iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.83268

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Role-Aware Behavioural Analytics for Insider Threat Detection in Learning Management Systems

Jisha Sreenath[1], Dr. Arun Mozhi Selvi[2]
Data and Cybersecurity, British Training Center, Ajman, UAE

Abstract: ***The rapid increase in LMS use in educational systems has enabled greater access to and flexibility in digital learning opportunities (e-Learning). But the increased use of these learning environments has also introduced new cybersecurity challenges, particularly regarding insider threats. Insider threats can come from authorized users, such as students, teachers, and administrators. Unlike external cyberattacks, detecting an insider threat is more difficult, since the bad actor (the person committing the act) will normally be using their legitimate credentials and typical access privileges to commit the malicious act. Traditionally, most technologies for detecting insider threats in LMSs use general anomaly-detection processes in their design and place limited focus on the behavioral differences associated with specific roles and task types.***

The proposed research study presents a behavioral analytics framework for detecting insider threats in LMS's based on the behavioral characteristics of students and teachers. This framework uses interaction logs and activity data collected from the Open University Learning Analytics Dataset (OULAD) to produce a comparative evaluation of both groups' behavioral characteristics. Analysis of behavioral indicators, such as logon frequency, session duration, resource access behavior, abnormal access time periods, and excessive downloads, was conducted to establish behavioral profiles for both user types and determine what constitutes "normal" behavior versus "anomalous" behavior. One of the most critical components of this framework is the inclusion of a behavioral labeling mechanism based on role to improve understanding of the context regarding a suspicious action within LMS's. The purpose of this research is to improve the ability to identify suspicious behaviors within an organization using context and behavior-based intelligent methods.

Keywords: Insider Threat Detection, Behavioral Analytics, Learning Management System (LMS), Cybersecurity, Role -Aware Analysis.

I. INTRODUCTION

With the proliferation of digital learning and online learning platforms, modern educational systems have undergone a significant transformation. Most of these educational institutions use Learning Management Systems such as Moodle, Canvas, and Blackboard to provide courses, deliver assessments, communicate, and track student activities. Educational institutions widely use Learning Management Systems (LMS) because they provide environments with greater accessibility, scalability, and flexibility.

With the growing use of LMS, new significant cybersecurity threats have emerged. LMS systems contain sensitive data such as student records, assessment data, course materials, examination content, and communication records; thus, they are attractive targets for attackers. Cyberattacks, data breaches, and unauthorized activities can pose major security threats to learning management systems. Although external cyberattacks pose a major threat to online learning systems, insider threats are among the most critical problems in cybersecurity.

Insider threat is a threat originating within a system (e.g., a student, instructor, administrator, or staff member). Insiders may or may not intentionally misuse their system privileges and steal or change data, modify student grades, bulk download materials, misuse privileges, or access unauthorized data/information. An insider threat cannot be easily detected, unlike an outside threat, because an insider will use valid credentials and appear normal.

Current methods of insider threat detection rely on rules or static access control models and are often unable to detect anomalous activities in LMSs. With advancements in Artificial Intelligence, machine learning, and behavioral analytics, there are new opportunities to identify suspicious user behavior by analyzing user activity. Behavioral analytics is an analysis method for user activity, such as access logs, system logs, usage logs, and login details, to distinguish normal from anomalous activities.

Many studies have proposed methods to detect insider threats in LMS using machine learning or anomaly detection. However, research on role-based behavioral models to detect insider threats in the education environment is limited. Many research papers analyze behavior using general assumptions that apply to all user types, without differentiating between students, instructors, and administrators.

©IJRASET: All Rights are Reserved

In fact, the expected behavior is varied with respect to the role, for example: student behavior of accessing the gradebook is suspicious, but instructor accessing the gradebook could be normal, student downloading too much material could be anomalous, but instructor could be normal, and many others.

In this research, a role-aware behavioral analytics framework to detect insider threats in the Learning Management System is proposed. The framework analyzes individual behaviors in a role-based and interactive way. In this study, behaviors are observed using the Open University Learning Analytics Dataset (OULAD) to examine indicators such as login frequency, login duration, resource access behaviors, assessment interaction behaviors, and unusual activities.

The core contribution of this research is a novel role-aware anomaly analysis for insider threat detection in online learning environments, aimed at increasing understanding of human behavior. The aim is to help educational institutions increase their cybersecurity and minimize the risk of insider threats.

