Logfile-Driven Risk Assessment of Security Threats in LMSs Using Fuzzy Logic

MOE MOE SAN[1], KHIN MAY WIN[2]
[1] Faculty of Computer Science, University of Computer Studies (Pathein), Myanmar
[2] Faculty of Information Science, Technological University (Taunggyi), Myanmar

Abstract- The rapid expansion of online Learning Management Systems (LMS) has heightened the need for robust security mechanisms to mitigate various risks. This paper presents a fuzzy logic-based framework for assessing security threats in online LMS environments, utilizing logfile data as input. The system extracts logfiles from the LMS server, preprocesses them into a structured CSV format, and identifies key risk factors, such as login failure attempts, suspicious IP addresses, brute force attacks, and unauthorized access attempts. These risk factors are then quantified to serve as crisp input values for a fuzzy inference system (FIS). The core of the proposed approach involves fuzzification of the identified risk factors, applying a set of 20 predefined fuzzy rules based on security principles. These rules are employed within a rule-based fuzzy method to classify the severity of risks. The system defuzzifies the output to generate a final risk assessment categorized into four levels: low, medium, high, and critical. This real-time risk classification enables administrators to quickly identify and respond to security threats in a proactive manner.

Indexed Terms- Fuzzy Logic, Risk Assessment, Security, Learning Management System

I. INTRODUCTION

The increasing reliance on Learning Management Systems (LMSs) in educational institutions has brought significant advancements in online education, offering seamless learning environments for students and educators. However, as LMS platforms manage vast amounts of sensitive user data, they have become prime targets for cybersecurity threats. These threats, such as unauthorized access attempts, data exfiltration, malware attacks, and suspicious login activities, can compromise not only data confidentiality but also the overall integrity and availability of educational services.

Every educational institution in the world is creating an LMS that is easy to use or providing various online learning options. As a result, online learning management systems are the focus of new technology used by all academic service providers (Paramita Chatterjee..2023). There is some risk associated with LMS technologies. Numerous vulnerabilities exist in LMS, including those related to availability, confidentiality, and integrity (Preecha Pangsuban..2015). In LMS environments, such as Moodle, security threats can manifest in various forms, including unauthorized access attempts, brute force attacks, unusual login patterns, and network intrusion attempts. Identifying and mitigating these risks requires a robust framework capable of analyzing vast amounts of log data generated by the LMS and its underlying infrastructure.

Traditional risk assessment methods often struggle to adapt to the dynamic and evolving nature of cyber threats. Static models rely heavily on fixed thresholds and predefined conditions, which may not capture the nuances of real-time security risks. To address these limitations, this study introduces a fuzzy logic-based approach for security risk assessment tailored specifically for LMS environments. By leveraging logfile data from LMS servers, this approach provides a more adaptable and interpretable method for classifying risk levels as low, medium, high, or critical.

The proposed method processes security-related data such as unauthorized access attempts, multiple failed logins, and suspicious IP activities, transforming them into fuzzy inputs. Through the application of fuzzy inference rules and defuzzification techniques, the model evaluates risk scores and categorizes threats effectively. This dynamic approach not only accommodates incomplete or ambiguous data but also adapts to varying security contexts within LMS platforms.

This paper highlights the advantages of using fuzzy logic for risk assessment in LMSs by demonstrating its ability to provide nuanced security evaluations. This system emphasizes its effectiveness in managing security threats in real-time, ensuring the confidentiality, integrity, and availability of LMS platforms.

II. LITERATURE REVIEW

Security risk assessment is critical in safeguarding Learning Management Systems (LMS) and cloud-based environments due to their increased adoption and vulnerability to cyber threats. Various methodologies and models have been proposed to address these challenges, ranging from statistical frameworks to fuzzy logic-based approaches.

Nada et al. (2017) provided a comprehensive survey of risk assessment models for cloud computing, outlining evaluation criteria that emphasize scalability, adaptability, and real-time threat detection. Similarly, Khogali and Ammar (2018) presented a methodological approach to assess security risks in cloud computing, offering insights into risk prioritization and mitigation strategies tailored for academic environments.

In the context of LMS, Maniah et al. (2019) proposed a framework for assessing security risks using statistical techniques to analyze threats in educational settings. Their approach identifies vulnerabilities based on cloud computing principles, addressing risks specific to e-learning systems. Jouini and Rabai (2017) extended the discussion by introducing a risk management model for Infrastructure as a Service (IaaS), highlighting its applicability in cloud environments and its potential adaptation for LMS.

