SAMBA OPENLDAP: AN EVOLUTION AND INSIGHT

Ayodele Nojeem Lasisi
Faculty of Information and Communication Technology
International Islamic University, P.O. Box 10, 50728
Kuala Lumpur, Malaysia

Musibau Akintunde Ajagbe
Faculty of Management and Human Resource Development
Universiti Teknologi Malaysia, 81310 Skudai Johor-Malaysia

Abstract--Directory services facilitate access to information organized under a variety of frameworks and applications. The Lightweight Directory Access Protocol is a promising technology that provides access to directory information using a data structure similar to that of the X.500 protocol. IBM Tivoli, Novell, Sun, Oracle, Microsoft, and many other vendor features LDAP-based implementations. The technology's increasing popularity is due both to its flexibility and its compatibility with existing applications. A directory service is a searchable database repository that lets authorized users and services find information related to people, computers, network devices, and applications. Given the increasing need for information — particularly over the Internet — directory popularity has grown over the last decade and is now a common choice for distributed applications. Lightweight Directory Access Protocol (LDAP) accommodates the need of high level of security, single sign-on, and centralized user management. This protocol offers security services and integrated directory with capability of storage management user information in a directory. Therefore at the same time the user can determine application, service, server to be accessed, and user privileges. It is necessary to realize files sharing between different operating systems in local area network. Samba software package, as the bridge across Windows and Linux, can help us resolve the problem. In this paper, we try to explore previous literature on this topic and also consider current authors work then come out with our views on the subject matter of discussion based on our understanding.

Keywords: OPENLDAP; Evolution; UNIX; Samba

1.0 Introduction

LDAP, each web-based application can be united using single identification of user information stored in the directory of LDAP server. Recent development in the business and communication world has been acknowledged to be a result of the advancement of the internet technology which has brought positive impact in all sectors of human endeavor. This development also supports the progress of web-based applications required by government institutions, private sectors and education institutions across the globe. Considering the current trend where web based applications is used for business activities, and security level, user's identification requirement became one of the major preoccupations. Client server applications on web server started to be used widely and growing fast. Data confidentially and user authentication became more and more important. Access to web applications which is connected to LAN or single host will attract other parties which have no access to the network and application to enter the application. Therefore, mechanism to identify users which have privilege to access the application is needed. However, in line with the growing number of web server applications, each application will need to authenticate user or member. Therefore the user will have a lot of username and pass word to remember, this will complicate the user. For the simplification purpose, the authentication method for user by using Lightweight Directory Access Protocol (LDAP) has been introduced in 1993 [1].This method accommodates the need of high level of security, single sign-on, and centralized user management which offers services of security and integrated directory specially with capability of storing and managing user information in a directory. Therefore at the same time the user can determine application, service and server that need to be accessed at his own privilege.

With this authentication method by using The user can access every application easily without having to remember more than one username or password as well as privilege to users according to the existing information on the LDAP server.

The use of a single platform restricts users' choice of suitable application software. This is especially clear in academic, engineering, and other IT intensive enterprise domains, where in recent years UNIX and its descendants have expanded their application range while Windows clients and servers still keep their positions and popularity in the market. In order to maximize the users' freedom of choice it is inevitable to introduce multiplatform enterprise systems. However, this poses significant integration problems such as differences in authentication mechanisms and incompatibility of storage sharing technologies [2, 3]. It is difficult in integrating authentication information and user's data storage for both Windows and UNIX environment. This is because both Windows and

UNIX have different models and use different technologies for implementing them. Authentication in a Microsoft Windows domain environment makes use of NT Domain Controller or Active Directory, and Common Internet File System (CIFS)/Server Message Block (SMB) protocol for shared resources such as data storage and print services. Whereas, authentication in a UNIX system uses Network Information System (NIS) or LDAP, and Network File System (NFS) is used for sharing data storage. The two technologies are incompatible. Basically, the change of a password or data in one of the systems is not reflected in the other and as a result, users are often confused in the heterogeneous environment of Windows and UNIX. This article is arranged as follows. We will do an in-depth literature review about LDAP directory service, LDAP authentication, LDAP working system, and system architecture hierarchical, samba server types and features then we conclude on our findings and make some few recommendations.

2.0 Survey of Previous Studies

The implementation of OpenLDAP and Samba has been carried out by various system administrators and researchers and has proved to have worked. Both OpenLDAP and Samba have been implemented together, with other applications or independently as the case maybe. Before going through the relevant literatures, a brief insight into what OpenLDAP and Samba is described. Samba is a free software re-implementation of SMB/CIFS networking protocol, originally developed by Australian Andrew Tridgell [4]. Samba provides file and print services for various Microsoft Windows clients and can integrate with a Windows Server domain, either as a Primary Domain Controller (PDC) or as a domain member as of version 3 [4,5]. It can also be part of an Active Directory.