II. LITERATURE REVIEW

The rapid evolution and adoption of Learning Management Systems (LMSs) have revolutionized education by making learning more flexible, accessible, and technology-enabled. This growth has brought new cybersecurity issues, such as phishing, unauthorized access, malware distribution, and insider attacks, to light. Of these attacks, those launched by authorized users are considered the most damaging because they already have the privileges needed to access sensitive information. Therefore, educational institutions are looking to implement intelligent cybersecurity measures to effectively identify anomalies in user behavior in LMSs [1].

Initial research for detecting insider threats concentrated on rule-based systems and static access control procedures. Such mechanisms could recognize predefined malicious patterns and security violations, but failed to detect sophisticated behavioral anomalies and attack patterns. As a consequence of typical insider threats utilizing stolen but genuine login credentials, conventional signature-based approaches that tend to mistake anomalous behavior as a standard user activity were inadequate, and the research has shifted towards using artificial intelligence (AI), machine learning, and behavioral analytics for anomaly detection and insider threat detection [2].

Behavioral analysis techniques are used to investigate patterns in users' interactive behavior and identify deviations from their typical behavior. Past research has shown that studying indicators of user behavior, such as login frequency, session length, patterns of accessing various resources, and interaction history, can improve the performance of an anomaly detection system in a digital environment [3]. The analysis of behavioral aspects is appropriate for the educational environment, as interaction logs from an LMS platform provide sufficient information about student and tutor actions, assessment results, communications, and learning activities [4].

A few studies have used various machine learning algorithms to detect insider threats. Ensemble learning algorithms, such as Random Forest (RF), are robust for high-dimensional behavioral datasets and classification problems due to their efficiency and interpretability [5]. Isolation Forest (IF) has proven to be widely useful for anomaly detection, as it helps isolate anomalies regardless of the data labels [6]. Moreover, combining supervised and unsupervised algorithms in various ways can improve anomaly detection and reduce the false-positive rate [7].

Recent research efforts are also focusing on deep learning-based and sequential behavioral analysis methods for predicting insider threat, particularly by analyzing the sequence of user behavior so the system can adapt to changing malicious user behavior [8]. Oversampling techniques such as Synthetic Minority Over-sampling Technique (SMOTE) and Adaptive Synthetic Sampling (ADASYN) are also used to minimize class imbalance [9].

The Open University Learning Analytics Dataset (OULAD) is the most commonly used dataset for studying student behavior and interactions in an online learning environment. OULAD consists of learner data on personal demographics, interaction with course activities, assignments, and the Virtual Learning Environment. Researchers have used OULAD to study learning analytics, predict student performance, investigate behavior, and analyze anomalies [10]. Very few studies have been published on using OULAD to detect insider threats in the LMS environment.

Existing solutions for insider threat detection in LMS are lacking in several respects. Mostly, the focus is on general anomaly detection with very little attention to role-based behavioral deviations. This is because most students, teachers, and administrators are treated similarly in terms of their behavior. It is important to acknowledge that user expectations regarding their behavior may differ from those of students, teachers, and administrators. So what might be normal behavior for a student might be suspicious to a teacher, and vice versa [11].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Role-aware behavioral analysis is thus required in educational settings for accurately detecting insider threats. In this study, a framework for role-aware behavior analysis that classifies normal and anomalous behaviors of students and teachers in the LMS environment is presented.

III. RESEARCH GAP

In recent years, the dramatic proliferation of digital learning environments and Learning Management Systems (LMSs) has also significantly heightened concerns around cybersecurity risks in education. Contemporary LMS systems store large volumes of sensitive academic data, such as test scores, student information, learning resources, and institution-wide communication logs. Consequently, these systems have become an attractive target for both malicious external actors and malicious insiders [1]. While external threats such as viruses, phishing schemes, and network intrusions have received extensive research attention, insider threats remain among the hardest cyber threats to identify due to their occurrence within authorized access [2].

Recent advancements in artificial intelligence (AI) and machine learning have enabled intelligent anomaly detection systems that can monitor and distinguish between normal and anomalous user behavior [3]. The application of machine learning algorithms, behavioral profiling, and anomaly detection systems in both organizational and enterprise security environments has been well studied [4]. Similarly, behavioral analysis has emerged in education to track learner interactions, predict academic achievement, and monitor engagement in digital learning systems [5].

