International Digital Organization for Scientific Research ISSN: 2579-079X
IDOSR JOURNAL OF SCIENCE AND TECHNOLOGY 6(1):52-62, 2021

Design and Implementation of Enhanced Security Information System for Corporate Platform.

Osondu O. Ezekiel[1], Akawuku I. Godspower[2], and Ofuasia Cyril[3]

[1, 2, 3] Department of Computer Science, Nnamdi Azikiwe University, UNIZIK, Awka, Nigeria.

ABSTRACT

With the exponential development and speedy growth of information economy, information security urgency is expedient. This paper presents a security model cryptograph algorithm which would enable authentication and authorization of access from different platforms in Information systems, providing a Biometric authenticating and authorization system that would identify any access from diverse platform of the organization. The experimental testbed is Nnamdi Azikiwe University Student portal with different application modules running in different server; each server/application provides its own authentication and authorization request to the systems resources by users. The Object-oriented Hypermedia Design Method- Java 2 Enterprise Edition (OOHDM- J2EE) is the methodology adopted for this research. Consequently, result showed that within this framework, users enjoy seamless, secure access to partners' services via a single sign-on (SSO) to multiple applications.

Keywords: Authentication, Authorization, Information system, Cryptograph algorithm.

INTRODUCTION

The U.S. National Information Systems Security Glossary defines "Information Systems Security" as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. [1].

The security of industry's systems and information is essential to its safety and soundness and to the privacy of users and customers information's. Information security enables an institution to meet its business objectives by implementing business systems with due consideration of information technology (IT)- related risks to organization, business and trading partners, technology service providers, and customers. [2].

National Academy of Sciences (2017) asserts that Organizations and people that use computers can describe their needs for information security and trust in systems in terms of Confidentiality, Integrity, Authorized manner, Availability.

RELATED WORKS

[3] has it that, Information security is the protection of information and information systems from unauthorized access, disclosure, modification, destruction or disruption.

Case 1: In the work of [4] on "Portable Secure Identity Management". This work focused on developing identity maintenance and distribution system, and the storage of profile data on a centrally accessible, yet distributed system

Case 2: [5] provided a glimpse into the issues in identity management, these include privacy issues or risk related to the stealing of identity (identity theft) yet not exploited.

Case 3: These authors [6] significantly focused on applying identity-based cryptography (IBC) to web services. The key idea is to generate and use public keys based on publicly available information which can be used to uniquely identify users yet the geo-location component was not integrated.

Case 4: [7], published a paper titled "Federated Identity- Management Protocols–Where User Authentication Protocols May Go", and this paper suggested and discussed Federated identity management as providing a simple user management in an increasingly dynamic world. The paper also discussed the functionalities of Federated identity management protocols though theoretical.

In conclusion, the above reveals the gap in existing security models hence the design and implementation of enhanced security information system for a corporate platform, particularly in the face of advanced global risk and vulnerabilities experienced in information systems.

MATERIALS AND METHODOLOGY

The material ranges from hardware to Operating System, to the development tools. Object-Oriented Hypermedia Design Methodology (OOHDM) was adopted.

Hardware Requirements

The hardware requirement is grouped into namely, server side and client side as depicted in the table below:

Table 1:Hardware Requirement of the System

COMPONENT	SERVER SIDE	CLIENT SIDE
MEMORY	8 GB RAM + 2GB GRAPHICS ADAPTER	250 MB RAM
CPU	8 GHZ	1GHZ
HARD DISK	1 TB	1 GB OR Higher
WEB CAMERA	NOT REQUIRED	REQUIRED
FINGER PRINT SCANNER	NOT REQUIRED	REQUIRED

Software Requirements

Software denotes programs that run on computers, the hardware. They comprise of the entire set of programs, procedures, and routines with the operation of a computer system. The software requirements for the new system are:

Table 2: Software Requirement

COMPONENT	SERVER SIDE	CLIENT SIDE
OPERATING SYSTEM	Windows 2003 Server	Windows 8.1 or Higher
WEB BROWSER	MSIE 9 OR HIGHER; Google Chrome 8 or Higher; or Mozilla 10 or Higher	MSIE 9 OR HIGHER; Google Chrome 8 or Higher; or Mozilla 10 or Higher
DBMS	MSQL 5 OR higher	NOT REQUIRED
WEB SERVER	XAMPP 7 OR Higher	NOT REQUIRED
MS OFFICE SUITE	NOT REQUIRED	MS EXCEL 2007 OR HIGHER

Development Tool Requirements

The following tools were used HTML 5, JavaScript, Cascading Style Sheet (CSS) version 3 and PHP 7. PHPMyAdmin Database Management System (DBMS) will be used to model and implement the NAUSSOPDB backend.

Methodology

The OOHDM- J2EE is the methodology adopted for this research work to design user management module using two factor authentication and authorization system for Nnamdi Azikiwe University

Awka Student Portal for managing user's privileges and access rights. Hash Functions encryption algorithm will be used in encrypting and decrypting identity data. To construct authentication and authorization model, Federation will be used. Federation is an identity management technology that makes identities portable across domains so that they can be efficiently shared with and leveraged by trusted partners. It provides the mechanism whereby an enterprise can accept that external users have already been authenticated by a trusted partner and can grant them access without having to be responsible for managing all their identity information. Within this framework, users enjoy seamless, secure access to partners' services via a single sign-on (SSO) to multiple applications noted by Sun Microsystems (2011).

