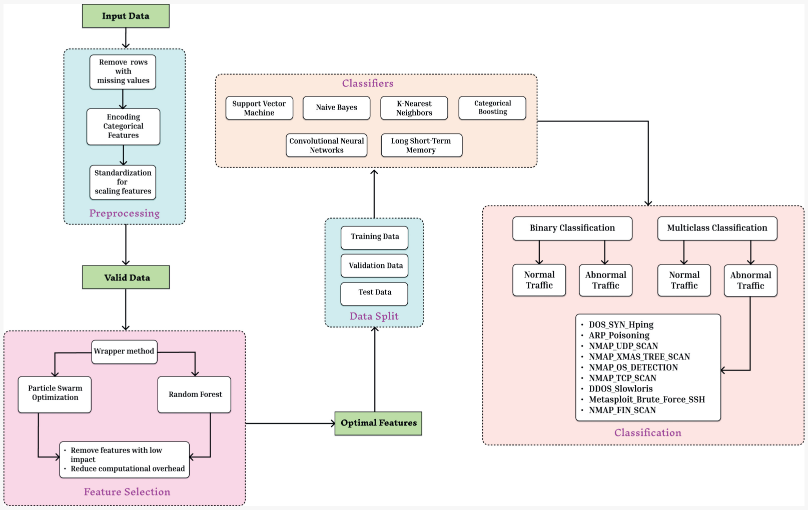
AI-powered intrusion detection system outperforms traditional methods in securing IoT networks



Flowchart of the Proposed Framework.

GA, UNITED STATES, April 16, 2025 /EINPresswire.com/ -- A recent study introduces an advanced anomaly-based intrusion detection system (IDS) designed to address the increasing cyber threats targeting Internet of Things (IoT) devices. By combining machine learning (ML) and deep learning (DL) models with particle swarm optimization (PSO) for feature selection, the system achieves remarkable performance. Tested on the RT_IoT2022 dataset, the system's top performer, CatBoost, achieved an impressive 99.85% accuracy, making it one of the most accurate IDS solutions for IoT environments. This innovation offers a powerful tool to detect and classify complex attacks in real-time, enhancing cybersecurity for resource-constrained IoT networks.

As Internet of Things (IoT) devices proliferate in sectors like smart cities, healthcare, and industrial systems, they have become prime targets for cyberattacks such as Distributed Denial of Service (DDoS), ransomware, and botnets. However, traditional security methods struggle to cope with these attacks due to the limited computational power of IoT devices and the dynamic nature of cyber threats. Anomaly-based intrusion detection systems, which identify deviations from normal behavior, have emerged as a promising solution. However, these systems often face challenges such as high computational costs and an increased rate of false positives. This calls for the development of more efficient, scalable, and accurate IDS tailored specifically for the unique constraints and challenges of IoT environments.

Published (DOI: 10.1016/j.dsm.2025.02.005) on February 24, 2025, in Data Science and Management, a team of researchers from Al Yamamah University and Ecole nationale Supérieure d'Informatique introduced a novel intrusion detection system (IDS) that integrates PSO-optimized machine learning and deep learning models. The system, tested on the

RT_IoT2022 dataset, demonstrated exceptional accuracy in detecting and classifying IoT intrusions. CatBoost emerged as the leading model, achieving 99.85% accuracy, setting a new benchmark in IoT security. The study underscores the potential of bio-inspired algorithms like particle swarm optimization (PSO) to enhance the efficiency and effectiveness of cybersecurity solutions in resource-constrained IoT networks.

The study's innovation lies in its hybrid approach, where PSO optimizes feature selection, reducing computational overhead while maintaining high accuracy. Six models—SVM, KNN, CatBoost, Naïve Bayes, CNN, and LSTM—were evaluated, with CatBoost excelling in both binary classification (99.85% accuracy) and multiclass classification (99.82%), outperforming other methods such as QAE-f16 by 2.6%. The RT_IoT2022 dataset, which includes real-world attack scenarios like ARP poisoning and DDoS, served as a robust testing ground. Notably, PSO helped reduce SVM training time by 23x with minimal loss in accuracy, addressing the resource limitations of IoT devices. However, challenges remain, such as misclassifying rare attacks like NMAP FIN scans due to dataset imbalance, highlighting areas for future refinement.

Dr. Mourad Benmalek, the study's corresponding author, highlighted the significance of their findings, stating, "Our PSO-enhanced framework not only achieves unprecedented accuracy but also optimizes resource usage, making it practical for real-world IoT deployments. CatBoost's outstanding performance showcases the potential of gradient boosting in cybersecurity, while PSO's efficiency opens doors for lightweight IDS solutions that are ideal for IoT environments with limited resources."

The implications of this IDS framework are vast, extending across industries reliant on IoT, including healthcare, smart grids, and industrial automation. By minimizing false positives and computational costs, the system enables scalable, real-time threat detection, which is crucial for industries that rely on continuous, uninterrupted service. Organizations can enhance regulatory compliance, safeguard sensitive data, and build customer trust through robust cybersecurity measures. Future research may focus on exploring hybrid models and improving real-time adaptability, further enhancing IoT defenses against evolving threats. This study sets a new benchmark for ML/DL applications in cybersecurity, providing a vital step toward stronger IoT protection in the face of increasingly sophisticated cyberattacks.

References
DOI
doi.org/10.1016/j.dsm.2025.02.005

Original Source URL
https://doi.org/10.1016/j.dsm.2025.02.005

Lucy Wang
BioDesign Research
email us here