OpenLDAP is an open source implementation of the LDAPv2 and LDAPv3 protocols used to access centrally stored information over the network [6, 5].

Mentioned below are some of the important features of OpenLDAP;

- *LDAPv3 Support*: OpenLDAP supports Simple Authentication and Security Layer (SASL), Transport Layer Security (TLS), and Secure Sockets Layer (SSL), among other improvements. Many of the changes in the protocol since LDAPv2 are designed to make LDAP more secure.

- *LDAP Over IPC*: OpenLDAP can communicate within a system using inter-process communication (IPC). This enhances security by eliminating the need to communicate over a network.

- *Updated C API*: Improves the way programmers can connect to and use LDAP directory servers.

- *LDIFv1 Support*: Provides full compliance with the LDAP Data Interchange Format (LDIF) version 1.

- *Enhanced Stand-Alone LDAP Server*: Includes an updated access control system, thread pooling, better tools, and much more.

Famous authors such as [3, 7] in their work "Integrating Network Services of Windows and Unix for Single Sign-On", describe a resource sharing scheme which unifies authentication information and users' data storage on Windows and Unix services, using LDAP and Samba suite. The result is a reduction in the administrative cost of running a mixed Windows and UNIX network services.

More researchers [8, 9, 10, 11] based on the network environment and demand for Secondary and Elementary school in Taiwan used Openldap to integrate common used service authentication systems in which Samba is one of them. The others were FTP and Open Webmail Account [8, 7].

In the realization of file sharing between Linux and Windows based on Samba [12], he introduces SMB protocol and Samba configuration, the method of how to realize reversible files sharing between Linux and Windows based on software packages were used.

Swanson and Lung [6] also implemented together Samba and OpenLDAP; they declared the use of OpenLDAP as the core directory service for a mixed environment. The LDAP server provides a shared e-mail directory, login for Linux and Microsoft Windows clients, auto mount of home directories and file sharing for all clients.

OpenLDAP was deployed as a stand-alone server. In that study, it was described how architecture, key data structures, and proposed methods of enhancing interoperability and performance of their component matching implementation in the OpenLDAP open source directory software suite. They researchers proposed the use of component matching in-online certificate validation and in Web services security and show that LDAP component matching implementation exhibits the same or higher performance [5].

Qadeer et al [13] presented in their paper the technique to manage user profiles and authentication using LDAP.The Lightweight Directory Access Protocol is an open industry standard that's gaining wide acceptance as a directory-access method. As the name suggests, LDAP is the lightweight version of the Directory Access Protocol and is a direct descendent of the heavyweight X.500, the most common directory-management protocol. Although they use a similar structure for data representation, LDAP and X.500 have several fundamental differences [14, 15].

• LDAP operates over the TCP/IP stack, whereas X.500 uses the OSI stack.

• LDAP's protocol element encoding is less complex than that of X.500.

• Each LDAP server uses a referral mechanism.

Many software vendors support LDAP due to its flexibility and the fact that it integrates with an increasing number of data retrieval and management applications. LDAP is thus an evolving ground for research on new and existing data management practices.

2.1 LDAP Overview

Recently, numerous LDAP-based servers have been commercialized, ranging from mega-scale public servers such as BigFoot and Infospace to small, workgroup-based LDAP servers. In between are the several educational institutions and private organizations that have installed and configured directory servers to provide information about faculty, staff, and students in a way that works with the organizations' mail service, authentication systems, and application- and resource-access control. Data typically stored under LDAP includes configuration files for network device drivers, user entries, application preferences, user certificates, and access control lists.LDAP's flexibility lets administrators create new attributes that can better serve their applications. With mail services, for example, a typical LDAP entry might contain attributes such as the mailLocalAddress, mailHost.UserCertificate (which stores the user's certificate in binary form), ipLoginPort, and ipLoginHost (for when the user makes a dial-up connection).

2.1.1 LDAP Directory

LDAP directories are databases arranged as hierarchical information trees representing the organizations they describe. Today, many companies support LDAP-based directory services, and the directory market is becoming quite competitive. Standalone directory vendors such as IBM Tivoli, Novell, Sun Microsystems, Oracle, and Microsoft feature mature and effective LDAP-based implementations with robust multivendor integration capabilities [10]. OpenLDAP, a suite of open-source directory software, is becoming competitive with these commercial directory servers as well.

