Babylonian Journal of Internet of Things
Vol. 2025, **pp**. 153–175
DOI: https://doi.org/10.58496/BJIoT/2025/010; ISSN: 3006-1083
https://mesopotamian.press/journals/index.php/BJIoT

Research Article

Enhancing Digital Infrastructure Security in Education: Securing Access and the Moodle Platform

Husham Abd AL-Kareem[1,2,*], Hadeel M Saleh[3]

[1] *University of Tenaga Nasional (UNITEN), Malaysia*
[2] *Islamic University of Lebanon, Lebanon*
[3] *Center for Continuing Education, University of Anbar, Iraq*

ARTICLE INFO

Article History
Received 3 May 2025
Revised 20 Jun. 2025
Accepted 13 Sep. 2025
Published 11 Oct. 2025

Keywords:
Learning Management System,
Moodle Cyber security,
Two-Factor Authentication,
Cloud Computing,
Microsoft Azure,
Data Encryption.

ABSTRACT

This study is to analyse the implementation of a Learning Management System (LMS), and its improvement the (LMS) at the Islamic University of Lebanon, with a particular focus on improving the security of the (LMS) as regards of keeping sensitive data and maintaining a secured reliable e-learning environment. The paper discusses best practices, and what both the technical and organizational security measures that must be adhered to in order to secure either of these platforms, should be.Technically, the research provides cloud hosting services for hosting Moodle platform, such as Microsoft Azure, which provides advanced features in security, including safeguarding against cyber threats, advanced data encryption and so on. Additionally, It showed that encrypting data-in-transit, as it moves from the source to the destination, with secure protocols helps to mitigate the risk of data breaches or interception by unauthorized third parties.The two-factor authentication is provided as the primary user account protection mechanism, according to the research recommendation from a user perspective. The guide also suggests making passwords that are a combination of upper and lower case letters and symbols, as well as not including any personal information within the password. As well as that, he also promotes application (mobile phones or email) authentication to improve the level of security of the login solution. In this study, we want to present a systematic and practical guide to enhance the security of e-learning platform in academic settings, integrating cloud-based technologies with right security mechanisms at the level of devices and the level of users.

1. INTRODUCTION

The educational sector has been significantly relying on digital technologies and e-learning management systems such as Moodle have become indispensable infrastructure to academic institutions. The changes that the world is witnessing at the current time have inevitably created a new reality, especially due to the health crises, including the COVID-19 pandemic, which the world is currently witnessing, which prompted a number of universities to adopt distance learning as an alternative to the regular teaching method to activate the process. This transition has uncovered new security challenges that directly impacts information confidentiality, system integrity, and user trust [1]. Moodle (and other online learning platforms in general) are highly attractive with their flexibility and accessibility anywhere, anytime but also an easy target for cyber attackers. Research has demonstrated that e-learning environments are prone to various types of attacks including, but not limited to, brute force attacks, credential stuffing, phishing, and user privilege manipulation. This also points out the need to strengthen the security perimeter of these platforms with advanced solutions and technologies [2]. Another common practice to secure the devices from unauthorized access is to implement the multi-factor authentication (OTP, TOTP, Biometric Authentication etc.). At the network and server level, advanced security technologies like File Integrity Monitoring, Cloudflare services, and cloud computing platforms like Microsoft Azure, are all designed to ensure that service will continue to be available even during a distributed attack [3].With that being said, monitoring should not be the only measure to be depended upon, but rather help provide a comprehensive set of organizational policies about access rights, limiting the access point from malicious devices or websites, and ensuring their system is constantly scanned for its vulnerability. Based on this, training those who use personal protections is also vital in ensuring the system as a whole stay secure [4].The present study provides information about security of Moodle platform at Islamic university of Lebanon (IUL). It aims to create an all-in-one security system that truly fills the existing gaps. These consist of high-assurance authentications, restrictive access

*Corresponding author. Email: Hishamabd1818@gmail.com

polices, risk assessment, and network protection that assist the digital learning environment to be more sustainable, and keep the privacy and the data of the learners safe [5].

2. LITERATURE REVIEW

A literature survey is done previously on various methodologies, which aims to protect the Network and communications in various business scenarios. As a protocol to enable secure communications between applications over the Internet, Dierks /Rescorla (2015) implemented the Transport Layer Security (TLS). Ciphertext They also use many TLS (Transport Layer Security) protocol with some programs, such as when its appropriate usage in privacy and email, protective for cross application messaging and Voice over Internet Protocol (VoIP), wherein the best level of protection use incorporated authentication, security, and encryption. It consists of TLS Log and Handshake protocol It is based on the SSL protocol itself, and it's most recent version is 1.3 [6]. Virtual private network (VPN): solution No. 12VPNs are essential if you are a remote user.VPN, on the other hand, interlinks remote sites belonging to one entity, ensuring security in data sharing between organizations and remote sites through establishment of a virtual private network. In addition, network firewalls have also been investigated as a critical line of defense in the protection of networks from unauthorized access and with different types of firewalls such as physical and software firewalls. In a Cisco ASA device comparison, we found the performance of the device to be so high that it not only performed excellently against various forms of attack, but also outperformed the competition in all performance categories. [7]In contrast, there has been more research on the role of network application firewalls (WAFs) in safeguarding web-based applications against rising attacks [5–7]. WAF applications are vital part of securing online applications and its importance was depicted in 2013 by Razzaq presenting a performance-based analysis of WAF [1]. It is also suggested that the systems of monitoring the integrity of sensitive files can also be used and they can be executed in real time that can record all the operations being done on these sensitive files making use of the particular security analysis tools like the Wire shark to assess the real time network information from the connected networks and provide the flexibility of making easily the detection of the unauthorized activities in the particular delicate areas of the networks. [8] Proposed Solution: In order to resolve the network's security issues, the VLAN technology in conjunction with TACACS+AAA servers would be used. Such technology would help decrease the risks arising from various vulnerabilities and network attacks that might happen due to the misalignment of the network. According to Arfin and MD, FortiGate firewall was used, as "it has all the features to secure any small or big internal business network — from protecting against the external attackers to securing the network files and mail servers". The device may work by IPsec tunnel and VPN to connects between the worksites and in addition, the device requires a two-factor security advantages authentication. Belinda: Cloud flare as a solution: Cloud flare proposed to help Save the Org to protect organizations from attacks that may happen online. The technology uses a content distribution network to address the security issues. It also has servers in different countries and is versatile to help users prevent attacks. The technology is free and does not necessarily require an advanced subscription, as it all also features SSL, which helps increase the speed of the network. Marnie: Microsoft Teams as a solution: The solution is used as a focal online learning platform with various features that may help teachers to increase interaction and supervision of the online platform. It provided the protection of integration of security across the field of all the security field in an Org. Moreover, the two users have a two factor authored as an option to use. Zhang and Dongsong compared the e-learning with traditional learning by explaining the new IT course for Modern Biology. They made a conclusion that e-learning is an effective alternative in the situation when the registration to educational institutions is unavailable due to the pandemia of such disease as the coronavirus. Costa, Carolina, Helena Alvilos, and Leonor Teixe discussed the Moodle platform and the central tools to be provided, such as: "assignments, chats, forums, quizzes and other tools that exist such as calendars and glossaries for reminding and deepening access to information.". Platforms such as Google Meet, Zoom, Microsoft Teams, and Google Classroom and their role in education in institutions were discussed GI Singh, Ravinder Singh and Soumya Awasat added that the focus of security is primarily vital in the post pandemic situation when we watched an increase in attacks on educational applications during COVID-19 pandemic. As a catering video conferencing application, Zoom has a wide range of security issues, which was later solved step by step with the updates and patches. This application has a different interface that supports 100 participants and 49 screen videos plus screen sharing and group chats. [12] Google Classroom is an open education platform that offers educational applications to anyone with a Gmail account. It is the perfect space for structure and time-management, as teachers can track the progress of learning and sort activities in several educational modalities. Moodle is another open-source e-learning platform that offers you effective security and course management tools. Security issues in platform sessions were also tackled by researchers [13], who suggested to consider the generic Secure Socket Layer (SSL) protocol to handle security issues associated to data transmission and movement. Luminita and Defta Costinela introduced essential security aspects required for e-learning platforms (authentication, access control, confidentiality, integrity, availability, and non-repudiation) and gave a solution that can help avoid illegal access to accounts [22]. Table 1 clarify a summary of previous study. [13]

TABLE I: SUMMARY OF PREVIOUS STUDY

Topic	Technology/Tool	Purpose of Study	Reference Number
Online Security	TLS Protocol	Provide security for internet communications between applications such as email and IP-based messaging	[6]
Network Firewalls	Cisco ASA Firewall	Protect networks from unauthorized access and analyze performance metrics like throughput and latency	[7]
Web Application Security	Web Application Firewall (WAF)	Evaluate WAF performance in securing web applications	[8]
Fort iGATE Firewall	Fort iGATE	Protect internal networks from external threats using (IPsec) tunnels, (VPN), and two-factor authentication	[9]
Enterprise Protection via CDN	Content Delivery Network (CDN)	Protect enterprises from online attacks and speed up network performance	[10]
E-learning	Moodle	Compare e-learning with traditional learning and facilitate student collaboration in educational environments	[11]
Online Learning Platforms	Google Meet, Zoom, Microsoft Teams, Google Classroom	Enhance security on online learning platforms and ensure data protection during the COVID-19 pandemic	[12]
Moodle Platform Security **E-learning Platform Security**	Moodle Two-factor authentication, Access Control	Improve platform security by using SSL protocol to protect data and traffic Ensure account protection from unauthorized access through multiple security measures	[13]

3. SECURITY MEASURES FOR LMS PLATFORMS: SUMMARY

3.1 Protecting Against Threats and Vulnerabilities

- User authentication: It is essential to have strong user authentication using two-factor authentication (2FA), biometric verification, Single Sign-On (SSO). Require unique passwords (at least) the stars in the sky, and tell users how to create strong ones.
- Access Control: Implement Role-Based Access Control (RBAC) to remove the principle of least privilege – users could be access only needed resources. Perform regular policy access audits
- User: Ensure secure communication by encrypting your messages using TLS encryption protocols which guarantee your connections and protect valuable information being sent back and forth.
- Data security and Data- at –rest/ Data-at-transit Encryption. Use a secure storage way, backup your data from time to time and make sure that everything complies with such regulations as for example GDPR.
- Perform Regular Security Audits Security tests, penetration testing and vulnerability scanning to spot and fix security flaws
- Training on Security Awareness: Offer user Training W.R.T security practices, Phishing prevention and Secure data handling to the users.

3.2 Integrating Security Measures into the LMS Platform

- Centralized Security Policy: Create a united security policy consisting of an authentication, access control and data protection.
- Biometric Authentication and SSO Boost security with biometric authentication and add SSO for a simpler yet secure user access.
- Email and Mobile Device Security — Set up secure email communications and ensure that mobile device encryption is mandatory for accessing the LMS.
- Constant Security Assessments: Vogel, cyber startup company provides regular vulnerability scanning penetration testing to find out the weaknesses.

- Institute Real-time Monitoring and Incident Response: Offers real time a monitoring on security status and a response plan against incidents.

3.3 External Layer Security

- ISP security: Under this program, ESPs will be required to work with ISPs for implement firewalls, intrusion detection systems etc. The aim is to safeguard unauthorized access from internet boarders.
- Cloud flare Or Equivalent Security Platforms — Use platforms such as Cloudflare to prevent damage due to DDoS attacks and other cyber threats.
- IIS Security: Apply patches and harden configurations on IIS servers.
- Access Control: Create an IP filtering and access control for blocking external access.
- Monitor and Audit Security: Regularly audit the security measures from an external perspective to review how effective all of which are.

