Inventions on LDAP data storage- A study based on US patents

Umakant Mishra
## Contents

Contents .................................................................................................................................................. 1  
1. Introduction ........................................................................................................................................ 2  
2. Study on LDAP data storage .............................................................................................................. 2  
  2.1 Objectives of the study ................................................................................................................ 2  
  2.2 Major areas of Invention .............................................................................................................. 2  
  2.3 Patents analyzed for the study ....................................................................................................... 3  
3. Data storage mechanism in LDAP .................................................................................................... 3  
4. Inventions on LDAP data storage ..................................................................................................... 4  
  4.1 Data mapping in RDBMS for searching LDAP data ....................................................................... 4  
  4.2 Data security in LDAP service ....................................................................................................... 5  
  4.3 Storing Object Oriented LDAP data in RDBMS ......................................................................... 6  
  4.4 Data replication for LDAP ............................................................................................................ 7  
  4.5 Storing sparse hierarchical ACL data in RDBMS for LDAP ........................................................ 8  
5. Other related inventions .................................................................................................................... 8  
6. Summary and Findings of the study ................................................................................................. 9  
  6.1 Distribution of patents .................................................................................................................. 9  
  6.2 Hot areas in LDAP data storage .................................................................................................. 10  
  6.3 Trends of evolution in LDAP storage .......................................................................................... 10  
Reference to patents: .............................................................................................................................. 11  
Other references: ..................................................................................................................................... 11
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.¹

2. Study on LDAP data storage

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

2.1 Objectives of the study

- What are the inventions made on LDAP data storage and on which aspects of data storage?
- Is there any trend in the series of inventions?
- Which problems on LDAP data storage are not solved yet? In other words which problems need to be addressed in future?
- Which aspects of LDAP data storage are yet unexplored? What are the possible areas of improvements in future inventions?

2.2 Major areas of Invention

- One major area that attracts the inventors is to find mechanism of storing hierarchical LDAP data in relational database structure. Similar attempts are also made to store ACL data, semi-structured data and various other types of data into LDAP with RDBMS as backing store.

- The other area that attracts the inventors is to create special tables, such as index tables, catalog tables etc. in order to increase the efficiency in data processing, searching and other activities.

- Yet another area that attracts inventors is to find the compatibility of different types of databases used for LDAP storage. This involves conversion from one type of storage to other, data transfer and replication etc. basically by using plug-ins, translators, brokers, data independent formats etc.

2.3 Patents analyzed for the study

- “Method of hierarchical LDAP searching with relational tables” (US Patent 6085188)

- “Method for securing sensitive data in a LDAP directory service utilizing a client and/or server control” (US Patent 6339827)

- “Method and system for representing and accessing object-oriented data in a relational database system” (US Patent 6587856)

- “Method and system for data replication” (US Patent 6615223)

- “Method for storing sparse hierarchical data in a relational database” (US patent 6438549).

3. Data storage mechanism in LDAP

As LDAP does not provide any specification on the data storage, different vendors can implement different mechanism for data storage as found suitable to the specific vendor or environment. Although underlying data storage system between different LDAP servers can differ, this disparity does not affect the functionality or interaction of LDAP clients. LDAP protocol does not expose this disparity in data storage to the LDAP clients or users of LDAP interface.

For example, an LDAP server may store data in a Flat file, or in RDBMS. The LDAP client applications such as LDAP enabled web browsers like Netscape communicator and Internet Explorer can use LDAP directory interface without having knowledge on the underlying data storage mechanism.
The above model highlights the following major functions of LDAP. The LDAP server stores the directory information in a database. It provides the capability for directory information to be queried or updated. It offers a rich set of searching capabilities. The client makes a TCP/IP connection and sends requests to an LDAP server. Simple as a web server, the LDAP server responds to the requests of LDAP clients. LDAP servers provide their service using a default port 389.

4. Inventions on LDAP data storage

There are not many inventions on data storage and management specifically for LDAP database. The above six patents were found to be more relevant to this topic out of the 60 patents analyzed for the study.

The reason for not having many patents on LDAP data storage is not because of its less importance. Rather a large number of patents are issued on database management in general. Although all those inventions on database management holds good for LDAP scenario, they don’t mention about “LDAP” in their documentation.

However, we will not analyze all those inventions on database management in the present study. We will consider only those inventions that specifically mention about LDAP database.

