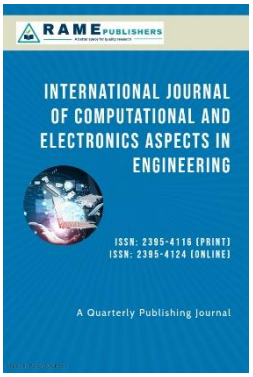
International Journal of Computational and Electronic Aspects in Engineering
Volume 7, Issue 3, July 2026, pp 44-53
Special Issue of National Conference on Emerging Innovative Trends in Computer Applications
https://doi.org/10.26706/ijceae.7.3.20260707

Behavior-Aware Risk Modeling for Insider Threat Detection Using Temporal User Activity Analysis

Sakshi Wankhede*, Achal Laxman Deshmukh, Kunali Ratnakar Tarare

Master of Computer Application, Suryodaya College of Engineering & Technology, Nagpur, India

*Correspondence: sakwan132000@gmail.com



Abstract: Detecting insider threats isn't easy, mainly because the users involved already have legitimate access to organizational systems. This makes it hard to tell the difference between normal, everyday activity and actions that could actually be harmful. Many traditional methods depend on fixed rules or basic anomaly detection, but these often fail to notice the slow, subtle changes in behavior that develop over time. In this study, a behavior-aware insider threat detection framework is introduced that focuses on how user activity evolves over time, rather than trying to interpret intentions or psychological factors. The system continuously monitors key activities such as login patterns, access frequency and session behavior and uses this information to generate a dynamic risk score for each user. Simply put, it compares what a user is doing now with their usual behavior and looks for consistent changes that could signal potential risk. To make detection more reliable, the framework includes a threshold-based alert mechanism. Instead of reacting to one-off unusual actions, it generates alerts only when changes in behavior persist over time. This helps cut down on false alarms and ensures that alerts are more meaningful and useful for security teams. The framework was tested using simulated behavioral data and the results show that this time-based risk scoring approach can effectively distinguish between normal and suspicious behavior. Overall, the findings highlight how important it is to analyze behavior over time when trying to detect insider threats early. The system is also designed to be scalable, making it well-suited for high-security environments such as defense organizations and critical infrastructure systems.

Keywords: Insider Threat Detection, Behavioral Analysis, Risk Scoring, Temporal Analysis, Cybersecurity

Article – Peer Reviewed
Received: 1 March 2026
Accepted: 30 June 2026
Published: 31 July 2026

Cite this article: Sakshi Wankhede, Achal Laxman Deshmukh, Kunali Ratnakar Tarare, "Behavior-Aware Risk Modeling for Insider Threat Detection Using Temporal User Activity Analysis", *International Journal of Computational and Electronic Aspects in Engineering*, vol. 7, issue 3, pp. 44-53, 2026.
https://doi.org/10.26706/ijceae.7.3.20260707

1. Introduction

Insider threats are becoming a major concern within the current cybersecurity environment. Unlike outsiders, insiders, such as employees or individuals working within an organization, are already authorized to access the organization's information and resources. Therefore, insider threats are extremely difficult to detect using current cybersecurity tools. These insider threats may manifest themselves through different means, such as leaking sensitive information or accessing information without a valid reason or using confidential information in an improper manner.

Currently, most cybersecurity tools and systems are designed mainly to detect and prevent threats coming from outside the organization. These tools usually depend on a set of rules or basic anomalies. However, insider threats resemble normal work activities, making it extremely difficult to detect anything unusual. On the other hand, human nature is such that it changes over time.

According to research, it is possible to improve insider threat detection by analyzing user behavior over a period of time. However, most of the current systems consider all users equally and do not take into account the changes in user behavior. For instance, working late hours or accessing more files may simply imply that the user is extremely

busy and not necessarily up to any wrongdoing. Therefore, it is essential to focus on user behavior over a long period rather than a single unusual act.

To solve this problem, the study introduces a new approach for behavior-aware risk modeling that emphasizes the changes in user behavior over time. Instead of making assumptions about the intentions of the user, the system monitors the user's actions, such as the time spent on accessing the resources and the frequency with which resources are being used. Then, it compares these with the user's historical data to determine a risk score for the user.

The main contributions of this study are:

• A framework for tracking user behavior over time

• Developing a baseline user behavior model for each user

• Introducing a risk scoring system instead of a classification system

• Evaluation using simulated data for an organization

To put it simply, this approach tries to detect insider attacks before they happen while avoiding false alarms due to changes in normal user behavior. By emphasizing gradual changes in user behavior, this approach provides a more realistic approach to the problem than traditional methods.

