# Design and Implementation of Network Identity and Access Management System in a Higher Learning Institutions

Calvin Swatulani Silwizya[1] and Aaron Zimba[2]
*1 School of Information and Communication Technology, Zambia University College of Technology, Ndola.*
*2 Department of Computer Science, ZCAS University, Lusaka*
*Corresponding Author Email: csilwizya@zut.edu.zm*

**ABSTRACT – In developing nations most higher learning institutions authenticate users using pre-shared key and this type of security does not provide user identity. The use of a pre-shared key in network authentication is a major problem because the system cannot identify who has access to the network. How can trust be established with a user who has not been seen? User access rights and identities require proper management and have to be controlled along the various phases of the cycle. Moreover, this paper aims to investigate and design the model and framework of secure and easy-to-implement identity and access management that would serve as a blueprint for the implementation of IAM in higher learning institutions. A mixed-method approach was used that includes both qualitative and quantitative. Multiple regression and correlation analysis was performed with the successful implementation of the identity and access management system as the dependent variable and critical practices, considerations in the design, higher learning institutions' ICT policy, and personnel skills as independent variables.**

***Index terms:*** **Extensible Authentication Protocol, Identity Provider, Identity and Access Management, Single Sign On.**

## I. INTRODUCTION

Trusting a person, we are exchanging information with, whom we are not able to see is difficult. However, to create trust with users in this huge network, various digital identity models require to be built to attempt to authenticate users [22]. Identification, authorization authentication, and accountability are essential functions in providing the required services on higher learning institutions' network. Identity and access management has proven to be a key enabling technology in most higher learning institutions, identity and access management has proven to be a key enabling technology. This technology does not only automate the handling of user-level access accounts and their privileges largely, but it also permits a system integration into the existing system processes and offers comprehensive interfaces to managing ICT services and processes. Despite the implementation of identity and access management systems in a few higher learning institutions in developing countries, there are challenges in the design, development, implementation, and maintenance of the system [6].

Trusting a user in a digital ecosystem is a wide topic and a very important one to promote healthy interactions amongst all participants. Trust is more linked to security, technical reliability, respecting user privacy, or authenticity of data and information obtained from internet. Despite the fact that a number of attempts has been made by international and local organisations to help higher learning institutions implement identity and access management, there has not been an overall success [6].

An attempt to help higher learning institutions implement identity and access management by Zambia Research and Education Network through training and deployment has, however, not yielded the overall expected results. In Zambia, there are challenges that the design, implementation, and deployment of network identity and access management such as eduroam have come with. These challenges have negatively affected the implementation. Devices that use legacy wireless adapter cards fail to work with eduroam authentication processes, hence replacement costs become a burden to users of the institution network which discourages and retards eduroam service appreciation [6]. This paper greatly enables higher learning institutions to effectively implement identity and access management. Students and Staff in a remote location can access institution's network services and e-resources using institution's bandwidth. In this regard, students would be able to access institution services and e-resources without directly purchasing the bundles or bandwidth. The paper determines design and architectural works that can positively enhance accessibility, usability and implementation of identity and access management for higher learning institutions. Furthermore, it would establish the critical considerations and best practices for the implementation of identity and access management in higher learning institutions which would improve performance and the overall information and communication technology service delivery. On the other hand, it reveals factors that affect and promote successful overall implementation and use of identity and access management in higher learning institutions. Furthermore, it would announce the concept of using digital credentials for effective authentication and promote creation of policies for easy access management.

This paper suggests the enhancement of system design and effective implementation network identity and access management system that will provide correct access to resources by legitimate users at the right time while preventing unauthorized users from gaining access, it also identifies the critical technology to be used in the design of network identity and access management, create an enterprise framework, determine and enhance the architectural model of network identity and access management.

## II. RELATED WORKS

This paper reviewed literature concerning federal user access, integration with proof of concept, single sign-on, federal user access, decentralized authentication, systems integration, and easy authentication of use devices. Several national research and education networks (NRENs) have built up identity and access management to enable the use of authentication and authorization infrastructures (AAIs), which are referred to as federations to ensure that ICT services can be utilized across higher education institutions (HEI's) borders. For instance, the German federation DFN-AAI provides users from different universities to enroll in e-learning programs and courses offered by other universities in German [13]. Therefore, with such federations, international groups of users, such as researchers in the funded project, fail to access ICT services provided by others, such as a project-wide, collaboration web server, crossing federation borders is become technically not possible due to system architectural design. Users from one federation are not able to access services from another federation [13].