The integration of fuzzy logic into risk assessment is exemplified by Liu and Guo (2016), who utilize fuzzy entropy weight models for cloud security, enabling nuanced evaluations of ambiguous or uncertain data. Amini et al. (2018) further develop fuzzy logic-based methodologies to evaluate and prioritize risks, showcasing their flexibility in adapting to dynamic security landscapes. Sivasubramanian et al. (2017) focus on statistical models for cloud computing risk assessment, providing a comparative analysis of traditional and fuzzy logic methods.

Pangsuban et al. (2015) analysed risk assessment for Moodle LMS using log files, demonstrating the significance of real-time data collection and preprocessing in identifying security anomalies. Malele (2023) emphasized the importance of cybersecurity in cloud-based online learning environments, highlighting the need for robust assessment frameworks to protect sensitive data and maintain institutional credibility.

Recent advancements include hybrid models combining statistical methods with fuzzy logic, as presented by Latif et al. (2013) and Soleymani et al. (2021). These approaches enhance the precision of risk assessment by leveraging the strengths of both methodologies. Additionally, Wahlgren and Kowalski (2013) advocate for escalation approaches in IT security risk management, underscoring the need for adaptable solutions in cloud computing.

This literature review illustrates the progression from traditional statistical models to sophisticated fuzzy logic-based frameworks for risk assessment in LMS and cloud computing environments. These studies provide a foundation for developing a flexible, scalable, and adaptive risk assessment model tailored to the unique challenges of LMS security.

A. Overview of Risk Assessment in LMSs

Learning Management Systems (LMSs) are integral to modern educational environments, enabling seamless delivery of academic content and interactions between students and educators. However, their online nature and the sensitive data they handle expose them to a wide range of cybersecurity threats, including unauthorized access, malware, and data breaches [5][21]. Risk assessment in LMSs is a critical process aimed at identifying, analyzing, and mitigating these threats to ensure the integrity, confidentiality, and availability of the system. Effective risk assessment frameworks can provide educational institutions with actionable insights to safeguard their systems, enhance user trust, and maintain compliance with cybersecurity standards [4][12][18].

B. *Statistical Methods for Security Risk Assessment*

Traditional statistical methods have been widely employed in cybersecurity for risk assessment. Techniques like calculating mean and standard deviation help identify outliers, representing anomalous or potentially malicious activities [8] [15]. For example, statistical models can be used to detect excessive failed login attempts or unusually large data transfers [6] [9]. While these methods are efficient in processing large datasets and identifying trends, they often lack the ability to manage uncertainty and ambiguity inherent in real-world security data. This limitation highlights the need for complementary or alternative approaches to address the dynamic and complex nature of LMS security threats [3] [17].

C. *Fuzzy Logic in Cybersecurity*

Fuzzy logic offers a flexible and robust alternative to traditional risk assessment models by handling uncertainty and imprecision effectively. In the context of LMS security, fuzzy logic can classify security risks based on linguistic variables (e.g., "low," "medium," "high") rather than rigid numerical thresholds [10] [20]. By processing data from log files and applying well-defined fuzzy rules, the model evaluates security threats across multiple dimensions, such as unauthorized access attempts, suspicious IPs, and unusual activity patterns [7] [11] [23]. This adaptability makes fuzzy logic particularly suitable for complex and evolving security landscapes, where static thresholds may fail to capture subtle anomalies [18] [22].

D. *Limitation of Existing Approaches*

Despite their widespread adoption, existing risk assessment approaches often face significant limitations when applied to LMS environments. Some statistical methods may struggle with ambiguous or incomplete data, leading to inaccuracies in risk classification [9] [14]. Similarly, rigid rule-based systems lack the flexibility to adapt to new and emerging cyber threats, which are increasingly sophisticated [16] [19]. Furthermore, many traditional models require extensive manual intervention to adjust thresholds or parameters, making them less practical for dynamic and large-scale systems like LMSs [13] [15][23]. These limitations underscore the importance of exploring hybrid and intelligent approaches, such as fuzzy logic and machine learning, to address the unique challenges of LMS cybersecurity [1] [17] [20].

