iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VI **Month of publication:** June 2024

DOI: https://doi.org/10.22214/ijraset.2024.63374

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

Review of Security Practices for Cloud Based Online Learning Platform

Shankar Sharan Tripathi[1], Vijaya Chaturvedi[2], Jitendra Kumar Singh[3], Abhinav Patel[4], Aman Parganiha[5], Anurag Pandey[6]
[1, 2, 3, 4, 5, 6]*Department of Computer Science & Engineering, Shri Shankaracharya Technical Campus, Bhilai (C.G.), India*

Abstract: ***Education is the basic need of human beings. It basically equips them with the knowledge to analyze, understand and build new things. With the boom of affordable internet students can easily connect with teachers from even different continents to learn. Online learning platforms break down geographical barriers. Learners can access high-quality content from anywhere and anytime, regardless of their location. This is particularly impactful for those in remote areas or with limited access to traditional educational institutions. The cloud-based architecture ensures scalability and accessibility, allowing students to learn from anywhere with an internet connection. Prior to cloud, upfront investment was to be made to deploy a learning platform. With the cloud technology's pay as per usage the cost has been significantly reduced. The Online Learning platform empowers educators to craft adaptive courses and foster collaborative learning experiences for their students. The objective of this research paper is to conduct a comprehensive review of the security practices of cloud-based Learning Management Systems (LMS) with a focus on understanding best security measures identifying common vulnerabilities and threats, and proposing effective strategies for mitigating risks and enhancing the overall security of these systems.***
Keywords: Cloud based Learning Platform, Security Measures, Cloud Security.

I. INTRODUCTION

The advent of the internet and digital technologies has transformed the traditional methods of learning and paved the way for digitized education. The digitization of education has brought numerous benefits, making learning more accessible, interactive, and personalized.

The digital era has facilitated the development of online learning platforms, virtual classrooms, and learning management systems (LMS). These digital tools have enabled students to access educational resources and materials from anywhere in the world, breaking down geographical barriers.

It has also empowered the teacher by providing centralized content planning and LMS platforms allow teachers to organize and deliver course materials, such as lecture notes, presentations, videos, and multimedia resources, in a structured and accessible manner. Students can easily access these resources from anywhere, at any time, fostering self-paced learning and enabling better preparation and revision.

The platform empowers educators with a comprehensive admin role. This role allows them to create, manage, and update their course content, ensuring complete control over their learning materials. Educators can manage their students (e.g., enrolling students, tracking progress, providing feedback), while administrators retain overall platform control, fostering a secure and well-organized learning environment.

There are some security challenges that need to be kept in mind when developing such a learning platform. Some of the major challenges are Data Privacy, Content Security, Authentication and Authorization, Inter process communication, Access controls, Data loss.

The initial layer of protection involves integrating a strong Authentication mechanism for verifying the identity. With authentication, Authorization should be implemented to control and verify access privileges. A robust role-based access control system ensures clear segregation of duties.

By implementing some security measures, the platform fosters a secure learning environment for educators and students, building trust and protecting valuable educational content. It also leverages the power of cloud computing for seamless content delivery. This ensures exceptional scalability, allowing us to readily accommodate a growing user base without compromising performance. Furthermore, the platform employs Docker containers, a cutting-edge containerization technology, to isolate and package our application. This enhances security by creating a secure environment for each course, safeguarding both content and user data.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

Cloud-based technologies have revolutionized Online Learning Applications by offering a multitude of advantages. This approach eliminates the need for local software installations, allowing educators and students to access the platform from anywhere with an internet connection. Also the security is enhanced as data is stored in secure cloud servers, often backed by robust disaster recovery plans. Cloud-based applications also empower collaboration, as educators can readily share and update course materials, fostering a dynamic learning environment.

II. RELATED WORKS

Cloud-based learning management systems (LMS) have emerged as a transformative technology in the education domain, offering numerous advantages such as increased accessibility, scalability, and cost-effectiveness. However, the migration of sensitive educational data and resources to the cloud has also raised significant security concerns that must be addressed through robust architectural designs and security controls.