4.1 Data mapping in RDBMS for searching LDAP data

Background Problem:
As LDAP protocol does not specify about a data storage mechanism for the LDAP server, different vendors implement different mechanisms to store the tree structure. The query language (such as SQL) used by different vendors also differs to some extent. However all these query mechanisms end up using recursive queries to handle hierarchical structures in LDAP entries. Recursive queries do not work efficiently with large number of records in RDBMS. There is a need for a better data organization for faster searching.
Solution provided by US Patent 6085188:
US Patent 6085188 discloses a method of organizing hierarchical LDAP data to be stored in a relational database used as a backing store for LDAP. The invention proposes to add two more relational tables in the LDAP database. These two tables store the unique identifier of all the parents and of all the children, and stores entries for parent child relationship.

According to the invention, these two tables of parent child relationship enhance the performance of searching. When a query comes from the client, the query does not search recursively search the hierarchical LDAP directory, rather searches these relationship tables first. The query can easily find the relationships from these relationship tables as they already store the relationship entries. This method of storing data tables improves performance of LDAP searching.

4.2 Data security in LDAP service

Background Problem:
The LDAP directory stores various data on users, computers and various other objects in the network. It also stores confidential data as well. Unfortunately, the present implementation of LDAP does not have a security mechanism. The data is stored in clear-text form or in “as is” format. This is not suitable to store confidential data such as passwords. There is a need to provide security to store and retrieve sensitive data in LDAP.

Solution by US Patent 6339827
US Patent 6339827 discloses a method of maintaining security in a directory service. As per the invention the lightweight directory access protocol (LDAP) is extended to include two controls, one client-control and one server-based control for securing sensitive data in the directory service.
According to the invention, the client control is to be implemented on a client machine, and/or the server control is to be implemented on the server machine. The client control will comprise a control block including identification information, a signature control block and a digital signature. This provides security to the sensitive data provided from a client application to the directory service. The server side control similarly includes necessary controls to provide security for the data within the directory service.

The invention is flexible to activate either client-control or server-control or both. In other words, it is not required to have both client and server controls to be implemented together. A client machine may implement the client control irrespective of whether a server involved in the directory operation is running the server control.

4.3 Storing Object Oriented LDAP data in RDBMS

**Background problem**
RDBMS is a good choice for storing LDAP data. It provides advanced database transactions, data consistency, recovery etc. It is also designed to interoperate with standard SQL to access and modify data. But object oriented data (like LDAP data) are different in structure than relational data and hence not suitable to be stored in a relational database. In order to store object oriented data in RDBMS, a separate table is provide for each object class, which causes waste of system resources. Besides it also makes the system rigid, as each change in the object class requires a modification in the database schema. There is a need for an improved method for storing object oriented LDAP data in RDBMS.

**Solution provided by US Patent 6587856**
US Patent 6587856 presents a method of storing and accessing object-oriented data in a relational database. The invention uses catalog tables that correlate object identification numbers to specific attribute values.

According to the invention, there will be a table called “attribute_store table” containing the information describing objects and object attributes of the system. Secondly, there will be “catalog tables” which store indexes to the “attribute_store table”. A separate catalog table is maintained for each attribute type that is indexed. These catalog tables improves efficiency in searching. Thirdly there will be “distinguished_name table” that stores identification information for objects.

The invention is also expanded further in US Patent 6834286, which is a continuation of the above patent 6587856.
4.4 Data replication for LDAP

Background problem
Data replication is used to maintain multiple copies of the same database in a distributed database system. Data replication improves performance of data access as an application can access the logically “closest” copy of the data, reduces minimize network traffic and provides fault tolerance.

However, the conventional methods of data replication are not suitable for replication of LDAP data. The addition or deletion of replication nodes in a conventional LDAP system often results in system downtime to implement configuration changes.

The other limitation of traditional replication method is that it does not work in a heterogeneous environment where the replication site may have a different schema for its database. There is a need for an efficient replication system for LDAP replication.

Solution provided by US Patent 6615223
US Patent 6615223 discloses a method of data replication for LDAP servers. According to the invention, when the first server will receive a change request it will change the data in that site. Then it will generate a change record in a schema independent format and send it to the second replication site. The second replication site will implement the corresponding changes in that site.

```
<table>
<thead>
<tr>
<th>Format independent change record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
</tr>
<tr>
<td>LDAP database</td>
</tr>
<tr>
<td>Change request at the First site</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Format independent change record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
</tr>
<tr>
<td>LDAP database</td>
</tr>
<tr>
<td>Replication at the second site</td>
</tr>
</tbody>
</table>
```

This method of data replication works fine even in heterogeneous environments as change records are transferred in a schema independent format. The method supports addition, deletion, and modification of data to be replicated in a distributed environment.
4.5 Storing sparse hierarchical ACL data in RDBMS for LDAP

Background problem
Security for LDAP is provided through ACLs (Access Control Lists). The ACL contains the information about distinguished names and their access rights. According to ACL requirements, every entry must have an owner and at least one ACL. The Access Control List (ACL) data is sparse hierarchical in structure. In past, such hierarchical data was stored in an editable flat file as it is difficult to manage within a relational database.

