TwinGuard: An Adaptive Digital Twin for Real-Time HTTP(S) Intrusion Detection and Threat Intelligence

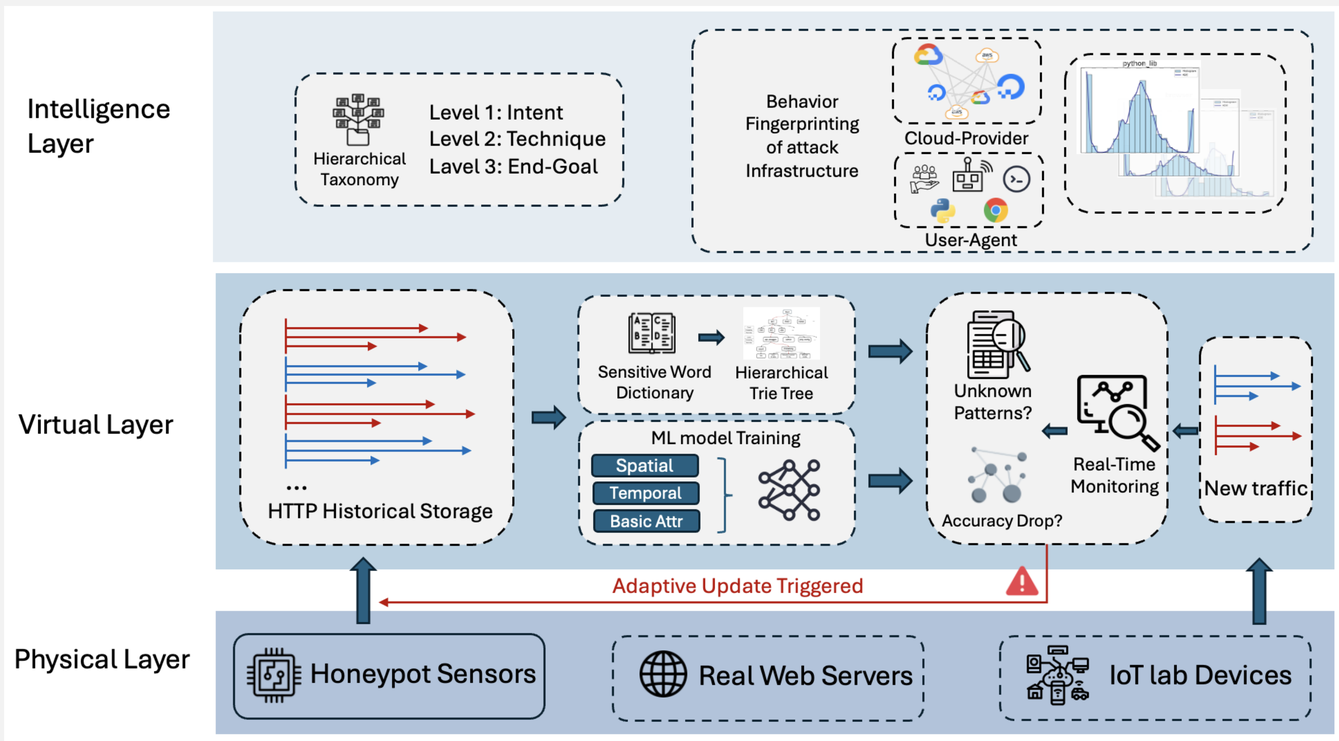
Yuanyuan Zhou, Dr. Anna Maria Mandalari

Department of Electronic and Electrical Engineering

Motivation

- HTTP(S)-based attacks on IoT/Web systems are increasing evasive
- Static rules are insufficient for modern, adaptive threats

Three-Layer Design



Key Features:

Modular **Lightweight** **Extensible**

- Hierarchical Labeling
- Attacker Fingerprinting
- Reveals what, where, and how threats evolve

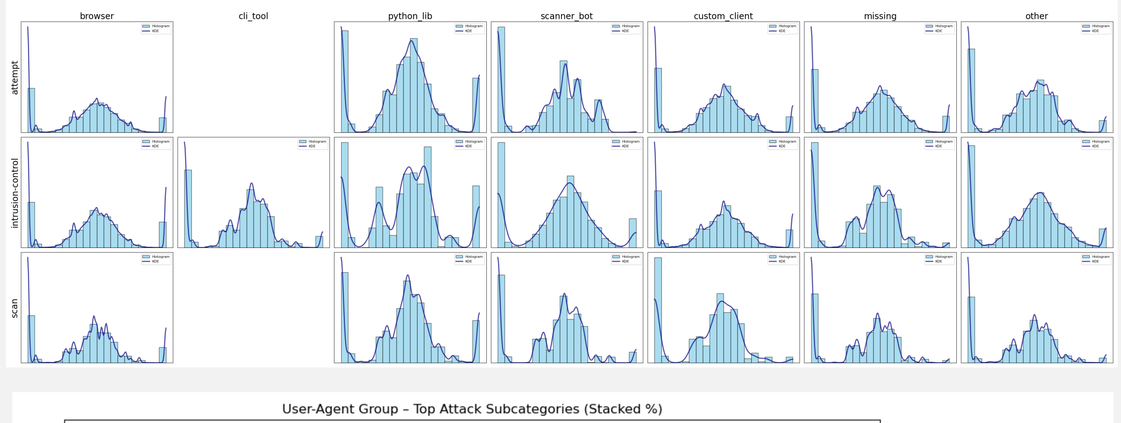
- Trie-Based Path Model matching
- Keyword dictionary for Granularity Reduction
- ML Classifiers for IDS
- Sliding-Window retraining Mechanism