SYSTEM DESIGN

We consider the existing system with a view to discovering the problem areas and making further efforts to improve on the problem areas. The overall emphasis will be of the security policies and algorithms of the previous, adopting a modern methodology to implementing an enhanced security model for information systems for corporate platform. Then the System design entails the designing of each module or class and sub module within the proposed system which is aimed at meeting the objective(s) of this work. More specifically, Nnamdi Azikiwe University student portal platform is used to demostrate the enhanced security frameworkdesigned.

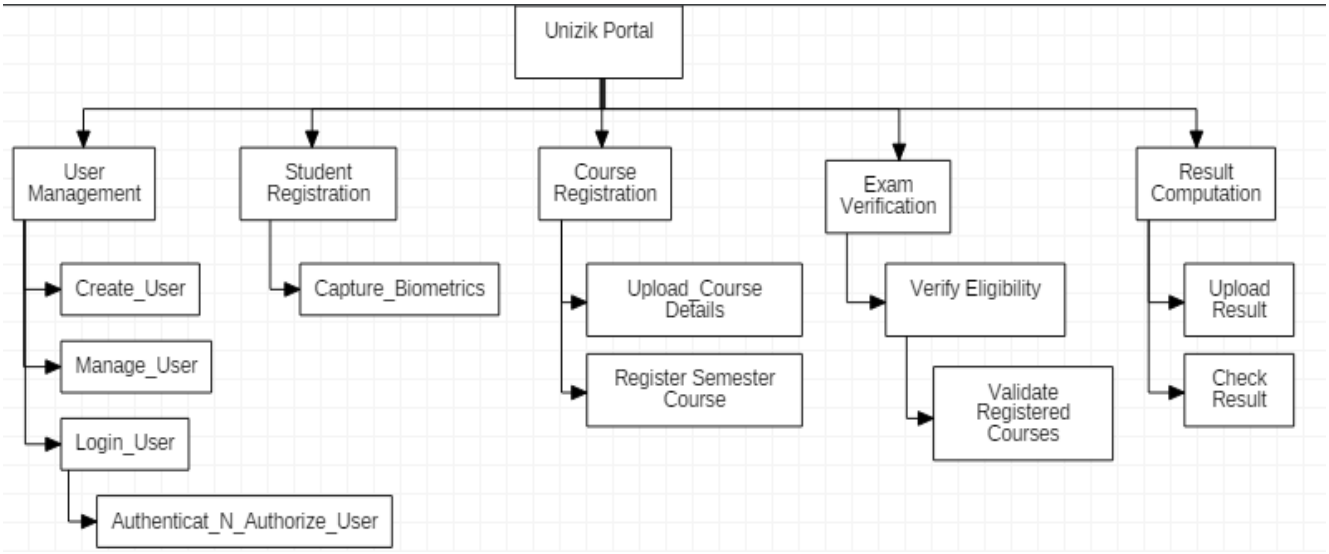


Figure 1:High Level Model of the Proposed System

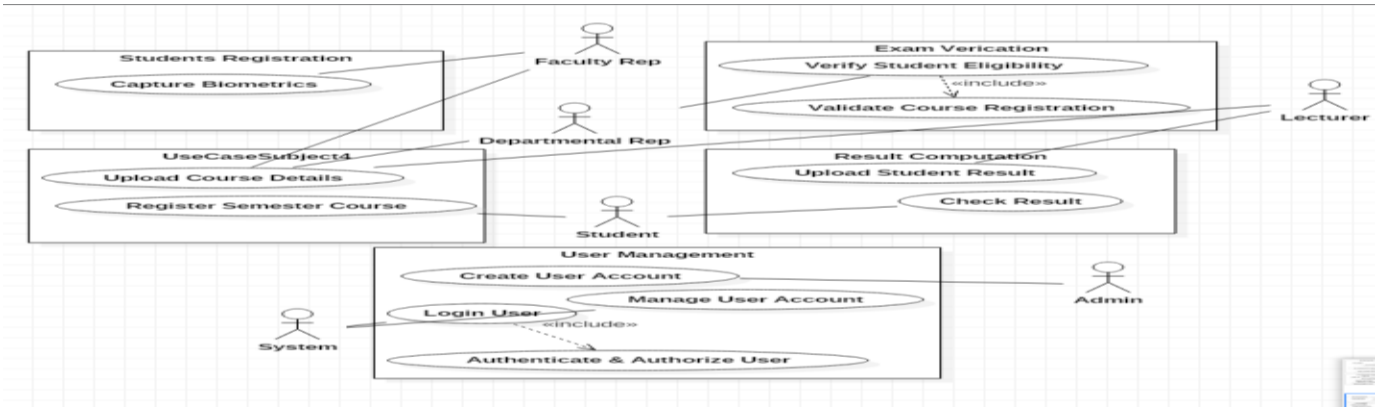


Figure 2: Use Case Diagram of the Proposed System

Database Design and Structure PHPMyAdmin Database Management System (DBMS) was used to design/ model and implement the Database NAUSSOPDB.