However in many cases RDBMS is used as the backing store for LDAP. It would be desirable to store ACL data in a relational database in order to store that data in LDAP.

Solution provided by US Patent 6438549
US Patent 6438549 discloses a method of securing sparse access control list (ACL) data in a relational database used as a backing store for LDAP. According to the invention the ACL data is stored in multiple tables, such as an owner table, a propagation table, a permissions table and a source table. The method reduces the activities involved in searching and updating ACL.

5. Other related inventions

Online directory service with multiple database
US patent 5918227 discloses a method of accessing multiple directory databases though a “gater” or intermediate computer. The first gater receives the requests and passes them to other gaters. The gaters communicate between themselves to access various LDAP databases and reply to the client directly independent of the first gater.

Data migration for LDAP
US Patent 6915287 discloses a method and software tool that is useful to migrate data from LDAP directory to another LDAP directory where the schemas for the two directories are not the same. The tool first compares the schema of a source directory to the schema of the destination directory. Then it updates the schema of the destination directory to be compatible with the source directory’s schema.
Providing extended Access Control to LDAP Protocol
US Patent 6633872 provides a method of providing extendible access control to LDAP protocol. The extendible ACL can be implemented as a plug-in within the scope of LDAP server. According to the method, the user is associated with an access control group and the LDAP operation is reformatted based on the access rights of his access control group.

Reverse indexing LDAP database for faster searching
US Patent 6199062 discloses a method to speed up wildcard searching in an LDAP directory using RDBMS. The RDBMS normally includes a forward index, which is not efficient for wildcard (“*”) searching. The invention uses a reverse index of the character strings in the relational database. In case of general searching it uses the forward index, whereas in case of wildcard searching it uses the reverse index to speed up the search.

LDAP cache mechanism
US Patent 6347312 discloses a method of faster searching of LDAP data in RDBMS. The invention uses a cache to store the search results retrieved in response to the search queries. The invention uses two sets of caches. The first cache receives a set of identifiers indexed by a filter key of the search query. The second cache stores the search results corresponding to the set of identifiers in the first cache. When the same queries come again and again, the LDAP server serves the results from the cache instead of sending requests to the backend database.

6. Summary and Findings of the study

6.1 Distribution of patents
- There are very few inventions related to data storage for LDAP. Only five patents were found to be more relevant and five other were found to be less relevant to this topic. All of them are presented above in this article.

(Note: As mentioned above, the reason for not having many patents on LDAP data storage is not because of it's less importance. Rather a large number of patents are issued on database management in general. Although all those inventions on database management holds good for LDAP scenario, they are not included in this study.)

- Most patents on LDAP data storage (covered under the study) are found to be assigned by either International Business Machines or Oracle International Corporation.)
6.2 Hot areas in LDAP data storage

The analysis finds that the inventions try to improve the following aspects of LDAP system.

- Improve the method of storing for faster searching and updates.
- Storing Object Oriented directory data in Relational Database.
- Implementing various mechanisms to RDBMS to make efficient for LDAP backing store.
- Implementing security for LDAP data.
- Possibility of storing various types data (of different nature and structure) into the directory database.
- Improving data maintainability. Maintaining data consistency in large distributed environments.
- Implementing methods for data replication, duplication, backup etc.

6.3 Trends of evolution in LDAP storage

The following trends are prominent among the inventions on LDAP data storage.

- Increasing speed in LDAP data access- Inventions want to store data in such a way that will support faster searching.
- Increasing controllability in LDAP service- Inventions tend to increase data integrity, data maintainability, data backup and replication, data security and such other features to improve control of LDAP service.
- Increasing easiness to “configure and implement” and increasing easiness to “maintain and administer” are two obvious trends.
- Increasing standardization- Inventions are looking for Increasing interoperability to facilitate integration with other systems, databases or services, supporting conversion and migration.
Reference to patents:


Other references:


About the author

After working for more than 18 years in various fields of Information Technology Umakant is currently doing independent research on TRIZ and IT since 2004. He last worked as Director and Chief Technology Officer (2000-2004) in CREAX Information Technologies (Bangalore). Before that he worked as IS/IT manager (1996-2000) for ActionAid India (Bangalore).

Umakant is a Master in Philosophy (MA), Master in Business Administration (MBA), Bachelor in Law and Logic (LLB), Microsoft Certified Systems Engineer (MCSE+I), Certified Novel Engineer (CNE), Master Certified Novell Engineer (MCNE), Certified Intranet Manager (CIM), Certified Internet Professional (CIP), Certified Software Test Manager (CSTM) and holds many other global IT certifications.