2. Problem Statement

Nowadays organizations make extensive use of digital technologies to deal with protecting their sensitive information. Although robust security controls are implemented to protect organizations from any possible cyber-attacks from outsiders, it is much more difficult to detect insider threats. The main reason for this is that insiders are already authorized to access the information and perform activities and hence, any actions performed by them, either intentionally or unintentionally, appear like normal activities performed by others as well.

It has been seen that most traditional systems used to detect insider threats operate on a set of rules or thresholds. These systems usually assume that every user behaves in a similar manner and do not consider any differences between them. Therefore, sometimes normal activities performed by insiders, such as working late hours to meet deadlines or using more information during peak hours, are sometimes identified as threats.

Another major issue identified while trying to detect insider threats is that most traditional systems do not consider changes in user behavior over time. In most traditional systems, the focus is on identifying abnormal activities performed by insiders at a given point in time. However, it has been seen that insider threats take place gradually and hence, any subtle changes are ignored.

Apart from that, most existing systems classify users in a very rigid manner, i.e., either as a normal or a malicious user. This does not take into account the real nature of insider threats, as in real-life situations, insider threats are not as straightforward as this classification suggests, as they involve a certain amount of uncertainty as well. As a result, a new approach that continuously monitors the behavior of the user and then assigns a risk level according to the degree of deviation from normal behavior is required.

What are the ways in which the changing behavior of individual users over a period of time can be effectively modeled in order to detect insider threats at an early stage, without causing false alarms or making assumptions about the intentions of the user?

To answer this research question, a behavior-aware risk modeling framework for insider threats has been proposed, which continuously monitors the behavior of the user over a period of time and then calculates the risk level according to the changes in the user's behavior. In other words, a more practical, realistic and reliable way of identifying potential insider threats at an early stage can be proposed.

3. Literature Review

However, insider threats still remain a major concern in the modern information security environment. One of the major problems related to insider threats is the fact that, owing to their authorized nature, insider threats cannot be easily detected, as this kind of attack appears to be normal system behavior. In the early stages of research related to insider threat detection, only rule-based and anomaly-based detection methods were implemented for the detection of unusual

behavior patterns. However, according to the research by Gheyas and Abdallah [5], this method can only be implemented for the detection of obvious problems; otherwise, it is not capable of dealing with complex changes in user behavior. This method is also not dynamic enough to be implemented in real-life situations.

As the research related to insider threat detection advances further, a significant shift can be observed from the implementation of machine and deep learning methods for the improvement of the accuracy of insider threat detection. In their research, Yuan and Wu [1] proved that the study of changes in user behavior can be a better approach than the implementation of fixed rules for the detection of insider threats, as this method is more likely to be effective for insider threat detection scenarios. In another research by Al-Mhiqani et al. [2], the use of behavior-based detection methods, which are machine learning-based, is more appropriate for insider threat detection scenarios, as insider threats take a long time to appear.

Recently, research has been conducted with the focus of gaining in-depth knowledge about user behavior. For example, Nasir et al. [3] proposed a framework that can be implemented to analyze user behavior by employing deep learning techniques and evaluated the accuracy of the proposed framework by comparing it with traditional approaches. It was evident that the proposed framework was able to attain increased accuracy in this regard. Moreover, Wang et al. [4] proposed another extension of the same research by employing deep clustering techniques to analyze user behavior data collected from different sources. This research also emphasized the importance of employing user activity logs collected from different sources to detect complex patterns of user behavior that have the potential to cause security risks in the near future. Apart from this, Kim et al. [15] also emphasized the importance of analyzing user sessions to comprehend user behavior, as user access patterns can be employed to detect user behavior in a more efficient manner.

More complex approaches have also been proposed to deal with real-time detection scenarios where there is a scarcity of labelled data. For example, Liu et al. [6] proposed a temporal activity modeling approach (LSTM) to detect user behavior and this approach was able to detect subtle changes in user behavior with the scarcity of labelled data. Moreover, Nguyen & Yiu [16] proposed another real-time approach to detect user behavior by employing user behavior analysis and this approach was not only efficient in detecting user behavior but also took into account the uncertainty factor to avoid false alarms. Apart from this, Qiao et al. [7] proposed another approach to analyze user behavior by employing complex approaches such as GCN and Bidirectional Long Short-Term Memory (Bi-LSTM).

