**ParticleDeep: IoT Cybersecurity Optimization Framework**

**Overview**

Developed a novel network forensic framework, **ParticleDeep**, leveraging Particle Swarm Optimization (PSO) to enhance Multi-Layer Perceptron (MLP) models for IoT cybersecurity threat detection. This project optimized MLP hyperparameters to improve classification accuracy and generalization on IoT network datasets, addressing challenges like class imbalance and complex attack patterns.

**Key Features**

* **Advanced Optimization**: Utilized PSO to fine-tune MLP hyperparameters (hidden layer size, learning rate, regularization strength) in a 3D search space, achieving a best AUC of 0.9938 on the original dataset.
* **Comprehensive Data Preprocessing**: Implemented robust data cleaning, feature extraction, and conversion (e.g., string-to-numeric, IP address to 32-bit integers) across large-scale IoT datasets (over 73M records).
* **Balanced Dataset Handling**: Applied SMOTE (oversampling) and Tomek Links (undersampling) to address class imbalance, improving rare-class detection (e.g., Data Exfiltration, Keylogging).
* **Feature Selection with Random Forest**: Identified critical features (e.g., duration, protocol, state) contributing to model performance, reducing overfitting and computation time.
* **Performance Evaluation**: Achieved high precision, recall, and F1-scores (weighted avg: 0.89) across multiple sampling strategies, with visualizations for AUC, accuracy, and F1-score trade-offs.
* **Scalable Implementation**: Used Python libraries (NumPy, Pandas, Scikit-learn, Matplotlib) for efficient data processing, modeling, and visualization.

**Impact**

* **Enhanced Cybersecurity**: Improved MLP model accuracy and robustness for detecting IoT network threats like DDoS, DoS, and Reconnaissance, critical for real-world cybersecurity applications.
* **Rare-Class Detection**: Oversampling strategy boosted performance on rare but high-impact attack types, ensuring balanced detection in imbalanced datasets.
* **Future Potential**: Laid groundwork for advanced PSO implementations to optimize deeper network architectures, scalable to more complex IoT environments.

**Technologies Used**

* **Python**: NumPy, Pandas, Scikit-learn, Matplotlib
* **Machine Learning**: Multi-Layer Perceptron (MLP), Random Forest, PSO
* **Data Handling**: SMOTE, Tomek Links, StandardScaler, SimpleImputer

**Results**

* **Best AUC**: 0.9938 (original dataset), 0.9918 (oversampled), 0.9909 (undersampled)
* **Weighted F1-Score**: 0.89 (original), with oversampling improving rare-class F1-scores (e.g., 0.98 for labels 7, 8)
* **Key Hyperparameters**: Hidden layer neurons (109–200), learning rate (~0.004–0.006), regularization alpha (0.0001)

*ParticleDeep demonstrates the power of combining PSO with deep learning to secure IoT networks, offering a scalable and robust solution for modern cybersecurity challenges.*

**AIoT-Sentry: Survey on AI-Driven Anomaly Detection for IoT Security**

**Overview**

Conducted a comprehensive survey, **AIoT-Sentry**, analyzing AI-based anomaly detection techniques for enhancing IoT security across general and specialized domains (e.g., Industrial IoT, Medical IoT, Drone IoT, Smart Grids). The study synthesizes recent contributions, evaluates AI techniques, datasets, and their applicability, and identifies gaps to guide future research in IoT cybersecurity.

**Key Features**

* **Systematic Literature Review**: Analyzed 24 journal papers (2023–2024) from digital libraries (Google Scholar, IEEE Xplore, Elsevier, etc.) using targeted search terms like "Anomaly detection IoT" and "AI-based anomaly detection."
* **AI Techniques Explored**: Covered supervised (e.g., ANN, SVM, XGBoost) and unsupervised (e.g., Autoencoders, GANs) methods, with a focus on deep learning (CNN, LSTM) and ensemble approaches for intrusion detection.
* **Domain-Specific Insights**: Established relationships between IoT applications (e.g., Medical IoT, Industrial IoT) and optimal AI techniques/datasets, e.g., CNN+LSTM for Industrial IoT, XGBoost for Medical IoT.
* **Dataset Analysis**: Evaluated key datasets (Bot-IoT, IoT-23, Edge-IIoTset, AWID, UNSW-NB15) for training anomaly detection models, addressing challenges like class imbalance and preprocessing complexity.
* **Research Questions Addressed**: Identified dominant AI techniques, prevalent datasets, attack types (e.g., DDoS, keylogging), and IoT subfields benefiting most from AI-driven security solutions.
* **Critical Gaps Identified**: Highlighted the need for larger, diverse datasets, computationally efficient models, and explainable AI (XAI) for real-time anomaly detection.

**Impact**

* **Enhanced IoT Security Framework**: Provided a roadmap for selecting AI techniques and datasets tailored to specific IoT applications, improving threat detection accuracy and robustness.
* **Research Guidance**: Offered actionable insights for researchers by linking AI methods to IoT subfields, addressing limitations like dataset scalability and model generalizability.
* **Practical Applications**: Supported advancements in secure IoT environments, including smart grids, healthcare, and industrial systems, by identifying effective anomaly detection strategies.

**Technologies and Methods**

* **AI Techniques**: ANN, CNN, LSTM, B-LSTM, GRU, SVM, KNN, XGBoost, Autoencoders, GANs, Ensemble Methods
* **Datasets**: Bot-IoT, IoT-23, Edge-IIoTset, AWID, UNSW-NB15, NSL-KDD, WUSTL-EHMS-2020, CICIDS2017
* **Tools**: Systematic review methodology, digital libraries (Google Scholar, IEEE Xplore, Elsevier, ScienceDirect, Hindawi)

**Key Findings**

* **Dominant Techniques**: Deep learning (CNN, LSTM) and ensemble methods outperform traditional ML for complex IoT environments; hybrid models (e.g., CNN+LSTM) excel in Industrial IoT.
* **Dataset Suitability**: Bot-IoT and ToN-IoT are versatile for general IoT; WUSTL-EHMS-2020 is ideal for Medical IoT; CICIDS2017 suits Drone IoT.
* **Attack Detection**: Effective against DDoS, DoS, keylogging, data exfiltration, and novel attacks, with ensemble methods achieving up to 95% accuracy.
* **Future Directions**: Emphasized the need for XAI, federated learning, and real-time detection to address scalability and computational challenges.

*AIoT-Sentry underscores the transformative role of AI in securing IoT ecosystems, offering a clear guide for researchers and practitioners to enhance anomaly detection across diverse IoT applications.*