Machine learning applications in cybersecurity: From development to deployment

Dr. Holly Yuan

University of Wisconsin-Stout

Menomonie, WI

yuanh@uwstout.edu

Introduction

- Program Director, Computer Networking & Cybersecurity
- Professor
- Cybersecurity Research Center Director
- Certifications: CCIE Enterprise, CCNP, CISM, AWS, VMware, CEH, Linux
- Teaching Focus: Cybersecurity, Networking, Capstone courses
- Research Interests: Cloud Security, Zero Trust, Workforce Development in Cybersecurity

2025 CAE Community Symposium

2025 CAE Community Symposium

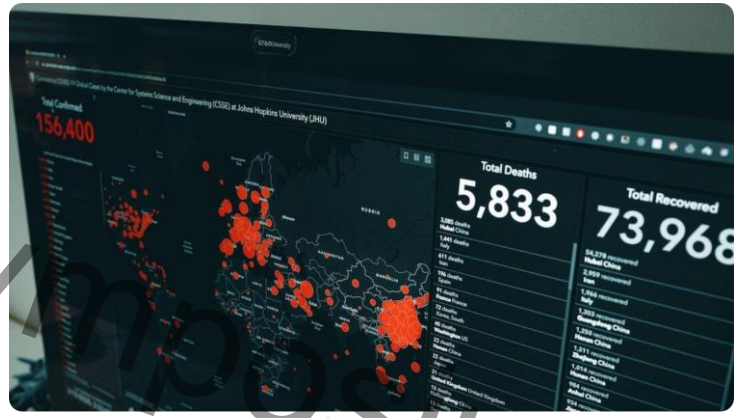
How familiar are you with AI Applications in Cybersecurity?

