Avinashilingam Institute for Home Science and Higher Education for Women
(Deemed to be University Estd. u/s 3 of UGC Act 1956, Category A by MHRD)
Re-accredited with 'A++' Grade by NAAC.CGPA 3.65/4, Category I by UGC
Coimbatore – 641 043, Tamil Nadu, India

PLAGIARISM CHECK REPORT (THESIS)

1.	Name of the Research Scholar	Asha. S
2.	Roll No. and Year of Registration	20PHCSF005, 2021
3.	Department	Computer Science
4.	Name of the Research Guide	Dr. D. Shanmugapriya
5.	Title of the Thesis / Dissertation	A Hybrid Machine Learning Approach for Detecting Intentional and Unintentional Insider Threats with Mitigation Through Behavioral Biometrics and User Profiling Mechanisms
6.	Similarity Content (%) Identified	**4%**
7.	Software Used	Turnitin
8.	Date of Verification	08-07-2025

Note : The report is excluding 14 Consecutive words, Review of Literature and Quoted Materials.

Checked by :

8/7/25
Information Scientist

Asha. S
Research Scholar

08.07.25
Assistant Librarian

8/7/25
Research Guide

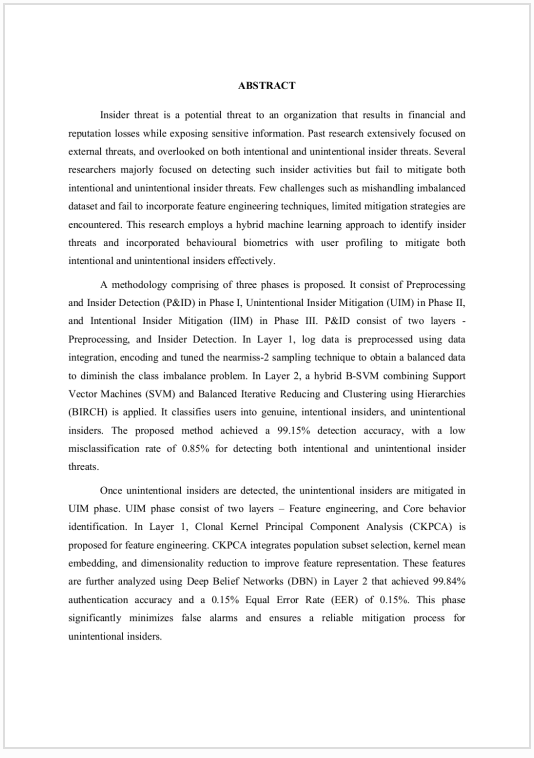
Date: 08-07-2025

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Central Library Avinashilingam
Assignment title:	Paper 2024
Submission title:	A Hybrid Machine Learning Approach for Detecting Intentional...
File name:	Plagiarism_AI.doc
File size:	3.87M
Page count:	121
Word count:	27,967
Character count:	163,830
Submission date:	08-Jul-2025 04:15PM (UTC+0530)
Submission ID:	2333685937



ABSTRACT

Insider threat is a potential threat to an organization that results in financial and reputation losses while exposing sensitive information. Past research extensively focused on external threats, and overlooked on both intentional and unintentional insider threats. Several researchers majorly focused on detecting such insider activities but fail to mitigate both intentional and unintentional insider threats. Few challenges such as mishandling imbalanced dataset and fail to incorporate feature engineering techniques, limited mitigation strategies are encountered. This research employs a hybrid machine learning approach to identify insider threats and incorporated behavioural biometrics with user profiling to mitigate both intentional and unintentional insiders effectively.

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. P&ID consist of two layers - Preprocessing, and Insider Detection. In Layer 1, log data is preprocessed using data integration, encoding and tuned the nearmiss-2 sampling technique to obtain a balanced data to diminish the class imbalance problem. In Layer 2, a hybrid B-SVM combining Support Vector Machines (SVM) and Balanced Iterative Reducing and Clustering using Hierarchies (BIRCH) is applied. It classifies users into genuine, intentional insiders, and unintentional insiders. The proposed method achieved a 99.15% detection accuracy, with a low misclassification rate of 0.85% for detecting both intentional and unintentional insider threats.

Once unintentional insiders are detected, the unintentional insiders are mitigated in UIM phase. UIM phase consist of two layers – Feature engineering, and Core behavior identification. In Layer 1, Clonal Kernel Principal Component Analysis (CKPCA) is proposed for feature engineering. CKPCA integrates population subset selection, kernel mean embedding, and dimensionality reduction to improve feature representation. These features are further analyzed using Deep Belief Networks (DBN) in Layer 2 that achieved 99.84% authentication accuracy and a 0.15% Equal Error Rate (EER) of 0.15%. This phase significantly minimizes false alarms and ensures a reliable mitigation process for unintentional insiders.

Copyright 2025 Turnitin. All rights reserved.

A Hybrid Machine Learning Approach for Detecting Intentional and Unintentional Insider Threats with Mitigation Through Behavioral Biometrics and User Profiling Mechanisms

by Central Library Avinashilingam

Submission date: 08-Jul-2025 04:15PM (UTC+0530)
Submission ID: 2333685937
File name: Plagiarism_AI.doc (3.87M)
Word count: 27967
Character count: 163830

A Hybrid Machine Learning Approach for Detecting Intentional and Unintentional Insider Threats with Mitigation Through Behavioral Biometrics and User Profiling Mechanisms

ORIGINALITY REPORT

4%	2%	3%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Asha S, Shanmugapriya D, Padmavathi G. "Malicious insider threat detection using variation of sampling methods for anomaly detection in cloud environment", Computers and Electrical Engineering, 2023 Publication	<1%
2	Asha S., Shanmugapriya D.. "Understanding insiders in cloud adopted organizations: A survey on taxonomies, incident analysis, defensive solutions, challenges", Future Generation Computer Systems, 2024 Publication	<1%
3	Nhien Rust-Nguyen, Shruti Sharma, Mark Stamp. "Darknet Traffic Classification and Adversarial Attacks Using Machine Learning", Computers & Security, 2023 Publication	<1%
4	i-scholar.in Internet Source	<1%