Authentic Learning of Machine Learning in Cybersecurity with Portable Hands-on Labware

Hossain Shahriar (PI), Kennesaw State University, NSF Award#2100115
Fan Wu (PI), Tuskegee University, NSF Award#2100134

Challenge:

- As cybersecurity threats grow in complexity, early detection of security vulnerabilities and threats is needed.
- Machine learning (ML) approaches enable the analysis of large amounts of data and could be used to predict and prevent future cybersecurity threats.

Solution:

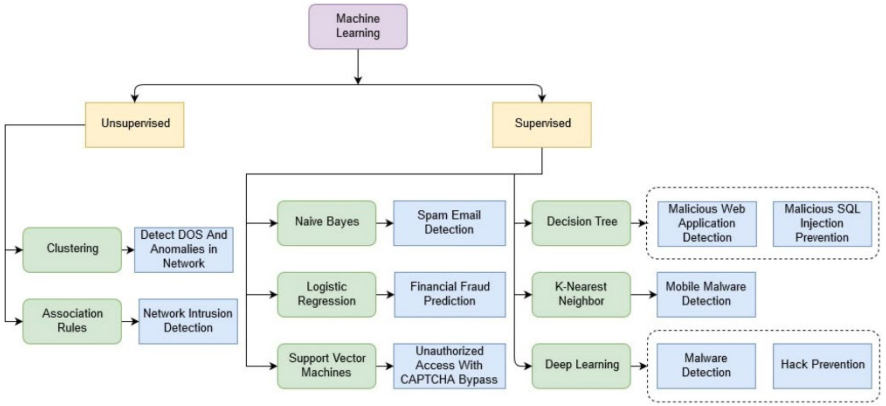
- The project design and develop ten portable labware modules that will support a broad audience to learn ML in cybersecurity effectively and result in more efficient student engagement.
- Machine learning based Hands-on lab practice on real-world topics, consists of a pre-lab, hands-on lab, and a student add-on post-lab.

Scientific Impact:

- Authentic learning approach has been increasingly popular for teaching cybersecurity but is less commonly used to teach ML in cybersecurity.
- The hands-on lab modules will support a wide audience to effectively learn the subjects and result in more efficient student learning and engagement.

Broader Impact & Participation:

- This project enhances the cybersecurity curricula by adopting authentic learning approaches that engage students' active learning and problem-solving capabilities.



List of Modules:

- M0. Getting Started with CoLab on ML for CyberSecurity
- M1. Naive Bayes for spam email filtering
- M2. Logistic Regression for financial fraud prediction
- M3. Neural network algorithms for network DOS detection
- M4. Convolutional Neural Network (CNN) for CAPTCHA Bypass
- M5. Decision Tree for Website Phishing
- M6. Deep learning for malware classification and protection
- M7. Support Vector Machine (SVM) for anomaly-based intrusion detection
- M8. K-Means clustering for ransomware detection
- M9. Decision Tree for malicious web application detection (malicious pages, URLs, HTTP requests)
- M10. K-Nearest Neighbors (KNN) classification for user behavior anomaly