS yang sama dengan pemantul. Bagi ujian kedua, dapatan menunjukkan bahawa kelajuan adalah 25% lebih cepat apabila menggunakan MCS dengan Dua-LDAP daripada menggunakan MCS yang sama dengan pemantul. Bagi ujian ketiga pula, dapatan menunjukkan bahawa kelajuan adalah 33% lebih cepat apabila menggunakan MCS dengan Tiga-LDAP daripada menggunakan MCS yang sama dengan pemantul. Di samping itu, sistem ini juga mampu memberikan langkah keselamatan tertentu, contohnya dalam risiko pemusatan dan keautentikan “mengelog masuk” bagi MCS. Dapatan kajian menunjukkan bahawa, langkah keselamatan baru ini mampu memberikan capaian “mengelog masuk” MCS sehingga 75% berbanding dengan sistem yang sedia ada.

ENHANCEMENT OF LOGIN PROCESS MULTI-SERVER CONMMNICATION FOR MULTIMEDIA CONFERENCING SYSTEM (MCS) USING DISTRIBUTED LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

ABSTRACT

Video conferencing systems are rapidly growing and spreading through various computing areas due to their benefits in efficiently producing communication between people from just about many different locations all over the world. One of the systems that is widely being used in Malaysia is the Multimedia Conferencing System (MCS). In ordinary cases, MCS users need to know the address of the server they have account on to be able to login and use the system. If that particular server is down or off-line users need to have a different account on a different MCS server to be able to use the system. Moreover, MCS user's information (including user name and password) is not secured since it is saved as text in the MCS server. Consequently, we propose a new entity to be added in the MCS system, which is the LDAP server and directory. By using the centralized LDAP server for multiple MCS servers and redesigning the MCS server to communicate with LDAP, users can easily login through any server since their database will be located at the LDAP server and can securely be accessed from any other connected user of the MCS servers. LDAP does more than just providing authentications to users. On the other hand, the new MCS server design speeds up the invitations among users where they can discover each other faster based on the usage of the LDAP query and the use of distributed LDAP servers to distribute the load between Multiple LDAP servers. As a

result, our approach proved that the time taken for the invitation process was less than that time taken through the old system. In short, the results consist of three tests where each test involves three scenarios. In the first test, the results showed that the speed was 17% faster when using MCS with One-LDAP instead of using the same MCS with the reflector. In the second test, the results showed that the speed was 25% faster when using MCS with Two-LDAP instead of using the same MCS with the reflector. In the third tests, the results showed that the speed was 33% faster when using MCS with Three-LDAP instead of using the same MCS with the reflector. Moreover, the proposed system supported some security measurements in term of centralization risk and authentication of “log in” for MCS. The results showed that, the new security measurement supported a secured “log in” access for MCS in a 75% more than the support of the previous security measurement.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Recently, Multimedia Conferencing Systems (MCS) that is emerged at Universiti Sains Malaysia (USM) have become more popular as they are conducted through many suitable applications that require gathering distant people to make them virtually meet inside a virtual conference room/hall. Once people are connected together through these systems, they may visually interact with each other using video signals to carry their image animated data. This depends on the use of a webcam from a side and the screen from another side and vice-versa. People may also vocally interact with each other by using microphones that carry voice and sounds signals from one user of a speaker system to other user and vice-versa. People may further interact by exchanging documents between each other. All the above mentioned methods of communication can be combined with an online text exchange service, also known as chatting, therefore, many input units, including keyboards, mice, microphones and webcams will receive input from different users to broadcast the processed information into different users' output units, including screens, speakers and printers. Figure 1.1 illustrates different types of data with their input and output devices as the most basic idea of Multimedia Conferencing Systems.

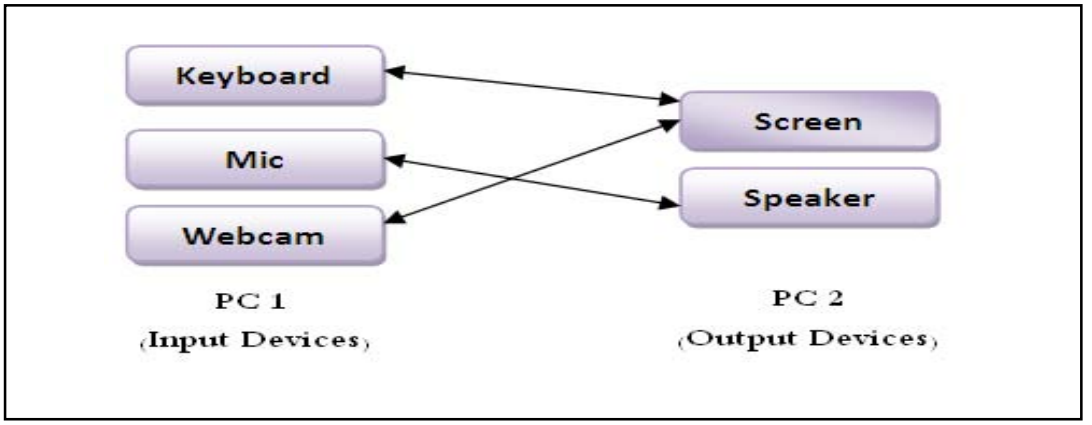


Figure 1.1: Basic idea of conferencing system

Multimedia Conferencing Systems (or MCS) are a revolutionary system that overcomes the obstacles of gathering distant people into one virtual room or hall for conferencing (Ramadass, S. and Abouabdalla, O., 1999). Another additional benefit of MCS is that it connects as many people as it can to communicate with each other, especially distant people. The MCS systems may connect people throughout the internet rather than the LAN/intranet (Garcia *et al*., 2001). In MCS, only authorized users are allowed to join the conference, this is called "Authentication". Currently there is no proper authentication in MCS. Nevertheless, this thesis has established a new idea, which involves leaving authentication process to separate entity and redesign the MCS server to be able to communicate with the new entity.

After doing research on authentication methods and systems, we found out that LDAP (Lightweight Directory Access Protocol) server is the appropriate solution to be used as the authentication entity. LDAP is considered to be as a set of directory services that provides a protocol and a data model for naming and authentication (http://en.wikipedia.org/wiki/Ldap, 2009).

LDAP technology provides centralized point of authentication and provides built-in functionalities for security related issues, such as securing the connection, establishing and starting the session and ending up the session and the connection established previously. This approach for authentication requires a dedicated LDAP server and an interconnecting module to connect into the login interface in the MCS. As the user enters his credentials, these credentials will be passed to the LDAP server which will test them in the LDAP directory. The usage of LDAP technology brings many benefits including the provision of a centralized point for security issues as authentication is transferred to another standalone system. In addition, the solution provided in this thesis will provide an enhanced security features for encryption and decryption of the authentication process.

