JOURNAL LA MULTIAPP

VOL. 07, ISSUE 04 (818-831), 2026
DOI: 10.37899/journallamultiapp.v7i4.5930

Efficient Detection of Anomalous User Behavior in Cloud Environments Using Simulated Mouse Dynamics and a Hybrid Ensemble Model

Uqba bn Nafaa Mohammed[1], Zeyad Farooq Lutfi[1], Raed Waheed Kadhim[1]

[1]*Computer Science Department, Collage of Science, Mustansiriyah University, Baghdad-Iraq*

**Corresponding Author: Uqba bn Nafaa Mohammed*
E-mail: uqba80@uomustansiriyah.edu.iq

Article Info

Article history:
Received 27 June 2026
Received in revised form 29 July 2026
Accepted 2 September 2026

Keywords:
Cloud Security Monitoring
Anomalous Behavior Detection
Behavioral Biometrics
Support Vector Machine

Abstract

This study proposes a lightweight and interpretable framework for identifying suspicious behavior within a cloud-based environment through the use of simulated mouse dynamics and a voting ensemble classifier. Contrary to existing approaches that heavily focus on the use of deep learning techniques, this study utilizes a combination of three classical machine learning classifiers: XGBoost, Random Forest, and Support Vector Machine (SVM). The proposed framework utilizes a voting classifier that achieved a test accuracy of 51.1%, effectively identifying 36 anomalous user sessions. To further increase the interpretability of this framework, this study incorporates a voting classifier based on the use of Shapley Additive Explanation (SHAP), which identifies the most influential behavioral features used to make a prediction. This study shows that a combination of engineered behavioral features, anomaly detection through Isolation Forest, and ensemble voting can provide a lightweight, scalable, and deployable framework for real-time cloud security monitoring without requiring any intrusive biometric techniques.

Introduction

The rapid advancement of digital communication technologies has significantly increased the complexity of cyber threats, especially in remote and cloud-based systems (Cremer et al., 2022; Nisha & Pramod, 2024; Mallick & Nath, 2024; Zhukabayeva et al., 2025). Behavioral anomalies in digital systems, especially in virtual user sessions, have become a major concern in the fight against external cyber threats using firewalls, intrusion detection systems, etc. (Khan et al., 2019; Saxena et al., 2020).

The detection of suspicious user behavior without the use of biometric systems like fingerprints, iris scans, etc., becomes a major challenge in cloud-based systems and enterprise environments (Patel, 2026; Zhou, 2025; Vijaykumar & Kashikar, 2026). However, the use of behavioral biometrics, which focuses on mouse dynamics, provides a cost-effective, unobtrusive, and real-time monitoring solution (Khan et al., 2024; Antal & Fejér, 2020).

Mouse dynamics involve the study of the behavior of a user using a computer mouse to capture attributes like the speed of mouse movement, acceleration, click frequency, etc. Mouse dynamics help create a unique profile of a user to detect anomalies (Khan et al., 2019; Quraishi & Bedi, 2022).

Research gap and novelty

Despite the fact that past studies utilized deep learning techniques like BiLSTM or rule-based systems to detect abnormal behavior in cloud computing environments, there is still a knowledge gap regarding the development of lightweight, transparent, and deployable frameworks that can effectively detect abnormal behavior without relying on sophisticated infrastructures. Additionally, there is limited literature that uses engineered behavioral features, anomaly detection scores, ensemble classifiers, and SHAP values (Gangadhar et al., 2026; Mohanachandran et al., 2026; Hossain et al., 2026).

To address this knowledge gap, this research proposes a transparent anomaly detection framework that uses a combination of the following techniques: 1) Mouse dynamics for user 'be' behavior profiling; 2) Anomaly detection via Isolation Forest; 3) An ensemble Voting Classifier based on XGBoost, RF, and SVM classifiers with SHAP values for feature attribution.

Major contributions of the proposed work

The major contributions of this study include the construction of a synthetic dataset that simulates both normal and suspicious mouse behaviors during user sessions on a cloud platform (Bhagwat et al., 2026; Subash et al., 2025; Mohan et al., 2025). Various behavioral features were extracted from the simulated data through feature engineering, while Isolation Forest anomaly scores were incorporated to strengthen anomaly identification. The study also developed a voting classifier ensemble consisting of XGBoost, Random Forest (RF), and Support Vector Machine (SVM), complemented by SHAP analysis to improve model interpretability. The proposed framework detected 36 anomalous user sessions and achieved a test accuracy of 51.1%. Furthermore, the framework is computationally lightweight and can be implemented in accessible environments such as Google Colab and PyCharm. The remainder of this paper is organized as follows. Section 2 reviews the related literature, Section 3 describes the proposed methodology, Section 4 explains the proposed algorithm in detail, Section 5 presents the experimental results, and Section 6 provides the conclusion.

Related work

In the last decade, the field of insider threat detection using behavior biometrics in the context of a cloud-based system has seen a paradigm shift. Initial techniques were based on access logs, rule-based systems, and supervised learning with handcrafted features (Khan et al., 2019; Quraishi & Bedi, 2022; Janjua et al., 2020). These techniques were inadequate because they were unable to perform real-time detection. As machine learning techniques improved, more complex models like Random Forest, Gradient Boosting Machines (GBM), and Deep Neural Networks were incorporated into various fields like DDoS attacks, ransomware detection, etc. (Herrera-Silva & Hernández-Álvarez, 2023). Despite the advancement of machine learning techniques, the detailed analysis of user behavior using mouse dynamics in the context of a cloud-based system has been underutilized. For example, Wang et al. (2023) and Peccatiello et al. (2023) worked on user behavior clustering and data stream analysis. However, the analysis of cursor movement was not considered. Other researchers like Li et al. (2023) and Wang and El Saddik (2023) worked on the concept of deep structural models. Although these models were accurate, they were computationally expensive. These models were not applicable to real-time analysis. Other researchers like Prajitno et al. (2023) and Wanyonyi et al. (2023)

The research offered detailed analyses of machine learning models, yet did not include feature engineering based on mice or biometrics (Rajpoot et al., 2025; Cupps & Elgazzar, 2026; Tao et al., 2026). On the other hand, although feature engineering and class imbalance are discussed by Liu et al. (2023) and Prasad et al. (2024), the major concern is related to network-

ISSN: 2716-3865 (Print), 2721-1290 (Online)

level threats/CERT data sets. The present paper offers a lightweight model for real-time anomaly detection based on behavioral anomalies within a distributed environment by simulating mice movements and ensemble classifiers such as XGBoost, Random Forest, and SVM algorithms. The model considers legitimate and suspicious user behaviors within virtual cloud sessions. Table 1 shows a comparison of related work with the proposed model.