III. PROPOSED RISK ASSESSMENT ARCHITECTURE

The system architecture for the proposed risk assessment model includes interconnected components designed to, identify security risks, extract and preprocess log files from LMS server and classify the risk level using a fuzzy logic-based system. The architecture ensures adaptability to evolving threats in LMS environments through dynamic updates to rules and thresholds.

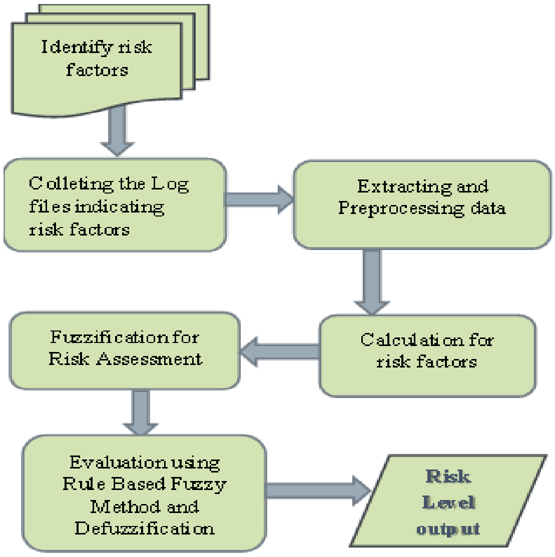
Identify risk factors
Colleting the Log files indicating risk factors
Extracting and Preprocessing data
Calculation for risk factors
Fuzzification for Risk Assessment
Evaluation using Rule Based Fuzzy Method and Defuzzification
Risk Level output

Figure 1: Proposed Risk Assessment System Architecture

A. *Identification for Security Risk Factors*

The process starts with identifying key security risk factors that affect LMS environments. The table below presents a prioritized list of risk factors, ranked from highest to lowest importance, as identified by standard organizations like the National Institute of

Standards and Technology (NIST) or cybersecurity researchers such as MANNANE Nada et al. (2017) and Ishraga Mohamed Ahmed Khogali (2018), among others.

Table 1: Prioritized List of Security Risk Factors

Rank	Risk Factor	Risk Level
1	Unauthorized Access Attempts	Extremely High
2	Data Exfiltration Activities	Very High
3	Suspicious IP Addresses	High
4	Multiple Failed Login Attempts	High
5	Malware Detection Events	High
6	User Privilege Changes	Moderate
7	Unusual Access Times or Patterns	Low

1) Unauthorized Access Attempts

Unauthorized access attempts are identified by analyzing failed login patterns. Repeated failed login attempts within a short time frame often indicate brute-force attacks or credential-stuffing activities. These attempts may come from the same or multiple user accounts and can compromise the system if left unchecked. Detecting these patterns is critical for early intervention to prevent potential breaches.

2) Multiple Failed Login Attempts

Multiple failed login attempts are a subset of unauthorized access that indicates persistent attempts to access accounts without proper authorization. This risk factor measures the frequency and patterns of such attempts from the same user or IP address over a defined period. An unusually high count of failed attempts raises the suspicion of automated hacking tools or malicious users.

3) Suspicious IP Activity

Suspicious IP activity involves monitoring access behaviors from IP addresses. This includes detecting:

- Multiple failed login attempts originating from the same IP.
- Access from blacklisted or geographically unusual IP addresses.
- Rapidly switching IP addresses for the same user.
- These behaviors suggest malicious intent, such as distributed denial-of-service (DDoS) attacks or attempts to bypass security controls.

4) Unusual Access Times or Patterns

Access during odd hours, such as late at night or outside standard working hours, is flagged as unusual access behaviors. This risk factor captures access attempts during predefined non-standard times, which may indicate unauthorized usage or malicious activity. A high frequency of access during unusual times often correlates with cyberattacks, particularly when paired with other risk indicators.

5) Data Exfiltration Activities

Data exfiltration refers to unauthorized transfers of sensitive data from the LMS. This is identified by monitoring file downloads or uploads that exceed typical data transfer thresholds. For instance, large data transfers by a user who typically accesses only minimal information might signal an insider threat or a compromised account.

6) Malware Detection Events

Malware detection tracks attempt to execute malicious scripts or upload harmful files to the LMS. These events include the detection of malware signatures or suspicious file uploads that do not conform to normal LMS usage. Such activities indicate attempts to disrupt the system or compromise its security.

