Inventions on LDAP access interface- a TRIZ based analysis

Umakant Mishra
Inventions on LDAP access Interface
-A TRIZ based Analysis of US Patents

By- Umakant Mishra, Bangalore, India

http://umakantm.blogspot.in

Contents

Contents ................................................................................................................................. 1
1. Introduction ........................................................................................................................ 2
2. Study on LDAP data access interface .............................................................................. 2
   2.1 Objectives of the study ................................................................................................. 2
   2.2 Major areas of Invention ................................................................................................ 3
   2.3 Patents analyzed for the study ...................................................................................... 3
3. LDAP data Interface Mechanism .................................................................................... 3
4. Major Concerns in LDAP data interfacing ..................................................................... 4
5. IFR for LDAP data access and presentation ................................................................... 4
6. Inventions on improving LDAP interface for data access ............................................. 5
   6.1 Automated distinguished name lookup ....................................................................... 5
   6.2 Interface to manage multiple LDAP .......................................................................... 6
   6.3 Automatically retrieving proprietary and standard formats from LDAP ............... 7
   6.4 Directory services user-interface extensions architecture ....................................... 9
7. Other related inventions .................................................................................................... 10
   7.1 Network directory access mechanism ....................................................................... 10
   7.2 Providing extendible Access Control for LDAP Protocol .......................................... 10
   7.3 Implementing smart HTML mail using LDAP .............................................................. 10
   7.4 Generating SQL query statements for LDAP Search Filter ...................................... 11
   7.5 Spoken name announcement feature ....................................................................... 11
   7.6 Implementing SQL in LDAP queries ......................................................................... 11
   7.7 Online directory service with multiple database ....................................................... 11
   7.8 XML-LDAP Adapter for data transfer ........................................................................ 12
   7.9 Retrieving style sheets from LDAP based on partial character matching .................. 12
   7.10 Data management interoperability in heterogeneous directory structure ................ 12
8. Summary and Findings of the study ............................................................................... 13
   8.1 Distribution of patents ............................................................................................... 13
   8.2 Hot areas in LDAP interfacing and presentation ....................................................... 13
   8.3 Trends of evolution in LDAP data access and presentation ...................................... 13
   8.4 Predicting future inventions on LDAP data access, interfacing and presentation ...... 14
Reference to patents: ............................................................................................................ 14
Other references: .................................................................................................................. 15
1. Introduction

Lightweight Directory Access Protocol (LDAP) is an IETF open standard to provide directory services in the network. LDAP was initially developed at the University of Michigan with an objective to include most of the features of X.500, while eliminating the burdens and difficulties of the same.

The current Version of LDAP is LDAP V.3 released in December 1997 (RFC 2251). Other specifications of LDAP can be found in different RFCs on the IETF (Internet Engineering Task Force) website.

With the growing use of Internet, LDAP is becoming more and more popular to provide directory services to a wide range of applications. This led to patenting several inventions relating to LDAP operation and application. This study on LDAP data storage is a part of the main study on LDAP based on 60 selected patents on LDAP from US Patent database.

2. Study on LDAP data access interface

This study on LDAP data access interface is a part of the above-mentioned study on LDAP. The study is mainly based on the analysis of US patents. The methodology followed is the same as the above.

2.1 Objectives of the study

The objective of the study is to know:

- What are the inventions made on LDAP data access interface, data presentation and formatting?
- What is the Ideal Final Result (IFR) in LDAP data accessing and presentation? Is there any trend in the series of inventions?
- Which problems on LDAP data formatting and presentation are not solved yet? In other words which problems need to be addressed in future?
- Which aspects of LDAP data access interface, data formatting and presentation are yet unexplored? What are the possible areas of improvements in future inventions?
- Which Inventive Principles or other techniques of TRIZ are useful to analyze such inventions?
2.2 Major areas of Invention

- One important area that attracts the inventors is to develop an improved user interface for accessing and manipulating directory data.

- Developing an administrative interface to manage LDAP servers.

- The other area that attracts inventors is to store data in various formats in LDAP directory and retrieve the data in a desired format.

- Another area is to use style sheets, voice interface and other mechanism to improve the format of presentation.

- Interfaces capable of filtering data according to the desired criteria.

