INTERNATIONAL JOURNAL OF SOFTWARE ENGINEERING & COMPUTER SYSTEMS (IJSECS)
ISSN: 2289-8522 e-ISSN: 2180-0650
VOL. 7, ISSUE 1, 36 – 46
DOI: https://doi.org/10.15282/ijsecs. 7.1.2021.4.0080

ORIGINAL ARTICLE

Se-LMS: Secured learning management systems for smart school

O.J. Falana[1]*, I.O. Ebo[2], O. Akinwunmi[3], I.O. Odom[4]

[1]Department of Computer Science, Federal University of Agriculture Abeokuta, Nigeria.
[2, 4]Department of Computer Science and Mathematics, Mountain Top University, Ibafo, Nigeria
[3]Department of Computer Science, D.S.Adegbenro ICT Polytechnic Itori-Ewekoro, Nigeria.
.

ABSTRACT – One of the research topics that focus on Information Communication Technology in Education is Learning Management System (LMS). LMS is a web-based software application developed to create, manage, and delivered e-learning courses. Many research works have been conducted on different learning options in LMS. However, the increased use of LMS has brought with it the security issues such as the denial of service attack, malware and privacy. In order to protect the different actors of LMS such as students, instructors and controlling authorities, this paper proposes a multi-factor authentication and identity management for securing LMS. Se-LMS is capable of dynamically authenticating users using different methods such as a seamless combination of Oauth2.0 and 2FA or Username/Password and 2FA as proposed. Also, the paper explains the situation and existing research relating to security in Learning Management Systems in smart school. The proposed framework has been applied to cloud-based LMS to show the ability to mitigate an attack.

ARTICLE HISTORY
Revised: 23 May 2020
Accepted: 28 Sept 2020

KEYWORDS
Learning Mmanagement System (LMS), learning, cloud computing, OAuth2.0, smart school, Se-LMS

INTRODUCTION

Over the past few years, the Learning Management System (LMS) has become an important component of teaching and learning in higher education institutions. In recent times, it has gained widespread acceptability among individuals, education institutions, local or national authorities due to the spread of COVID-19. LMS is any type of learning accomplished by computer technology, particularly those web base technologies [1]. The term LMS is a broad concept, covering a wide scope of applications, procedures, and expressions such as online learning, net learning, computer-based learning, virtual or simulated instruction, and electronic cooperation [2].

Australian national training specialist reports that electronic learning or LMS has a more extensive idea than learning under the web, which contains a wide scope of utilizations and procedures that apply electronic media for introducing proficient preparing and adaptable learning [3-4]. The growing students' enrolment and the flexibility in the supply of adequate education resources have necessitated the need for the development of LMS which is an important component of the smart school. Smart school is typically associated with the seamless integration of digital technology and architecture through efforts to improve the sustainability, adaptability, governance, and efficiency of learning environments [5-6]. Learning will be more fascinating, simulating, persuading and important as smart schools develop [7].

Security and privacy remain a very big challenge to LMS due to its openness and growing popularity. According to Security [8], cyber-attacks on education facilities have been on the increase due to the nature of sensitive information collected from the students to make it easier for the educators. Given the complexity of today’s educational institution networks and the threat to their security compared to a decade ago, it is glaring that the traditional security solutions and weakness in network security are not going to stop the attacks. More so, most LMS platforms make use of conventional security approaches and processes which include verification, validation and permission. Any security design for LMS must address the data availability, data integrity from unauthorised access and security incidents. A public key infrastructure (PKI) approach that provides security properties and services for LMS was proposed by Jorge, Santi and Josep [9]. This approach uses techniques which includes a digital signature, certificate, certification authorities, key stores and time stamping. However, this approach is not scalable, will just provide the traditional password verification if the private keys cannot be protected and can be very burdensome in large environments such as the LMS. An algorithm that]creates strong password and checks for the strength of password was proposed by Gabor et al. [10]. This algorithm will make it difficult for hackers to have access, however, once a password is compromised through spyware, denial of service attack will occur on the LMS platform for such users.

Considering these challenges, we develop a system capable of combining multi-factor authentication and identity management to secure LMS by ensuring data availability, data integrity, validation and verification, access control, confidentiality, acceptance, audit service and failure management. The rest of the paper is structured as follows. Section

*CORRESPONDING AUTHOR | O. J. Falana | ✉ falanafalanaoj@funaab.edu.ng

2 describes the related work. Section 3 presents the architecture for the proposed Se-LMS. Finally, section 4 covers the implementation and conclusion of Se-LMS

RELATED WORK

Structuring a smart school is to develop a domain of instructing, learning, and improving the system of education management [11]. There is a need for cooperation among student and educators, high plausibility of transmitting quality and verified the information and expanding the potential capacities of the students to learn at their rate consistently with the instructing process. The e-learning is a novel innovation in the instructive field in which transmitting and sharing data is finished by Personal Computers (PC) and PC nets. A smart school is a physical school whose administration and control depends on technology and computer webs, and the content of most courses is electronic [12]. To expand the significance of electronic teaching and learning, the educational framework ought to be alongside the progressions of present-day society, as well as improving the use of present-day advancements of data and technologies in educational systems, and subsequently setting up and improving smart schools.

Zhu et al. [13] proposed a framework for smart education. This framework portrays three essential elements in smart education: smart environments, smart pedagogy, and smart learner. The authors suggested some levels of smart education capabilities based on their research that students should master to address advanced societal issues. These capabilities are basic knowledge, core competencies, comprehensive skills, personalized expertise, and collective intelligence. proposed an application framework for a smart education system based on mobile and cloud systems. The smart education system and multi-feature information are special terms embedded in the original digital learning materials and can be recovered from various social media automatically by a survey of multi-aspect information originating from social media on the smart education environment including cell phones or electronic writing boards without relying upon information recovery ability [14]. The authors implemented the approach based on transforming model which empowers the movement of the first computerized learning material to the smart education environment. Also, it has a simple operation flow for trainees named "three-step selection flow". Smart Education System (SES) Framework derived from Model-View-Controller (MVC) design depends on the system architecture that enables triple mashup against the original digital learning material, screen gadgets and external social media before users. All these functionalities have been executed on cloud systems..

Gabor et al. [10] noticed some security issues in e-learning stages and proposed an algorithm that creates solid passwords to secure data while offering the likelihood to check the strength of the produced password. To make digital task progressively proficient, that is, to make things harder for hackers and cause them to consistently look for and grow new techniques to break passwords which will prompt an increasingly fast advancement of information and communication technology.

With the Internet of things growing rapidly, there is an increasing attack on IT infrastructure. Roldán et al. [15] introduced an intelligent architecture combining complex events processing and machine learning to detect IoT attacks. The authors used graphical-based authentication to authenticate users. The Behaviour-based learning approach is proposed by Li et al. [16] to mitigate threat occasioned by IoT device communication changes. Both Local and global attributes are modelled and processed by Neural network to identify errors and resources access.