Please share your response! ☺

A. Very Familiar

B. Somewhat Familiar

C. Not Familiar At All

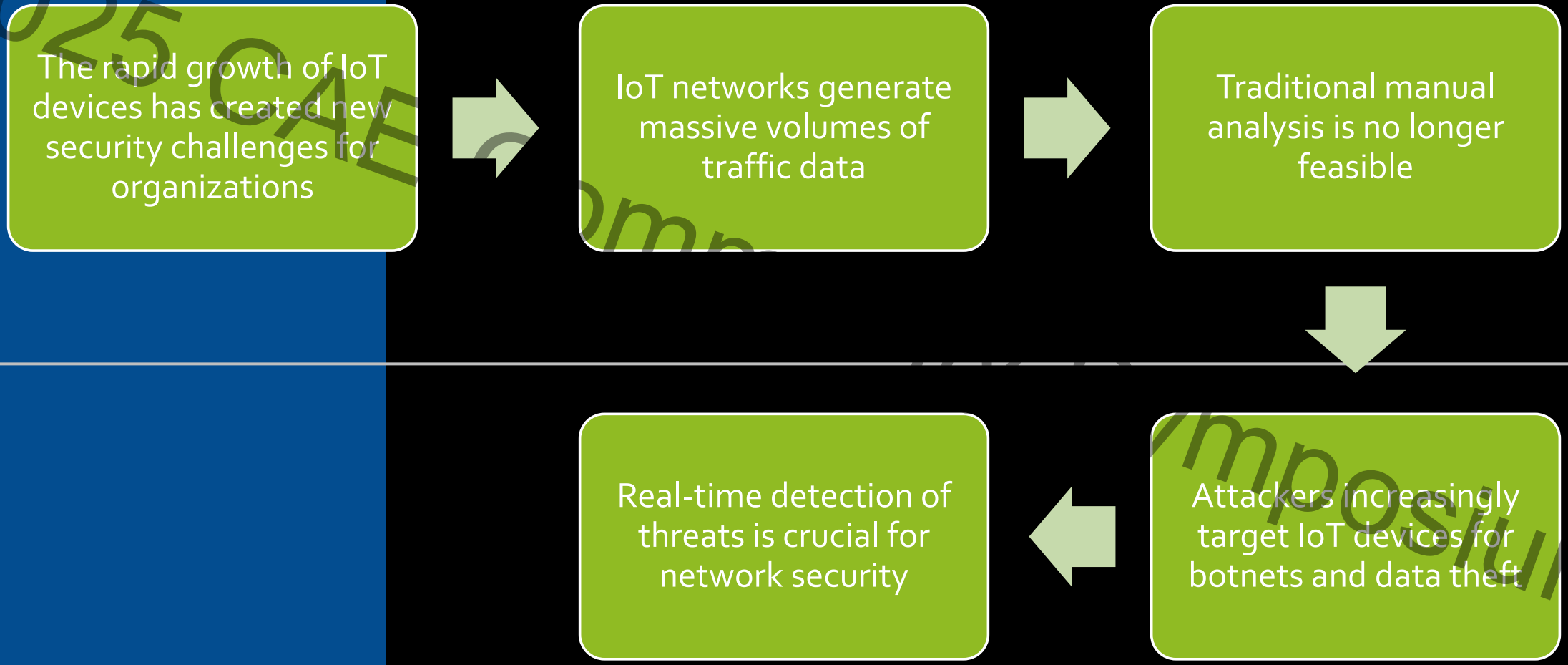


2025 CAE Community Symposium

Complex Threat Landscape

- **Data Volume:** Massive data sets challenge real-time analysis.
- **Attack Speed:** Rapid execution leaves minimal reaction time.
- **Complex Patterns:** Evolving threats bypass traditional detection methods.

AI in Action: Business Context



2025 CAE Symposium

2025 CAE Community Symposium

Our Goal: Use a dataset (RT-IoT 2022) to train a machine learning model to automatically detect malicious network traffic in real-time IoT environments.

Dataset Description

2025 CAE Community Symposium

- **The RT-IoT2022 Dataset is a collection of real-world network traffic data from IoT environments.:**
  - Size: 123,117 network traffic samples
  - Features: 85 network traffic characteristics
  - Types: Mix of normal and attack traffic patterns
  - Source: Real-world IoT infrastructure data
  - Attack types: DDoS, ARP poisoning, and malware
- **Key Features Include:**
  - Protocol types
  - Service types
  - Flow duration
  - Packet statistics
  - Network behavior patterns

2025 CAE Community Symposium

Prepare Data for Training
separate features (X) from Target (y), splits data: 80% for training, 20% for testing

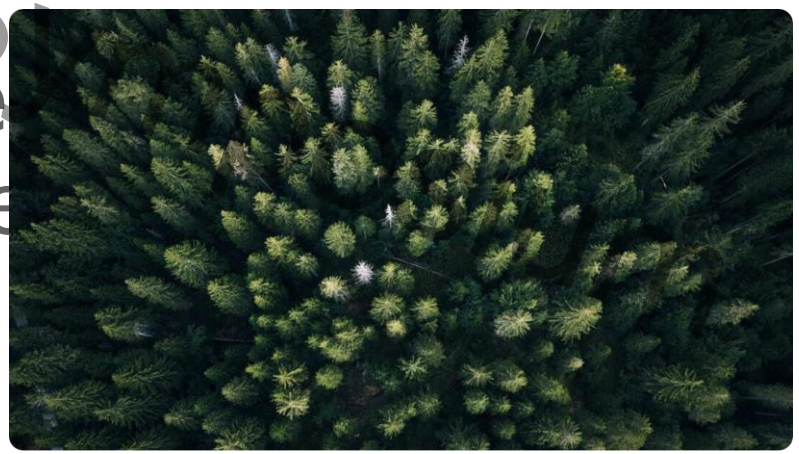
Train the Model
Implemented supervised ML.