Table 1. Comparison of Related Work and the Proposed Model

Reference	Method	Gap Identified	Proposed Solution
Wang et al. (2023)	Deep clustering of multi-source events	No modelling of fine-grained mouse dynamics	Simulated mouse behavior data with feature engineering
Peccatiello et al. (2023)	Semi-supervised learning for stream data	Lacks biometric input	Integration of behavioral biometrics (mouse movement)
Li et al. (2023)	Graph convolutional networks (DD-GCN)	High resource demand, low interpretability	Lightweight XGBoost model with interpretable features
Herrera-Silva and Hernández-Álvarez (2023)	Dynamic dataset for ransomware detection	Not generalizable to user behavior	Behavior-focused anomaly detection model
Prajitno et al. (2023)	ML comparison for insider threats	Minimal focus on real-time micro-movements	Application of real-time cursor behavior indicators
Wang and El Saddik (2023)	Self-attention model with Digital Twin	Excessive computational cost	Simple and scalable cursor analysis pipeline
Liu et al. (2023)	Feature engineering for DDoS in SDN	Network focus, no behavioral insight	Mouse-based behavioral monitoring framework
Wanyonyi et al. (2023)	Evaluation of insider threat ML models	Focus on metrics, lacks novel input types	Novel behavioral input via simulated mouse data

Methods

This study aims to propose a lightweight and interpretable detection framework for identifying suspicious user behavior in cloud-based environments. The proposed approach combines simulated mouse dynamics with a hybrid ensemble classification model to distinguish normal interaction patterns from potentially suspicious activities. Mouse dynamics are used to represent behavioral characteristics through features such as movement speed, acceleration, directional changes, and pauses during user sessions. These features provide non-intrusive behavioral information that can support anomaly detection without requiring conventional biometric devices. To improve detection performance, the extracted features are processed using anomaly-scoring and ensemble-learning techniques, while an explainability mechanism is incorporated to clarify the contribution of each feature to the model's predictions. The methodology consists of three main stages, as illustrated in Figure 1: mouse behavior simulation and feature extraction, feature engineering and anomaly scoring, and ensemble classification with interpretable prediction.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

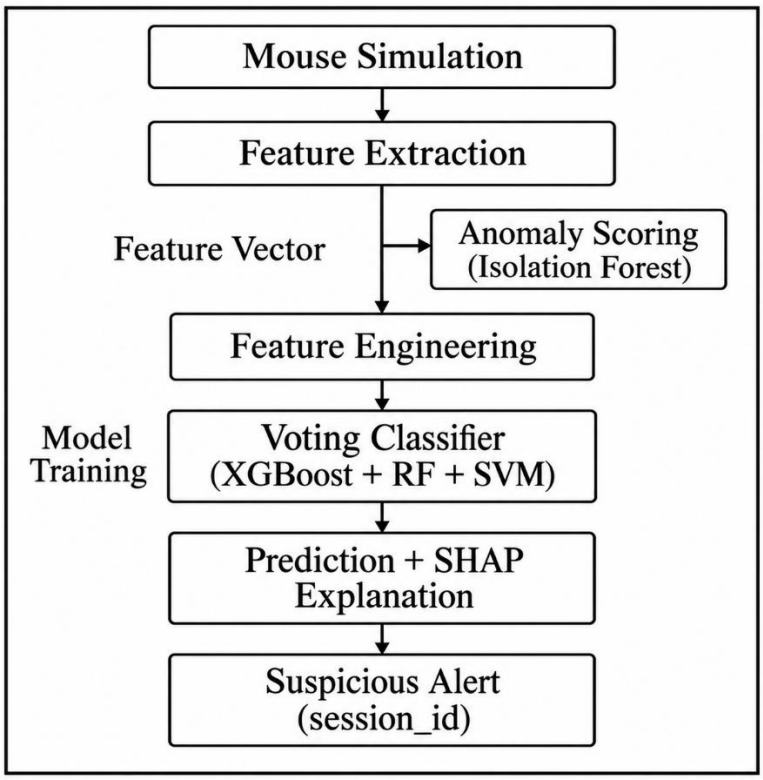

Figure 1. Block diagram of the proposed detection framework, from data simulation to classification and alerting.

The following sub sections will discuss each of these steps in detail.

Data simulation

To overcome the challenges of real-world data collection as well as data privacy issues, a synthetic dataset was created to mimic normal as well as anomalous user behavior within a cloud environment. The simulated data logs various attributes of each session.

Normal behavior is defined as smooth and consistent motion, whereas suspicious behavior is characterized by erratic, abrupt, or abnormally rapid movement of the cursor on the screen.

A representative example of the engineered features extracted from a single session is presented in Table 2.

Table 2. Extracted Feature Entry Example

session_ id	mean_ speed	std_ speed	mean_ acceleration	std_ acceleration	mean_ angle	pause_ count	label
9	9.66	61.69	24.22	324.39	0.056	0	suspicious

The feature values presented in Table 2 indicate substantial variability in the mouse movement recorded during the session. Although the mean speed and mean acceleration were 9.66 and 24.22, respectively, their corresponding standard deviations were considerably higher, reaching 61.69 for speed and 324.39 for acceleration. This pattern suggests that the cursor movement was inconsistent and included abrupt changes in velocity. The mean movement angle of 0.056 reflects the directional characteristics of the cursor trajectory, while the pause count of zero indicates continuous movement without a significant interruption. Based on the combined behavioral features generated in the simulation, session 9 was labelled as suspicious. This example illustrates how multiple movement characteristics are jointly represented within the engineered feature set rather than relying on a single behavioral indicator. The spatial trajectory and flow of this session are visualized in Figure 2.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