3.4 Internal Layer Security

- User Access Control: Multi-factor authentication (MFA) & Users access to based on roles.
- No Servers shall be left unattended: update underperforming servers as and when required, deploy IDS/IDPS to track incoming/outgoing network traffic.
- Data Encryption: Protect data with SSL/TLS to keep it private.
- IDPS Implementation: Equip internal networks to gaze for malicious activity and attacks.
- Segment your network: Segregate sensitive information by using network segmentation to limit what server users can access.
- Security Audits: Perform regular internal security audits and penetration-test your systems to check the strength of security measures.

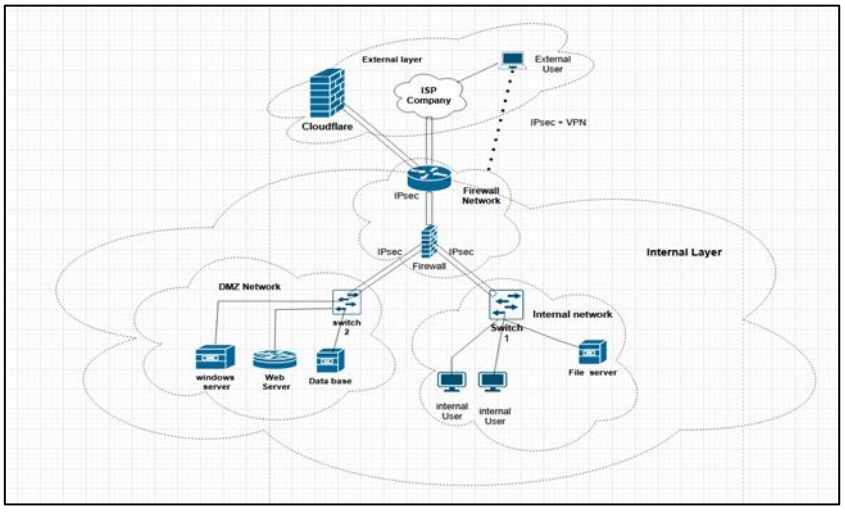

FIG.1. HIGH-LEVEL DIAGRAM OF NETWORK ORGANIZATION

4. HARDWARE SECURITY

4.1 External Network

The external network has the role of connecting local area networks (LAN) and wireless area networks (WAN) of the local area network to the external user accessing the LMS (Moodle, for example) from outside the local area network. The edge router, which is the first funnel point to which external users connect, connects to the network of the organization via its Internet Service Provider (ISP). IP based ACLs on edge router To alleviate this threat, additional security can be adapted by integrating things like Cloud flare, utilizing protocol layer protection such as IIS and IPsec to secure the data between two points, monitor active users, and utilizing group policy in addition to truly limit whom has elevated permission.

4.2 Internal Network

On the other hand, devices within the organization access the internal net using private IP address ranges. It resides outside of the internet and allows firms to store data and manage files through centralized servers. The internal network does not require access to the outside internet, but provides local transfer and management of data more efficiently.

4.3 Firewall Network

Firewalls filter traffic and control access and complement other security methods to protect external and internal layers of the network. The edge router is the gateway and the first firewall device using firewall software to protect the communication with the ISP while IPsec encrypts the data. All of the inbound and outbound traffic passes through a firewall which then monitors and filters this traffic using security policies, providing VPN services and two factor authentication with the user.

4.4 Demilitarized Zone (DMZ)

It provides a segregated network called DMZ that manages user traffic from internal to external systems. Access is monitored and controlled by firewalls, group policies, and log servers. Coupled with Cloud flare and SSL/IPsec, the all edge routing ensure that whatever is sent over the wire, it cannot be intercepted.

5. SOFTWARE SECURITY

5.1 Security Measures for LMS (Moodle) Platform

Software security is a core aspect of an organization's and user's data security especially when using Learning Management Systems (LMS) such as Moodle. Basic encryption methods like advanced encryption, cryptographic codes, file locking, and domain whitelisting are foundational to improved security on the platform. MFA is also integrated into the system for extra data protection when integrating to third party applications.

5.2 Security Practices in Educational Organizations

- Authenticates: In addition to the password, two-factor authentication (2FA) prompts users to authenticate through mobile devices (through apps, SMS, or email), to provide an added security layer.
- Authorization: The user is given access to the system using an individual username and password, which is stored in group policies or a TACACS server. The stored information decides whether permissions can be granted.
- Group Policies restrict users (guests, managers, or teachers) from accessing specific features they do not need to interact with, providing effective user privileges that prevent misuse and protecting sensitive features from unauthorized access.
- Secure Sockets Layer (SSL)—SSL technology keeps data during transmission by the means of encryption secure by preventing unauthorized access, modification, or interception, contributing to secure communication between networks of servers.

6. MOODLE LMS

Security features of the Moodle platform

Moodle has a number of protection mechanisms that are implemented for the protection of user data and enhance the security. And comes with security features such as group policies, file histories, etc., which you can use to create user access. To do this, this data is communicated over the air during transmission with secure methods, especially with encryption methods such as the SSL protocol.

a. Authentication

Self-avoid Password Reset: Allows users to change their password via net sites and many other self- disciplined methods leading to company offloading of IDENTIFICATION department.

Email & Authentication: Email Confirmation serves as a tool for confirming the identity of users signing up onto an app, whereas this keeps user identities protected while its at it dealing with login as well (so funny puns).

Multi-factor Authentication (MFA) – Enhances security with methods such as phone call verification and mobile app notifications that provide greater variety than hardware tokens alone.

b. Access Control

The platform authenticates user data so that no-one else has a axis to it and it keeps thedevice serial number, IP address,

location. If an unknown device tried to log in, then a user will be notified via email.
The user needs to get validated on both, i.e., LMS admin and User when he logs in on multiple devices simultaneously.

c. Login Management

User Login Check: Checks for login credentials and check for user presence.
First Time Login : To save user details and make an API call for authentication for the first login.
Subsequent logins: Matches credentials and sends an approval for the login.
Single sign on: Post approval users will not have to re-enter their credentials to access the platform.

d. Security Best Practices

Frontline Guard Beating: Tighten arrangements for hard secret word and guarantee that such solid secret word and required is in reality front line guard. Central Management: A system for managing user accounts and access control makes it easier to control access. SSO Integration: Reduces verification to one set of credentials, minimizing logins. Conditional Login: Using conditional login based on variables, such as location or device, adds an additional layer of security in levels. Privileged Account Protection: Monitoring all movements of privileged account, and controlling them to detect odd behavior Multi-Factor Authentication (MFA) Deployment: By requiring more than one form of authentication to build extra layers that help secure the learning platform on several levels.
If these measures are applied wisely, the Moodle platform is sure to provide secure endpoints, safeguard sensitive data and greatly improve overall security for everyone involved. The four main elements that make up the online courses that are created via the Moodle platform; users, enrolled programs, and databases, are depicted together in this schematic.

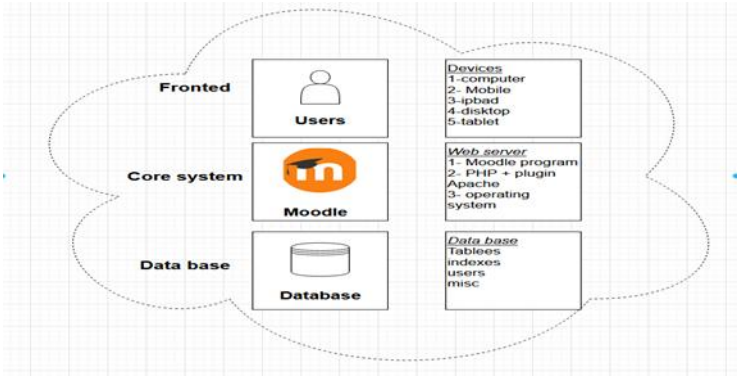

FIG. 2. HIGH-LEVEL DIAGRAM OF MOODLE PLATFORM

7. MOODLE USER AUTHENTICATION AND SYSTEM OPERATIONS

Users, whether internal or external, access Moodle through devices like iPads or laptops. The Moodle database stores user details, including device serial numbers, and can block users or restrict access to a single device. Upon login, the session request is sent from the firewall to the database to verify the username. Based on the database's response, the user is authenticated for login. Core systems manage network traffic, directing it to the appropriate destinations. Moodle operates on both Windows and Linux servers, offering flexibility in deployment and compatibility with any operating system.

8. LMS AT ISLAMIC UNIVERCITY COLLAGE

8.1 LMS Platform Access and Security at IUL

At IUL, the LMS platform is governed by policies for both internal and external users. A load balancing server is used to manage the high volume of external user logins, preventing overload. Internal users, however, bypass the load balancer and access the LMS server directly via a fixed IP address from the DNS server, ensuring faster session speeds and increased security by using private IP addresses.
The platform utilizes SSL certification to secure communication between the LMS server and the database, keeping the database protected. LMS infrastructure for Moodle platform at Islamic University collage designed the same as the figure below.

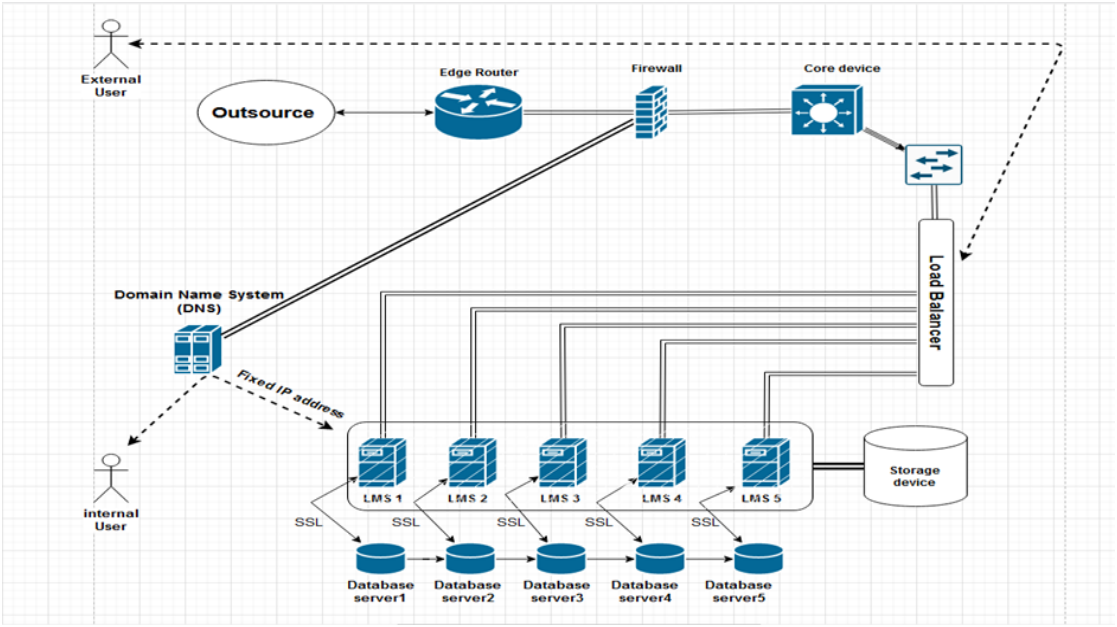

FIG.3. LMS INFRASTRUCTURE AT IUL

9. NETWORK AND SECURITY SETUP AT IUL

At IUL, the core device is a Cisco router responsible for routing traffic using protocols like EIGRP, OSPF, RIP, or static routing. It is connected to a firewall that controls access for administrators to the network. A Layer 2 switch connects the load balancer to the core device, routing traffic and managing session requests through VLANs to prevent loops. The DNS server matches hostnames to IP addresses and manages internal and external name resolution. Internal users with fixed IP addresses are allowed direct access to the LMS, bypassing the load balancer.