2.3 Patents analyzed for the study

- US Patent 6408306, “Method and system for automated distinguished name lookup”

- US Patent 6490619, “Method and system for managing multiple lightweight directory access protocol directory servers”,


3. LDAP data Interface Mechanism

LDAP offers a rich set of searching capabilities. The client makes a TCP/IP connection and sends requests to an LDAP server. The LDAP server executes the search (or update) command and returns a sequence of responses to the client. The search responses may contain SearchResultEntry (the attributes and values satisfying the search conditions), SearchResultReference (URL of the referral servers), ExtendedResponse or SearchResultDone (success or failure of search operation) data types.

LDAP server may store data in a Flat file, in RDBMS or in any other database. The LDAP client applications can use LDAP directory interface without having knowledge on the underlying data storage mechanism. LDAP can be mapped onto any other directory system so long as the X.500 data and service model as used in LDAP is not violated in LDAP interface.
However, the clients should not assume that the servers support any particular schemas without prior agreement with the servers. After getting the data from the server, it is the client who makes use of it or presents it in the desired format.

4. Major Concerns in LDAP data interfacing

- The individual entries are stored in the directory server. But different clients may need the same data in different format. LDAP specification does not provide any mechanism of accessing data in different format.

- LDAP provides features to search the properties of an entry based on its distinguished name. But remembering distinguished names can be difficult for a user.

- The system administrator needs an administrative interface to manage multiple LDAP servers.

- The LDAP directory should not be confined to store only textual data. It should be able to store and serve images, audio, video, animations and other kinds of data as required.

5. IFR for LDAP data access and presentation

According to TRIZ, ideality is a function of its benefits and costs. **Ideality = \( \frac{\sum \text{Benefits}}{\sum \text{Costs} + \sum \text{Harm}} \)**. So the Ideal Final Result in LDAP access and presentation can be achieved by increasing all useful functions of the LDAP presentation and decreasing all harmful functions of the same. An analysis of the LDAP system may find the following as IFR for LDAP administration.

<table>
<thead>
<tr>
<th>Should have (Positive features)</th>
<th>Should not have (Negative features)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The LDAP server should be able to provide all data requested by the client data in the desired format.</td>
<td>• The LDAP server should never become overloaded.</td>
</tr>
<tr>
<td>• The LDAP server should be able to store all types of data including text, image, audio, video, binary and others. It should support the known formats and unknown formats too.</td>
<td></td>
</tr>
<tr>
<td>• The server should validate all additions and modifications to the directory by the user.</td>
<td></td>
</tr>
<tr>
<td>• The user interface to manage LDAP server should be so simple as to be used by any system administrator.</td>
<td></td>
</tr>
</tbody>
</table>
6. Inventions on improving LDAP interface for data access

As we discussed above there are inventions on various aspects of integrating LDAP with other directories. We will analyze such inventions in the following pages.

6.1 Automated distinguished name lookup

Background problem

Each resource in the LDAP server is identified by a unique distinguished name. To perform any operation on the directory entries, the user must specify the distinguished names of the directory entries. But it is often difficult for the user to remember the unique distinguished names to feed to the LDAP server. Besides manually specifying a full distinguished name is time-consuming and error-prone. There is a need to get a lookup support to identify the unique distinguished name.

Solution provided by Patent 6408306

US Patent 6408306 discloses an automated distinguished name lookup system for the LDAP operation. The invention provides a dialog window where the user enters an identifier string, which is not a distinguished name but contains some part of the distinguished name. The LDAP server executes a search and displays one or more distinguished names that match with the user entry. The user then selects the desired distinguished name for LDAP directory operation.

TRIZ based analysis

The LDAP system should automatically display the unique distinguished name for the resource desired by the user (Ideal Final Result). The LDAP system should find the distinguished name based on a partial entry made by the user (Desired Result).
The system may not be able to display the desired entry based on a partial entry using a wildcard format, but the system can display all the matching entries satisfying the wildcard format (Principle-16: Partial or excessive action). The user then easily chooses the desired distinguished names out of the list.