2.1.2 LDAP Evolution

LDAP is currently in version 3, and we expect its ongoing evolution to address interconnection with X.500 directory services and thus facilitate the construction of a global Internet directory [16]. Meta directories, which manage integration and data flow between directory servers, offer one step toward the "marriage" of X.500 and LDAP servers. Many LDAP vendors, including Sun, Novell, and Microsoft, support metadirectories, and such support seems to be a trend for LDAP-based applications.
LDAP data management, particularly storage and retrieval, could improve significantly by tuning XML's integration with LDAP. Earlier efforts in XML data caching using the LDAP framework support this trend. As an example, HLCaches, an LDAP-based hierarchical distributed caching system for semi-structured documents, has shown promising improvements by integrating caching in an XML- and LDAP-tuned environment [16, 17]. This approach implemented an XMLDAP cache based on the OpenLDAP server and showed that the average access times have improved in comparison to more conventional caching schemes. Current LDAP momentum is quite promising in terms of an Internet-wide LDAP adoption for data management frameworks involved in querying, indexing, caching, and security.

2.1.3 LDAP Working System

The working mechanism of LDAP is similar to X.500, due to the fact that it is based on a client-server model. Query process from client also similar with the method in X.500. To make a query, client will send an identifier (Relative Distinguish Name) which will take the attributes. Client transmits that query packet over TCP/IP, and the server will be looking for identifier on LDAP Directory Information Tree (DIT) which is stored on LDAP server. When it is found, the result will directly be sent back to the client's computer. But if not found, the result is a pointer to other LDAP server that can be accessed to find the information required by client [18].

2.2 SAMBA

Samba came to the rescue in solving this confusion with users about Windows and UNIX. Samba is an open source suite that provides seamless data storage sharing and print services to CIFS/ SMB clients, and enables computers running UNIX to get in on the action, communicating with the same networking protocol as Microsoft Windows and appearing as another Windows system on the network from the perspective of a Microsoft Windows client [19, 17]. An LDAP server manages authentication and configuration information for a variety of services. Each service asks information via its LDAP module to that LDAP server, and authenticates. OpenLDAP is used for this purpose [10, 18].
It would be suitable and useful as a source of reference for small and medium scale enterprise [20] looking for an alternative solution for the highly costly solutions from IT providers [3, 17].
Samba benefits are:

- Single authentication for both Windows and UNIX
- Access to files and data in both platforms
- Flexibility leading to ease of sharing resources

OpenLDAP benefits are:

- Very fast reads
- Flexible data types
- Nearly universal application support
- Fine-grained control over access to data
- Distributed storage and replication

Figure 1 below shows a Windows domain environment by using Samba with LDAP. It consists of three kinds of Samba servers, a Primary Domain Controller, a Backup Controller, and a Domain Member Server.

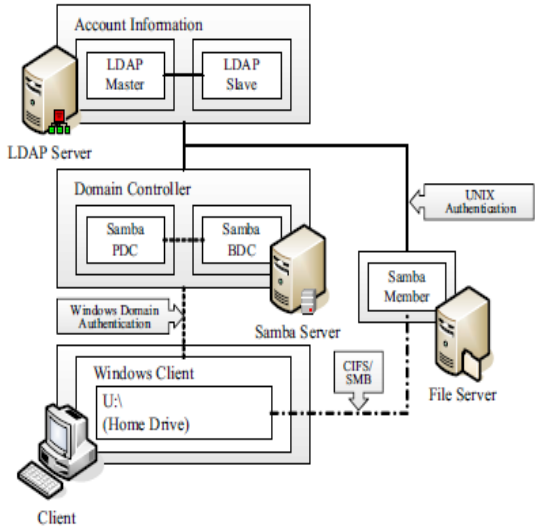

Figure 1. Samba Domain Controller with LDAP [3]

2.2.1 Samba Server Types

Samba server types can be configured in three different ways namely, Standalone server, Domain Member and Domain Controller.

2.2.1.1 Standalone server

Standalone servers are independent of domain controllers on the network [21, 19, 17]. They are not domain members and function more like workgroup servers. In many cases a standalone server is configured with a minimum of security control with the intent that all data served will be readily accessible to all users.

The term standalone server means that it will provide local authentication and access control for all resources that are available from it. In general this means that there will be a local user database. In more technical terms, it means resources on the machine will be made available in either share mode or in user mode [22, 21, 23].

