Journal of Computer Science and Technology
Publication Date: 31st August 2026
https://jcst-international-peer-reviewed-journal.iarrj.com/

ADAPTIVE AI SECURITY MODEL FOR LEARNING MANAGEMENT SYSTEMS (AASMLMS)

EGLAL Osman[1]
Department of Computer Science, Taif University, Saudi Arabia.
Email: *Ijlalosmans25@gmail.com*

ABSTRACT

Learning Management Systems (LMSs), such as Blackboard and Moodle, have become fundamental platforms for delivering education in universities and training institutions. The increasing reliance on these platforms has significantly expanded the attack surface, exposing sensitive educational data and user accounts to various cybersecurity threats, including unauthorized access, credential theft, insider misuse, and abnormal learning behaviors. Although existing security mechanisms employ traditional authentication techniques and Artificial Intelligence-based intrusion detection methods, most solutions focus on isolated security events and lack adaptive decision-making capabilities based on comprehensive user behavioral and contextual information.

This paper proposes the Adaptive AI Security Model for Learning Management Systems (AASM-LMS), an intelligent cybersecurity framework that integrates behavioral analytics, learning activity analysis, contextual security factors, Artificial Intelligence-based threat prediction, and adaptive security response within a unified architecture. The proposed framework introduces the Learning Behavioral Risk Index (LBRI) to continuously assess cybersecurity risks by combining authentication behavior, learning activities, contextual information, AI-based threat prediction, and user privilege levels into a dynamic risk assessment process. To demonstrate the applicability of the proposed framework, this study presents a conceptual experimental validation scenario using a Moodle-based learning environment. The scenario illustrates how AASM-LMS continuously monitors user behavior, identifies abnormal activities, dynamically estimates cybersecurity risks, and applies adaptive security responses while maintaining the continuity of legitimate learning activities. The proposed framework provides a practical foundation for developing intelligent, adaptive, and behavior-aware cybersecurity solutions for next-generation Learning Management Systems.

Keywords: Learning Management Systems (LMS); Cybersecurity; Artificial Intelligence; Adaptive Security; Behavioral Analytics; Learning Behavioral Risk Index (LBRI); Threat Detection; Moodle.

Introduction

The rapid digital transformation of higher education has fundamentally changed the way teaching, learning, and academic administration are conducted. Universities worldwide increasingly rely on Learning Management Systems (LMSs), such as Blackboard, Moodle, Canvas, and Brightspace, among others, to support online and blended learning, manage educational resources, deliver assessments, and facilitate communication between instructors and students [1], [8]. The widespread adoption of these platforms has significantly improved educational accessibility, flexibility, and learning efficiency while simultaneously generating massive volumes of sensitive academic and personal data [2], [13].

Despite their educational benefits, Learning Management Systems have become attractive targets for cybercriminals due to the valuable information they contain and their continuous accessibility through the Internet [4], [6]. Modern LMS platforms store students' personal information, examination questions, grades, attendance records, research materials, financial information, and institutional documents. Consequently, cyberattacks targeting educational institutions have increased considerably in recent years, including phishing attacks, credential theft, ransomware, malware injection, SQL injection, distributed denial-of-service (DDoS) attacks, insider threats, and unauthorized access [5], [12]. Such attacks may disrupt educational services, compromise sensitive information, and negatively affect institutional reputation and operational continuity.

To mitigate these risks, higher education institutions commonly implement traditional cybersecurity mechanisms including authentication protocols, role-based access control, encryption techniques, firewalls, intrusion detection systems, and periodic vulnerability assessments [3], [9]. Although these approaches provide an essential level of protection, they primarily rely on predefined rules and static security policies, limiting their ability to identify sophisticated cyber threats that continuously evolve or imitate legitimate user behavior [10], [14]. The dynamic nature of online learning environments further complicates this challenge because users frequently access LMS platforms from different devices, geographical locations, and network environments while exhibiting highly diverse learning behaviors.

Recent advances in Artificial Intelligence (AI) have introduced new opportunities for enhancing cybersecurity through intelligent threat detection, behavioral analysis, anomaly detection, predictive risk assessment, and automated incident response [21], [23]. Machine learning and deep learning algorithms have demonstrated remarkable performance in identifying complex attack patterns that cannot easily be detected using conventional rule-based approaches [24], [26]. Nevertheless, the application of AIdriven cybersecurity within Learning Management Systems remains relatively limited. Most existing studies emphasize learning analytics, student performance prediction, recommendation systems, and intelligent tutoring rather than adaptive cybersecurity specifically designed for LMS environments [27], [30].

Furthermore, existing adaptive cybersecurity frameworks have primarily been developed for enterprise information systems, cloud infrastructures, healthcare applications, and Internet of Things (IoT) environments [31], [35]. These frameworks generally evaluate security risks using contextual indicators such as login history, device characteristics, network attributes, and geographical location while overlooking educational behavioral information generated during learning activities. Consequently, valuable indicators—including learning duration, course navigation, assessment participation, assignment submission behavior, and interaction with educational resources—remain largely unused for cybersecurity purposes [16], [20].

Motivated by these limitations, this paper proposes the Adaptive AI Security Model for Learning Management Systems (AASM-LMS), an intelligent cybersecurity framework that integrates Artificial

Intelligence, behavioral analytics, contextual awareness, dynamic risk assessment, and adaptive security response within a unified architecture specifically designed for LMS environments. Unlike existing approaches, the proposed framework continuously monitors user behavior and educational activities, computes the Learning Behavioral Risk Index (LBRI), and dynamically adapts security decisions according to the evolving cyber risk level. By incorporating educational behavioral information into cybersecurity decision-making, the proposed framework aims to improve threat detection accuracy, reduce false alarms, strengthen adaptive access control, and enhance the overall security, resilience, and trustworthiness of Learning Management Systems.

The main contributions of this paper are summarized as follows:

1. A comprehensive review of recent cybersecurity challenges affecting Learning Management Systems and existing Artificial Intelligence-based security approaches.
2. Identification of key research gaps related to adaptive cybersecurity within LMS environments.
3. Development of the Adaptive AI Security Model for Learning Management Systems (AASM-LMS) that integrates behavioral analytics, contextual awareness, Artificial Intelligence, adaptive risk assessment, and security decision-making within a unified architecture.
4. Introduction of the Learning Behavioral Risk Index (LBRI) and an intelligent adaptive security workflow for continuously monitoring user activities and dynamically adjusting security responses according to the estimated cyber risk.
5. Demonstration of the proposed framework through a conceptual experimental validation scenario illustrating its applicability within Moodle-based Learning Management Systems.

The remainder of this paper is organized as follows. **Section 2** reviews the existing literature on cybersecurity challenges in Learning Management Systems, Artificial Intelligence for cybersecurity, adaptive security models, and the identified research gaps. **Section 3** presents the proposed Adaptive AI Security Model for Learning Management Systems (AASM-LMS), including its architecture, operational workflow, Learning Behavioral Risk Index (LBRI), and adaptive learning cycle. **Section 4** presents an experimental scenario and conceptual model validation. **Section 5** discusses the strengths, limitations, and practical implications of the proposed framework.

Finally, **Section 6** concludes the paper and outlines future research directions.

2. Literature Review

2.1 Security Challenges in Learning Management Systems

Learning Management Systems (LMSs) have become the backbone of digital education by supporting course management, online assessments, learning resources, communication, and academic administration in higher education institutions **[1]**. The widespread adoption of platforms such as Blackboard, Moodle, Canvas, and Microsoft Teams has significantly increased the amount of sensitive academic information stored electronically, including students' personal information, examination materials, grades, and institutional records **[1]**. These platforms are therefore considered critical information systems whose security directly affects the continuity and reliability of educational services **[2]**.

The rapid digital transformation of universities has also expanded the attack surface of LMS platforms. Since these systems are continuously connected to the Internet and accessed by students, instructors, administrators, and external users, they are increasingly exposed to cybersecurity threats including unauthorized access, phishing attacks, credential theft, malware injection, ransomware, SQL injection, cross-site scripting (XSS), distributed denial-of-service (DDoS) attacks, and insider threats **[1]**. Recent studies further indicate that cloud-based deployment and third-party service integration introduce additional security risks related to identity management, data privacy, API security, and cloud infrastructure vulnerabilities **[2]**.

Traditional security mechanisms adopted in LMS environments mainly depend on static authentication, role-based access control (RBAC), encryption, firewalls, antivirus software, and periodic vulnerability assessments **[1]**. Although these mechanisms provide a basic level of protection, they remain largely reactive because they rely on predefined security rules and signatures. Consequently, they have limited capability to detect sophisticated attacks that exploit legitimate user credentials or mimic normal user behavior, particularly in modern online learning environments where user activities continuously change **[3]**.

Recent investigations have further demonstrated that the increasing complexity of Learning Management Systems has introduced new cybersecurity challenges beyond traditional network attacks. Modern LMS platforms are closely integrated with cloud services, video conferencing systems, mobile applications, digital libraries, payment gateways, and artificial intelligence tools, creating highly interconnected educational ecosystems **[9]**. Although these integrations improve the learning experience, they simultaneously increase the number of potential attack vectors and expose educational institutions to supply-chain attacks, insecure APIs, third-party software vulnerabilities, and cloud misconfigurations **[9]**, **[10]**.

Another critical issue concerns identity management and user authentication. Most existing LMS platforms continue to rely on conventional username-password authentication, with optional multi-factor authentication available in some institutions **[11]**. However, recent cybersecurity reports indicate

that compromised credentials remain one of the primary causes of successful attacks against educational systems because attackers increasingly exploit phishing campaigns, password reuse, credential stuffing, and social engineering techniques rather than software vulnerabilities alone **[12]**. Consequently, authentication based solely on user credentials is no longer sufficient to protect modern digital learning environments.

Researchers have also highlighted the growing importance of protecting users' privacy within LMS environments. Educational platforms continuously collect sensitive information regarding students' learning activities, assessment performance, attendance records, browsing history, communication logs, and behavioral interactions **[13]**. Such information represents valuable educational assets; however, unauthorized disclosure or misuse may violate privacy regulations and negatively affect both students and educational institutions **[13]**, **[14]**.

Several recent studies therefore recommend shifting from static security mechanisms toward intelligent security frameworks capable of continuously evaluating contextual information throughout the user's learning session **[8]**, **[14]**. Instead of making security decisions only during the login process, adaptive security mechanisms continuously analyze behavioral patterns, device characteristics, geographical location, access time, network conditions, and learning activities to estimate dynamic security risks and respond accordingly **[14]**. This evolution represents a significant paradigm shift in LMS cybersecurity and establishes

Despite the significant progress achieved in strengthening LMS cybersecurity, existing security solutions still exhibit several fundamental limitations. First, most security mechanisms are reactive, meaning that they detect attacks only after suspicious events have occurred rather than predicting malicious behavior at an early stage **[14]**. Second, the majority of current solutions analyze isolated security events, such as login attempts or network traffic, without considering the complete educational context in which user activities occur **[15]**. Consequently, legitimate learning behaviors may be incorrectly classified as malicious activities, while sophisticated attackers who imitate normal users may remain undetected.

Another limitation identified in recent studies is the limited utilization of educational behavioral data for cybersecurity purposes. LMS platforms continuously generate rich learning data, including login frequency, learning duration, navigation sequences, assignment submission patterns, quiz participation, discussion activities, and resource access history **[16]**. However, most existing security frameworks ignore these valuable behavioral indicators and instead depend mainly on conventional security logs and authentication records **[17]**. This limitation reduces the capability of current cybersecurity systems to distinguish between normal educational behavior and abnormal activities associated with compromised accounts or insider attacks.

Moreover, current security models generally employ fixed security policies that apply similar protection mechanisms to all users regardless of their roles, learning patterns, or risk levels **[18]**. In practice,

however, students, instructors, administrators, and external users exhibit significantly different behavioral characteristics and security requirements. Applying identical security policies to these diverse user groups often leads either to unnecessary security restrictions that negatively affect usability or to insufficient protection for high-risk accounts **[19]**.

These observations indicate that future LMS cybersecurity solutions should move beyond conventional rule-based protection toward adaptive intelligence capable of continuously learning from user behavior, contextual information, and historical security events **[20]**. Artificial Intelligence, particularly machine learning and behavioral analytics, offers promising capabilities for predicting cyber threats, dynamically assessing security risks, and automatically adapting security decisions according to continuously changing educational environments. Therefore, recent research has increasingly focused on integrating AI technologies into cybersecurity frameworks to provide proactive, adaptive, and context-aware protection for Learning Management Systems.

2.2 Artificial Intelligence for Learning Management Systems Security

Artificial Intelligence (AI) has emerged as one of the most promising technologies for enhancing cybersecurity by enabling intelligent decision-making, automated threat detection, and predictive risk analysis [21]. Unlike conventional security mechanisms that depend on predefined rules and manually configured signatures, AI-based security systems continuously learn from historical and real-time data, allowing them to identify previously unseen attack patterns and adapt to evolving cyber threats [22]. These capabilities have encouraged researchers to investigate the integration of AI into Learning Management Systems (LMSs) to improve their resilience against increasingly sophisticated cyberattacks.

Machine Learning (ML) has become the dominant AI technique employed in cybersecurity research. Supervised learning algorithms, including Decision Trees, Random Forest, Support Vector Machines (SVM), Extreme Gradient Boosting (XGBoost), and Artificial Neural Networks (ANN), have demonstrated high effectiveness in malware detection, intrusion detection, spam filtering, and attack classification [23]. In parallel, unsupervised learning techniques such as K-Means clustering, Isolation Forest, and Autoencoders have been widely adopted for anomaly detection because they can identify abnormal behaviors without requiring labeled attack datasets [24]. These characteristics make machine learning particularly suitable for protecting LMS environments where new attack patterns continuously emerge.

Recent advances in Deep Learning (DL) have further improved cybersecurity performance through the automatic extraction of complex behavioral patterns from large-scale datasets [25]. Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) models have achieved promising results in intrusion detection,

malicious traffic classification, phishing detection, and ransomware identification [26]. Unlike conventional machine learning algorithms, deep learning models can capture temporal relationships and sequential behavioral patterns, making them particularly useful for analyzing continuous user activities within Learning Management Systems.

Another emerging research direction involves behavioral analytics powered by Artificial Intelligence. Instead of relying solely on authentication credentials, AI-based behavioral security continuously monitors users' interactions with the system, including login frequency, navigation patterns, typing behavior, device characteristics, access time, learning duration, assessment activities, and communication behavior [27]. These behavioral characteristics enable security systems to establish dynamic user profiles capable of identifying suspicious deviations that may indicate compromised accounts or insider attacks [28].

Despite these significant advances, existing AI-based cybersecurity studies have primarily focused on enterprise networks, cloud infrastructures, Internet of Things (IoT) environments, financial systems, and healthcare applications [29]. Comparatively fewer studies have investigated AI-driven cybersecurity specifically within Learning Management Systems, and most existing LMS-related studies emphasize learning analytics, student performance prediction, recommendation systems, or intelligent tutoring rather than adaptive cybersecurity [30]. This imbalance highlights an important research opportunity for developing specialized AI security models tailored to the unique operational characteristics and behavioral dynamics of Learning Management Systems.

2.3 Adaptive AI-Based Security Models

The rapid evolution of cyber threats has encouraged researchers to move beyond traditional static security mechanisms toward adaptive security models capable of continuously assessing risks and dynamically adjusting security responses according to changing operational conditions [31]. Unlike conventional security approaches, adaptive security integrates continuous monitoring, contextual awareness, behavioral analysis, and intelligent decision-making to provide proactive protection against sophisticated cyberattacks. These capabilities are particularly important in Learning Management Systems, where user behavior changes continuously throughout teaching and learning activities.

Adaptive security frameworks commonly employ risk-based authentication (RBA), continuous authentication, user and entity behavior analytics (UEBA), and contextaware access control to evaluate the legitimacy of user activities throughout an active session rather than relying exclusively on the initial login process [32]. Instead of granting permanent access after successful authentication, these models continuously calculate dynamic risk scores based on multiple contextual attributes such as geographical location, device type, login history, network characteristics, access time, user behavior, and previous security events [33]. Whenever the calculated risk exceeds predefined thresholds, additional security controls—including multi-factor authentication, privilege restriction, session monitoring, or automatic account suspension—may be activated automatically.

Recent advances in Artificial Intelligence have significantly enhanced adaptive security by enabling security systems to learn continuously from historical incidents and realtime behavioral data [34]. Machine learning algorithms can identify subtle behavioral deviations that are difficult to detect using rule-based approaches, thereby improving the detection of compromised accounts, insider threats, credential misuse, and advanced persistent attacks. Moreover, AI-driven adaptive security continuously updates its decision models according to newly observed behaviors, allowing the security framework to remain effective even when attackers modify their attack strategies.

Despite these advances, most adaptive security models have been developed for enterprise information systems, cloud infrastructures, financial services, and healthcare applications [35]. Comparatively limited attention has been given to Learning Management Systems, whose operational characteristics differ considerably from conventional enterprise environments. LMS users frequently change devices, access locations, learning schedules, and interaction patterns due to the flexible nature of online education. Consequently, applying enterprise-oriented adaptive security models directly to LMS platforms may generate excessive false alarms or overlook malicious activities that imitate legitimate learning behaviors.

Furthermore, existing AI-enabled adaptive security frameworks generally utilize traditional cybersecurity indicators such as login attempts, network traffic, endpoint events, or system logs while largely ignoring educational behavioral information generated during learning activities. Valuable contextual indicators—including course navigation behavior, assignment submission patterns, assessment participation, discussion activities, learning duration, resource utilization, and academic interaction history—remain underutilized despite their potential contribution to distinguishing legitimate educational behavior from malicious activities. This limitation represents a significant research gap and motivates the development of a specialized adaptive AI security model designed specifically for Learning Management Systems.

2.4 Research Gap

The literature review demonstrates that significant progress has been achieved in securing Learning Management Systems through conventional cybersecurity mechanisms and, more recently, through Artificial Intelligence-based security solutions. Nevertheless, several important research gaps remain unresolved.

First, the majority of existing studies focus on protecting general information systems, enterprise networks, cloud infrastructures, healthcare systems, or Internet of Things (IoT) environments rather than Learning Management Systems [21], [35]. Consequently, the unique operational characteristics of LMS platforms, including continuous educational interactions, diverse user roles, and dynamic learning behaviors, have received relatively limited attention.

Second, most current LMS security solutions continue to rely primarily on static authentication mechanisms, access control policies, encryption, and signature-based intrusion detection systems [4],

[9]. Although these mechanisms provide an essential level of protection, they remain reactive and are generally unable to identify sophisticated attacks that imitate legitimate educational activities or gradually evolve over multiple learning sessions.

Third, existing AI-based cybersecurity studies mainly utilize traditional security data such as network traffic, authentication logs, endpoint events, and system alerts while largely ignoring educational behavioral information generated within Learning Management Systems [23], [27]. Valuable indicators—including learning duration, assessment participation, course navigation sequences, assignment submission behavior, discussion forum interactions, and resource utilization—remain underexploited despite their potential to improve cyberattack detection.

Fourth, current adaptive security frameworks generally estimate security risks using contextual information such as device characteristics, geographical location, login history, and network conditions [32], [33]. However, they rarely integrate educational context and learning behavior into dynamic risk assessment models, limiting their effectiveness when deployed in higher education environments.

Finally, most existing AI security models emphasize attack detection without providing intelligent adaptive response mechanisms capable of automatically selecting appropriate security actions according to continuously changing risk levels [31], [34]. Consequently, human intervention is still required in many cybersecurity incidents, increasing response time and reducing the effectiveness of incident mitigation.

Based on these observations, this study proposes the Adaptive AI Security Model for Learning Management Systems (AASM-LMS). Unlike previous approaches, the proposed framework integrates Artificial Intelligence, behavioral analytics, contextual awareness, adaptive risk assessment, and dynamic security response within a unified architecture specifically designed for Learning Management Systems. The proposed model continuously evaluates user behavior, educational activities, contextual information, and cybersecurity indicators to predict potential threats and automatically adapt security decisions according to the estimated level of cyber risk.

Table 1. Comparison of Existing Security Approaches for Learning Management Systems

Ref.	Platform	AI Used	Adaptive Security	Behavioral Analysis	Main Limitation
[4]	General Higher	Partial	✗	✗	Focuses on integrating AI with

Education traditional security

[7] Moodle ✗ ✗ ✗ Vulnerability analysis only

Discusses AI adoption rather than

[8] Blackboard / LMS Partial ✗ ✗

security architecture

[9] Cloud LMS ✗ ✗ ✗ Reviews cloud security challenges

[10] Higher Education ✓ Partial ✗ No LMS-specific adaptive model

[14] General Systems ✓ ✓ Partial Not designed for LMS

General

[21] ✓ ✓ Partial Generic security assurance framework

Cybersecurity

Focuses on AI applications rather than

[30] LMS ✓ ✗ ✗ cybersecurity

Table 2. Comparison Between Existing Studies and the Proposed AASM-LMS

Feature	**Existing Studies**	**Proposed AASM-LMS**
LMS-specific architecture	Partial	✓
AI-based threat prediction	Partial	✓
Continuous behavioral monitoring	Limited	✓
Educational behavior analysis	✗	✓
Context-aware risk assessment	Partial	✓
Dynamic adaptive response	Limited	✓

Continuous risk scoring	Limited	✓
User behavior analytics	Partial	✓
Learning activity analysis	✗	✓
Automated security decision engine	✗	✓

As summarized in Table 2, none of the reviewed studies simultaneously integrates behavioral analytics, AI-based threat prediction, adaptive risk assessment, educational activity analysis, and continuous learning within a unified cybersecurity framework specifically designed for Learning Management Systems.

2.5 Summary of Literature Review

The reviewed literature demonstrates that significant progress has been achieved in applying Artificial Intelligence to cybersecurity and in developing adaptive security mechanisms for various computing environments. Existing studies have successfully utilized machine learning, anomaly detection, behavioral analytics, and contextual information to improve cyber threat detection. However, these approaches have largely focused on enterprise networks, cloud computing, healthcare systems, and Internet of Things (IoT) environments.

Within Learning Management Systems, previous research has primarily emphasized learning analytics, academic performance prediction, recommendation systems, and conventional security mechanisms rather than adaptive AI-driven cybersecurity. Furthermore, existing LMS security studies rarely incorporate educational behavioral information—including course navigation, assessment participation, learning duration, and resource interaction—into cybersecurity decision-making.

Based on these observations, a clear research gap exists in developing an intelligent cybersecurity framework that integrates Artificial Intelligence, behavioral analytics, contextual awareness, adaptive risk assessment, and educational behavioral information within a unified architecture specifically designed for Learning Management Systems. This gap motivates the development of the proposed Adaptive AI Security Model for Learning Management Systems (AASM-LMS), presented in the following section.

3. Proposed Adaptive AI Security Model for Learning Management Systems (AASM-LMS)

3.1 Overview of the Proposed Model

Based on the research gaps identified in Section 2, this study proposes the Adaptive AI Security Model for Learning Management Systems (AASM-LMS), a conceptual cybersecurity framework that integrates Artificial Intelligence, behavioral analytics, contextual awareness, dynamic risk assessment, and adaptive security response into a unified architecture specifically designed for Learning Management Systems.

The increasing sophistication of cyber threats targeting Learning Management Systems requires security solutions that extend beyond conventional authentication and rulebased protection mechanisms. Existing LMS security approaches primarily focus on preventing known attacks using static security policies, predefined signatures, or isolated intrusion detection techniques. Although these mechanisms provide an essential level of protection, they lack the capability to continuously evaluate user behavior, dynamically assess cyber risks, and automatically adapt security responses according to evolving threats. Consequently, a more intelligent and adaptive security framework is required to address the complex cybersecurity challenges associated with modern digital learning environments.

To overcome these limitations, this paper proposes the Adaptive AI Security Model for Learning Management Systems (AASM-LMS). The proposed model integrates Artificial Intelligence, behavioral analytics, contextual awareness, dynamic risk assessment, and adaptive security response into a unified cybersecurity framework specifically designed for LMS environments. Rather than relying exclusively on login credentials or predefined security rules, AASM-LMS continuously analyzes educational activities, user behavior, contextual information, and system security events throughout the entire learning session.

The proposed framework operates according to a continuous security lifecycle. Initially, user activities and contextual information are collected from the Learning Management System, including authentication logs, course navigation behavior, assessment participation, assignment submission records, resource access patterns, device information, network characteristics, and session attributes. These heterogeneous data sources are then preprocessed and transformed into behavioral and contextual features suitable for Artificial Intelligence analysis.

Following data preprocessing, the AI-based Behavioral Analytics Engine continuously evaluates user activities to identify behavioral deviations from established learning patterns. Simultaneously, the Dynamic Risk Assessment Engine integrates behavioral indicators with contextual security information to calculate a continuously updated cyber risk score representing the probability of malicious activities. Based on the calculated risk level, the Adaptive Security Decision Engine automatically determines the most appropriate security response without interrupting legitimate learning activities whenever possible.

Unlike conventional LMS security architectures, which usually perform security verification only during user login, the proposed AASM-LMS continuously reassesses cyber risks throughout the entire educational session. This continuous evaluation enables the framework to detect compromised accounts, insider threats, abnormal learning behaviors, privilege misuse, and sophisticated attacks that gradually evolve over time while minimizing unnecessary security interruptions for legitimate users.

Overall, the proposed model establishes an intelligent, adaptive, and context-aware cybersecurity framework capable of improving attack detection accuracy, reducing false-positive rates, strengthening adaptive access control, and enhancing the resilience of Learning Management Systems against emerging cyber threats.

Table 3. Main Components of the Proposed AASM-LMS

Component	**Function**
Data Acquisition Layer	Collects authentication logs, learning activities, user interactions, and contextual information from the LMS.
Data Preprocessing Layer	Cleans, normalizes, integrates, and prepares collected data for AI analysis.
Behavioral Analytics Engine	Learns normal user behavior and detects abnormal learning activities.
AI Threat Prediction Engine	Predicts potential cyber threats using Machine Learning models.
Dynamic Risk Assessment Engine	Calculates a real-time cyber risk score using behavioral and contextual indicators.
Adaptive Security Decision Engine	Selects the most appropriate security response according to the estimated risk level.
Security Response Layer	Executes adaptive actions such as MFA, privilege restriction, session monitoring, temporary blocking, or administrator notification.
Continuous Learning Module	Updates AI models continuously using newly collected behavioral and security data.

3.2 Architecture of the Proposed AASM-LMS

The proposed Adaptive AI Security Model for Learning Management Systems (AASMLMS) is designed as a multi-layer intelligent cybersecurity architecture that continuously monitors user behavior, analyzes contextual information, predicts cyber threats, evaluates dynamic security risks, and automatically selects appropriate security responses. Unlike conventional LMS security frameworks that perform authentication only during user login, AASM-LMS continuously evaluates security throughout the entire learning session.

The architecture consists of seven tightly integrated layers, each responsible for a specific cybersecurity function. Together, these layers establish an adaptive decisionmaking framework capable of protecting Learning Management Systems against both known and emerging cyber threats.

Layer 1: Data Acquisition Layer

This layer collects security-related information from multiple LMS components. The collected information includes authentication logs, user profiles, course access history, assignment submissions, examination activities, discussion forums, file downloads, device characteristics, browser information, IP addresses, geographical locations, timestamps, and network attributes. These heterogeneous data sources provide the foundation for intelligent security analysis.

Layer 2: Data Preprocessing Layer

Raw data collected from different LMS modules are cleaned, normalized, integrated, and transformed into structured datasets suitable for Artificial Intelligence processing. Missing values, duplicated records, noisy events, and inconsistent log entries are handled before feature extraction.

Layer 3: Behavioral Analytics Engine

The Behavioral Analytics Engine serves as the core analytical component responsible for transforming raw educational activities into meaningful behavioral indicators that support adaptive cybersecurity decisions**.**

This layer represents one of the main innovations of AASM-LMS.

Instead of monitoring login events only, the proposed model continuously analyzes educational behavior such as:

Login frequency

Learning duration

Navigation sequence

Assessment participation

Assignment submission patterns

Forum participation

Resource access behavior

Session duration

These behavioral indicators are used to establish a dynamic behavioral profile for every LMS user.

Layer 4: AI Threat Prediction Engine

Rather than replacing conventional security mechanisms, the AI Threat Prediction Engine complements existing authentication and access control mechanisms by providing predictive intelligence based on continuously evolving behavioral patterns.

Machine Learning algorithms continuously analyze extracted behavioral features to estimate the probability of malicious activities.

Depending on available datasets, the prediction engine may employ:

Random Forest

XGBoost

Support Vector Machine (SVM)

LightGBM

The prediction output is represented as a probability score rather than a binary decision.

Layer 5: Dynamic Risk Assessment Engine

Unlike previous studies that depend only on authentication events, the proposed engine combines:

AI prediction score

User behavior score

Contextual information

User privilege level

Device trust level

Network trust level

These factors are integrated to calculate a Dynamic Risk Score (DRS) representing the current cybersecurity risk associated with each active session.

Layer 6: Adaptive Security Decision Engine

Based on the calculated Dynamic Risk Score, the model automatically selects one of several adaptive security actions.
For example:

Risk Level	**Security Action**
Low	Continue monitoring
Medium	Request Multi-Factor Authentication
High	Restrict sensitive functions
Critical	Suspend session and notify administrator

Unlike static security policies, these decisions are continuously updated whenever new behavioral information becomes available.

Layer 7: Continuous Learning Layer

Every confirmed security incident becomes new training data for the Artificial Intelligence model. Consequently, the prediction model continuously improves over time without requiring complete manual retraining, enabling the security framework to adapt to newly emerging attack techniques.

3.3 Learning Behavioral Risk Index (LBRI)

The Learning Behavioral Risk Index (LBRI) is one of the principal contributions of the proposed Adaptive AI Security Model for Learning Management Systems (AASMLMS). Unlike conventional cybersecurity approaches that primarily rely on authentication logs, network traffic, or isolated security

events, the proposed index combines both cybersecurity indicators and educational behavioral information to estimate the current security risk associated with each active LMS session.

The LBRI continuously evaluates users' activities throughout the learning session rather than making security decisions only during the login process. This continuous assessment enables the proposed model to identify abnormal behavioral patterns at an early stage while minimizing unnecessary interruptions to legitimate learning activities.

To estimate the security risk, the proposed index considers five categories of information that are commonly available in Learning Management Systems.

Authentication Behavior (AB): evaluates user authentication activities, including login frequency, failed login attempts, session duration, login consistency, and authentication history.

Learning Activity Behavior (LAB): analyzes educational interactions such as course navigation, learning duration, assignment submissions, assessment participation, discussion forum activities, and learning resource access.

Contextual Security Factors (CSF): examines contextual information associated with each session, including device type, browser characteristics, IP address, geographical location, access time, and network environment.

Threat Prediction Score (TPS): represents the probability of malicious behavior estimated by the Artificial Intelligence engine after analyzing the collected behavioral and contextual information.

User Privilege Level (UPL): reflects the sensitivity of user permissions within the LMS. Administrative accounts generally require stronger protection than instructor or student accounts because they possess higher access privileges.

To enable adaptive cybersecurity decision-making, this study introduces the Learning Behavioral Risk Index (LBRI), a composite risk metric designed to quantify the cybersecurity risk associated with an active LMS session. The proposed index integrates five complementary behavioral and contextual factors into a single dynamic score, allowing the framework to continuously evaluate user trustworthiness and determine the appropriate adaptive security response.

$$LBRI = \sum_{i=1}^{5} w_i F_i$$

where

F_1= Authentication Behavior (AB)

F_2= Learning Activity Behavior (LAB)

F_3= Contextual Security Factors (CSF)

F_4= Threat Prediction Score (TPS)

F_5= User Privilege Level (UPL)

The weighting factors (w_i)represent the relative contribution of each component to the overall security assessment, where:

$$\sum_{i=1}^{5} w_i = 1$$

The resulting LBRI value ranges from 0 (minimum security risk) to 1 (maximum security risk). Higher values indicate a greater likelihood that the current user session contains suspicious or malicious activities requiring adaptive security intervention.

Based on the calculated LBRI value, the proposed model classifies user sessions into four security levels, allowing the Adaptive Security Decision Engine to automatically determine the most appropriate response.

LBRI Range	**Risk Level**	**Adaptive Security Response**
0.00 – 0.30	Low	Continue normal monitoring
0.31 – 0.60	Medium	Request additional authentication (MFA)
0.61 – 0.80	High	Restrict sensitive LMS functions and increase monitoring
0.81 – 1.00	Critical	Suspend the session, notify the administrator, and initiate incident response procedures

Unlike conventional security mechanisms that perform authentication only once at the beginning of a user session, the proposed LBRI is continuously updated as new behavioral and contextual information becomes available. Consequently, AASM-LMS can dynamically adapt its security decisions according to continuously changing user behavior, thereby improving threat detection accuracy while reducing false alarms and minimizing unnecessary disruptions to legitimate learning activities.

3.4 Operational Workflow of the Proposed AASM-LMS

The operational workflow of the proposed AASM-LMS framework consists of a continuous cybersecurity cycle that monitors user activities, evaluates security risks, and dynamically adapts security responses throughout the learning session. Unlike conventional LMS security mechanisms that perform authentication only at the beginning of a session, the proposed framework continuously reassesses user trustworthiness based on behavioral, contextual, and security-related information.

The workflow begins when a user authenticates to the Learning Management System. Authentication information, including user identity, login time, device characteristics, network information, and user privilege level, is collected as the initial security context. Once authentication is completed, the Behavioral Analytics Engine continuously monitors educational activities, such as course navigation, assessment participation, learning duration, assignment submissions, and interactions with educational resources.

The extracted behavioral information, together with contextual security attributes, is forwarded to the AI Threat Prediction Engine, where Artificial Intelligence techniques analyze behavioral patterns and estimate the probability of malicious or abnormal activities. The resulting threat prediction is combined with authentication confidence, contextual security information, and user privilege level to calculate the Learning Behavioral Risk Index (LBRI).

Based on the computed LBRI value, the Adaptive Security Decision Engine dynamically determines the appropriate security response. Depending on the estimated risk level, the framework may continue the learning session without interruption, request additional authentication, increase behavioral monitoring, restrict access to sensitive LMS functions, or temporarily suspend the session for further verification.

Finally, validated behavioral information and confirmed security incidents are stored within the Continuous Learning Module. These data are used to refine behavioral profiles and improve future threat prediction, enabling the proposed framework to continuously adapt to evolving cyber threats and changing user behaviors.

Table 4. Operational Workflow of AASM-LMS

Step	Process	Output
1	User Authentication	User session initiated

2	Continuous Data Collection	Behavioral and contextual data
3	Data Preprocessing	Cleaned and structured security features
4	Behavioral Analytics	User behavior profile
5	AI Threat Prediction	Threat Prediction Score (TPS)
6	LBRI Calculation	Dynamic cyber risk value
7	Adaptive Security Decision	Appropriate security action
8	Continuous Learning	Updated AI models

3.5 Algorithm of AASM-LMS Algorithm 1

Algorithm 1. Adaptive AI Security Workflow of AASM-LMS

Algorithm 1 summarizes the operational sequence of the proposed AASM-LMS framework. The algorithm begins by collecting behavioral and contextual information from the Learning Management System, followed by AI-based behavioral analysis and threat prediction. Subsequently, the Learning Behavioral Risk Index (LBRI) is computed to estimate the current cybersecurity risk. Finally, the Adaptive Security Decision Engine selects and executes the most appropriate security response, while validated security events are incorporated into the Continuous Learning Module to improve future threat detection performance**.**

Algorithm 1: Adaptive AI Security Decision Workflow

Input:

User authentication information User behavioral activities

Contextual security information

User privilege level

Output:

Adaptive security decision

Begin

1. **Authenticate user credentials.**
2. **Collect contextual security information:**

   - Device characteristics

   - Network information

   - Login location

   - Login time

3. **Monitor learning activities:**

   - Course navigation

   - Learning duration

   - Assignment submission

   - Assessment participation

   - Resource access - Discussion forum activities

4. **Perform behavioral analytics.**
5. **Execute AI-based threat prediction.**
6. **Calculate the Learning Behavioral Risk Index (LBRI).**
7. **Determine the current risk level.**

8. If LBRI is Low

Allow normal learning session.

9. Else if LBRI is Medium

Request Multi-Factor Authentication (MFA).

10. Else if LBRI is High Restrict sensitive LMS functions Increase behavioral monitoring.

11. Else

Suspend the session Notify the system administrator.

12. Store validated behavioral information.

13. Update the Continuous Learning Module.

14. Return adaptive security decision.

End Algorithm

3.5 Architecture of the Proposed AASM-LMS

Figure 1 illustrates the overall architecture of the proposed **Adaptive AI Security Model for Learning Management Systems (AASM-LMS)**. The architecture integrates Artificial Intelligence, behavioral analytics, contextual awareness, dynamic risk assessment, and adaptive security response into a unified cybersecurity framework specifically designed for Learning Management Systems.

The workflow begins with the **Learning Management System**, where users interact with educational services through normal academic activities such as authentication, course access, assignment submission, examinations, discussion forums, learning resource utilization, and communication tools. These interactions generate both educational and security-related information that serves as the primary input to the proposed framework.

The collected information is transferred to the **Data Acquisition Layer**, which gathers authentication logs, user activities, contextual information, device characteristics, network attributes, and session metadata from different LMS modules. The collected data are then forwarded to the **Data Preprocessing Layer**, where data cleaning, normalization, integration, and feature extraction are performed before Artificial Intelligence analysis.

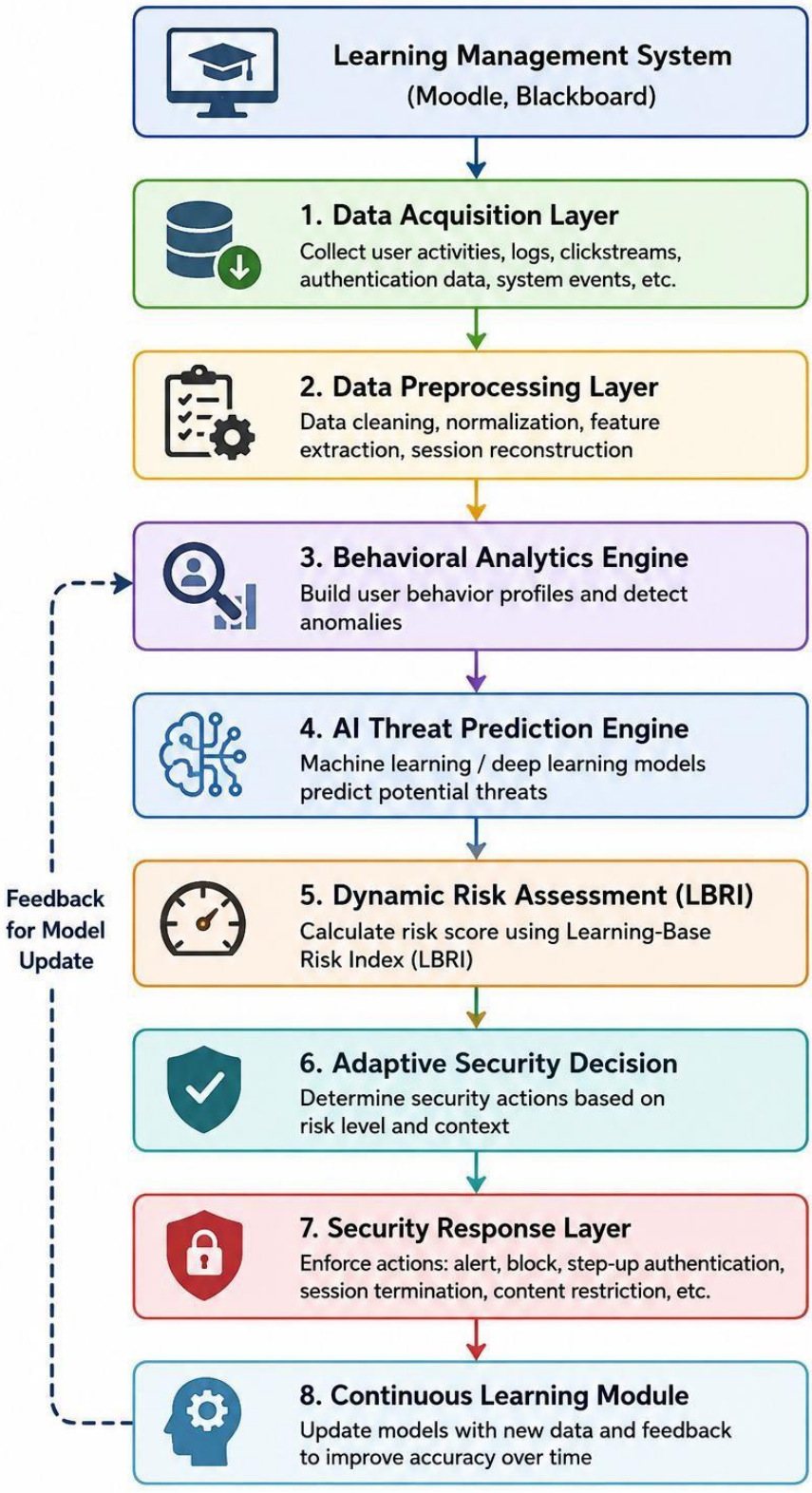
The processed information is subsequently analyzed by the **Behavioral Analytics Engine**, which continuously learns normal educational behavior and identifies abnormal behavioral deviations. Simultaneously, the **AI Threat Prediction Engine** evaluates the processed data using machine learning algorithms to estimate the probability of malicious activities.

Both outputs are combined within the **Dynamic Risk Assessment Engine**, where the proposed **Learning Behavioral Risk Index (LBRI)** is calculated to estimate the current cybersecurity risk associated with each active user session. The calculated risk score is then transmitted to the **Adaptive Security Decision Engine**, which automatically determines the most appropriate security response according to the estimated threat level.

Depending on the calculated LBRI value, the framework may continue normal monitoring, request additional authentication, restrict sensitive LMS functions, increase security monitoring, or temporarily suspend suspicious sessions. All security decisions are recorded within the **Continuous Learning Module**, allowing confirmed security incidents and validated user behaviors to improve future AI prediction models through continuous model updating.

By integrating behavioral intelligence with adaptive cybersecurity mechanisms, the proposed architecture establishes a closed-loop security framework capable of continuously learning from previous experiences while dynamically responding to evolving cyber threats.

Figure 1. *Architecture of the Proposed Adaptive AI Security Model for Learning Management Systems (AASM-LMS).*



AI Threat Prediction Engine :

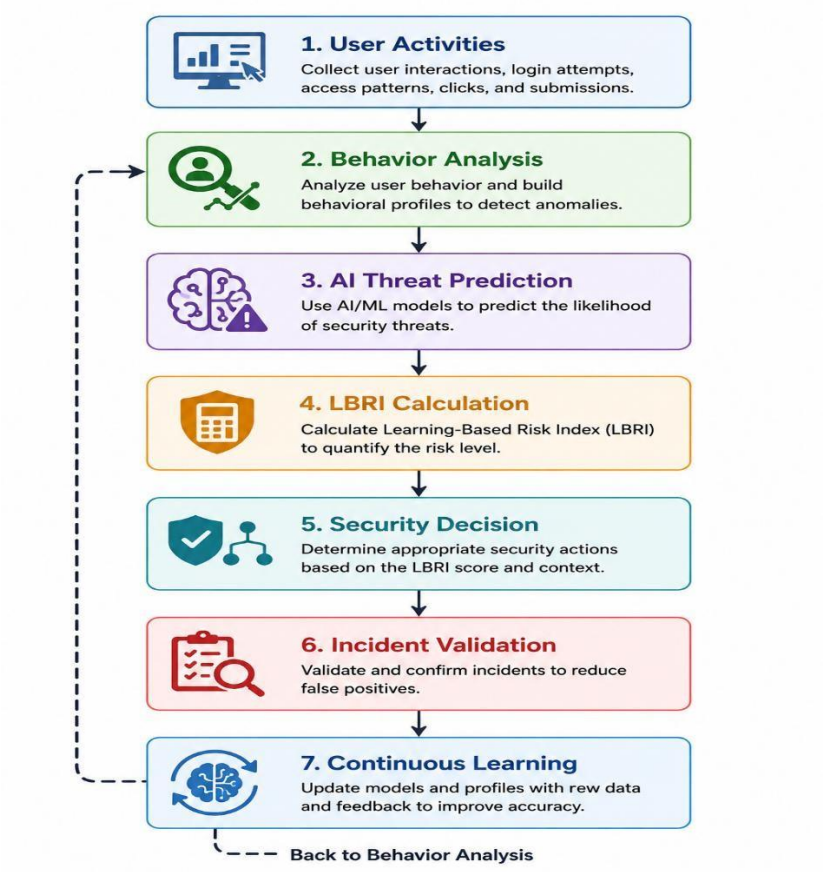
[• Feature Extraction - • Machine Learning Model - Threat Prediction]

Behavioral Analytics

[• Login Behavior - Learning Activities - Context Analysis]

Although the architecture presented in Figure 1 illustrates the main functional components of the proposed AASM-LMS, the framework is designed to operate as a continuously evolving adaptive security system rather than a static protection mechanism. After each completed user session, newly collected behavioral information and confirmed security incidents are stored within the Continuous Learning Module. These data are subsequently utilized to refine the behavioral profiles and retrain the AI Threat Prediction Engine, enabling the framework to continuously improve its threat detection capability, adapt to newly emerging attack patterns, and reduce false-positive decisions over time. This adaptive learning process ensures that the proposed model evolves together with changes in user behavior and the cybersecurity threat landscape.

Figure 2. Continuous Learning and Adaptive Threat-Detection Cycle of the Proposed AASM-LMS.



4. Experimental Scenario and Model Validation

4.1 Experimental Environment

To demonstrate the applicability of the proposed Adaptive AI Security Model for Learning Management Systems (AASM-LMS), this section presents a conceptual validation scenario based on a Moodle

learning environment. The purpose of this scenario is not to evaluate the performance of specific machine learning algorithms, but rather to illustrate how the proposed framework operates in a realistic educational context and how its adaptive security components interact to support intelligent cybersecurity decision-making.

Assume that a student logs into Moodle using valid credentials from a registered personal device located within the university network. During the initial authentication stage, the system verifies the user's identity and establishes the initial security context based on authentication confidence, device characteristics, network information, login time, and user privilege level. After successful authentication, the Behavioral Analytics Engine continuously monitors the student's learning activities. These activities include course navigation, learning duration, access to educational resources, participation in online quizzes, assignment submissions, and interactions within discussion forums. Under normal conditions, these behavioral patterns remain consistent with the student's historical learning profile, resulting in a low Learning Behavioral Risk Index (LBRI) and allowing uninterrupted access to LMS services.

Consider a second scenario in which the same user account suddenly exhibits unusual behavior. The account accesses multiple courses within a short period, downloads an unusually large number of learning resources, repeatedly attempts to access restricted administrative functions, and connects from an unfamiliar network environment. Although the user's credentials remain valid, these activities deviate significantly from the established behavioral profile. The AI Threat Prediction Engine analyzes the observed behavioral and contextual information and identifies the session as potentially malicious. Consequently, the calculated LBRI increases, prompting the Adaptive Security Decision Engine to initiate appropriate protective actions. Depending on the estimated risk level, the framework may request multi-factor authentication, increase behavioral monitoring, temporarily restrict access to sensitive LMS functions, or suspend the active session for additional verification.

Following security verification, confirmed behavioral information is transferred to the Continuous Learning Module, where it becomes part of the historical behavioral knowledge base. This adaptive learning process enables AASM-LMS to refine future threat prediction models, improve behavioral profiling accuracy, and continuously adapt to newly emerging cyber threats without disrupting legitimate educational activities.

Overall, this conceptual validation scenario demonstrates how the proposed framework integrates behavioral analytics, contextual awareness, Artificial Intelligence, dynamic risk assessment, and adaptive security response into a unified cybersecurity workflow suitable for modern Learning Management Systems.

4.2 Experimental Cybersecurity Scenario

To demonstrate the operational behavior of the proposed Adaptive AI Security Model for Learning Management Systems (AASM-LMS), a representative cybersecurity scenario is considered within a Moodle-based educational environment. The scenario illustrates how the proposed framework processes user activities, evaluates behavioral patterns, estimates cybersecurity risks, and dynamically applies adaptive security responses.

Initially, a student accesses the Learning Management System using valid authentication credentials from a recognized device and network environment. During the early stages of the learning session, the student's activities remain consistent with previously learned behavioral patterns, including normal course navigation, access to enrolled learning materials, participation in discussion forums, and completion of online assessments. Consequently, the Behavioral Analytics Engine identifies the session as normal, resulting in a low Learning Behavioral Risk Index (LBRI) and allowing uninterrupted access to educational resources.

As the session continues, several abnormal behavioral events begin to occur. The user logs into the LMS from an unfamiliar device and geographic location, accesses multiple courses within a short period, rapidly downloads a large number of learning resources, and attempts to view administrative pages that are unrelated to the assigned academic role. Although each event may appear legitimate when considered independently, their combined occurrence represents a significant deviation from the user's historical learning behavior. The Behavioral Analytics Engine detects these behavioral anomalies by comparing current activities with the established user profile. Simultaneously, the AI Threat Prediction Engine analyzes the extracted behavioral and contextual features to estimate the probability that the observed activities correspond to malicious behavior or account compromise. Based on the outputs of both components, the Dynamic Risk Assessment Engine calculates the Learning Behavioral Risk Index (LBRI). As additional abnormal activities are observed, the LBRI increases progressively from a low-risk state to medium, high, and eventually critical risk levels. This dynamic evaluation enables the framework to continuously reassess the security status of the active session rather than relying solely on the initial authentication process.

According to the calculated LBRI value, the Adaptive Security Decision Engine automatically selects the most appropriate security response. Depending on the severity of the detected risk, the framework may request multi-factor authentication, temporarily restrict access to sensitive LMS functions, increase behavioral monitoring, notify the system administrator, or suspend the active session until further verification is completed.

Following the completion of the security investigation, validated behavioral information and confirmed security incidents are stored within the Continuous Learning Module. These data are subsequently

utilized to refine behavioral profiles and improve future AI-based threat prediction, enabling the proposed framework to adapt continuously to evolving cyber threats and changing user behaviors.

The presented experimental scenario demonstrates the practical operation of the proposed AASM-LMS framework and illustrates how the integration of behavioral analytics, artificial intelligence, dynamic risk assessment, and adaptive security response can enhance cybersecurity protection while preserving the continuity of legitimate learning activities.

Table 5. Adaptive Security Responses During the Experimental Scenario

Observed Activity	**Behavior Analysis**	**LBRI Level**	**Adaptive Security Response**
Normal login from a recognized device	Normal user behavior	Low	Continue normal learning session
Login from an unfamiliar device	Moderate behavioral deviation	Medium	Request Multi-Factor Authentication (MFA)
Large-scale downloading of learning resources	Suspicious learning behavior	High	Restrict downloads and increase monitoring
Attempt to access unauthorized administrative pages	Critical behavioral anomaly	Critical	Suspend session and notify the administrator

4.3 Validation Summary

The experimental scenario presented in this study provides a conceptual validation of the proposed Adaptive AI Security Model for Learning Management Systems (AASMLMS). Rather than focusing on implementation-specific performance metrics, the validation demonstrates how the proposed framework integrates behavioral analytics, artificial intelligence, contextual awareness, dynamic risk assessment, and adaptive security response into a unified cybersecurity process. The scenario illustrates that the proposed framework is capable of continuously monitoring user activities throughout the learning session instead of relying solely on initial authentication. By combining authentication behavior, learning activity patterns, contextual security information, AIbased threat prediction, and user privilege levels, the Learning Behavioral Risk Index (LBRI) provides a dynamic representation of the current cybersecurity risk associated with each active session.

The adaptive decision-making mechanism further demonstrates the practical applicability of the proposed model. As user behavior changes during the learning session, the calculated LBRI is continuously updated, enabling the framework to dynamically adjust security responses according to the estimated threat level. This adaptive capability supports proactive cybersecurity protection while minimizing unnecessary interruptions to legitimate educational activities. Furthermore, the incorporation of the Continuous Learning Module enables the proposed framework to improve its behavioral knowledge over time. By utilizing validated security incidents and historical behavioral information, the Artificial Intelligence models can gradually adapt to newly emerging cyber threats and evolving user behavior, thereby enhancing the long-term effectiveness of the proposed security framework.

Although the present study focuses on conceptual validation, the proposed architecture establishes a practical foundation for future implementation within real Learning Management Systems. Future experimental investigations may evaluate the proposed framework using operational LMS datasets and compare its performance with existing cybersecurity approaches based on standard security evaluation metrics.

5. Discussion

The proposed Adaptive AI Security Model for Learning Management Systems (AASMLMS) addresses several limitations identified in existing LMS cybersecurity research by integrating Artificial Intelligence, behavioral analytics, contextual awareness, dynamic risk assessment, and adaptive security response into a unified security framework. Unlike conventional LMS security approaches that primarily rely on authentication, access control, and signature-based intrusion detection, the proposed model continuously evaluates user behavior throughout the entire learning session. This continuous assessment enables earlier detection of suspicious activities while reducing dependence on static security policies.

One of the most significant contributions of AASM-LMS is the incorporation of educational behavioral information into cybersecurity decision-making. Previous studies have predominantly focused on traditional security indicators such as authentication logs, network traffic, and system events [23], [31]. In contrast, the proposed framework considers learning-specific behavioral attributes—including course navigation, learning duration, assignment submissions, assessment participation, discussion activities, and resource utilization—as valuable indicators for identifying abnormal behaviors. By combining educational and cybersecurity information, the proposed model provides a more comprehensive understanding of user activities within Learning Management Systems.

Another important contribution is the introduction of the Learning Behavioral Risk Index (LBRI), which consolidates multiple behavioral and contextual indicators into a single dynamic risk measure. Rather than making binary security decisions immediately after authentication, AASM-LMS continuously

updates the estimated security risk as new user activities are observed. This adaptive approach enables the framework to respond more effectively to evolving cyber threats while minimizing unnecessary interruptions to legitimate educational activities.

The proposed architecture also provides considerable flexibility for deployment across different Learning Management Systems. Since the framework relies primarily on standard LMS logs and behavioral information that are commonly generated by platforms such as Moodle, Blackboard, Canvas, and similar systems, the proposed model can be integrated with existing educational infrastructures without requiring substantial modifications to the underlying LMS architecture. This characteristic increases its practical applicability for higher education institutions seeking to enhance cybersecurity while preserving the normal teaching and learning experience.

The conceptual validation presented through the experimental scenario further demonstrates the practical applicability of the proposed framework. The scenario illustrates how behavioral analytics, AI-based threat prediction, the Learning Behavioral Risk Index (LBRI), and adaptive security decision-making operate together to identify abnormal learning behaviors and dynamically apply appropriate security responses. Although the validation does not involve a full-scale implementation or experimental performance evaluation, it confirms the logical consistency of the proposed architecture and demonstrates its potential applicability in realistic Learning Management System environments.

From an Artificial Intelligence perspective, the Continuous Learning Module represents another important advantage of the proposed framework. As confirmed security incidents and validated behavioral patterns become available, they are incorporated into the security knowledge repository to continuously refine behavioral profiles and improve future threat prediction capabilities. This adaptive learning mechanism enables AASM-LMS to evolve alongside emerging cyber threats and changing user behaviors, supporting long-term improvements in cybersecurity protection.

Despite these strengths, several challenges should be acknowledged. The effectiveness of the proposed framework depends on the availability of comprehensive behavioral information generated by Learning Management Systems. Institutions with limited logging capabilities or incomplete behavioral records may reduce the effectiveness of behavioral analysis and adaptive risk assessment. In addition, privacy, ethical considerations, and compliance with institutional data protection policies must be carefully addressed when collecting and analyzing educational behavioral data.

Future research should focus on implementing the proposed framework within operational Learning Management Systems and evaluating its effectiveness using real educational environments. Further investigations may compare different Artificial Intelligence techniques for behavioral analysis and threat prediction, evaluate the effectiveness of the Learning Behavioral Risk Index (LBRI) under various cybersecurity scenarios, and explore explainable AI, federated learning, and privacypreserving approaches to enhance transparency, scalability, and data protection in adaptive LMS cybersecurity frameworks.

Conclusion

The rapid adoption of Learning Management Systems (LMSs) in higher education has introduced new cybersecurity challenges that extend beyond the capabilities of traditional authentication and access control mechanisms. As cyber threats continue to evolve, educational institutions require intelligent security frameworks capable of continuously monitoring user behavior, adapting to changing security conditions, and responding proactively to potential attacks without disrupting legitimate learning activities.

This paper presented the **Adaptive AI Security Model for Learning Management Systems (AASM-LMS)**, a conceptual cybersecurity framework that integrates Artificial Intelligence, behavioral analytics, contextual awareness, dynamic risk assessment, and adaptive security response within a unified architecture. To support adaptive decision-making, the study introduced the **Learning Behavioral Risk Index (LBRI)**, which combines authentication behavior, learning activities, contextual security information, AI-based threat prediction, and user privilege levels into a single dynamic risk indicator for continuous cybersecurity assessment.

In addition to the proposed architecture, the study described the operational workflow of AASM-LMS, presented its adaptive learning cycle, and introduced an experimental validation scenario to demonstrate how the framework operates within a realistic Moodle-based educational environment. The validation scenario illustrated the interaction among the framework components and demonstrated how abnormal user behavior can be detected and addressed through adaptive security decisions without requiring a full-scale implementation.

Compared with conventional LMS security approaches, the proposed framework emphasizes continuous behavioral monitoring rather than one-time authentication, enabling security decisions to evolve dynamically throughout the learning session. Furthermore, the Continuous Learning Module allows the framework to refine its behavioral knowledge over time, supporting long-term adaptability against emerging cyber threats while maintaining the continuity of legitimate educational activities.

Although the present study focuses on conceptual design and scenario-based validation, the proposed framework establishes a practical foundation for future research and implementation in real Learning Management Systems. Future work will include deploying AASM-LMS in operational educational environments, validating the Learning Behavioral Risk Index (LBRI) using real LMS behavioral data, comparing different Artificial Intelligence techniques for behavioral threat prediction, and investigating explainable AI (XAI), federated learning, and privacy-preserving approaches to further improve the

effectiveness, transparency, and scalability of adaptive cybersecurity solutions for Learning Management Systems.

To further emphasize the research contributions of the proposed framework, Table 6 summarizes the major cybersecurity capabilities addressed in previous LMS security research and compares them with the proposed AASM-LMS. The comparison highlights how the proposed framework integrates multiple security functionalities into a unified adaptive architecture while addressing several research gaps identified in the literature

Table 6. Comparative Summary of Existing Research and the Proposed AASM-LMS Framework

Security Capability	**Existing Research**	**Proposed AASM-LMS**
Authentication Mechanisms	✓	✓
Role-Based Access Control	✓	✓
Multi-Factor Authentication	✓	✓
AI-Based Threat Detection	✓	✓
Behavioral Analytics	Partial	✓
Learning Activity Analysis	Limited	✓
Context-Aware Security Analysis	Partial	✓
Dynamic Risk Assessment	Partial	✓ (LBRI)
Continuous Session Monitoring	Limited	✓
Adaptive Security Response	Partial	✓
Continuous Learning Mechanism	Limited	✓
Integration of Educational and Security Behaviors	✗	✓
LMS-Specific Adaptive Architecture	Partial	✓
Unified AI-Based Security Framework	✗	✓

References

[1] P. A. Pillajo Garcia and D. F. Avila Pesantez, “Cybersecurity Analysis in E-Learning Platforms: A Systematic Literature Review,” *Perspectivas*, vol. 5, no. 1, pp. 19–29, 2023, doi: 10.47187/perspectivas.5.1.179.

[2] V. Malele, “Cybersecurity Cloud-Based Online Learning: A Literature Review

Approach,” *Journal of Information Systems and Informatics*, vol. 5, no. 4, pp. 1623– 1632, Dec. 2023, doi: 10.51519/journalisi.v5i4.583.

[3] M. Ilić, V. Mikić, L. Kopanja, and B. Vesin, “Intelligent Techniques in E-learning: A Literature Review,” Artificial Intelligence Review, vol. 56, no. 12, pp. 14907–14953, 2023. doi: 10.1007/s10462-023-10508-1.

[4] M. M. A. Parambil, J. Rustamov, S. G. Ahmed, Z. Rustamov, A. I. Awad, N. Zaki, and F. Alnajjar, “Integrating AI-based and Conventional Cybersecurity Measures into Online Higher Education Settings: Challenges, Opportunities, and Prospects,” Computers & Education: Artificial Intelligence, vol. 7, Art. no. 100327, 2024. doi: 10.1016/j.caeai.2024.100327.

[5] O. Afolalu and M. S. Tsoeu, “Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions,” Future Internet, vol. 17, no. 12, Art. no. 575, 2025. doi: 10.3390/fi17120575.

[6] S. E. Arias Calderón, F. J. Villarroel Córdova, B. R. Ureña Zúñiga, and Y. B. Aman Collaguazo, “Análisis de Vulnerabilidades en Moodle: Una Revisión Sistemática sobre Seguridad en LMS,” Arandu UTIC, vol. 12, no. 1, pp. 4090–4105, 2025. doi: 10.69639/arandu.v12i1.859.

[7] S. A.-L. Akacha and A. I. Awad, “Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders,” Sustainability, vol. 15, no. 19, Art. no. 14132, 2023. doi: 10.3390/su151914132.

[8] N. S. Alotaibi, “The Impact of AI and LMS Integration on the Future of Higher Education: Opportunities, Challenges, and Strategies for Transformation,” Sustainability, vol. 16, no. 23, Art. no. 10357, 2024. doi: 10.3390/su162310357.

[9] V. Baneș, C. Ravariu, B. Appasani, and A. Srinivasulu, “A Novel Two-Factor Authentication Scheme for Increased Security in Accessing the Moodle E-Learning Platform,” Applied Sciences, vol. 13, no. 17, Art. no. 9675, 2023. doi: 10.3390/app13179675.

[10] S. Watini, G. Davies, and N. Andersen, “Cybersecurity in Learning Systems: Data Protection and Privacy in Educational Information Systems and Digital Learning Environments,” International

Transactions on Education Technology (ITEE), vol. 3, no. 1, pp. 26–35, 2024. doi: 10.33050/itee.v3i1.665.

[11] T. T. Sulaiman, “A Systematic Review on Factors Influencing Learning Management System Usage in Arab Gulf Countries,” Education and Information Technologies, vol. 29, no. 2, pp. 2503–2521, 2024. doi: 10.1007/s10639-023-11936-w.

[12] Verizon Business, Data Breach Investigations Report (DBIR) 2025, Verizon Business, Apr. 2025. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[13] European Union Agency for Cybersecurity (ENISA), Cybersecurity in Education: Challenges and Opportunities, Athens, Greece: ENISA, Nov. 2024. [Online]. Available: https://www.enisa.europa.eu/

[14] S.-F. Wen, A. Shukla, and B. Katt, “Artificial Intelligence for System Security Assurance: A Systematic Literature Review,” International Journal of Information Security, vol. 24, Art. no. 43, 2025. doi: 10.1007/s10207-024-00959-0.

[15] Z. T. Pritee, M. H. Anik, S. B. Alam, J. R. Jim, M. M. Kabir, and M. F. Mridha, "Machine Learning and Deep Learning for User Authentication and Authorization in Cybersecurity: A State-of-the-Art Review," Computers & Security, vol. 140, Art. no. 103747, 2024. doi: 10.1016/j.cose.2024.103747.

[16] A. Alzahrani, N. Alharbi, and A. Alshahrani, “A Survey on Machine LearningBased User Authentication and Intrusion Detection Systems: Challenges and Future Directions,” IEEE Access, vol. 12, pp. 1–15, 2024.

[17] G. Siemens, “Learning Analytics: The Emergence of a Discipline,” American Behavioral Scientist, vol. 57, no. 10, pp. 1380–1400, 2013. doi: 10.1177/0002764213498851.

[18] S. W. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[19] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2024, Athens, Greece: ENISA, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[20] S. Mohamed Alhidaifi, M. R. Asghar, and I. S. Ansari, "A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions," ACM Computing Surveys, vol. 56, no. 8, Art. 196, 2024. doi: 10.1145/3649218.

[21] M. Husák, J. Komárková, E. Bou-Harb, and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 640–660, 2019. doi:

[22] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges," Cybersecurity, vol. 2, no. 1, Art. no. 20, 2019. doi: 10.1186/s42400-019-0038-7.

[23] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, X. Bellekens, and R. Atkinson, "A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets," Future Internet, vol. 12, no. 10, Art. no. 318, 2020. doi: 10.3390/fi12100318.

[24] S. Vyas, V. Mavroudis, and P. Burnap, "Towards the Deployment of Realistic Autonomous Cyber Network Defence: A Systematic Review," ACM Computing
Surveys, vol. 58, no. 1, Art. no. 5, 2025. doi: 10.1145/3729213.

[25] S. Khan, C. Devlen, M. Manno, and D. Hou, "Mouse Dynamics Behavioral Biometrics: A Survey," ACM Computing Surveys, vol. 56, no. 6, Art. no. 154, 2024. doi: 10.1145/3640311.

[26] S. M. Kasongo and Y. Sun, "A Deep Learning Method with Wrapper Based Feature
Extraction for Wireless Intrusion Detection System," IEEE Access, vol. 8, pp. 57837–57845, 2020,

[27] Z. Pan, L. Biegley, A. Taylor, and H. Zheng, "A Systematic Review of Learning Analytics Incorporated Instructional Interventions on Learning Management Systems," Journal of Learning Analytics, vol. 10, no. 3, 2023. doi: 10.18608/jla.2023.8093.

[28] C. Wang, H. Tang, H. Zhu, J. Zheng, and C. Jiang, "Behavioral Authentication for Security and Safety," Security and Safety, vol. 3, Art. no. 2024003, 2024. doi: 10.1051/sands/2024003.

[29] A. H. Ali, M. Charfeddine, B. Ammar, B. Ben Hamed, F. Albalwy, A. Alqarafi, and A. Hussain, "Unveiling Machine Learning Strategies and Considerations in Intrusion Detection Systems: A Comprehensive Survey," Frontiers in Computer Science, vol. 6, Art. no. 1387354, 2024. doi: 10.3389/fcomp.2024.1387354.

[30] D. Vergara, G. Lampropoulos, Á. Antón-Sancho, and P. Fernández-Arias, "Impact of Artificial Intelligence on Learning Management Systems: A Bibliometric Review," Multimodal Technologies and Interaction, vol. 8, no. 6, Art. no. 62, 2024. doi:

10.3390/mti8060062.

[31] E. Bertino, “Zero Trust Security: An Enterprise Guide to Architecture and Implementation,” IEEE Security & Privacy, vol. 20, no. 5, pp. 14–21, 2022.

[32] International Telecommunication Union (ITU-T), “Threat Analysis and Guidelines for Securing Password and Passwordless Authentication Solutions,” ITU-T Recommendation X.1283, Sep. 2024.

[33] S. W. Rose, M. B. Jones, O. Borchert, and S. M. Mitchell, Digital Identity Guidelines, NIST Special Publication 800-63, Revision 4. Gaithersburg, MD, USA: National Institute of Standards and Technology, Aug. 2025. doi: 10.6028/NIST.SP.80063-4.

[34] D. Giarimpampa, R. Meier, T. F. Bissyandé, V. Lenders, and J. Klein, "Exploring the Role of Artificial Intelligence in Enhancing Security Operations: A Systematic Review," ACM Computing Surveys, vol. 58, no. 3, Art. 66, 2025. doi: 10.1145/3747587.

[35] P. Melzi, C. Rathgeb, R. Tolosana, R. Vera-Rodriguez, and C. Busch, "An Overview of Privacy-Enhancing Technologies in Biometric Recognition," ACM Computing Surveys, vol. 56, no. 12, Art. 310, 2024. doi: 10.1145/3664596.