Turnbull et al. [17] carried out an empirical study of the usage of LMS in Australia and China. The authors compared and contrast the research methodologies adopted in both countries. The study concluded that Chinese studied employed a more quantitative approach than Australian studies. An understanding of the differences can help shapen the future development of LMS. However, the review was focused on English language publication, including Chinese language publication will help to enhance the quality of the review.

Soykan and Şimşek [18] examined studies published on LMS from 2010 to 2014. The authors obtained 76 articles from three journals indexed in Social Sciences Citation Index (SSCI) to determine the trend in LMS. The results revealed that the number of developed LMS are increasing and researchers are looking for new and secured LMS.

In a similar work by Dobre [19], a study of different types of LMS options available for Higher Institution was carried out. Among the various options are Proprietary LMS, cloud-based LMS, Open Source LMS and Hybrid LMS. The author concluded that three factors that will influence the choice of LMS are the students' population, budget and the variety of expertise.

Amin et al. [20] proposed a password-based secure communication between fog device and cloud resources. The authors developed a protocol which comprises office stages such as system set up, registration on the cloud, system authentication, handshaking between fog device and user and transmission of a message between fog device and cloud.

RESEARCH METHODOLOGY

The design of a secured Learning Management System for Smart School is presented in Figure 1. The general idea behind proposed research is to analyse users' authentication process to enhance the security of the system.. The design has three major components Users' Authentication, Identity Management and Learning Resources.

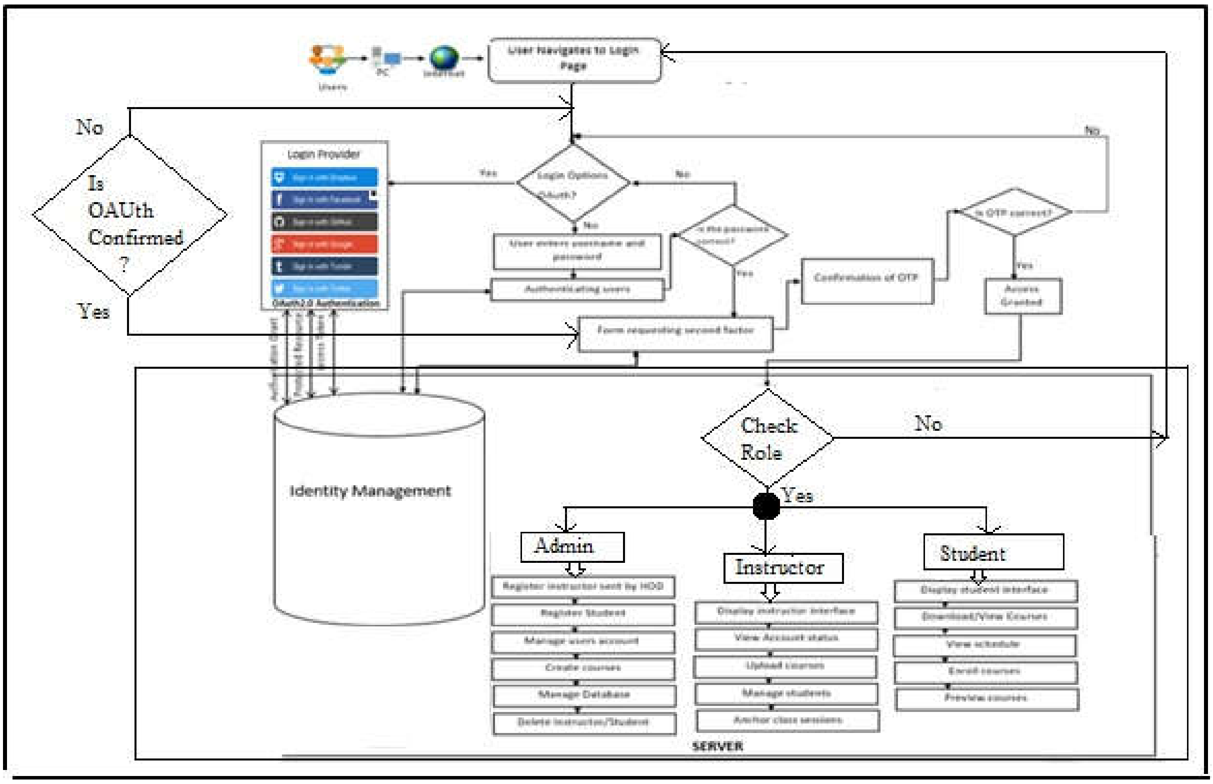


Figure 1. Flowchart of Se-LMS for smart school

User's Authentication

Dynamic authentication approach is employed to authenticate users into the LMS platform. This helps to create a per-session authenticator i.e. it changes with each authentication session between the applicant and the verifier. In general, the proposed dynamic authenticator seamlessly combined three authentication techniques: OAuth2.0 Authentication, Username and Password and 2-Factor Authentication for user authentication. The system uses two authentication techniques at a time, such as the combination of OAuth2.0 and 2FA or Username and Password together with 2FA authentication.

In the case of compromise in the credentials of the actors (e.g. email address of one of the actors is hacked) using OAuth2.0 login providers or username and password will not prevent the intruder. The 2FA authentication will provide a further security check and mitigate such attack by enforcing GoogleAuthenticator rather than the emailing of code. This is achieved by cross-checking the familiarity of users location, IP address and devices used. Most common LMS employed one of these techniques which made it possible for hackers to quickly bypass the authentication phase.

i. OAuth2.0 Authentication

OAuth is an open standard for access delegation. It provides to a client a secure delegated access (i.e. the process of granting someone permission to your files and respond to requests for you) to server resources on behalf of a resource owner [21]. It requires a client and server. End-users can gain access to the e-learning system via social login only if they registered using OAuth2.0 technique such as Facebook, Google+, Twitter and so on.

ii. Username and Password

The user enters a password that is at least seven characters long and has at least one or more numeric and uppercase characters mixed with it and so on, to gain access to the Learning Management System after they have been registered to the system.

iii. 2-Factor Authentication (2FA)

2FA is an extra layer of security for a user's account in e-learning management. It requires users to provide a second piece of identifying information in addition to a password. The user has two options to select from, which is either Email or Google Authenticator. However, Google Authenticator is enforced in this system when a user tries accessing the learning resources from unfamiliar locations. The 2FA is based on Time-based One-Time Password Algorithm (TOTP) alongside HMAC-based One Time Password (HOTP) as shown in pseudocode 1

Pseudocode 1

1. The first step is to create an HMAC hash from a secret key and counter
   hmacHash = HMAC-SHA-1(secretKey, counter);
2. Obtain the offset which is the last 4 bits of hmacHash [index_19]
3. Concatenate the bytes from hmacHash[offset] to hmacHash[offset+3] and store the last 31 bits to truncatedHash
4. Finally, using a simple modulo operation to obtain the one-time password that is a reasonable length.