Storage devices are used for storing large amounts of data, such as course lectures, as Moodle itself does not handle large data storage. Fixed IP addresses, assigned by DNS, allow authorized internal users to bypass the load balancer for priority access. SSL technology ensures secure data transmission between servers and clients, preventing unauthorized interception, and is critical for securing external web servers.

10. HARDWARE SECURITY HARDWARE SECURITY

10.1 Security Measures in Moodle Platform

To enhance security and protect user privacy on the Moodle platform, policies and measures are implemented based on user roles (e.g., guest, student, teacher, admin). Group policies control access and protect against hackers. Log files track user activities, including login/logout events and actions like viewing courses or taking assessments. Each user has a profile containing course details, personal information, and password management options. Users with appropriate permissions can view others' profiles. Course content, including student folders, tasks, and grades, is accessible through user profiles. The system logs user activity, including login and logout events, for monitoring and security purposes. Internet Information Services (IIS) supports SSL with Server Name Indicator (SNI), allowing virtual domain identification during SSL negotiation.

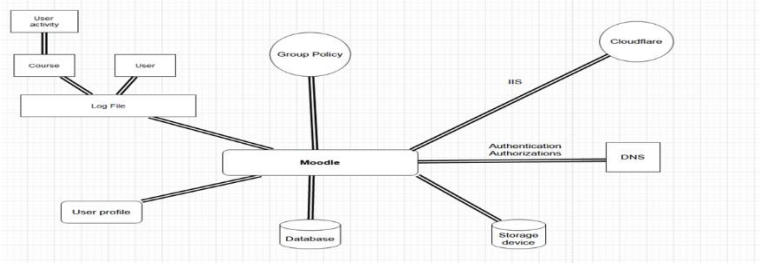

FIG. 4. HARDWARE SECURITY AT IUL

10.2 Security Measures for Ims

Group Policies and User Access
In the LMS, default group policies include "teacher," "student," and "admin," with the option to create additional groups and apply restrictions based on roles. For example:

- **Students** can access class materials, submit assignments, and participate in discussions.
- **Teachers** can manage classes, upload materials, grade assignments, and provide feedback.
- **Staff** handle academic affairs and attendance records.
- **Admins** integrate student, course, and enrollment data.

10.3 Security Measures for Ims

Far Away from Guessable Information Make Use of Strong and Complex Passwords Email verification and similar secondary authentication methods improve security. Role-based user privileges are managed so only appropriate access is permitted.

Software Security Features

Authorization: Strong authentication protocols protect user identities and transactions. Something like two-factor verification makes it hard for hackers to penetrate by another means, account lockouts after a number of failed logins keeps them from using password guessing attacks. Login credentials are protected with bank-grade encryption, both in transit and at rest, so no one can snatch up passwords. Logins from unexpected geographic locations tospoof account takeovers with the help intrusion detection systems and so forth. Encryption of data — All data transfers go through mandatory SSL/TLS tunnels, the military-strength cryptography provides complete privacy of students and teachers regardless of the network; The backend databases as well are not decipherable minus a clearance. User Roles and Permissions: A role-based access control system provides faculty with tailored permissions based on their teaching responsibility and keeps students out of sensitive administration screens. System admin can only see what they need for troubleshooting the issues. Secure APIs: APIs are built using security-focused methodologies and they are critically checked for vulnerabilities prior to being exposed to third-party clients. Gateway policies impose strict authentication requirements that prevent unauthorized scripting. Constant Changes: Technetium specific platform code is merged immediately after testing of downstream allied open-source projects defense mechanisms and bug fixes. This timely patching directly prevents exploit attempts and avenues from being abused by cybercriminals. Monitoring and Logging: Predictive analytics through AI alert admins when there are deviations from the norm, accidental or malicious, and provide an exhaustive audit trail to fix issues before an evolving threat becomes too damaging. Data Backup: In the event of the worst-case scenario, users lose no valuable work through foolproof backup standard operating procedures and disaster recovery blueprints. Offsite replication eliminates the window of opportunity for being affected by accidental misfortunes or deliberate ransoms. Each of these strong defenders of the security, path, up, sustain the LMS, integrity, availability and confidentiality commitments, ensuring that the military grade security our-screened for decades for even classified national interest operations works for students, or teachers, or even institutional data.

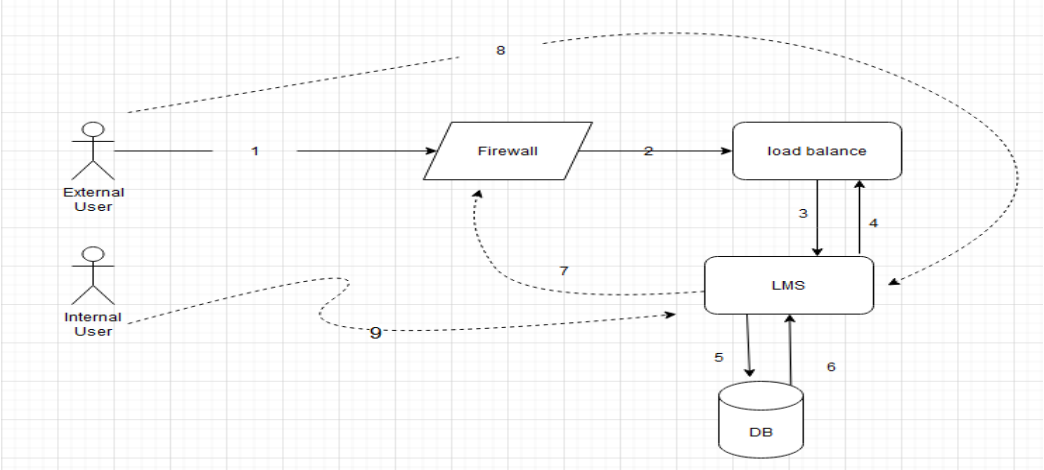

FIG.5. SOFTWARE SECURITY AT IUL

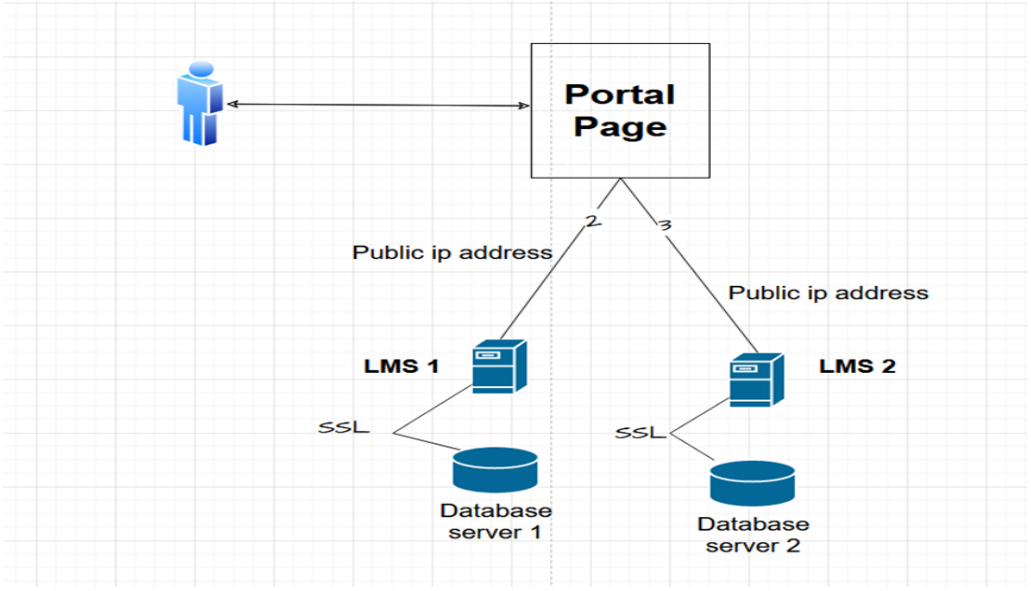

FIG. 6. MOODLE PROCESS FOR LOGIN AT IUL

11. WEAKNESSES AT THE ISLAMIC UNIVERSITY OF LEBANON (IUL)

1. **Insecure Moodle Portal:** The Moodle portal lacks adequate security measures, making it vulnerable to unauthorized access and potential data breaches. Enhancing its security is necessary to protect user information.
2. **Lack of Two-Factor Authentication (2FA):** Two-factor authentication is not implemented, leaving user accounts exposed. Enabling 2FA would add an extra layer of protection and reduce the risk of unauthorized access.
3. **Weak Password Policy and Sharing:** The current password policy is insufficient, and password sharing may compromise account security. A stronger password policy and awareness campaigns are needed to address these risks.
4. **LMS Platform on Local Server:** The LMS is hosted on the university's local server, which may lack the security benefits of cloud-based solutions. Migrating to a secure, cloud-based infrastructure could improve security, scalability, and redundancy.

12. EXPERIMENTAL RESULTS

Far Away from Guessable Information Make Use of Strong and Complex Passwords Email verification and similar secondary authentication methods improve security. Role-based user privileges are managed so only appropriate access is permitted.

Software Security Features

Authorization: Strong authentication protocols protect user identities and transactions. Something like two-factor verification makes it hard for hackers to penetrate by another means, account lockouts after a number of failed logins keeps them from using password guessing attacks. Login credentials are protected with bank-grade encryption, both in transit and at rest, so no one can snatch up passwords. Logins from unexpected geographic locations tospoof account takeovers with the help intrusion detection systems and so forth. Encryption of data — All data transfers go through mandatory SSL/TLS tunnels, the military-strength cryptography provides complete privacy of students and teachers regardless of the network; The backend databases as well are not decipherable minus a clearance. User Roles and Permissions: A role-based access control system provides faculty with tailored permissions based on their teaching responsibility and keeps students out of sensitive administration screens. System admin can only see what they need for troubleshooting the issues. Secure APIs: APIs are built using security-focused methodologies and they are critically checked for vulnerabilities prior to being exposed to third-party clients. Gateway policies impose strict authentication requirements that prevent unauthorized scripting. Constant Changes: Technetium specific platform code is merged immediately after testing of downstream allied open-source projects defense mechanisms and bug fixes. This timely patching directly prevents exploit attempts and avenues from being abused by cybercriminals. Monitoring and Logging: Predictive analytics through AI alert admins when there are deviations from the norm, accidental or malicious, and provide an exhaustive audit trail to fix issues before an

evolving threat becomes too damaging. Data Backup: In the event of the worst-case scenario, users lose no valuable work through foolproof backup standard operating procedures and disaster recovery blueprints. Offsite replication eliminates the window of opportunity for being affected by accidental misfortunes or deliberate ransoms. Each of these strong defenders of the security, path, up, sustain the LMS, integrity, availability and confidentiality commitments, ensuring that the military grade security our-screened for decades for even classified national interest operations works for students, or teachers, or even institutional data. The system needed improved security, and Microsoft Azure was recommended. Azure has multiple layers of security and disaster recovery capabilities that make it more secure from common threats such as DDoS attacks, Phishing, changing of content… etc. In addition to Azure providing storage with high resiliency and great speed, it allows you to easily integrate in Moodle through authentication via Azure Active Directory (AAD) Instead, it is suggested to adopt Azure within this infrastructure along with security implementation for encryption and two-factor authentication. The setup is tested with Moodle and Azure integration through AAD can be implemented successfully giving all the advantages of using Moodle. This is a system that needs to be installed on Microsoft Authentication app and then uses login credentials access provided by the IT department. By implementing these recommendations, the Lebanese Islamic University will be able to improve security within the LMS, ensuring the protection of sensitive data and information, enhancing user safety, and providing a secure learning environment. Fig.7 User Moodle process login by Microsoft Azure