No special action is needed other than to create user accounts. Standalone servers do not provide network logon services. This means that machines that use this server do not perform a domain logon to it. Whatever logon facility the workstations are subject to is independent of this machine. It is, however, necessary to accommodate any network user so the logon name he uses will be translated (mapped) locally on the standalone server to a locally known user name [22,19].

- Features and Benefits

Standalone servers can be as secure or as insecure as needs dictate. They can have simple or complex configurations. Above all, despite the hoopla about domain security, they remain a common installation. If all that is needed is a server for read-only files or for printers alone, it may not make sense to effect a complex installation. For example, a drafting office needs to store old drawings and reference standards. None can write files to the server because it is legislatively important that all documents remain unaltered. A share-mode read-only standalone server is an ideal solution [22, 24].

Another situation that warrants simplicity is an office that has many printers that are queued off a single central server. Everyone needs to be able to print to the printers, there is no need to effect any access controls, and no files will be served from the print server. Again, in this case a share-mode standalone server makes a great solution [21].

2.2.2.2 Domain Member

Samba must be able to participate as a member server in a Microsoft domain security context, and Samba must be capable of providing domain machine member trust accounts; otherwise it would not be able to offer a viable option for many users [21, 23].

- Features and Benefits

MS Windows workstations and servers that want to participate in domain security need to be made domain members. Participating in domain security is often called Single Sign-On (SSO)- [22,24].

Samba can join an MS Windows NT4-style domain as a native member server, an MS Windows Active Directory domain as a native member server, or a Samba domain control network. Domain membership has many advantages:

- MS Windows workstation users get the benefit of SSO.
- Domain user access rights and file ownership/access controls can be set from the single Domain Security Account Manager (SAM) database (works with domain member servers as well as with MS Windows workstations that are domain members).
- Only MS Windows NT4/200x/XP Professional workstations that are domain members can use network logon facilities.
- Domain member workstations can be better controlled through the use of policy files (NTConfig.POL) and desktop profiles.
- Through the use of logon scripts, users can be given transparent access to network applications that run off application servers.

- Network administrators gain better application and user access management abilities because there is no need to maintain user accounts on any network client or server other than the central domain database (either NT4/Samba SAM-style domain, NT4 domain

that is back ended with an LDAP directory, or via an Active Directory infrastructure) [22,23,25].

2.2.2.3 Domain Controller

Samba can act as either a Primary Domain Controller (PDC) or Backup Domain Controller (BDC).
The Primary Domain Controller or PDC plays an important role in MS Windows NT4. In Windows 200x domain control architecture, this role is held by domain controllers. In the case of MS Windows NT4-style domains, it is the PDC that initiates a new domain control database. This forms a part of the Windows registry called the Security Account Manager (SAM). It plays a key part in NT4-type domain user authentication and in synchronization of the domain authentication database with BDCs [22, 17].
The following are necessary for configuring Samba as an MS Windows NT4-style PDC for MS Windows NT4/200x/XP clients:

- Configuration of basic TCP/IP and MS Windows networking.
- Correct designation of the server role (security = user).
- Consistent configuration of name resolution.
- Domain logons for Windows NT4/200x/XP Professional clients.
- Configuration of roaming profiles or explicit configuration to force local profile usage.
- Configuration of network/system policies.
- Adding and managing domain user accounts.
- Configuring MS Windows NT4/2000 Professional and Windows XP Professional client machines to become domain members.

The following provisions are required to serve MS Windows 9x/Me clients [23,24]:

- Configuration of basic TCP/IP and MS Windows networking.
- Correct designation of the server role (security = user).
- Network logon configuration (since Windows 9x/Me/XP Home are not technically domain members, they do not really participate in the security aspects of Domain logons as such).
- Roaming profile configuration.
- Configuration of system policy handling.
- Installation of the network driver "Client for MS Windows Networks" and configuration to log onto the domain.
- Placing Windows 9x/Me clients in user-level security - if it is desired to allow all client-share access to be controlled according to domain user/group identities.
- Adding and managing domain user accounts.

Samba can act as a Backup Domain Controller (BDC) to another Samba Primary Domain Controller (PDC). A Samba PDC can operate with an LDAP account backend. The LDAP backend can be either a common master LDAP server or a slave server. The use of a slave LDAP server has the benefit that when the master is down, clients may still be able to log onto the network. This effectively gives Samba a high degree of scalability and is an effective solution for large organizations. If you use an LDAP slave server for a PDC, you will need to ensure the master's continued availability – the slave finds its master down at the wrong time, you will have stability and operational problems [10, 11, 2].
While it is possible to run a Samba BDC with a non-LDAP backend, that backend must allow some form of "two-way" propagation of changes from the BDC to the master. At this time only LDAP delivers the capability to propagate identity database changes from the BDC to the PDC. The BDC can use a slave LDAP server, while it is preferable for the PDC to use as its primary an LDAP master server [22, 26].

