UC San Diego

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

ILLINOIS TECH

Efficient Host Intrusion Detection using Hyperdimensional Computing

Yujin Nam†, Rachel King*, Quinn Burke*, Minxuan Zhou^
Patrick McDaniel* and Tajana Rosing†

†University of California, San Diego
*University of Wisconsin, Madison
^Illinois Institute of Technology

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON
• MADS&P

Darktrace

Attack trends: Cloud-Based Cyber-Attacks and the Rise of Alternative Initial Access Methods

This blog details how cyber attackers are increasingly using
including Dropbox and Microsoft 365 to stealthily bypass d

Cyber Magazine

Gigamon Sound Alarm on Cloud Security as Unseen Attacks Soar

Gigamon's latest Hybrid Cloud Security Survey shows unseen cyber attacks have increased 20% year on year.

SC Media

Poll finds cloud contributing to cyberattack proliferation

The survey of over 1000 security and IT leaders found that
contributes to increased cyber risk, with 83% of responden

CybersecurityNews

Massive Cyber Attack On AWS Targets 230 Million Unique Cloud Environments

Thales

Cloud Resources have Become Biggest Targets for Cyberattacks, finds Thales

Thales today announced the release of the 2024 Thales Cloud Security Study, its annual assessment on the latest cloud security threats,...

n was detected by Unit 42 researchers that manipulated
ons using cloud systems.

Darktrace

Attack trends: Cloud-Based Cyber-Attacks and the Rise of Alternative Initial Access Methods

This blog details how cyber attackers are increasingly using
including Dropbox and Microsoft 365 to stealthily bypass d

Cyber Magazine

Gigamon Sound Alarm on Cloud Security as Unseen Attacks Soar

cyber attacks have

SC Media

Poll finds clou

The survey of over 1
contributes to increa

illion Unique

Thales

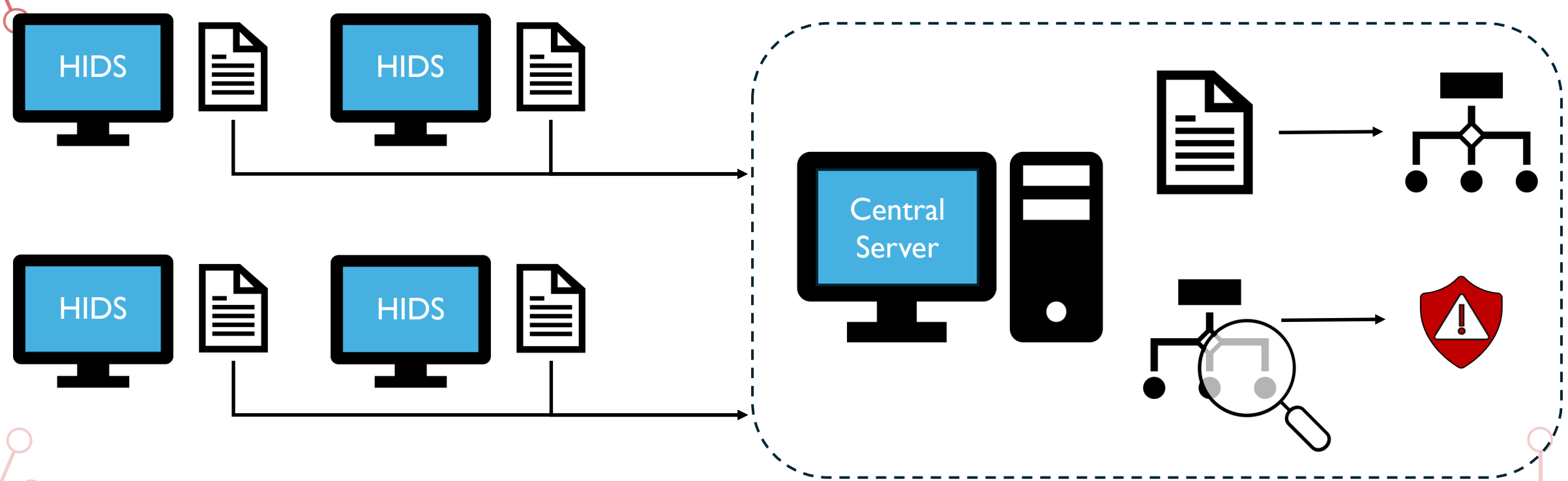
Cloud Resources have Become Biggest Targets for Cyberattacks, finds Thales

Thales today announced the release of the 2024 Thales Cloud Security Study, its annual assessment on the latest cloud security threats,...