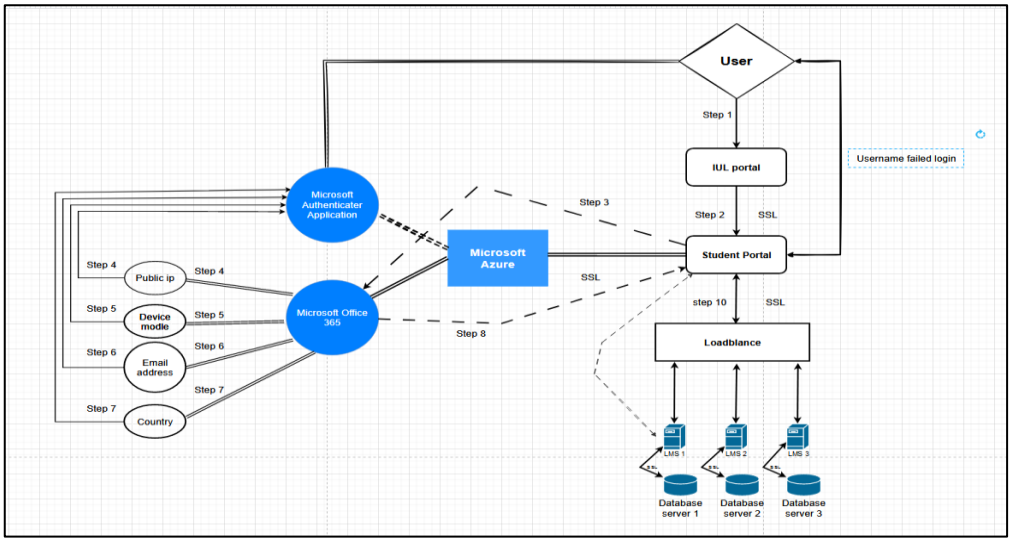

FIG.7. USER MOODLE PROCESS LOGIN BY MICROSOFT AZURE

User Login Process: -

Step 1: - The user will login to the IUL portal that is published for anyone in the world and login to the student porta by clicking on it the page will transfer to the student portal.

Step 2: - The student portal wanted the username and Id authenticator from the authenticator application.

Step 3: - When the user input the username and ID the portal will check the username if it's existing will send the session request check to Microsoft Office 365 from Azure connection to check some requirements (Username ID, email address, public Ip address, device model, country at the time login) all this must check valid of not from office365.

Step 4: - Microsoft Office 365 will check the last public Ip login and compare it with the public now if we have to change will be sent a request to the authenticator application to confirm login, if approve the request will processing with step 5.

Step 5: - Microsoft Office 365 will check the last device model login and compare it with the device model now if there is a change will be sent a request to the authenticator application to confirm login, if approve the request will processing with step 6.

Step 6: - Microsoft Office 365 will check the last email address and ID login and compare with username and ID now if there is a change will be sent a request to the authenticator application to confirm login, if approve the request will processing with step 7.

Step 7: - Microsoft Office 365 will check the last user country login and compare it with the country now if there is a change will be sent a request to the authenticator application to confirm login, if approve the request will processing with step 8.

Step 8: - After we existing the user's student login office365 will back the session to the portal by step 8 to open Moodle to a user.

Step 9: - The student portal will be sent a request to the LMS server through load balance.

Integrating the Moodle platform with Microsoft Azure enhances the reliability and performance of the system at the Lebanese Islamic University (IUL), offering benefits in terms of scalability, security, and performance. The university must comply with Azure policies regarding the number of users in the Learning Management System (LMS) and implement authentication tools within a single framework to verify email, IP address, country, and login via new devices. This will help resolve the issue of logging into the system across multiple devices with the same username. Regarding the security of the Moodle portal at IUL, the issue was classified as high risk, as the lack of security exposes the system to distributed denial of service (DDoS) attacks, which can lead to portal downtime and performance disruption. During the audit, it was found that the student and faculty portal is not sufficiently secured, as communication occurs via a public IP address and an unencrypted port, exposing the system to hacking and unauthorized access. To mitigate these risks, it is recommended to implement SSL/TLS encryption with a "full (hardened)" configuration to ensure that data sent between the client and the platform is encrypted using a secure hash function, making it impossible for attackers to decrypt the data even if it is intercepted.

FIG. 8. MOODLE PORTAL AT IUL

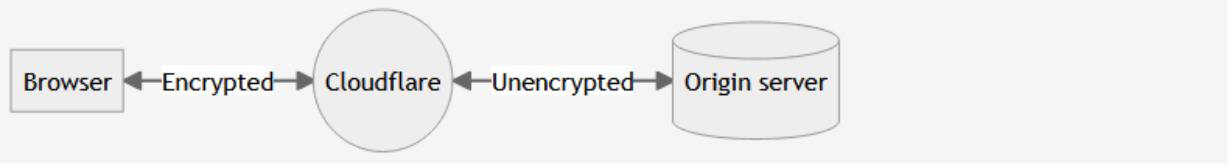

FIG. IX. FLEXIBLE - SSL/TLS ENCRYPTION MODES

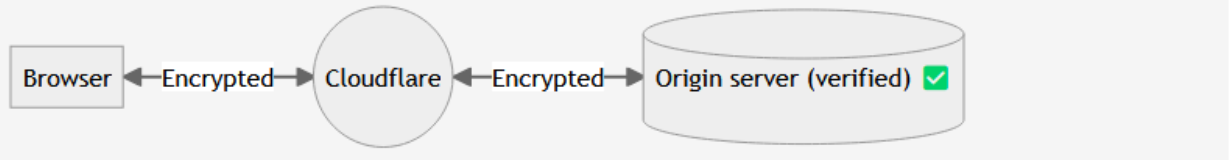

FIG. 9. FULL (STRICT) - SSL/TLS ENCRYPTION MODES

12.1 Two Factor Authentication Not Enabled (security to manage access)

- **Risk Rating: Medium –** The absence of multi-factor authentication (2FA) on the Moodle platform at the Lebanese Islamic University increases the risk of unauthorized access to user accounts, even if passwords are leaked.
- **Comments:** Access control is critical to security, and multi-factor authentication provides an additional layer of protection. It requires users to provide a second verification factor, such as a code sent to their phone or a fingerprint, during the login process.
- **Implications:** Enabling multi-factor authentication significantly enhances account security by adding an additional barrier to attackers attempting unauthorized access, as they require the second authentication factor, which is typically difficult to obtain or replicate.

Recommendation: It is highly recommended to enable multi-factor authentication for the Moodle platform at IUL. This can be done using authentication solutions provided by Cloud flare and Azure, which offer methods such as email verification, phone call verification, or authentication apps. This will enhance security and protect user accounts from unauthorized access.

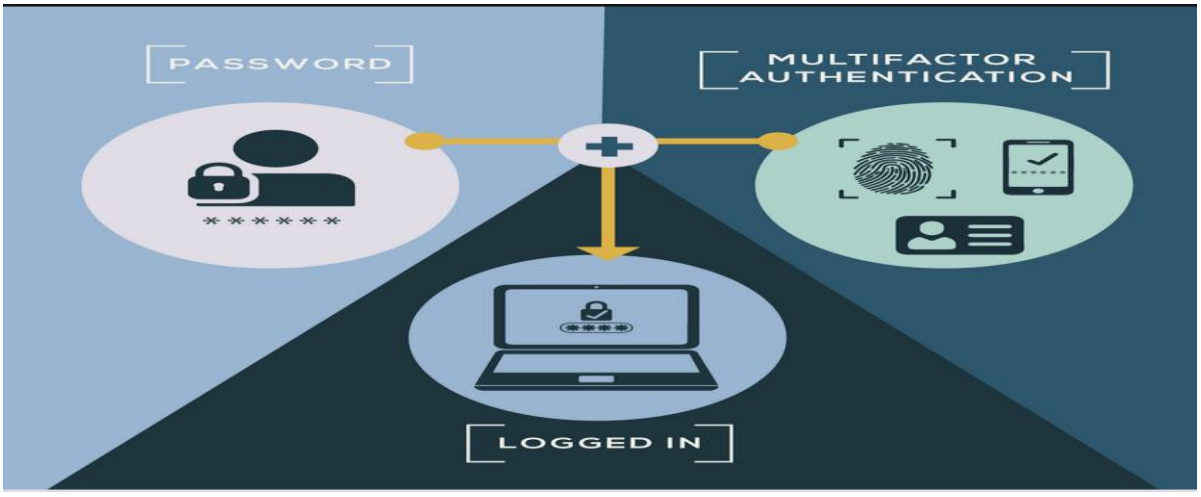

FIG. 10. TWO-FACTOR AUTHENTICATION PROCESS

12.2 Results and recommendations regarding passwords in Moodle

a. Sharing usernames and passwords

- **Risk Rating:** High – Sharing passwords through unsecured channels increases the risk of unauthorized access, leading to data leaks, data tampering, and system disruption, especially during exams.
    a. **Notes:** Controls and policies should be implemented to prevent unsecured password sharing. Sharing passwords without security measures exposes accounts to compromise.
- **Implications:** Without a policy, password sharing becomes an easy target for attackers. Enforce the use of encrypted passwords and avoid using personal data or sharing passwords through unsecured channels.
- **Recommendation:** It is essential to establish a policy for sharing passwords through secure channels, ensuring passwords are encrypted and obtaining user consent. Documents should also be signed when sharing passwords to ensure the confidentiality and security of the data.

b. Not customizing password policy

- **Risk Rating: Medium –** Weak passwords threaten account security and can be exploited by hackers using various tools.
- **Notes:** Without a standardized password policy, some users may choose weak passwords, increasing the chances of unauthorized access.
- **Implications:** The lack of a standardized password policy allows for weak passwords, making accounts vulnerable to hacking.

- **Recommendation:** A strong password policy should be documented and implemented, including authentication mechanisms and specifying a minimum password length, the number of uppercase and lowercase letters, numbers, and special characters.