According to [6] each higher learning institution has different policies that guides how network resources are accessed. For instance, some learning institutions allow specific traffic such us (e.g. torrents, Facebook, and YouTube) to pass yet others may disallow the same traffic due to different reasons. However, the author did not state how the design, implementation and methodology can be enhanced in order to have standardised user access levels across the federation.

The Single Sign On is a mechanism that provides the user with the ability to input the same access information and password to logon and access multiple services and applications within an enterprise or federation.

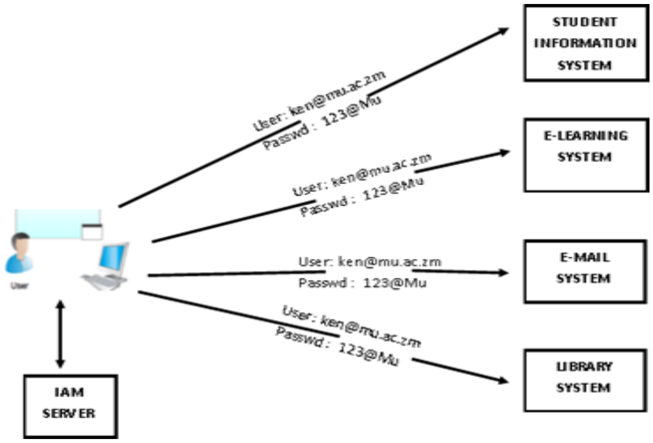

Figure 1: Proposed Single Sign-On Framework

The authentication in higher learning's information systems would also be based on digital certificates. In most instances this is not often the case due to a different design of system platforms and login techniques used in a Universities or Colleges.

Authentication is a process of validating users to ascertain who they claim to be while authorization is a process of granting access to files or services [19]. IAM methods mainly rely on passwords to authenticate users however, it may not be able to keep up with the reality of the future especially where large number of devices would be interconnected [13].

Unlike other papers considered above, this paper endeavored to present a road map of an optimal architectural design of Identity and Access Management that can effectively and efficiently be implemented in higher learning institutions in developing countries. In a few higher learning institutions where eduroam is operational, the implemented technology has challenges connecting and authenticating windows devices, hence and additional software called Secure Windows Terminal Services (secure_wts) has to be installed on windows devices that are connecting to eduroam to achieve the connectivity. Considering higher population of students prevailing in higher learning institutions it is almost impossible to install secure_wts application on all windows devices. It is against this background that this paper proposed an enhanced design and implementation of identity and access management in higher learning institutions in Zambia. Therefore, the paper reviewed literature with regard to federal user access, integration with proof of concept, single sign on, federal user access, decentralised authentication, systems integration and easy authentication on Devices.

## IV. METHODOLOGY

A mixed-method research approach was used in this paper therefore both qualitative and quantitative methods were considered to collect data on the challenges in managing user access to institution network. The approach taken for the research was based on both the exploratory study and the Design Science (Hevner and Chatterjee, 2010) as this was intended to design an identity and access management system that is able meet the prevailing Zambian demand and environmental conditions. In in this paper Spiral model was employed as it combines architecture and prototyping by stages. This model also allowed some adjustments during the development cycle for the effective operations, designs, implementation and management of identity and access management infrastructure resources at the selected University.

In the design, a phased approach was adopted by implementing MySQL Database System to evaluate the Identity and Access Management. Research questions were administrated to stakeholders in higher learning institutions and national research education network who are in the ICT field. Based on this, data was gathered and an analysis was performed. User accounts were designed to provision/de-provision, permissions, roles will be created, role permissions and how they will be assigned and revoked from users. Further to this, IAM logs environment was developed to monitor eligibility of user's credentials, account hijacking and data breaches. The logs also enable IAM administrators to filter the number of failed and successful login and correct access to the ICT applications and services.