7) User Privilege Changes

Unauthorized or unusual changes to user privileges, such as elevating a standard user to an administrator role without proper authorization, pose significant security risks. This risk factor involves monitoring user account modifications that may indicate insider threats or compromised accounts. Anomalies in privilege changes are flagged for immediate investigation.

B. Collecting The Log Files Indicating Risk Factors

The system collects raw log files from LMS servers, such as access logs and error logs, which contain information about user activity, system errors, and potential security threats. These logs are essential for monitoring and identifying security risks. Logs provide timestamped records of events, including IP addresses, usernames, error codes, and data transfer activities.

1) Access Logs: These logs capture details about every access request made to the LMS, such as

the timestamp, IP address, request type (GET or POST), status code (success or failure), and user agent (browser or device type). Access logs help in identifying patterns of suspicious behaviors or brute force attacks, including unusual access times, data exfiltration attempts, and repeated failed access attempts.

2) Error Logs: These logs record error events in the LMS, such as failed login attempts, invalid login tokens, or attempts to access unauthorized resources. Error logs are essential for detecting potential security threats, such as unauthorized access attempts and suspicious user activity.

C. Extracting and Preprocessing Data

Once the log files are collected, they undergo preprocessing to ensure the data is clean, structured, and suitable for analysis. Preprocessing steps include:

- Data Filtering: Removing irrelevant or incomplete entries.
- Normalization: Standardizing log file formats for uniformity.
- Feature Extraction: Identifying critical attributes, such as timestamps, IP addresses, and activity types, for risk factor calculations.

The following table represents the csv file generated after extracting and preprocessing the error log file.

Table 2 : Sample Preprocessed csv File

Timestamp	Client IP	Username	Error Messa	User Agent
2024-09-15	10.7.7.254	student 1	Invalid	Mozilla/ 5.0
2024-09-15	10.7.7.254	student 1	Invalid	Mozilla/ 5.0
2024-09-15	10.7.7.254	student 1	Invalid	Mozilla/ 5.0
2024-09-15	10.7.7.254	teacher 4	Invalid	Mozilla/ 5.0
2024-09-15	192.168.1.45	admin	Access	Mozilla/ 5.0
2024-09-16	172.16.0.5	teacher 1	Invalid	Mozilla/ 5.0
2024-09-16	172.16.0.5	teacher 1	Invalid	Mozilla/ 5.0

D. Calculation for Risk Factors

After preprocessing, the system calculates the defined risk factors. This involves:

- Grouping Data: Categorizing log entries by criteria such as username or IP address.
- Counting Incidents: Quantifying the occurrences of security-related events, such as failed login attempts or unusual access times.
- Threshold Comparison: Comparing calculated values to predefined thresholds to determine risk levels for each factor.

The following table presents the sample csv file after calculating the defied risk factors.

Table 3: Sample csv File After Calculating Each Risk Factor

Unauthorized Access Attempts	Failed Login Attempts	Suspicious IP	Data Exfiltration Activities	Malware Detection Events	User Privilege Changes
9	14	15	200	8	7
5	3	4	500	0	2
4	3	3	400	0	0
4	1	1	300	1	1
1	1	1	500	1	1
2	1	1	300	0	0
2	1	1	200	2	1

E. Fuzzification for Risk Assessment

The fuzzification process is a fundamental step in the fuzzy logic-based risk assessment framework. It transforms the crisp input values (quantified risk factors) into fuzzy values, making it possible to handle uncertainties and ambiguities inherent in risk assessment. In online Learning Management Systems (LMS), the fuzzification of risk factors provides a flexible and interpretable assessment of risks by converting numerical measures into linguistic categories such as *Low*, *Medium*, *High*, and *Critical*.
This table shows the sample input crisp value of each risk factor for fuzzification.

Table 4: Sample Input Crisp value of Each Risk Factor

Risk Factors	Crisp Input Value of Each Risk Factor
Unauthorized Access Attempts	9
Data Exfiltration Activities	200 MB
Suspicious IP Addresses	15
Multiple Failed Login Attempts	14
Malware Detection Events	8
User Privilege Changes	7
Unusual Access Times or Patterns	15

This Table displays the sample fuzzy sets of each risk factor.