12.3 Moodle App Policy Simulation

Moodle runs on a virtual machine (VM) or hosted in the cloud, where the application gets a local IP address for secure login

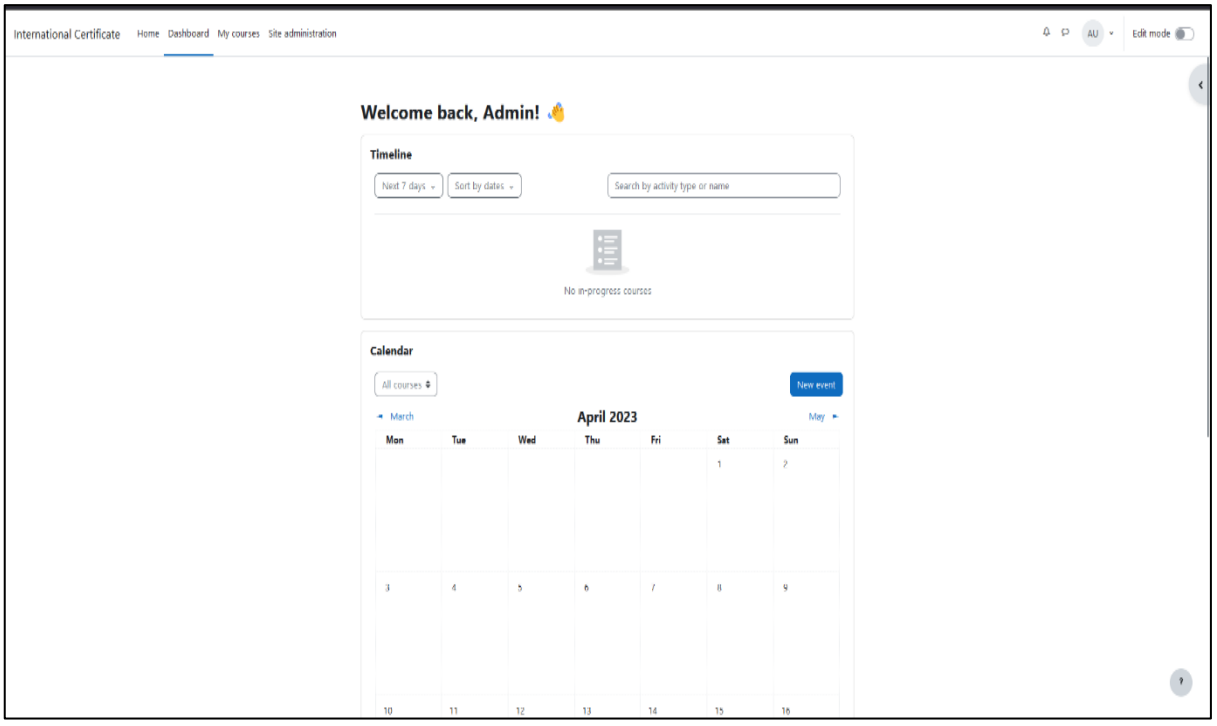

FIG. 11. RUNNING MOODLE APPLICATION ON A VIRTUAL MACHINE

Login to Moodle by the private Ip address from (VM) and go to site administer > security.

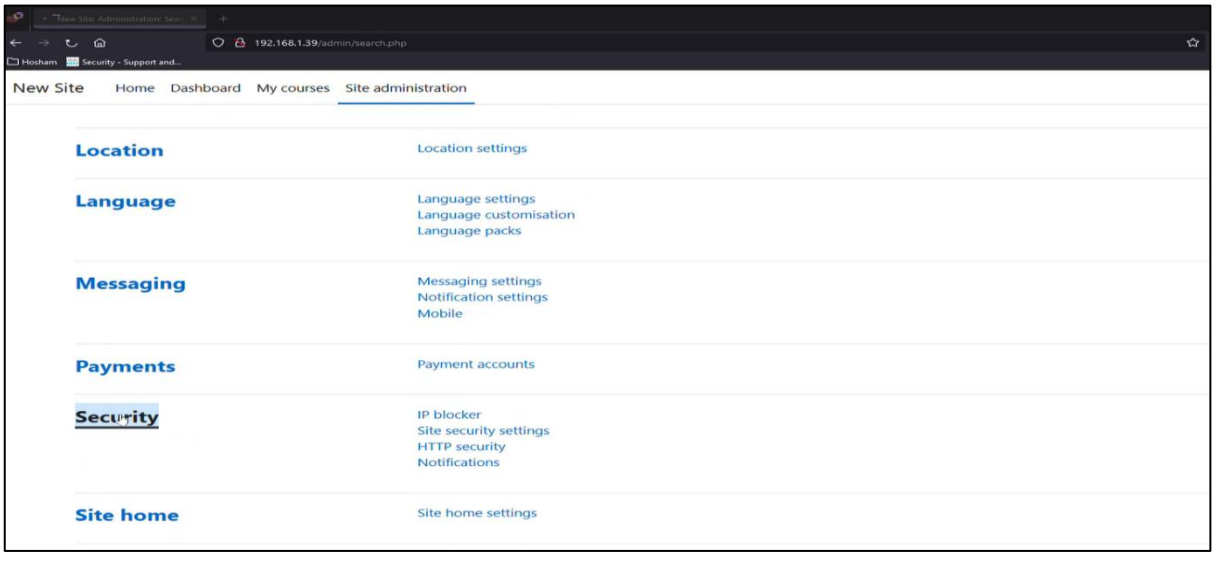

FIG. 12. SECURITY SETTING ON MOODLE PLATFORM

Going to password policy and enabling by default it is not enabled and implement the suggestion work above (Recommendation) side.

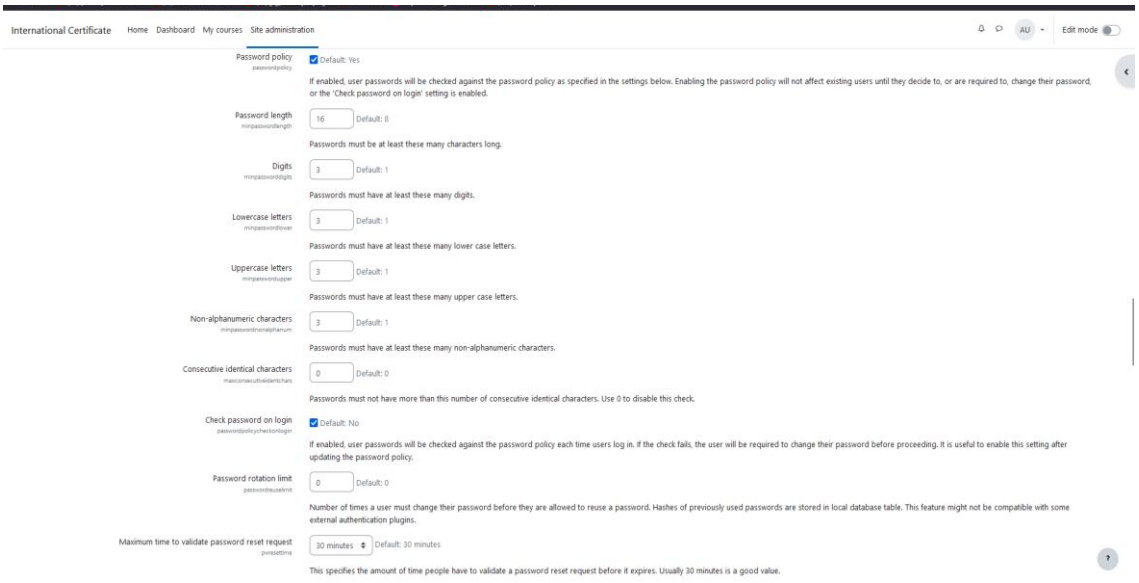

FIG. 13. PASSWORD POLICE DETAILS

After the implementation the suggestion of password policy go to add new user for checking the password policy grate or not by going to Site administration >> users as shown below

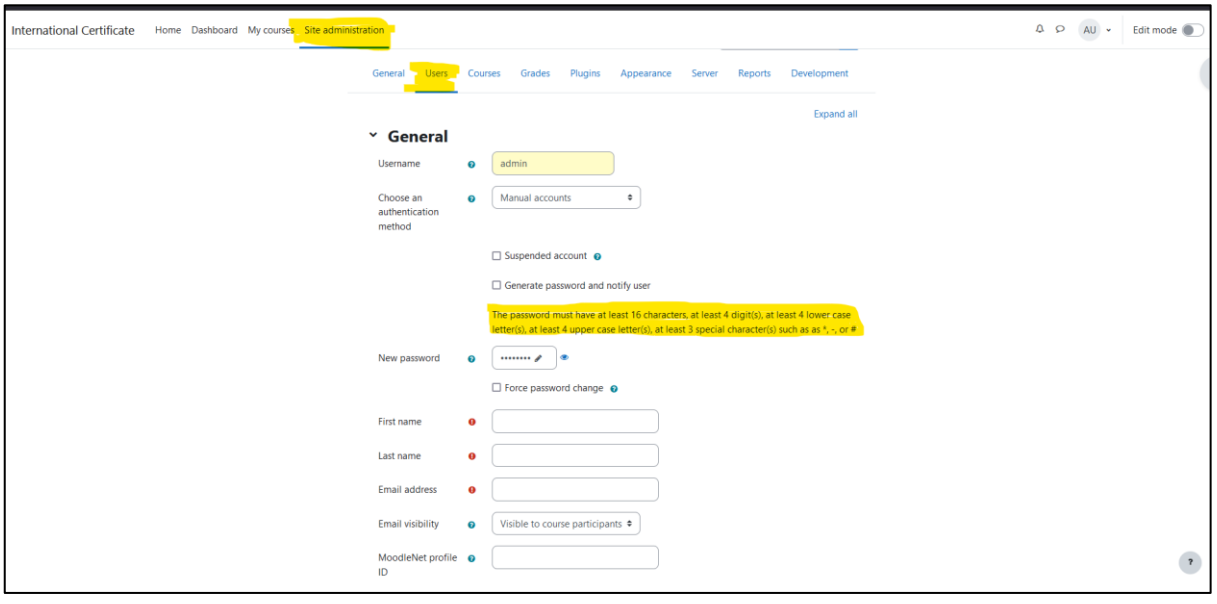

FIG. 14. ADD NEW USERNAME AND PASSWORD

If the not creating the username and password with the policy the

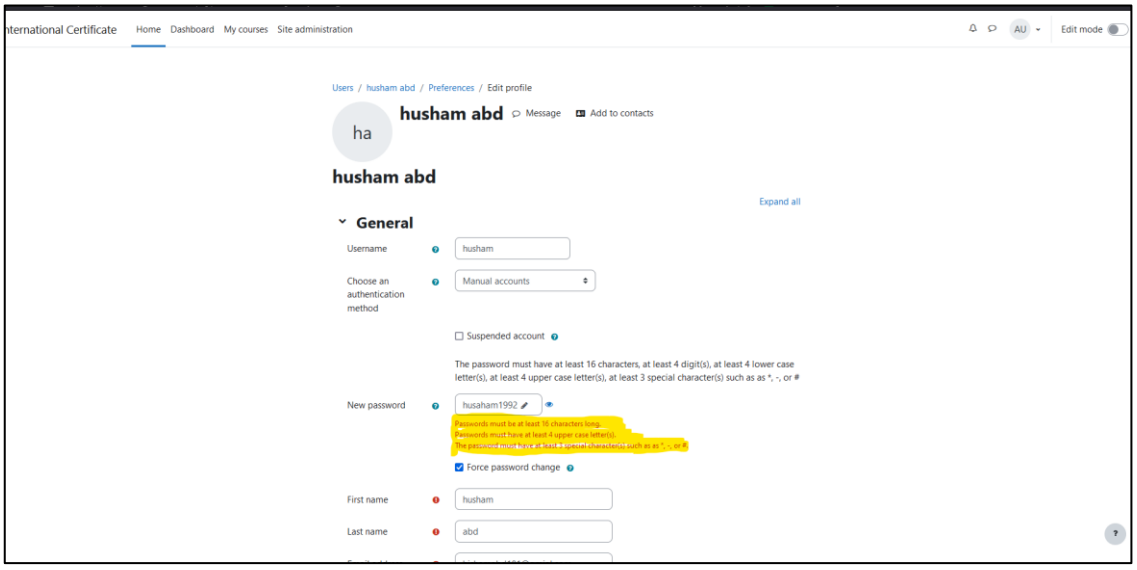

FIG. 15. ERROR LOG FOR THE USER NOT USING THE PASSWORD POLICY

12.4 Findings and Recommendations on Security in Moodle

SaaS usage

Risk Rating: Medium – A cloud hatched Moodle through a SaaS is likely to be less affected by energy cuts, catastrophes, and maintenance challenges. This is an important step and even more so for a platform like moodle which caters to a lot of users. Notes: SaaS stands for Software as a Service, which means access to software online offered by a third-party provider that you do not need to worry about managing complex software or hardware. You can host it on the cloud and then the scalability and security of the data can be availed during crucial times like exams. Recommendation: Since having a Moodle platform based locally has an effect on service availability because of the power cuts and political issues in Lebanon, we highly recommend to have the platform hosted on the cloud.