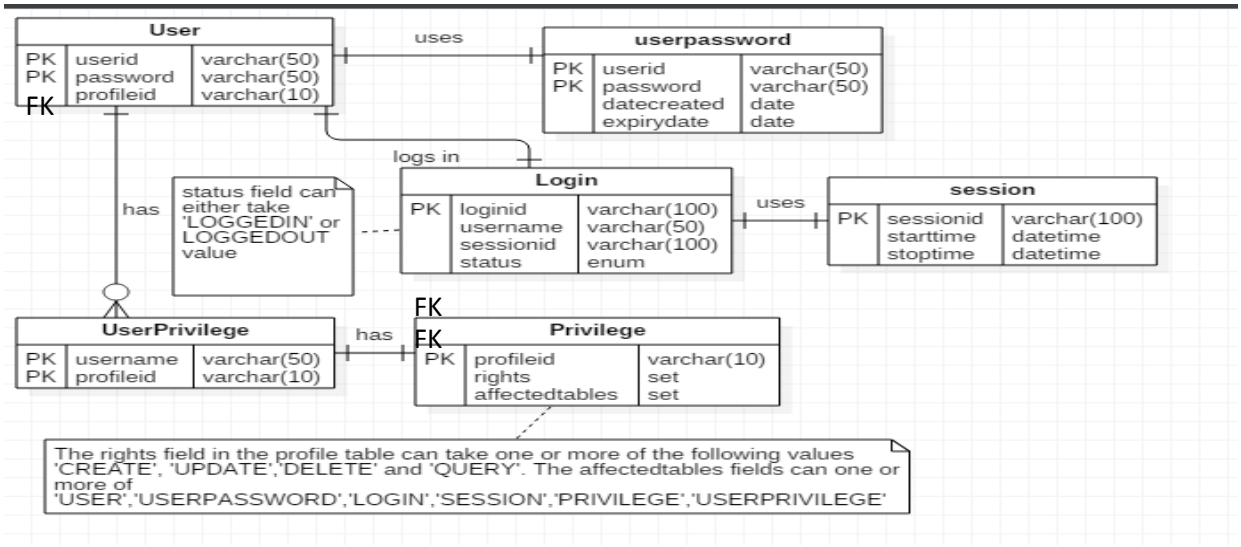


Figure 3(a) Entity Relationship Diagram of UserDB

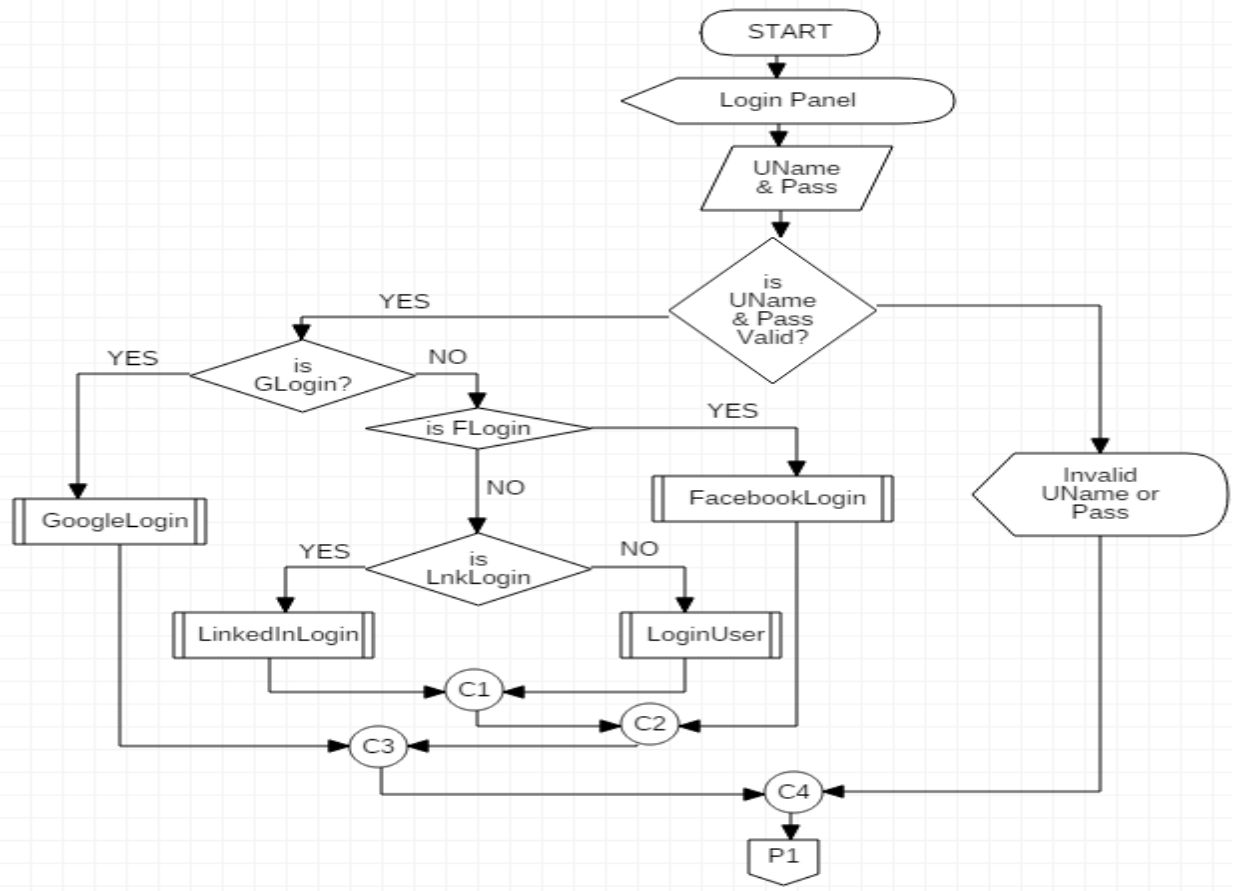


Figure 4: System Flow Chart

SYSTEM DEVELOPMENT AND IMPLEMENTATION

The development of the new system was done modularly. Then writing the security policies and algorithm for the system adopting the methodology discussed in the previous aspect of this work. The following languages were used to develop the program for the new system: HTML 5, JavaScript, Cascading Style Sheet (CSS) version 3 and PHP 7. While Integrated Development Environment (IDE) used is Sublime (Text Editor).