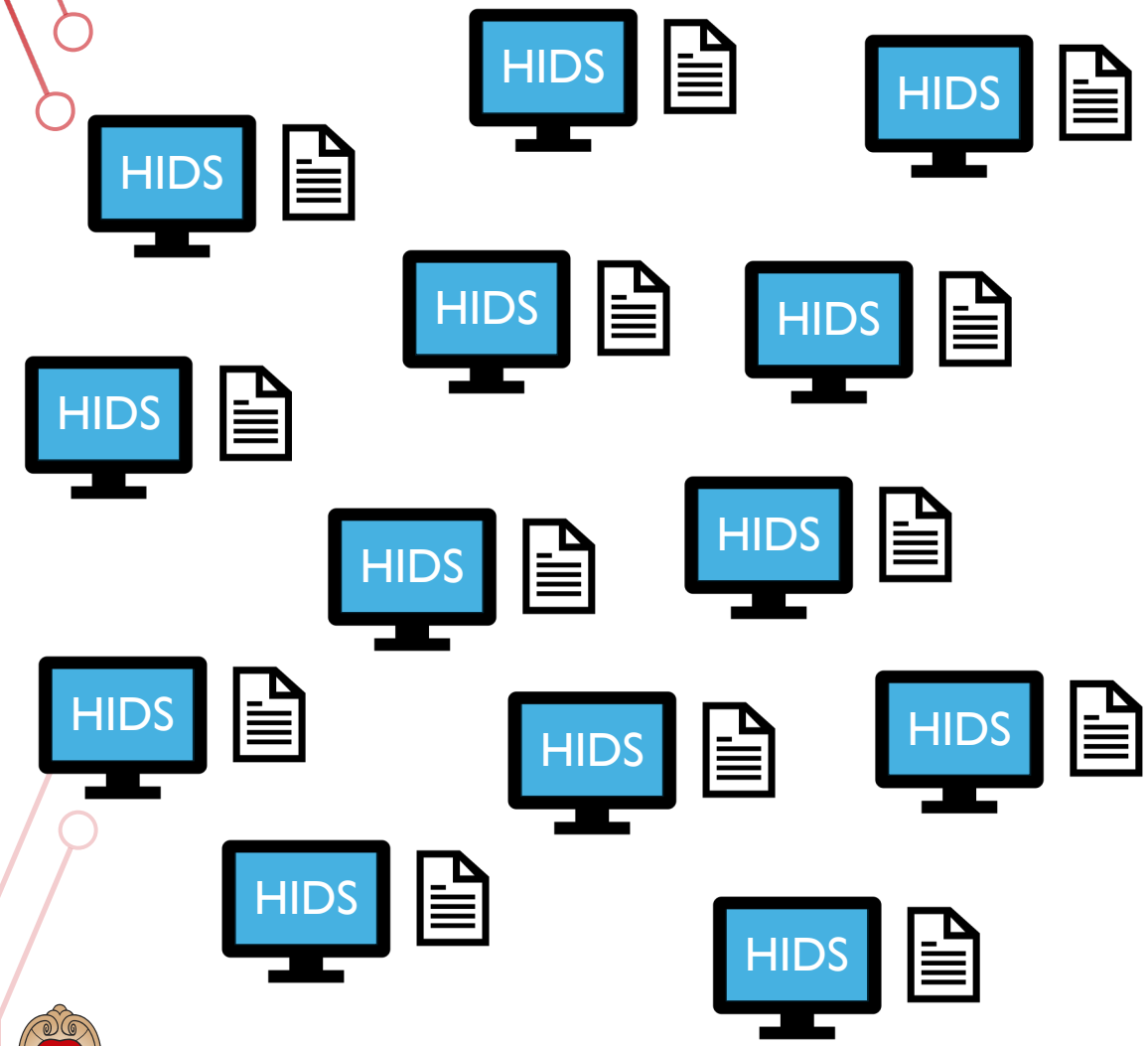
chers that manipulated
ons using cloud systems.