Algorithm 1: Multi-level Authentication

```
Algorithm  Multi_level Authentication

Input      :      User_name, Password
Output     :      start_Activity
Access_code ← requestPermission(User_name, password)
Key_phrase  ←  DeriveBytes(Access_code, 10000);
byte[]hash  ←   key_phrase.GetBytes(20);
SavedPasswordHash  ←   Convert.ToBase64String(hashBytes);
RC <- requestCode
// compare with stored password in database
If login_option === stored_password:
    byte[] c, byte[] d;
    diff = c.length ˆ d.length
    for(int i=0; i<c.length && d.length; i+++)
           diff  ←   c[i] ˆ d[i]
           return diff == 0;
if login_option ===0auth:
{

Get configurationservice(serviceCollection, services)
ChallengeScheme =  “”
clientId = configuration( getCliendId)
clientSecret = configuration(getClentsecret)
callBack Path = createpathString(sign)
AuthorizationEndpoint = get(tokenEndpoint, userInformation)
 While AuthorizationEndpoint True;
    Claim_action.Map(claimTypes.NameIdentifier,  “Id” )
    Claim_action.Map(claimTypes.Name,  “Name” )
    Claim_action.Map(claimType.login,  “login” )
    Claim_action.Map(claimTypes.url,  “http…” )
    Request = new RequestMessage(Claim_action.Map(userInformation,access_token
}
While login_option == True:
    // Generate OTP using Google Authenticator
    byte[] Key, OTP_SHA1()
    Using(RandomNumberGenerator rng <- new RNGCryptoServiceProvider())
    Key <-  new byte[HMACSHA1.Create().HashSize[8];
    Rng.GetBytes(Key);
    time <- 30
    for T  in  CounterNow(time):
           seconds = DateTime.UtcNow - new DateTime (DateTimeKind.UTC)
           Return Second. TotalSeconds/time;
Return start_activity
```

Identity and Access Management (IDAM)

IDAM part is in charge of dealing with users' identity and other objects. Specifically, it aims to supplement the usefulness that is given through the Authentication segment. IDAM depends on two conventions to be specific credential issuance and demonstrating as represented underneath:

i. the subject demands a credential from the IDAM Service, which goes about as an Issuer.
ii. IDAM administration plays out certain checks to approve the properties for which the subject apply for the certification.
iii. to get a credential, the subject needs an accreditation structure which is given by the IDAM administration to approval reason
iv. finally, the issuer replies to the subject by sending a cryptographic message with the confirmation of the accuracy and the traits signature. The subject confirms this cryptographic material and dependent on this message, it creates and stores the qualification.

Learning Content Repository

Se-LMS repositories incorporate search and recover features, metadata authoring and altering features, licensed innovation controls, and regular content creating instruments. Through a Web administrations interface, teachers and understudies can look, recover, and alter the content in the Se-LMS. It follows a system convention known as hypertext move convention (HTTP).

From the technical point Se-LMS materials are organized as follows:

- Course bundle - a set of files (with the substance, designs, and so forth.) that can be run from Se-LMS framework. They are mostly word processing report designs, which ensure transferability between stages.
- Activity – a structure which permits the gathering of shareable articles, resources and some other exercises for example Test, Assessment,
- Sharable Content Object – a part intended to organize content that will be handled (run, given to understudy) in LMS and which may interact with the system to send data about student progress. Sharable Content Object is used to record course parts which flexibly or confirm content.
- Asset, resources, file

Entity-Relationship model for Se-LMS

The LMS relationship model describes how documents in the database are linked to one another. At the easiest stage, it produces a 1: N (one-to-many) connection between the two entities by adding a lookup field to any entity. Users can match multiple of that entity’s child documents to a single parent entity record with the lookup field entities by adding a lookup field. Figure 2, 3 and 4 show the relationship model for users’ registration, Activity and Identity management for this research work