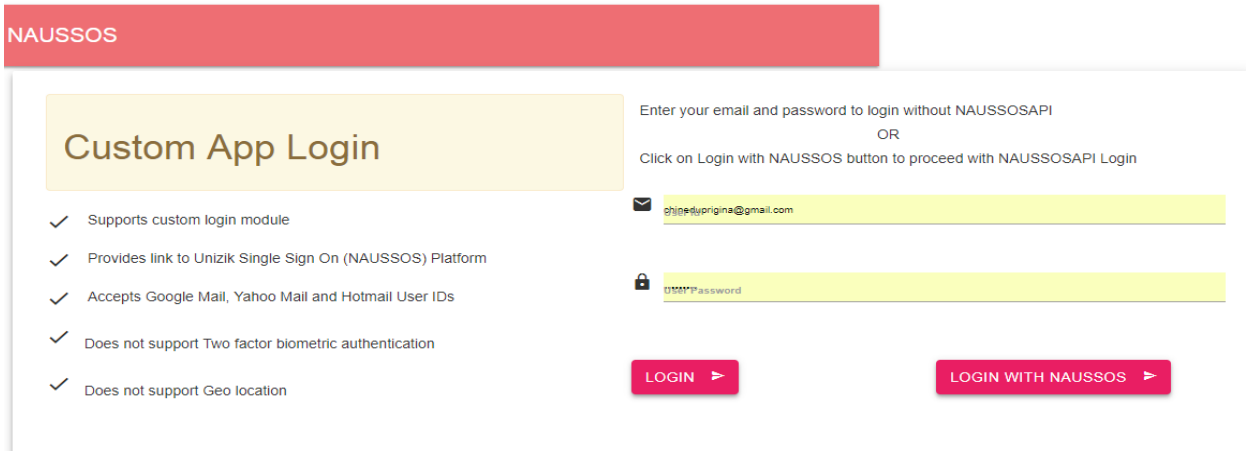


Figure 1 Application Login

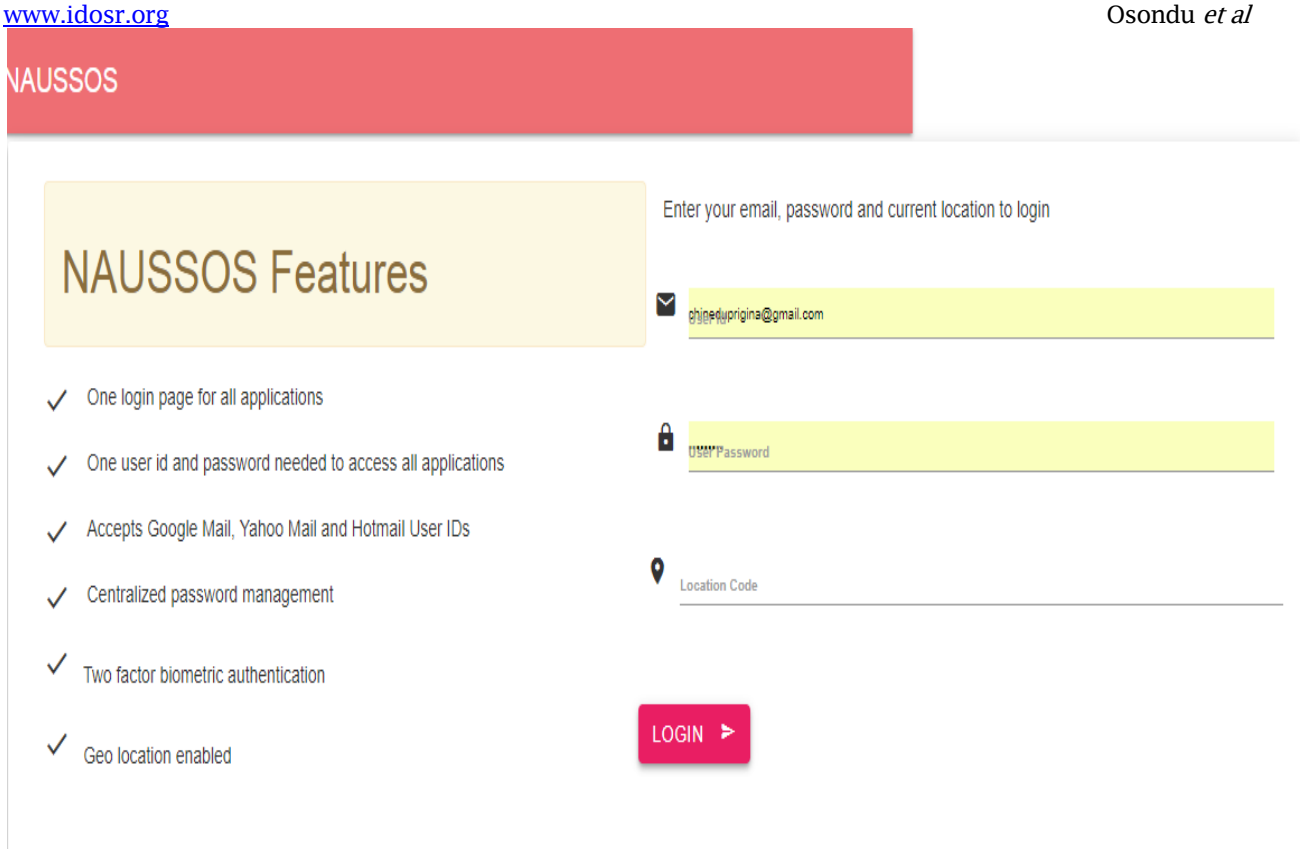


