Decision letter (Initial Submission)

Decision on Manuscript # CPE-25-0596

From: nitin@iitrpr.ac.in
To: arulselvam.cse@hicet.ac.in, arulselvamme@gmail.com, tamijeselvy@gmail.com

12-Aug-2025

Dear Dr. P. Arul Selvam:

Manuscript # CPE-25-0596 entitled "Explainable AI (XAI) for Insider Threat Detection: Balancing Security and Transparency in Cloud Computing" which you submitted to Concurrency and Computation: Practice and Experience has been reviewed and the comments of the referee(s) and Associate Editor are included at the bottom of this letter.

I felt that your paper requires some revision before it can be reconsidered and hope that you will submit a revised version of your manuscript that takes into account the comments of the referee(s), which are included at the bottom of this letter. Your revision is due in 90 days, on 10-Nov-2025. If you require an extension please contact the Editorial Office at CCPE@wiley.com.

Associate Editor Recommendation: Recommendation #1: Major Revision

Our journal is currently transitioning to Wiley's Research Exchange submission portal. Please read these instructions carefully.

If you submitted your manuscript through our Research Exchange site, you will see a link below to submit your revised manuscript:
https://wiley.atyponrex.com/submissionBoard/1/ecc72128-5c37-4563-a1ea-05b424c7748b/current
(If no link appears, the instructions in the next paragraph.) Click on the link or go to wiley.atyponrex.com/journal/cpe. Sort by journal and submission status to locate this manuscript, then click the "Revise submission" button to submit your revision. You will be able to respond to the reviewer follow comments when asked to "Upload your Author Response". All supplementary and additional files will be carried over when you submit a revised manuscript. You may be required to provide additional files at the revision stage.

If you submitted your manuscript through ScholarOne, please use this link to submit your revised manuscript:
*** PLEASE NOTE: This is a two-step process. After clicking on the link, you will be directed to a webpage to confirm. ***

https://mc.manuscriptcentral.com/cpe?URL_MASK=f91099ec82224d639aa3a6bbcb55322e
Click on the link or go to https://mc.manuscriptcentral.com/cpe and enter your Author Center, where you will find your manuscript title listed under "Manuscripts with Decisions." Under "Actions," click on "Create a Revision". You will be able to respond to the comments made by the reviewer(s) in the space provided. Your original files are available to you when you upload your revised manuscript. Please delete any redundant files before completing the submission.

Please note that submitting a revision of your manuscript does not guarantee eventual acceptance, and your revision may be subject to re-review by the referee(s) before a decision is rendered.

Thank you and I look forward to reading your updated paper soon.

Sincerely,

Decision letter (Initial Submission)

Decision on Manuscript # CPE-25-0596

Associate Editor
Comments to the Author :
Request authors to incorporate the review suggestions in a revision.

Referee(s)' Comments to Author:

Reviewer: 1

Comments to the Author
Core idea of the manuscript is good but that is not enough to publish the paper in a reupdated journal. Explanation of methodology section is so moderate. Experimental analysis also not satisfactory. So, the decision is that the manuscript can not be accepted

Reviewer: 2

Comments to the Author
XAI Implementation: Clarify how SHAP, LIME, and counterfactual reasoning are applied and how their outputs support threat interpretation.

Evaluation: Include baseline comparisons with black-box models and address performance in large-scale or real-time cloud environments.

Security Analyst Role: Explain how analysts use the XAI insights in practice; user feedback or examples would strengthen this.

Reviewer: 3

Comments to the Author
The manuscript presents a timely and relevant contribution to the field of cloud security, focusing on the integration of Explainable AI (XAI) techniques for insider threat detection. There are few minor corrections required in the manuscript.

1. On first use, all acronyms (e.g., SHAP, LIME, XAI) should be fully expanded with their abbreviations in parentheses. This is done inconsistently throughout the paper.
2. The paper proposes integrating SHAP, LIME, and counterfactuals with common ML algorithms (like XGBoost, RF, Neural Nets). However, these combinations are already well documented in recent literature. The novelty of the paper must be discussed.
3. XAI techniques could leak sensitive attributes when explaining decisions. The privacy preserving concerns must be discussed within the scope of the paper.
4. Metrics like "Explainability Score" and "Fidelity Score" are not formally defined.
5. Future work is conceptually good but lacks technical depth.
6. Experimental results are comprehensive, but there is limited discussion on scalability, data privacy in explanation, and computational performance under real-time constraints. 7. A concern is the overstatement of detection accuracy of 96.4%, in results and conclusion do not align with the values shown in Table 1.
8. Reference numbers may be checked again. Please see ref. numbers [5] and [10] which appear inline without clear matching in-text context.
9. Please ensure consistency in reference formats.

a good addition, and the figures and tables make the results easier to follow.
Given the importance of the topic and the potential of the paper, it is suggested that a few points be addressed to help improve the overall quality of the work.