2.3 Other Implementation of LDAP

LDAP has some popular implementations namely:

- OpenLDAP, an open LDAP suite (Discussed).
- Novell's NetWare Directory Service (eDirectory).
- Microsoft's Active Directory.
- iPlanet Directory Server (This was split between Sun and Netscape a while back. Netscape Directory Server has since been acquired by Red Hat, which has, in turn, released it to the open source community.).
- IBM's SecureWay Directory.

2.3.1 Novell's NetWare Directory Service (eDirectory**):**

Also called Novell eDirectory. It is an X.500 compatible directory service software product initially released in 1993 by Novell, Inc. for centrally managing access to resources on multiple servers and computers within given networks [27].

- Features

Novell Directory Services is a hierarchical, object oriented database that represents all the assets in an organization in a logical tree [27]. Assets can include people, positions, servers, workstations, applications, printers, services, groups, etc. the use of dynamic rights inheritance and equivalence allows both global and fine grained access controls to be implemented efficiently. Access rights between objects in the tree are determined at the time of the request and are determined by the rights assigned to the objects by virtue of their location in the tree, any security equivalences and individual assignments. eDirectory supports partitioning at any point in the tree and replication of that partition to any number of servers. Replication between each server occurs periodically using deltas of the objects to reduce LAN/WAN traffic. Each server can act as a master of the information it holds (providing the

replica is not read only). Additionally, replicas may be filtered to only include defined attributes to increase speed.
It supports platforms such as Windows 2000, Windows Server 2003, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, Novell NetWare, Sun Solaris, IBM AIX and HP-UX [28, 27, 25].

2.3.2 Microsoft's Active Directory**:** Active Directory is a technology by Microsoft that provides a variety of network services including LDAP-like directory services, Kerberos-based authentication, DNS-based naming and other network information [25]. Using the same database, for use primarily in Windows environments, Active Directory also allows administrators to assign policies, deploy software, and apply critical updates to an organization. Active Directory stores information and settings in a central database. Active Directory networks can vary from a small installation with a few computers, users and printers to tens of thousands of users, many different domains and large server farms spanning many geographical locations [25].

2.3.3 iPlanet Directory Server: It is a product brand that was used jointly by Sun Microsystems and Netscape Communications Corporation when delivering software and services as part of a non-exclusive cross marketing deal that was also known as "A Sun/Netscape Alliance" [29].

2.3.4 IBM's SecureWay Directory**:** The IBM SecureWay Directory is billed as a highly scalable, cross-platform LDAPv2 and LDAPv3 directory server that runs on IBM AIX, OS/400, OS/390, Sun Solaris, and Windows NT [30]. It is standard based and complies not only with the Internet Engineering Task Force (IETF) LDAP RFCs but also with the Network Application Consortium's Lightweight Internet Person Schema (LIPS) and the Management Task Force Common Information Model schema, which incorporates the Directory Enabled Networks (DEN) schema [30].

3.0 Virtualization

Virtualization allows for multiple virtual machines, each with its own operating systems running in a sandbox, shielded from each other, all in one physical machine. Each virtual machine shares a common set of hardware, unaware that it is also being used by another virtual machine at the same time [31, 17].
In addition to using virtualization technology to partition one machine into several virtual machines, it can be used to combine multiple physical resources into a single virtual resource. An example of this is the storage virtualization, where multiple network storage resources are pooled into what appears as a single storage device for easier and more efficient management of these resources [32, 17].
Other types of virtualization include:

- *Network Virtualization:* splits available bandwidth in a network into independent channels that can be assigned to specific servers or devices.
- *Application Virtualization:* separates applications from the hardware and the operating system, putting them in a container that can be relocated without disrupting other systems.
- *Desktop Virtualization:* enables a centralized server to deliver and manage individualized desktops remotely. This gives users a full client experience, but let IT staff provision, manage, upgrade and patch them virtually, instead of physically [32].

Server virtualization software allows you to run multiple guest computers on a single host computer with those guest computers believing they are running on their own hardware [17]. By doing this, you gain all the benefits of any type of virtualization:

- Portability of guest virtual machines,
- Reduced operating costs,
- Reduced administrative overhead,
- Server consolidation,
- Testing & training,
- Disaster recovery benefits and more.

