18.ENHANCED MACHINE LEARNING TECHNIQUES FOR DETECTING BEHAVIOR-BASED INTRANET ATTACKS

Mooli Pavithra
Department of MCA
Rajeev Gandhi Memorial College
of Engineering and Technology
Nandyal

Mr.K.R. Harinath M.tech (Ph.D.)
Department of MCA
Rajeev Gandhi Memorial College
of Engineering and Technology
Nandyal

Intranet security is a critical concern in modern organizations as cyber threats continue to evolve. Traditional security measures often fail to detect sophisticated insider attacks and behavioral anomalies. This study presents an advanced approach to detecting intranet attacks using machine learning techniques. By leveraging behavioral analysis, extraction, and anomaly detection algorithms, the proposed model identifies malicious activities in real time. Various classification algorithms, including Decision Trees, Random Forest, and Deep Learning models, are evaluated for their effectiveness distinguishing normal and suspicious behaviors. The proposed system enhances cybersecurity by improving detection accuracy and reducing false positives. Experimental demonstrate that the model outperforms conventional security mechanisms, making it a promising solution for securing intranet environments against internal and external threats.

 ISBN: - 978-81-985365-8-7