The research instrument was assessed for reliability using the Cronbach Alpha analysis and the coefficient for reliability of the paper. Daniel [7] postulates that the reliability coefficient above .863 or 86.3% shows that the instrument is reliable enough to be use in the paper. Correlation analysis was used to establish the strength and direction of the relationship between the variables in the paper.

Identity and Access Management system was segmented into three (3) systems as follows:

i. Radius Server Authentication System
ii. MySQL Database
iii. Web Interface

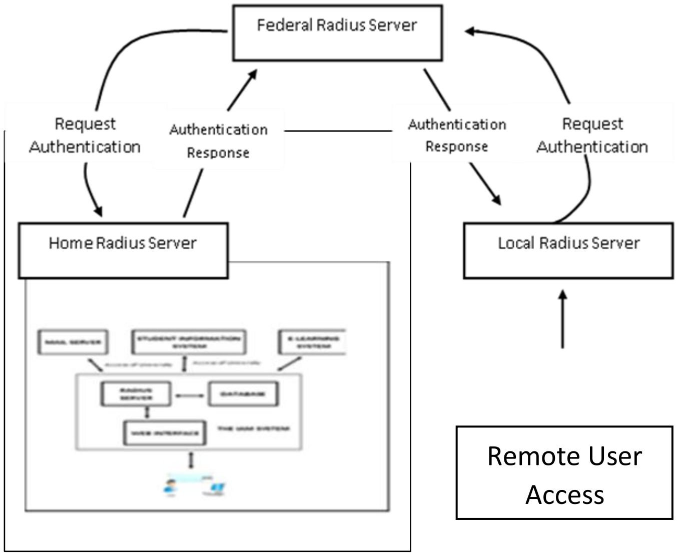

Figure 2: IAM Framework design

The entire system was built on a Linux Operating System Environment and the following are the tools and technology that will be used:

i. Ubuntu Server 20.04
ii. Nginx Web Server
iii. MySQL Database System
iv. PHP, HTML and CSS for coding
v. Free radius

## V. SYSTEM DEVELOPMENT

The Identity and Access Management System design phase focused on outlining the technology that was used in the actual implementation of the system. The system incorporates a number of components that builds it up. The first one is the web-based administration front-end that is used to run and manage components of the system in an easy and professional way. The interface was built with modern web technology as a central dashboard to manage users, devices, free radius and debugging. This system is built on free radius and is designed to run on apache or Nginx web servers has advanced features but is also easy to get started with initially.

This Identity Access Management System Design model provides decentralized and secure the IAM system and improves systems setup in higher learning institutions in Zambia as shown in figure

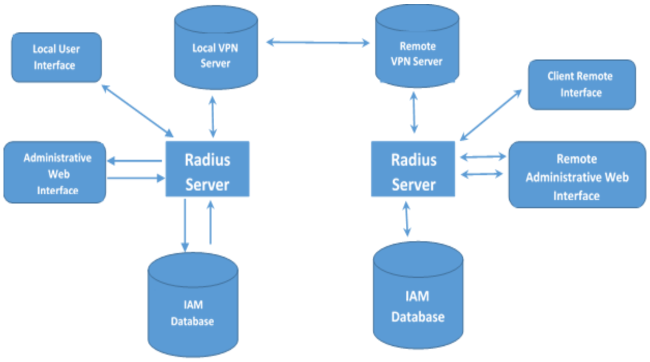

Figure 3: Decentralized and Secure Identity Model

There are multiple components considered in the design of the IAM system. This includes provisioning, management of accounts, governance of identities, authenticating, access control, federating of identities and authorization. IAM components were further sub divided. Identity governance shows the role of engineering, analysis of identities, duties segregation, consolidation of roles, delegation of identities, management of risks and compliance. Authenticating users includes multi-factor process, risk-based authentication on the other hand access control relates to access control based on specific attributes or roles and policies that are designed. Federation of identities streamlines single sign on and out, management of session and sharing of attributes.

The implementation required the design of database with tables that would be used to store data and information of the identity and access management system. In IAM, the database defines the identity that has what access to a specific resource. Permission is grouped into roles and policies instead of granting direct access to the end user. The grouped members are assigned into roles, and it is the roles that are granted to authenticated members hence the design and creation of a database.