Major issues:

1. Lack of transparency in the data source(s) (Section 4,1, Page 9)
This section mentions that “real-world cloud activity reports” were used to evaluate the model, but no explanation is provided about the data sources, how the data was accessed, the time frame, or the collection method.
Suggestion: For greater transparency or validation of this section, it is essential to clarify how and where the data was collected, and whether it was extracted from a real environment or was simply structured like operational reports.

2. Unclear definition of the “Explainability Score” (Table 1 and Figure 5)
The paper presents this score as a user-focused metric, but it doesn’t explain how it’s technically calculated, what components it includes, or whether it’s based on any known method or source.
Suggestion: Since explainability is one of the main objectives of the paper, the paper would benefit from a clearer explanation of how the explainability score is calculated, including its components and scoring method — or a reference if it follows an existing approach.

3. Unclear source of comparative models (Table 1)
Although the proposed model has been compared with models such as Decision Tree + XAI (SHAP), Random Forest + XAI (LIME), and other hybrid models, it is not clear whether these comparisons were reproduced by the authors or if the results were taken from previous studies.
Suggestion: Clarifying this point would strengthen both the methodological validity and the novelty of the work.

4. Lack of formal statistical analysis (Section 4.4, page 11)
The paper reports several detection metrics such as Accuracy, Precision, Recall, and F1-Score, but does not include any statistical analysis (e.g., t-tests, standard deviation, or confidence intervals). This weakens the strength of inference and the reliability of the reported differences.
Suggestion: Including at least one statistical test or variability measure would help support the performance comparison more convincingly.

Minor issues:

1. Lack of clearly stated innovation compared to prior work (Sections 1.3, page 2 and 2.4, page 5)
Although the research objectives are presented in Section 1.3 and the research gaps are discussed in Section 2.4, the paper does not clearly explain what its specific innovation is compared to previous studies—whether in terms of the model, methodology, type of data, or evaluation approach.
Suggestion: To make the contribution of the paper clearer, it would help if the authors explained more directly what makes their work different from earlier studies — for example, at the end of the introduction or wherever it is considered most appropriate.

2. Unclear use of incremental learning (Section 3,3, page 8)

The paper states that the model learns continuously using incremental learning techniques, but it doesn't explain what methods or algorithms are used.
Suggestion: It would help to clarify which technique is used for incremental learning.

3. Incorrect citation of reference [9] (Section 4.3, Page 11)

Decision letter (Initial Submission)

Decision on Manuscript # CPE-25-0596

In the beginning of the paragraph, where the paper refers to specific numbers—such as a 27% reduction in false positives—or mentions SHAP outputs, no direct citation to the relevant figures is provided.
Suggestion: It would be better to include figure references (e.g., Figure 6 and Figure 7) in the same sentences to avoid ambiguity and improve citation consistency.

5. Inconsistent accuracy claim (Section 4.4, Page 11)
It is mentioned that the proposed model achieves an accuracy of 96.4%, but no model in Table 1 shows this value. The highest reported accuracy in the table is 95.2%, which belongs to a non-XAI model, while the relevant XAI-based model shows 94.5%.
Suggestion: This number should match the table, or—if it comes from a separate experiment— it would be helpful to briefly explain where it comes from and how it was evaluated.

Final Recommendation: Major Revision
A major revision is recommended so the authors can strengthen the paper by addressing the key points discussed above.

Reviewer: 5

Comments to the Author
In this paper, authors investigate the insider threats that pose a significant risk to cloud computing environments. As traditional AI-based threat detection systems are not effective, the authors explores the use of Explainable AI (XAI) to enhance insider threat detection by providing transparency and interpretability in cloud security systems. The proposed approach integrates machine learning (ML) models with explainability techniques, such as SHAP (Shapley Additive Explanations), LIME (Local Interpretable Model-Agnostic Explanations), and counterfactual reasoning, to help security analysts understand the factors influencing threat detection. By applying XAI-driven anomaly detection to real-world cloud activity datasets, our study demonstrates that interpretable models can accurately detect insider threats while minimizing false positives. The findings highlight the importance of balancing security, accuracy, and explainability to build more trustworthy AI-driven security frameworks.
However, the paper is difficult to be accepted in its current state. The problems of the paper is listed below:
In the first place, the paper is poorly written and organized, which makes it hard to understand the motivation as well as the contributions of the proposal in this paper. The authors failed to point out the current development of threat detection in cloud, especially the concrete purpose they designed the proposal.
In the second place, the novelty of the proposed scheme is also poor. The work in this paper looks like an implementation of several tools in threat detection in cloud rather than a research paper. Thus, it is hard to make it clear what the novelty or contribution in this paper.
In the last place, there exists a large amount of typo errors in this paper and the authors are unable to validate their proposal by effectively comparing with SOTA schemes. All of these failures make it hard to read and accept for this paper.