

---

## ABSTRACT

---

Network security is crucial for preserving privacy and safeguarding private information. Recent laws relevant to current web services have increased the need for intrusion detection systems, which protect data and mitigate the impact of attacks. Effective feature selection is crucial for lowering dimensionality and enhancing detection accuracy to enhance the execution of IDS. The current study's objective is to offer a novel approach to feature selection by integrating Particle Swarm Optimization (PSO) and Cuckoo Search (CS) algorithms. This study evaluates the efficiency of various optimization strategies for feature selection in the CICIoT2023 dataset, which contains a wide variety of IoT attack scenarios, aimed at enhancing intrusion detection systems. To identify and prioritize the most significant features, the current methodology uses a hybrid feature selection framework that combines the advantages of both local search efficiencies from PSO and global search capabilities from CS. Following that, the chosen features are then fed into three classifiers: Multi-Layer Perceptron (MLP), Random Forest (RF), and AdaBoost. The experimental outcomes demonstrate that the CS-PSO hybrid model significantly improves attack detection accuracy, outperforming previously reported methods on the same dataset. This research contributes to advancing network security in IoT environments by addressing the growing demand for adaptive and effective IDS solutions, instilling greater confidence in the resilience of IoT networks.

---