Identity and Access Management System: a Web-Based Approach for an Enterprise

Mohammed Kabiru Hamza [1], **Hassan Abubakar** [1], **Yusuf Mohammed Danlami** [1]

[1] *Usmanu Danfodiyo University*
P. M. B. 2346, Sokoto, Nigeria

DOI: 10.22178/pos.40-1

LCC Subject Category:
TK7885-7895

Received 28.10.2018
Accepted 20.11.2018
Published online 30.11.2018

Corresponding Author:
Mohammed Kabiru Hamza
kabiru.mohammed@udusok.edu.ng

Abstract. Managing digital identities and access control for enterprise users and applications remains one of the greatest challenges facing computing today. An attempt to address this issue led to the proposed security paradigm called Identity and Access Management (IAM) service based on IAM standards. Current approaches such as Lightweight Directory Access Protocol (LDAP), Central Authentication Service (CAS) and Security Assertion Markup Language (SAML) lack comprehensive analysis from conception to physical implementation to incorporate these solutions thereby resulting in impractical and fractured solutions. In this paper, we have implemented Identity and Access Management System (IAMSys) using the Lightweight Directory Access Protocol (LDAP) which focuses on authentication, authorization, administration of identities and audit reporting. Its primary concern is verification of the identity of the entity and granting correct level of access for resources which are protected in either the cloud environment or on-premise systems. A phased approach methodology was used in the research where it requires any enterprise or organization willing to adopt this must carry out a careful planning and demonstrated a good understanding of the technologies involved. The results of the experimental evaluation indicated that the average rating score is 72.0 % for the participants involved in this study. This implies that the idea of IAMSys is a way to mitigating security challenges associated with authentication, authorization, data protection and accountability if properly deployed.

Keywords: Identity Management; Access Management; Identity and Access Management; LDAP Server; SSO.

INTRODUCTION

Traditionally, software applications within an organization's information system are deployed and placed inside the organization's boundaries. Thus, the organization has a "trust area", which is defined by static methods, being monitored and controlled by the experts of the IT department. In most cases, the "trust area" encapsulates the core organizational network, systems and applications that are managed in-house, being organized in the form of a data center. The data center can be either managed by experts from within the organization or outsourced to an external service provider (in this case, the organization usually reserves the right to control and to have the final word on the manner security policies are formulated and implemented). In a "traditional" model, the access to the information resources of the organization is secured through a set of specialized systems, implemented at the network level [2].

Nowadays, many organizations have faced the complex problem of managing identities and credentials for their technology resources. What used to be a simple issue that was confined within the walls of the data center has become a growing and exponentially complex problem facing organizations of all sizes. For instance, many large organizations are unable to effectively manage the identities and access permissions granted to users, especially in distributed IT environments. Over the last several years, IT departments have built system administration (SA) groups to manage the multitude of servers, databases, and desktops the organization uses. However, even with the creation of SA groups, managing access to the organization's resources remains a challenge. Even with this expansion, human resources and manual processes are sometimes unable to handle the complex tasks and excessive administrative overhead needed to manage user identities within the organization.

What's more, in recent years regulatory requirements have added complexity and increased external scrutiny of access management processes. These regulatory requirements and prudent business practices have led organizations to grant individuals access at the most granular feasible level, forcing managers to determine what specific rights are needed, rather than granting users access to resources they do not actually need to do their jobs. Although what is commonly referred to as Identity and Access Management (IAM) has become an industry-accepted term, there are many definitions in use, depending on the industry, product vendor, or professional consultant. However, the core premise remains the same [1].

Identity management system is used for providing the security of user access, managing users, credential verifications and check whether the right persons are to access the resources provided by the services. Authentication of users is performed in different ways like password, biometrics, token-based or certificate based. In most organizations, the risk, cost and efforts towards managing identity increases along with the growth of the organization. For the proper management of the identities, every organization needs a well-defined identity management system. This helps the organization to reduce the risk associated with identity management as well as the cost and the time required to fulfill the employee's identity and access needs [4].

Access control mechanism is essential for authorization in the cloud-based services. The access control system is used to determine whether the right person is accessing the resources with predefined access policies. The main aim of this mechanism is to facilitate the security and privacy of resources. When the access control mechanism is efficient, it protects any unauthorized access to the network. There exists a different variety of models and technologies in access management. In a cloud environment, the same cloud is used for different organizations with different policies that lead to the chance of accessing resources by unauthorized persons. The different access control models used are Mandatory Access Control model, Discretionary Access Control (DAC) model, Role Based Access Control (RBAC) model, Policy-Based Access Control (PBAC) model and Risk-Based Access Control (RBAC) model [11].

The access management system works in association with identity management system for typically managing the user access to the associated resources or applications. A well-established access management system in an organization has multiple functionalities and benefits [5]. Identity and Access Management (IAM) refers to the processes, technologies, and policies that manage access of identities to digital resources and determine what authorization identities have over these resources. For an individual user, IAM generally concerns several processes. The user can create, remove or adjust a user account within an application. Users also have a measure of authentication to prove their identity. Authentication measures can range from a combination of username and password to multifactor authentication where smartcards, generated tokens and /or biometric data can be combined to make the authentication stronger. For organizations, IAM is generally used much more intensively as organizations represent multiple users (employees) using multiple digital resources. This requires extensive propagation of user accounts and better monitoring and audit capabilities [9].

The existing approaches to Identity and Access Management (IAM) are concentrating on offering framework/architecture/model solutions. But, these approaches lack a comprehensive analysis from conception to physical implementation to incorporate these solutions making it impractical and fractured solutions. In this research work, we implemented an Identity and Access Management System using a directory service (LDAP server) which combined the merits of Single Sign-On and access control to bring about security mitigation.

RELATED WORKS

This section reviews the existing research works related to Identity and Access Management in an enterprise by highlighting the strengths and weaknesses of each work. Several researchers have proposed different approaches and models to address the various types of authentication and authorization issues.