6.2 Interface to manage multiple LDAP

Background problem

In a distributed environment the LDAP may be spread across multiple servers in the network. LDAP provides a mechanism of chasing referrals, i.e., if the search is not found in the server, the server may return the URL of another server for referral. But this method has some limitations. While chasing the referrals, the client must bind to each reference server. This means, the bind request will either be treated as an anonymous request or the client will be prompted for login information. Besides the user cannot customize the search process. For example, he cannot restrict the search only to two servers. The LDAP search forces all servers to be searched.

There is a need for an improved method of searching and manipulating data within a set of servers in a distributed network.

Solution provided by Patent 6490619

Patent 6490619 discloses a centralized interface for locating a server in a distributed network using the Lightweight Directory Access Protocol (LDAP). The interface searches multiple servers on the network, displays a tree of servers and provides tools to search the tree of servers for an entry.

The Directory Management Tool (DMT) interface has three major areas, viz., the navigation panel, status area, and work area. The user can customize to view all
the servers or only a few selected servers. Using this friendly user interface, the user can browse the tree structure to find the desired directory and perform the desired action.

**TRIZ based analysis**

The user should be able to search on multiple LDAP servers but without suffering the limitations of LDAP referral mechanism (Ideal Final Result).

The invention proposes a Directory Management Tool that allows the user to operate on multiple LDAP servers spread across a distributed environment (Principle-24: Intermediary).

The DMT allows the user to do authenticated operation on any Server connected through DMT unlike an LDAP referral where the user has to login for each referred server (Principle-9: Prior Counteraction).

The user can search across the entire servers or a customized subset of servers, unlike in LDAP referral where the query is forced to search across all the servers (Principle-15: Dynamize).

**6.3 Automatically retrieving proprietary and standard formats from LDAP**

**Background problem**

Different computer systems require data in different formats. Although in many cases attempts have been made to standardize the formats, still many computers need data in specific formats for different reasons. It is necessary to store both standard and proprietary formats and make the specific formats as required.

One solution is that the user will first retrieve all the formats available and then select the best format from the retrieved format (Principle-16: Partial or excessive action). This would increase network traffic and make the process slow. There is a need to automatically retrieve either the proprietary formats or the standard formats from the LDAP directory.

**Solution provided by US Patent 6850928**

US Patent 6850928 discloses a method to address the above-mentioned deficiencies of the prior art. The attributes of an entry may have one or more proprietary format and one standard format. The invention provides a method of automatically retrieving the entry in a desired format from a directory database.

The system includes (1) a request reception module that receives a LDAP request for an attribute of the directory object that is expressed in a proprietary format and (2) a request fulfillment module, associated with the request reception module. If the directory object contains the attribute expressed in the proprietary
format, the request fulfillment module retrieves the attribute expressed in the proprietary format from the database. If the directory object does not contain the attribute expressed in the proprietary format, the request fulfillment module retrieves the attribute expressed in a standard format from the database and recasts the attribute expressed in the standard format.

For example, a directory client may request a person’s name to be presented in Kanji characters. If the directory contains the desired proprietary format, the request is fulfilled. If the proprietary format does not exist in the database, the LDAP responds the name in standard format (say English).

In another example, let us say an image may be stored in a proprietary format (GIF) and a standard format (TIFF). A client requests for an image in GIF format (proprietary in this case). If GIF image is not available in the database, LDAP response will contain the image in TIFF (standard) format.

TRIZ based analysis
The LDAP server should provide the data in the specific format as desired by the user (Ideal Final Result). But LDAP server may not contain the format required by the client (Contradiction). Besides, the LDAP client may not support the format provided by LDAP server (Contradiction).

The invention allows LDAP to respond with the format requested by the client (Principle-15: Dynamize). It also supports format substitution, for example, when the proprietary format (say GIF) is not available, it allows graphic image substitution and returns the standard format (say TIFF) (Principle-28: Mechanics substitution).
6.4 Directory services user-interface extensions architecture

Background problem

Although many people use LDAP for storing various network resources, LDAP does not provide any common user interface for adding new resources to the network environment. That is why the network administrator sometimes has to physically go to each computer on the network to manually reconfigure the computer to enable it to recognise the new structure.