As a whole, the field has clearly evolved from simple rule-based systems towards more sophisticated, behavior-aware systems enabled by machine learning technologies. Despite these advances, however, significant challenges remain, for example, in dealing with real-world organizational data, minimizing false positives and making these systems easier to understand and trust.

As a result of these advancements, this research proposes a framework for a temporal, behavior-aware risk modeling system. This system continuously monitors user behavior and determines risk scores based on how behavior changes over time. In other words, the aim here is to detect insider threats better and earlier, as well as address the shortcomings of existing solutions.

4. Proposed Methodology

It is proposed that in this section, the rationale for the proposed behavior-aware risk modeling framework for insider threat detection would be explained in a more natural and understandable way. It is proposed that the idea behind this section would be that the system would be able to monitor the behavior of the user for a particular period of time and would be able to detect if there is any change in the behavior of the user, which may be considered a risk for the system. Unlike the approaches based on the behavior and emotions of the user, this system would be based on the actions of the user.

4.1 System Architecture

The proposed system will be composed of four main modules, which are as follows:

- User activity data collection
- Behavioral feature extraction
- Temporal behavior analysis
- Risk scoring and alerts

All these modules have different functions, which are used in the process of transforming the collected data from the system into useful knowledge. This process begins with the collection of user activity data from the system logs. Once the user activity data is collected, useful features are then extracted from the collected data. After useful features are extracted from the user activity data, analysis of the features is then conducted in order to understand how the behavior of the user changes over time.

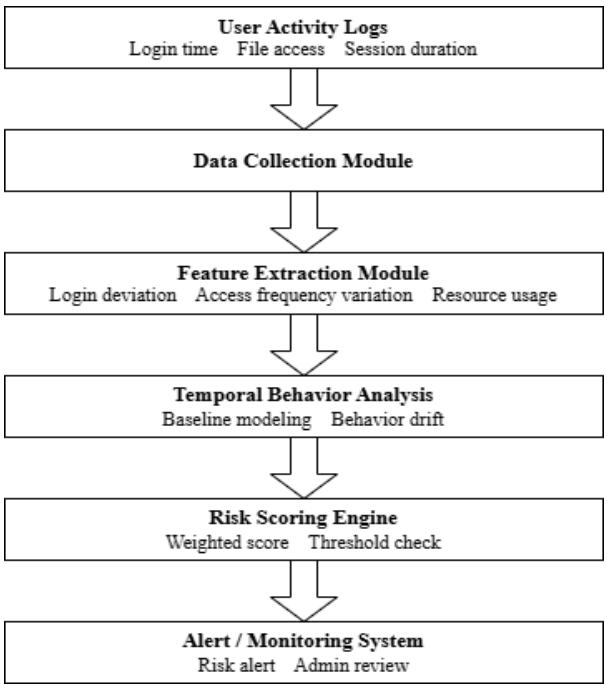


Figure 1. System architecture of the proposed behavior-aware risk modeling framework for insider threat detection.

Figure 1 depicts the overall architecture of the proposed framework. The proposed system is designed to follow a modular approach. Each component is designed to perform a specific task. This makes the system more manageable, efficient and scalable. By dividing the entire process into specific stages, from collecting the data to analyzing the behavior and evaluating the risks, the proposed system can efficiently transform the raw user behavior information into a more meaningful form for the early detection of insider threats.

4.2 User Activity Data Collection

Information regarding the activities of the user is obtained through the use of organizational system logs. The organizational system logs provide information about the activities that are taking place on a day-to-day basis between the user and digital resources. This is a real-life scenario where the activities of the user occur most of the time.

Information obtained through the use of organizational system logs:

- Login and logout time
- Session time
- Files and resources used by the user
- Frequency of usage of the resources by the user
- Sequence of the activities of the user

In order to maintain the privacy of the user information, the user information is kept anonymous before performing research on the information obtained by the use of the organizational system logs. The system does not use real information present in the files and communication. It uses the meta data for the maintenance of user information privacy while keeping the information useful.