Table 5: Sample Fuzzy Sets of Each Risk Factor

No	Risk Factor	Low	Medium	High	Critical
1	Unauthorized	0–10	10–20	20–30	30+
2	Suspicious IP	0–8	8–15	15–20	20+
3	Multiple Failed	0–10	10–20	20–35	35+
4	Data Exfiltra	0–150	150–400 MB	400–700	700+ MB
5	Malware	0–2	2–4	4–6	6+
6	User Privileg	0–2	2–4	4–6	6+
7	Unusual	0–15	15–25	25–40	40+

Convert the crisp values from log files into fuzzy values using triangular membership functions. For instance, for the fuzzy set Using equations as follows. For the low, high and critical use triangular membership function,

$$\mu_{Risk}(x{:}a,b,c) = \begin{cases} 0 & if\ x \leq a \\ \dfrac{x-a}{b-a} & if a < x \leq b \\ \dfrac{c-x}{c-b} & if b < x \ \leq c \\ 0 & if\ x \geq c \end{cases}$$

For the medium using trapezoidal membership function

$$\mu_{Risk}(x{:}a,b,c,d) = \begin{cases} 0 & if\ x < a\ or\ x > d \\ \dfrac{x-a}{b-a} & if a \leq x \leq b \\ 1 & if b \leq x \ \leq c \\ \dfrac{d-x}{d-c} & if c \leq x \ \leq d \end{cases}$$

Here, a ,b ,c and d are the bounds for the fuzzy set.

F. *Evaluation Using Rule-Based Fuzzy Method and Defuzzification*

In this step, a set of predefined fuzzy rules is applied to evaluate the overall risk level. The Rule-Based Fuzzy Inference System (FIS) uses a set of predefined rules to evaluate risk based on combinations of different risk factors. In this system, 20 rules have been defined to interpret the potential risk level in online Learning Management System (LMS). These rules take into account combinations of various risk factors such as Unauthorized Access Attempts, Suspicious IPs, Failed Login Attempts, Data Exfiltration, Malware Detection, User Privilege Changes, and Unusual Access Times. The fuzzy rules allow for a nuanced assessment by evaluating these factors together, leading to an overall risk level that is categorized as Low, Medium, High, or Critical.

Each rule in the FIS is structured in an "if-then" format, which is typical in fuzzy logic systems. Each rule applies a set of conditions to the fuzzy variables and then assigns a corresponding risk level. This system defined 20 rules as follows:

- Rule 1: If unauthorized access attempts are High and multiple failed login attempts are Medium, then risk is High.
- Rule 2: If unauthorized access attempts are Critical or data exfiltration activities are High, then risk is Critical.
- Rule 3: If malware detection events are Medium and user privilege changes are Low, then risk is Medium.
- Rule 4: If unauthorized access attempts are High or suspicious IP addresses are High, then risk is High.
- Rule 5: If unauthorized access attempts are Medium and multiple failed login attempts are Medium, then risk is Medium.

- Rule 6: If unusual access times are Medium and data exfiltration activities are Medium, then risk is Medium.
- Rule 7: If malware detection events are High or data exfiltration activities are High, then risk is High.
- Rule 8: If user privilege changes are High and multiple failed login attempts are High, then risk is High.
- Rule 9: If data exfiltration activities are High and malware detection events are Medium, then risk is High.
- Rule 10: If failed login attempts are Critical, then risk is Critical.
- Rule 11: If unauthorized access attempts are Critical and multiple failed login attempts are High, then risk is Critical.
- Rule 12: If unusual access times are High and data exfiltration activities are Medium, then risk is Medium.
- Rule 13: If multiple failed login attempts are Low and user privilege changes are Medium, then risk is Low.
- Rule 14: If failed login attempts are Medium, then risk is Medium.
- Rule 15: If unauthorized access attempts are Low and multiple failed login attempts are Low, then risk is Low.
- Rule 16: If failed login attempts are Low and data exfiltration activities are Low, then risk is Low.
- Rule 17: If multiple failed login attempts are Critical and user privilege changes are High, then risk is Critical.
- Rule 18: If suspicious IP addresses are High and data exfiltration activities are Medium, then risk is Medium.
- Rule 19: If unauthorized access attempts are Medium and suspicious IP addresses are Medium, then risk is Medium.
- Rule 20: If multiple failed login attempts are High and user privilege changes are Medium, then risk is High.

These rules represent potential security scenarios, allowing the system to detect complex risk patterns by evaluating the interaction between risk factors.