[3] Discusses the impact of cloud computing on e-learning platforms as it reduces the need for maintaining infrastructure and cloud technologies enables dynamic scalability and efficient use of resources.

[4] Describes a survey related to the awareness of providers security risks and potential measures.

[5] Discusses the various security issues, different types of attacks, threats, challenges in cloud based learning platforms. Security at different models (IaaS, SaaS, PaaS) is discussed along with proposed solutions.

[13] Reviews the various cryptographic techniques used to secure data across the whole end-to-end cloud-based e-learning platforms. It proposes an implementation framework across an end-to-end cloud-based e-learning architecture using multi-agent software.

III. CLOUD BASED TECHNOLOGIES

Cloud-based technologies are applications, services, and tools that leverage the cloud infrastructure. These resources are not physically located on your device but are delivered on-demand over the internet. For example if one has to access electricity from a power grid, they don't need to own the power plant, just a connection to use it. In essence, cloud computing and cloud-based technologies have revolutionized how one can access and utilize computing resources.

A. There are Three Main Cloud Service Models

1) Infrastructure as a Service (IaaS)
2) Platform as a Service (PaaS)
3) Software as a Service (SaaS)

B. Benefits of Cloud-Based Technologies

1) *Scalability:* Cloud computing environments offer unparalleled scalability, enabling businesses and organizations to dynamically provision and deprovision computing resources, such as storage, processing power, and network bandwidth, in response to fluctuating demands.
2) *Accessibility:* Cloud-based applications and services can be accessed from anywhere with an internet connection, providing greater flexibility and mobility for users.
3) *Security:* Cloud service providers invest heavily in security measures to protect user data and applications.
4) *Reliability:* Replicated data storage and disaster recovery plans offered by cloud providers ensure high availability and minimize downtime.

IV. VIDEO PROCESSING

Video processing refers to a broad range of techniques used to manipulate and analyze video data. It's essentially working with video files to modify them in various ways for different purposes such as Converting video from one format, Trimming unwanted portions, arranging clips, adding transitions, and incorporating titles or effects, Compressing video data to reduce file size for storage or transmission (streaming) and Removing interlacing artifacts from videos captured with certain methods, resulting in a smoother viewing experience.

In an online Learning Platform efficiently delivering high-quality video lectures is crucial. This requires video processing techniques to optimize video content for streaming within the platform. By leveraging FFmpeg for video processing and HLS streaming, the application can deliver high-quality video lectures efficiently, enhancing the learning experience for students with smooth playback and accessibility features.

1) *FFmpeg:* FFmpeg is a powerful open-source command-line tool for processing multimedia files, including video. Within an LMS, FFmpeg can be used for various video processing tasks such as Transcoding, Resizing, Bitrates Adjustment and Embedding Subtitles or Captions.
2) *HLS Streaming:* HLS (HTTP Live Streaming) is a popular video streaming protocol widely used in online learning platforms. The major work handled by HLS Streaming are Video Segmentation, Playlist Generation and Delivery of data over HTTP.

Benefits of using FFmpeg and HLS Streaming :-

a) *Improved Video Delivery:* HLS allows for adaptive bitrate streaming. The learner's device can dynamically adjust the video bitrate based on their available internet bandwidth, ensuring smooth playback without buffering issues.
b) *Efficient Storage:* Storing segmented video files can be more efficient than storing large single video files.
c) *Flexibility:* HLS is compatible with a wide range of devices and video players, making it a versatile solution for online learning platforms.
d) *Scalability:* HLS can handle a large number of concurrent viewers efficiently.

V. SECURITY MEASURES

A. Authentication

Authentication is the process of verifying the identity of a user, or an entity trying to access a resource or system. It is a crucial security measure that ensures only authorized individuals or entities can gain access to sensitive information, applications, or services. Common authentication strategies with their common pitfalls and mitigation measures.