Despite significant strides in insider threat detection, current approaches implemented in LMS systems face several key research limitations. While much current research aims to maximize the accuracy of anomaly detection using machine learning algorithms, little emphasis has been placed on context-specific behavioral differences across user roles in an LMS environment [6]. In many situations, users are not analyzed by role but as a monolithic group. However, the nature of student, teacher, and administrative user behavior varies widely across an LMS due to their differing privileges and interaction requirements. This lack of role-specific behavioral understanding increases the potential for both misinterpreting malicious behavior and failing to detect it [7]. For example, a teacher who frequently accesses or modifies student grades may be perceived as malicious, whereas a student who accesses or modifies grades is clearly unauthorized. Also, activities like large downloads of learning resources or unusual activity patterns at certain hours may not pose the same level of risk when performed by a teacher as by a student [7]. Generalized anomaly detection thus often fails to yield an accurate, contextual understanding in the educational cybersecurity environment.

Another relevant gap in the literature has been the lack of specialized insider threat datasets designed for LMS contexts. Much of the existing insider threat research relies on enterprise-level cybersecurity datasets, none of which accurately reflect educational behavior [8]. While data sources such as the Open University Learning Analytics Dataset (OULAD) provide extensive information on user interactions in a learning environment, their use in insider threat research has been somewhat limited. Existing educational studies employing OULAD typically focus on learning analytics and academic performance prediction, rather than cybersecurity or insider threat detection [9].

In brief, in most current insider threat detection models, technical detection algorithms and technical performance dominate, while behavioral interpretation and contextual learning receive little attention [10]. In a continuous, interactive learning scenario in which users consistently interact with a learning management system, embedding role-aware behavioral intelligence can lead to better anomaly detection and lower false-positive rates. Hence, to bridge this gap in the literature, this paper proposes a role-aware behavioral analytics framework for insider threat detection in the learning management system. It embeds the concept of user role into behavioral profiling and anomaly detection. It aims to evaluate the performance of the proposed framework in distinguishing between students' and teachers' behaviors, and the model's potential to detect insider threats with improved accuracy.

IV. PROPOSED FRAMEWORK

This paper discusses a role-aware behavioral analytics framework for detecting insider threats in Learning Management Systems (LMSs). It is designed to capture users' behavioral interactions based on their specified role and to detect anomalies that might constitute an insider threat. The existing anomaly detection scheme treats all users' behavior equally; our framework uses role to derive the significance of behavior, thereby increasing anomaly detection.

The system has been designed primarily to analyze behavioral discrepancies between students and teachers using interaction data captured in LMS activity logs. A massive amount of behavioral information is generated on educational platforms, including login logs, resource access, exam activities, communication patterns, and session behaviors. These behavioral indicators are analyzed collectively, along with user role information, to improve the likelihood of detecting atypical behavior.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The proposed framework comprises six main steps: data collection, data preprocessing, role identification, feature extraction, anomaly analysis, and classification, as depicted .