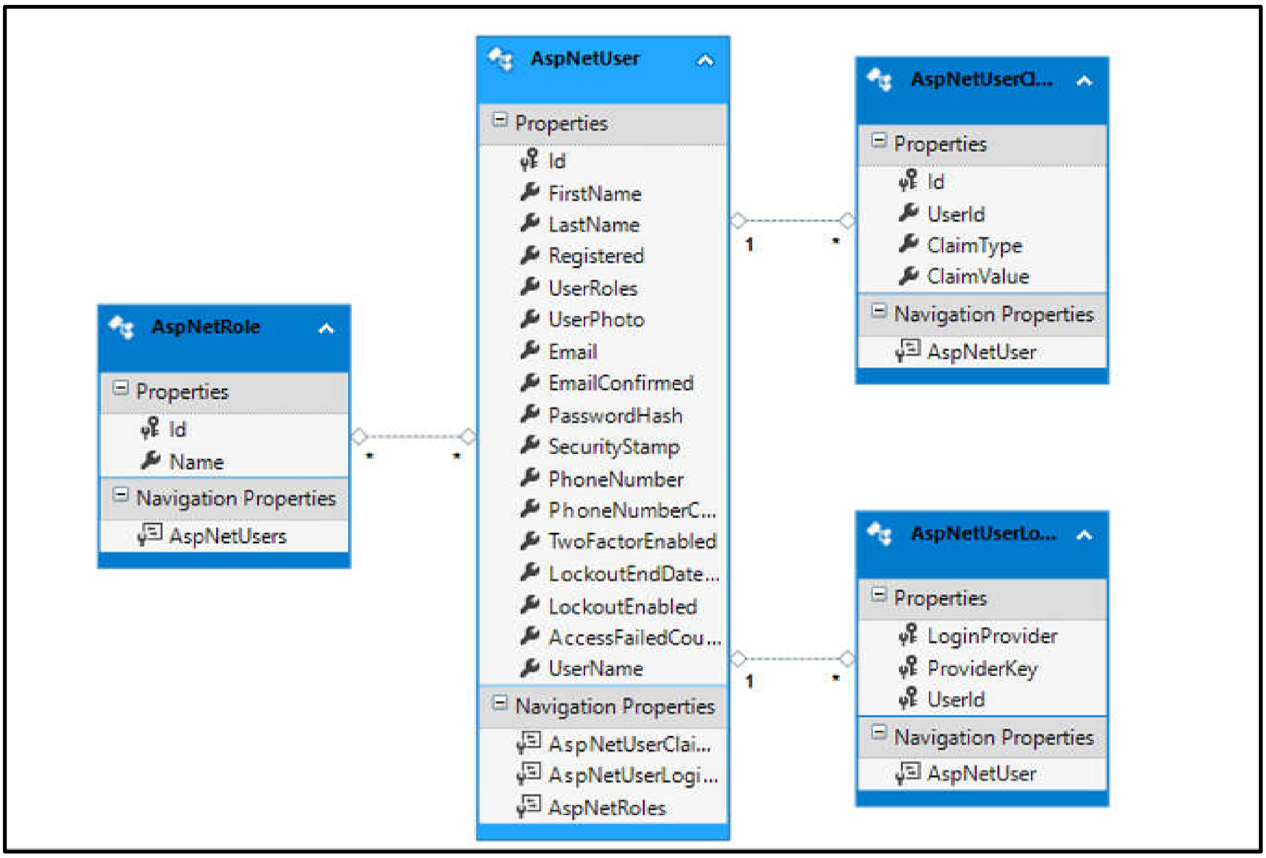


Figure 2. Relational Model for user registration versus roles entity

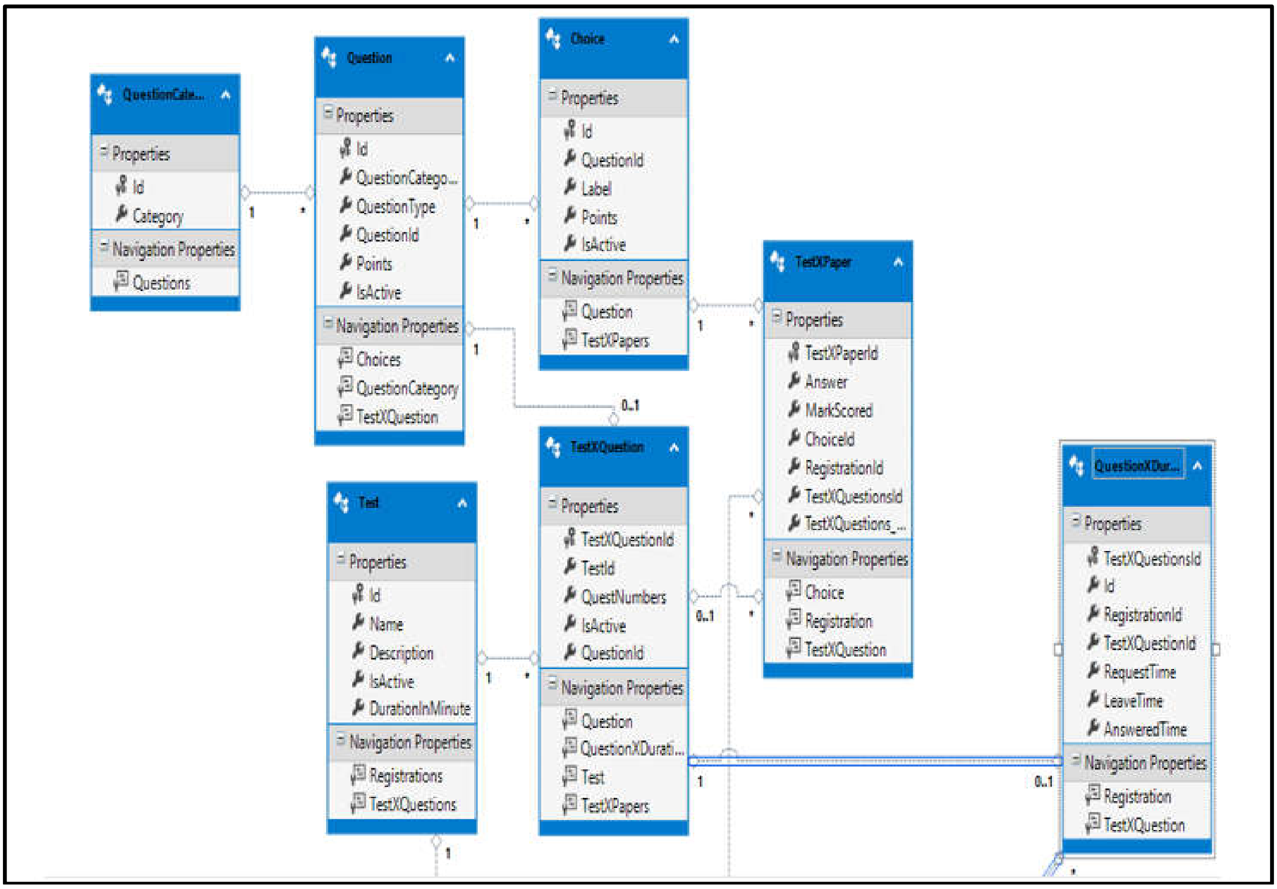


Figure 3. Relational Model for activity

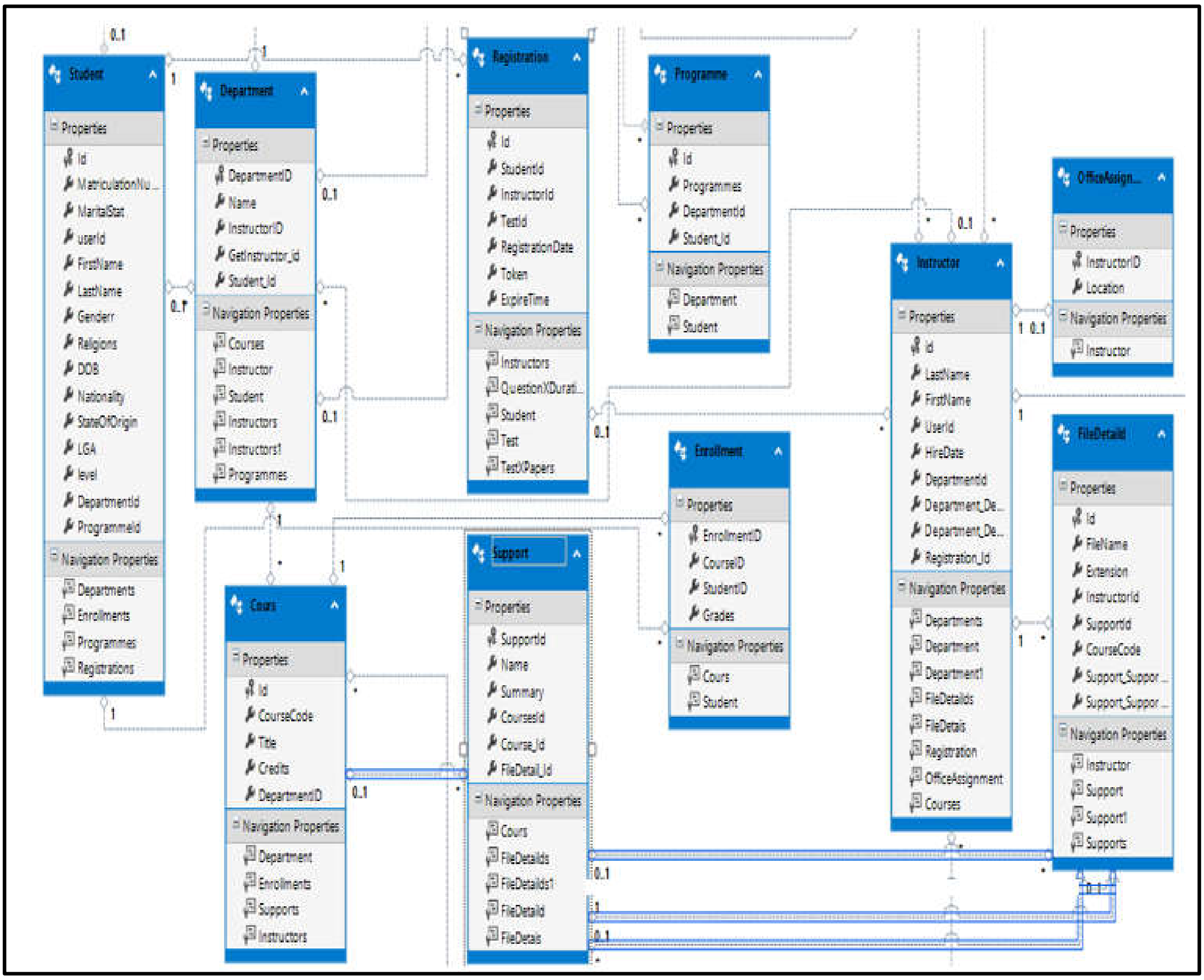


Figure 4. Relational Model for identity management

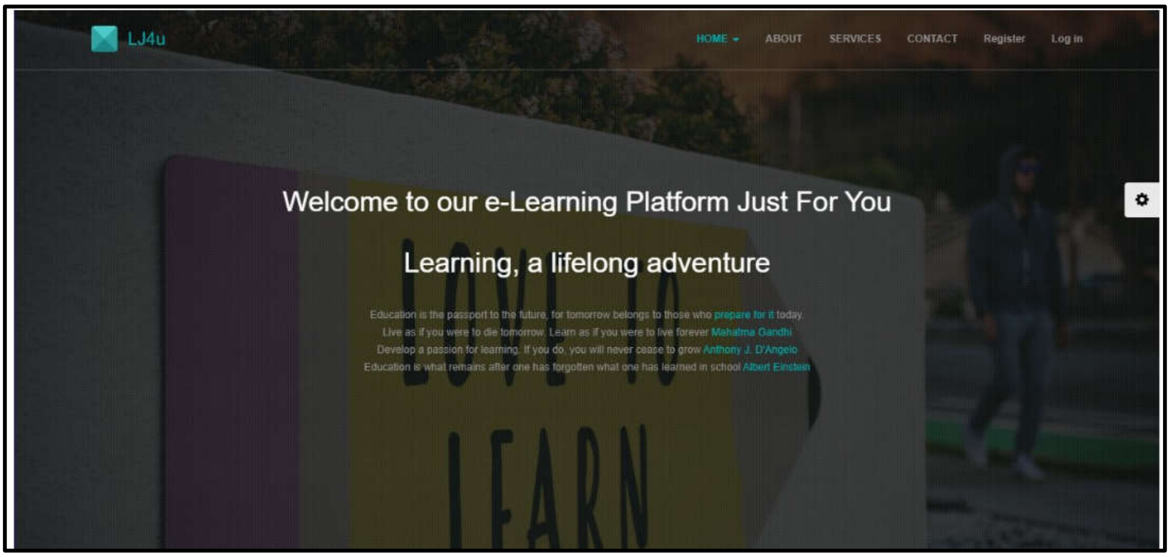
EXPERIMENTAL RESULTS

To show the implementation of Se-LMS, we used Asp.net Model View Controller (MVC) to develop the learning system for cloud computing. MVC is a design pattern used to decouple data (model), user-interface (view), and application logic (controller). This pattern helps in achieving separation of concerns. The data classes are stored in one of the patterns, which is the model. The logic part deals with the logic part of the system and the user-interface where technologies like HTML, JavaScript, and other front-end technologies, would be in the view. Using the website MVC pattern, requests are routed to a controller responsible for working with the model to perform actions and/or collect data. The controller selects the view to display and the model to display. The View renders the final page, based on the data in the Model.