Authors proposed a multi-tenancy authorization system using Shibboleth for the cloud-based environment. The main idea is to demonstrate how an organization can use Shibboleth to implement in practice a system of access control in a cloud computing environment, without a trusted third

party. The Shibboleth is an authentication and authorization infrastructure based on SAML that uses the concept of federated identity. However, the proposed work lack an alternative authorization method, where the user once authenticated, carries the access policy, thus the authorization process will no longer perform or repeated again at the application level.

In the article [3], a new architecture to manage identity and control access to resources in a multi-tier cloud infrastructure was proposed. The architecture comprises of two major components; middleware and central IAM to manage user and infrastructure related data. Middleware sits in front of a resource provider and handles time-consuming, decision making such as authentication and authorization, while the repository handles data manipulation. The architecture has been implemented on Canadian SAVI testbed. The system is developed on an IAM solution for the multi-tier infrastructure such as SAVI testbed. However, the proposed work needs a substantial amount of effort to define roles and assign them.

In the article [10], an Identity and Access Management (IAM) architecture that aims to address strong authentication, data loss prevention and security as a service was proposed. It also tries to achieve a comprehensive identity information management, authentication and access control mechanism. The proposed architecture has four components viz; Cloud Resource Provider (CRP), Identity Management (IDM), Policy Management (PM) and Resources Engine and Access Decision Making (REPD), with the security architecture workflow at hand. Therefore, any user who needs to access resources must go through the security enforcement-authentication first, followed by the access control according to his/her privileges which are authorized. However, the proposed IAM architecture drawbacks were that it was not implemented and as such could not be tested and verify the scalability and performance of the architecture as claimed by the authors, this work only provides a theoretical framework.

In the paper [4], an integrated identity and attribute based access management system for cloud web services was proposed. In the proposed integrated approach, the hybrid architecture for authentication and attribute based control (ABAC) for authentication was utilized. It consists of Identity Management and Access Management models. In order to get the cloud web services, the user has to authenticate through an identity system from the initiated application which is Identity Management. There is a mechanism to validate the access token with identity system and perform the authorization on the cloud. However, this work only provides and demonstrated a theoretical framework.

In the article [8] a model called Claim-Based Identity Management scheme with the extension for cloud applications and provides a more secure way to access cloud services was proposed. It uses a new form of Security Assertion Markup Language (SAML) security token is generated, by building and deploying claim-based applications besides existing application result in simpler migration. Claim-Based Architecture makes use of a single UserID and Password to get access to many applications those residing in the clouds or across the clouds. However, the work laid so much emphasis on identity management leaving out the access management in the cloud.

Researchers [5] proposed a hybrid authentication and authorization model for secure and user-friendly web-based applications. The proposed model utilizes the advantages of Discretionary Access Control (DAC), Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) access models along with SAML 2.0 technology. The model roles are dynamically identified with the help of ABAC base access control roles at the IAM system and inform the target application with the help of SAML technology. The proposed IAM system stores all the user attributes information application roles/entitlement, organizational policies and access control roles. However, the proposed system lacks the capability of keeping Audit and Reporting features.

Authors [7] proposed an identity and access management as a service (IAMaaS) framework that primarily focuses on authentication, authorization, administration of identities and audit. It is also a concern with verification of identity and granting correct access for resources which are protected in the cloud environment. When the user logs in, his/her credentials are verified and a token is generated which is passed to the protected resources in the private cloud such as devices, data, and application server. In this way, the entire Identity and Access Management functionality can be managed. However, the framework is yet to be integrated into SECaaS and only demonstrated a proof-of-concept (POC).

METHODOLOGY

A phased approach was adopted using a Lightweight Directory Access Protocol to evaluate the Identity and Access Management (IAMSys). Research questions were administrated to different stakeholders in the field of computing, based on this, data was gathered and analyzed. User accounts will be provisioned/de-provisioned, permissions, roles will be created, role permissions will be mapped, roles will be assigned and lastly, roles will as well be revoked from user accounts. In addition to this, IAM logs in the place where there is provision for monitoring eligible user's credentials, data breaches, account hijacking. This will enable us to know the number of attempted login that is failed, successful login and even correct access to the IT resources etc.

Research framework

The framework for this research is made up of several stages. These stages include problem formulation, previous IAM system Proof-of-Concept, proposed IAM implementation and conducting test experiments.

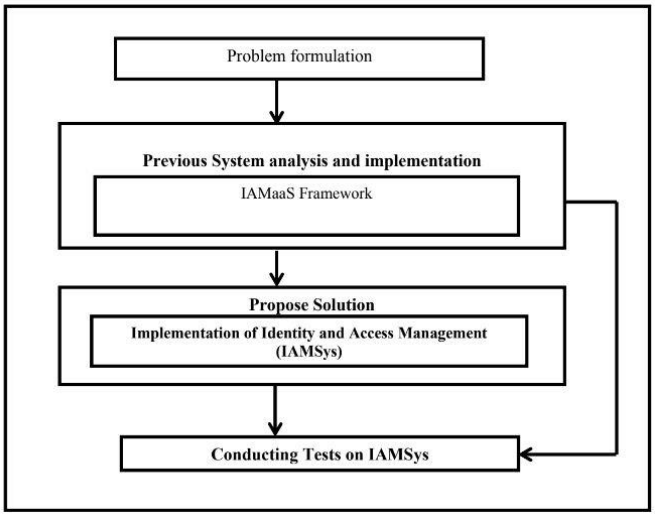

Figure 1 – Research Framework

Problem formulation

A critical literature review of the existing proposed Identity and Access Management (IAM) was carried out at the beginning of the research work. The review discussed several approaches to IAM implementation along with their strengths and weaknesses. However, the research problem was identified as stated in the review of related literature.