Figure 2: NAUSSOS Login Page

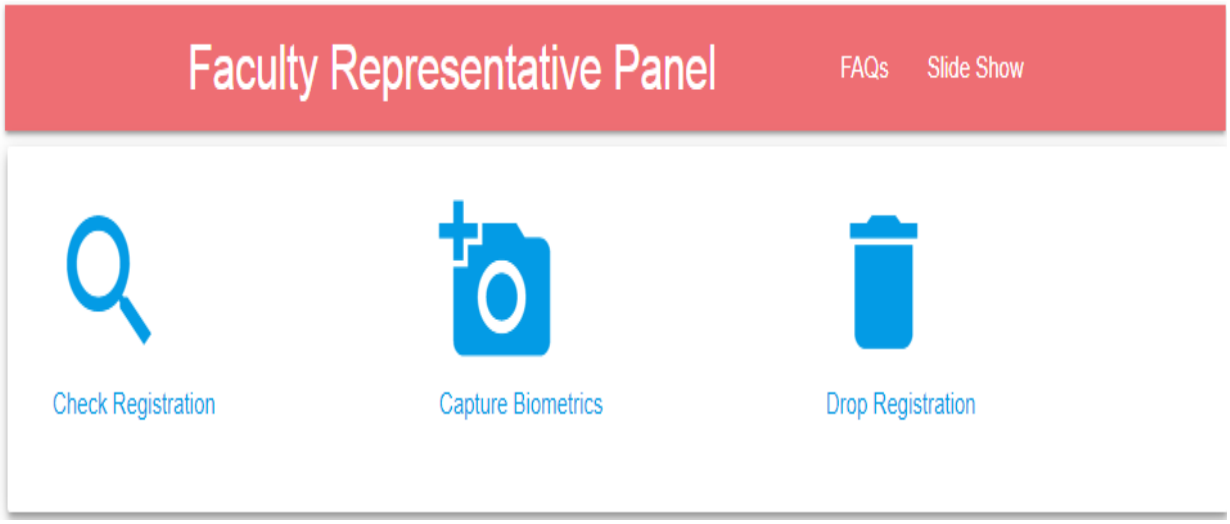


Figure 3: Faculty Representative Control Panel

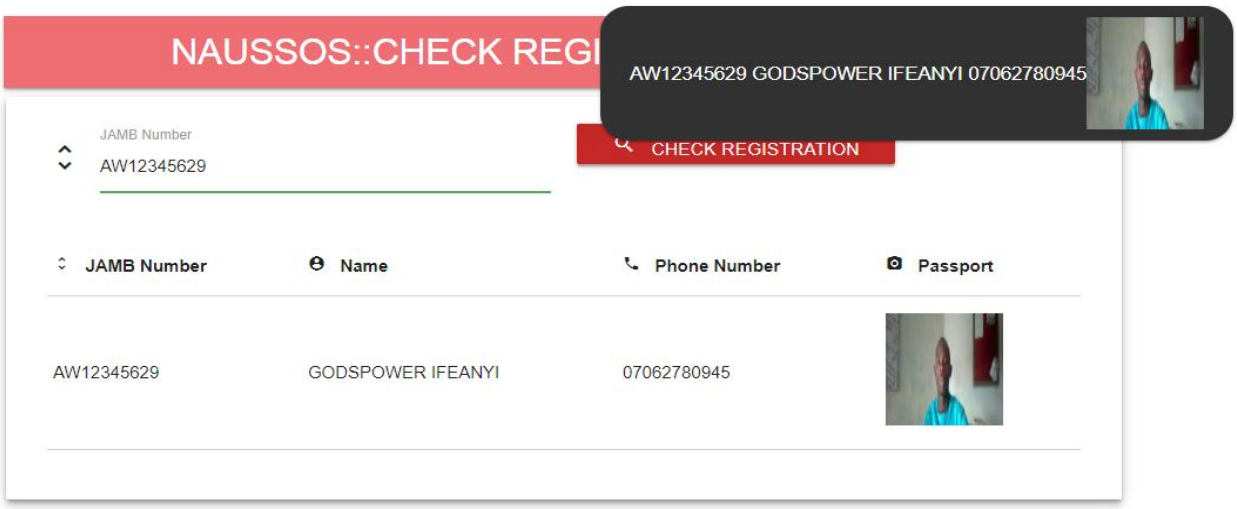