1) Credential-Based Authentication

Credential-based authentication is a method where users provide a combination of username or email and password to gain access to a system or application.

a) *Common Pitfalls:* Storing password in plain text format, password reuse, weak password.
b) *Mitigation Measures:* Using hashing algorithms such as Argon2 or Bcrypt. To prevent weak passwords, the platform can implement strong password policies like minimum 8 or 16 characters required along with usage of capital letters, small letters, numbers and symbols. Also implementing rate limiting would help prevent attacks such as brute force attacks.

2) Single Sign-On

Single Sign-On (SSO) is an authentication mechanism that allows users to access multiple applications or services with a single set of credentials. Instead of maintaining separate usernames and passwords for each application, SSO provides a centralized authentication system that acts as a trusted identity provider.

SSO can be provided by an organization or can even be social login such as Google.

a) *Common Pitfalls:* Token Theft, Session Management, Man-in-the-Middle Attacks
b) *Mitigation Measures:* Using secure protocols for token generation, transmission, and validation (e.g. OAuth, SAML, OpenID Connect). For google sign-on use of code verifier and Proof Key for Code Exchange (PKCE) functionality.

3) Multi Factor Authentication

Multifactor authentication is an authentication strategy that involves using two or more than two forms of credentials to verify the identity.

Authentication factors can be broadly divided into 3 types: Knowledge (something you know), Possession (something you have), Inference (something you are).

In multifactor knowledge along with possession or inference factor is combined to increase the security.

Most basic form of Multi-Factor authentication is the use of Time based One Time OTP (TOTP) applications like Microsoft Authenticator. In this the user scans the QR code which contains a unique secret key and the authenticator app saves the detail.

The basic url form of TOTP is

otpauth://totp/[Issuer]:[Account]?secret=[SecretKey]&issuer=[Issuer]

Best Practices: Generate strong cryptographically secure random secrets unique for each user, store secrets in encrypted format.

4) Authentication Persistence

Authentication Persistence refers to the mechanisms used to maintain a user's authenticated state across multiple requests or sessions in a web application or system. It is a crucial aspect of user experience and security in cloud-based learning platforms, as it allows users to access resources seamlessly without having to re-authenticate for every request.

However, if not implemented correctly, authentication persistence can introduce security vulnerabilities and expose the platform to potential attacks.

a) *Common Pitfalls:* Insecure Storage of Authentication Tokens, Weak Token Generation and Management, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF)

b) *Mitigation Strategies:* Store authentication tokens securely, either in encrypted form or using secure storage mechanisms like HTTP-only cookies or web storage with appropriate security headers.

Use cryptographically secure random number generators and strong encryption algorithms (e.g., AES, SHA-256) for generating authentication tokens.

Implement anti-CSRF tokens (e.g., synchronizer token pattern) to protect against CSRF attacks. Use the SameSite attribute for session cookies to mitigate cross-site request risks.

Implement input validation at both client and server side and prevent XSS vulnerabilities.

Use of Content Security Policy (CSP) headers to restrict the execution of untrusted scripts in web pages.

B. Authorization

Authorization is the process of determining whether the authenticated user has the access to resources or if they can perform certain actions. Authorization is enforced after the authentication is successful.

Authorization models and mechanisms can vary depending on the system's requirements and complexity. Some standard authorization models include:

1) *Role-Based Access Control (RBAC):* Users are assigned roles (e.g., student, instructor, administrator), and permissions are granted based on those roles. This model simplifies access management by grouping users with similar responsibilities and access requirements.

2) *Attribute-Based Access Control (ABAC):* Access decisions are based on attributes associated with the user (e.g., department, location, enrollment status) and the resource (e.g., course level, subject area). ABAC allows for more granular and dynamic access control.

3) *Discretionary Access Control (DAC):* Resource owners (e.g., instructors) have the ability to grant or revoke access to their resources (e.g., course materials) for specific users or groups.

4) *Mandatory Access Control (MAC):* Access rules are centrally defined and enforced by the system based on predefined security policies and classifications of data and users.

