

Samba Openldap Performance in a Simulated Environment

Ayodele Nojeem Lasisi¹, Mohiuddin Ahmed²

^{1,2}Faculty of Information and Communication Technology

^{1,2}International Islamic University

P.O.Box 10, 50728 Kuala Lumpur, Malaysia

Musibau Akintunde Ajagbe³

³Faculty of Management and Human Resource
Development

³Universiti Teknologi Malaysia,
81310 Skudai Johor-Malaysia.

Abstract-- The Information Technology world is developing so fast and it is been reported that Open Source tools will eventually take over proprietary tools in no to distant future. The Open Source Community is integrating its products with that of the proprietary ones and the integration of Windows machines into Linux network is evident of such practices. The purpose of this project is to implement Samba with OpenLDAP in a simulated environment. This implementation is conducted within a virtual environment by simulating the setup of Linux and Windows Operating systems by reducing physical setup of machines. Samba will act as an interface between Linux and Windows, files will be accessible to both server and client. OpenLDAP stores the user accounts and configuration files. A performance test carried out on Samba determining effect on CPU power and Memory usage shows a decrease in the CPU power and an increase in Memory usage.

Keywords: SAMBA; OpenLDAP; Simulated environment

1 INTRODUCTION

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 [1, 2]. 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.

It is difficult in integrating authentication information and user's data storage for both Windows and UNIX environment [1]. 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 [1,3]. 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.

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 [2,4,5].

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. The purpose of this project is to implement Samba with OpenLDAP in a simulated environment. This implementation is conducted within a virtual environment by simulating the setup of Linux and Windows Operating systems by reducing physical setup of machines. Samba will act as an interface between Linux and Windows, files will be accessible to both server and client. OpenLDAP stores the user accounts and configuration files [3, 6, 7]). A performance test is carried out on Samba to determine the effect on CPU power and Memory usage.

2 SURVEY OF RELEVANT LITERATURE

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 [6].

Samba is a free software re-implementation of SMB/CIFS networking protocol, originally developed by Australian Andrew Tridgell. 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. It can also be part of an Active Directory. Samba as a Primary Domain Controller has been implemented in this current project [8].

2.1 Samba Server Types

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

- Standalone server

Standalone servers are independent of domain controllers on the network. 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 [9, 10, 8].

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 [8].

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 or she uses will be translated (mapped) locally on the standalone server to a locally known user name [11,12].

- 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 [12].

- 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 [12, 13].

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.

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 [6,12].

2.2 Other Implementations of LDAP

LDAP has some popular implementations namely:

- OpenLDAP, an open LDAP suite [5, 6, 3].
- 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 [14, 10].

2.2.1 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 [10,15,16]

2.2.2 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.

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 [15].

2.2.3 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”[17,4].

2.2.4 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 [14]. It is standards 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.

2.3 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 [11, 18].

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 [18].

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 [18, 9].
- *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 [18].

However, server virtualization and network virtualization has been deployed for the purpose of this project. 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. 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 [2, 8].

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 [19, 20].

The general representation of virtualization is depicted in Figure 1 below.

The general representation of virtualization is depicted in Figure 1 below.

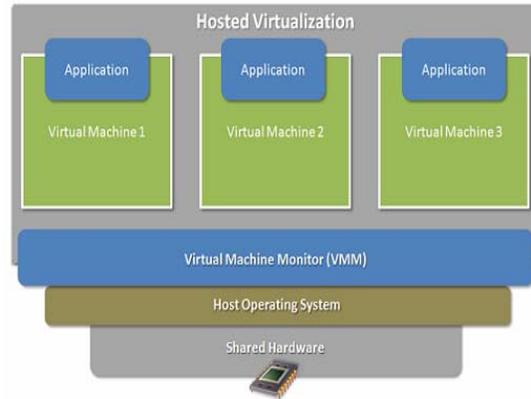


Figure 1. Hosted virtualization architecture, virtual machine monitor (VMM) software is installed on a host operating system [18].

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 [16, 18]. The project study made use of the hosted virtualization.

3.0 METHODOLOGY/PROJECT IMPLEMENTATION

3.1 Problem Statement

The purpose of this project is to implement Samba with Open Lightweight Directory Access Protocol (OpenLDAP) [15, 3, 5, 6, 13] in a simulated environment. The implementation is conducted within a virtual environment by simulating and setting up Linux and Windows Operating systems which help to reduce setting up machines physically in different locations. The present study is concerned with:

- i. Implementing Samba as an interface between Linux and Windows.
- ii. Implementation of a file system accessible on both server and client.
- iii. Implementing OpenLDAP for storing configuration files.
- iv. Testing the file server for its performance in a virtual environment.