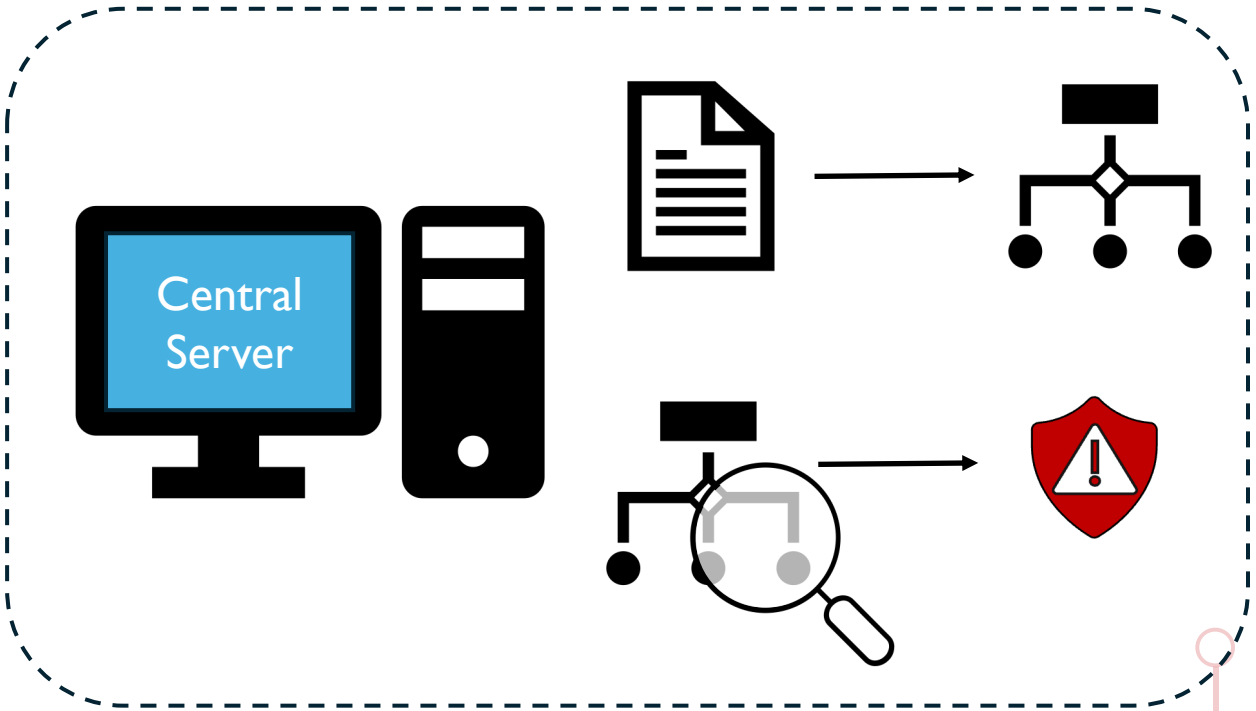
Security is ***critical*** to the success of computing systems.