Basic model for implementing role based access control:

The database model for implementing role-based access control (RBAC) typically consists of three main tables: Users, Roles, and Permissions (or RolePermissions). Here's an example of how the database model might look like:

i. Users Table:
- UserID (Primary Key)
- Username
- Password
- Email
- RoleID (Foreign Key referencing the Roles table)

ii. Roles Table:
- RoleID (Primary Key)
- RoleName
- Description

iii. Permissions Table:
- PermissionID (Primary Key)

- PermissionName
- PermissionDescription

iv. RolePermissions Table:
- RoleID (Foreign Key referencing the Roles table)
- PermissionID (Foreign Key referencing the Permissions table)
- GrantedAt

The relationships between the tables would look like:
- A User belongs to one Role.
- A Role can have multiple Users assigned to it.
- A Role can have multiple Permissions granted to it (many-to-many relationship).
- A Permission can be granted to multiple Roles (many-to-many relationship).

When a user attempts to perform an action in the application, the system would check the user's assigned role, retrieve the permissions associated with that role from the RolePermissions table, and determine if the requested action is permitted based on the role's permissions.

C. Use of secure protocols

Secure Protocols establish a set of rules and encryption methods to ensure data privacy, integrity, and authenticity during transmission. Secure protocols are specific technical solutions that implement encryption and other security measures across different layers during communication.

1) Securing Network Connections

a) HTTPS (Hypertext Transfer Protocol Secure): HTTPS operates at the Application Layer, it is the secure version of HTTP, the protocol underlying web browsing. HTTPS encrypts communication between the web browser and the website user visits. For example, when students access the learning platform, HTTPS ensures a secure connection between their device and the platform's servers. This encrypts all data exchanged, including login credentials, course materials, and student progress data, protecting it from eavesdropping or tampering.

b) SSH (Secure Shell): SSH is a secure protocol used for remote login to server machines. It encrypts both data and user authentication, ensuring secure access and preventing unauthorized login attempts. SSH is crucial for system administrators and developers managing servers remotely. This is useful when the system administrator or the developer is trying to access the cloud platform for managing resources.

c) TLS/SSL (Transport Layer Security/Secure Sockets Layer): TLS/SSL secures communication between applications on a network. It primarily operates at the Transport Layer, encrypting data streams between applications like web browsers and web servers (HTTPS).

For best security practices the latest version of TLS must be used. (Currently it is TLS 1.3)

Cipher suites are combinations of cryptographic algorithms used for key exchange, encryption, and message authentication during an SSL/TLS session. When processing payments, it is essential to use strong and secure cipher suites that provide adequate protection for sensitive financial data

It is crucial to use SSL/TLS certificates issued by trusted Certificate Authorities (CAs). These CAs are responsible for validating the identity of the website or server and issuing digital certificates.

Trusted CAs include well-known organizations like Comodo, DigiCert, GlobalSign, which are trusted by major browsers and operating systems.

Proper certificate validation should be implemented to ensure that the server's certificate is valid, not expired, and issued by a trusted CA. This helps prevent man-in-the-middle attacks and ensures secure communication with the intended server.

2) Securing Data at Rest

a) Disk Encryption: Full-disk encryption tools use secure protocols to encrypt your entire hard drive or specific storage volumes. This renders your data unreadable in case of physical theft or unauthorized access to your device.

b) File Encryption: Software applications often allow you to encrypt individual files or folders using secure protocols. This protects sensitive data even if someone gains access to your storage device.

3) Secure Authentication

a) *Secure Hash Algorithms (SHA):* These are cryptographic hash functions used to verify the integrity of data. SHA algorithms generate a unique "fingerprint" for a file. If the file is altered in any way, the fingerprint will change, allowing verification of file integrity during downloads or data transfers.

b) *Digital Signatures:* Digital signatures use secure protocols like public-key cryptography to electronically sign documents. This ensures the authenticity of the signer and prevents document tampering. Digital signatures are widely used in secure document management and electronic transactions.