Figure 4: Check Registration Control Panel
Check Student's Result Panel

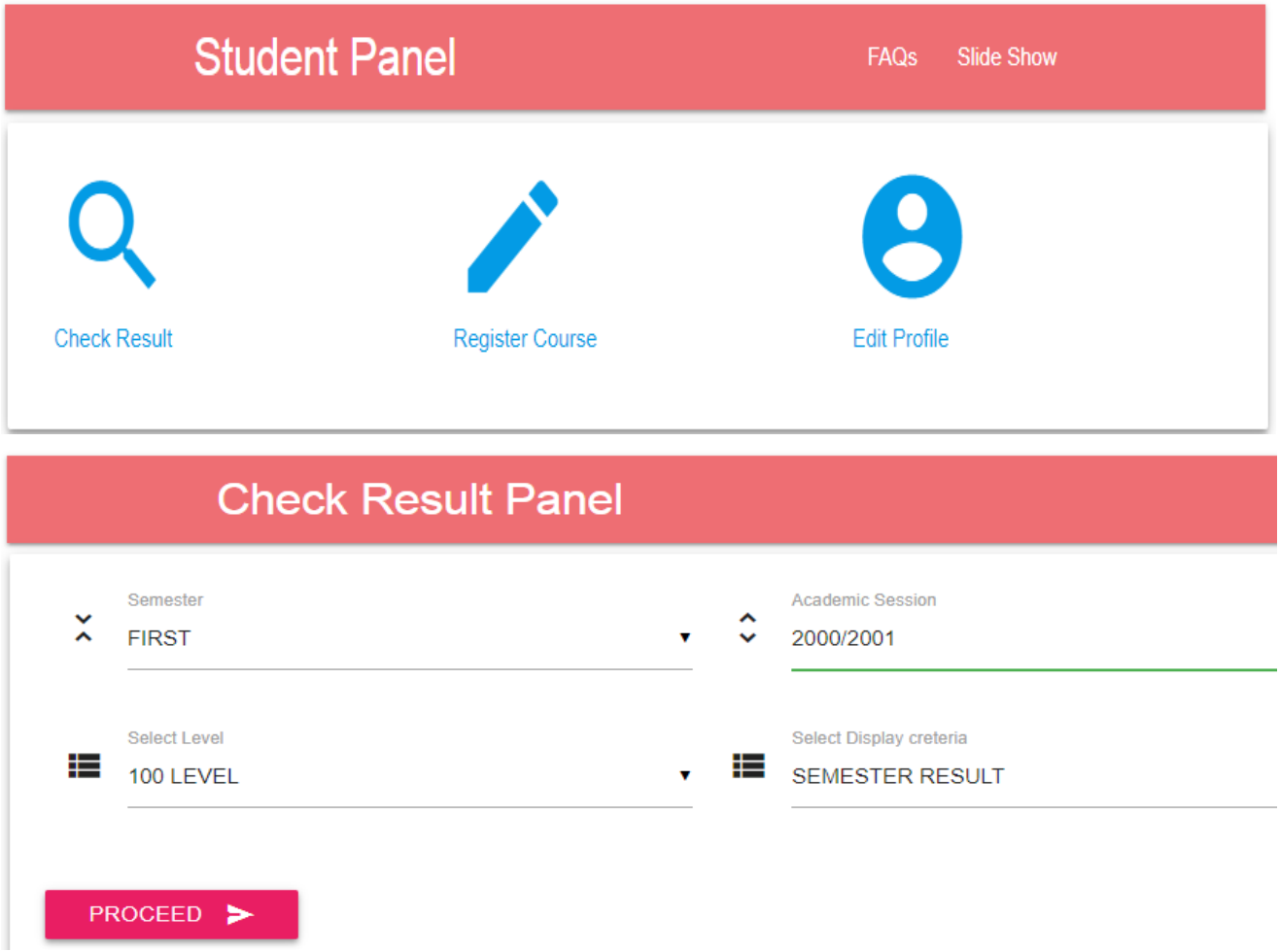


