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 5, March 2026
Impact Factor: 8.2

Mitigating Insider Threat : A Neural Network Approach for Enhanced Security

Ms Bejjanki Pooja[1], B. Aditya[2], Ch. Sirisha[3]
Gandamalla Samatha[4], Kandhi Gayathri[5], Yellaboina Harshith Kumar[6]
Assistant Professor, Department of CSE[1,2,3]
UG Student, Department of CSE[4,5,6]
CMR Technical Campus, Hyderabad, Telangana, India
poojareddybejjanki@gmail.com, Adi.sacs@gmail.com
237r1a05e6@cmrtc.ac.in, 237r1a05f2@cmrtc.ac.in, 237r1a05k1@cmrtc.ac.in

Abstract: *Insider threats represent a significant cybersecurity challenge within IoT-enabled institutional environments due to the exploitation of legitimate access for malicious activities. Traditional insider threat detection (ITD) approaches often struggle with issues such as data imbalance, high dimensionality, and evolving user behaviors. This research presents a detection model leveraging a neural network to address these challenges effectively. The proposed model captures complex patterns in insider threat data and improves the accuracy of detection.*

Additionally, Principal Component Analysis (PCA) is employed for feature extraction, while K-means clustering is used to group user activity patterns. To handle data imbalance, data augmentation techniques are applied. Furthermore, optimization techniques are used to fine-tune the model parameters, ensuring better performance. Experimental evaluation on the CMU CERT insider threat dataset demonstrates the effectiveness of the proposed model, achieving high detection accuracy and a low false alarm rate. Compared to existing methods, the approach enhances detection performance, model robustness, and computational efficiency, making it a reliable solution for securing IoT infrastructures against insider threats.

Keywords: *Traditional insider threat detection*

DOI: 10.48175/IJARSCT-31933