D. Video DRM

Video Digital Rights Management (DRM) is a set of technologies and techniques used to protect and control the distribution and consumption of digital video content in cloud-based learning platforms. Video DRM aims to prevent unauthorized access, copying, and redistribution of protected video content.

Video DRM systems allow content providers to define and enforce various usage policies and restrictions. These policies are typically specified in the licenses or rights objects issued to authorized users.

1) Some Common usage Policies Include

a) *Limiting The Number Of Concurrent Playbacks Or Devices:* Restricting the number of simultaneous streams or devices that can access the content at the same time.

b) *Preventing Screen Recording Or Capturing:* Disabling the ability to record or capture the video content during playback.

c) *setting expiration dates or playback windows:* Defining a time period during which the content can be accessed or limiting the total number of playbacks.

2) Watermarking and Forensic Tracking

Digital watermarking techniques can be employed to embed unique identifiers or metadata into the video content itself. These watermarks are typically imperceptible to viewers but can be detected and extracted for forensic purposes.

If a watermarked video is found in an unauthorized distribution channel, the watermark can be used to trace the source of the leak and identify the user or device from which the content originated. This forensic tracking capability acts as a deterrent against unauthorized sharing or piracy.

E. Denial of Service

Denial of Service (DoS) attacks are a significant security concern for cloud-based learning platforms. These attacks aim to disrupt or make services unavailable to legitimate users by overwhelming the system's resources or exploiting vulnerabilities.

DoS attacks involve flooding the target system, application, or network with an overwhelming amount of traffic or requests, rendering it unable to respond to legitimate requests. The goal is to exhaust the system's resources, such as bandwidth, computing power, or memory, causing it to become unresponsive or crash.

DoS attacks can be launched from a single source (single-source attack) or from multiple distributed sources (Distributed Denial of Service, or DDoS, attack).

1) Impact on cloud-based learning platforms

Disruption of online classes, lectures, or live streaming sessions, affecting students' ability to attend and learn.

Denial of access to learning management systems (LMS), course materials, assignments, or assessments.

Degradation or unavailability of collaboration tools, communication channels, or discussion forums.

Potential loss of data or interruption of critical processes, such as grading or student registration.

2) Mitigating DoS Attacks

Implementing network-level protection mechanisms, such as firewalls, intrusion detection/prevention systems (IDS/IPS), and web application firewalls (WAFs). The free option is Cloudflare.

Cloudflare offers robust DDoS mitigation services that can effectively protect cloud-based learning platforms against various types of DoS and DDoS attacks. Their globally distributed network can absorb and filter out malicious traffic, preventing it from reaching the platform's origin servers.

Cloudflare's WAF can detect and block application-layer attacks, such as SQL injection, cross-site scripting (XSS), and other common web application vulnerabilities. This helps protect the learning platform's web applications and APIs from being exploited or used as entry points for DoS attacks.

Cloudflare's rate limiting capabilities can help mitigate volumetric DoS attacks by enforcing limits on the number of requests or connections from a single IP address or a group of IP addresses. This can prevent legitimate users from being overwhelmed by excessive traffic during an attack.

F. Infrastructure Security

Infrastructure security refers to the practices, controls, and measures implemented to protect the underlying infrastructure components that support and deliver cloud-based applications and services, such as a learning management system (LMS).

It encompasses various aspects, including physical security, network security, server hardening, and virtualization security, among others. Ensuring robust infrastructure security is crucial for maintaining the confidentiality, integrity, and availability of the LMS and the sensitive data it handles.

a) Network Security: Network segmentation: The process of network segmentation involves the division of a network into distinct zones or segments. (e.g., DMZ, internal networks, management networks) and implementing appropriate access controls and firewalls between them.

b) Firewall and Intrusion Prevention: Deploying firewalls and intrusion prevention systems (IPS) to monitor and control inbound and outbound network traffic, blocking unauthorized access attempts and potential threats.

c) Secure Network Protocols: Implementing secure network protocols (e.g., SSH, HTTPS, VPNs) for remote administration and data transfer, ensuring encryption and integrity.

d) Network Monitoring and Logging: Continuously monitoring network traffic and logging events for security analysis and incident response.