4.3 Behavioural Feature Extraction

Once the data is collected, it is then processed. The raw logs are converted into structured features based on user behavior, which varies over time. The features include:

• Deviations in login time, i.e., deviation of current login time from average login time of user

• Variation in access frequency, i.e., sudden increase or decrease in frequency of accesses

• Diversity of resource usage, i.e., number of different files accessed by user

• Variation in session duration, i.e., variation in duration of session from normal behavior

• Variation in activity sequence, i.e., variation in normal sequence of user activities

4.4 Temporal Behaviour Modelling

For each user, a personalized baseline is constructed based on their past activity. This is a representation of what "normal" looks like for the user under typical working conditions. In order to monitor the evolution of user behavior over time, tools such as a sliding window and moving average can be employed.

Unlike a system that reacts to a specific abnormal occurrence, the system identifies patterns that change gradually and persist over a long period. It identifies consistent and related changes across various features, which can help detect changes in user behavior that may indicate a potential insider threat.

4.5 Risk Scoring Mechanism

Instead of classifying users as either normal or malicious, a risk score is assigned to users based on how much their current behavior deviates from their normal patterns.

The risk score is determined based on the deviations observed in the user's behavior. Each deviation is given a certain weight based on its importance. Greater importance is given to long-term deviations that have been consistent over time because they are more likely to reflect a genuine cause for concern.

If the risk score is high, it implies that there is a high likelihood that the user's behavior is suspicious. Instead of using a hard limit to determine whether a user should be flagged or not flagged, adaptive limits are used to determine whether a user should be flagged or not flagged.

The risk score for a user at time t is given by the equation:

$$Risk_t = \sum_{i=1}^{n} w_i \cdot D_i(t)$$

Where $D_i(t)$the normalized deviation of the ith is behavioral feature and w_i is the corresponding weight. Persistent and long-term deviations are given higher weights to emphasize sustained behavioral drift.

4.6 Alert Generation

If the risk score of a user is high for a period of time, then a system alert is issued. Such alerts are not considered for classifying users as malicious users; rather, they are considered to be a warning that requires further analysis.

This approach prevents the system from making decisions on its own, thereby reducing the chances of incorrect classification and promoting responsible decision-making.

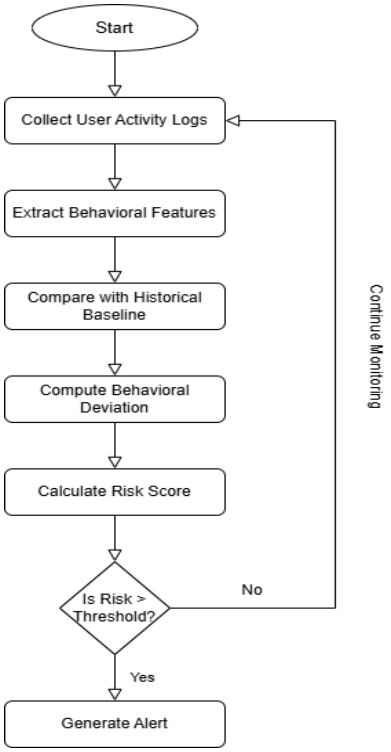


Figure 2. Workflow of the proposed temporal behavior-based insider threat detection system.

Figure 2 describes the overall workflow for the proposed system. The workflow starts with data collection for users' activities, then feature extraction for user behavior, analysis of user behavior over time with risk score computation and finally alerts for risk scores that are high for a period of time. This workflow describes how raw data obtained from system logs is eventually transformed into useful information for the detection of insider threats.

5. Results And Analysis

To analyze its effectiveness of the proposed behavior-aware insider threat detection framework, a temporal risk scoring technique was used and a test was conducted using simulated user behavior information. The information used in the test was carefully generated to resemble real-life behavior patterns as closely as possible, based on the CERT Insider Threat Dataset [29]. The system tracks the user's behavior and compares what the user is currently doing with how the user behaved in the past in order to calculate a risk score for the user. In other words, the risk score represents how much the user's behavior is changing and whether these changes could represent a potential risk or not.

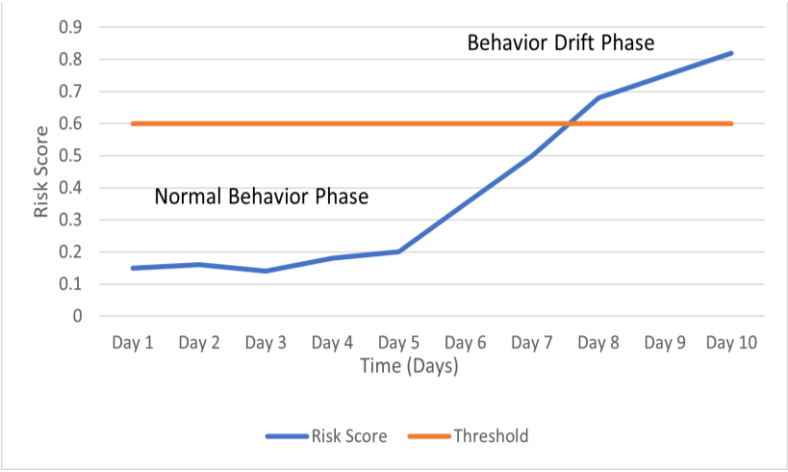


Figure 3. Variation of user risk score over time showing behavioral drift.

