Real-Time Threat Intelligence and Automated Prevention Using Micro Intelligent System Technology and Explainable Tree-Based Models

Authors Uddipan Ghosh, Ankan Sarkar, Siddhartha Roy, Apurba Nandi, Avik Kumar Das, Pratik Saha

Publication date 2026/3/18

Conference 9th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)

Description Cyber-attacks are getting faster, smarter, and undetectable by traditional security measures. DDoS, password cracking, port scanning malware, and phishing attacks get evolved and tend to bypass conventional and outdated security configurations. To address this challenge, our project contributes to an adaptive cyber threat detection system with a hybrid machine learning strategy that integrates three robust models Random Forest, XGBoost, and LightGBM. Each of these models has something valuable: Random Forest is good on big noisy data, XGBoost improves by learning from its mistakes, and LightGBM provides fast responses but accurate output. Integrating the findings of the three models led to developing a system that was more accurate and better in threat detection and less prone to false alarms. We tested the system using actual cyber attack datasets, and the result showed that our hybrid model ...