1) Server and Operating System Security:

a) Hardening: Configuring servers and operating systems according to security best practices, removing unnecessary services, applying the principle of least privilege, and enabling security features (e.g., secure boot, disk encryption).

b) Patching and Updates: Implement security patches released by OS and updates to address known vulnerabilities in operating systems, applications, and software components.

c) Secure Configuration Management: Implementing secure configuration management processes to ensure consistent and secure server configurations across the infrastructure.

d) Secure Remote Access: Enabling secure remote access methods (e.g., SSH, VPNs) for administrative purposes and enforcing strong authentication and access controls.

2) Virtualization and Container Security:

a) Hypervisor Security: Securing the hypervisor layer (e.g., VMware ESXi, Microsoft Hyper-V) through hardening, patching, and access controls.

b) Virtual Machine (VM) and Container Isolation: Ensuring proper isolation and separation of VMs and containers to prevent unauthorized access or resource contention.

c) VM and Container Lifecycle Management: Implementing secure processes for deploying, migrating, and decommissioning VMs and containers, including secure image management and patching.

3) Storage Security

a) Data Encryption: Encrypting data to protect against unauthorized access and data breaches.

b) Access Controls: Implementing role-based access controls and least privilege principles for storage systems and data repositories.

c) Backup and Disaster Recovery: Establishing secure backup and disaster recovery processes to ensure data availability and business continuity in case of incidents or failures.

4) Identity and Access Management (IAM)

a) User Authentication and Authorization: Implementing strong authentication mechanisms (e.g., multi-factor authentication, single sign-on) and granular role-based access controls for users accessing the learning platform and infrastructure components.

b) Privileged Access Management: Strictly controlling and monitoring privileged access to critical infrastructure components, following the principle of least privilege.

c) Auditing and Logging: Maintaining comprehensive audit trails and logs for user activities, access attempts, and administrative actions for security analysis and compliance purposes.

5) Security Monitoring and Incident Response

Security information and event management (SIEM): Deployment of SIEM solutions to centralize and analyze security logs, detect potential threats, and facilitate incident response.

a) Vulnerability Management: Regularly scanning and assessing the infrastructure for vulnerabilities, prioritizing and addressing identified risks.

b) Incident Response Planning: Developing and testing incident response plans to effectively detect, contain, and recover from security incidents affecting the infrastructure.

G. Insider's Threat

Insider threats mainly originate from within the organization, by authorized users who have legitimate access to the platform and potentially sensitive data. An authorized user with access to system administration tools could disrupt platform operations by deleting data, altering configurations, or launching denial-of-service attacks. An insider could download or export student data (names, contact information, grades) and sell it on the black market or use it for identity theft.

By implementing secure login processes, user activity monitoring with a focus on privacy, and robust security measures, the platform can create a trusted learning environment that fosters student engagement, improves educational outcomes, and protects sensitive user data within your cloud-based online learning platform.

The platform offers secure login methods beyond simple usernames and passwords. This can include Multi-factor Authentication, Social Logins etc.

Monitoring user login logs and activities in Online Learning Platform can be a valuable tool for security purposes and improving the learning experience. However, it's crucial to strike a balance between comprehensive monitoring and user privacy.

1) Login Logs: Capture essential details like username, timestamp, IP address, and successful/failed login attempts. This helps identify suspicious activity like brute-force attacks or unauthorized access attempts.

2) User Activity: Track actions related to learning activities, including -

a) Course access and completion

b) Time spent on modules and materials

c) Downloads of learning materials

d) Participation in forums and discussions

e) Performance in quizzes and assignments.

VI. CONCLUSION

"Review of Security Practices for Cloud Based Learning Platform"

The cloud-based online learning platform offers a dynamic and secure solution for the modern educational landscape. With its commitment to data security, user privacy, and accessibility, this cloud-based Online learning application empowers educators to easily create and deliver engaging learning content, manage student progress, and foster collaboration in a virtual classroom environment and students to access high-quality learning materials anytime, anywhere, on a variety of devices, and personalize their learning experience at their own pace.