Example of server virtualization products are: VMware Server, Workstation, Player, and ESX Server; Microsoft Virtual PC and Virtual Server; Xen; Virtual Iron [33].
Network virtualization is the ability to refer to network resources logically rather than having to refer to specific physical devices, configurations or collection of related machines [34].

2.3.1 Virtual Networking Connection Options

There are basically three networking connection options that can be created in a virtual environment namely Bridged networking, Network Address Translation (NAT) and Host-Only networking [35].

2.3.1.1Bridged Networking

Although bridged virtual machines use the physical network connections on the host system, each virtual machine is treated as an independent client on the network. As such it will obtain an IP address from the network's DHCP server, or will require a static IP address to be manually configured if DHCP is not used. Virtual machines using bridged networking will be able to communicate directly with both the host system and other clients on the network to which the host is connected [35, 36].

3.1 Network Address Translation

One or more virtual machines share the IP and MAC address of the host system for the purposes of communicating with the external network. Virtual machines are able to communicate with other clients on the network to which the host is connected, but will appear to those clients as the host system, rather than as individual network clients. This approach allows multiple virtual machines to operate using a single IP address. IP addresses are allocated dynamically to NAT based virtual machines by VMware Server's internal DHCP server. Communication with the external network can only be established by the virtual machine. It is not, therefore, possible for a client on the

external network to initiate a connection with a NAT based virtual machine (although *port forwarding* may be configured to allow traffic to a particular port, such as HTTP traffic on port 80, to be directed to a specific virtual machine) [35,36].

4.0 Host-Only Networking

Host-Only networking creates a private sub-net within the host for virtual machines for which no external network access is required or desired. Virtual machines configured with host-only networking can communicate directly only with the host system and virtual machines which are also members of the same host-only network. The virtual machines cannot, however, communicate with the network to which the host is connected. IP addresses are allocated to Host-only based virtual machines by VMware Server's internal DHCP server [35, 36].

The general representation of virtualization is depicted in Figure 2 below.

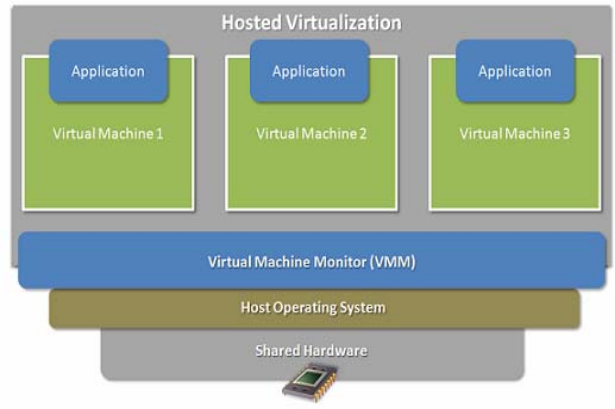

Figure 2. Hosted virtualization architecture, virtual machine monitor (VMM) software is installed on a host operating system

Generically speaking, in order to virtualize, you would use a layer of software that provides the illusion of a "real" machine to multiple instances of "virtual machines". This layer is traditionally called the Virtual Machine Monitor (VMM). VMM could itself run directly on the real hardware - without requiring a "host" operating system. In this case, the VMM is the (minimal) OS. VMM could be hosted, and would run entirely as an application on top of a host operating system. It would use the host OS API to do everything [37, 38, 39].

5.0 Conclusions and Suggestion for future research

Considering different empirical findings by various previous authors as represented in literature review both past and present, it was reported that virtualization allows for multiple virtual machines to run on a single physical machine, sharing the resources of that single computer across multiple environments. Different virtual machines can run different operating systems and multiple applications on the same physical computer. Lasisi [17] also reported that the implemented Samba OpenLDAP in a simulated environment has the capability of having two virtual operating systems, Linux and Windows installed on a single machine. The Samba suite and OpenLDAP were installed on Linux with the Windows serving as the clients for accessing and sharing files in Linux. This setup leads to a reduction in the amount of hardware that is required for installation and potentially reducing the amount of physical space needed with a reduction on cost. Findings in previous literature also indicated that based on performance test, Samba reveal that as the number of query increases, the CPU power remaining decreases, the Memory usage increases moderately and a cross-point was found indicating the maximum queries (at 270) that can be sent to the server.

The integration of Microsoft Windows and UNIX through the use of Samba (which implements Single Sign-On) and OpenLDAP usually permit for the provision of a resource sharing scheme, which unifies authentication information and users' data storage on multiplatform and other network services. This effort resulted in the vast reduction in the administrative cost of running a mixed Windows and UNIX network services. Users' convenience improves and the new integrated system also shows the flexible extendibility to the future. This is also consistent with the report of [3] that with the use of open source software there no need for new software cost for this migration.