Screenshot of the Implementation Stages

The screenshots of the implementation stages show the different views of the users depending on their roles with a brief description of what it entails in Figure 5.

Home Screen



Welcome to our e-Learning Platform Just For You

Learning, a lifelong adventure

Education is the passport to the future, for tomorrow belongs to those who prepare for it today.
Live as if you were to die tomorrow. Learn as if you were to live forever Mahatma Gandhi
Develop a passion for learning. If you do, you will never cease to grow Anthony J. D'Angelo
Education is what remains after one has forgotten what one has learned in school Albert Einstein

Figure 5. Welcome page

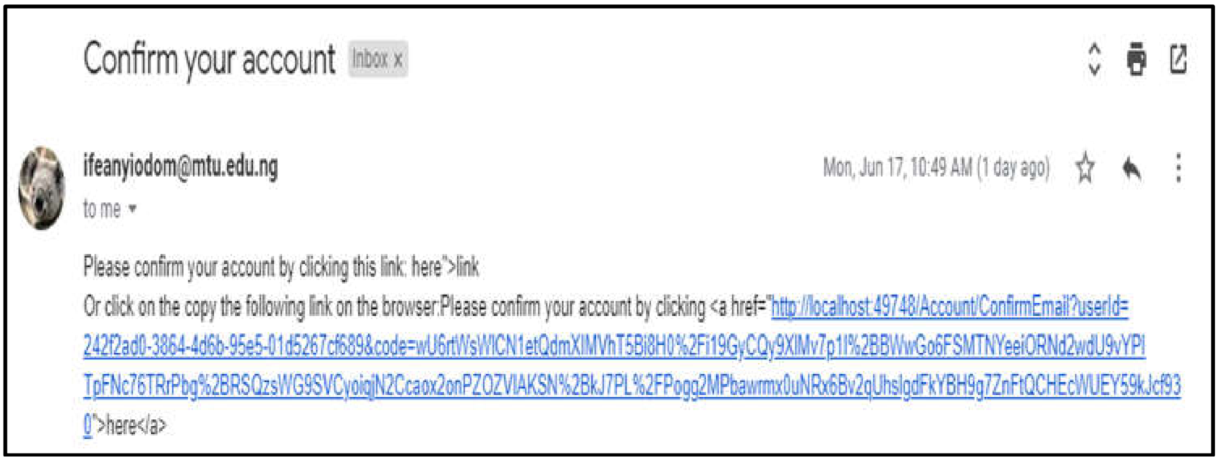
This is the first page that appears when the URL of the Learning Management System is typed in any browser. While on this page subject can choose to register and continue to access files, resources and access the contact us page.

Authentication of Users

To access the learning modules users log in with their existing learning account or create a new one. The user must first register or be registered by the administrator. To access the registration page, the user navigates to the registration link on the upper right-hand side and fill in all the mandatory fields, before clicking the registration button for a successful registration

a. **Confirmation of Account**

Email verification is a method to verify that the user has an email account. A message is sent to the user's email to verify his/her account. This particular message contains a unique link. This link will help in the email verification of the user as shown in Figure 6. Once the user clicks on the link, the particular comment automatically is approved. This entire process is called email verification, and this helps in the improvement of security of an email account.



Confirm your account Inbox x

ifeanyiodom@mtu.edu.ng
to me

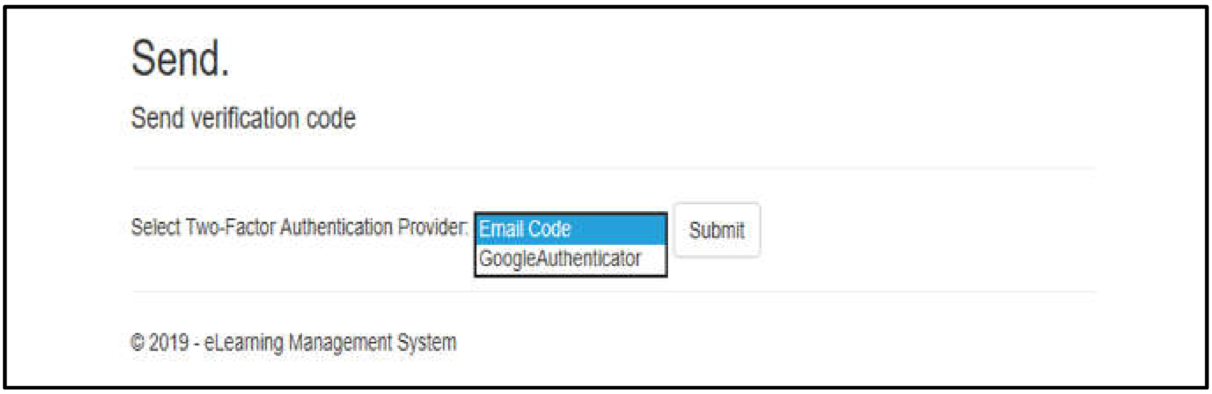
Mon, Jun 17, 10:49 AM (1 day ago)

Please confirm your account by clicking this link: here">link
Or click on the copy the following link on the browser:Please confirm your account by clicking <a href="http://localhost:49748/Account/ConfirmEmail?userId=242f2ad0-3864-4d6b-95e5-01d5267cf689&code=wU6rtWsWICN1etQdmXIMVhT5Bi8H0%2Fi19GyCQy9XIMv7p1l%2BBWwGo6FSMTNYeeiORNd2wdU9vYPlTpFNc76TRrPbg%2BRSQzsWG9SVCyoiqjN2Ccaox2onPZOZVIAKSN%2BkJ7PL%2FPogg2MPbawmx0uNRx6Bv2qUhslgdFkYBH9g7ZnFtQCHEcWUEY59kJcf930">here</a>

Figure 6. Email verification

b. **2FA Selection**

The user’s account is automatically set for the 2FA mode. The user has two options to select from to authenticate their account using the selected 2FA. You can select Email or Google Authenticator as in Figure 7.



Send.

Send verification code

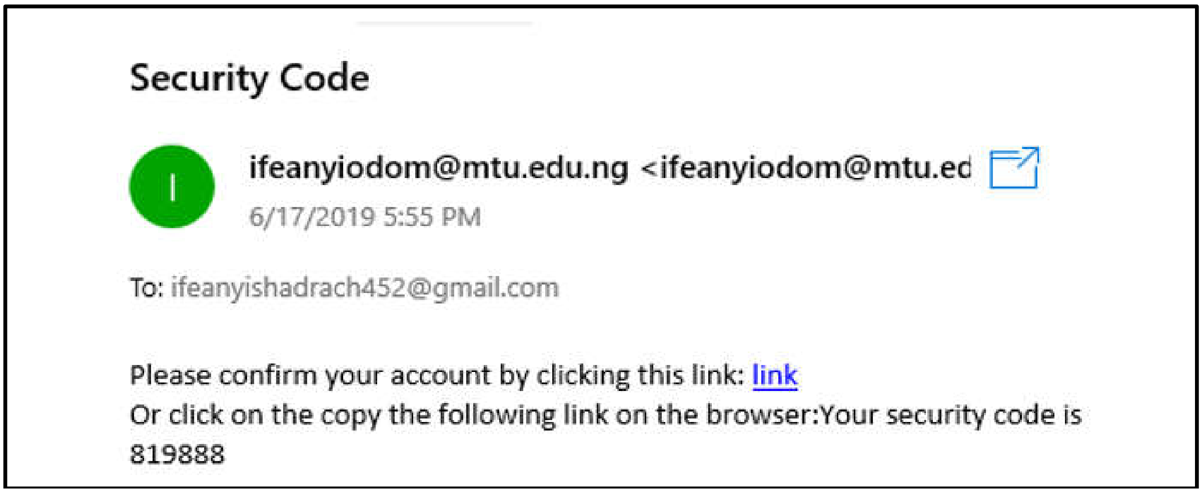
Select Two-Factor Authentication Provider: Email Code / GoogleAuthenticator

© 2019 - eLearning Management System

Figure 7. 2FA Selection

2FA Email Code

Selecting the Email code, a 6-digit code is sent to the users' registered email account. The user then enters this 6-digit code into his/her account and is then granted full access as shown in Figure 8.



Security Code

ifeanyiodom@mtu.edu.ng <ifeanyiodom@mtu.ed

6/17/2019 5:55 PM

To: ifeanyishadrach452@gmail.com

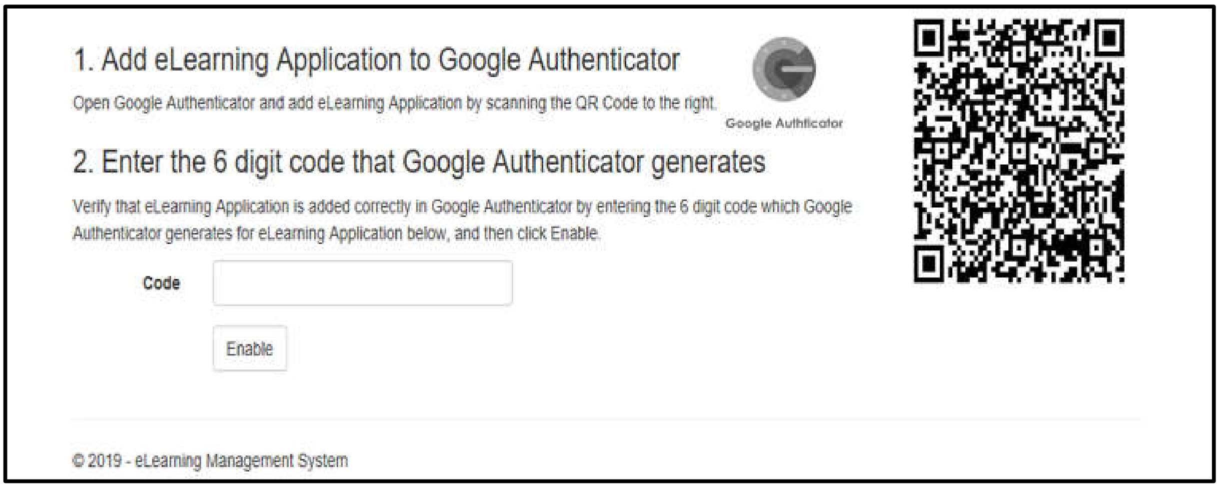
Please confirm your account by clicking this link: link

Or click on the copy the following link on the browser:Your security code is 819888

Figure 8. 2FA Email code

b. 2FA Google Authenticator

Google Authenticator helps us to implement Two-Factor Authentication by adding a layer of security to the e-learning system with something the user knows and something the user has. Google authenticator is software-based implementing two-step verification services by using the Time-based One-Time Password Algorithm (TOTP) alongside the HMAC-based One-Time Password algorithm. Users ought to enter the six-digit to eight-digit generated in addition to their normal login details as shown in Figure 9.



1. Add eLearning Application to Google Authenticator

Open Google Authenticator and add eLearning Application by scanning the QR Code to the right.

2. Enter the 6 digit code that Google Authenticator generates

Verify that eLearning Application is added correctly in Google Authenticator by entering the 6 digit code which Google Authenticator generates for eLearning Application below, and then click Enable.

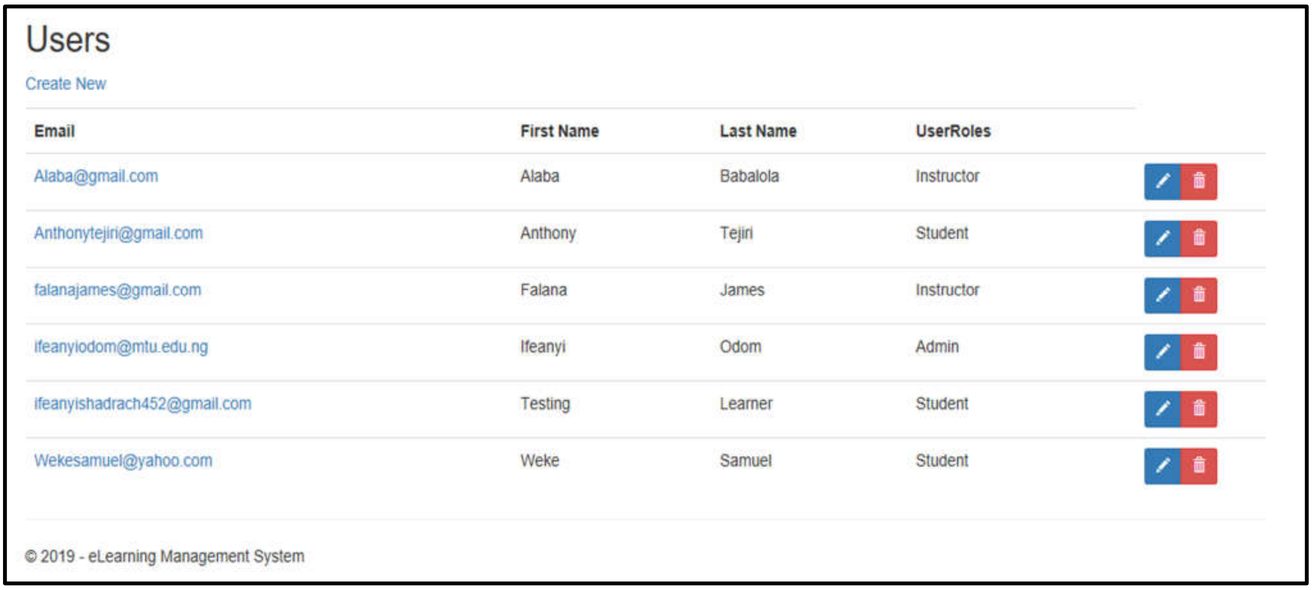
Code

© 2019 - eLearning Management System

Figure 9. 2FA Google authenticator.

c. Admin Manage Users

In this interface, as shown in Figure 10, the admin is tasked with the management of all users in the system. The Administrator can edit users profile as well as delete users from the system.



Users

Create New

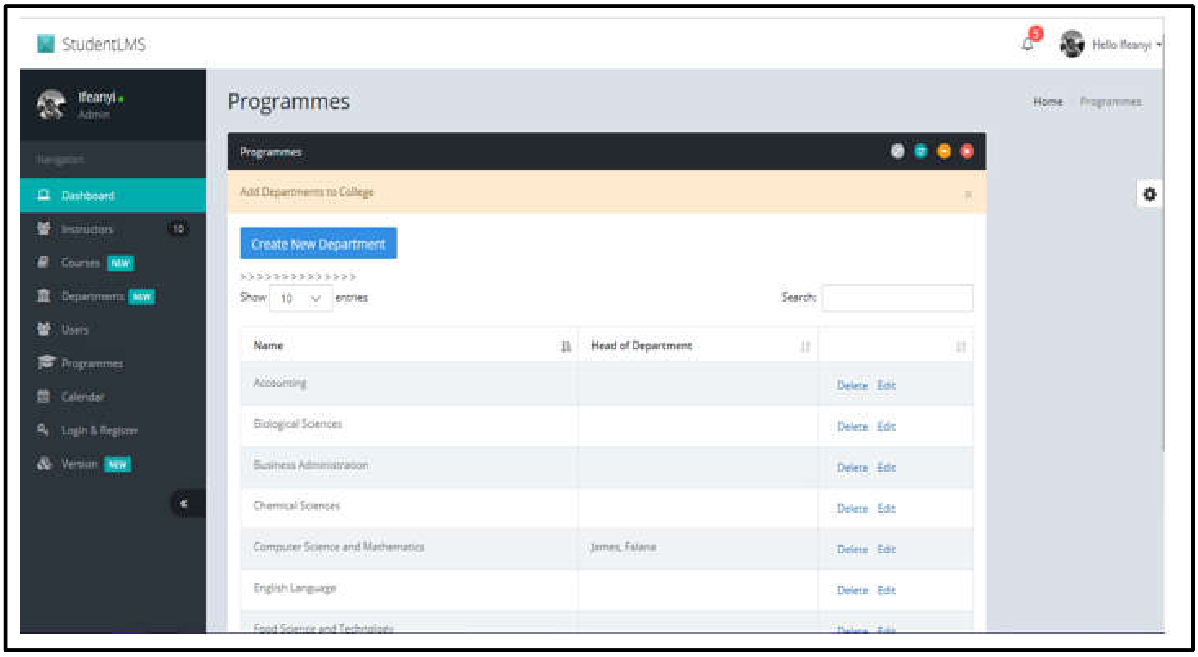
Email	First Name	Last Name	UserRoles	
Alaba@gmail.com	Alaba	Babalola	Instructor	✎ 🗑
Anthonytejiri@gmail.com	Anthony	Tejiri	Student	✎ 🗑
falanajames@gmail.com	Falana	James	Instructor	✎ 🗑
ifeanyiodom@mtu.edu.ng	Ifeanyi	Odom	Admin	✎ 🗑
ifeanyishadrach452@gmail.com	Testing	Learner	Student	✎ 🗑
Wekesamuel@yahoo.com	Weke	Samuel	Student	✎ 🗑

© 2019 - eLearning Management System

Figure 10. User management

Add Departments

The administrator is in charge of adding new departments to the e-learning system, as well as assigning the Head of Department to the Department and managing other related activities as in Figure 11.



Programmes

Programmes

Add Departments to College

Create New Department

Show 10 entries

Search:

Name	Head of Department	
Accounting		Delete Edit
Biological Sciences		Delete Edit
Business Administration		Delete Edit
Chemical Sciences		Delete Edit
Computer Science and Mathematics	James, Falana	Delete Edit
English Language		Delete Edit
Food Science and Technology		Delete Edit

Figure 11. Adding departments

CONCLUSION

Having discovered that e-learning and Learning Management Systems have become an essential part of our everyday life, more users are embracing these systems, and more targeted attacks are also launched, most especially via social login. Our model can be used to mitigate these attacks on Learning Management Systems via the multi-factor authentication and identity management approach. Our model can deal with situations where social login, username and password or email access have been compromised, or in a ubiquitous environment. The system protects actors information and learning resources. Also, this approach ensures data availability, data integrity, validation and verification, access control, confidentiality, acceptance, audit service and failure management. The future work we are looking into is multifactor authentication using facial recognition and ID card capturing for user authentication into the LMS resources.

REFERENCES

[1] P. Zaman, and B. Mirza, "A Survey on Effective Elements on Educational Function of Electronic Learners in Higher Education: Presenting Successful Model Based on Users Idea," *Scientific-Research Magazine of Educational Courses, 16,* 130-164, 2010.

[2] S. M. J. Jalali, E. Mahdizadeh, M. R. Mahmoudi, and S. Moro, "Analytical assessment process of e-learning domain research between 1980 and 201," *Analytical assessment process of e-learning domain research between 1980 and 2014*(1), pp. 43-56, 2018.

[3] P. Nicholson, "A history of e-learning,"*Computers and education* (pp. 1-11): Springer, 2007.

[4] D. Niki, and L. Avril, "Reviewing the landscape of ICT and teacher education over 20 years and looking forward to the future," *Technology, Pedagogy and Education*, Volume 20, Issue 3, p: 247-261: Special, 2011, doi: 10.1080/1475939X.2011.610928

[5] E. de Freitas, D. Rousell, and N. Jäger, "Relational architectures and wearable space: Smart schools and the politics of ubiquitous sensation," *Research in Education*, pp. 0034523719883667, 2019.

[6] A. Montazami, M. Gaterell, and F. Nicol, "A comprehensive review of environmental design in UK schools: History, conflicts and solutions," *Renewable and Sustainable Energy Reviews, 46*, pp. 249-264, 2015.

[7] M. S. Ibrahim, A. Z. A. Razak, and H. B. Kenayathulla, "Smart principals and smart schools," *Procedia-social and behavioral sciences, 103*, pp. 826-836, 2018.

[8] Security, R., "Common Cybersecurity Threats in Education", 2019, Retrieved 27th June, 2020, from blog.rsisecurity.com/common-cyber-security-threats-in-education/

[9] M. M. Jorge, C. Santi, and P. Josep, "Security in Learning Management Systems: Designing collaborative learning activities in secure information systems," eLearning Papers, ISSN: 1887-1542 www.elearningpapers.eu, paper 28, pp. 1-3, April 2012.

[10] A. M. Gabor, M. C. Popescu, and A. Naaji, "Security Issues Related To E-Learning Education," *International Journal of Computer Science and Network Security (IJCSNS), 17*(1), pp. 60, 2017.

[11] X. Cheng, and R. Xue, *"Construction of smart campus system based on cloud computing."* Paper presented at the 2016 6th International Conference on Applied Science, Engineering and Technology, 2016.

[12] M. Attaran, S. Attaran, and B. G. Celik, "Promises and challenges of cloud computing in higher education: a practical guide for implementation," *Journal of Higher Education Theory and Practice, 17*(6), 2017.

[13] Z. -T. Zhu, M. -H. Yu, and P. Riezebos, "A research framework of smart education," *Smart learning environments, 3*(1), pp. 4, 2016.

[14] W. W. Ali, H. M. Nor, A. Hamzah, and N. Alwi, "The conditions and level of ICT integration in Malaysian Smart Schools," *International Journal of Education and Development using ICT, 5*(2), pp. 21-31, 2009.

[15] J. Roldán, J. Boubeta-Puig, J. L. Martínez, and G. Ortiz, "Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks," *Expert Systems with Applications, 149*, pp. 113251, 2020.

[16] D. Li, L. Deng, W. Liu, and Q. Su, "Improving communication precision of IoT through behavior-based learning in smart city environment," *Future Generation Computer Systems*, 2020.

[17] D. Turnbull, R. Chugh, and J. Luck, "Learning management systems: a review of the research methodology literature in Australia and China," *International Journal of Research & Method in Education*, pp. 1-15, 2020.

[18] F. Soykan, and B. Şimşek, "Examining studies on learning management systems in SSCI database: A content analysis study," *Procedia computer science, 120*, pp. 871-876, 2017.

[19] I. Dobre, "Learning Management Systems for higher education-an overview of available options for Higher Education Organizations," *Procedia-social and behavioral sciences, 180*, pp. 313-320, 2015.

[20] R. Amin, S. Kunal, A. Saha, D. Das, and A. Alamri, "CFSec: Password based secure communication protocol in cloud-fog environment," *Journal of Parallel and Distributed Computing, 140*, pp. 52-62, 2020.

[21] B. Gao, F. Liu, S. Du, and F. Meng, "*An OAuth2. 0-Based Unified Authentication System for Secure Services in the Smart Campus Environment,"* Paper presented at the International Conference on Computational Science. pp. 752-764, 2018.