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 1, March 2026

Impact Factor: 8.2

AI-Based Cyber Threat Detection System: An Integrated Approach Using Machine Learning for Network, Email, and Malware Security

Dr. Anup Bhange[1], Anisha Awaze[2], Hema Kuhikar[3]

Head, Department of Master of Computer Application[1]
PG Scholar, Department of Master of Computer Application[2,3]
KDK College of Engineering, Nagpur, India
anup.bhange@kdkce.edu.in, awazeasuresh.mca24f@kdkce.edu.in,
kuhikarhnarendra.mca24f@kdkce.edu.in

Abstract: *The rapid proliferation of cyber threats such as network intrusions, phishing emails, and malware attacks has necessitated the development of intelligent, automated security systems. Traditional signature-based solutions are ineffective against zero-day attacks and evolving threat patterns. This paper presents the design and implementation of a comprehensive AI-based Cyber Threat Detection System that integrates Machine Learning (ML) and Deep Learning techniques to detect network anomalies, phishing emails, and malicious files in real time. The proposed system comprises three core modules: Network Threat Detection using Isolation Forest, Email Security Monitoring using NLP-based classification with TF-IDF vectorization, and Malware Detection using supervised ML models like Random Forest. A unified real-time dashboard provides live monitoring, anomaly alerts, and detailed analytics. Experimental evaluation demonstrates high detection accuracy with reduced false positives while maintaining lightweight performance, making the system suitable for deployment in organizational environments.*

Keywords*:* Cybersecurity, Anomaly Detection, Isolation Forest, Phishing Detection, Malware Analysis, Machine Learning, Real-time Monitoring, TF-IDF, Random Forest, AI Security System

DOI: 10.48175/IJARSCT-31469