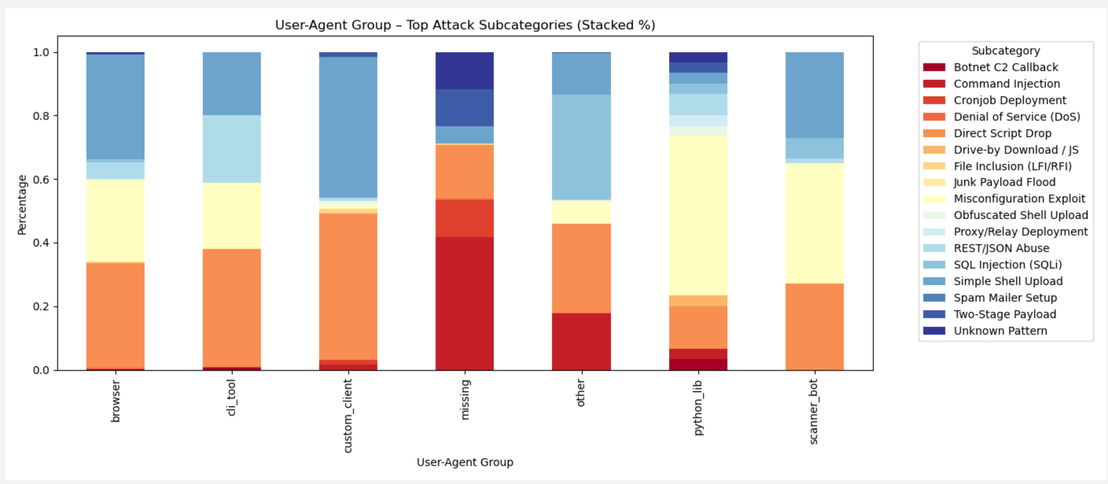
- Capture Real-world HTTP(S) attacks

Behavioral Fingerprinting of Attack Infrastructure

Features: URI Embeddings, Headers, Connection Metadata
Visualization: Signature Profiles, Histograms + KDEs, JS Divergence, Taxonomy Mapping

User-Agent Groups Profiling for example





Results

From Cloud Providers

Distinct Patterns across scanner Bot

Variability reflects tooling, scripting or spoofing

Useful for **behavior-based** Intrusion clues

From Cloud Providers

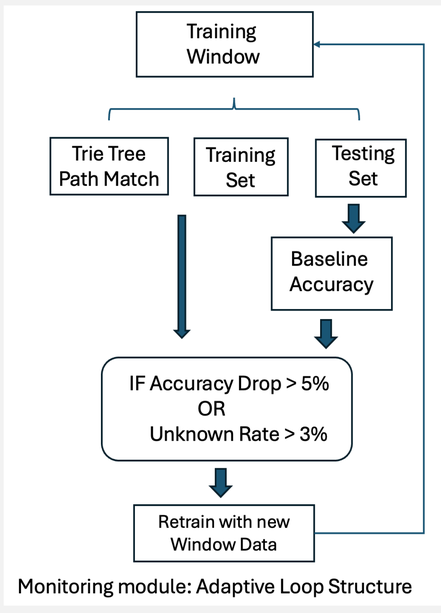
Similar Patterns across orgs → share attack logic

Low Divergence despite slight exploit preferences shifts

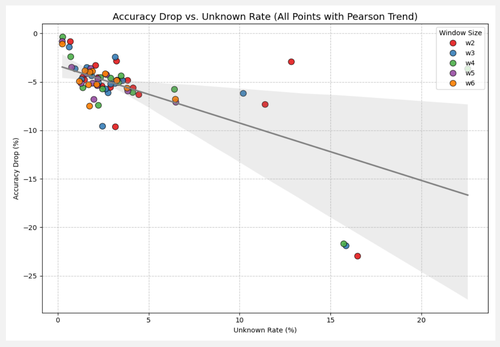
Consistent Profiles

Adaptive Responsiveness In Real-Time Monitoring

Trie Tree → Unknown Patterns
ML models → General IDS



Monitoring module: Adaptive Loop Structure

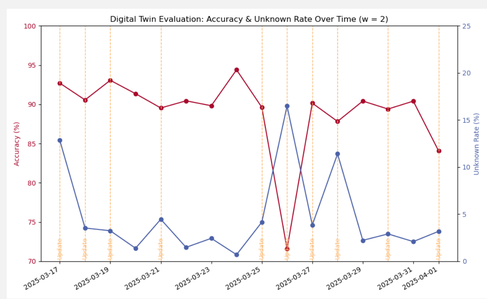


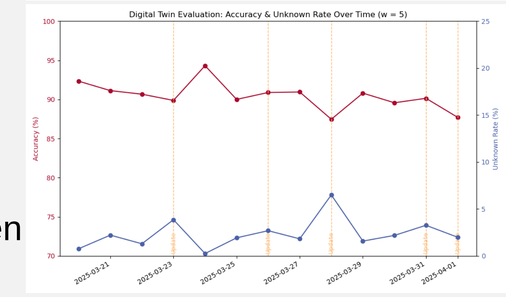
Pearson trend shows **strong negative correlation** between accuracy drop and unknown rate

w = 2
- Fast Reaction
- Frequent Updates
- Higer Volatility

w = 5
- Stable Accuracy
- Fewer Updates
- Lower Unknown Rate

w = 5 offers a good trade-off between adaptability and stability





Conclusion

- **Real-time & Adaptive Protection:**
  90% accuracy with periodic retraining; 25K+ unknown sequences detected, >99% match rate during stable periods.

- **Behavioural Insight:**
  Labelling and fingerprinting reveal attacker origin, tooling, and evolving strategies.

yuanyuan.zhou,23@ucl.ac.uk

a.mandalari@ucl.ac.uk