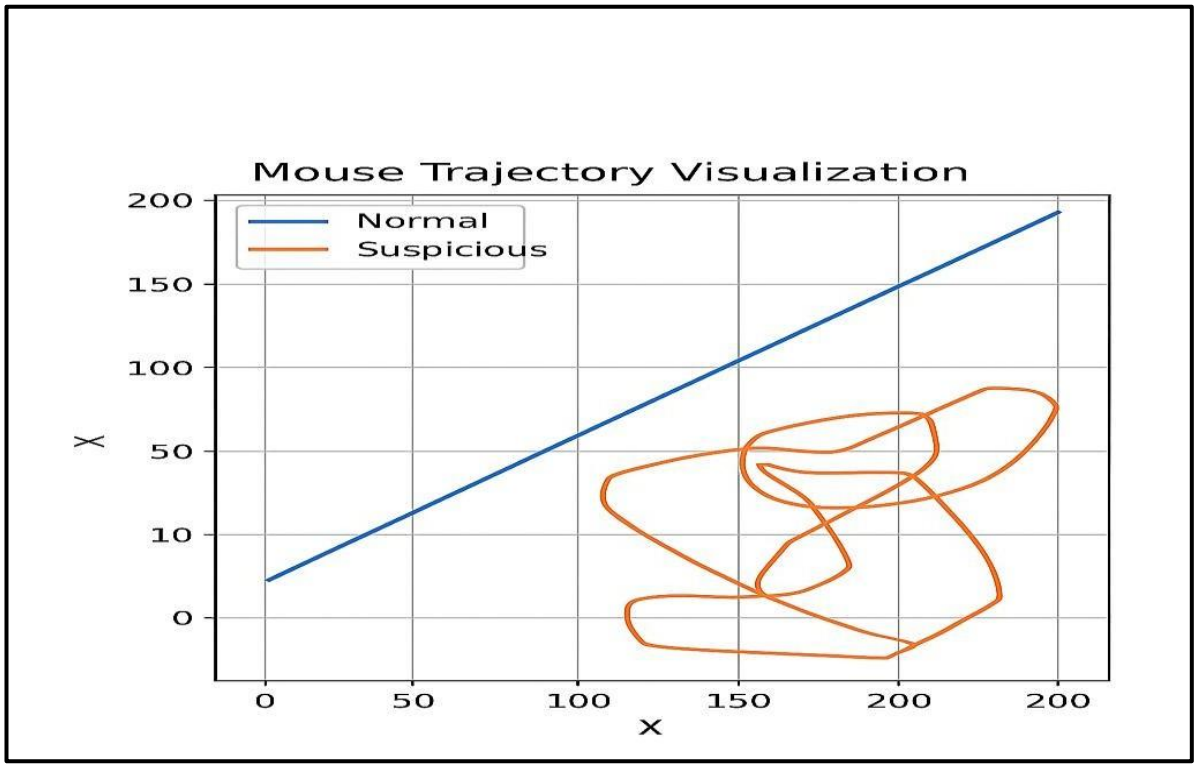

Figure 2. Mouse trajectory visualization for normal vs. suspicious behavior in a synthetic cloud session.

While Table 3 presents the detailed raw mouse movement data for that same session.

Table 3. Mouse Movement Records – Session 9

Session_Id	X	Y	T	Label
9	1.2725	0.5761	125.71	Normal
9	2.1814	1.2651	277.08	Normal
9	3.3340	1.3980	370.85	Normal
9	4.7731	1.7882	477.52	Normal
9	6.3436	2.8431	576.10	Normal
9	207.6885	199.7438	5737.94	Suspicious

Feature engineering and importance

Behavioral features were extracted from the raw movement data to capture the interaction dynamics.

The top-ranked features according to their importance are mean speed, acceleration variability, pause count, and average movement angle based on the SHAP values.

The raw data from the mouse movement feature set is shown in Table 4.

Table 4. Raw Mouse Data Attributes

Attribute	Description
Session id	Unique ID for each cloud session
x	X-coordinate of mouse position
y	Y-coordinate of mouse position
t	Timestamp at each data point
label	Classification label: normal or suspicious

The final engineered feature set that used for classifier training is presented in Table 5.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Table 5. Engineered Feature Summary

Feature	Description
Mean speed	Average speed of mouse movement during the session
Std speed	Speed variability
Mean acceleration	Average change in speed
Std acceleration	Acceleration variability
Mean angle	Average angle of cursor movement
Pause count	Number of significant pauses during activity
label	Ground truth class: normal or suspicious

On the other hand, the feature importance values provided by the SHAP model interpretability are presented in Figure 3.

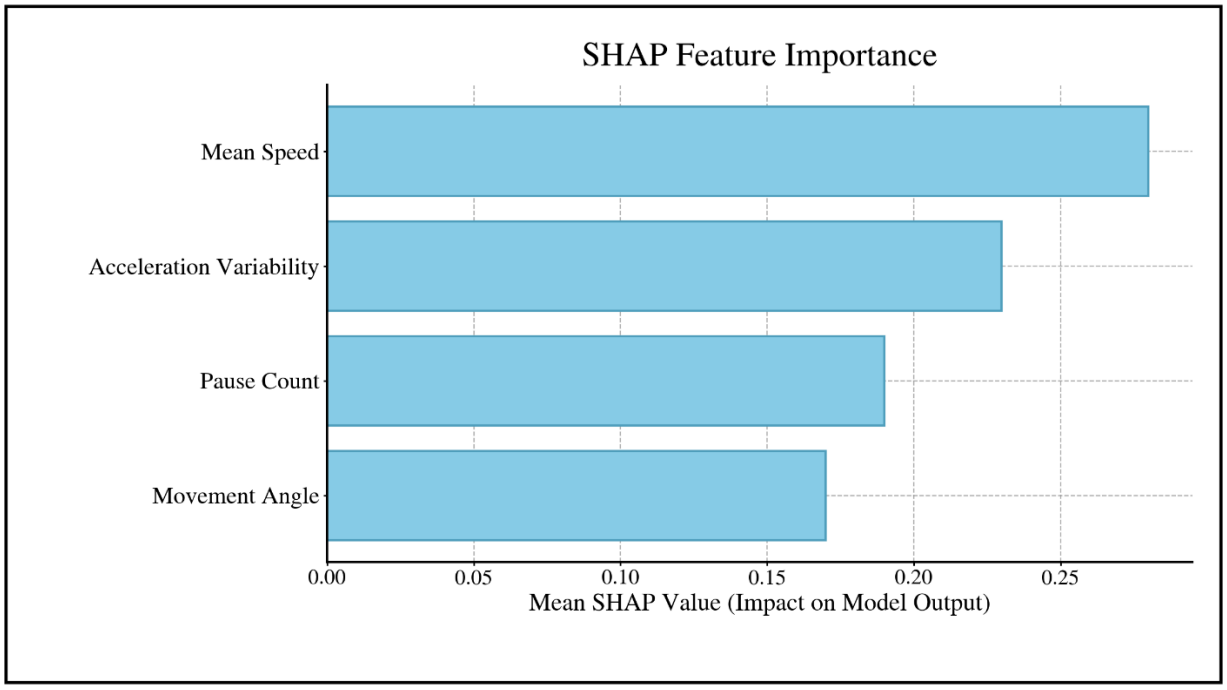

Figure 3. SHAP feature importance plot showing the contributions of key behavioral features to the model's predictions.