Figure 3 illustrates the changes in a user's risk score over a period of time. Initially, the risk score for the user remains constant at a lower level, implying that the user is behaving normally and performing tasks as expected.

As time progresses, the risks score gradually increases. This indicates that the user's behavior is starting to change. This change in the user's behavior over a certain period is called behavioral drift. This change may occur for various reasons, including unusual login hours and increased resource access. Unlike other methods, this method can detect this change in the user's behavior. This makes it easier to detect the potential risks.

After the risk score crosses a certain threshold limit, the system identifies the user as a potentially risky user and sends an alert. This system is more reliable compared to other methods because it only depends on the user's consistent behavior over a certain period rather than their unusual behavior.

From the above results, it is clear that analyzing user behavior over a certain period is more feasible compared to other methods for insider threat detection. This is because the proposed method can provide early signs of insider attacks by analyzing the user's long-term behavior rather than their short-term behavior. This method can be more useful for high-security applications, including defense systems.

6. Discussion

The results of this research have shown that temporal behavior-aware risk scoring is a useful, practical and reliable method for detecting insider threats and for helping to eliminate false alarms. By constantly monitoring the behavior of the user, the system is able to detect gradual changes in behavior, also known as behavioral drift. This is an important factor for detecting insider threats. The experiments conducted on this method using simulated data based on the CERT dataset [29] have shown that gradual changes in login times, access frequencies and session durations are important factors for detecting insider threats. This method is therefore useful for detecting possible risky behavior.

One of the most important aspects of this method is that it monitors the behavior of individual users rather than assuming that everyone behaves in the same way. By knowing the behavior of an individual user, the system is able to avoid false alarms by distinguishing between normal situations and malicious behavior. Another important aspect of this method is that it does not categorize users into normal and malicious behavior. Instead, it generates a risk score for each user. This helps security personnel to have a better idea about different levels of risk.

The next factor that makes a huge difference is the use of temporal analysis. This means that the system does not depend on a single point of time to get results, like other systems do. Instead, it uses techniques such as moving averages to get results. This makes it possible for the system to get early signs of potential problems before they become critical. This would not be possible with other systems.

As with everything in life, there are some limitations to the results obtained so far. To start with, the results obtained so far are based on simulations. This means that they do not necessarily reflect what would happen in real life. Secondly, the system uses predetermined weights to calculate risk. This means that there might be a need to adjust these weights depending on where the system is used in the future.

As seen from the results obtained so far, a temporal behavior-aware risk modeling framework is a very proactive way of handling insider threats. This is due to two main reasons. Firstly, this method makes it possible for potential problems to be detected early. Secondly, this method eliminates false positives. This makes it very useful in very critical situations where accuracy is paramount.

The following table presents the comparative study of existing verses proposed approach:

Table 1. Comparative table of Insider threat detection of existing approaches and proposed approach

Feature	Existing Approach	Proposed Approach
Detection Method	Rule-based, anomaly detection, ML/DL models	Temporal behavior-aware risk modeling
Behavior Analysis	Limited or static behavior patterns	Continuous monitoring of user behavior over time

Data Sources	Mostly single-source logs	Multi-source data (logs, activity, patterns)
Adaptability	Low (fixed rules, less dynamic)	High (learns behavior changes dynamically)
Detection Accuracy	Moderate	Improved accuracy using temporal analysis
Real-Time Detection	Limited or delayed	Supports near real-time monitoring
Handling Subtle Threats	Poor (misses slow changes)	Detects gradual behavioral changes
False Positives	High	Reduced using risk scoring mechanism
Computational Complexity	Moderate to High	Optimized with efficient modeling
Practical Implementation	Difficult in real-world scenarios	Designed for practical and scalable deployment

The comparison above indicates that previous methods are static, rule-based and needs to configure the model, without detection of gradual and intelligent insider threats. The present system improves them and, with the analysis of temporal behavior along with dynamic risk scoring, unrecognized insider threats can be detected earlier.