Research Motivation



Research Motivation

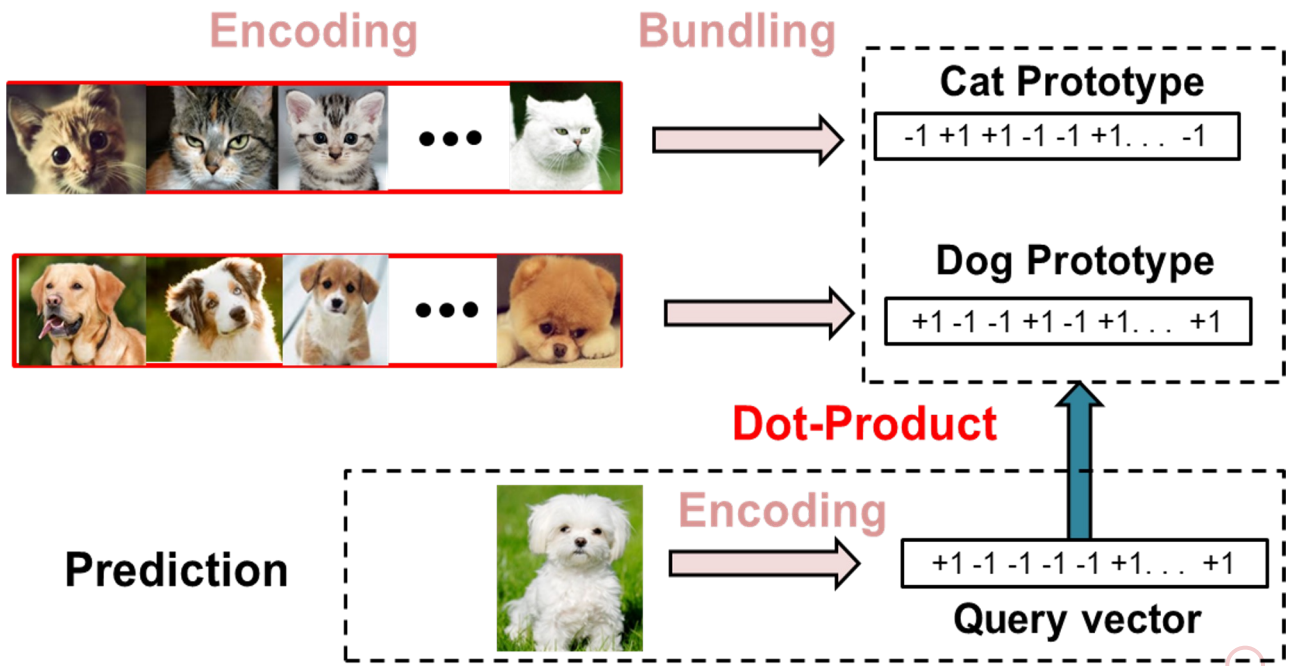




Research Motivation

Hyperdimensional Computing:

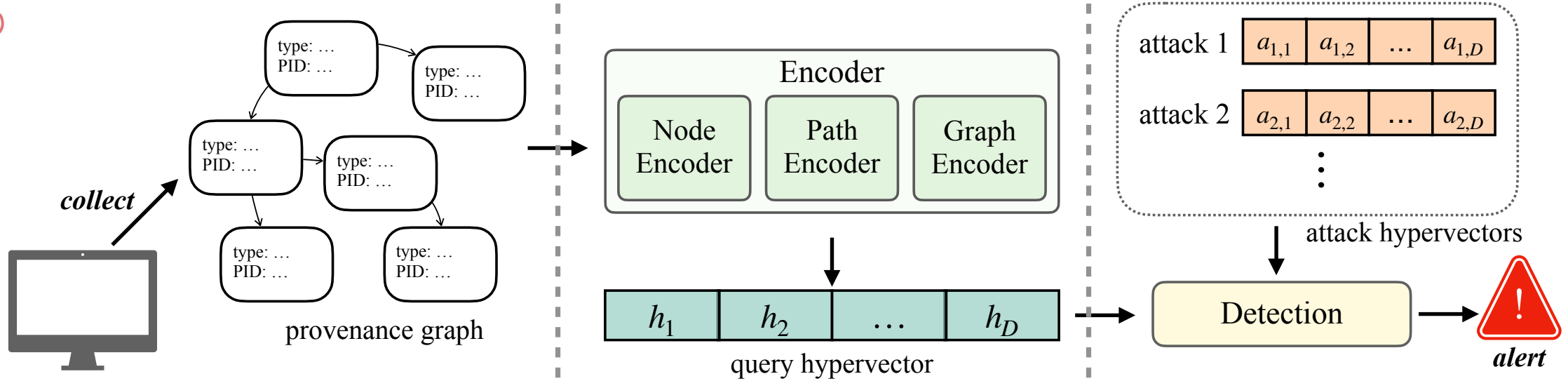
- Lightweight, highly efficient computing framework
- Input data is ***encoded*** into hyper vectors
- Useful in classification, graph prediction, and pattern recognition



Research Question

Can we leverage hyperdimensional computing to develop an intrusion detection system which accelerates performance while maintaining high accuracy?