Figure 5: Student's Control Panel

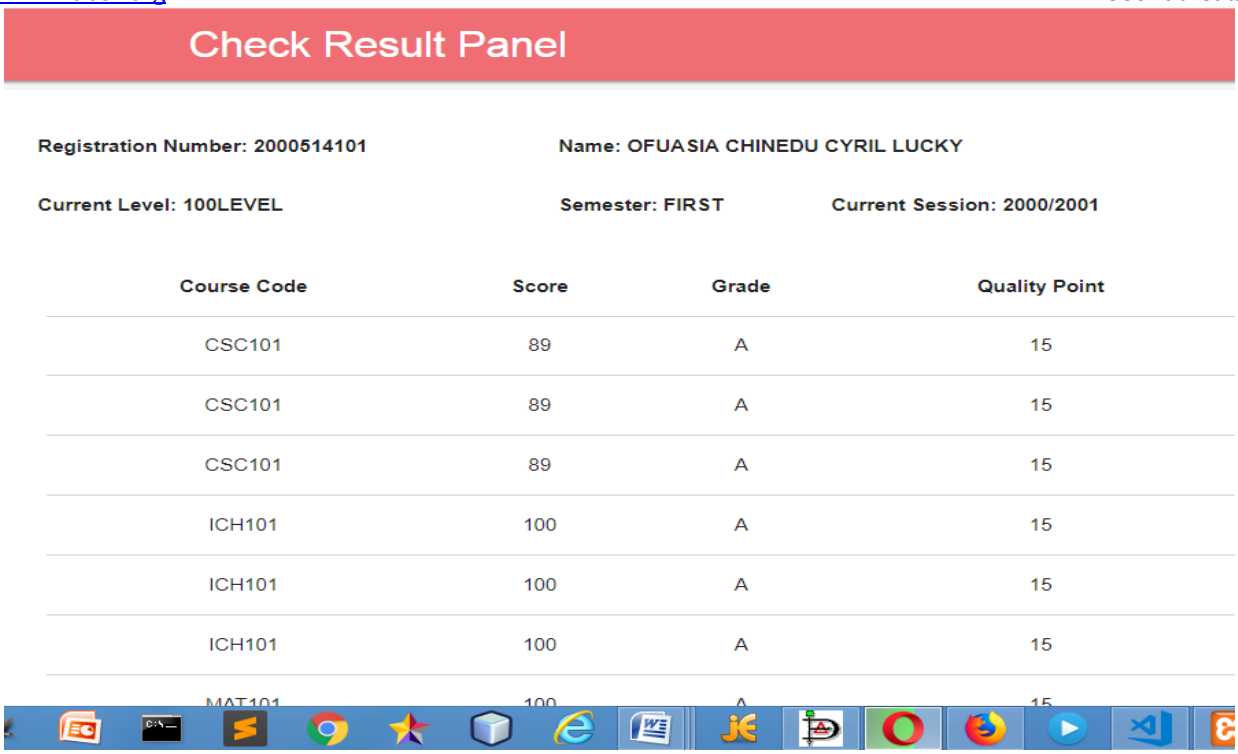
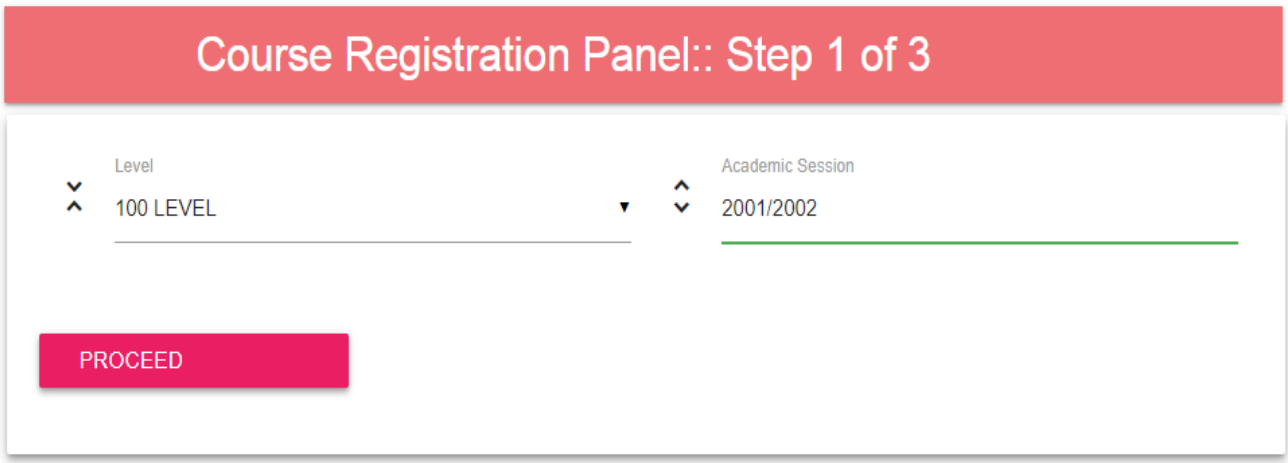