Evaluate the Model
Makes predictions on test data, show accuracy of overall correct predictions

2025 CAE Community S

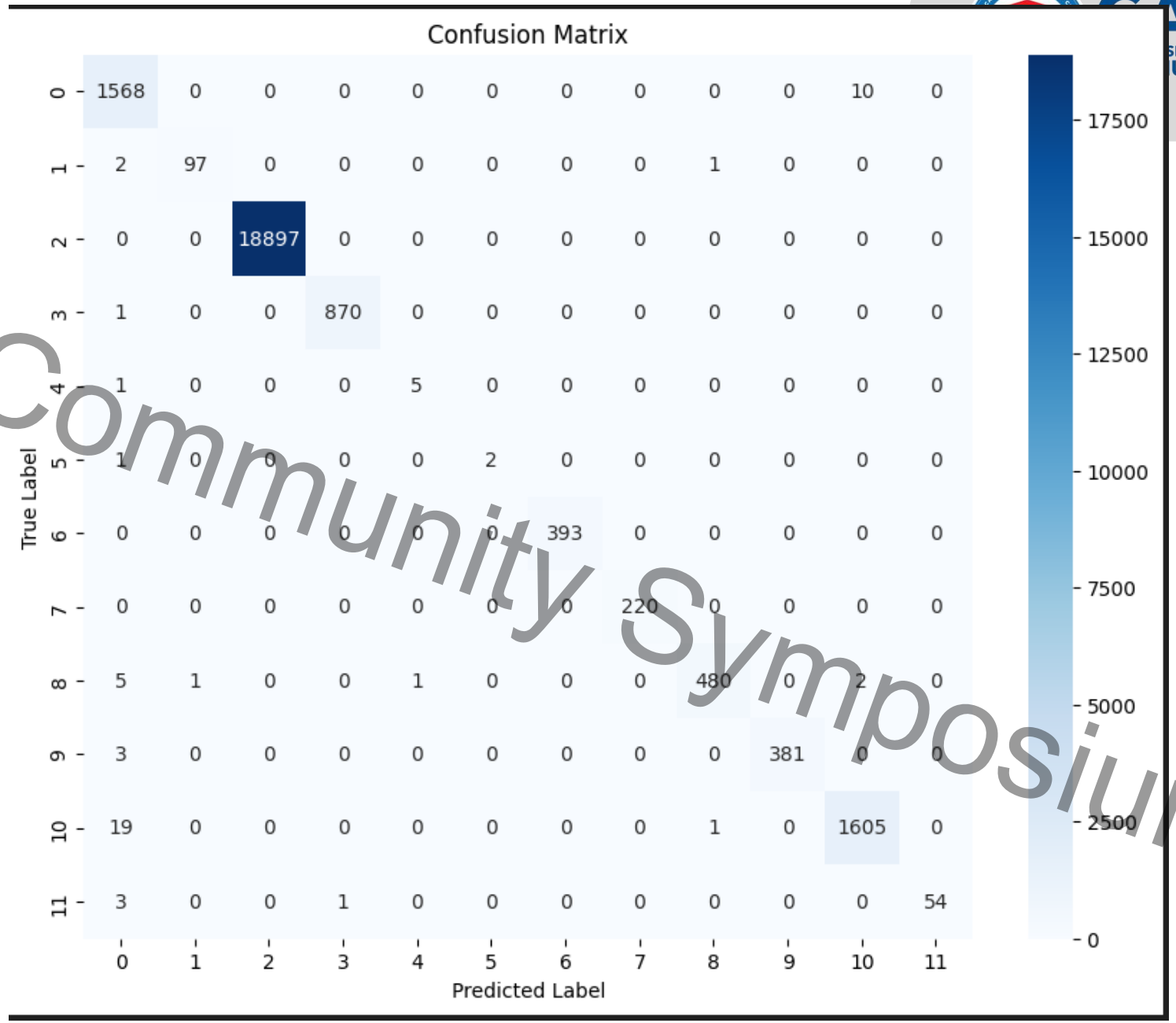
Random Forest Classifier

- Works by creating multiple decision trees (forest).
- Each tree makes a prediction (votes)
- The final prediction is the majority vote from all tree



Evaluating Effectiveness

99.7% Accuracy
in identifying anomalies.



2025 CAE Community Symposium