Identity and Access Management as a service (IAMaaS) framework was proposed that primarily focuses on authentication, authorization, administration of identities and audit, it is also a concern with verification of identity and granting correct access for resources which are protected in the cloud environment. The implementation has been done in form of a web server running under Windows OS Virtual machine in a public cloud setup. The IAM core and IAM manager have been implemented in a separate Virtual machine. The client is first registered and the credentials are stored in the MySQL database. The user password is stored in an encrypted form so that it is not visible to anyone not even the Cloud Service Provider. When the user logs in, his/her credentials are verified and a token is generated which is passed to the protected resources in the private cloud viz. devices, data, application server etc. In this way, the entire Identity and Access Management functionality can be managed. It is provided as a Cloud Service to the client through a browser and different types of devices (Desktops and Mobiles devices etc.) can also access it. However, the framework is yet to be integrated into SECaaS and only demonstrated a proof-of-concept (POC).

Proposed solution implementation

The implementation of Identity and Access Management System (IAMSys) proposed focuses on deploying the system using Lightweight Directory Access Protocol (LDAP) server for managing Identities and Access control. LDAP Account Manager (LAM) is a web frontend that will be used for managing entries (e.g. users, groups, organizational units etc) stored in an LDAP directory server. In addition to the aforementioned, MySQL also will be used to handle access management phase of the system where roles, permissions, role permissions will be mapped, users role will be provisioned. Role assignments and revoking of roles would be handled at the administrative panel. The section also explains how some of the Authentication Management and Access management components of the IAM system is implemented. Some of the application modules are as follows:

1. Authentication management. This module describes user provisioning, user de-provisioning either through LDAP Account Manager (LAM) or through the Administrative Panel of the IAM system.

User Account Provisioning: This can be done via the IAM system or LDAP Account Manager, using the IAMSys, the admin is expected to enter the username, common name, first name, Lastname, password and the organizational unit the user belongs to and finally click the Submit button.

User Authentication: This authenticate users that are already provisioned in the LDAP Server, upon login by the user, if the user enters either incorrect username or password, the IAM system will prompt the user with an error message that "Invalid Credentials, either username or password is incorrect".

IT Resource Page: On login successful, the user will see a page that contains permissions (Dspace, Admin, Moodle) etc assigned to him/her as the case may be. The user will be prompted with a page that will display permissions he/she is assigned i.e. based on user's role.

Accessing Restricted Pages: In an event where a user is attempting to access a restricted page, he/she will be prompted with a 404 error page prompting, "You are attempting to access a restricted page, please login properly".

De-Provisioning Users: This delete a user and this can be done only by the admin of the IAM system by a supply of the username for example. kabiru.mohammed, if the user exists, the system prompts the admin user with a success message that "the user is de-provision successfully".

Password Reset: This module reset user's password; this can only be done by the user with the admin role.

2. Access management. This module describes access control mechanism for authorization for the IT resources, and this will be used to determine whether the right person is accessing the resources with predefined access policies, the main aim of the mechanism is to facilitate the security and privacy of the IT resources. The module contains create permissions, create a role, create role permissions (mapped role/permissions), assigned a role, revoke role.

Create Permissions: In this module, permissions are created as depicted in Figure 2, permissions in this context mean applications or IT resources a user can access based on the access policy definition, here the admin user is expected to enter the permission title and URL where the permission will be accessed.

Create Role: In this module, roles are created, roles are the designation of a user as defined by an enterprise, e.g. Lecturer, Lecturer II, Cloud Developer, Cloud Administrator etc, and here the admin user is expected to enter the role title as described in Figure 3.

Create Role/Permissions: In this module, permissions and roles are mapped, meaning what a particular role assignee should be able to view or see in terms of permissions as highlighted in Figure 4.