Figure 6: Display Student's Result Panel



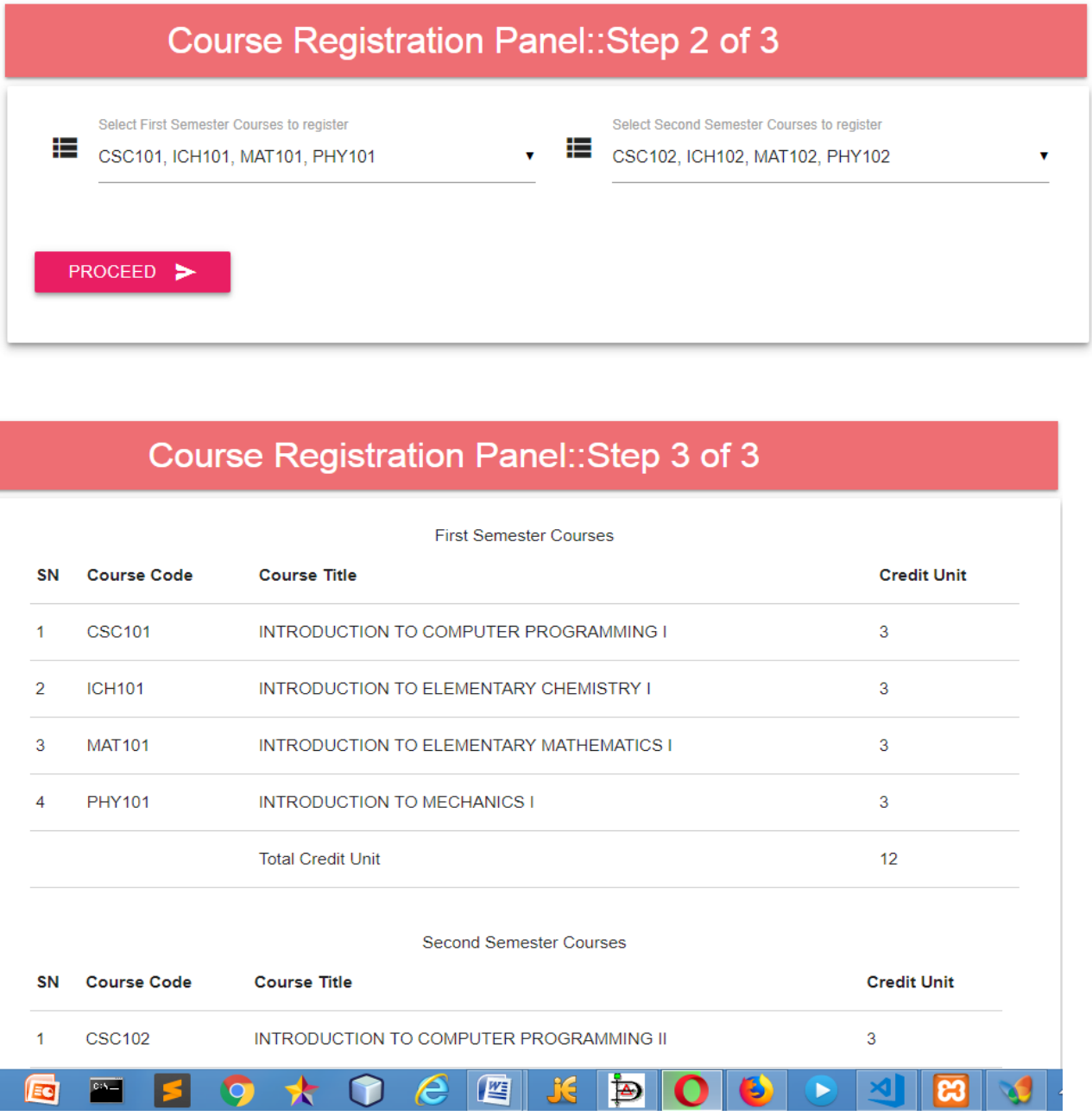


Figure 7: Student's Course Registration

RESULTS AND DISCUSSION

We were able to achieve the main objectives of the research work which is creating a central user authentication and authorization portal for Nnamdi Azikiwe University portal system using the OAuth (Open Authentication) protocol. Google, Face book and LinkedIn sign on were integrated into the NAUSSOS, thereby enabling staff and students with either of these accounts to securely login to NAUSSOS portal system. Users system's fingerprinting and geo-location techniques to capture system unique signature and identify user location is another of concern for further implementation.

SUMMARY, CONCLUSION AND RECOMMENDATION

In this work, have designed and implemented a system to enhance security in Information Systems specifically on corporate platforms or enterprises. The researchers implemented Authentication and Authorization systems to ensure the Confidentiality, Integrity and Availability of an information System.

The result showed that the proposed enhanced security model for information systems of cooperate platform (UNIZIK) used handled multiple authorization and authentication menace, that only one login page will direct all login requests of the different modules to one Single Sign On Server (SSOS), which will in turn redirect users to their requested resources/ module when authenticated, leveraging on the Geo-location integration for location validation. The emergence of this newly developed system will solve the shortcomings of the existing systems and also reduce time and resources incurred while using the existing system.

Our Conclusion, the security model for information systems of cooperate platform will handle user's data separately from the applications sensitive data by storing the user's data on a separate server from the applications servers improving security. Memory resources of both user and applications servers are fully optimized. Consequently, User data is transparent to all applications within the school information systems domain irrespective of the hosting server. Finally, ease to generate single users' access right reports for all the modules with simplified Users Audittrail.

REFERENCES

1. Crampton, J., Lim, H. W., and Paterson, K. G. (2007). What Can Identity-Based Cryptography Offer to Web Services? UK: Information Security Group, Royal Holloway, University of London, Egham.
2. Federal Bureau of Investigation [FBI]. (2002). Biometrics Technology Introduction. Retrieved From https://www.dhs.gov/biometrics Retrieved 21st March 2020
3. Federal Financial Institute Examination Council. [FFIEC] (2006). Information Security. Retrieved From http://ithandbook.ffiec.gov/media/222209/info_sec_2006.pdf Retrieved 21st March 2020
4. Information Systems Audit and Control Association [ISACA] (2011). Geo-location: Risk, Issues and Strategies. Retrieved From http://www.isaca.org/groups/professional-english/wireless/groupdocuments/geolocation_wp.pdf Retrieved 21st March 2020
5. Linda Pesante. (2008). Introduction to Information Security. Retrieved From https://www.uscert.gov/sites/default/files/publications/infosecurity basics.pdf Retrieved 21st March 2020
6. Microsoft Corporation. (2016). Web Application ASP.NET. Retrieved From Microsoft Corporation website https://msdn.microsoft.com/en-us/library/aa286485.aspx 21st March 2020
7. National Academy of Sciences [NAS] (2017). Concepts of Information Security Retrieved From. https://www.nap.edu/read/1581/chapter/4 Retrieved 21st March 2020
8. Pfitzmann, B. and Waidner, M (2004). Federated Identity-Management Protocols Where User Authentication Protocols May Go.
9. SAP NetWeaver Single Sign – On (2011). Product Management SAP NetWeaver Identity Management & Security.
10. Staite, C. (2010). Portable secure identity management for software engineering retrieved from https://dl.acm.org/doi/10.1145/1

810295.1810375 Retrieved 2nd Feb. 2020

11. Sun Microsystems (2011). Identity Federation: Transcending the Boundaries of Business for Secure Collaboration. Retrieved https://www.sans.org/reading-room/whitepapers/auditing/introduction- information-system-risk-management-1204
12. Taylor, Lips and Organ (2010). Identity Management. Retrieved https://www.sans.org/reading-room/whitepapers/auditing/introduction- information-system-risk-management-1204
13. University of Nevada, Las Vegas (2015). Definition of Information Security. Retrieved From http://oit.unlv.edu/network-and-security/definition- information-security.