Besides, there is no common interface for the user to access and view attributes of the network resources. Ideally when a new resource is added to the network and made available to the network users, all user interfaces should automatically recognise the new resource. Thus, there is a need for an extensible resource-sharing environment in a computing network in which user interface information can be propagated across a computer network.

Solution provided by patent 6498612:

US patent 6498612 discloses an extensible user interface by storing user interface information in a display database. The directory objects are bound to the display information in the display database and displayed according to the display information. The display database will contain pointers, which contain pointers to software component modules that are stored locally on the workstation or remotely on a server or both. The user interface application will first check to see if the software module is stored locally on the workstation. If the module is not found locally, then the user interface application will attempt to retrieve the module from the server over the network.

After retrieving the display specifier, the user interface application displays the directory data according to the display specifier. Accordingly, when a database
schema is changed, changes are made to the display database and not locally. These changes in the display database are propagated to all workstations that access the display database or software modules.

**TRIZ based analysis**

The newly added devices in a network should be automatically added to the directory and made visible to the users (Ideal Final Result).

The display characteristics of the directory data are stored in a display database. The user interface displays the directory object according to the display characteristics in the display database (Principle-24: Intermediary).

7. Other related inventions

7.1 Network directory access mechanism

US patent 6553368 discloses a method to integrate LDAP directory to other directories without converting the data. As per the invention, the data in the first directory remains in its own format and data in the other directories also remain in their own formats. The access rights and access methods of directory entries are stored in a Directory Access Control Domain (DACD). But the directory access mechanism is capable of accessing different directories through different protocols (Principle-33: Homogeneity).

7.2 Providing extendible Access Control for LDAP Protocol

US Patent 6633872 provides a method of providing extendible access control to LDAP protocol. According to the method, after the LDAP server authenticates the user, the user is associated to a particular access control group. The access control group may include several application specific parameters (Principle-3: Local Quality), such as directory service parameters. The directory service parameters can include security levels, permissions or access rights.

After the user is associated with an access control group, the LDAP operation is reformatted (Principle-28: Mechanics Substitution) based on the parameters in the access control group and provided to the search engine. The extendible ACL can be implemented as a plug-in within the scope of LDAP server.

7.3 Implementing smart HTML mail using LDAP

Emails use two most common formats, viz., plain text and HTML formatting. There are some email clients, which support only plain text and does not support HTML formatting.

US Patent 6728757 discloses a method of smart HTML email system that automatically and intelligently converts and distributes the user's e-mail documents to both HTML-capable and plain text e-mail clients. Depending on the
address of the recipient, the email client will send a query to the LDAP server to find out whether the addressee is HTML capable or not. If the addressee is known to be HTML-capable, the document is transmitted as is. On the other hand, if the addressee is not known to be HTML-capable the document is converted to plain text and does not contain any HTML formatting (Principle-15: Dynamize, Principle-36: Conversion).

7.4 Generating SQL query statements for LDAP Search Filter

US Patent 6748374 presents a method of maintaining object-oriented data in a relational database. The invention also provides a method for automatically generating a SQL query statement to search for particular entries in the DIT stored in RDBMS (Principle-25: Self service, Principle-36: Conversion). The invention can generate only one single SQL statement for any LDAP search filter. This reduces the number of requests and thereby reduces the system and network overload to perform the search (Principle-40: Composite). The invention proposes to use three intermediary tables including a catalog table, which increases the speed of searching (Principle-24: Intermediary).

7.5 Spoken name announcement feature

US Patent 6810113 discloses a method of using LDAP in a messaging system which would allow messaging services to provide senders with announcements regarding the recipients. According to the invention the information on the senders and recipients will be stored in LDAP server. When a message sender’s messaging platform (MP) finds the spoken name data of the recipient from the Directory (or other sources) the MP makes a presentation to the sender (Principle-23: Feedback). With the implementation of the spoken name announcement feature, the sender becomes sure that his or her message will be made available to the recipient intended by the sender.

7.6 Implementing SQL in LDAP queries

US Patent 6356892 discloses a method of converting LDAP filter expressions to an SQL query to retrieve the matches from the backend database. The method parses an LDAP filter-based query to find the elements and logical operators and generates an SQL sub-query according to a set of translation rules (Principle-28: Mechanics Substitution). The LDAP filter is efficiently mapped into an SQL sub-query. The SQL sub-queries are then combined into a single SQL query according to a set of combination rules (Principle-5: Merging, Principle-40: Composite).