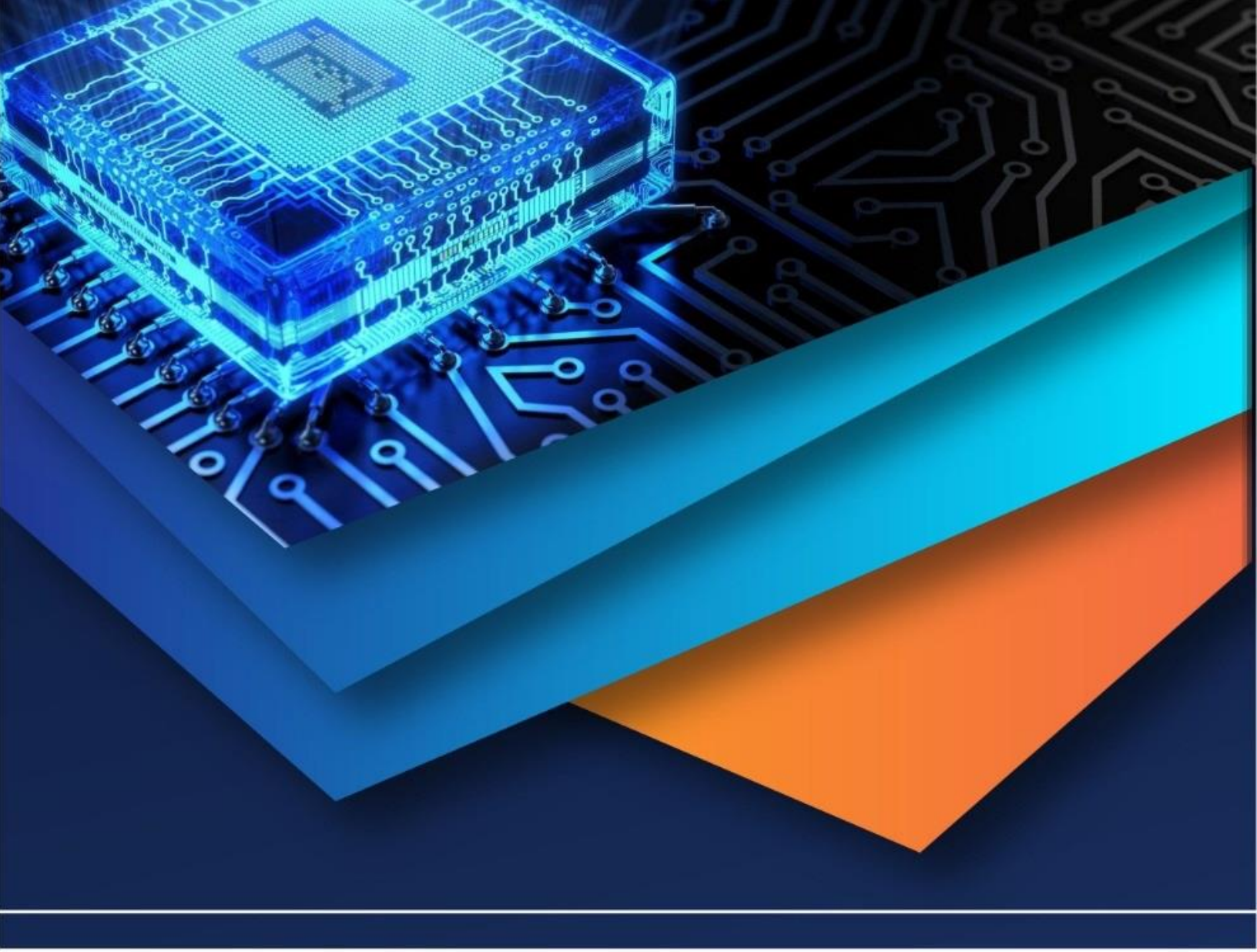
REFERENCES

[1] Hassan Faisal Aldheleai, Mohammad Ubaidullah Bokhari, Abdulsalam Alammari - "Overview of Cloud-based Learning Management System", International Journal of Computer Applications (0975 – 8887) Volume 162 – No 11, March 2017.