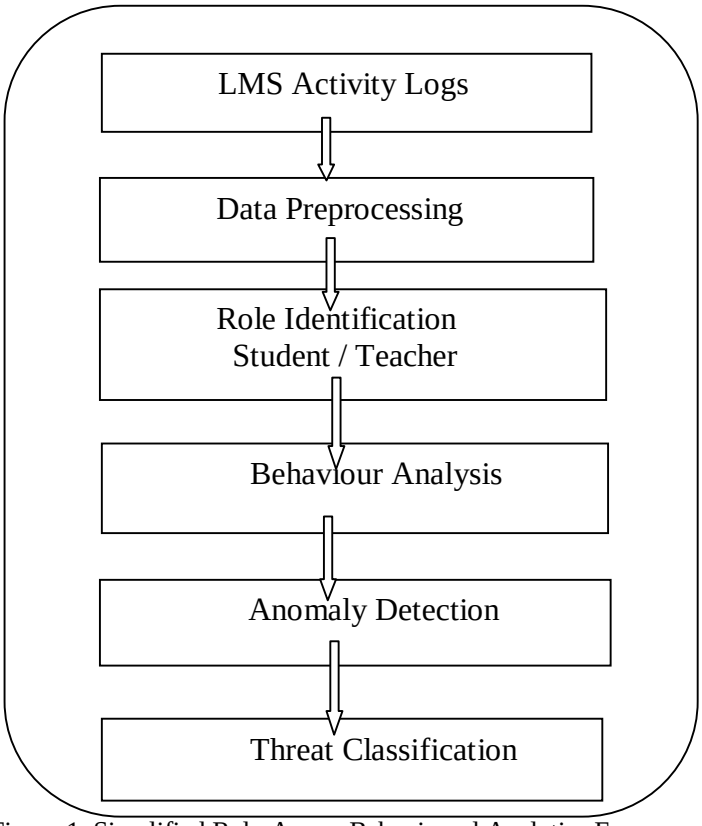


Figure 1. Simplified Role-Aware Behavioural Analytics Framework

A. Data Collection

The framework uses behavioral interaction data retrieved from the Open University Learning Analytics Dataset (OULAD). OULAD is an anonymized record of learner activities along with demographic details, virtual learning environment interactions, submissions to assignments, and course activity data. OULAD is one of the richest behavioral interaction logs of user activities on the web. The information available for this system is: Login frequency.

Session duration

Access to resource patterns

Assignment interactions

Clickstream actions

Download activities

Access patterns based on time

B. Data Preprocessing

The collected data is preprocessed to improve its quality before it can be used for behavioral analysis. Missing, duplicated, and erroneous records are cleaned during this phase. Imputation or deletion of values depends on the extent of data incompleteness. Behavioral attributes are converted to a machine-readable format using encoding and normalization methods. Numerical attributes, such as the number of logins and session length, are standardized to ensure that the different behavioral observations have comparable scales.

C. Role Identification

One of the building blocks of the suggested framework is Role identification. The identified roles are defined in the system in which they operate - i.e., the LMS, and are between the student and the teacher. Because user behavior expectations differ widely across users with these roles, the framework analyzes behavior accordingly.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

For example,
Frequent access to an assessment might be considered a normal student activity, but changing grades could be suspicious for a student and completely normal for a teacher. Bulk data downloads can be both a student's or a teacher's normal or abnormal activity, depending on the role and the surrounding context.
Hence, it can be concluded that role context may help improve the analysis of user activity and reduce the number of false positives detected in the system.

D. Behavioural Feature Extraction

The framework derives behavioral features from the LMS interaction log to analyze user actions. The behavioral features selected for analysis were identified based on their relation to insider threat detection and anomaly detection. Some key behavioral indicators were selected as:
Frequency of login
Session duration
Number of accessed resources
Frequency of assessment access
Download behavior
System access time
Interaction click stream patterns

E. Behavioural Anomaly Analysis

Behavioral anomaly detection is performed by comparing the current user behavior with a predefined behavioral baseline for each user role. Activity is marked suspicious or anomalous if it is significantly different from standard user behavior for the user role.
Typical behavioral anomalies:
Large resource downloads
Suspicious midnight access to the system
Unusual clickstream
Unauthorized grade access attempts
Too many login attempts
Irregular usage patterns
Framework provides an anomaly within the context of the user role to better understand behavior and threat:

F. Threat Classification

After anomaly detection, suspicious behaviors are categorized by severity and Insider Threat characteristics. Behavioral characteristics are divided into Normal behavior and anomalous behavior based on the degree of deviation and the context-aware risk factors of the activities.
The proposed framework will assist educational organizations in identifying potential Insider Threats and enhancing overall monitoring in the learning management system. Furthermore, combined with role-aware contextual information analysis, the proposed behavioral analysis-based framework could be applied to build up a flexible, scalable, and intelligent insider threat detection mechanism for online learning platforms.

V. RESEARCH METHODOLOGY

In this work, a quantitative and behavioral analytics research methodology is proposed for insider threat detection in Learning Management Systems (LMS). It centers on mining user interaction behavior and detecting unusual actions using role-aware behavioral profiling. This method integrates educational behavioral analysis and cybersecurity surveillance mechanisms to understand better the context of insider threats on online learning platforms. The methodology consists of dataset selection, behavioral data preparation, feature extraction, role-based behavioral classification, anomaly analysis, and performance evaluation. The workflow of this methodology is created to discover malicious insider behaviors based on students/teachers' behavior differentiation.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

A. Research Design

This study proposes a behavioral anomaly-detection method for tracking user activities in educational systems using LMS interaction data. This has used a role-aware analytical approach to analyze and differentiate between the behavioral norms of different user groups. The focus of the study is to find abnormal behavior patterns to detect insider misuse. The methodology comprises: Behavior analysis, Role-aware profiling, Education interaction analysis, Anomaly detection concepts, and Machine learning-supported behavior tracking. The research design helps analyze behavioral anomalies and provides context for identifying suspicious activities.