1.2 Problem Statement

In the current MCS, a user's information is stored in the MCS servers as plain text file. Users can only login to the server they had account on. If the MCS server is down, users will need to have account on another MCS server to be able to use such services. More obviously, when the user starts the login process, the username and password are sent as a text, and the MCS will only compare them with a simple table found on the MCS server. Moreover, when a user wants to invite a user from different server to a conference, he has to go through the user's lists in all other servers (one-by-one) in order to locate the user he is looking for. This invitation process will take a long time if the number of servers connected to one system is big. As an example, if the number of servers in a single system is 20, the user has to check 20 user lists (in worst case) to find and invite another user.

1.3 Motivation and Justification

When signing up, process is done on the same MCS system where all users are required to login into the same server, however, when making authentication using LDAP server, the authentication process will be centralized. Hence, any permitted user will connect to one MCS system that might login into that particular MCS by connecting the MCS to the LDAP server. Consequently, any user may be invited if he either has a name in the same MCS server or his name is registered in another server. Centralized authentication process will bring many benefits and will enhance the overall security of the MCS system, for example, the user will have to have only one unique username, and thus, the time consumed to set up a new account for MCS system will be minimized. This thesis will concentrate on redesigning the MCS server to be able to communicate with LDAP server. The new system will use distributed LDAP servers to distribute the load between Multiple LDAP servers. This will also enhance the security of MCS as the login process is unsecured in the current MCS implementation, therefore, LDAP will enhance the security through its built-in support for SSL secure connection over the TCP/IP.

1.4 Objectives of the Research

In this research, the objective comprises redesigning current MCS for more secure log in process and faster invitation among users.

1.5 Scope of the Research

This thesis overcomes the problem of creating multiple accounts for the same user in multiple MCS servers. It concentrates on providing central and secure

authentication for MCS users. It will also enhance the speed of inviting users from multiple MCS servers to a video conference. Other services for MCS users are outside the scope of our research even though the proposed solution may enhance other services provided to MCS users.

1.6 Contributions

Several studies have discussed the issue of using LDAP as directory service and authentication entity. Some of these used an integrated approach while others focused on specific features and functionalities that LDAP can provide. The main contribution of this research is to redesign and implement the new MCS server that is able to communicate with a centralized authentication entity (LDAP server) which will result of MCS users will use one single user name and password to login and use MCS services.

1.7 Research Methodology

The research methodology is done based on the following main steps: the research procedure and the theoretical framework.

1.7.1 Research Procedure

The following highlighted steps are a base for research procedures of this research:

- Analyzing Multimedia Conferencing System (MCS).
- Investigate and search for centralized authentication method or system suitable for MCS.

- Analyzing the new centralized authentication method or system.
- Designing interconnectivity between MCS and the new centralized authentication method or system.

1.7.2 Theoretical Framework

The MCS and new centralized authentication method or system can be interconnected using an intermediate software module that interconnects between them. In our study, we choose LDAP to be the centralized authentication system because MCS will get the benefits of the centralized authentication database of LDAP.

This thesis will be a case study as a typical approach for a qualitative research and investigation types. Also, the thesis will propose a new module that implements the LDAP tool through the user authentication process for MCS in the USM computer laboratories in order to connect as many users as possible with each other without making new accounts at each connecting time. Finally, the implementation of the method is done in the lab experiment.

1.8 Thesis's Organization

This thesis is organized into six chapters. The first chapter introduces a general background of the LDAP and MCS then it presents the problem statement of our study followed by the objective of this thesis and the research contribution. Chapter 1 ends by highlighting the research methodology. In Chapter 2, backgrounds to both the Multimedia Conferencing System (MCS) and the Lightweight Directory

Access Protocol (LDAP) are discussed in more details. It also lists and explains several previous studies that are related to the given topic. In Chapter 3, the research methodology is explained in more details. In Chapter 4, the implementation is presented and the results of the implementation are covered in Chapter 5. Finally, in Chapter 6, the conclusions of the research work and suggested future works are highlighted.

CHAPTER 2

BACKGROUND AND LITERATURE REVIEW

2.1 Introduction

MCS has taken place through real conferences since it is reliable and efficient. With the highly demands of electronic conferencing systems, MCS is aimed to be a desirable facility based on the use of LDAP. This use will improve the way users try to access to each others' accounts. Accordingly, in this chapter, a general background of LDAP and MCS will be discussed. In Section 2.2, a background of the MCS and its main entities are discussed. Sections 2.3 to 2.8 provide a comprehensive background of LDAP. In Section 2.9 distributed LDAP is presented. In Section 2.10, a study on centralized servers for authentication and special services is presented. A summary of this chapter is given in Section 2.11.

2.2 Multimedia Conferencing System (MCS)

MCS is a multipoint conferencing system that is easy to be integrated into an existing network. It relies on Real-time Switching (RSW) control criteria (Ramadass and Subramaniam, 1995) as a controlling protocol to manage sessions. In addition, the Document Conferencing (DC) unit (Ramadass *et al*., 2004) is a feature to MCS which is responsible for sharing files and managing Instant message conversation among users of MCS. Figure 2.1 illustrates the components of MCS and the different types of communications that occur between them.