After applying the fuzzy inference rules, the resulting fuzzy output needs to be converted into a single crisp value, known as defuzzification. This step is essential to produce a quantifiable risk level, allowing the fuzzy system to communicate results in a clear, actionable format.

The Centroid Method (also known as the Center of Gravity or Center of Area method) is used for defuzzification in this system. This method calculates the center of the area under the aggregated fuzzy set. It provides a balanced way of translating the fuzzy output into a crisp risk level by considering all membership values and their locations within the output space.

Dividing the output range into segments for each fuzzy set. Predefined risk levels for the output risk score (0-1)
Low: 0 to 0.25
Medium 0.25 to 0.5
High 0.5 to 0.75
Critical 0.75 to 1.0
To calculate the centroid using the following equation integrate over the range where

$$z^* = \frac{\int_{Z_{min}}^{Z_{max}} z \,.\, \mu\,(z)\,dz}{\int_{Z_{min}}^{Z_{max}} \mu\,(z)\,dz}$$

Where:

- Z represents the possible risk level values.
- μ(Z) represents the membership value of the risk level at Z.

The result is a crisp value, for example, 0.68, which might place the risk level in the "High" category.

The final output of the fuzzy inference system is a crisp risk score and a corresponding risk level category. This output is useful for security administrators in assessing the security posture of the LMS and taking appropriate actions.

IV. EXPERIMENTAL RESULTS

In real-world scenarios, the system was applied to real-time log files from LMS servers of two universities, generating risk scores and risk level results tailored to each institution's LMS environment.

This table displays the outputs of risk score and risk level results of different log files from LMS servers.

Table 6: Experimental Risk Score and Risk Level Results for Different Log Files from LMS Servers

Number of Days (log	LMS server	Risk Score	Risk Level
2days	University 1	0.41	Medium
2 days	University 2	0.6	High
7days	University 1	0.63	High
7days	University 2	0.8	Critical

The analysis of LMS server logs from two universities over different time periods highlights significant variations in risk levels, emphasizing the importance of continuous monitoring. For a 2-day logging period, University 1 exhibited a medium risk score of 0.41, indicating moderate security risks in the short term without immediate threats. In contrast, University 2 showed a higher risk score of 0.6, falling into the high-risk range, which suggests more pressing security concerns even in a short observation window.

Over a 7-day monitoring period, the risk scores escalated for both universities, with University 1 reaching a high-risk score of 0.63 and University 2 increasing to a critical risk score of 0.8. This significant rise indicates a cumulative effect of security events, such as unauthorized access attempts, multiple failed logins, or suspicious activities. These results underscore the critical role of extended monitoring, as longer observation periods provide deeper insights into evolving security patterns, allowing educational institutions to identify and address emerging threats more effectively and proactively safeguard their LMS environments.

This system presents experimental results obtained from evaluating the risk assessment model on datasets of varying sizes: 1,000, 5,000, and 50,000 records. Examining datasets of different scales aims to reveal the model's performance, consistency, and accuracy in identifying security risks across a range of data volumes. This analysis is crucial for assessing the robustness and scalability of the proposed fuzzy logic-based approach, ensuring its effectiveness when applied to both smaller and larger datasets typical of real-world LMS server logs.

Through comparative evaluation, the impact of dataset size on risk score and classification output is explored, focusing on metrics such as accuracy, precision, recall, and F1-score. This approach provides insights into the model's reliability and the effectiveness of its risk level assessments across different data volumes, ultimately guiding its potential deployment in educational institutions with diverse data management needs.

Table 7: Experimental results for Evaluation of The System

Number of Tests	Number of Records	Accuracy	Precision	Recall	F1-Score
Test 1	1000	76 %	85%	76%	75%
Test 2	5000	80%	87%	80%	79%
Test 3	50000	82%	88%	81%	81%

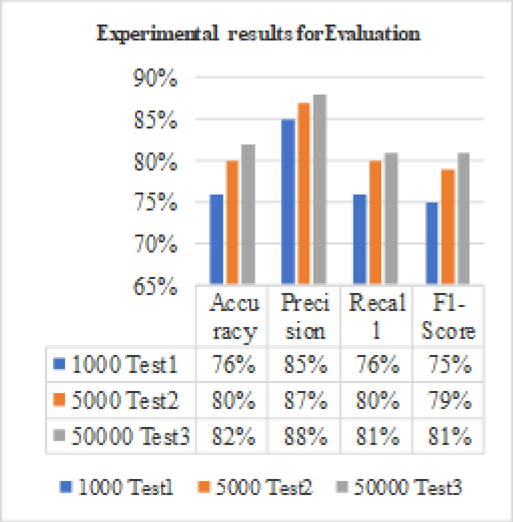

Figure 2: Experimental Performance Evaluation Result for The Proposed System

V.