12.5 Use a VPN app

Risk Rating: Medium – The VPN policy on Moodle increases security to potential attacks like DDoS, because it ensures that all the users are getting approval from the server to access the application. Note: VPNs are widely employed in organizations to ensure an additional layer of security, and reduced chances of cyber-attack. Conclusions: The VPN provides security and lessens the risk of external attacks like DDoS, and helps response time be faster and overall security to be higher. OVE: VPN SYSTEM: It must be recommended to maintain the organization and increase protection as well as data against hackers. A VPN offers capabilities like encryption and truly unique factor verification.

12.6 VPN Policy Simulation on Moodle App

- **Download Open VPN**: The user downloads the app from the Google Play Store or another source depending on the operating system.
- **Generate an Open VPN configuration file**: A configuration file containing the necessary certificates and keys is created on the organization's primary device.
- **Distribute the configuration file**: The file is sent to users who wish to connect via Open VPN.
- **Log in using the public IP:** The user logs in via the app using the primary device's public IP.
- **Assign a private IP address:** The user is assigned a private IP address through DHCP.

By following these steps, users will be able to securely connect to the organization's network via Open VPN, providing an additional layer of security through the allocation of a private IP address.

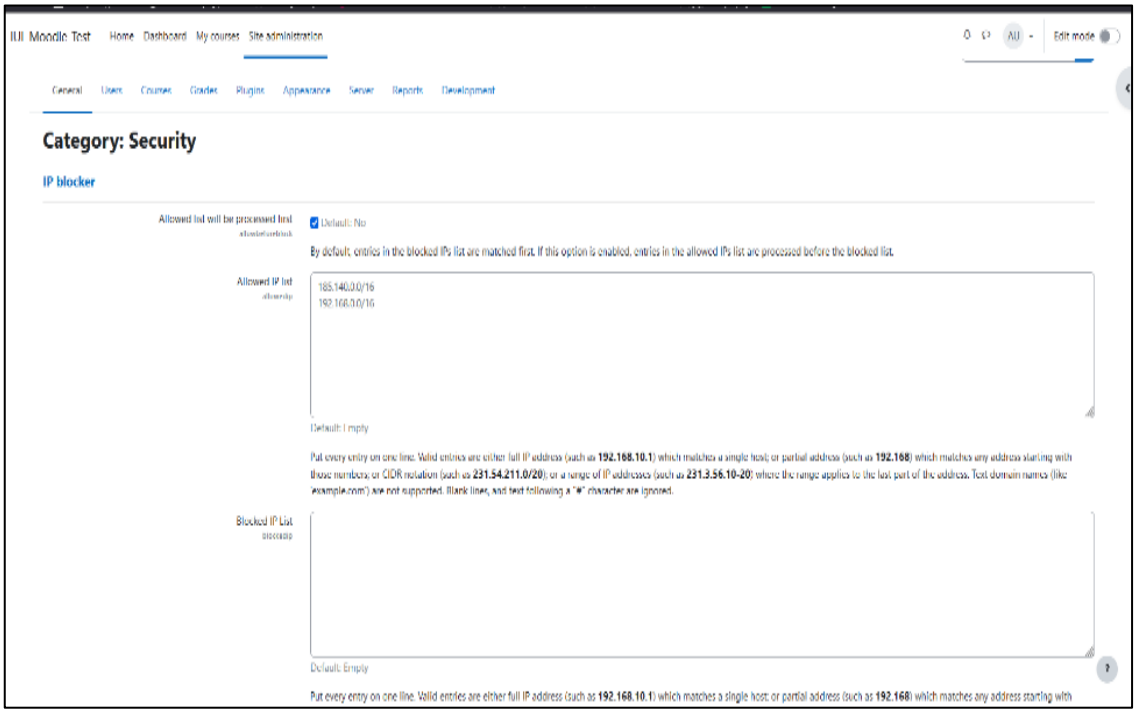

FIG. 16. ALLOWED LIST AND BLOCK LIST FROM MOODLE SIDE

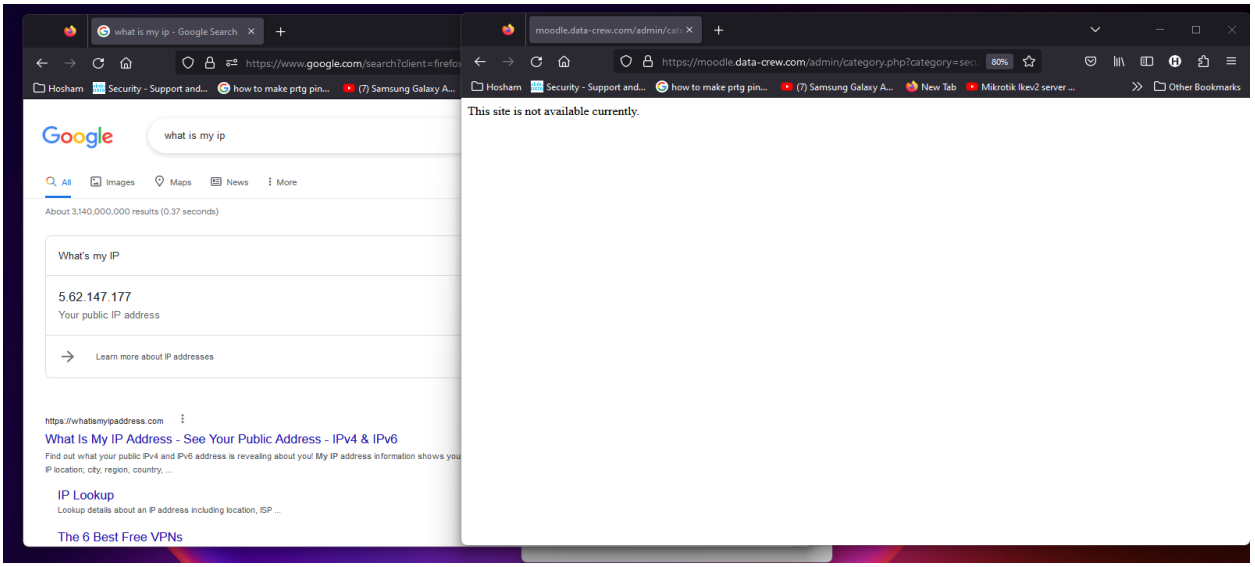

FIG. 17. USER TRYING TO LOGIN MOODLE

In Figure 17, the user cannot log in to Moodle because he is not using the OpenVPN application and does not have the IP address allowed by Moodle. However, when the user connects to OpenVPN, he will be given an IP address within the range allowed by Moodle, as shown in Figure 17.

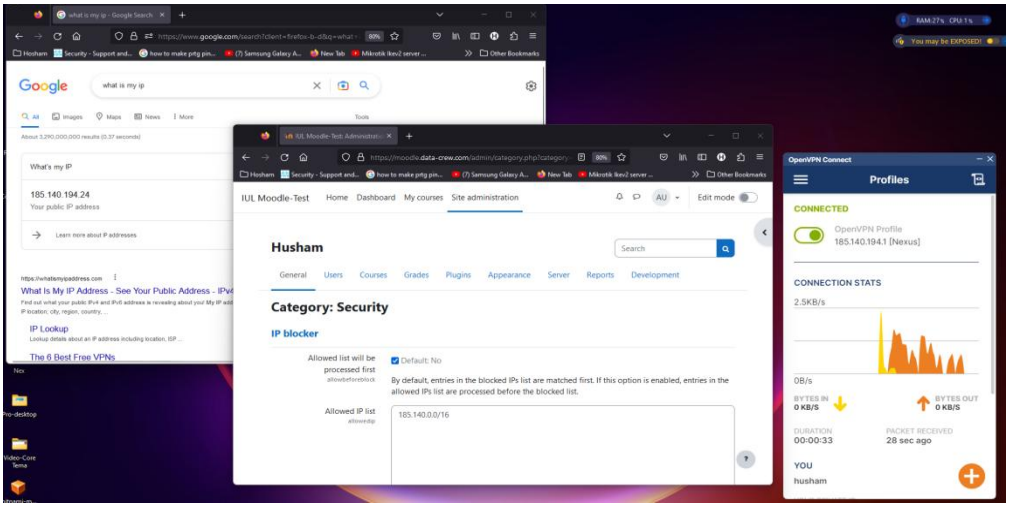

FIG. 18. USER TRYING TO LOGIN MOODLE BY USING THE OPENVPN APPLICATION

12.7 Username and password authentication implementation

User-level authentication is implemented using PHP code that connects to an external server via the Moodle platform's "Authentication via External Web Service" plugin. Authentication includes username and password verification, as well as IP address, email, and country verification to determine the user's location and the legitimacy of the login. By connecting to the external server, we verify each new login to Moodle, enhancing security and ensuring access only to authorized users from specific organizations.

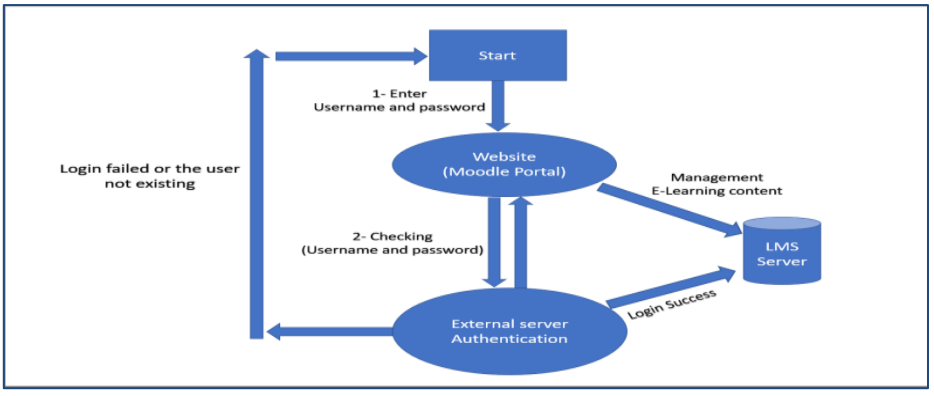

FIG. 19. FLOWCHART MOODLE INTEGRATION WITH EXTERNAL AUTHENTICATION SERVER

12.8 Moodle integration with external authentication server

- **Start:** The starting point in the flowchart.
- **Initialize the plugin:** Initialize the authentication plugin, load the configuration, and select the authentication type.
- **Get user data:** Get the username and password.
- **Call an external web service:** Call the web service and pass user data and default parameters.
- **Verify authentication result:** Examine the web service response to determine whether authentication was successful.
- **Return authentication status:** Return the authentication status (true or false) to the calling code.