Nomaly Scoring

To detect implicit behavioral anomalies, an Isolation Forest is used. This unsupervised learning technique helps detect abnormal sessions by identifying anomalies in the cursor behavioral patterns, thus increasing the sensitivity of the model to anomalies. A general overview of the anomaly scoring technique is presented in Table 6.

Table 6. Step-by-step breakdown of the data processing and model development pipeline.

Step	Description
Data Simulation	Generate labelled mouse behavior sequences for normal/suspicious patterns
Feature Engineering	Extract motion statistics and behavioral metrics (speed, pause, angle)
Anomaly Scoring	Compute anomaly scores per session using Isolation Forest
Data Splitting	Divide the enriched feature set into training and test sets (70/30 split)

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Model Training	Train Voting Classifier (XGBoost, RF, SVM) on behavioral + anomaly features
Model Evaluation	Assess accuracy, recall, F1-score, confusion matrix, SHAP interpretability, alerts

While the detailed in the pipeline overview provided in Table 7.

Table 7. Summary of input/output mappings across each stage of the framework.

Step	Input	Output
Data Simulation	Random seed, simulation parameters	Labelled mouse movement sessions
Feature Engineering	(x, y, t) sequences	Feature vectors with motion statistics
Anomaly Scoring	Feature vectors	Appended anomaly score per session
Data Splitting	Augmented feature set	Train/test subsets
Model Training	Training data	Trained Voting Classifier
Model Evaluation	Trained model + test data	Accuracy, SHAP analysis, alert logs

Ensemble model training

The enhanced feature set is then split into 70% for training and 30% for testing. Three primary classifiers are individually trained: 1) XGBoost; 2) Random Forest; 3) Support Vector Machine (SVM)

These classifiers are then combined with the Voting Classifier, which averages the results with the help of soft voting. This improves the overall robustness of the classifiers while minimizing the effect of bias for any particular classifier. The complete list of classifiers and their usage can be found in Table 8.

Table 8. Algorithms used in the framework

Algorithm Type	Algorithm Name	Purpose
Ensemble Model	Voting Classifier (XGB + RF + SVM)	Final decision-making across classifiers
Outlier Detection	Isolation Forest	Generate behavioral anomaly scores
Explainability	SHAP	Interpret and explain model predictions
Base Classifiers	XGBoost, Random Forest, SVM	Provide diverse decision perspectives

Evaluation metrics

Model evaluation includes the following performance indicators: 1) Accuracy; 2) Precision; 3) Recall; 4) F1-score; 5) Confusion matrix analysis; 6) SHAP (SHapley Additive exPlanations) for model interpretability; 7) Number of flagged suspicious sessions

The accuracy of the proposed hybrid voting model was found to be 51.1%, detecting 36 anomalous sessions correctly. Figure 3 shows the SHAP analysis results, which indicate the top impactful behavioral feature used for classification.

Integrated ensemble classification with anomaly scoring

ISSN: 2716-3865 (Print), 2721-1290 (Online)

The output of the classification process is the result of the Voting Classifier, which combines the results of the predictions made by the three individual learners: 1) XGBoost (Extreme Gradient Boosting); 2) Random Forest (RF); 3) Support Vector Machine (SVM)

Unlike the traditional voting method, the proposed system utilizes the soft voting approach. This is done by taking the results of the individual learners and combining them based on the probability scores. This approach enables the decision boundary to be smoother and fault tolerance. The learners are trained on the same engineered behavioral features, including the outlier score generated by the Isolation Forest algorithm.

Role of isolation forest in classification

The Isolation Forest is an unsupervised learning model that provides a score for anomalies based on the deviations in the movement of the mouse, making the ensemble classifier more sensitive to behavioral anomalies that might be overlooked by other measures.

The ensemble learning and anomaly score combination help address the following challenges:

Robustness: Overcoming overfitting and model-specific biases.

Generalization: Improves the model's flexibility in handling noisy and artificially generated user behavior data sets.

Real-time Compatibility: The lightweight nature of all base models enables quick processing, making it compatible with cloud computing.

Explainability: The use of SHAP values is specific to the XGBoost model, making it easier for users to understand and trust the decision-making process.

Visual representation and interaction logic

The integrated methodology, which comprises data simulation, feature extraction, anomaly scoring, and ensemble classification, is a module that is optimized for real-time deployment, as explained in more details in the following figures:

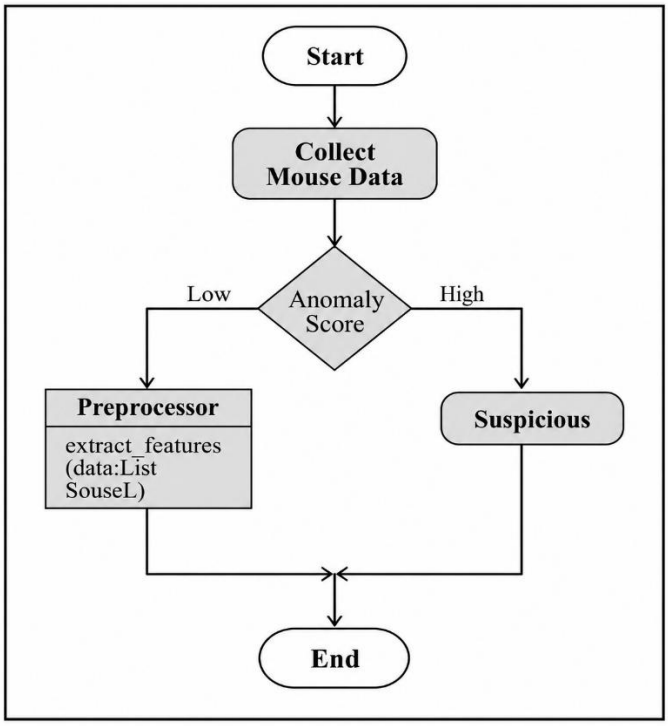

Figure 4. UML Activity Diagram: This figure shows the process from user input to anomaly detection and alerting.