CONCLUSION

This research has proposed and validated a fuzzy logic-based risk assessment model tailored for Learning Management Systems (LMS), addressing unique cybersecurity challenges in educational environments. The fuzzy logic model was designed to interpret complex risk factors from LMS log files, translating various security indicators such as unauthorized access attempts, suspicious IPs, and data exfiltration into comprehensive risk assessments. Through fuzzification and defuzzification processes, the model classified potential security threats into defined risk levels (low, medium, high, critical), offering an adaptable, interpretative approach for LMS security evaluation.

The fuzzy logic-based approach provides distinct advantages over traditional risk assessment models. Specifically, it enables more nuanced classifications, accommodates ambiguous or incomplete data, and adapts readily to evolving threat landscapes within online LMS environments. The fuzzy model also showed consistency in accuracy across large datasets, confirming its scalability and robustness for real-time security assessments in LMS infrastructures. This adaptability ensures that the model aligns well with the operational demands and dynamic nature of educational institutions' cybersecurity needs.

REFERENCES

[1] MANNANE Nada, BENCHARHI Youssef, BOULAFDOUR Brahim, REGRAGUI Boubker, Survey: Risk Assessment Models for Cloud Computing: Evaluation Criteria, 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech) ,2017, IEEE, pp.1-5. https://ieeexplore.ieee.org/document/8284712

[2] Ishraga Mohamed Ahmed Khogali, Prof. Hany Ammar, “A Methodology for The Assessment of Security Risk in Cloud Computing”, Sudan University of Science and Technology. College of Graduate Studies, December 2018.

[3] Maniah, Benfano Soewito, Ford Lumban Gaol, Edi Abdurachman, Risk Assessment on Cloud Computing for The Learning System in the Education Environment, IEEE 2019 International Conference on Engineering Technology and Education (TALE) (2019). https://ieeexplore.ieee.org/document/9225941

[4] Mouna Jouini, Latifa Ben Arfa Rabai, A Security Risk Management Model for Cloud Computing Systems: Infrastructure As a Service, Springer International Publishing AG, 2017,pp.594-608. https://link.springer.com/chapter/10.1007/978-3-319-72389-1_47

[5] Vusumuzi Malele, “Cybersecurity Cloud-Based Online Learning: A Literature Review Approach”, Journal of Information Systems and Informatics, December 2023. https://journal-isi.org/index.php/isi/article/view/583

[6] Jun.Liu and Zuhua Guo, Research On Cloud Security Risk Assessment Based on Fuzzy Entropy Weight Model, Advanced Science and Technology Letters Vol.139 (EEC 2016), pp.390-395, 2016.

[7] Paramita Chatterjee, Rajesh Bose, Subhasish Banerjee and Sandip Roy, Enhancing Data Security of Cloud Based LMS, Springer International Publishing, 25 February 2023, Volume 130, pages 1123–1139 https://link.springer.com/article/10.1007/s11277-023-10323-5

[8] Erdal Cayirci, Alexandr Garaga, Anderson Santana and Yves Roudier, A Cloud Adoption Risk Assessment Model , In Proceedings of the IEEE/ACM 7th International Conference on Utility and Cloud Computing, 2014. https://ieeexplore.ieee.org/document/7027615

[9] Nada Ahmed and Ajith Abraham, Modeling Security Risk Factors in A Cloud Computing Environment, Journal of Information Assurance and Security, ISSN 1554-1010 Volume 8 (2013) pp. 279-289. http://ajith.softcomputing.net/jias2.pdf

[10] A.Amini, N.Jamil, A.R. Ahmad and H.Sulaiman, A Fuzzy Logic Based Risk Assessment Approach for Evaluating AND Prioritizing Risks in Cloud Computing Environment, Springer International Publishing AG, Volume 5, 2018, Pages 650-659.

https://irepository.uniten.edu.my/entities/publication/2b708165-b1bc-4cc1-bcc0-926224746873