To improve the authentication process, an external web server is used to verify user details. If the username exists in the database, a value of zero is returned, indicating successful login. If the login details are incorrect, a value of one is returned. To facilitate monitoring, Moodle provides debugging capabilities, allowing administrators to review login details and diagnose any problems that may arise.

12.9 Php Code: -

```
<?php
defined('MOODLE_INTERNAL') || die();
$CFG =;
require_once($CFG->libdir.'/auth lib.php');
class auth_plugin_ws extends auth_plugin_base {
    public function __construct() {
        $this->authtype = 'ws';
        $this->config = get_config('auth_ws');
        if (isset($this->config->default_params) && !empty($this->config->default_params)) {
            $params = explode(',', $this->config->default_params);
            $defaultparams = array();
            foreach ($params as $p) {
                list($paramname, $value) = explode(':', $p);
                $defaultparams[$paramname] = $value;
            }
            $this->config->ws_default_params = $defaultparams;
        } else {
            $this->config->ws_default_params = array();
        }
    }
    public function user_login($username, $password): bool
    {
        $functionname = $this->config->auth_function;
        $params  = array(
            $this->config->auth_function_username_paramname => $username,
            $this->config->auth_function_password_paramname => $password
        );
        $result = $this->call_ws($this->config->serverurl, $functionname, $params);
        return ($result->{$this->config->auth_function_resultClass}->{$this->config->auth_function_resultField} == true);
    }
    private function call_ws($serverurl, $functionname, array $params = array()) {
    $serverurl = sprintf("%s?wsdl", $serverurl);
    $params = array_merge($this->config->ws_default_params, $params);
    try {
        $client = new SoapClient($serverurl);
    } catch (SoapFault $e) {
    }
    try {
        $resp = $client->__soapCall($functionname, array($params));
        return $resp;
    } catch (Exception $e) {
        echo "Exception:\n";
        echo $e->getMessage();
        echo "===\n";
        return false;
    }
}
    public function prevent_local_passwords() {
        return true;
    }
    public function is_internal() {
        return false;
    }
    public function is_synchronised_with_external() {
        return false;
```

```
    }
    public function can_change_password() {
        return false;
    }

public function change_password_url() {
        if (isset($this->config->changepasswordurl) && !empty($this->config->changepasswordurl)) {
            return new moodle_url($this->config->changepasswordurl);
        } else {
            return null;
        }
    }
    public function can_reset_password()
   public function user_update_password($username, string $newpassword) {
    // Implement the logic to update the user's password using the external web service
    $functionname = $this->config->changepassword_function;
    $params = array(
        $this->config->changepassword_function_username_paramname => $username,
        $this->config->changepassword_function_newpassword_paramname => $newpassword
    );
    $result = $this->call_ws($this->config->serverurl, $functionname, $params);
    // Return true or false based on the password change result
    return                                  ($result->{$this->config->changepassword_function_resultClass}->{$this->config-
>changepassword_function_resultField} == true);
    }
}
    protected function setAuth(string $auth): auth_plugin_ws
    {
        $this->auth = $auth;
        return $this;
    }
```

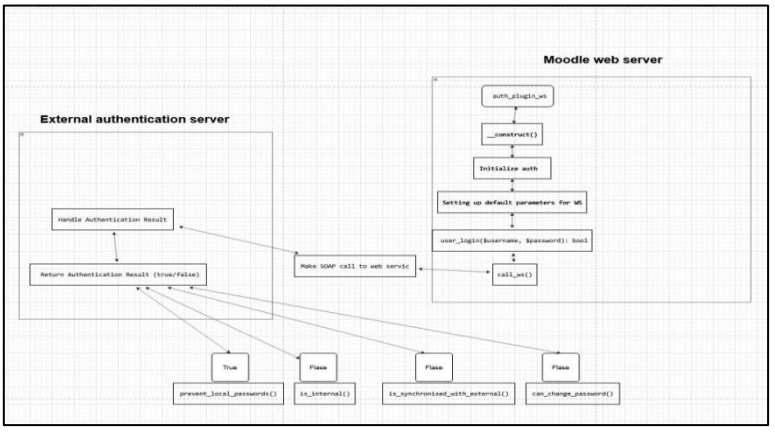

FIG. 20. A FLOWCHART TO VISUALIZE THE LOGIC OF THE (AUTH_PLUGIN_WS) CLASS.

Here's a description of each process in the flowchart

12.10 Moodle Authentication Integrations

- construct (): Initializes the auth_plugin_ws class, sets the authentication type to 'ws', and retrieves the configuration settings.
- Set WS Default Parameters: Checks for default parameters in the configuration and sets them for the web service.
- Initialize Auth: Initiates the authentication process.

- user login ($username, $password): Processes the user login by calling the authentication function via the web service and verifying the result.
- call_ws(): Makes a SOAP call to the external web service with the specified parameters.
- Make a SOAP call: Sends a SOAP request to the external web service and retrieves the response.
- Handle the authentication result: Processes the authentication response and handles any errors or exceptions.
- Return Auth Result (true/false): Returns the authentication result based on the web service response.
- prevent_local_passwords(): Determines whether local passwords should be prevented (returns true).
- is_internal(): Determines whether authentication is internal (returns false).
- is_synchronized_with_external(): Determines whether authentication is synchronized with an external source (returns false).
- can_change_password(): Determines whether the password can be changed (returns false).
- change_password_url(): Specifies the URL for changing the password, based on the configuration settings.
- can_reset_password(): Determines whether the password can be reset (not implemented in the schema).
- user_update_password($username, $newpassword): Updates the user's password using an external web service and returns the result.
- setAuth($auth): Sets the auth property of the auth_plugin_ws class and returns the instance of the class.Overall, the flowchart represents the control flow and interactions between different processes and functions within the auth_plugin_ws class for web service authentication in Moodle.

```
defined('MOODLE_INTERNAL') || die;
if ($ADMIN->fulltree) {
  $settings->add(new admin_setting_configtext('auth_ws/serverurl',
                        get_string('serverurl', 'auth_ws'),
                        get_string('serverurl_desc', 'auth_ws'),
                        '', PARAM_TEXT));
  $settings->add(new admin_setting_configtext('auth_ws/default_params',
                        get_string('default_params', 'auth_ws'),
                        get_string('default_params_desc', 'auth_ws'),
                        '', PARAM_TEXT));
  $settings->add(new admin_setting_configtext('auth_ws/auth_function',
                        get_string('auth_function', 'auth_ws'),
                        get_string('auth_function_desc', 'auth_ws'),
                        '', PARAM_TEXT));
  $settings->add(new admin_setting_configtext('auth_ws/auth_function_username_paramname',
                        get_string('auth_function_username_paramname', 'auth_ws'),
                        get_string('auth_function_username_paramname_desc', 'auth_ws'),
                        '', PARAM_TEXT));
  $settings->add(new admin_setting_configtext('auth_ws/auth_function_password_paramname',
                        get_string('auth_function_password_paramname', 'auth_ws'),
                        get_string('auth_function_password_paramname_desc', 'auth_ws'),
                        '', PARAM_TEXT));
  $settings->add(new admin_setting_configtext('auth_ws/auth_function_resultClass',
                        get_string('auth_function_resultClass', 'auth_ws'),
                        get_string('auth_function_resultClass_desc', 'auth_ws'),
                        '', PARAM_TEXT));
  $settings->add(new admin_setting_configtext('auth_ws/auth_function_resultField',
                        get_string('auth_function_resultField', 'auth_ws'),
                        get_string('auth_function_resultField_desc', 'auth_ws'),
```

```
                    '', PARAM_TEXT));

    $settings->add(new admin_setting_configtext('auth_ws/changepasswordurl',
                    get_string('changepasswordurl', 'auth_ws'),
                    get_string('changepasswordurl_desc', 'auth_ws'),
                    '', PARAM_TEXT));
    $deleteopt = array();
    $deleteopt[AUTH_REMOVEUSER_KEEP] = get_string('auth_remove_keep', 'auth');
    $deleteopt[AUTH_REMOVEUSER_SUSPEND] = get_string('auth_remove_suspend', 'auth');
    $deleteopt[AUTH_REMOVEUSER_FULLDELETE] = get_string('auth_remove_delete', 'auth');

    $settings->add(new admin_setting_configselect('auth_ws/removeuser',
      new lang_string('auth_remove_user_key', 'auth'),
      new lang_string('auth_remove_user', 'auth'), AUTH_REMOVEUSER_KEEP, $deleteopt));
}
```

12.11 Authentication Settings Using Auth_ws in Moodle

- auth_ws/serverurl: A text field specifying the URL of the web service used for authentication.
- auth_ws/default_params: A text field specifying the default parameters for the web service to be included in each request.
- auth_ws/auth_function: A text field specifying the name of the authentication function in the web service.
- auth_ws/auth_function_username_paramname: A text field specifying the name of the username parameter in the authentication function.
- auth_ws/auth_function_password_paramname: A text field specifying the name of the password parameter in the authentication function.
- auth_ws/auth_function_resultClass: A text field specifying the class name of the object representing the authentication result.
- auth_ws/auth_function_resultField: A text field specifying the name of the field in the object containing the authentication result.
- auth_ws/changepasswordurl: A text field specifying the URL for changing the password. auth_ws/removeuser: A selection field to specify the user removal behavior (save, suspend, delete).

These settings are displayed on the admin settings page when $ADMIN->fulltree is verified as true. This allows the plugin to be configured to connect to an external authentication server and provide an additional layer of security by verifying user data.

Site administration >> plugins >> Install plugins>> choose zip file >> install plugin from the ZIP file.