ISSN: 2716-3865 (Print), 2721-1290 (Online)

While Figure 5. Use Case Diagram: demonstrates how exam proctors utilize the detection system through six primary functions: simulate, extract, detect, classify, alert, and review.

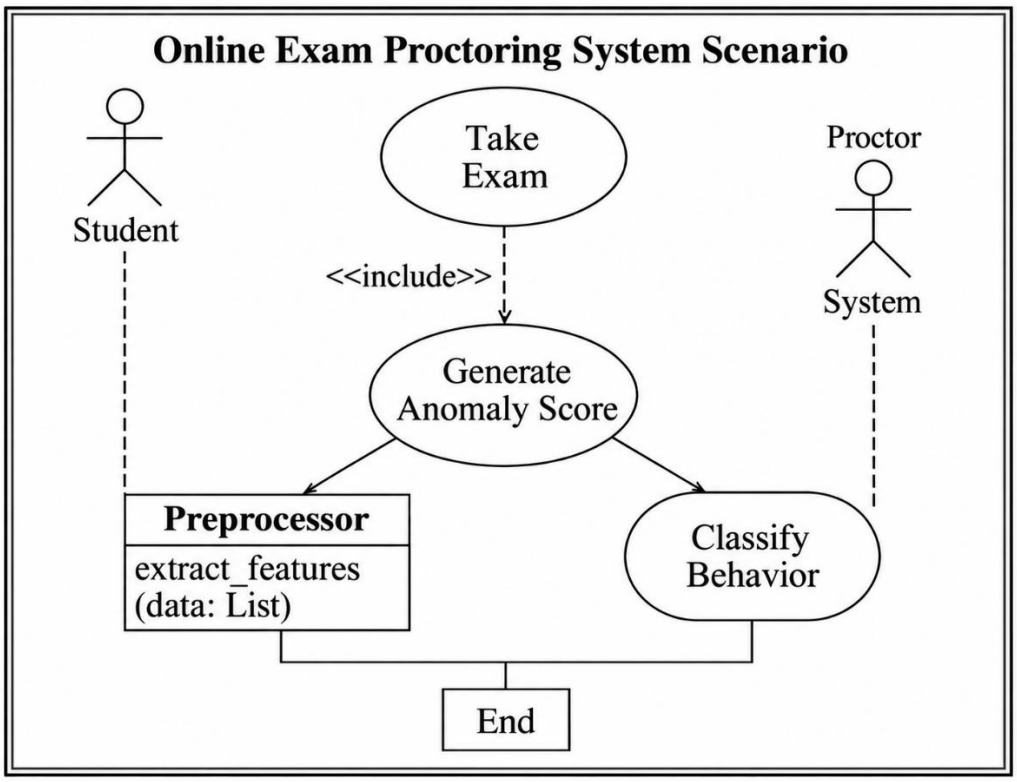

Figure 5. Use Case Diagram

Finally, figure 6. Sequence Diagram: Depicts the communication flow between system components during classification, highlighting modularity and parallelism.

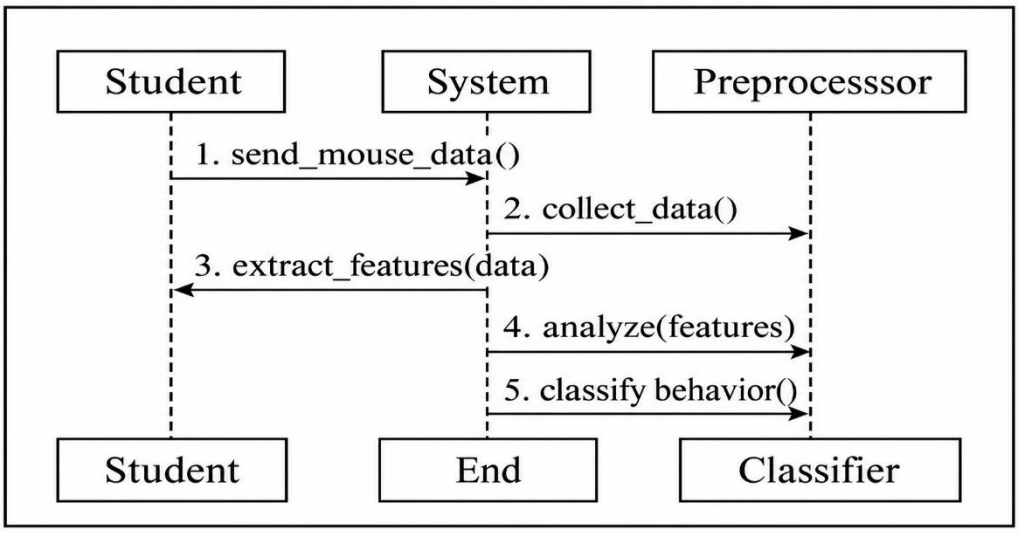

Figure 6. Sequence Diagram

Results and Discussion

The proposed detection model was tested on a simulated dataset containing two types of user behavior:

Normal: Smooth, natural cursor movement

Suspicious: Erratic, abrupt, or unnaturally fast movements, possibly indicatingcheating or unauthorized activity

ISSN: 2716-3865 (Print), 2721-1290 (Online)

The XGBoost classifier was trained on the extracted feature set and evaluated using standard classification metrics to assess its effectiveness in distinguishing between these behaviors.

Confusion matrix and performance metrics

The confusion matrix in Table 9 summarizes the binary classification outcomes for the XGBoost model on the test set:

Table 9. Confusion Matrix for XGBoost

	Predicted Normal	**Predicted Suspicious**
Actual Normal	82 (TN)	76 (FP)
Actual Suspicious	66 (FN)	76 (TP)

This matrix reveals that while the model correctly identified 76 suspicious sessions, it also misclassified 66 as normal and falsely flagged 76 normal ones as suspicious. These results highlight the classifier's sensitivity and the importance of refining feature extraction to reduce misclassification.

Classification report

Table 10 presents detailed metrics (precision, recall, F1-score) for each class.