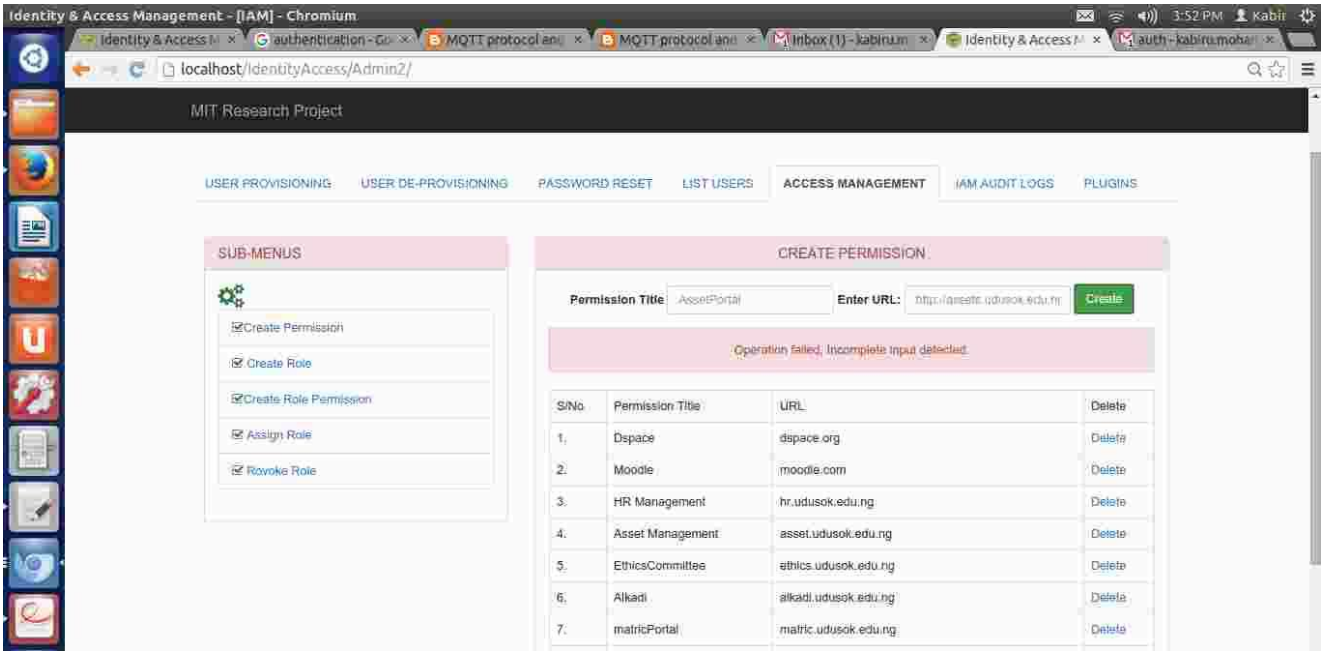

Figure 2 – Access management module displaying permission creation

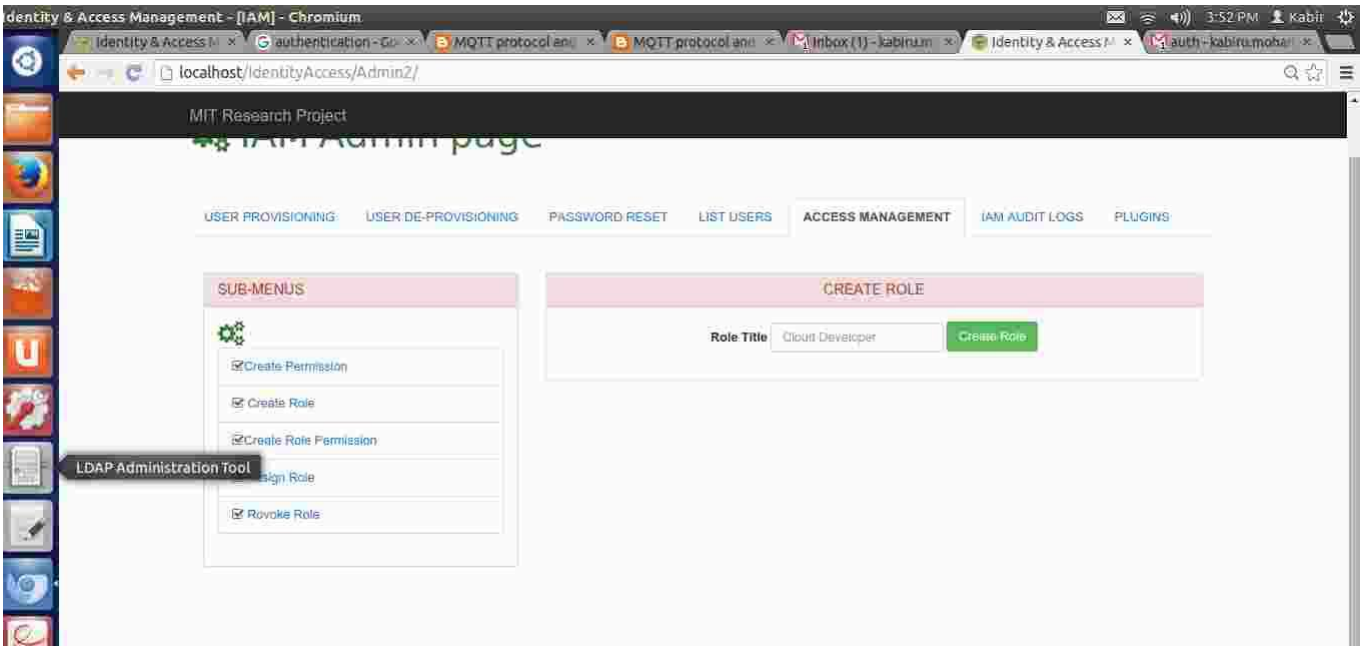

Figure 3 –Role creation page

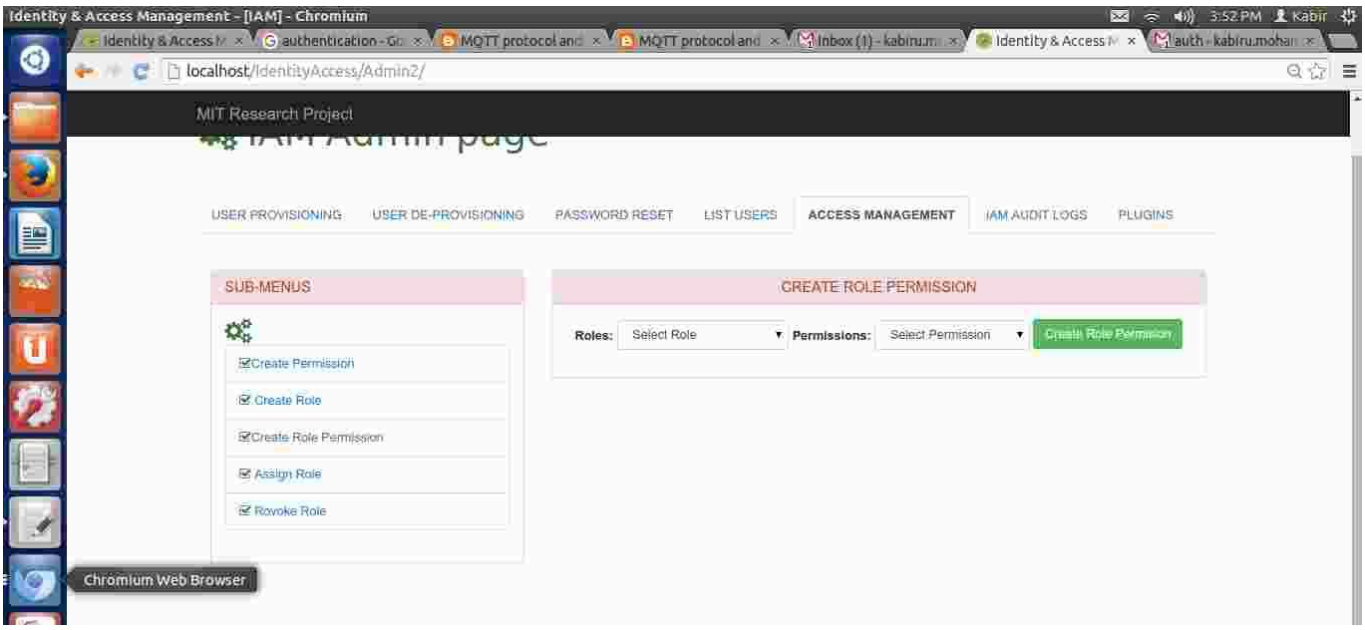

Figure 4 – Role permissions mapping page

Assign Role: In this module, role is assigned to users of the IAM system, more than a single role can be assigned to a user, for example, a DVC Admin role and a Lecturer role all assigned to a single user, and this can be done by selecting user from the dropdown menu and roles or role assign as the case may be as shown in Figure 5.

Revoke Role: In this module, role can be revoke from a user of the IAM system, more than a single role can be revoked from a user, for example, a DVC Admin role and a Lecturer role all can be revoke from a single user or different users, and this can be done by selecting user from the drop-down menu and roles or role revoke as the case may be as depicted in Figure 6.

IAM Audit Reporting: This is a module that is responsible for monitoring users' activity on the system as shown in Figure 7.

List Users: This module work by selecting from the drop-down menu the DN i.e. the distinguished name of a particular group the admin user is targeting, for example, ou=academic, ou=staff, ou=people, dc=udusok, dc=edu, what this connotes is that the admin is targeting staff from the academic circle as described in Fig. 8.