B. Dataset Description

The data used in this study is the Open University Learning Analytics Dataset (OULAD), a popular public-domain educational dataset often used in learning analytics and behavioral research. The OULAD is composed of anonymized learning interaction data collected from online courses hosted by the Open University (UK). The dataset comprises: students' demography, students' assessment records, virtual learning environment's interaction log, students' involvement in a course, and learning resource access behavior. Clickstream interactions log: This comprises all interactions with the LMS made by the student. OULAD was chosen as it consists of in-depth behavioral interaction logs and can model user activities within an LMS, identifying both legitimate and potentially non-legitimate activity .

C. Data Preparation

To enhance data quality, uniformity, and analytical trustworthiness, data preprocessing was implemented. Cleaning procedures, including the removal of missing, duplicated, and contradictory records, were used to correct faulty data. Handling of missing values involved using various methods, such as imputation and deletion, based on the incompleteness rate. The preprocessing also involved:

Behavioral feature normalization,
Categorical data encoding,
Activity filtering,
Interaction log standardization.
Behavioral records were organized by user role after processing.

D. Behavioural Feature Engineering

To address the problem of extracting meaningful cues about insider threat behavior within an LMS, behavioral feature engineering was performed. The behavioral variables were chosen on their applicability to anomaly detection and the nature of user activity in LMS environments. The behavioral features identified are: frequency of logins, session duration, frequency of resource accesses, frequency of assessment interactions, file downloads, timing of access, and patterns of clickstream interaction. These features were used to formulate behavioral baselines for students and teachers, respectively, and departures from these expected behavioral patterns may serve as possible cues of suspicious activity.

E. Role-Based Behavioural Classification

A role-aware classification mechanism was also incorporated to provide meaning to behaviors during anomaly analysis. The roles in an LMS context include students and teachers. A behavior that poses risks is interpreted based on the user's role: for example, constant access to grade lists may be routine for teachers but not for students. Another example of role interpretation: accessing a large chunk of course material may indicate abuse, depending on the user's role. The anomaly of logging in late at night can also be explained based on a user's role. Role-aware behavioral analysis yields meaningful explanations of anomalies and reduces ambiguity when searching for insider threats.

F. Anomaly Identification

An anomaly was detected due to deviations in behavior patterns from the role-specific behavior profiles. Anomalous/suspicious behavior was any activity that did not significantly comply with the baseline behavior models. Some of the anomalies that were identified were,

Download of a large volume of resources
Log in at an unexpected time

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Unusual frequency of user interaction
Inappropriate access to assessments
Suspicious clickstream behavior
To better understand insider threat behavior, anomalies were sought within the constraints defined for the assigned user role.

G. Evaluation Approach

This framework was tested for its effectiveness in identifying anomalous behaviors in the LMS system. The accuracy of observed behaviors and the ability to interpret the anomaly are evaluated to assess how useful role-based behavior analysis can be in the e-learning cybersecurity field.
Behavioral anomaly detection, correct interpretation and understanding of anomalies, and correct role-aware differentiation in behavior were observed and evaluated in relation to detecting suspicious insider activities. The evaluation provided a way to understand the effectiveness of role-aware behavioral analytics in bolstering LMS security and enhancing insider threat awareness in educational institutions.

VI. RESULT

In this part, the behavioral findings and the results of anomaly detection achieved by using the proposed role-aware behavioral analysis framework are reported. In this part of our study, role-aware behavioral analytics was applied to identify suspicious insider behavior within the LMS, focusing on students' and teachers' learning interaction patterns. The outcomes show the importance of including contextual role information in behavioral analytics to enhance understanding of the insider threat.

A. Behavioural Analysis of LMS Users

Behavioral analysis of students and teachers revealed a significant difference in interactions within the LMS environment for both groups. Students interacted with the learning content, tests, quizzes, and courses; whereas the teachers used the system to score tests and assessments and to supervise instruction.
Some of the behaviors where the students and teachers had differing patterns:
Frequency of logins.
Patterns of learning resource access.
Length of sessions.
Frequency of assessments used (including tests and quizzes).
Patterns of usage across time.
Download activity.
These behavioral patterns suggest the value of role-aware behavioral analysis in anomaly detection within educational systems.