Considering the support of LDAP authentication method with the single sign-on mechanism which permits several server applications to authenticate using the same credential of the user on a centralized LDAP server directory. Results indicate that from a test bed the access time used by a user with credential and LDAP tend to get longer compared with if user access directly to database web server. Findings from empirical study show that access speed is inversely related with the access time required, although the access time is inversely related with the average packet/sec and throughput value on the network [40].Further report indicate that the performance of the LDAP authentication mechanism is based on the variation of different user or different location if analyzed from the programming code point of view.

6.0 REFERENCES

[1] XLNT Software, "Handling XML Documents Using Traditional Databases," Aug. 2002; www.surfnet.nl/innovatie/ surfworks/xml/xml-databases.pdf.

[2] Carter, G. (2003). LDAP System Administration. Sebastopol, CA: O'Reilly Media, Inc.

[3] J. Futagawa, Integrating Network Services of Windows and UNIX for Single Sign-On. International Conference Proceedings of Cyberworlds, 2004.

[4] A. Tridgell, Retrieved October 9, 2009, from http://samba.org/ftp/tridge/dbench/README.6

[5] S.S. Lim, H.J. Choi, D.K. Zeilenga, *Design and Implementation of LDAP Component Matching for Flexible and Secure Certificate Access in PKI*. 4TH PKI R&D Workshop, NIST, Gaithersburg MD. IBM Corporation, 2005.

[6] C. Swanson, and M. Lung, OpenLDAP Everywhere. Linux Journal, no. 135, 2005.

[7] H. Chu, *OpenLDAP 2.4 Highlights*. Symas Corp, 2007.

[8] C. Hung, C. Yang, *The Integration of Network Service Authentication Design and Implementation for Secondary and Elementary Schoo,2006l.*

[9] Samba Team, *Samba HOWTO Collection*, January 6, 2004.

[10] OpenLDAP, Retreived May 7, 2009, from http://en.wikipedia.org/wiki/OpenLDAP

[11] Manage OpenLDAP, Retrieved July 5, 2009, from http://ocw.novell.com/suse-linux- enterprise/upgrading-to-certified-linux-engineer-10/3076_11_manual.pdf, 2007.

[12] Z. Huili, Realization of Files Sharing between Linux and Windows based on Samba. *International Seminar on Future BioMedical Information Engineering. IEEE Computer Society, 2008.*

[13] A.M. Qadeer, M. Salim, S.M. Akhtar, Profile Management and Authentication using LDAP. *International Conference on Computer Engineering and Technology. IEEE Computer Society, 2009.*

[14] T.A. Howes, *The Lightweight Directory Access Protocol: X.500 Lite*, tech. report TR-95-8, Center for Information Technology Integration, Univ. of Michigan, 1995.

[15] M. Wahl, T. Howes, and S. Kille, "Lightweight Directory Access Protocol (v3)," IETF RFC 2251, Dec. 1997; www.ietf. org/rfc/rfc2251.

[16] P.J. Maron and G. Lausen, *HLCaches: An LDAP-Based Distributed Cache Technology for XML*, tech. report TR-147, Inst. for Computer Science, Univ. Freiburg, 2001.

[17] A.N. Lasisi, Samba Openldap Performance in a Simulated Environment. An unpublished thesis submitted to the Faculty of Information and Communication Technology, International Islamic University, Kuala Lumpur, Malaysia in partial fulfilment of the Award of Master of Information Technology, 2009.

[18] M. Salim, M. S. Akhtar, M. A. Qadeer, Second International Workshop on Knowledge Discovery and Data Mining*Data Retrieval and Security using Lightweight Directory AccessProtocol/IEEE pp.685-688,2009.*

[19] Server World. (n.d.). Build Network Server. Retrieved August 2, 2009, from http://www.server-world.info/en/

[20] M.A. Ajagbe, K. Ismail, S.A. Aslan, and L.S. Choi, Investment in Technology Based Small and Medium Sized Firms in Malaysia: Roles for Commercial Banks. International Journal of Research in Management and Technology (IJRMT), vol.2, no.2, pp.147-153, 2012.

[21] H.J. Terpstra, Standalone Servers. Retrieved November 14, 2009, from http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/StandAloneServers.html, 2003.