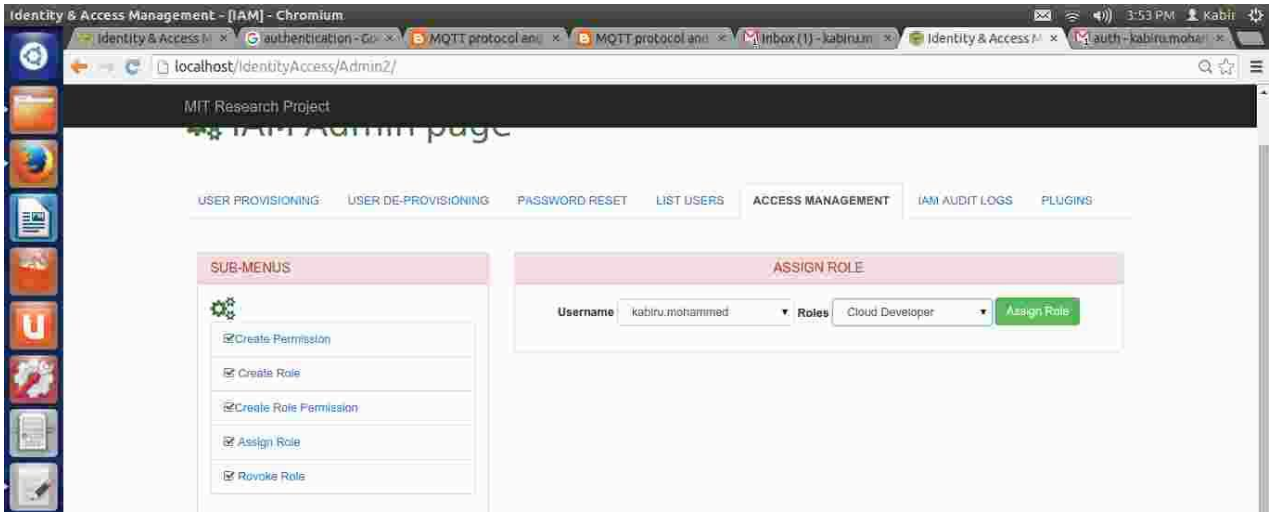

Figure 5 – Role assignment page

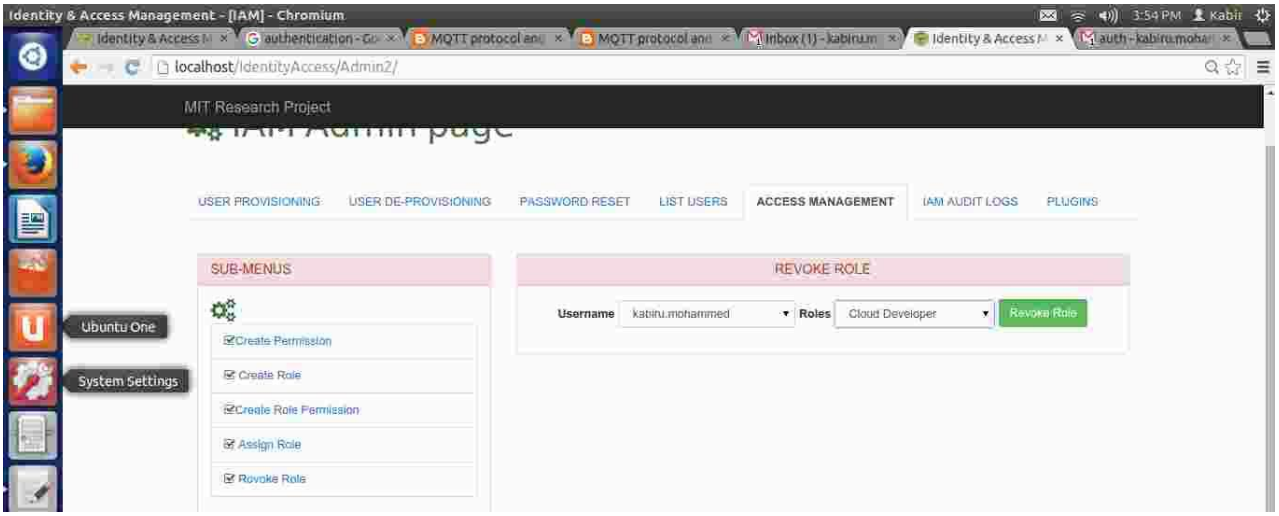

Figure 6 – Revoke role page

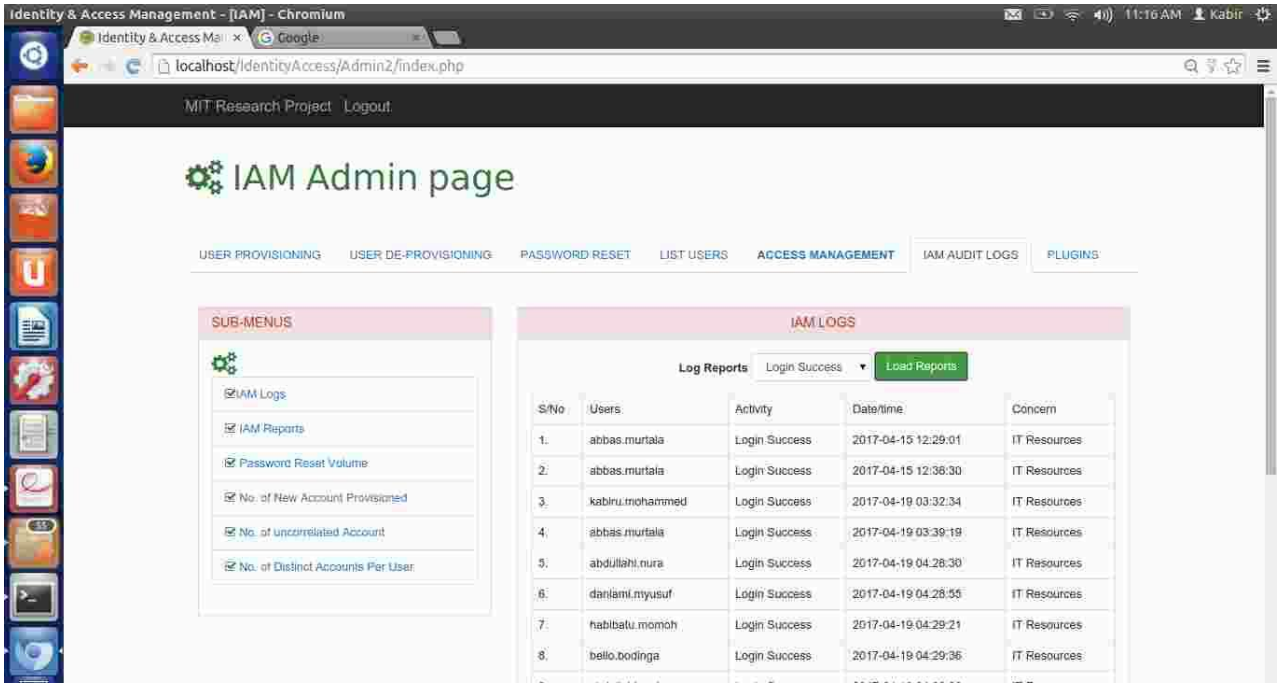

Figure 7 – IAM Audit reporting page

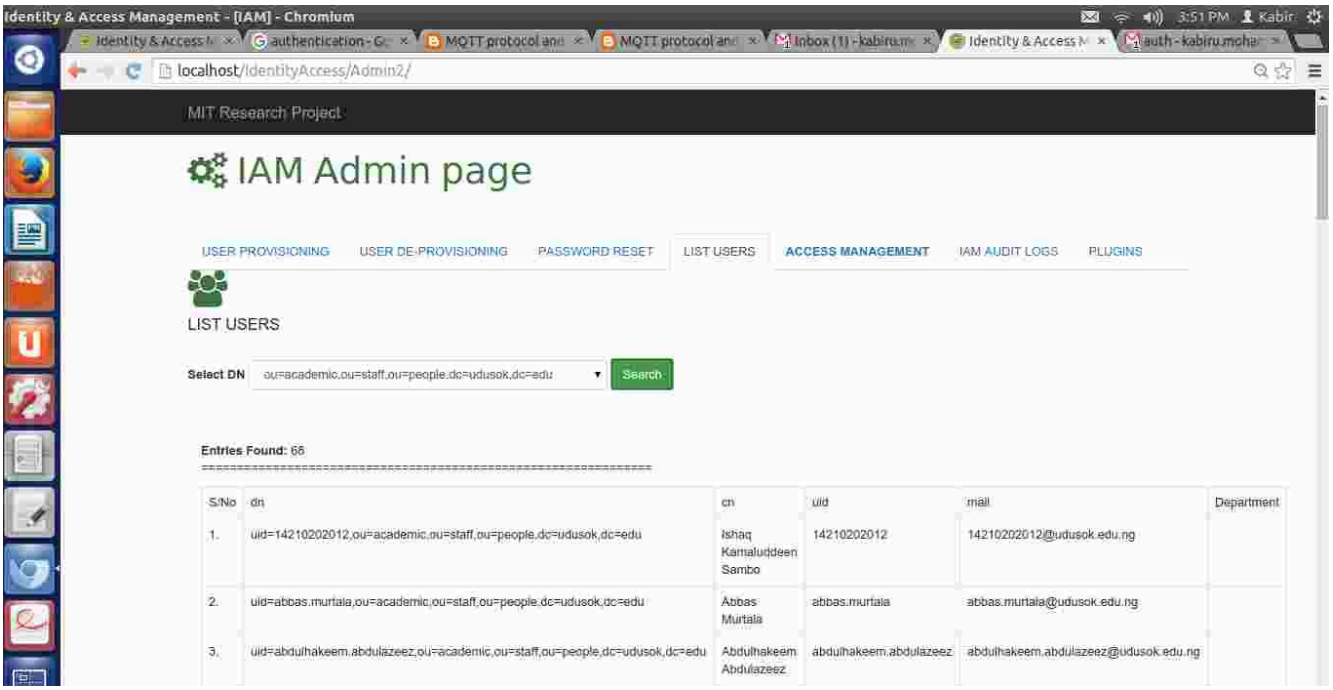

Figure 8 – List users page with their respective distinguished name

Conducting test experiments

In conducting experimental test, dummy accounts will be provisioned that will enable users to authenticate through LDAP Account Manager (LAM), upon successful authentication of user credentials, there is a mechanism to validate the accessibility with the LAM and perform authorization; the authorization will be performed by the access manager that will cover the processes and technology for determining without any error the resources that each user is entitled to access as well as the user's rights in relation to the accessed resources or that a user has the current permission to access IT resources. In addition to this, there is a provision for monitoring, audit and reconcile, password management provided by the admin manager. Authentication and authorization metrics will be used to evaluate IAM-Sys in other to determine the authenticity and role assignment data generated. This will enable us to know the number of attempted login that is failed, a number of successful logins, correct access to IT resources etc.

Experiments environment. This section presents the experiments of the environment such as computer resources, experimental procedure and the experimental setup that are used for this research. These resources are used to deploy and evaluate the proposed system.

Computer and software resources. The proposed IAM system will be implemented using the LDAP 3.0. The tool is a preferred choice because it contains the needed module that handles user provisioning, user de provisioning, group creation. The LDAP 3.0 is installed on a computer system running on an Ubuntu Operating System with 2.40 GHz processor and 6 GB of RAM. The minimum recommended hardware and software requirement for this experiment are as follows:

Required Software: Ubuntu Linux 12.04 Operating System; LDAP ftp://ftp.openldap.org/pub/OpenLDAP/openldap-release/openldap-2.4.44.tgz

Pre-requisites Software: The following pre-requisites software are to be install before installing LDAP / LAM. They can be installed through *apt-get* command from Ubuntu repository: pcap (libpcap-dev); PCRE (libpcre3-dev); Libdnet (libdumbnet-dev).

Experimental procedure. To evaluate the Identity and Access Management System (IAMSys), LDAP Server will be configure and deploy and various test will be conducted. This approach will have at its core directory service such as Lightweight Directory Access Protocol (LDAP) that contains and stores security attributes for the users.

The LDAP server setup will include among the following (a) provisioning users; (b) de-provisioning of users (c) Authorization management (d) Audit and reporting in the IAM.

Experimental setup. Software that will be used for the implementation includes; LDAP application will be install on Server running Ubuntu Linux 12.02 LTS. The latest version of LDAP application can be downloaded and install from LDAP web site. LDAP datastore is used with LDAP Account Manager to log users and its activities: Apache acts as a web server; PHP My Admin that acts a front end for MySQL; PHP will acts the scripting language within the LDAP server.