In order to implement this task Linux, Nginx, MySQL, PHP (LEMP) was required to be installed. After all the installation and configurations were done a test was done to verify if all configurations were successful. The implementation phase, the database is installed on the respective hardware and to run an optimized database on the software and hardware platform. This also requires establishing a database security and give the various users access applicable to their requirements. Tables where designed to hold variety of data.

### A. System User Interface Design

The design of user interface encompasses an interactive activity where different stakeholders can interact at different levels of fidelity on various devices and computing platforms.

In this IAM system the interfaces were divided in to two (2) categories:

#### i. The Administrative Interface

This is the interface used to manage the identity and access management configurations. The interface is used to create users, add access points, define realms, configure virtual private network and entirely manage the system.

### B. The Client Portal and Administrative User Interface

This is the interface used by client users in order to be authenticated and gain access to the network or internet. This is the interface which the administrator logs in to do configurations of the system. The admin user is required to enter the username and the password in order to authenticate and gain access to the identity and access management system. The admin user can perform tasks such as creating client and admin users, adding access points (AP) and network access server (NAS), configuring remote and local network access, create realms and monitoring network traffic.

### C. System Testing

The IAM system acceptance testing and evaluation was carried out during system testing. The system was evaluated successfully. From results obtained the concept of IAM System as a way to mitigating security loopholes associated with authentication, authorization, data protection and accountability when effectively deployed in a federal standard protocol.

Identity and Access Management (IAM) integrates organizational processes, policies of security, and ICT technologies to assist management of digital identities in organisations that are attributed to users which analyses user's identity, how their identity can be proved and what resources can be accessed and controlled.

## VI.RESULTS PRESENTATION AND ANALYSIS

System acceptance evaluation and testing was performed and a total of 45 questionnaires were administered to participants. The participants included systems administrators, network administrators, ICT technicians and campus network users in higher learning institutions.

Usability Scale (SUS) Questionnaires were administered in selected higher learning institutions. In order to calculate the system usability, scale the data collected and analysed using SPSS as indicated in the table 2.

Table: 2 System Usability Scale

| Item | Mean | Std. Deviation | Skewness | Kurtosis |
|---|---|---|---|---|
| IAM System Design effectiveness | 1.85 | 0.791 | 1.296 | 2.134 |
| IAM System usability | 2.12 | 1.078 | 1.567 | 2.264 |

Statistics from data on this variable were slightly above the mean as reflected by a mean of 1.85 and 2.12. The majority of the IAM system expert and administrator's response indicated that the proposed IAM system meets the design effectives and system usability in improving security and network accessibility in higher learning institutions. Evaluation was conducted on the assumptions over regression analysis using normal probability plot obtained from the SPSS output as shown in figure 6.

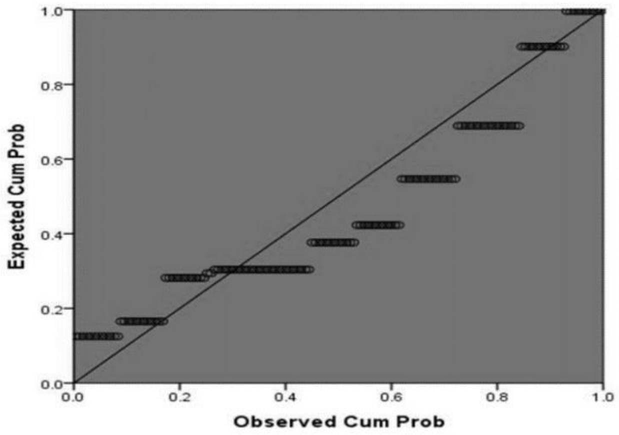

Figure 6 Normal Probability Plot

Practical comparatives were performed to prove the practical contributions of this paper. In the presentation of results obtained in this research it was found that:

- Implementation of effective and reliable authentication of IAM improves security and access of the network in higher learning institution in Zambia.

## VIII. CONCLUSION

Implementation of this IAM system provides a strong base system for an enterprise being on campus. In most higher learning institutions in developing countries, this identity and access management will prove to be a key in enabling technology which does not only automate the handling of user accounts and their roles to a large extend, but also promote tight integration into the existing organizational processes and provides comprehensive interfaces to ICT service management processes. The paper brings out designs and architectural works that can positively enhance accessibility, usability and implementation of identity and access management for higher learning institutions.