3.2 Research questions

This study seeks to address the following research questions:
How Samba act as an intermediary between Windows users and Linux users by providing authentication (Single-Sign on) between the two platforms?

- i. How sharing of file systems and shared printers are installed on both server and client?

- ii. How OpenLDAP which stores configuration file with Samba server requesting authentication from the LDAP server before granting user access?
- iii. If performance test on the file server has an effect on the CPU and Memory in a virtual environment

	Minimum Disk Space for Setup: 80GB	
--	------------------------------------	--

3.3 The main objective is to implement Samba with Open Lightweight Directory Access Protocol (OpenLDAP) which are:

- Authentication for Linux and Windows.
 - i. One password.
 - ii. Sharing files and printers.
 - iii. Data transparency to the users.
 - iv. Redundant authentication servers.
 - v. Storing of configuration files and user accounts.
 - vi. File server performance test in a virtual environment.

3.4 System Requirements

It encompasses the overall system setup with the hardware and software requirements. Hardware specifications such as the CPU, Memory and disk Space and the software required for Samba and LDAP.

The table below represent the system specifications.

Table 1 System Specification

	Hardware Requirements	Software Requirements
LDAP Server	64-bit Architecture Computer AMD Athlon family, or compatible processor(s). Minimum RAM: 384MB Minimum Disk Space for Setup: 10GB	SUSE Enterprise Linux, OpenLDAP version 3
LDAP Client	64-bit Architecture Computer AMD Athlon family, or compatible processor(s). Minimum RAM: 384MB Minimum Disk Space for Setup: 10GB	SUSE Enterprise Linux, OpenLDAP version 3
Samba Server	64-bit Architecture Computer AMD Athlon family, or compatible processor(s). Minimum RAM: 384MB Minimum Disk Space for Setup: 10GB	SUSE Enterprise Linux, Samba
Window Service	64-bit Architecture Computer AMD Athlon family, or compatible processor(s). Minimum RAM: 256MB Minimum Disk Space for Setup: 15GB	Windows XP Professional
Host	64-bit Architecture Computer AMD Athlon family, or compatible processor(s). Minimum RAM: 2GB	Red Hat Enterprise Linux (CentOS 5.3)

4.0 VIRTUALIZATION SETUP

VMware Server was downloaded and installed on the host machine running CentOS 5.3. Within the virtual environment, SUSE Enterprise Linux machine and a Windows XP Professional machine were created. OpenLDAP server was installed and configured and was able to authenticate the users created on the LDAP server. Samba also have been installed and configured. As mentioned earlier in this report, Samba has been configured as a Primary Domain Controller (PDC) with an LDAP backend by specifying in the (smb.conf) file of the Samba configuration and also including the samba schema in the (slapd.conf) file of the LDAP configuration. The project setup within the virtualization environment is depicted in Figure 2 below.

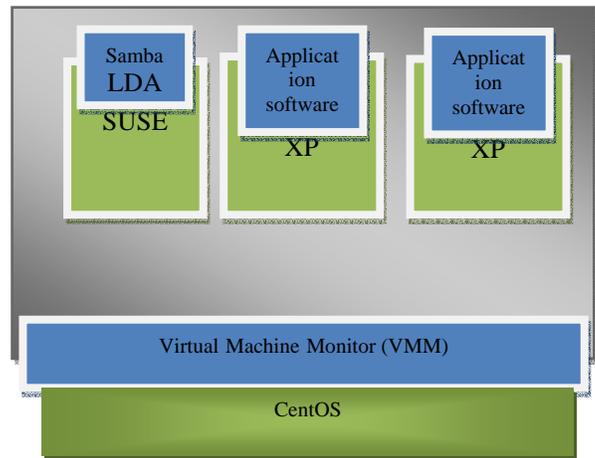


Figure 2. Setup in Virtual environment

Below are the screenshots of the VMware Server Console showing SUSE [13, 19] Enterprise Linux and Windows XP Professional as shown in Figure 3 and 4.

Figure 3 below depicts the system setup of Samba Primary Domain Controller with OpenLDAP.