Application testing. In this phase testing of the IAMSys, each unit, module or component was tested during and after scripting to ensure that the functionality of IAMSys functions according to identity requirements, each module was tested against any security and privacy breaches, for example, in an attempt to access IT resources without proper login, it flag an error and report to the activity_log of the system, all other modules were tested independently (Table 1).

Table 1 – Identity and Access Management test Result

No	Test	Expected Result	Result
1	Login	Enter to application menu in appropriate access	Successful
2	User Provisioning	Users are added/provisioned into the LDAP server successfully and are / or edited where needed	Successful
3	User de-provisioning	Users are deleted/ or de-provisioned from the IAM system by the admin in an event where there is no clear need for user service	Successful
4	Password Reset	Users are at liberty to modify their password thrice in a month	Successful
5	List Users	Admin can list all users of the IAM system with their respective role and their distinguished names	Successful
6	Access Management	Permission creation, role creation, synchronization of role/perm, role assignment and role revocation	Successful
7	IAM Audit logs	Successful login, unsuccessful login attempts are queried by the admin	Successful
8	Logout	Exit from the IAM Application System	Successful

User evaluation of the system. Acceptance testing and evaluation of the IAMSys was carried out during system testing by the stakeholders in the field of computing at the Usmanu Danfodiyo University Datacenter. John Brooke SUS questionnaire was used to evaluate the system after the system testing, the questionnaire responded to the stakeholders will determine the level of acceptance of the system after testing by the users, if the system is evaluated successful and accepted by the stakeholders, the next activity is to carry out a pilot run of the new system before finally deploying the IAMSys.

RESULTS AND DISCUSSION

A total of 20 questionnaires were filled by participants. The System Usability Scale (SUS) which is a 20-Question Questionnaires were administered among some stakeholders like system admin, network technician at both campuses of Usmanu Danfodiyo University, Sokoto (Figure 9).

To get the SUS Score, multiply the total score by 2.5

$$Avarage\ score = \frac{1440}{20} = 72.0\ \%$$

It is now evident from the above evaluation results obtained with SUS score average of 72.0 % of the participants aligned to the idea of IAMSys that it is a way to mitigating security challenges associated with authentication, authorization, data protection and accountability when properly deployed in an enterprise using a lightweight standard protocol.

CONCLUSIONS

In this paper, we implemented Identity and Access Management (IAMSys) to curb major problems associated with cloud web services among which are verification of eligible user's credentials, protection of credentials, data breaches, account hijacking, uncorrelated account faced by most enterprises. The implemented IAM system provides a strong identity and access management system to an enterprise being it on-premise or on cloud web related services.

