IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, January 2026
Impact Factor: 7.67

Artificial Intelligence (AI)- Based Threat Detection Models for Privileged App Abuse in Modern Systems

Maunik K. Shah
Independent Researcher
IEEE Senior Member
maunik.shah27989@gmail.com

Abstract: *The insider threat is becoming one of the most talked-about and pressing problems in cybersecurity. This occurrence highlights the need for specialized detection systems, methodologies, and tools to enable fast and accurate identification of malevolent insiders. This paper presents a strong detection system to use the CERT r5.2 dataset, which has been preprocessed with features that improve relevance through statistical aggregation, encoding, z-score normalization, and PCA-based dimensionality reduction. To increase identification of infrequent harmful behaviors, oversampling and class-weighted learning are used to overcome class imbalance. A convolutional neural network (CNN) trained in one dimension is used for automatic feature extraction. Experimental findings demonstrate near-perfect performance under all conditions, with an AUC value up to 1.000 and F1-score, recall, accuracy, and precision all above 99.9%. Results from comparisons with both conventional ML and other DL methods show that the suggested model is superior. This research provides a scalable solution to the problem of proactive insider threat detection and establishes that the framework is effective, resilient, and applicable in real-world security systems. A dependable solution for proactive insider threat identification, the framework is scalable, interpretable, and applicable to real-world security systems*

Keywords: Cybersecurity, Privileged App Abuse, insider Threat Detection, Android Security, Malware Detection, Permission Analysis, API Call Monitoring, Machine Learning

DOI: 10.48175/IJARSCT-31019