A HYBRID MACHINE LEARNING APPROACH FOR DETECTING INTENTIONAL AND UNINTENTIONAL INSIDER THREATS WITH MITIGATION THROUGH BEHAVIORAL BIOMETRICS AND USER PROFILING MECHANISM

By

Ms. S. Asha

(20PHCSF005)

Supervisor

Dr. D. Shanmugapriya

Assistant Professor

A Thesis Submitted to

Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore – 641 043

In partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Computer Science

July 2025

80_RECOMMENDATION

The proposed research employs a hybrid machine learning approach that successfully identifies insider threats and incorporated behavioural biometrics with user profiling to mitigate both intentional and unintentional insiders, laying a strong foundation for future advancements. Potential directions include:

A methodology comprising of three phases is proposed. It consist of Preprocessing and Insider Detection (P&ID) in Phase I, Unintentional Insider Mitigation (UIM) in Phase II, and Intentional Insider Mitigation (IIM) in Phase III.

Phase I of Preprocessing and Insider Detection ensures detection and classification of both intentional and unintentional insider threats using tuned Nearmiss-2 sampling technique with hybrid B-SVM algorithm that successfully handles class imbalance problem with minimal misclassification rate. However, future research could focus on real-time deployment and analyse the daily log activities using Agentic AI, and explainable AI techniques with privacy preserving learning to ensure secure, and trustworthy insider threat detection.

Phase II of Unintentional Insider Mitigation successfully mitigates unintentional insiders using combined CKPCA for feature engineering with Deep Belief Network for user authentication which achieves increased mitigation accuracy and minimal error rate. Future research into adaptive multimodal authentication framework, continuous learning strategies, and deep learning models to enhance mitigation accuracy for mitigating unintentional insiders.

Phase III of Intentional Insider Mitigation successfully mitigates intentional insider using decision tree to predict user risk for user profiling mechanism. The current approach profiles low risk users into Allowlist and high risk users into Denylist. However, the future research could implement new list as “Re-entry” where intentional insiders from Denylist can be forwarded to Allowlist based on adaptive trust evaluation, behavioral re-authentication, and compliance validation mechanisms.