7. Future Work

There are different ways in which the proposed behavior-aware insider threat detection system can be improved for better effectiveness and usability:

i. Evaluation on Real-World Datasets: The study is purely based done on simulated data that mimicked CERT dataset [5] and evaluating the framework using real organizational data will give better perspective of its actual utility. Real environments Harsh Metadata conjunction, URL deflation is quite complex, with different user behaviors and work patterns that evolve across time, so this step would help ensure that the system does indeed function in real life on a daily basis.

ii. Machine Learning Models Candidate: People love Machine Learning; people usually tend to move towards the smartness approach. Random Forests, LSTM networks or autoencoders can learn progressively the behavior of patterns and when evolutions of pattern occurs that previous systems will not detect — letting the system become more adaptive as it goes.

iii. New Behavioral Features: Broadening the scope of user behavior could improve this framework. Also, monitoring network usage, changes to files and the activity and interactions across all systems can provide a broader view of user behavior which helps improve detection accuracy as a way to prevent internal threats.

iv. Dynamic Thresholds: Rotating the thresholds based on some context, whether it be user role or time of day otherwise load or saturation. This would help eliminate noise for alerts that do not require action, while maintaining enough sensitivity to identify legitimate threats within an organization or its defenses.

v. Monitor in Real-Time and Respond: When the system works in real-time, it would greatly increase its practical value. By constantly assessing the risk and producing alerts in real-time, as well as interfacing with Security Information and Event Management (SIEM) systems — organizations can respond much quicker, more efficiently, to potential threats.

vi. Behavioral Drift Analysis Across the Groups: Future enhancements can also go beyond just individual users and perform the analysis at the team or department level. By comparing behaviors at an individual level with behavioral group patterns, one could even pinpoint the uncommon activities or coordinated insider threats that could otherwise be difficult to detect.

vii. Democratizing Machine Learning: Transparency is utilized to the same degree as accuracy. Additionally, this approach should also be able through some explainable AI methods to provide an explanation of the reason why a user

being considered risky. This can inform the security analyst about what is precipitating an alert, so that they can make a more knowledgeable decision based on fact rather than myth or "black-box" results.

By following these pathways, the framework can be further developed as an adaptive, scalable and legacy solution. It could even better capture the complexity of real-world environments and produce more precise, human-readable insider risk intelligence. This will make the system more tamper-proof from within.

8. Conclusion

The main contribution that this research provides is a framework for detecting insider threats, particularly based on the natural evolution or drift that user behavior follows. This is different from using traditional rules or reacting to unusual isolated events because it is more likely for insider threats to be detected at an early stage.

The main component that this framework provides is a risk score, particularly based on the natural evolution or drift that user behavior follows in areas such as login, access and session, etc. The results that this research provides prove that using a time-based approach is quite effective, particularly in detecting suspicious behavior at an early stage. This framework is particularly valuable for detecting insider threats, particularly because it can continuously monitor how user behavior evolves; therefore, it is particularly valuable for use in areas that are considered critical, such as defense agencies. This framework can also be improved in the future, particularly based on using real-world data.

References

[1] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," *Computers & Security*, vol. 104, pp. 1–15, 2021.

[2] M. N. Al Mhiqani, R. Ahmad, Z. Z. Abidin and W. Yassin, "A review of insider threat detection: Classification, machine learning techniques, datasets and challenges," *Applied Sciences*, vol. 10, no. 15, 5208, 2020.

[3] R. Nasir, M. Afzal, R. Latif and W. Iqbal, "Behavioral based insider threat detection using deep learning," *IEEE Access*, vol. 9, pp. 67220–67230, 2021.

[4] J. Wang, Q. Sun and C. Zhou, "Insider threat detection based on deep clustering of multi-source behavioral events," *Applied Sciences*, vol. 13, no. 24, 13021, 2023.

[5] I. A. Gheyas and A. E. Abdallah, "Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis," *Big Data Analytics*, vol. 1, article 6, 2016.

[6] S. Liu, F. Wang, J. Hu and X. Wang, "Temporal activity modeling for insider threat detection using LSTM networks," *Journal of Information Security and Applications*, vol. 70, 103152, 2023.