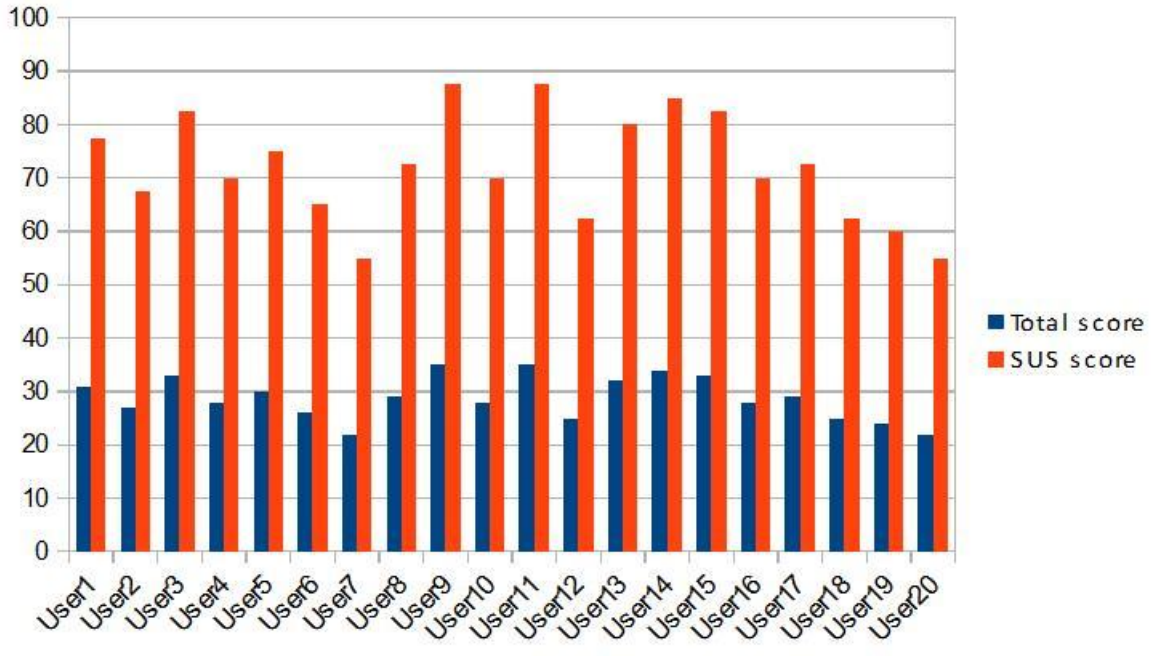

Figure 9 – Bar chart showing total score and the corresponding SUS score the participants

To analyzed and evaluate the IAMSys, SUS questionnaires administered to expert and system admin in the field of Identity Management were used which 72.0 % of the participants aligned to the idea of IAMSys that; it is a way to mitigating security challenges associated with authentication, authorization, data protection, and accountability when properly deployed in an enterprise using a lightweight standard protocol.

Identity and Access Management (IAM) has emerged to help enterprises meet today's business challenges, IAM merges business processes, security policies, and technologies to help organizations manage digital identities (user attributes which describe who users are, how they prove their identity and the resources they can access) and control resources access. Identity and Access Management system is recommended to any enterprise:

– with a large volume of staff where users are provisioned often and often;

– where there is a need to monitor who accessed what and to what extent;

– that have their application and their users not on a single repository;

– where Single Sign-On is a priority among diverse application an enterprise or organization.

As a future work, the research can be extended to accommodate applications that authenticate users using MySQL databases by a way of syncing users provisioned already in MySQL with LDAP server and also to store directory in a relational database engine, such as MySQL or Oracle, by configuring and installing iODBC2 for database backend support.

REFERENCES

1. Bresz, F., Renshaw, T., Jeffrey R., & Torpey, W. (2007, November). *Identity and Access Management*. Retrieved from https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%209%20-%20Identity%20and%20Access%20Management.pdf
2. Dragoş, M. M. (2012). Cloud Identity and Access Management– A model proposal. *Accounting and Management Information Systems, 11*(3), 484–500.
3. Faraji, M., Kang, J.-M., Bannazadeh, H., & Leon-Garcia, A. (2014). Identity access management for Multi-tier cloud infrastructures. *2014 IEEE Network Operations and Management Symposium (NOMS)*. doi: 10.1109/noms.2014.6838229

4. Indu, I., & Anand, P. M. R. (2015). Identity and access management for cloud web services. *2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*. doi: 10.1109/raics.2015.7488450

5. Indu, I., & Anand, P. M. R. (2016). Hybrid authentication and authorization model for web based applications. *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. doi: 10.1109/wispnet.2016.7566324

6. Leandro, M. A., Tiago J., Daniel R. S., Carla M.W, & Carlos B. W. (2012). *Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environment using Shibboleth*. Retrieved from https://www.researchgate.net/publication/257200931_Multi-Tenancy_Authorization_System_with_Federated_Identity_for_Cloud-Based_Environments_Using_Shibboleth

7. Sharma, D. H., Dhote, C. A., & Potey, M. M. (2016). Identity and Access Management as Security-as-a-Service from Clouds. *Procedia Computer Science, 79*, 170–174. doi: 10.1016/j.procs.2016.03.117

8. Singh, A., & Chatterjee, K. (2015). Identity Management in Cloud Computing through Claim-Based Solution. *2015 Fifth International Conference on Advanced Computing & Communication Technologies*. doi: 10.1109/acct.2015.89

9. Sturrus, E., & Kulikova, O. (2016). Identity and Access Management. *Encyclopedia of Cloud Computing*, 396–405. doi: 10.1002/9781118821930.ch33

10. Yang, Y., Chen, X., Wang, G., & Cao, L. (2014). An Identity and Access Management Architecture in Cloud. *2014 Seventh International Symposium on Computational Intelligence and Design*. doi: 10.1109/iscid.2014.221

11. Younis, Y., Kifayat, K., & Merabti, M. (2014). An access control model for cloud computing. *Journal of Information Security and Applications, 19*(1), 45–60. doi: 10.1016/j.jisa.2014.04.003