Table 1 presents a comparison of behavioural activities observed across different LMS user roles.

Behavioural Activity	Student Behaviour	Teacher Behaviour	Suspicious Indicator
Login Frequency	Regular access during study periods	Frequent access for teaching and grading	Excessive repeated login attempts
Session Duration	Moderate session duration for learning activities	Extended sessions for course management	Unusually long inactive sessions
Resource Access	Access to assigned course materials	Access to multiple teaching resources	Access to restricted or unrelated materials
Assessment Interaction	Assignment submission and quiz participation	Assessment creation and grading	Unauthorised assessment access
Download Behaviour	Limited downloads for study purposes	Downloading instructional materials	Bulk or repetitive downloads
Access Timing	Mostly daytime or scheduled access	Flexible access depending on teaching activities	Repeated midnight or unusual-hour access

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Behavioural Activity	Student Behaviour	Teacher Behaviour	Suspicious Indicator
Grade Access	Limited or no grade modification access	Frequent grade review and modification	Student access to grading systems
Clickstream Behaviour	Sequential navigation through learning content	Administrative and instructional navigation	Irregular or automated navigation patterns
Communication Activity	Student discussions and messaging	Course announcements and feedback	Excessive or abnormal messaging behaviour
Administrative Access	Minimal administrative privileges	Limited course management privileges	Unauthorised privilege escalation attempts

B. Student Behavioural Patterns

In addition, the study was able to find the usual student behavior, which is primarily associated with the:
Continuous access to modules
Timed submission of assignments
Moderate download of modules
Normal access time
Normal download pattern
There are several activities where the student was behaving abnormally. Some of the questionable behaviors identified were:
An excessive number of course modules downloaded
Strange clickstream pattern
Access to the module at an odd time of day
Multiple failed login attempts
Unauthorized module access
These actions may result from internal abuse, stolen credentials, or abnormal activity in the LMS.

C. Teacher Behavioural Patterns

Based on teacher behavior analysis, typical behaviors observed were:
High rate of grade access
Activities related to grade management
Longer duration of sessions
Interactions related to course administration
Activities related to the management of instructional materials
It was found that while most of these activities might be legitimately expected as a part of a teacher's instructional role, some behaviors that were found as suspicious were:
Midnight login anomalies
High rate of grade correction activities
Unusually high rate of access
Large-scale data access patterns
Out-of-place interactions with the administrative system

D. Role-Aware Anomaly Interpretation

The role of behavioral anomaly analysis in interpreting behavior without awareness of the role has yielded an important finding: it is impossible to appropriately interpret certain behavioral anomalies without knowing the context in which they occur. Specific actions may be malicious when performed by a certain user role and legitimate when performed by a different user role. For instance:
Instructors access the grades page for many classes, and this should not be flagged. However, if a student accesses many grade pages, this could be suspicious behavior.
Downloading a significant number of files could also be misuse if outside normal learning activity.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Anomalies that appear after hours will need to be analyzed differently if a certain user is expected to access the system outside of regular hours.
The role-aware approach to analysis provides a deeper contextual understanding to detect behavioral anomalies and make better judgments about insider threats.

E. Behavioural Indicators Associated with Insider Threats

The role of behavioral anomaly analysis in interpreting behavior without awareness of the role has yielded an important finding: it is impossible to appropriately interpret certain behavioral anomalies without knowing the context in which they occur. Specific actions may be malicious when performed by a certain user role and legitimate when performed by a different user role. For instance:
Instructors access the grades page for many classes, and this should not be flagged. However, if a student accesses many grade pages, this could be suspicious behavior.
Downloading a significant number of files could also be a misuse if outside of normal learning activity.
Anomalies that appear after hours will need to be analyzed differently if a certain user is expected to access the system outside of regular hours.
The role-aware approach to analysis provides a deeper contextual understanding to detect behavioral anomalies and make better judgments about insider threats.

VII. DISCUSSION

This work shows that behavior analysis can significantly contribute to identifying insider threats on e-learning platforms. Role-aware context analysis provides deeper behavioral interpretation by separating role-specific and abnormal behavior.
The proposed system contrasts with typical generalized anomaly-detection systems by emphasizing contextual behavior understanding, which is highly crucial in the educational field due to varying role-specific user behaviors. Also, the applicability of behavior profiling systems for proactive security monitoring in LMS platforms is evident from the paper.
Also, the use of interaction data from educational contexts contributes to defining the expanding importance of multidisciplinary research where Artificial Intelligence, behavioral analysis, and educational security intersect. The suggested framework helps build an effective, adaptive, and scalable insider threat detection system that can operate in the modern context of digital learning.

VIII. LIMITATIONS

This study has some limitations. The research mainly used the Open University Learning Analytics Dataset (OULAD). This dataset was originally made for analytics, not for cybersecurity research. Because of this, it does not include insider attack scenarios specific to Learning Management Systems (LMS).
* One limitation is that the study mainly looked at students and teachers. It did not include LMS users, such as administrators or technical staff.
* Some unusual activities found during the analysis might be normal user behavior, not insider threats.
The proposed framework was tested using interaction data. It was not tested in real-time LMS monitoring environments. So, how well the framework works in educational systems is not fully known.
The study primarily focused on analytics and role-aware analysis. It did not explore deep learning models and explainable Artificial Intelligence (XAI) techniques much.
With these limitations, the study gives useful insights. It shows how important role-aware behavioral analytics is for improving insider threat detection in learning environments.

IX. CONCLUSION AND FUTUREWORK

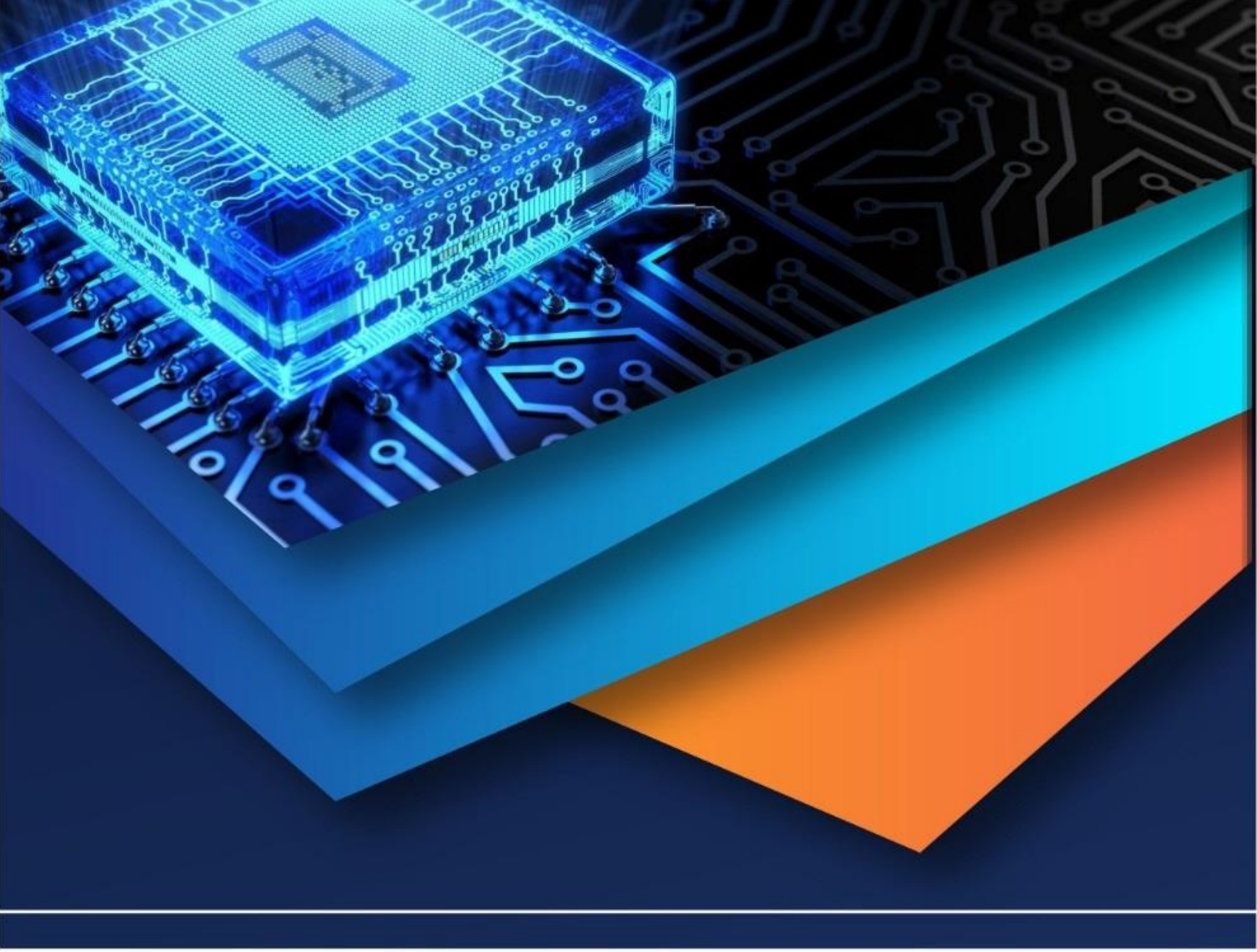
In this research project, a behavioral analytics framework for insider threat detection in Learning Management Systems (LMS) was proposed with a focus on including the concept of role awareness in the behavioral analytics of both students and teachers, to provide a better understanding (contextual) of behaviors that may be deemed suspicious due to their occurrence. The analysis of the findings suggests that including role awareness in behavioral analysis supports the effective identification of insider threats and enhances cybersecurity monitoring capabilities for Learning Management Systems (LMS). This study contributes to the growing body of research in the field of Educational Cybersecurity through its introduction of a combined approach of behavioral analysis with role-based analysis of anomalies for identifying (anomalous) behaviors in LMS. The proposed framework reinforced the importance of analyzing behaviors contextually to facilitate the determination of the legitimacy or suspicion of behaviors occurring in LMSs.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Future work may include integrating deep learning techniques, implementing sophisticated real-time monitoring systems, and integrating Explainable AI (XAI) technologies and methods into an adaptive insider threat detection system (System, LMS). Finally, future research could also investigate other user roles and add real-world Cybersecurity Data to strengthen the accuracy of behavioral analysis when monitoring for behaviors associated with potential threats.

REFERENCES

[1] B. Singh and B. Kumar, "Enhancing cyber security in e-learning portals: Challenges and solutions," *Educational Administration: Theory and Practice*, vol. 29, no. 4, pp. 1581–1586, 2023.
[2] M. Bishop, M. Carvalho, R. Ford, and X. Ou, "Insider threat detection: Progress and open challenges," *IEEE Security & Privacy*, vol. 18, no. 4, pp. 14–22, 2020.
[3] J. Yuan, J. Wu, X. Qiu, J. Guo, W. Li, and Y.-G. Wang, "Integrating behavior analysis with machine learning to predict online learning performance: A scientometric review and empirical study," *arXiv preprint arXiv:2406.11847*, 2024.
[4] X. Zhang, Y. Li, and H. Wang, "Behavioral analysis in STEM online courses using learning analytics," *Sustainability*, vol. 15, no. 10, p. 8235, 2023.
[5] T. Badal, A. Dutt, and M. A. Ismail, "Predictive modelling and analytics of students' grades: A systematic review," *Scientific Reports*, vol. 12, no. 1, p. 20122, 2022.
[6] G. M. Rao and D. Ramesh, "A hybrid and improved isolation forest algorithm for anomaly detection," in *Proceedings of the International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications*. Singapore: Springer, 2021, pp. 589–598.
[7] J. Yi, "Insider threat detection model enhancement using hybrid unsupervised outlier scores," *Electronics*, vol. 13, no. 5, 2024.
[8] A. Sharma and P. Verma, "Optimising insider threat prediction: Exploring BiLSTM networks and sequential features," *Data Science and Engineering*, Springer, 2024.
[9] R. Kumar and S. Patel, "Intrusion detection model for imbalanced dataset using SMOTE and Random Forest algorithm," *International Journal of Computer Applications*, vol. 185, no. 12, pp. 15–21, 2025.
[10] L. Jiang, "Detecting anomalous student engagement patterns in online learning using OULAD," in *Proceedings of the Educational Data Mining Conference*, 2022.
[11] A. Ali, M. Husain, and P. Hans, "Real-time detection of insider threats using behavioral analytics and deep evidential clustering," *arXiv preprint*, 2025.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)