[22] H.J. Terpstra, J. Allison, J.G. Carter, A. Tridgell, R.J. Vernooij, and G. Deschner, Domain Membership. Retrieved November 14, 2009, from http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/domain-member.html, 2003a.

[23] H.J. Terpstra, J.G. Carter, D. Bannon, and G. Deschner, Domain Control. Retrieved November 14, 2009, from http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-pdc.html, 2003b.

[24] H.J. Terpstra, and V.R. Jelmer, The Official Samba-3 HOWTO and Reference Guide

[25] (2nd ed.). Upper Saddle River, NJ: Prentice Hall PTR, 2006.

[26] Active Directory, Retrieved November 14, 2009, from http://en.wikipedia.org/wiki/Active_Directory

[27] Samba Software, Retrieved May 7, 2009, from http://en.wikipedia.org/wiki/Samba_(software)

[28] Novell's NetWare Directory Service (eDirectory). (2009). Retrieved October 3, 2009, from http://www.novell.com/products/edirectory

[29] SuSE/OpenLDAP/Samba Howto. Retrieved June 6, 2009, from http://www.stress-free.co.nz/suse_openldap_samba_howto, 2006.

[30] IPanet, Retrieved October 3, 2009, from http://en.wikipedia.org/wiki/IPlanet

[31] IBM's SecureWay Directory, Retrieved October, 3, 2009 from http://www.ibm.com/software/secureway/directory

[32] L. Wei-Meng, *What is Virtualization?* Retrieved November 14, 2009, from http://oreilly.com/pub/a/windows/2005/12/06/what-is-virtualization.html

[33] L. McCabe, *What is Virtualization, and Why Should You Care?*

[34] Retrieved November 14, 2009, from http://www.smallbusinesscomputing.com/testdrive/article.php/3819231

[35] D. Davis, *Server Virtualization, Network Virtualization & Storage Virtualization explained.* Retrieved November 21, 2009 from http://www.petri.co.il/server-virtualization-network-virtualization-storage-virtualization.htm, 2007.

[36] W.V. Hagen, *Professional Xen Virtualization.* Wiley Publishing, Inc, 2008.

[37] VMware Server 2.0 Essentials, Retrieved November 22, 2009, from http://www.virtuatopia.com/index.php/VMware_Server_Virtual_Network_Architecture

[36] C. Schroder, Linux Networking Cookbook. Sebastopol, CA: O'Reilly Media, Inc, 2008.

[37] An Introduction to Virtualization, Retrieved November 14, 2009, from http://www.kernelthread.com/publications/virtualization, 2004

[38] L. Malere, L. E. Pinheiro, *LDAP Linux HOWTO*. Retrieved August 10, 2009, from *www.tldp.org/HOWTO/LDAP-HOWTO/*

[39] E. Nemeth, S. Garth, R.T. Hein, Linux Administration Handbook (2nd ed.). Pearson Education, Inc., Upper Saddle River, New Jersey, 2007.

[40] S.F. Riri, and H. Syarif, IntegratingWeb Server Applications With LDAP Authentication: Case Study on Human Resources Information System of Ul-IEEE W4B-3 ISCIT 2006

AUTHORS PROFILE

M.A. Ajagbe has an MBA in marketing management from Ambrose Ali University Ekpoma, Nigeria. He worked as assistant sales manager, regional sales manager and area sales manager with Dansa Foods Ltd. (Dangote Grp Nig.), Danico Foods Nig. Ltd. and Fareast Mercantile Company Nig. Ltd. respectively. He is currently a Doctoral Degree Student with Universiti Teknologi Malaysia. His research interest is in financing Technology Entrepreneurs through venture capital. He has about 25 publications to his credit in reputable international conferences and Journals which cut across disciplines. He is an active member of these professional bodies; Associate Member, National Institute of Marketing of Nigeria, Associate Member, Nigerian Institute of Management, and British Council Management Express

Forum Nigeria. Ajagbe is also a research assistant with K-Economy, Integrity Research Alliance and Innovation and Commercialization Centre (UTM). Award; Best participant and Contributor, Business Strategy Building Workshop (Dangote Group Nigeria) 2006.International Doctoral Fellowship Award (UTM) 2011-Date (ajagbetun@yahoo.com).

A.N. Lasisi (**principal author**) holds a Masters degree at International Islamic Univeristy Malaysia (IIUM) with specialization in Computer Networking & Linux Administration and is currently a Doctoral Degree candidate at Universiti Teknologi Malaysia (UTM). His PhD research interest is in Computer Security with focus on malware. Lasisi is a member of Nigerian Computer Society and Nigerian Institute of Management (lasisiayodele@yahoo.com