[7] Z. Qiao, J. Zhang, Y. Liu and X. Zhou, "Graph neural networks for insider threat detection," *ACM Transactions on Privacy and Security*, vol. 26, no. 4, 17:1–17:24, 2023.

[8] E. Eberle and L. Holder, "Insider threat detection using graph-based approaches," *Journal of Applied Security Research*, vol. 4, no. 1, pp. 32–81, 2009.

[9] K. Le et al., "User behavior analytics for insider threat detection," *Future Generation Computer Systems*, vol. 97, pp. 678–688, 2019.

[10] N. Pastrana et al., "Cybersecurity insider threat detection using data mining," *Computers & Security*, vol. 85, pp. 1–14, 2019.

[11] B. Duncan et al., "Insider threat detection using machine learning," *Journal of Cyber Security Technology*, vol. 2, no. 3, pp. 123–145, 2018.

[12] M. Bishop et al., "Insider threat detection techniques: A survey," *Journal of Computer Security*, vol. 23, no. 4, pp. 1–30, 2015.

[13] R. Mitchell and I. Chen, "Behavior rule specification-based intrusion detection," *IEEE Transactions on Dependable and Secure Computing*, 2015.

[14] F. Magklaras and S. Furnell, "Insider threat prediction tool," *Computers & Security*, vol. 21, no. 1, pp. 62–73, 2002.

[15] J. Kim and H. Kim, "User behavior modeling for insider threat detection," *Expert Systems with Applications*, vol. 41, no. 8, pp. 3933–3941, 2014.

[16] D. A. T. Nguyen and S. M. Yiu, "A hybrid ML approach for real time insider threat detection," *IEEE Transactions on Dependable and Secure Computing*, 2024 (early access).

[17] A. Tuor et al., "Deep learning for unsupervised insider threat detection," *AAAI Workshops*, 2017.

[18] M. Salem and S. Stolfo, "Modeling user search behavior for insider threat detection," *IEEE Security & Privacy*, 2011.

[19] S. Axelrad, P. Sticha, O. Brdiczka and J. Shen, "A Bayesian network model for insider threat detection," *IEEE Security & Privacy Workshops*, 2013.

[20] J. Glasser and B. Lindauer, "Bridging the gap: Behavior-based insider threat detection," *IEEE Security & Privacy*, 2013.

[21] P. Parveen et al., "Unsupervised learning for insider threat detection," *ACM SIGKDD*, 2011.

[22] A. Patcha and J. Park, "An overview of anomaly detection techniques," *Computer Networks*, vol. 51, no. 12, pp. 3448–3470, 2007.

[23] M. Chandola et al., "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 41, no. 3, 2009.

[24] D. E. Denning, "An intrusion detection model," *IEEE Transactions on Software Engineering*, vol. SE-13, no. 2, pp. 222–232, 1987.

[25] H. Liu et al., "Hybrid anomaly detection framework for insider threats," *Security and Communication Networks*, 2020.

[26] Y. Chen et al., "Sequence learning for insider threat detection," *IEEE Access*, vol. 8, pp. 134160–134172, 2020.

[27] C. Legg et al., "Insider threat detection using contextual analysis," *Journal of Wireless Mobile Networks*, 2015.

[28] S. Eberle and L. Holder, "Discovering structural anomalies in graph-based data," *Data Mining and Knowledge Discovery*, 2007.

[29] CERT Insider Threat Dataset, Carnegie Mellon University, Software Engineering Institute, USA.

[30] L. Spitzner, *Honeypots: Tracking Hackers*, Addison-Wesley, 2003.

[31] F. R. Alzaabi and A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods," IEEE Access, vol. 12, pp. 30907–30927, 2024.

[32] K. Kamatchi and E. Uma, "Insights into user behavioral-based insider threat detection: Systematic review," *International Journal of Information Security*, 2025.

[33] F. Whitelaw, J. Riley and N. Elmrabit, "A review of the insider threat, a practitioner perspective within the U.K. financial services," IEEE Access, vol. 12, 2024.

[34] U. Rauf, F. Mohsen and Z. Wei, "A taxonomic classification of insider threats: Existing techniques, future directions & recommendations," Journal of Cyber Security and Mobility, vol. 12, no. 2, 2023.

[35] K. Kong, X. Jin, D. Liu, S. Xu, Z. Liu and G. Geng, "DPI-ITD: A dual-perspective information-driven framework for insider threat detection in IoT systems," IEEE Internet of Things Journal, vol. 12, no. 19, 2025.