7.7 Online directory service with multiple database

US patent 5918227 discloses a method of accessing multiple directory databases through an intermediate computer (gater). According to the invention there is an intermediate computer or gater in between the client and the directory servers (Principle-24: Intermediary). The intermediate computer receives the requests and passes them to one of the other directory servers. The other
directory servers (gaters) communicate with each other to retrieve the records and then communicate directly with the user independent of the first intermediate computer (gater) (Principle-21: Skipping).

7.8 XML-LDAP Adapter for data transfer

US Patent 7076488 discloses an arrangement for transforming data between an XML (Extensible Markup Language) data source and an LDAP interface. The arrangement includes an XML-LDAP adapter for transforming first data into second data (Principle-36: Conversion).

7.9 Retrieving style sheets from LDAP based on partial character matching

Patent 6463440 discloses a method of storing style sheet characteristics as LDAP objects in an LDAP directory. The style sheets may be encoded in Extensible Style sheet Language (XSL), Document Style Semantics and Specification Language (DSSSL), or any other style sheet language having equivalent semantics. The style sheets are stored in LDAP server and accessed dynamically whichever is desired (Principle-15: Dynamize). The invention provides a pattern matching technique to select the most appropriate style sheets based on partial characteristic mapping for a given document (Principle-15: Dynamize, Principle-16: Partial or excessive action).

7.10 Data management interoperability in heterogeneous directory structure

Patent 6484177 discloses a data management system that enables multiple heterogeneous systems to exchange information. The systems may be comprised of one or more networks, simple or complex file system, different types of databases or directory services like LDAP or Microsoft Active directory, they can still communicate each other (Principle-5: Merging). The invention uses a single virtual Data Management System (DMS) that may exist on a single homogeneous platform or distributed heterogeneous platform. The requests coming from the client are responded through this Data Management System (Principle-24: Intermediary).
8. Summary and Findings of the study

8.1 Distribution of patents
- A total of 14 patents are presented under this study. Out of those 4 are very much related to the topic and analyzed in detail. Rest 10 patents are less relevant to the topic and analyzed in brief.

- Out of the four patents analyzed above under this topic of data access interface, IBM assigns two, Microsoft assigns one and Avaya Technology Corporation assigns one.

8.2 Hot areas in LDAP interfacing and presentation
The analysis finds that the inventions try to improve the following aspects of LDAP system.

- Simplify the method of storing and accessing data from the directory.

- Using LDAP directory to store data in various formats and retrieve data in the desired format at the time of need.

- Improving the access and presentation mechanism of image, audio, video, animations and other types of data.

- Administrative interfaces to manage LDAP servers.

- Improving and customizing LDAP referral service.

8.3 Trends of evolution in LDAP data access and presentation
The following trends are prominent among the inventions on LDAP data storage.

- Increasing speed in LDAP data access- Inventions try to increase speed in user authentication, query execution, referral services and other activities.

- Increasing dynamization - Inventions try to let LDAP server store and serve directory data in different formats as required by the LDAP client.

- Increasing easiness to “configure and implement” and increasing easiness to “maintain and administer” are two obvious trends.

- Reducing system complexity- The LDAP query language, LDAP control language etc. should be simple to be efficiently used by the users and administrators.
8.4 Predicting future inventions on LDAP data access, interfacing and presentation

Based on the analysis we can predict more inventions on the following aspects of LDAP data access, formatting and presentation in future.

- Improved method of validating data before entering into the directory tree (Principle-9: Prior Counteraction).
- Accessing LDAP server from any kind of application (Principle-17: Another dimension).
- Efficient conversion of LDAP search filters to SQL queries (Principle-36: Conversion).
- Using LDAP for keeping citizenship information including photographs, fingerprints and other details. (Principle- Parameter change).
- Voice interface for communicating to LDAP (Principle- Mechanics Substitution).
- Improvements in formatting and displaying requested data on an LDAP client (Principle-35: Parameter change).
- Developing LDAP client components for visual development environment (Principle-35: Parameter change).

Reference to patents:


**Other references:**