[2] Paramita Chatterjee, Rajesh Bose and Sandip Roy - "A Review on Architecture of Secured Cloud Based Learning Management System", Journal of Xidian University, Volume 14, 2020.

[3] Prof Smita Parte , "Impact of Cloud Computing in E-Learning", International Journal of Innovative Science, Engineering & Technology, Volume 4. Available at www.ijiset.com, 2017.

[4] Chen, Y. & He, W. - "Security Risks and Protection in Online Learning: A Survey", International Review of Research in Open and Distributed Learning, Volume 14, 2013.
[5] M. Durairaj, A. Manimaran - "A Study on Security Issues in Cloud Based E-Learning", Indian Journal of Science and Technology, Volume 8, April 2015.
[6] Edeh Michael Onyema; Nwafor Chika Eucheria; Ugwugbo Ann Nneka; Rockson Kwasi Afriyie; Ogbonnaya Uchenna Nwoye - "CLOUD SECURITY CHALLENGES: IMPLICATION ON EDUCATION", International Journal of Computer Science and Mobile Computing(IJCSMC), Volume 9, Issue. 2, February 2020.
[7] Syam Kumar P, Subramanian R - "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.
[8] Gunasekar Kumar, Anirudh Chelikani - "ANALYSIS OF SECURITY ISSUES IN CLOUD BASED E-LEARNING", University of Boras, School of Business and IT.
[9] Olugbenga W. Adejo, Isaiah Ewuzie, Abel Usoro and Thomas Connolly - "E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastructure", I.J. Information Technology and Computer Science, April 2018.
[10] Rahman, A., Sarfraz, S., Shoaib, U., Abbas, G., & Sattar, M. A. (2016) - "Cloud based E-Learning, Security Threats and Security Measures". Indian Journal of Science and Technology, 9(48).
[11] Yassen AbdelKhaleq Najm, Suray Alsamaraee, Ahmed Adeeb Jalal - "Cloud computing security for e-learning during COVID-19 pandemic", Indonesian Journal of Electrical Engineering and Computer Science Vol. 27, No. 3, September 2022, pp. 1610~1618.
[12] Sajjad Hashemi, Seyyed Yasser Hashemi - "Cloud Computing for E-Learning with More Emphasis on Security Issues", International Journal of Computer, Control, Quantum and Information Engineering Vol:7, No:9, pp. 607-612, 2013.
[13] Lavanya-Nehan Degambur, Sheeba Armoogum, Sameerchand Pudaruth - "A Study of Security Impacts and Cryptographic Techniques in Cloud-based e-Learning Technologies", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 13, No. 1, pp. 58-66, 2022.
[14] Paramita Chatterjee, Rajesh Bose, Subhasish Banerjee, Sandip Roy - "Enhancing Security of Cloud based LMS by deploying secure Loopback Protocol", International Journal of Mechanical Engineering, Vol. 7 No. 1, pp. 1474-1481, January, 2022.
[15] Momeen Khan, Tallat Naz, Mohammad Awad Hamad Medani - "A Multi-Layered Security Model for Learning Management System", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 12, pp. 207-211, 2019.
[16] Prof. Poonam R.Maskare, Prof. Sarika R.Sulke - "Review Paper on E-learning Using Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 1281-1287.
[17] Ali, Radwan and Zafar, Humayun - "A Security and Privacy Framework for e-Learning" (2017). Faculty and Research Publications. 4137.
[18] Navneet, S.P and Rekha, B.S. (2014).Software as a Service (SaaS): Security issues and Solutions. International Journal of Computational Engineering Research, 4 (6), 68-71.
[19] DDOS Attacks
https://www.cloudflare.com/en-in/learning/ddos/what-is-a-ddos-attack/ (Accessed on 29/03/2024).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY