AI-Based Detection of Anomalous User Behavior in Moodle: A Literature Review on E-Learning Security

Ms. Jisha Krishnan K[1], Dr Arun Mozhi Selvi [2]

[1]PhD Scholar British University College, UAE
[2]Supervisor&Professor British University College, UAE

---***---

Abstract - The growing reliance on web-based education has positioned Learning Management Systems (LMS) such as Moodle at the center of educational operations. However, this trend exposes institutions to the threat of insider threats, meaning entities such as students, teachers, or administrators. Such threats involve unauthorised behaviour and grade hacking. This review of literature discusses 10 insider threat detection studies from learning contexts, focusing on the integration of user behaviour analytics (UBA) and artificial intelligence (AI). The survey also highlights the need for simulation-based models for normal and malicious behaviour modeling and serves as the basis for an AI-based detection system on LMS platforms like Moodle .

1. INTRODUCTION

The evolution of educational technology has transformed the traditional into a colourful,technology integrated learning environments. Among these technologies, Learning Management Systems (LMS) such as Moodle, Blackboard, and Canvas have emerged as indispensable tools in school,university and training organization management and delivery of education.

Moodle, in particular, is widely employed due to its open-source nature, customizable design, and strong course management,test support,and communication among learners. While LMS systems have revolutionized learning by encouraging accessibility, flexibility, and interactivity , also brought along serious cybersecurity issues.

First among them is the insider threat problem. Insider thre ats are posed by legitimate system users-students, teachers, administrators-misusing their legitimate access either intentionally or inadvertently.Some examples include unauthorized viewing of test questions, grade manipulation checking plagiarism, or data exfiltration. In most instances , such actions go unnoticed because of the built-in trust in these users and the minimal monitoring facilities in the LMS .

Unlike conventional external cyberattacks, which are generally met with responses via common security measures like firewalls and intrusion detection systems, internal attacks are more difficult and insidious.That typically involve behavior that is generally acceptable within context but departs from the normal habits of a user ,which become difficult to detect with rule-based systems alone. The most LMS environments lack real-time behavior analysis capability which makes proactive response to anomalies even more challenging.

With a view to overcoming these limitations, researchers and security professionals are increasingly exploring the synergy of Artificial Intelligence (AI) and User Behavior Analytics (UBA) in threat detection. UBA deals with profiling the normal user behavior and identifying anomalies that may be indicative of a security threat. When powered by machine learning algorithms, UBA systems can learn from historical activity, adapt to shifting patterns, and notify on behavior that deviates significantly from the norm. This approach is particularly thrilling in the context of LMS platforms, where structured log data—login times, access to resources, submission patterns, and navigation paths—can be leveraged to build intelligent detection models.

2. BACKGROUND AND KEY CONCEPTS

Learning Management Systems like Moodle now find themselves in the center of electronic learning with presentation functionality, grading, and user tracking . Along with greater acceptance comes increased cybersecurity concerns—predominantly insider threats due to legitimate users such as students or teachers misusing their authority to perform malicious or negligent operations. Common examples are unauthorized grading adjustments, leakage of data, and course activity manipulation.

Typical security controls like access controls or rule based static monitoring-generally fail to detect such attacks, especially when they have been crafted to mimic normal user behavior. This limitation has prompted the implementation of User Behavior Analytics (UBA), which monitors patterns in user behavior to detect anomalies.LMS systems , and Moodle specifically, provide rich logs (e.g., via mdl_logstore_standard_log) that can be harvested for behavior profiling.

Artificial Intelligence (AI), particularly machine learning , enhances UBA by enabling the system to learn patterns of behavior and identify outliers with minimal human involvement. Supervised and unsupervised learning approaches have been applied to threat detection tasks in various domains, including education .Because it is challenging to acquire actual insider threat information, simulation-based modeling is commonly used to emulate normal and adversarial behavior within LMS contexts. These technologies are used as a whole as the foundation to develop adaptive AI-driven threat detection systems in Moodle and other related platforms.

3. LITERATURE REVIEW

This review of literature took a sytematic and organized approach to search for, investigate, and merge relevant studies relevant to the detection of insider threats within e-learning environments, such as Moodle, User Behavior Analytics (UBA), and Artificial Intelligence (AI) solutions .

Yuan and Wu (2020) have a comprehensive overview of applying deep learning techniques to insider threat detection, a long-standing and costly cybersecurity issue. The authors argue that traditional machine lerning approaches, which rely mainly on feature engineering, fail to address high-dimensional, sparse, and complex behavioral data from insider activity. They review various deep learning models such as RNNs, CNNs, and GNNs that are proven to yield improved performance in identifying subtle and adaptive insider activities. However, the research also identifies crucial challenges such as data sparsity, lack of labelled instances, and explainability issues. Notably, the authors make recommendations for future research directions that encompass self-supervised learning, few-shot learning, and explainable AI to build the area further.This poll creates an excellent foundation for the understanding of how deep learning can help to further deepen the detection and prevention of insider threats in current digital environments.

Tao et al. (2025) propose an innovative insider threat detection model that integrates Test-Time Training (TTT) with an altered Residual Network architecture with the assistance of an Efficient Channel Attention (ECA) mechanism.Their system , which they name as TTT-ECA-ResNet, is especially designed to overcome constraints of the traditional RNNs and CNNs by identifying long-range and short-range dependencies in behavioral data. TTT enhances the ability of the model to learn adaptive hidden state representations by self-supervised learning at inference time, while the ECA-ResNet is intended to maximize channel-wise attention to better extract local patterns. On testing on the CMU CERT dataset, the model achieved an AUC score of 98.75% and F1-score of 96.81%, which surpassed traditional deep learning baselines such as LSTM, GRU, and even Transformer based variants such as ITD-BERT. This paper highlights the importance of hybrid temporal modeling and channel attention mechanisms to improve detection accuracy and recall. It also points out data imbalance and dynamic insider behavior issues , proposing avenues in model generalizability and low-latency deployment .

Singh and Kumar (2023) speak about growing cybersecurity concerns of modern e-learning portals , indicating their exposure to cyber threats in the form of data breaches, phishing, and malware attacks. The article emphasizes the necessity of cybersecurity for protecting confidential educational data, system integrity, and users' trust. It takes the Blackboard Learn intrusion as a case study to illustrate how vulnerabilities in authentication mechanisms and weak password policies can lead to large-scale data breaches. Furthermore, the study proposes a multi-layered security strategy that includes multi-factor authentication, secure coding, encryption, user training, and proactive patching. The authors also briefly discuss emerging technologies like Blockchain for secure credentialing and AI/ML for threat detection based on behavior , highlighting how they can transform cybersecurity in digital learning platforms. This paper contributes a socio-technical perspective to securing educational platforms, positioning cybersecurity as a pre-condition for the sustainability and integrity of digital learning ecosystems.

Baig and Yadegaridehkordi (2025) investigate the determinants of academic staff satisfaction with and the continued use of Generative AI (GenAI) tools in higher education. Drawing on the Unified Theory of Aceptance and Use of Technology (UTAUT) and the Expectation Confirmation Model (ECM), the study diagnoses significant constructs such as performance expectancy, ethical awareness, security and privacy, and facilitation conditions. According to data collected from 127 Pakistani open university teaching staff, the study identifies that usability , compliance with ethical standards, and data security perception play a decisive role in satisfaction with GenAI. Significantly, performance expectancy drives intention to utilize GenAI but is not correlated with satisfaction with GenAI—suggesting that experience and trust are more suitable predictors of continuous use. The paper recommends actionable advice for policymakers and institutions, advocating adaptive GenAI tools, robust support systems, and responsible AI deployment. It contributes a nuanced explanation of GenAI adoption in academia, emphasizing the simultaneous presence of technological affordances and user-centered determinants in shaping adoption patterns.

Hijji and Alam (2022) examine the evolving cybersecurity threats to organizations from the shift toward remote work during and after the COVID-19 pandemic .They introduce the Cybersecurity Awareness and Training (CAT) framework, with the purpose of evaluating and enhancing employees' cybersecurity capability. Following the NIST standards and using AI approaches like machine learning and natural language processing, the model is comprised of three levels—awareness, training, and assessment—each divided into particular practices. The authors demonstrate the CAT model by case studies in cybersecurity firms , provig its applicability to identify gaps in employees' skills and improve organizational readiness. By the incorporation of adaptive measurement of knowledge and means like gamification and simulation, the framework spans technological solutions with human factors in behavior. This research contributes a systematic, AI-powered approach to cybersecurity education for remote work environments encouraging awareness and training as core components of organizational resilience.

László Bognár and László Bottyán (2024) ,suggested a robust,empirically sound questionnaire to examine the behavior determinants that shape student's cybersecurity conduct. Their research utilized a comprehensive framework that applied both Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) to give confidence about the reliability and construct validity of the tool .Using this two-methods framework allowed the authors to elicit the nuanced aspects of cybersecurity awareness and behavior of university students.Furthermore, the study broadened its scope to examine differences in cybersecurity behavior along gender, age, discipline of study, and culture. Results revealed significant differences between practice and awareness, and it was clear that cybersecurity behavior was a product of several socio-demographic factors. These findings

concur with the perception that programs for educating and intervening on cybersecurity must be designed to leverage different students' experiences to better impact awareness programs in institutions of higher learning.

Haywood Gelman,John D. Hastings ,David Kenley , and Eleanor Loiacono (2024).Insider threats (InTs) , as regards their relatively low occurrence , pose a highly serious risk to information systems and organizational infrastructure.InT research crosses various disciplines like psychological, technical, and educational research .InT research has probed behavioral and cognitive indicators of insider risk in psychological research, while technical research has focused on detection tools like machine learning algorithms,user monitoring, and anomaly detection systems.Educational interventions, although less frequently discussed, aim to cultivate prevention and awareness skills via professional training courses.Where the majority of the literature has centered on detection and prevention strategies, comparatively few have identified training interventions based on psychological understanding, such as tracking behavioral indicators and promoting risk-aware attitudes.In an attempt to fill this gap, a series of recent reviews have tried to bring knowledge together from these diverse fields. For example, Johnson et al. (2022) conducted one of the earliest comprehensive reviews that systematically organized insider threat studies from psychological, technical, and educational perspectives. The findings highlight the imperative for behaviorally grounded training platforms that integrate these fields so that there is a better-rounded approach to avoiding insider threats.

Harjinder Singh Lallie, Andrew Thompson, Elzbieta Titis, and Paul Stephens (2023) provides specialized examination of the international education sector's cybersecurity threats, including universities, colleges, and schools . They examine the timeline of cyberattacks in an orderly fashion and with particular reference to the insider threat posed by students .According to the findings of fifty-eight documented attacks, the authors conclude that ransomware is the most prevalent external threat and hacking for financial reasons is the most common category of internal attack. The research not only identifies the susceptibility of schools to internal and external threats but also necessitates tailored mitigation strategies. The authors propose a multi-dimensional strategy, combining technical controls, policy interventions, and behavior monitoring, to enhance cybersecurity resilience . The research provides a valuable addition to the literature in bridging the research gap between threat analysis and actionable advice with a robust focus on the potential insider threat capability of students.

Nauman Nazar, Iman Darvishi, and Abel Yeboah-Ofori (2022) criticallyexamined the security and privacy concerns of widely used online learning tools such as Zoom, Google Meet, Microsoft Teams, and Cisco Webex. Their study aimed to ascertain the vulnerability level of these tools to cyberattacks and the protection level they offer to user data. The research employed a phased deployment method with virtualization environments, wherein three virtual machines (Windows and Linux) were established using Parallels Desktop to simulate an actual communication setting for testing the platforms . In setting up the experiment, the researchers downloaded and installed the target online learning tools into the virtual machines and tested them with a man-in-the-middle (MitM) attack with ARP poisoning. They recorded and analyzed meeting packets with Wireshark to test security measures on both platforms .What they discovered was that both platforms encrypt data at rest but that zoom is the only one that necessitates explicit configuration to turn on encryption , leaving customers open to exposure if defaults are not altered. Further, Zoom allows anonymous sign-ins,which can be a security concern if not offset by controls such as waiting rooms and meeting passwords.

In contrast, Cisco Webex differentiated itself by offering solid end-to-end encryption through a proprietary key management system to complement its overall security position. The study points out the urgent need for secure default configurations, user awareness,and organizational controls toward making secure the use of such platforms within academic settings. This work is part of the growing literature that puts considerable weight on the cybersecurity defecits in distance learning infrastructures, particularly as their reliance becomes increasingly robust worldwide.

Lourdes Cecilia Ruiz Salvador, Carlos Lenin Alvarez Llerena, and Dr. Huu Phuoc Dai Nguyen (2021) mention the growing cybersecurity challenges under digital learning , with greater reliance on online media for education. Their study highlights various cyber threats such as data breaches, phishing, and malware infection that endanger the integrity of educational systems as well as the security of user data.The authors state that a majority of online

learning sites lack proper security features, making them vulnerable to expllitation . Inadequate password habits and insider threats, including unauthorized access by users from within the education field , also heighten these risks.To minimize these threats, the study study identifies the importance of incorporating good authentication techniques, such as multi-factor authentication (MFA), and initiating cyber awareness training within both students and instructors to allow them to recognize and counter potential threats.Further, the study promotes safe, regularly updated platforms to enhance online learning security .Encrypted safeguarding of confidential data, imposition of access control, and regular backup of data are also proposed as prime strategies. Preemptive planning for cyber incident response is highlighted by the authors in order to be able to deal with and bounce back from likely attacks in an optimal manner. This research offers significant contributions to education cyber resilience discourse , yielding practical recommendations that will strengthen institutional cybersecurity measures.

Mei Song (2022) discusses the significant role played by insider threats, both intentional and unintentional , in organizational cybersecurity risks . Insider threats can result in data breaches , economic loss and reputational damage and hence are a high-interest research topic in cybersecurity. The study emphasizes the growing need to incorporate Explainable Artificial Intelligence (XAI) in cybersecurity systems as a means to improve threat detection , achieve more transparency , and build user trust.XAI's ability to generate interpretable explanations of complex AI-driven threat detection systems is particularly valuable in environments where insights into the rationale for alerts are required to make fully informed decisions . Nevertheless, Song (2022) posits several challenges associated with the successful deployment of XAI in cybersecurity. These include the trade-off between model accuracy and interpretability, the requirement for representative and high-quality data sets, and the difficulty in integrating XAI technologies with existing cybersecurity systems.This research contributes to the embryonic literature on the use of human-centered AI in cybersecurity, and more precisely in mitigating insider threats, by emphasizing the interplay between technological effectiveness and user comprehensibility. It argues that overcoming current limitations on the adoption of XAI is crucial to enabling its broader implementation in real-world security operations.

4. DISCUSSION

The literature under consideration indicates a trend towards using artificial intelligence (AI) and user behavior analytics (UBA) to detect insider threats in e-learning platforms. While traditional rule based approaches have established the basis for threat identification, there is a visible trend towards more dynamic and intelligent detection mechanisms through the implementation of machine learning (ML) and deep learning (DL) techniques.Shift from Static to Intelligent Models.Past research primarily discussed rule-based detection systems with predetermined rules , formulated on static patterns of activity or access intrusions to trigger alarms . These types of systems are not that effective at learning new user behavior or at identifying weak anomalies. Recent literature, particularly post-2019, shows a paradigm shift towards machine learning and behavior-based analytics. Techniques such as supervised learning (e.g., SVM, Random Forest), unsupervised models (e.g., Isolation Forest, K-means), and deep learning architectures (e.g., Autoencoders, RNNs) have shown promising results in identifying malicious insider activity with improved accuracy and reduced false positives.

Greater Simulation and Synthetic Data Use

Due to the sensitive nature of insider threat data , some studies utilized mock data sets or simulated activity of users to train and validate their models.Although this practice is necessary, it questions real-world deployability and generalizability .Few studies validated their models on real Moodle or LMS data sets, which creates difficulties for researchers when practical, deployable solutions are needed .

Underutilization of Moodle-Specific Features

Despite the widespread usage of Moodle and the robust logging capability , there are not many studies centered on Moodle as a platform. Out of the 10 papers that were reviewed very few made use of Moodle's mdl_logstore_standard_log or APIs for behavior tracking. This indicates a major flaw in Moodle-centric insider threat research, especially using real-time data streams and log-based behavior modeling.

Absence of Real-Time Detection Frameworks

Another key gap found is the lack of real-time detection models. Most of the work presented herein falls under offline analysis of log data or post-event anomaly detection. There is a clear requirement for models that can perform near real-threats are occurring.

Data and Evaluation Limitations

A universal flaw in a broad variety of studies is that there is no unified , openly available dataset for insider threat detection based on LMS.This hinders reproducibility as well as cross-model comparison. In addition, some studies use outdated or very simplified metrics for testing that do not capture the total effectiveness of proposed methods in real-world scenarios.

5. FUTURE WORK

The proposed framework, as represented in Figure 1, presents an initial model for AI and user behavior analytics-based insider threat detection in Moodle-based e-learning systems .In the future , the research will focus on applying and testing the proposed framework within a simulated Moodle environment set up on XAMPP.

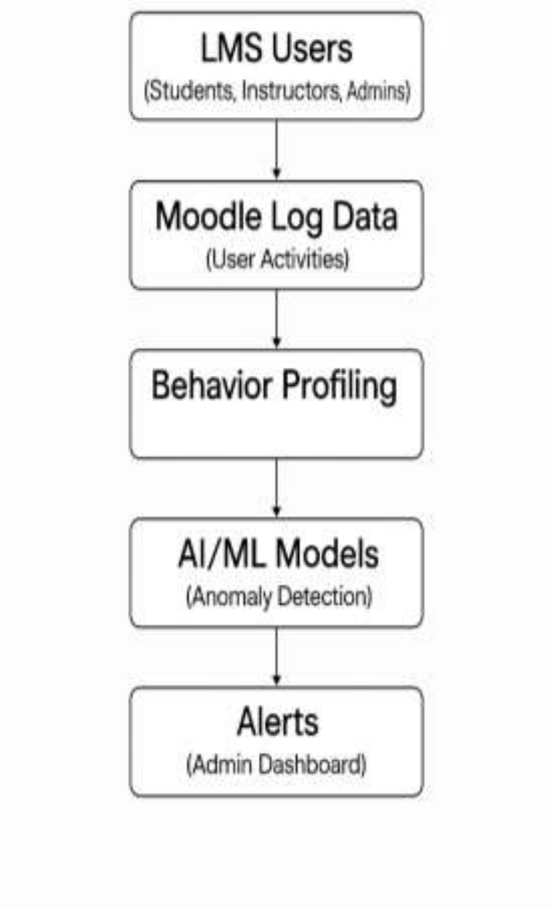

Figure 1. AI-Based Detection of Anomalous User Behavior in Moodle

The first step will be to deploy Moodle to generate and track diverse user interactions among administrators , teachers, and students. These interaction logs will be analyzed by a user behavior analysis tool capable of extracting behavioral patterns to be fed into machine learning analysis.Various supervised and unsupervised machine learning models will be trained to identify anomalous behavior indicating potential insider threats.

Future research will also study the ability to implement and design a continuous monitoring system that can process in near real-time in order to facilitate timely threat detection and response. Special care will be taken when deploying the anomaly detection module using combination of real and synthetic datasets in order to enhance model robustness. An explainable AI (XAI) layer may also be incorporated in order to ensure that decisions produced by the system are transparent and comprehensible by system administrators.Finally, the framework will be tested for scalability , flexibility across other LMS systems, and its viability of real-world application in schools. Care will also be taken to address ethical concerns such a data privacy,informed consent, and minimizing bias in behavioral profiling.

6. CONCLUSION

The increasing reliance on Learning Management Systems like Moodle has brought unprecedented improvements to the provision of education, but it also comes with complex cybersecurity challenges chiefly insider threats. This literature review discussed the latest research on the use of Artificial Intelligence (AI) and User Behavior Analytics (UBA) in detecting insider threats in online learning environments.While different studies give promising altern atives using supervised and unsupervised learning approaches ,there is still little substantial effort in xisting literature.Specifically, there is a critical lack of research utilizing Moodle's rich logging architecture , little employment of real-time or near real-time threat detection, and lack of simulation-based models that can help counter the shortage of labeled insider threat data. Additionally,most current frameworks do not enable realistic deployment strategies tailored to a academic institutions with open-source LMS architectures.In order to overcome these weaknesses, this paper proposes a simulation-based AI model that integrates behavior profiling, anomaly detection, and Moodle-specific data gathering for detecting potential insider threats. The proposed method has the capability to significantly improve early detection of malicious or unusual behavior by simulating normal and adversarial user behavior.

REFERENCES

[1] Yuan, S., & Wu, X. (2020). Deep learning for insider threat detection: Review, challenges and opportunities. Computers & Security, 99, 102087. https://doi.org/10.1016/j.cose.2020.102087

[2] Tao, X., Liu, J., Yu, Y., Zhang, H., & Huang, Y. (2024**).** An insider threat detection method based on improved test-time training model. High Confidence Computing, 4, 100283. https://doi.org/10.1016/j.hcc.2024.100283

[3] Singh, B., & Kumar, B. (2023). Enhancing cyber security in e-learning portals: Challenges and solutions. Educational Administration: Theory and Practice, 29(4), 1581–1586. https://doi.org/10.53555/kuey.v29i4.6502

[4] Baig, A., & Yadegaridehkordi, E. (2025). Factors influencing academic staff satisfaction and continuous usage of generative artificial intelligence (GenAI) in higher education. International Journal of Educational Technology in Higher Education, 22(5). https://doi.org/10.1186/s41239-025-00506-4

[5] Hijji, M., & Alam, G. (2022). Cybersecurity awareness and training (CAT) framework for remote working employees. Sensors, 22(22), 8663. https://doi.org/10.3390/s22228663

[6] Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. Education Sciences, *14*(6), 588. https://doi.org/10.3390/educsci14060588

[7] Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2023). Understanding cyber threats against the universities, colleges, and schools. arXiv. https://doi.org/10.48550/arXiv.2307.07755

[8] Nazar, N., Darvishi, I., & Yeboah-Ofori, A. (2022). Cyber threat analysis on online learning and its mitigation techniques amid COVID-19. In 2022 IEEE International Smart Cities Conference (ISC2) (pp. xx–xx). IEEE. https://doi.org/10.1109/ISC255366.2022.9922102

[9] Song, M. (2022). Explainable AI in identifying and preventing insider threats. ResearchGate. https://www.researchgate.net/publication/387225177_Explainable_AI_in_Identifying_and_Preventing_Insider_Threats

[10] Ruiz Salvador, L. C., Alvarez Llerena, C. L., & Nguyen, H. P. D. (2021). Digital education: Security challenges and best practices. Security Science Journal, 2(2), Article 4. https://doi.org/10.37458/ssj.2.2.4

[11] National Institute of Standards and Technology (NIST) – Cybersecurity Framework NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

[12] Educause – Security in Higher Education EDUCAUSE. (2022). Cybersecurity and privacy in higher education. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program

[13]Open Web Application Security Project (OWASP) – LMS Security Risks
OWASP. (2023). E-Learning Platforms Security Guidelines. https://owasp.org/www-project-top-ten-for-lms

[14] EDUCAUSE Review Article Smith, M. (2023). AI and Privacy in LMS: Where We Are and What's Next. EDUCAUSE Review. https://er.educause.edu/articles/2023/09/ai-and-privacy-in-lms-where-we-are-and-whats-next