|  |  |
| --- | --- |
| **Paper** | **Key SOTA Methods** |
| Evaluating the Effectiveness of AI-Based Phishing Detection in IoT Communication Protocols | - Supervised ML: Decision Trees, SVMs, lightweight neural nets tailored to IoT metadata  - NLP: TF-IDF and word-embedding features on MQTT/CoAP/HTTP payloads  - Behavioral Profiling: Anomaly detection on device command sequences  - Edge-Optimized Pipelines: Sub-millisecond inference engines per protocol  - Hybrid/Ensembles + continuous model updates |
| ML Techniques for Phishing Detection (MJAP’24) | - Extreme Gradient Boosting (XGBoost)  - Random Forest  - SVM  - Naïve Bayes  - Emphasis on comprehensive preprocessing (cleaning, feature extraction, normalization) |
| MLP Neural Network for Malicious Phishing URLs | - **Shallow MLP** trained on raw tokenized URLs - **Backprop feature-selection**: Learns discriminative URL tokens end-to-end - **Edge Deployable** - **Empirical Gains** |
| Phishing Attacks Detection: A Machine Learning-Based Approach | - **ANN vs. SVM vs. LR**  - **ANN (2×100-relu** - **SVM-RBF** - **Logistic Regression (tuned)** - Strong focus on **feature engineering** from email headers/body |
| Phishing Detection Using Machine Learning Techniques | - **Comparative study** of LR, DT, RF, AdaBoost, SVM, KNN, Gradient Boosting, XGBoost, and ANN - **Random Forest** & **XGBoost** |
| PhishIntel: Practical Deployment of Reference-Based Phishing Detection | - **Fast-Slow Task Architecture**: local blacklist & cache for sub-second responses, slow RBPD + crawler for zero-day - **Reference-Based PD** - **Scalable Deployment** on edge GPU instances |

Summary of SOTA Methods