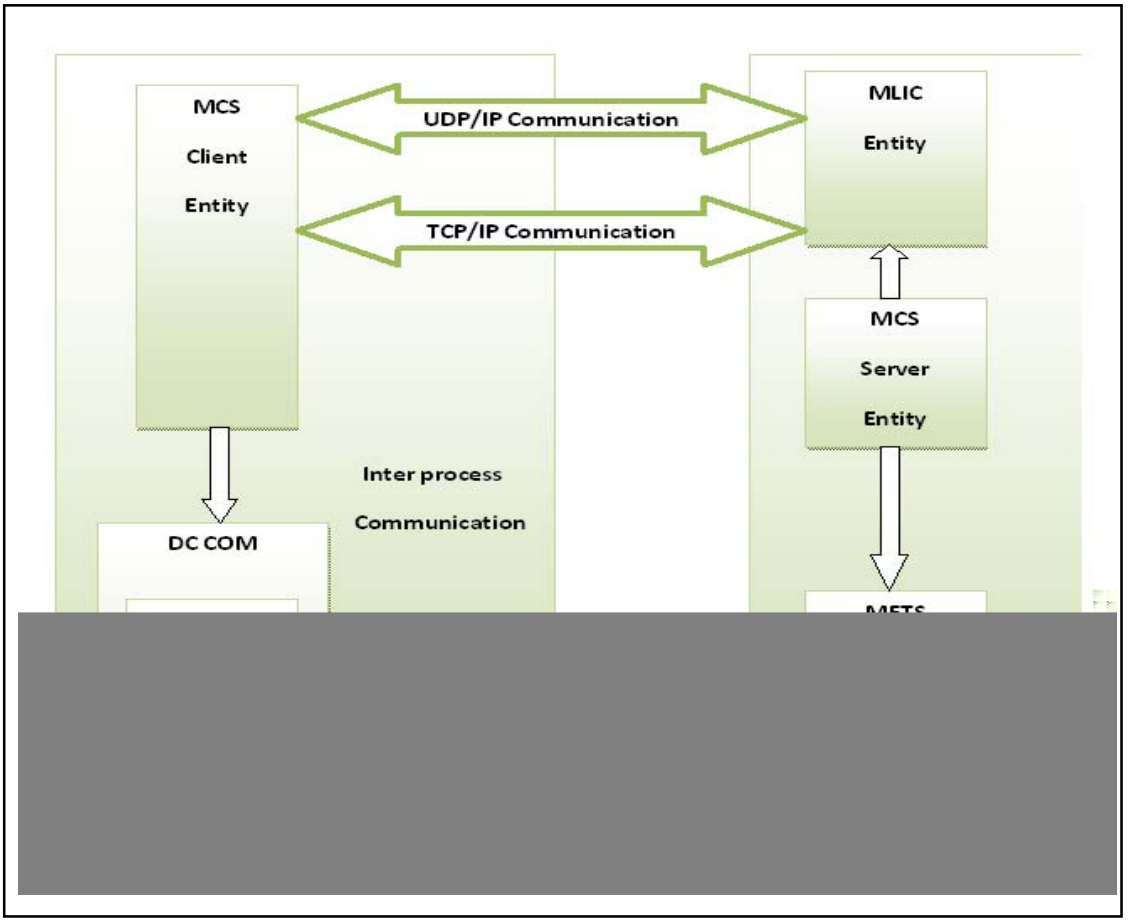


Figure 2.1: MCS Block Diagram (Saleh, 2004)

Video conferencing systems are divided into three types: point-to-point, point-to-multipoint and multipoint-to-multipoint. In the point-to-point conventional communication, both ends should use ISDN WAN links. This type of Video conferencing system has some setbacks such as: communication is only point-to-point and WAN link has to be dedicated for video conferencing only. In the point-to-multipoint video conferencing system, it becomes possible for more than two ends to communicate at the same time using a Multipoint Conference Unit (MCU). However, WAN links should be dedicated for video conferencing and additional WAN links should be found if one end wants to send data and emails as well as

conducting a video conference; in addition the WAN bandwidth needs to be increased according to the multipoint ends linked to the conference (mlabs, 2009).

MCS is a multipoint-to-multipoint video conferencing system. This system is considered to be the most efficient conferencing system (Ramadass *et al*., 2004). It allows holding conferences to as many people as required from any point of the world as it uses the existing LAN infrastructure (mlabs, 2009). Hence, ISDN lines and cabling are no more required. Moreover, the required bandwidth remains constant apart from number of the participants.

MCS is based on distributed network entities architecture and uses RSW control criteria to as a control mechanism. The main MCS entities are:

- The MCS server entity.
- The MCS client entity.
- The multilan IP converter (MLIC) entity.

2.2.1 The MCS Server Entity

This server entity performs the functions of a ‘conductor’ while the rest of the entities are like the ‘orchestra’. The server manages and monitors the conference; also it establishes a virtual point to point TCP link to all entities to handle control communications. The main functions of the server are as follows:

- Coordinates and manages all network entities involved in a multimedia conference.
- Uses RSW control criteria to control the conferencing.
- Providing users a platform to register/login to participate in conferences.

- Coordinates multicast address assignments for single and multiple conferences.
- Establishes inter-server links (only during multi-server conferences).
- Provides damage control when links break or when entities ‘crash’ (become ‘unplugged’).

2.2.2 The MCS Client Entity

The MCS client entity is the user based GUI application that works on the end user’s PC. The modules in the client entity are video module, audio module and document conference module (Sureswaran *et al*., 1999). The functions of the client are as follows:

- Multimedia captures (capture of audio, video and document information).
- Multimedia playback (display of audio, video and document information).
- Data packetization (for transmission) and data reconstruction (for receiving and playback).
- Communicate with the server to maintain the RSW Control Criteria.

Since client entity must follow distributed architecture standards, message passing is done using standard forms, i.e. TCP/IP and UDP. The workstation CPU only has to concentrate on Multimedia (Audio, Video and Document) captures, packaging, transmission and vice-versa. Functions like monitoring the conference, registering new users, establishing multi LAN links, etc. are handled by the server and other objects. This greatly improves speed and quality of transmission. Figure 2.2 shows the client objects connectivity.

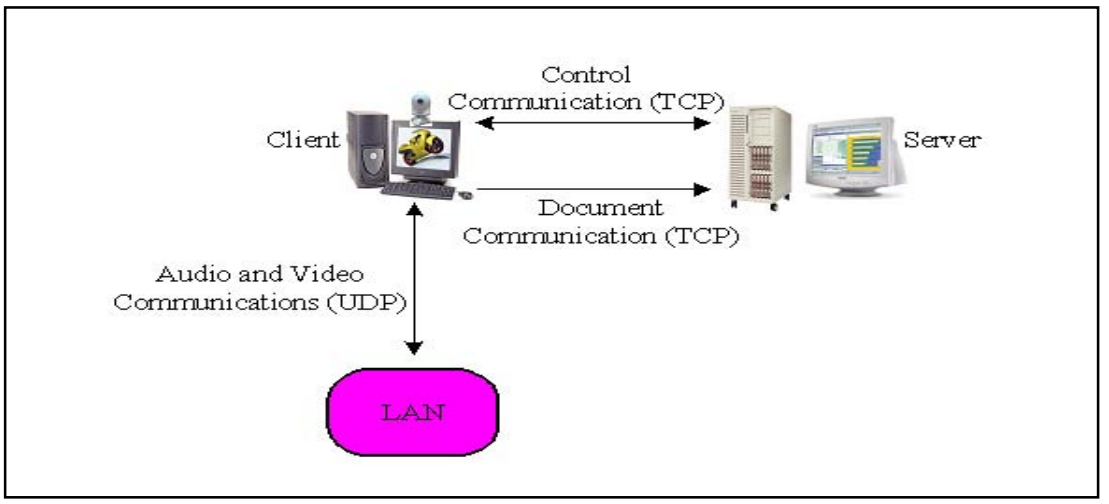


Figure 2.2: Client entity connectivity (Sureswaran *et al.*, 1999)

2.2.3 The MultiLan IP Converter (MLIC) Entity

Since media packets (audio and video) are transmitted as multicast packets, the WAN routers generally drop these packets. This means conference cannot be held between users from different LANs. Figure 2.3 shows the architecture without MLIC (Sureswaran and Wan, 1998).