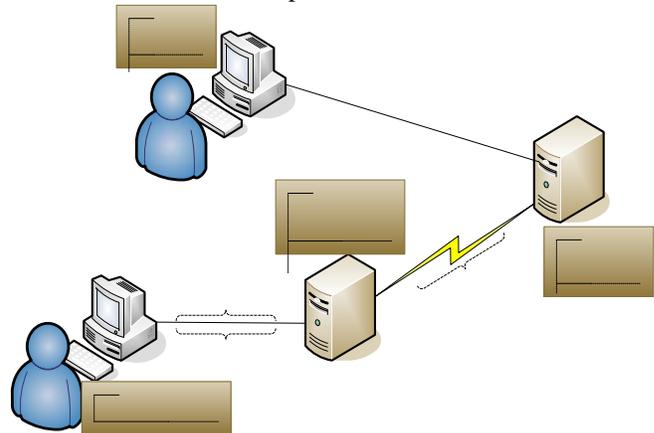


Figure 3. Samba PDC with OpenLDAP

The Windows users authenticate into the LDAP server through Samba acting as a Primary Domain Controller. The Samba PDC then fetches LDAP server to know if the user account is in its database and gives an acknowledgement or a confirmation back to Samba which in turns grant the user from the Windows domain access into it files and shares. Linux users gain access to the LDAP server via direct authentication.

4.1 Performance Testing

File serving is a typical server function. Dbench is an open source file server benchmark that mimics the behaviour of Netbench, the industry standard [21]. It was created by Andrew Tridgell, a developer for the open source project Samba, a SMB file and printer server for UNIX. Netbench is a commercial product created by Ziff Davis Media that measures the performance of a file server serving data to Windows clients [1]. The problem with Netbench is that it requires many physical machines to act as clients. Dbench has a very different philosophy. Tridgell believes that software should be accessible to all users. Thus the clients are simulated, reducing the physical hardware demand from many physical client machines to one physical machine to simulate all of the clients.

Dbench is open source, allowing anyone to use it for free and more importantly, know exactly what the code does to simulate the file server load. Dbench is the obvious choice for time, space, and money reasons. Dbench measures the file system on the server side by measuring the throughput of the disk I/O operations in MB/s.

Figure 4 below shows the tail end of a ten-minute dbench run. In this particular run, twenty-five client processes were simulated; the total mean throughput was 85.0927 MB/sec. the figure does not show a complete run, but dbench actually goes through three phases which are: warmup (a lighter load which allows disk throughput to slowly increase), execute (the most strenuous part of the benchmark), and cleanup (when any created files are deleted).

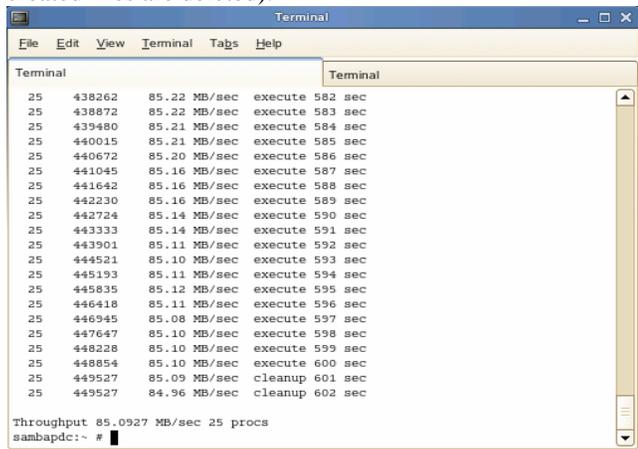


Figure 4. Tail end of dbench output, showing the cleanup and mean throughput

Dbench was run with the number of clients querying the server scaled in the following sequence: 1, 5, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 95, 100, 200, 250, 260, 270 as depicted in Table 2 below.

Table 2 Test Data

No of Clients (Query)	Throughput (MB/sec)	% CPU	% Memory
1	91.7561	95.7	0.1
5	91.1652	94.2	0.5
10	89.8667	93.3	1.0
15	89.0503	93.6	1.5
20	86.7879	91.7	2.0
25	80.8551	89.3	2.5
30	81.0336	89.7	3.0
35	74.0489	86.8	3.5
40	65.7049	88.5	4.0
45	50.4531	73.2	4.5
50	44.389	68.9	5.0
55	42.186	61.4	5.5
60	36.2346	62.4	6.0
65	39.2185	63.7	6.5
70	37.1362	62.5	7.0
75	35.4853	60.5	7.5
80	34.6912	61.0	8.0
85	35.1207	61.6	8.5
90	36.3942	58.2	9.0
95	33.2976	56.2	9.5
100	33.2866	57.2	10.0
200	24.8569	41.5	20.0
250	23.9635	36.2	25.0
260	19.8784	26.8	26.0
270	19.936	22.6	27.0

The result for the benchmark is shown in the Figure 5 below. It shows the results of the dbench component. As you can see as more clients are added, the file system performance drops off quite fast.