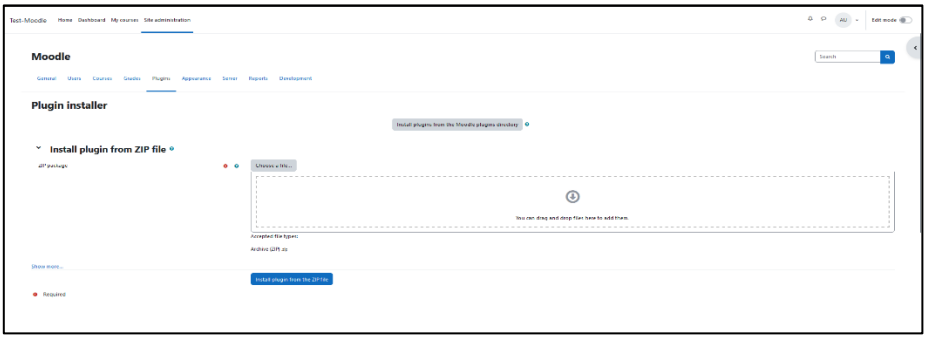

FIG. 21. PLUGIN PHP ZIP FILE TO MOODLE

The PHP code uploaded to Moodle platform from the install plugin future from Moodle side, we install and must be synchronization it with external server authentication as shown int figure below
Site administration >> plugins >> External webservice authentication

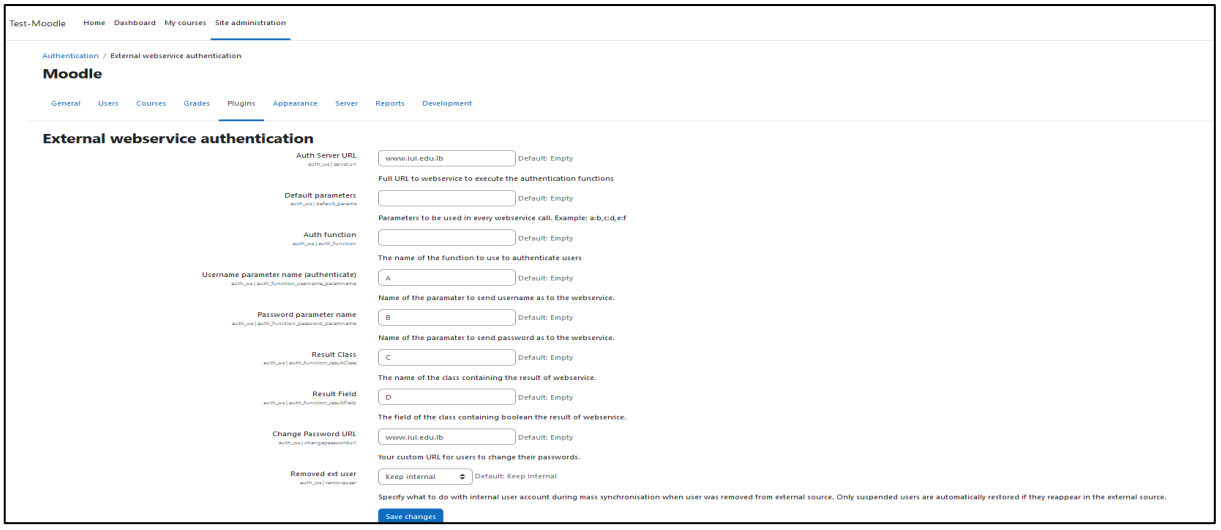

FIG. 22. CONNECTION MOODLE WITH EXTERNAL WEB SERVICE AUTHENTICATION

development>>Debagging>>display debagging message

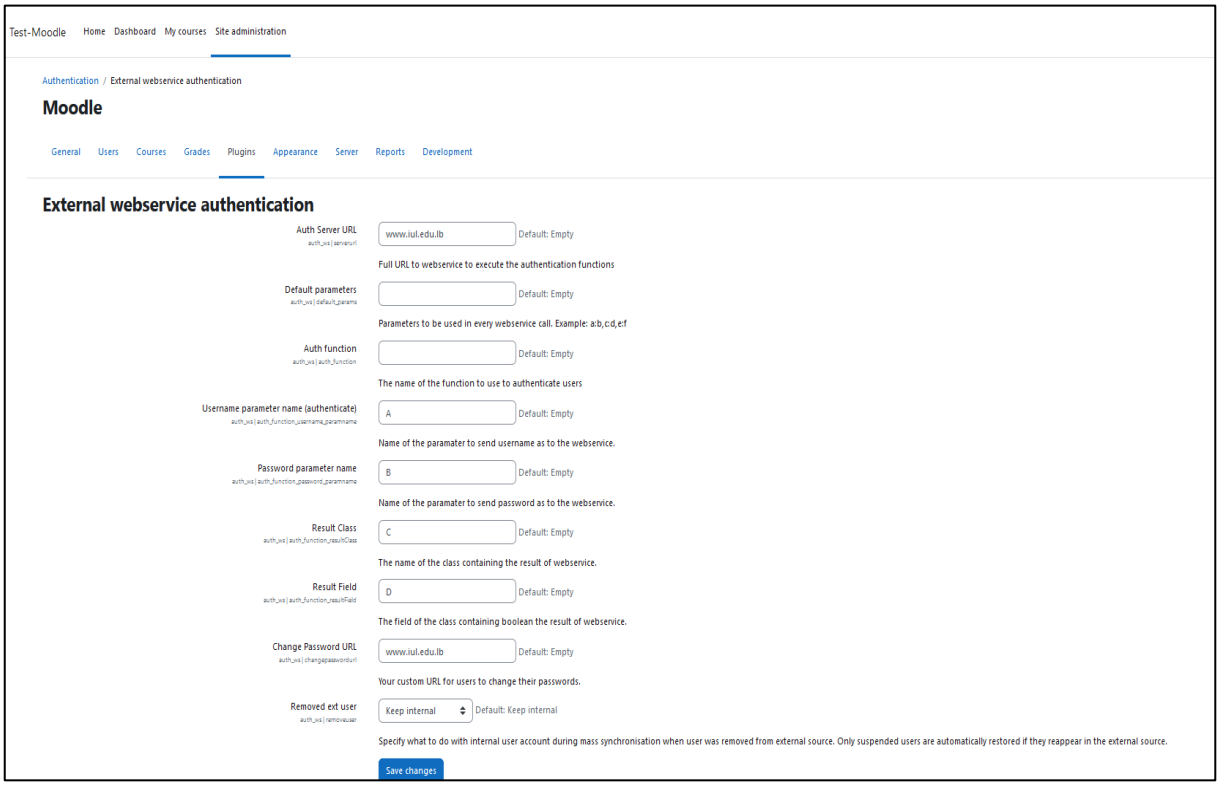

FIG. 23. ENABLE DEBAGGING ON MOODLE

To make debagging on any user that is going login to see the session request from the webserver to the authentication server and the response from the authentication server.

TABLE II: USING AUTHENTICATION

Aspect	Using Authentication	Not Using Authentication
User Identification	Users are uniquely identified by their username	No individual user identification
Access Control	Only authenticated users with valid credentials can access protected resources	No access control, anyone can access resources
Security	Provides an additional layer of security by requiring authentication	No authentication means lower security
Confidentiality	User data and sensitive information can be protected from unauthorized access	No protection for user data and sensitive information
Accountability	User actions can be traced back to specific individuals	Difficult to track user actions
User Management	Allows for user management, including user creation, deletion, and password resets	No user management capabilities
Personalization and Customization	Users can have personalized settings and preferences	No personalized settings or preferences
Compliance	Enables compliance with regulatory requirements by implementing access controls	Non-compliant with certain regulatory requirements
Authorization	Different levels of access can be granted to different users based on their roles and permissions	No role-based access control or fine-grained authorization
Auditability	Provides an audit trail of user activities for accountability and investigation purposes	No audit trail, making it difficult to investigate incidents
User Experience	Users can have their own profiles and settings for a personalized experience	Limited user experience customization

TABLE III: NOT USING AUTHENTICATION

Aspect	Connecting Moodle with Azure	Connecting Moodle without Azure
Hosting	Moodle can be hosted on Azure cloud	Moodle can be hosted on any server
Scalability	Azure provides scalable infrastructure	Scalability depends on server setup
Performance	Azure offers high-performance computing	Performance depends on server setup
Availability	Azure provides high-availability options	Availability depends on server setup
Cost	Azure hosting may incur additional costs	Cost depends on server configuration
Integration with Azure services	Can leverage Azure services and features	Limited integration capabilities
Security and Compliance	Azure offers robust security and compliance features	Security depends on server setup
Backup and Disaster Recovery	Azure provides backup and recovery options	Backup options depend on the server setup
Maintenance and Updates	Azure manages infrastructure maintenance and updates	Manual maintenance and updates required
Monitoring and Analytics	Azure offers built-in monitoring and analytics tools	Monitoring tools depend on server setup
Collaboration and Integration	Azure allows integration with other Azure services and tools	Limited collaboration options
Data Storage and Management	Azure provides scalable and secure data storage options	Data storage options depend on server setup
Security and Compliance	Azure offers robust security and compliance features	Security depends on server setup

12.12 Solutions That Suggesting in The Thesis

Recommendations for Enhancing Security in the Moodle Platform

- Implement Microsoft Azure: Use the Microsoft Azure cloud computing platform to enhance enterprise-wide security. Azure provides security policies, controls, and load balancing capabilities to protect the system from internal and external threats, as well as improve system responsiveness, maintenance, and data recovery.
- Implement user-level security policies: Enforce security policies to protect sensitive information, such as encrypting the home page to prevent attacks like DDoS, using strong passwords, and implementing multi-factor authentication to enhance security.

3. Use a VPN (L2TP/IPsec Pre-Shared Key): Implement VPN technology using L2TP/IPsec with a pre-shared key to ensure a secure connection between users and the Moodle platform.

- Moodle, ensuring only authorized users access private IP addresses.

13. CONCLUSION

The security of the Learning Management System (LMS) at the Lebanese Islamic University has been enhanced by integrating security policies into a single framework to prevent attacks and fraud, especially during exams. Security against cyber-attacks and natural disasters has also been enhanced using Microsoft Azure, which provides additional protection and facilitates maintenance and data recovery. Protecting applications from attacks is not an easy task, but it is

essential to ensure the success of the application and the security of information within the platform. It is essential for developers to understand the attack methods used by hackers and implement effective security policies such as multi-factor authentication and data encryption. On the other hand, students are recommended to develop security skills using effective solutions such as Microsoft and Cloud flare, which provide strong encryption and compliance with international security standards. Penetration tests should be used periodically to detect vulnerabilities to enhance security and protect sensitive data. It is proposed to implement international standards to ensure the security of the Moodle platform by integrating the LMS with multi-factor authentication into a single framework. Moving the application to the cloud, using email or biometric authentication, encrypting online data using SSL/TLS in a strict mode, and enforcing a strict password policy for users to enforce a specific IP address for login. Through these measures, the security of the platform can be ensured and user data can be better protected, contributing to the success of the platform and increasing user confidence in it.

Conflicts of Interest

Author declare no conflicts of interest.

Funding

Author, declare they have received no funding for this paper.

Acknowledgment

Non.

References

[1] S.-K. Chang, E. Jungert, T. Ichikawa, and P. K. Chan, "Macro University: A framework for a federation of virtual universities," Int. J. Comput. Process. Oriental Lang., vol. 13, no. 3, pp. 205–221, 2000.

[2] American Journal of Distance Education. [Online]. Available: http://www.ed.psu.edu/ACSDE/ajde/jour.asp

[3] EDUCOM Networking and Telecommunications Task Force, "A national higher education network: Issues and opportunities," NTTF Paper Number One. Princeton, NJ: EDUCOM, May 1987.

[4] The American Society for Engineering Education's Continuing Education and Distance Learning Catalog. [Online]. Available: http://www.learnon.org

[5] The International Journal of Distance Education Technologies. [Online]. Available: http://www.idea-group.com

[6] S. G. Schär and H. Krueger, "Using new learning technologies with multimedia," IEEE Multimedia, vol. 7, no. 3, pp. 40–51, 2000.

[7] [Online]. Available: https://ijrcs.org/wp-content/uploads/IJRCS202005022.pdf

[8] [Online]. Available: https://tech.hindustantimes.com/tech/news/zoom-vs-google-meet-vs-microsoft-teams-which-video-conferencing-app-to-for-story-wnBch1dX58MAC66uCVln3N.html

[9] CGI Security, "The cross-site scripting FAQ." [Online]. Available: [URL]

[10] OWASP - Open Web Application Security Project, "Top Ten Project." [Online]. Available: [URL]

[11] Mozilla Foundation, "Public Suffix List." [Online]. Available: [URL]

[12] Check Point, Firewall-1, version 3.0 White Paper, Jun. 1997. [Online]. Available: http://www.checkpoint.com/products/whitepapers/wp30.pdf

[13] A. Voronkov, "Usability of firewall configuration: Making the life of system administrators easier," Ph.D. dissertation, 2020.