**Reviewed Papers**

1. [**User Behavior Pattern - Signature Based Intrusion Detection**](https://sci-hub.se/https:/doi.org/10.1109/WorldS450073.2020.9210368)

The paper proposes a Pattern-Based Intrusion Detection Engine (PIDE) that detects unauthorized users by analyzing user behavior patterns using expert-defined rules. It compares the proposed model with an older model called Statistical-Based Intrusion Detection (SBID).

**Proposed Model: Pattern-Based Intrusion Detection Engine (PIDE)**

* **PIDE** uses **expert-defined rules** to compare real-time user behavior against predefined patterns.
* Rules are written as **if-then statements** using **JESS (Java Expert System Shell)**.
* It monitors various user activities, including:
  + **Keyboard usage** (typing speed and patterns)
  + **Mouse movements**
  + **File access times**
* If behavior deviates from the normal pattern, **PIDE** raises an alert and can block the user or terminate the session.

**Experiment and Results**

* Dataset: User profiles containing keyboard, mouse, application usage, and processor activity.
* Tool: **JESS** was used to implement and test rules.
* **PIDE** showed:
  + **75% overall accuracy**
  + **100% accuracy** in detecting unauthorized users.
  + Some false positives: 4 authorized users were falsely flagged as intruders.
* Comparison with **SBID**:
  + **PIDE** performed better in detecting unauthorized users.
  + **SBID** used **logistic regression** and **statistical mean** but had limitations with authorized users showing unusual behavior.

**Future Enhancements (as Suggested by Authors)**

* **Hybrid Approach:** Combine **PIDE** with **Anomaly Detection** to detect unknown attacks.
* **Machine Learning Integration:** Implement machine learning models to learn new patterns and reduce false positives.
* **Adaptive Rules:** Use automated rule generation to adapt to changing user behavior.

1. [**Introduced a New Method for Enhancement of Intrusion Detection with Random Forest and PSO Algorithm**](https://sci-hub.se/https:/doi.org/10.1002/spy2.147)

This paper proposes a new model for Intrusion Detection Systems (IDS) using a combination of Random Forest (RF) and Particle Swarm Optimization (PSO) algorithms. The goal is to improve detection accuracy and speed in identifying network intrusions.

**Datasets Used:**

* **UNSW-NB15 Dataset** – Contains modern attack types and normal network traffic features.
* **KDD-Cup’99 Dataset** – A benchmark dataset used for evaluating IDS models.
* **Intrusion Detection Systems (IDS)** are designed to detect unauthorized access or malicious activities in computer networks.
* There are two main approaches:
  + **Pattern-Based Detection:** Looks for known attack patterns.
  + **Anomaly Detection:** Flags unusual behavior that deviates from normal user activity.

**Proposed Method: Random Forest + PSO**

* **Random Forest (RF):**
  + An ensemble learning method that builds multiple decision trees for classification.
  + It uses **bootstrap sampling** and **random feature selection** to improve accuracy and prevent overfitting.
* **Particle Swarm Optimization (PSO):**
  + An optimization algorithm inspired by the social behavior of birds and fish.
  + It finds the optimal solution by moving particles (candidate solutions) through the search space, updating their positions based on individual and group experiences.

**How the Model Works**

1. **Feature Selection:**
   * Selects the most important features from the dataset using **PSO**.
   * Reduces the number of features to minimize computation time and improve accuracy.
2. **Random Forest Classification:**
   * Builds multiple decision trees using the selected features.
   * The final classification is based on the **majority vote** of the trees.
3. **Optimization with PSO:**
   * PSO optimizes the **entropy function**, reducing uncertainty and increasing classification accuracy.
   * It automatically groups non-numerical attribute values to reduce complexity without losing accuracy.
4. **Evaluation:**
   * The model is evaluated using **Confusion Matrix**, **Precision**, **Accuracy**, and **AUC (Area Under Curve)** metrics.
   * Results are compared with other models, including **Decision Tree (DT)**, **PSO-XGBoost**, and **PSO-Decision Tree (PSO-DT)**.

**3. Experimental Results**

* **Datasets Used:**
  + **UNSW-NB15**: Contains 49 features and 2,540,044 observations, representing modern attack types and normal network traffic.
  + **KDD-Cup’99**: A widely used dataset for IDS evaluation.
* **Performance Metrics:**
  + **Accuracy:** 97% with the proposed method, compared to 75.94% with conventional models.
  + **AUC:** 0.881, outperforming other models like **PSO-XGBoost (0.785)** and **PSO-DT (0.699)**.

**Comparison with Other Models**

* Outperformed **Decision Tree (DT)**, **PSO-XGBoost**, and **PSO-DT** models in terms of accuracy and speed.
* The **PSO-RF** model demonstrated better generalization and reduced overfitting compared to other ensemble methods.

**Future Enhancements (as Suggested by Authors)**

* **Hybrid Models:** Combine **PSO-RF** with other machine learning models like **Deep Learning** for better detection of unknown attacks.
* **Adaptive Feature Selection:** Implement dynamic feature selection to adapt to evolving attack patterns.
* **Cross-Dataset Validation:** Test the model on more diverse datasets to evaluate its generalization capability.
* **Real-Time Intrusion Detection:** Optimize the model for real-time detection in live network environments.