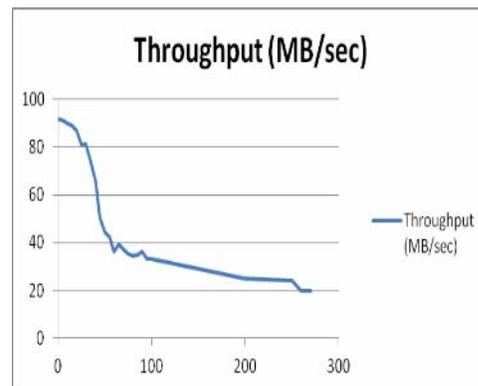


Figure 5. Dbench Result

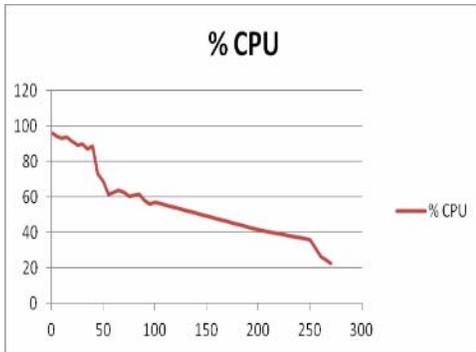


Figure 6. CPU Performance

The more the number of clients querying the file server, the more the task it takes the server to handle the entire file I/O. Thus, the CPU power remaining decreases as depicted in Figure 6. The memory usage increases steadily and linearly and makes a cross point as CPU power decreases. This is the optimum point that the file server can handle query at 270, depicted in Figure 7 below.

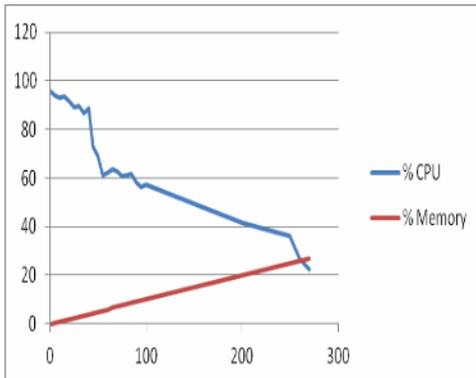


Figure 7. Optimum Capacity (at 270 queries)

5.0 CONCLUSION

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. The study has implemented Samba OpenLDAP in a simulated environment by having two virtual operating systems, Linux and Windows installed on a single machine i.e. the host operating system. 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. A performance test on Samba reveal that as the number of query increases, the CPU power remaining decreases and the Memory increases usage moderately. The graph depicted in Figure 7 shows a cross-point indicating the maximum queries (at 270) that can be sent to the server. The basic configurations for Samba OpenLDAP are the

(slapd.conf), (ldap.conf) and (smb.conf) files. The (slapd.conf) is for the configuration of LDAP server, the (ldap.conf) is for configuring the LDAP client and the (smb.conf) for Samba configuration. In setting up Windows XP Professional to join the domain, the Windows networking is checked to confirm if it is set up correctly i.e. TCP/IP. Click Start, Right-click My Computer and select Properties which brings up Network Identification Tab. Click the Computer name tab, this panel shows the Computer Description, the Full computer name, and the Workgroup or Domain name. Click the Change button and enter the domain name in the field below the radio button. Now click the OK button, a dialog box appears to put credentials (username and password) of a domain administrative account that has the rights to add machines to the domain. Enter the name "root" and the root administrative password of the Samba server. By clicking OK, a "Welcome to the specified domain" dialog box should appear. At this point the machine must be rebooted and joining the domain is now complete.

The integration of Microsoft Windows and UNIX through the use of Samba (which implements Single Sign-On) and OpenLDAP has allowed for the provision of a resource sharing scheme, which unifies authentication information and users' data storage on multiplatform. The authentication process is guaranteed compared to what is obtained in Windows because Linux stores hashed password against the cleartext password used by Windows. In Windows authentication systems, the client does not trust the server; Windows uses a challenge/response method for authentication. The issue with challenge/response method is that the server has to store plaintext-equivalent passwords which is locally encrypted and is a precaution against casual browsing. An intruder who gains access to the encrypted password can use them to access the associated accounts without the need for any further password cracking. This study provides system administrators with uniform authentication methods at both OS (i.e. Windows and UNIX) and application levels at minimal cost, and provides the users with reflexible and uniform interface to data storage and resources regardless of the platforms.