This research paper has addressed how decentralized, secure model and IAM best practices in the design and implementation of Identity and Access Management would benefit higher learning institutions in in the nation of Zambia. In order to effectively develop and implement Identity and Access Management System in higher learning institutions in Zambia, with regard to the findings needs to improve the level of skills of ICT personnel and deliberately encourage Universities and Colleges to acquire equipment identified in this paper. Policy stakeholders and managers in learning institutions in Zambia should standardise the ICT policies to enhance and have the same standard ICT operating procedures.

## REFERENCES

[1] Ajzen Icek, & Zemore Sarah. (2014). *Predicting substance abuse treatment completion using a new scale based on the theory of planned behavior—ScienceDirect*. https://www.sciencedirect.com/science/article/abs/pii/S0740547213001451

[2] Argyrous George. (2011). *Statistics for Research with a guide to SPSS. Second Edition*.

[3] Berk K.N, & Carey, P. (2010). *Data Analysis with Microsoft Excel*.

[4] Bergweiler, S., Deru, M., and Porta, D (2010) Integrating a multi-touch kiosk system with mobile devices and multimodal interaction. In Proc. of ITS'2010 Conf. on Interactive Tabletops and Surfaces. ACM Press, New York, 2010, pp. 245--246

[5] Bacharach, S. B. (1989). Organizational theories: Some criteria for evaluation. Academy of management review, 14(4), 496-515.

[6] Christopher Chembe, Douglas Kunda, & Macmillan Simfukwe. (2014). *Challenges and Benefits of Educational Roaming (eduroam) Service to ZAMREN Member Institutions*.

[7] Daniel, L. G. (1996). *Kerlinger's Research Myths*. 4.

[8] Detken. (2008) Trusted Network Connect – die sichere Einwahl mobile Mitarbeiter ins Unternehmen, Handbuch der Telecommunication, Deutscher Wirtschaftsdienst, 129. Ergänzungslieferung

[9] Dragoş, M. M. (2012). Cloud Identity and Access Management– A model proposal. Accounting and Management Information Systems, 11(3), 484–500

[10] Eren, E., & Detken, K.-O. (2010). *Identity and Access Management According to the Implementation of the Simoit Project and TNC@FHH*. *9*(1), 10.

[11] Musambo. L, M. Chinyemba and J. Phiri, "Identifying Botnets Intrusion and Prevention," Zambia ICT Journal, vol. 1, no. 1, pp. 63-68, 2017.

[12] Hommel, W. (2009). E-Learning in Shibboleth-based federations: The design rationale behind the German DFN-AAI E-Learning Profile. Proc*eeding of EUNIS 2009*.

[13] Johan Janssen. (2008). *Identity management within an organization*.

[14] Juliana De Groot. (2019). *What is Identity and Access Management*.

[15] Kennedy Abwao. (2019). *A Data Logger For Monitoring Maternal Vital Signs*. http://41.204.161.209/handle/11295/107135

[16] Koelewijn, G. (2009). *Identity & Access Management*. https://scholar.google.com/scholar?cluster=4720492852213417932&hl=en&as_sdt=0,5&sciodt=0,5

[17] Kunda. D and M. Chishimba, "A Survey of Android Mobile Phone Authentication Schemes," Mobile Networks and Applications - Springer, pp. 1-9, 2018.

[18] Latifa Boursas, & Wolfgang Hommel. (n.d.). *Efficient Technical and Organizational Measures for Privacy-aware Campus Identity Management and Service Integration*.

[19] Paulo Alves, & James Uhomoibhi. (2010). *Issues of e-learning standards and identity management for mobility and collaboration in higher education*.

[20] Rosencrance, Linda (2002) "SAML Secures Web Services", Computerworld, vol. 36, no. 35:30-30

[21] Sullivan, D. (2009). The definitive guide to security management. *Channel Partner Real Time Publications*.

[22] Valentine Gerard. (2019). *Designing the future identity: Authentication and authorization through self-sovereign identity*. https://repository.tudelft.nl/islandora/object/uuid:200f1df0-adda-47a1-894c-baf54133035a/datastream/OBJ/download