SPECIMEN FORMAT FOR THESES OF MONTH

Faculty	**:**	School of Physical Sciences and Computational Sciences
Department	**:**	Computer Science
Branch/ Area:	**:**	Artificial Intelligence, Cyber Security
Sub Subject Heading:	**:**	-
Candidate's Name	**:**	S.Asha
Candidate's Address with email	**:**	2/7B Kalliyappan Street, Rathinapuri, Sivanandha Colony, Coimbatore – 641027. asha.sharfudeen97@gmail.com
Title of the thesis	**:**	A Hybrid Machine Learning Approach for Detecting Intentional and Unintentional Insider Threats with Mitigation through Behavioral Biometrics and User Profiling Mechanism
(i) In Roman Script (ii) In roman Script		-
Nomenclature of Degree:	**:**	Ph.D
Month & Year of Enrolment:	**:**	January 2021
Month & Year of Registration:	**:**	January 2021
Month &Year of Submission:	**:**	July 2025
Month &Year of Award	**:**	February 2026
Name of Supervisor	**:**	Dr.D.Shanmugapriya
Designation of Supervisor	**:**	Assistant Professor and Head, Department of Information Technology

Centre/department/school in which research was conducted	**:**	Department of Computer Science, School of Physical Sciences and Computational Science
University's Name & Address	**:**	Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore – 641043.

Abstract within 300 words:

Insider threat is one of the major security challenges in any organization due to the substantial financial consequences while handling sensitive information. It is crucial to detect and mitigate both intentional and unintentional insider threats. At present, machine learning techniques have been scrutinized for detection and mitigation. However, past research fails to focus on developing a combined framework for detecting and mitigating both intentional and unintentional insider threats while handling class imbalance problem and advanced feature engineering. Hence, a novel methodology is proposed and introduced as a three-phase module: Phase-1) Preprocessing & Insider Detection, which preprocesses log data and uses a hybrid B-SVM algorithm to classify users into genuine, intentional and unintentional insider based on abnormal behavior; Phase-2) Unintentional-insider Mitigation (UIM), which authenticates unintentional insiders using behavioral biometric via keystroke dynamics and enhanced the performance using Clonal-Kernel Principal Component Analysis (CKPCA) with Deep Belief Network for classifying unintentional insider into genuine and intentional insider; and Phase-3) Intentional-insider Mitigation (IIM), which profiles users using Decision Tree based on risk predicted as high risk and low risk. The high risk user are profiled into Allowlist and low risk users are profiled into Denylist. The proposed methodology achieves high accuracy in detecting and mitigating insider threats, as evaluated and validated on the CERT Insider Threat Dataset and CIC darknet dataset.

With CERT dataset, P&ID detected 8 intentional and one unintentional insider among 250,078 logs. UIM mitigated one unintentional insider as an intentional insider. IIM profiled 57 genuine users in Allowlist and 8 intentional insiders in Denylist. In case of CIC darknet dataset, P&ID detected 4,783 intentional-Darknet users and 68 unintentional Darknet users among 134,305

daily activities. UIM mitigated 68 unintentional-Darknet users as 64 Intentional-Darknet, 4 benign users. IIM profiled 5063 benign users in Allowlist, 4847 Intentional-Darknet users in Denylist.

i) Major objectives :

The primary objective is to detect and mitigate both intentional and unintentional insider threats. The secondary objectives are as follows,

- To detect and classify both intentional and unintentional insider threats by effectively addressing the challenges of class imbalance and increased misclassification rate.
- To mitigate unintentional insiders by enhancing mitigation accuracy and minimized error rates in user authentication system.
- To mitigate intentional insiders through user profiling mechanism

ii) Hypothesis:

This research hypothesizes that the proposed three-phase methodology for intentional and unintentional insider threat detection and mitigation significantly enhances detection and mitigation accuracy for both intentional and unintentional insider threats compared to existing state-of-the-art methods.

iii) Methodology :

The methodology comprise of three phases: Phase I for Preprocessing and Insider Detection (P&ID), Phase II for Unintentional Insider Mitigation (UIM), Phase III for Intentional Insider Mitigation (IIM). Phase I (P&ID) consist of two layers: Preprocessing and Insider Detection. In the preprocessing layer, techniques such as data integration, encoding and a tuned nearmiss-2 sampling technique are performed to handle class imbalance problem in log data. In the Insider Detection layer, a hybrid B-SVM algorithm is applied to classify users into genuine users, intentional insiders, and unintentional insiders. Phase II (UIM) mitigates the unintentional insiders detected in Phase I. UIM consists of two layers: Feature engineering and Core Behavior Identification. In the Feature engineering layer, Clonal Kernel Principal Component Analysis (CKPCA) is proposed to improve feature representation. Then, in the Core Behavior Identification

layer, the extracted features are analyzed using Deep Belief Networks (DBN) to classify unintentional insiders into genuine users and intentional insiders.

Phase III (IIM) mitigates the detected intentional insiders using a user profiling mechanism based on their authentication outcomes. IIM consists of three layers: Data preprocessing, Model training and evaluation, and User profiling. Data preprocessing is performed using label encoding and train–test splitting. Model training and evaluation are conducted using a Decision Tree classifier to predict user risk levels as low-risk or high-risk. User profiling is then performed by profiling low-risk users into the Allowlist and high-risk users into the Denylist.

iv) Findings:

The methodology is evaluated using the CERT Insider Threat Dataset and validated using the CIC Darknet Dataset. Phase I (P&ID) achieved a detection accuracy of 99.15%, with a low misclassification rate of 0.85%, for detecting both intentional and unintentional insider threats using both the CERT Insider and CIC Darknet datasets. Phase II (UIM) achieved 99.84% mitigation accuracy and Equal Error Rate of 0.15% using both CMU keystroke and collected keystroke datasets. Phase III (IIM) achieved 100% accuracy for user profiling into the Allowlist and Denylist.

With CERT dataset, P&ID detected 8 intentional insiders and 1 unintentional insider among 250,078 log activities. UIM mitigated 1 unintentional insider as an intentional insider. IIM profiled 57 genuine users into the Allowlist and 8 intentional insiders into the Denylist. With CIC darknet dataset, P&ID detected 4,783 intentional-Darknet users and 68 unintentional Darknet users among 134,305 daily activities. UIM mitigated 68 unintentional-Darknet users as 64 Intentional-Darknet and 4 benign users. IIM profiled 5063 benign users in Allowlist and 4847 Intentional-Darknet users in Denylist.

Examiners

Internal Examiner : Dr. R. Sridaran Rajagopal,
Executive Dean (Faculty of Computer Applications) &
Executive Dean (Academic Quality Assurance),
Ganpat University, Gujarat.

External Examiner : Dr. B. Balamurugan Eswaran,
Professor & DVC Academics,
Texila American University,
Zambia.