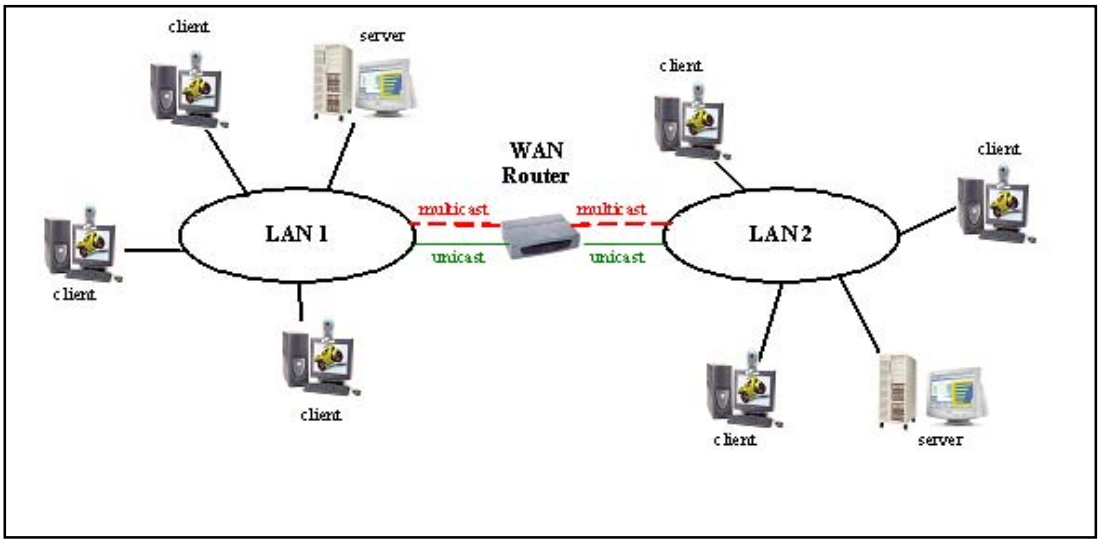


Figure 2.3: MultiLAN without MLIC (Sureswaran and Wan, 1998)

To make users from different LANs communicate with each other using audio and video multicast, an MLIC entity is needed. The MLIC converts these multicast packets to unicast packets to enable it to pass through these WAN routers and reach the other LAN. On the receiving end, another MLIC converts these unicast packets and retransmits them as multicast packets onto the other LAN (Saravanan and Sureswaran, 2000). The functions of the MLIC can be defined as follows:

- Audio/Video packets are transmitted by the client (active site) in LAN 1. MLIC in LAN 1 will:
  - Listen to specified port for Audio/Video UDP multicast packets.
  - Change to Audio/Video UDP unicast packets and transmit out.
- The converted packets then go through the WAN router to LAN 2. The MLIC in LAN 2 will then:
  - Receive Audio/Video UDP unicast packets from the MLIC in LAN 1.
  - Change Audio/Video UDP unicast to Audio/Video UDP multicast packets and retransmit within LAN 2.

Figure 2.4 shows the architecture with MLIC while Figure 2.5 shows MCS as multipoint-to-multipoint video conferencing system.

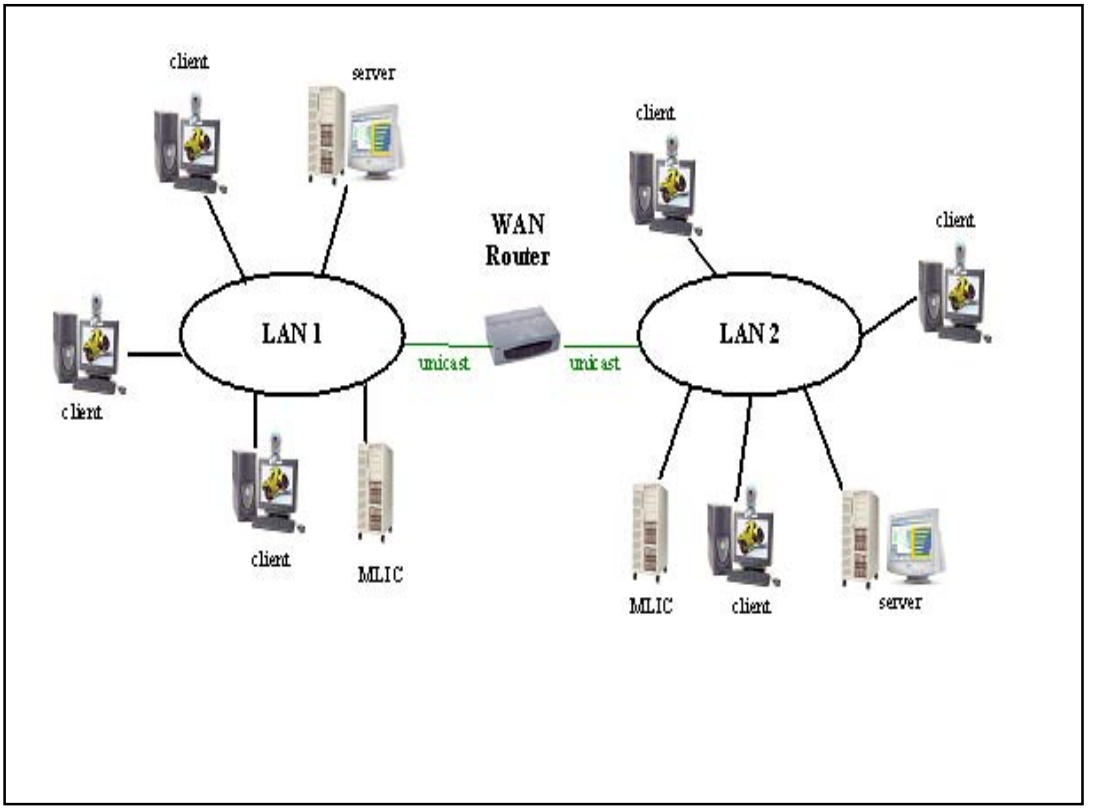


Figure 2.4: MultiLAN with MLIC (Saravanan and Sureswaran, 2000)

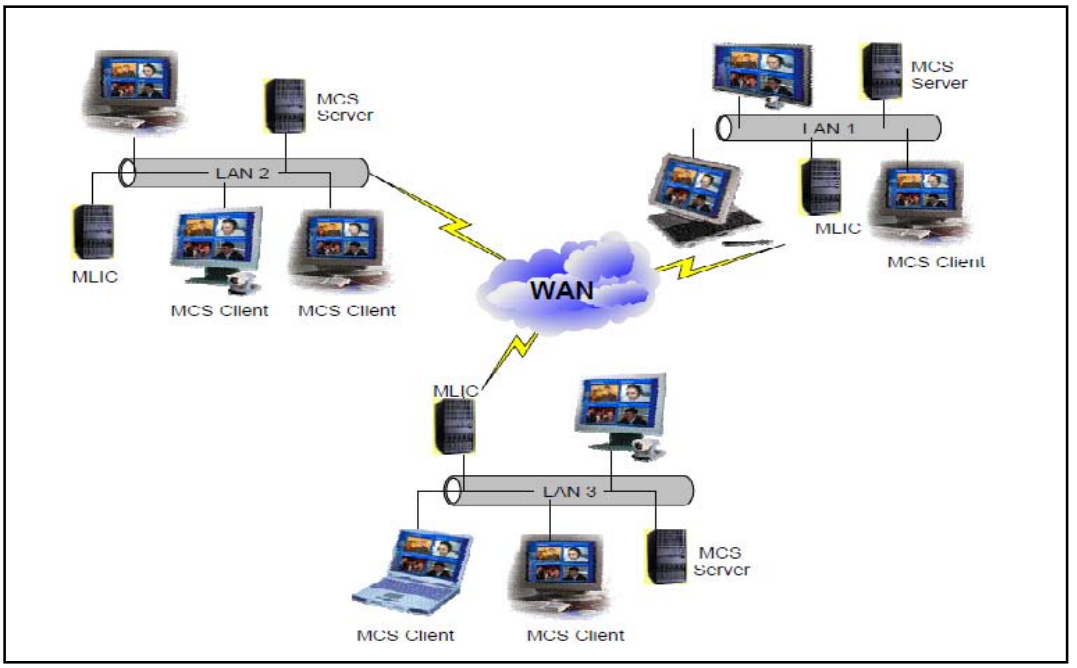


Figure 2.5: Multipoint-to-multipoint Systems (Mlabs, 2005)

2.3 Lightweight Directory Access Protocol: History and Future

The protocol LDAP is a standard for facilitating accessing directory services. It was derived from OSI X.500 model, namely (DAP). LDAP is better than DAP where it is accessed via the simpler TCP/IP instead of OSI stack. LDAPv3 includes an important security enhancement. The LDAP provides a protocol and a data model for naming and authentication. The main function of LDAP servers is to answer queries. The LDAP information model is also called the LDAP schema where it provides unique names by providing a name from a node to a root.

LDAP directory is accessed via authentication, queries and update operations. Access control lists (ACL's) manages accessing data under authorization. (Jill Gemmill *et al*., 2005). There are common applications for the LDAP. One of these applications comprises querying and modifying directory services running over TCP/IP (Koutsonikola, 2004). A directory can be imagined as a group of objects with related attributes organized logically or hierarchically. Depending on the model chosen, an LDAP directory tree is bounded according to politics, geography and/or organization. The most used structure for LDAP is the Domain Name System (DNS) for organization the uppermost levels of the tree or hierarchy. The deeper leaves in the LDAP tree may represent any particular object, such as: PCs, people, documents or anything representing a tree entry (or multiple entries). The current version of LDAP is LDAPv3 which is a version that accumulates previous versions and its specifications and requirements to be defined in a series of the Internet Engineering Task Force (IETF) standard track Requests for Comments (RFCs) (http://en.wikipedia.org/wiki/Ldap , 2009).

The directory services known as X.500 were based on the X.500 Directory Access Protocol (DAP). In the matter of fact, they need the Open Systems Interconnection (OSI) protocol stack. The LDAP directory servers lately replaced the X.500 directory servers as they support both DAP and LDAP, besides, the OSI suite is provided. Currently, X.500 directory protocols including DAP are used directly over TCP/IP as shown in Figure 2.6.

The LDAP protocol was created by the University of Michigan (Tim Howes *et al*., 1995). Earlier, this protocol was known as a Lightweight Directory Browsing Protocol (LDBP). It was renamed after adding directory updating functions in addition to directory browsing and searching functions. Moreover, this protocol has also influenced X.500 upcoming Internet protocols, including XML, XED, DSML, SPML and SLP **(**Amrita *et al*., 2007).

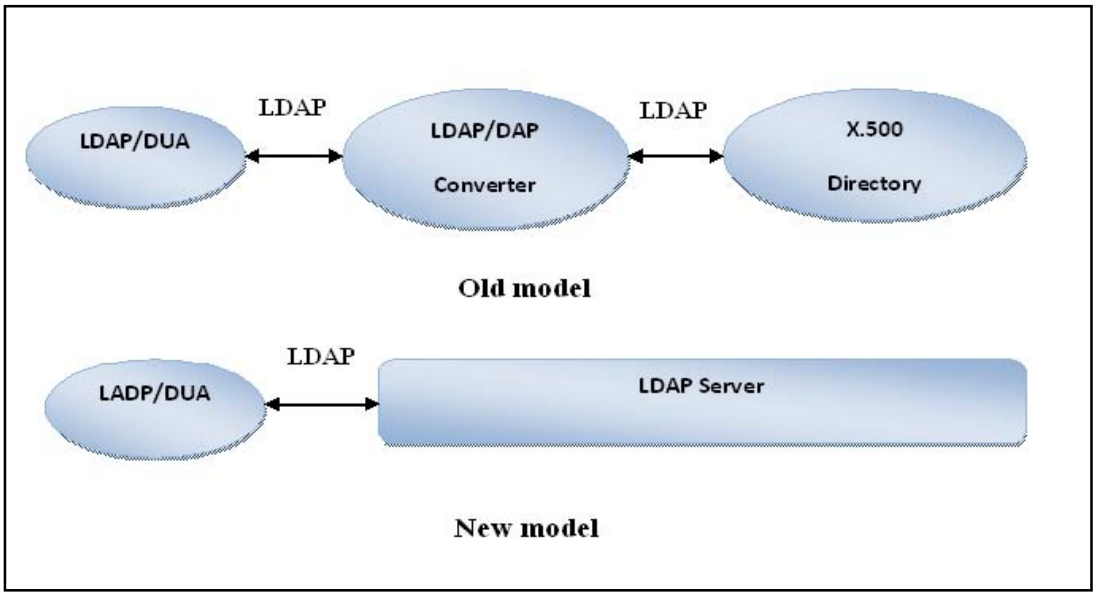


Figure 2.6: An old model and a new model of the LDAP server (Amrita *et al*., 2007)

2.4 LDAP Concepts and Operation

2.4.1 Entry

Entry is a collection of information for one object. The object may be a company, a department, a person or any shared resource. Each entry has its unique Distinguished Name (DN). DN consists of the entry (or Relative DN) which is also abbreviated as RDN and its parent entries connected in ascending order from the entry to the root (top) in the tree. Collectively, all the entries form the Directory Information Tree (DIT) as shown in Figure 2.7 (Ghosh and Mohanthy, 2004). Another example of DIT is illustrated in Figure 2.8.

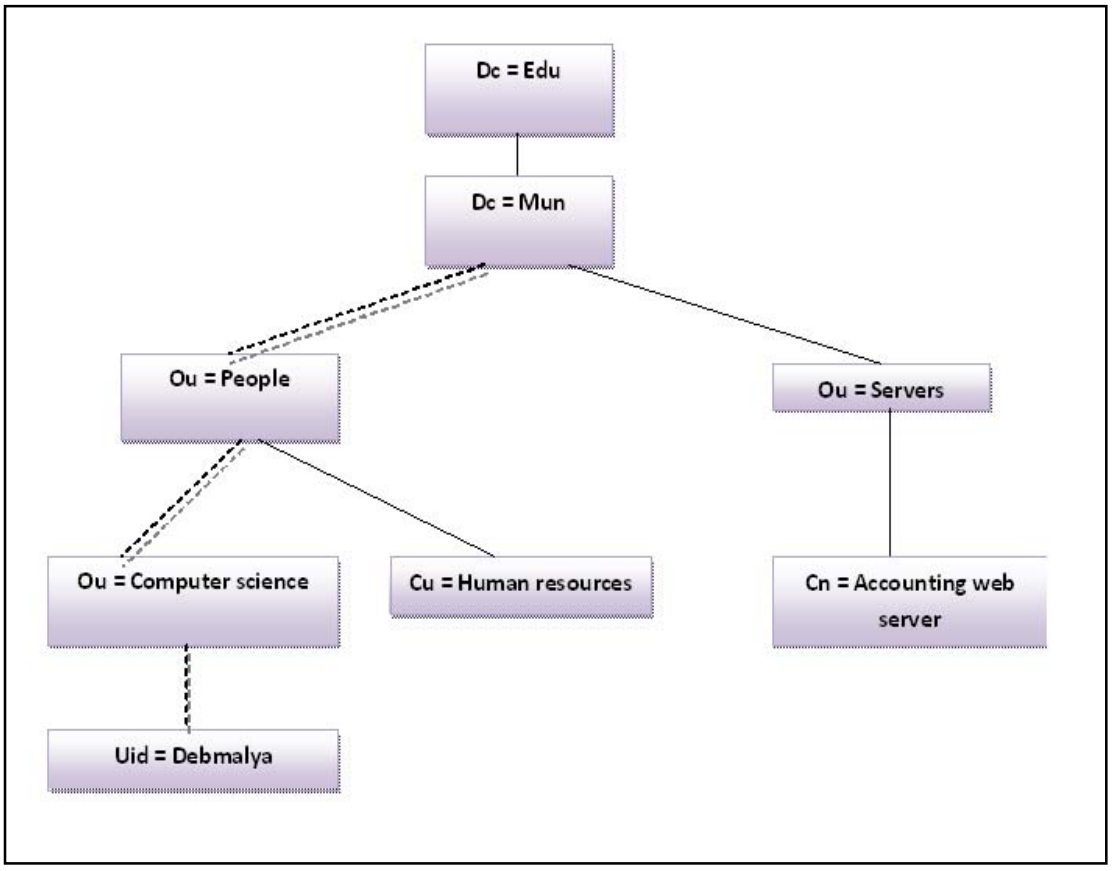


Figure 2.7: LDAP Directory Information Tree (DIT) (Ghosh and Mohanthy, 2004)

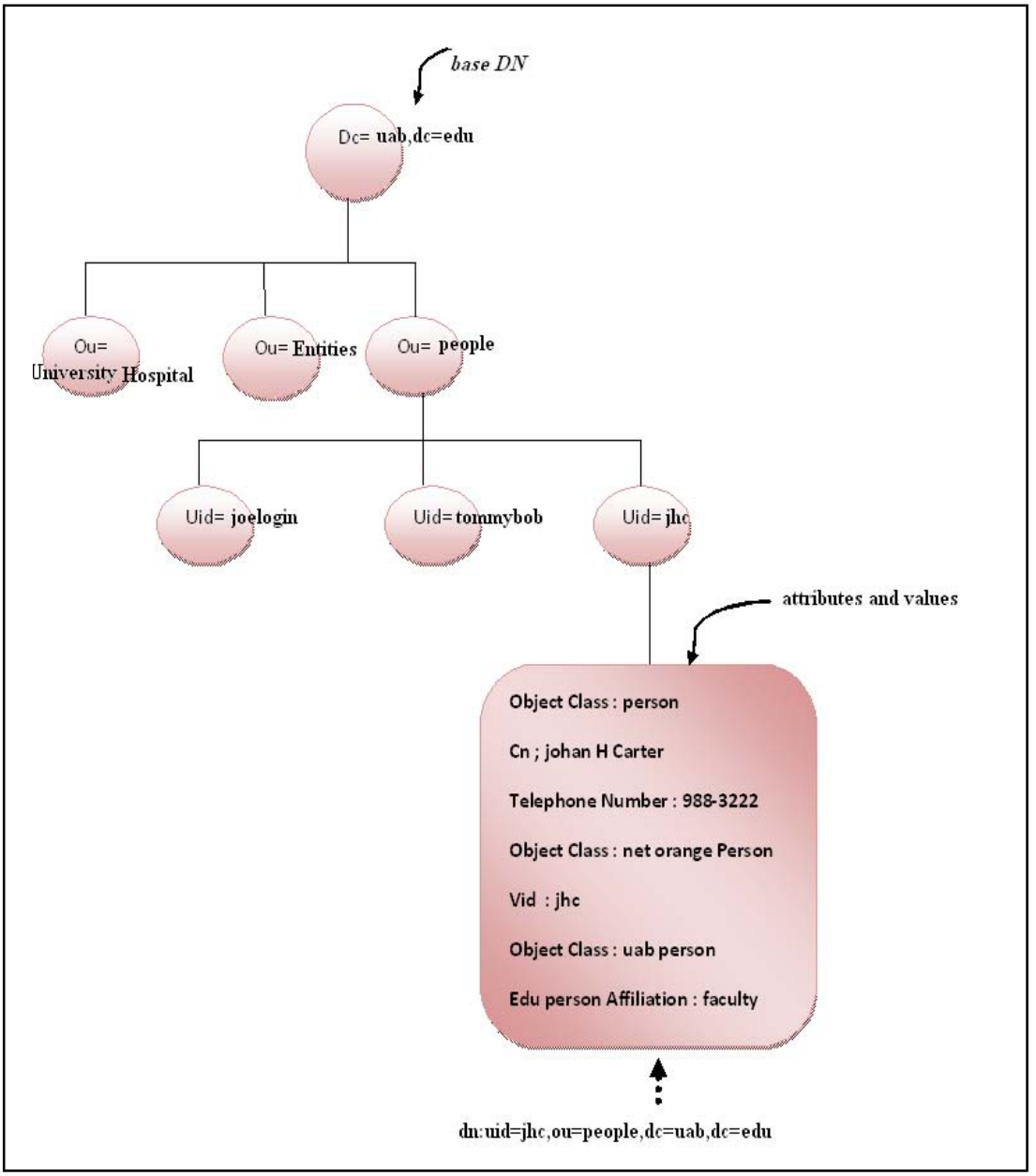


Figure 2.8: DIT Example and DN (Jill Gemmill *et al.*, 2005)

2.4.2 Attributes

An entry has got several attributes. Each attribute describes a unique feature of the entry. Each attribute consists of two components, a type and a value. Sometimes one attribute might have more than one value (Ghosh and Mohanthy, 2004).

2.4.3 Object classes

A class is a set of attributes used to define an entry. In a class, attributes are mandatory or optional (Ghosh and Mohanthy, 2004). In user authentication process, the object classes will be referred for real users, and the attributes are the user's credentials. The user object will be the concentration of the present research; therefore, this should be taken into consideration at implementation.

2.4.4 Query

These functions are used for retrieving information from a directory. Search needs a criterion, a scope and a starting point. The starting point is known as the base DN. The scope may be a single entry (base level) the children of an entry (one level) or the sub-tree of the DN (Ghosh and Mohanthy, 2004).

2.4.5 Update

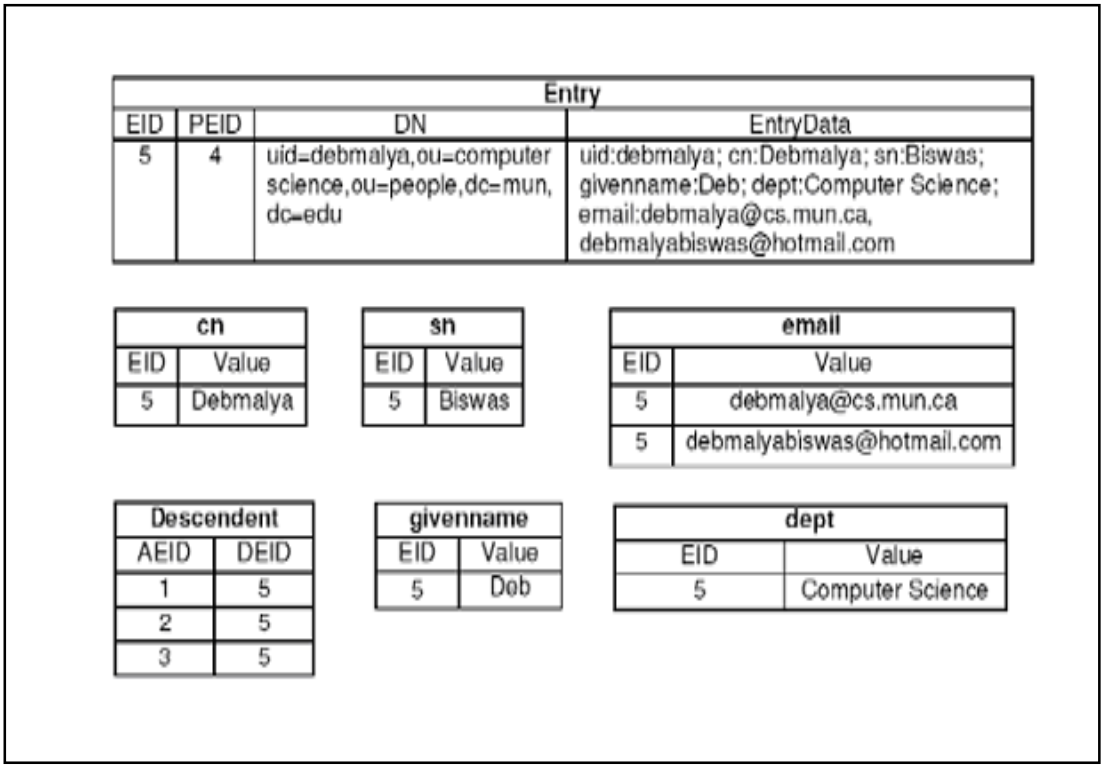
These functions are used to update contents of a directory. They also are used to update multiple attributes of one entry at the same time (Ghosh and Mohanthy, 2004).The update operations are (added, delete, modify) and modify DN all require the DN of the entry to change. Modify takes a list of attributes to modify and the modification to each: delete the attribute or some values, add new values, or replace the current values with the new ones.

2.5 LDAP Data Storage

As data in LDAP are stored hierarchically, B-trees and hierarchical databases would be options for LDAP storage. However, recently, relational databases (RDB) are the upcoming technology for LDAP storage **(**Debmalya and vidyasankar,2005). Figure 2.9 shows an example of a RDB implementation for LDAP.

There are multiple problems that can be solved by using the RDB mechanism. These are:

- Handling large amounts of data
- Complex searching
- Indexing services; and
- Resilience against failures



Entry

EID	PEID	DN	EntryData
5	4	uid=debmalya,ou=computer science,ou=people,dc=mun, dc=edu	uid:debmalya; cn:Debmalya; sn:Biswas; givenname:Deb; dept:Computer Science; email:debmalya@cs.mun.ca, debmalyabiswas@hotmail.com

cn

EID	Value
5	Debmalya

sn

EID	Value
5	Biswas

email

EID	Value
5	debmalya@cs.mun.ca
5	debmalyabiswas@hotmail.com

Descendent

AEID	DEID
1	5
2	5
3	5

givenname

EID	Value
5	Deb

dept

EID	Value
5	Computer Science

Figure 2.9: Relational Table Representation (Debmalya and Vidyasankar, 2005)

The information of an LDAP entry is contained in the "Entry" table where it supports the search of the LDAP. The main idea is to obtain the entry of the EID through this table. The descendant entries unique identifier (DIED) is contained in this table where each LDAP entry has a unique ID (AEID) (Shi *et al.*, 1998).

EID (Entry Identifier): is the LDAP entry's unique identifier.

PEID (Parent Entry Identifier): is the parent LDAP entry's unique identifier in the naming hierarchy.

DN (Distinguished Name): is the entry's distinguished name.

AEID (Ancestor Entry Identifier): is the ancestor LDAP entry's unique identifier.

DEID (Descent Entry Identifier): is the descent LDAP entry's unique identifier.

2.6 Models for LDAP

2.6.1 Informational Model

As mentioned above, an entry is the basic unit of storage which can be a (real-world) object. LDAP Data Interchange Format or LDIF is used normally to represent LDAP entries. For instance, in LDIF, familiar attributes such as age, sex and continent, could be used. Each entry may belong to one or more object class. The Object class definitions specify a type, mandatory and optional attribute types, and an identifier. Each attribute has a type, whose definition specifies a name and an object ID and an indicator for one or multiple values. Also matching rules are used for specifying how attributes are compared. In addition, there is an indicator for specifying who will use the attribute: a system or a user (Fink and Kobsa, 2006).

Also, restrictions can be used for the range or size of the attribute values as shown in Figure 2.10.

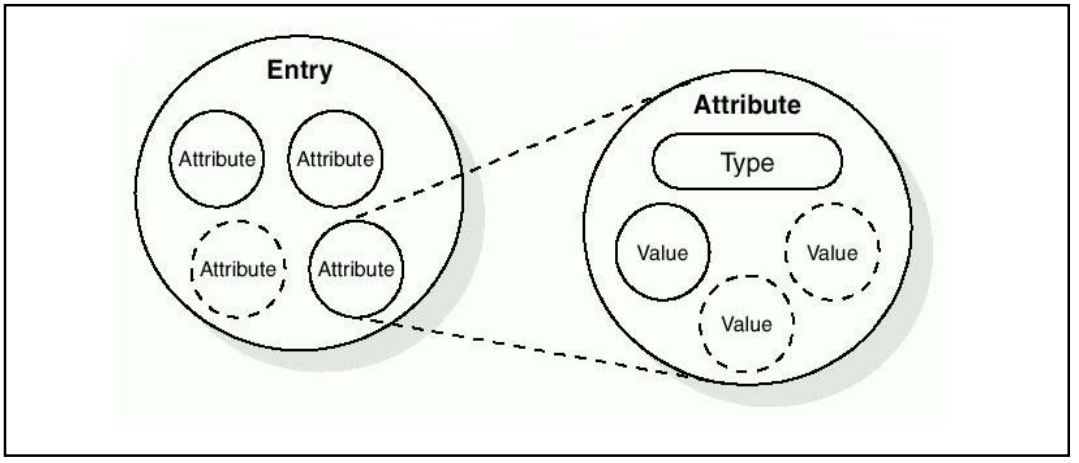


Figure 2.10: LDAP information storage (Fink and Kobsa, 2006)

2.6.2 Naming Model

LDAP naming is similar to hierarchical file system model. From this point, directory may contain files and/or sub-directories. There are some differences between the two models. One difference between a file system and LDAP is the root directory. In the file system, root directory is the common origin directory for all files and directories. In LDAP, the root is a special entry which contains the server-specific information. Another difference is that in the file system, one node can be either a file or a directory. However, one node in LDAP can be a set of values where at the same time these values can have children. The final difference is that the full path in the file system starts from the root to the leaf. Nonetheless, full names in LDAP are consisted of the leaf up to the root. LDAP also uses aliases, which seem as

shortcuts in file systems (Fink and Kobsa, 2006). Figure 2.11 illustrates an example of a distributed directory. It is specified only in LDAPv3.

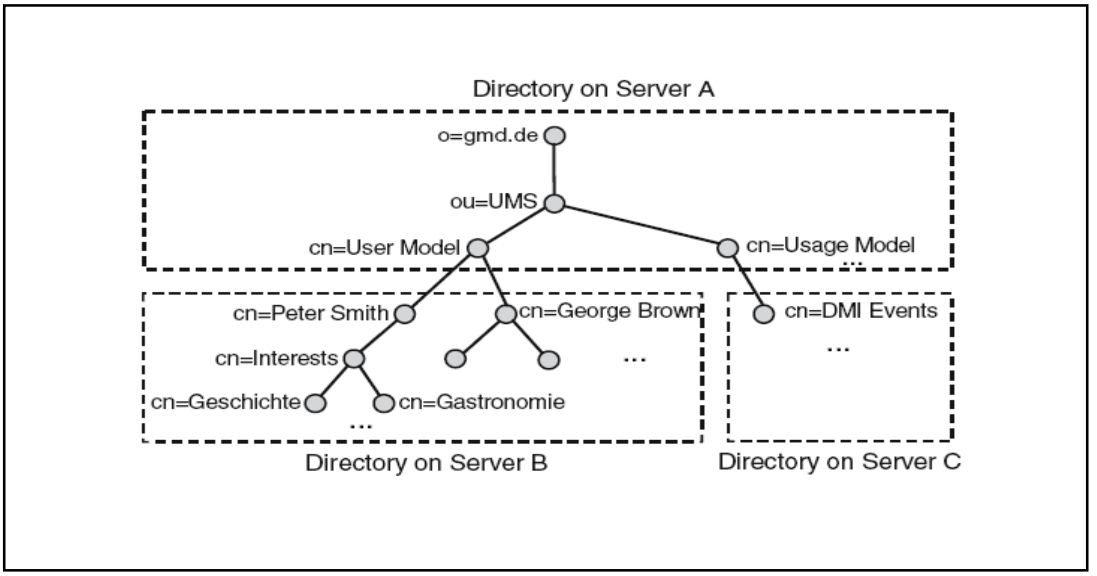


Figure 2.11: Distributed directory (based on Howes *et al.*, 1999)

2.6.3 Function Model

There are three types of operations: Query operations, such as: search and compare; Update operations, such as: add, delete, rename and modify; Authentication and control operations, such as: bind, unbind and abandon. These operations are used between clients and servers before operating through other operations (Fink and Kobsa, 2006).

2.6.4 Security Model

Authentication, signing and encryption are features of LDAP. An interface is offered by LDAP where this interface is a standard for identifying other parties including anonymity. Passwords can be interchanged in plain text; in SSL-secured

connection encryption; in X.509 certification via secure sockets layer (SSL), simple authentication and security layer (SASL) and Kerberos. Signing operation ensures exchanging information during authentication. Signing is supported through SSL, where each block is followed by a cryptographic checksum to verify the sender and the correctness of data. Encryption encodes exchanged information. During the negotiation in SSL, the client and the server agree upon a protocol, such as: Rivest Cipher 4(RC4), Data Encryption Standard (DES), and international data encryption algorithm (IDEA). Also message-digest algorithm 5 (MD-5) through simple authentication and security layer (SASL) interface is supported in LDAP (Fink and Kobsa, 2006). Figure 2.12 illustrates that.

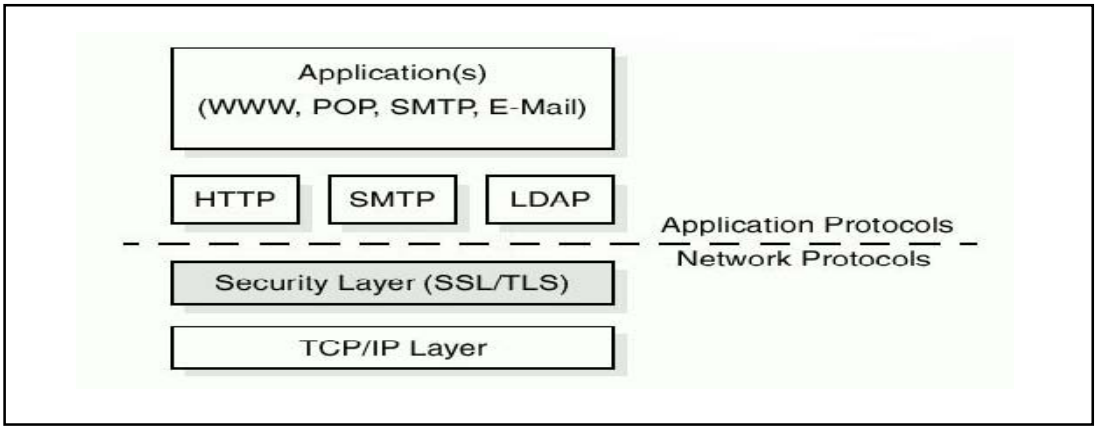


Figure 2.12: LDAP using SASL using SSL/TLS (Fink and Kobsa, 2006)

2.7 Directory Clients and Servers

Client/server model is a preferred model for accessing directories of LDAP. Applications cannot access directories directly; however, they call functions or Application Programming Interfaces (APIs) which contact a process that handles the operation on behalf of the application. After operations are being handled by APIs,