It would be suitable and useful as a source of reference for small and medium scale enterprise [22, 23] looking for an alternative solution for the highly costly solutions from IT providers.

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

6. REFERENCES

- [1] J. Futagawa, Integrating Network Services of Windows and UNIX for Single Sign-On. International Conference Proceedings of Cyberworlds, 2004.
- [2] 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>
- [3] Manage OpenLDAP. (2007). Retrieved July 5, 2009, from http://ocw.novell.com/suse-linux-enterprise/upgrading-to-certified-linux-engineer-10/3076_11_manual.pdf
- [4] S.S. Lim., H.J. Choi and 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.
- [5] OpenLDAP. (n.d.). Retrieved May 9, 2009, from www.openldap.org
- [6] OpenLDAP (2009). Retrieved May 7, 2009, from <http://en.wikipedia.org/wiki/OpenLDAP>
- [7] L. Malere and E. Pinheiro, *LDAP Linux HOWTO*. Retrieved August 10, 2009, from www.tldp.org/HOWTO/LDAP-HOWTO/
- [8] Server World. (n.d.). Build Network Server. Retrieved August 2, 2009, from <http://www.server-world.info/en/>
- [9] W.V. Hagen, *Professional Xen Virtualization*. Wiley Publishing, Inc, 2008.
- [10] Novell's NetWare, Directory Service- eDirectory (2009). Retrieved October 3, 2009, from <http://www.novell.com/products/edirectory>
- [11] L.Wei-Meng, *What is Virtualization?* Retrieved November 14, 2009, from <http://oreilly.com/pub/a/windows/2005/12/06/what-is-virtualization.html>
- [12] H.J.Terpstra, Standalone Servers. Retrieved November 14, 2009, from http://www.samba.org/samba/docs/man/Samba-HOWTO_Collection_StandAloneServers.html
- [13] SuSE/OpenLDAP/Samba Howto. (2006). Retrieved June 6, 2009, from http://www.stressfree.co.nz/suse_openldap_samba_howto
- [14] IBM's SecureWay Directory. Retrieved October, 3, 2009 from <http://www.ibm.com/software/secureway/directory>
IPanet, Retrieved October 3, 2009, from <http://en.wikipedia.org/wiki/IPanet>
- [15] Active Directory, Retrieved November 14, 2009, at http://en.wikipedia.org/wiki/Active_Directory
- [16] An Introduction to Virtualization. (2004). Retrieved November 14, 2009, from <http://www.kernelthread.com/publications/virtualization/>
- [17] iPanet. (2009). Retrieved October 3, 2009, from <http://en.wikipedia.org/wiki/IPanet>
- [18] L. McCabe, *What is Virtualization, and Why Should You Care?* Retrieved November 14, 2009, from <http://www.smallbusinesscomputing.com/testdrive/article.php/3819231>
- [19] VMware Server 2.0 Essentials. (2009). Retrieved November 22, 2009, from http://www.virtuatopia.com/index.php/VMware_Server_Virtual_Network_Architecture
- [20] E. Nemeth., S. Garth and R.T. Hein, *Linux Administration Handbook* (2nd ed.). Pearson Education, Inc., Upper Saddle River, New Jersey, 2007.
- [21] A.Triggell. (n.d.). Retrieved October 9, 2009, from <http://samba.org/ftp/tridge/dbench/README.6>
- [22] M.A. Ajagbe., C.S. Long., S.A. Aslan and K. Ismail, Investment in Technology Based Small and Medium Sized Firms in Malaysia: Roles for Commercial Banks. International Journal in Research in Management & Technology, vol.2, no.2, pp.147-153, 2012
- [23] K. Ismail., S.A. Aslan. and M.A. Ajagbe, An Investment Framework to Help Equity Financiers Select Tech SMEs in Malaysia. Interdisciplinary Journal of Contemporary Research in Business. ISSN 2073-7122, IJCRB Sept. Edition 2011, vol. 3, no. 5, pp. 966-983, 2011

AUTHORS PROFILE

M. Ahmed is currently a Lecturer with Jazan University, Saudi Arabia. He holds a PhD in Electrical Engineering at North Carolina Agricultural and Technical State University. His research interest is in Computer Networking, Linux Administration. Ahmed has published in some International Journals, conferences and seminars.

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 University 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 (lasisiyodele@yahoo.com).