[11] Yogeshwaran Sivasubramanian, Syed Zubair Ahmed and Ved Prakash Mishra, Risk Assessment for Cloud Computing, International Research Journal of Electronics & Computer Engineering (ISSN Online: 2412-4370), June 2017. https://www.researchgate.net/publication/318060716_Risk_Assessment_for_Cloud_Computing

[12] Preecha Pangsuban, Prachyanun Nilsook and Panita Wannapiroon, Systems Analysis of Risk Assessment for Moodle Learning in A LAMP Environment From Log Files, In Proceedings of the the Sixth TCU International e-Learning Conference, July 2015. https://www.slideshare.net/slideshow/systems-analysis-of-risk-assessment-for-moodle-learning-in-a-lamp-environment-from-log-files/51021976#2

[13] Hina Abrar, Syed Jawad Hussain, Junaid Chaudhry, Kashif Saleem, Mehmet A. Orgun and Jalal Al- Muhtadi, Craig Valli , Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry ,IEEE , February 2018. https://ieeexplore.ieee.org/document/9447848

[14] Muhammad Zulkifl Hasan , Muhammad Zunnurain Hussain, Zaima Mubarak, Adeel Ahmad Siddiqui, Ali Moiz Qureshi and Imran Ismail, Data Security and Integrity in Cloud Computing, 2023 International Conference for Advancement in Technology (ICONAT) Goa, India. Jan 24-26, 2023. https://www.researchgate.net/publication/369773592_Data_security_and_Integrity_in_Cloud_Computing

[15] Gunnar Wahlgren and Stewart Kowalski, IT Security Risk Management Model for Cloud Computing: A Need for a New Escalation Approach, International Journal of E-Entrepreneurship and Innovation, 4(4), 1-19, October-December 2013. https://www.igi-global.com/gateway/article/106896

[16] Maniah , Edi Abdurachmanb, Ford Lumban Gaol, Benfano Soewito, Survey on Threats and Risks in The Cloud Computing Environment, The Fifth Information Systems International Conference, 2019. https://www.sciencedirect.com/science/article/pii/S187705091931960X

[17] Alireza Shameli-Sendi and Mohamed Cheriet, Cloud Computing: A Risk Assessment Model, IEEE International Conference on Cloud Engineering, 2014. https://ieeexplore.ieee.org/document/6903468

[18] Rasim Alguliyev and Fargana Abdullayeva, Development of Fuzzy Risk Calculation Method for A Dynamic Federation of Clouds, Intelligent Information Management, 2015, 7, 230-241. https://www.scirp.org/journal/paperabs?paperid=58377

[19] Intan Sorfina binti Mohd Fadhil, Nurul Batrisyia binti Mohd Nizar and Raudatul Jannah binti Rostam, Security and Privacy Issues in Cloud Computing, TechRxiv Powered by IEEE, 14-06-2023. https://www.techrxiv.org/doi/full/10.36227/techrxiv.23506905.v1

[20] Zoltán Balogh and Milan Turčáni, Possibilities of Modelling Web-Based Education Using IF-THEN Rules and Fuzzy Petri Nets in LMS, Conference Paper in Communications in Computer and Information Science, November 2011. https://link.springer.com/chapter/10.1007/978-3-642-25327-0_9

[21] Esteban Vázquez-Cano, M.ª Luisa Sevillano García, Analysis of Risks in A Learning Management System: A Case Study in the Spanish National University of Distance Education (UNED), © NAER New Approaches in Educational Research, 2015. https://link.springer.com/article/10.7821/naer.2015.1.107

[22] Rabia Latif, Haider Abbas, Saïd Assar, Qasim Ali, Cloud Computing Risk Assessment: A Systematic Literature Review, Future Information Technology: FutureTech 2013, 276, Springer, pp.285- 295, 2014, Lecture Notes in Electrical Engineering, 978-3-642-40860-1. 10.1007/978-3-642-40861-8_42. Hal-02397600, 6 Dsec 2019. https://link.springer.com/chapter/10.1007/978-3-642-40861-8_42

[23] Mona Soleymani, Navid Abapour, Elham Taghizadeh, Safieh Siadat and Rasoul Karkehabadi, Fuzzy Rule-Based Trust Management Model for The Security of Cloud Computing, Hindawi Mathematical Problems in Engineering Volume 2021, Article ID 6629449, 14 pages, 15 June 2021. https://onlinelibrary.wiley.com/doi/epdf/10.1155/2021/6629449