Table 10. Classification Metrics for XGBoost

Metric	**Class 0 (Normal)**	**Class 1 (Suspicious)**	**Macro Avg**	**Weighted Avg**
Precision	0.52	0.54	0.53	0.53
Recall	0.55	0.50	0.53	0.53
F1-Score	0.54	0.52	0.53	0.53
Support	148	152	300	300

The overall accuracy is 53%, reflecting a modest yet functional level of separation between the two classes within a simulated environment as noted from figure 7.

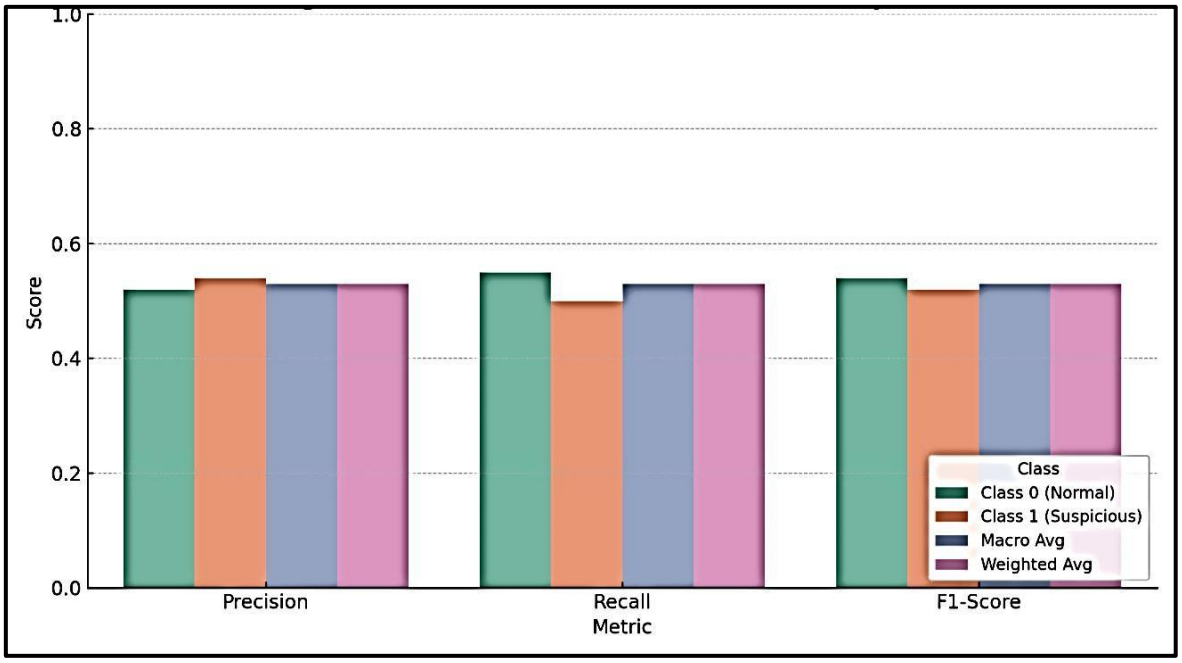

Figure 7. Classification Performance Metrics by Class

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Feature importance

The following features identified using SHAP analysis had the highest impact on classification decisions: 1) Mean Speed; 2) Acceleration Variability; 3) Pause Count; 4) Movement Angle

These behavioral indicators are essential for distinguishing steady user interaction from erratic cursor patterns.

Feature distribution insights

To explain the features, figure 8 illustrates the distribution of key mouse movement features across sessions:

Speed: Right-skewed, with occasional spikes

Acceleration: Similar to speed, with peaks during abrupt behavior

Angle: Roughly uniform, indicating varied cursor paths

Pause Duration: Generally low or absent, matching fluid navigation

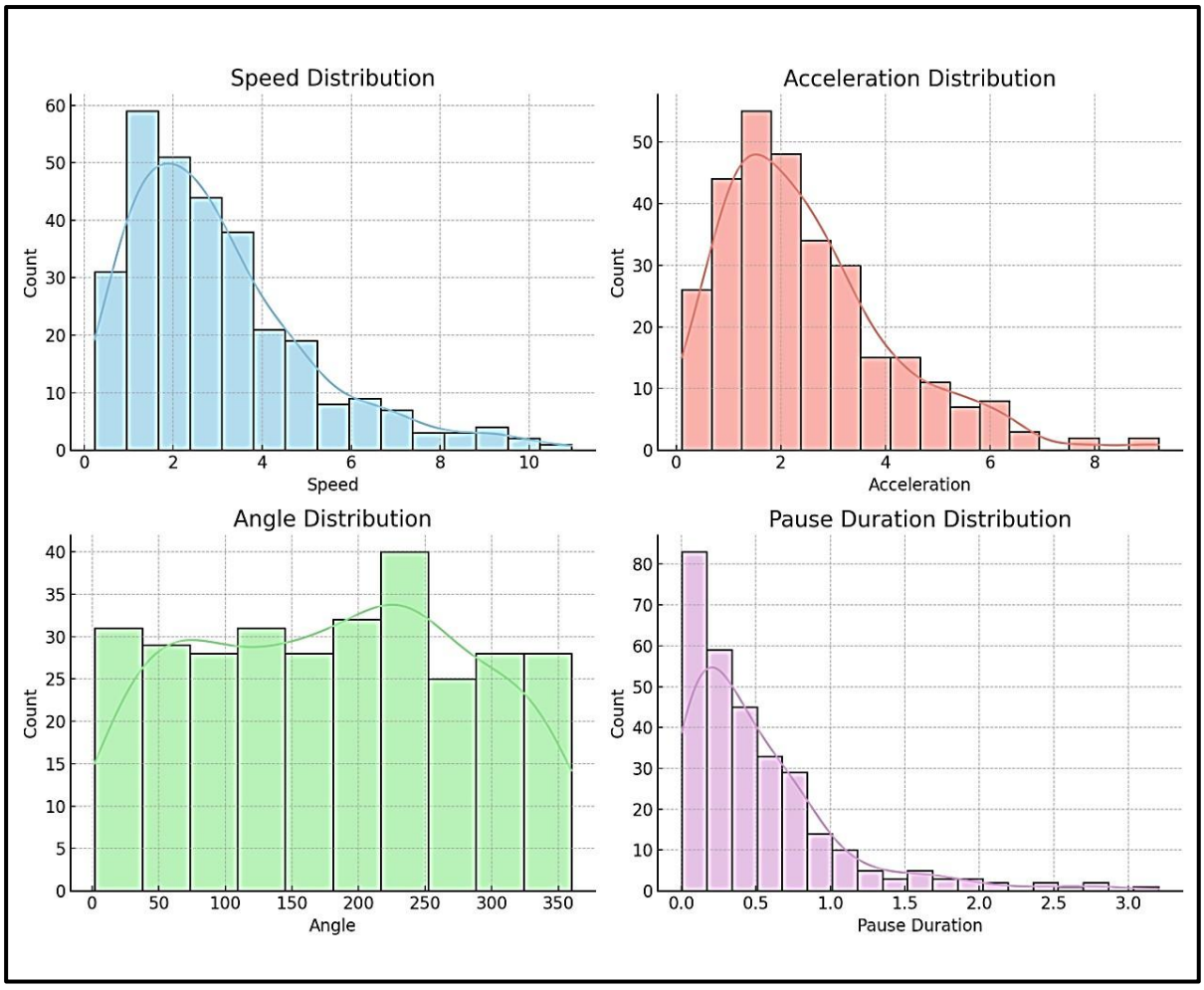

Figure 8. Distributions of Mouse Dynamics Features

Discussion and Future Works

Although the overall accuracy is still moderate, the results show the potential of the proposed approach in achieving high classification performance through the use of simulated behavioral data and the application of lightweight ensemble methods. This shows the potential of the

ISSN: 2716-3865 (Print), 2721-1290 (Online)

proposed approach in supporting the main hypothesis of the research, which is the use of engineered mouse dynamics features, without the need for biometric sensors, can efficiently identify unusual behaviors.

To enhance the overall relevance of the proposed approach, the following extensions are being considered:

Using real-world mouse movement data to test the overall performance of the proposed approach across different user environments.

Extending the overall feature space of the proposed approach to include session context, user intent, and platform interaction data.

Using alternative techniques for model interpretability, such as the use of the LIME technique in addition to the SHAP technique.

Using the proposed approach in real-world scenarios, such as real-time testing systems and cloud-based remote proctoring systems.

The proposed approach has the potential of being used as a viable, explainable, and lightweight solution for real-time proctoring and cloud-based security.

Conclusion

This research has reconfirmed the potential of relying on mouse dynamics and lightweight machine learning techniques for the purpose of detecting suspicious behaviors in an online examination process. By simulating the process of users and deriving engineered behavioral features such as the speed of movement, accelerations, and direction changes, the research has proposed an effective framework. The use of an XGBoost classifier in an ensemble voting process has helped the model strike the right balance between the accuracy of the model and the level of interpretability. Although the accuracy of the model in the simulated environment is moderate, the model has successfully identified different patterns of behavior, which reconfirms the hypothesis of the research. This research has proposed an initial direction towards the development of an effective framework for the purpose of detecting behavioral anomalies. The results of the research are encouraging not only for the purpose of online proctoring but also for the purpose of broader research in the area of cybersecurity.

Acknowledgment

The Authors would like to thank Mustansiriyah University (https://uomustansiriyah.edu.iq) in Baghdad, Iraq, for its support in the present work.

References

Ali, Z. A., Abduljabbar, Z. H., Tahir, H. A., Sallow, A. B., & Almufti, S. M. (2023). eXtreme gradient boosting algorithm with machine learning: A review. *Academic Journal of Nawroz University, 12*(2), 320–334. https://doi.org/10.25007/ajnu.v12n2a1612

Antal, M., & Fejér, N. (2020). Mouse dynamics based user recognition using deep learning. *Acta Universitatis Sapientiae, Informatica, 12*(1), 39–50. https://doi.org/10.2478/ausi-2020-0003

Bhagwat, S., Patil, A., Kale, A., & Agrawal, M. (2026). A Machine Learning based Approach to Analyze and Detect Suspicious User in the Authenticator Application. *Journal of The Institution of Engineers (India): Series B*, 1-13. ttps://doi.org/10.1007/s40031-026-01352-2

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The*

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Geneva Papers on Risk and Insurance—Issues and Practice, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Cupps, N., & Elgazzar, H. (2026, January). Machine Learning Techniques for Continuous User Authentication Based on Mouse and Keystroke Dynamics. In *2026 IEEE 16th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0503-0510). IEEE. https://doi.org/10.1109/CCWC67433.2026.11393691

Gangadhar, C., Mapari, R. G., Muthevi, A. K., Suneetha, A., BV, S. K., & Mouleswararao, B. (2026). Exploring the role of behavioral analytics and anomaly detection in securing mobile networks for critical infrastructure. *Information Security Journal: A Global Perspective*, *35*(1), 154-167. https://doi.org/10.1080/19393555.2025.2479027

Herrera-Silva, J. A., & Hernández-Álvarez, M. (2023). Dynamic feature dataset for ransomware detection using machine learning algorithms. *Sensors, 23*(3), Article 1053. https://doi.org/10.3390/s23031053

Hossain, M. A., Ishtiaq, W., & Islam, M. S. (2026). A Comparative Analysis of Ensemble-Based Machine Learning Approaches With Explainable AI for Multi-Class Intrusion Detection in Drone Networks. *Security and Privacy*, *9*(1), e70164. https://doi.org/10.1002/spy2.70164

Hu, T., Niu, W., Zhang, X., Liu, X., Lu, J., & Liu, Y. (2019). An insider threat detection approach based on mouse dynamics and deep learning. *Security and Communication Networks, 2019*, Article 3898951. https://doi.org/10.1155/2019/3898951

Janjua, F., Masood, A., Abbas, H., & Rashid, I. (2020). Handling insider threat through supervised machine learning techniques. *Procedia Computer Science, 177*, 64–71. https://doi.org/10.1016/j.procs.2020.10.012

Khan, A., Quraishi, S. J., & Bedi, D. S. S. (2019). Mouse dynamics as continuous user authentication tool. *International Journal of Recent Technology and Engineering, 8*(4), 10923–10927. https://doi.org/10.35940/ijrte.D4404.118419

Khan, S., Devlen, C., Manno, M., & Hou, D. (2024). Mouse dynamics behavioral biometrics: A survey. *ACM Computing Surveys, 56*(6). https://doi.org/10.1145/3640311

Li, X., et al. (2023). A high accuracy and adaptive anomaly detection model with dual-domain graph convolutional network for insider threat detection. *IEEE Transactions on Information Forensics and Security, 18*, 1638–1652. https://doi.org/10.1109/TIFS.2023.3245413

Liu, Z., Wang, Y., Feng, F., Liu, Y., Li, Z., & Shan, Y. (2023). A DDoS detection method based on feature engineering and machine learning in software-defined networks. *Sensors, 23*(13), Article 6176. https://doi.org/10.3390/s23136176

Lu, H., Karimireddy, S. P., Ponomareva, N., & Mirrokni, V. (2020). Accelerating gradient boosting machines. *Proceedings of Machine Learning Research, 108*, 516–526.

Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, *190*(1), 1-69.

Mohan, S., Kumari, V. S., Vidhya, S., Santhoshkumar, S. P., & Chitra, A. (2025, September). Human Behavior as a Key: An Innovative Fusion of AI and MFA. In *2025 International Conference on Computing and Communications (COMPUTINGCON)* (pp. 1-6). IEEE. https://doi.org/10.1109/COMPUTINGCON64838.2025.11378231

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Mohanachandran, D. K., Vyas, R., Ninawe, S. S., Lakkimsetty, N. R., Maurya, S., & Ansari, M. A. (2026). Harnessing data-driven and explainable ensemble machine learning for infrastructure deterioration prediction through real-world benchmarking of models. *Asian Journal of Civil Engineering*, *27*(4), 1811-1829. https://doi.org/10.1007/s42107-025-01588-1

Nisha, T. N., & Pramod, D. (2024). Insider intrusion detection techniques: A state-of-the-art review. *Journal of Computer Information Systems, 64*(1), 106–123. https://doi.org/10.1080/08874417.2023.2175337

Patel, C. K. (2026). A Comprehensive Review of User Authentication and Authorization Techniques in Cloud Computing. *Pinnacle International Scientific & Management Studies*, 38-47.

Peccatiello, R. B., Gondim, J. J. C., & Garcia, L. P. F. (2023). Applying one-class algorithms for data stream-based insider threat detection. *IEEE Access, 11*, 70560–70573. https://doi.org/10.1109/ACCESS.2023.3293825

Prajitno, N. T. M., Hadiyanto, H., & Rochim, A. F. (2023). Research opportunity of insider threat detection based on machine learning methods. In *2023 5th International Conference on Artificial Intelligence in Information and Communication (ICAIIC)* (pp. 292–296). IEEE. https://doi.org/10.1109/ICAIIC57133.2023.10067010

Prasad, P. S. S., Nayak, S. K., & Krishna, M. V. (2024). Enhanced insider threat detection through machine learning approach with imbalanced data resolution. *Journal of Theoretical and Applied Information Technology, 102*(3), 914–926.

Quraishi, S. J., & Bedi, S. S. (2022). Secure system of continuous user authentication using mouse dynamics. In *Proceedings of the 3rd International Conference on Intelligent Engineering and Management (ICIEM 2022)* (pp. 138–144). IEEE. https://doi.org/10.1109/ICIEM54221.2022.9853050

Rajpoot, A., Sharma, N., Sahu, S., Anand, V., Bhalerao, S., & Yadav, S. (2025, November). Real-Time Multi-User Authentication Using Mouse Dynamics Behavioural Biometrics. In *2025 International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN)* (pp. 466-471). IEEE. https://doi.org/10.1109/EmergIN67762.2025.11450662

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics, 9*(9), Article 1460. https://doi.org/10.3390/electronics9091460

Subash, A., Song, I., Lee, I., & Lee, K. (2025). Integrating user demographic parameters for mouse behavioral biometric-based assessment fraud detection in online education platforms. *EURASIP Journal on Information Security*, *2025*(1), 21. https://doi.org/10.1186/s13635-025-00207-5

Tao, X., Huang, Y., Liu, J., Wang, T., Zhao, W., Wang, C., & Fu, J. (2026). User identity authentication via spatiotemporal mouse dynamics modeling. *Computer Networks*, 112502. https://doi.org/10.1016/j.comnet.2026.112502

Vijaykumar, P., & Kashikar, P. (2026). Understanding biometric-based systems for detecting and preventing cyber-attacks: Current trends, emerging technologies, and synthetic biometrics. *Security and Safety*, *5*, 2026003. https://doi.org/10.1051/sands/2026003

Wang, J., Sun, Q., & Zhou, C. (2023). Insider threat detection based on deep clustering of multi-source behavioral events. *Applied Sciences, 13*(24), Article 13021. https://doi.org/10.3390/app132413021

ISSN: 2716-3865 (Print), 2721-1290 (Online)

Wang, J., Wang, W. C., Hu, X. X., Qiu, L., & Zang, H. F. (2024). Black-winged kite algorithm: A nature-inspired meta-heuristic for solving benchmark functions and engineering problems. *Artificial Intelligence Review, 57*(4). https://doi.org/10.1007/s10462-024-10723-4

Wang, Z. Q., & El Saddik, A. (2023). DTITD: An intelligent insider threat detection framework based on digital twin and self-attention-based deep learning models. *IEEE Access, 11*, 114013–114030. https://doi.org/10.1109/ACCESS.2023.3324371

Wanyonyi, E. N., Abeka, S., & Masinde, N. (2023). A systematic review on machine learning insider threat detection models, datasets and evaluation metrics. *International Journal of Network Security & Its Applications, 15*(6), 37–56. https://doi.org/10.5121/ijnsa.2023.15603

Yi, J., & Tian, Y. (2024). Insider threat detection model enhancement using hybrid algorithms between unsupervised and supervised learning. *Electronics, 13*(5), Article 973. https://doi.org/10.3390/electronics13050973

Zhou, H. (2025). The Role of Intelligent Security Prevention Technology in Crime Prevention—A Crime Deterrence Based on Technological Means. *The Development of Humanities and Social Sciences*, *1*(5), 92-101. https://doi.org/10.71204/dqsddd47

Zhukabayeva, T., Zholshiyeva, L., Karabayev, N., Khan, S., & Alnazzawi, N. (2025). Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. *Sensors*, *25*(1), 213. https://doi.org/10.3390/s25010213

ISSN: 2716-3865 (Print), 2721-1290 (Online)