Methodology



1 Signature Generation

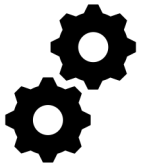
2 HDC Encoding

3 Threat Detection

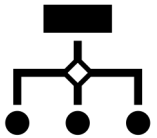
Signature Generation

Leverage SysFlow telemetry framework to gather events

Defined conditions which denote presence of attacks

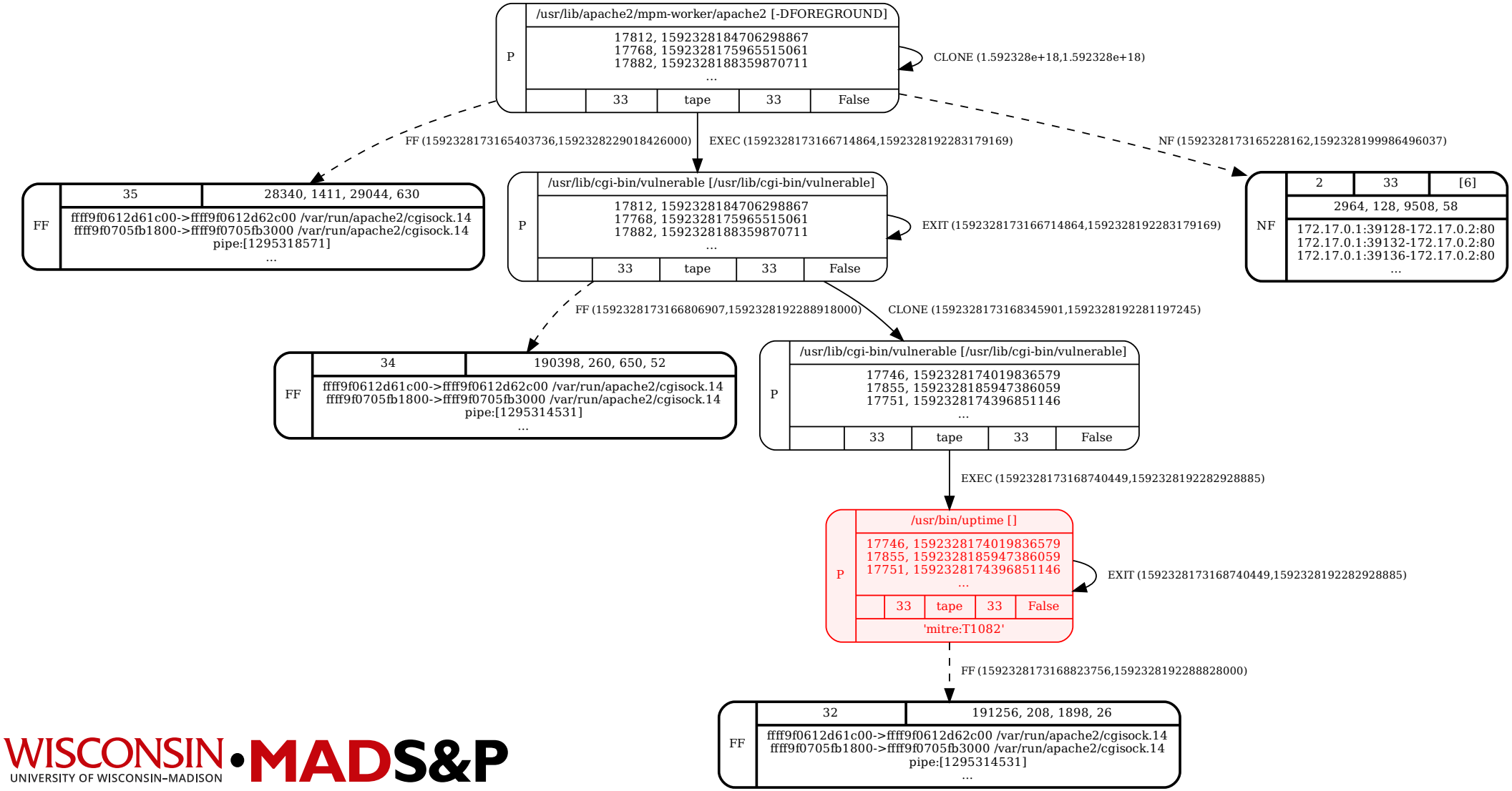


Policy engine to tag nodes in graph which match attack conditions

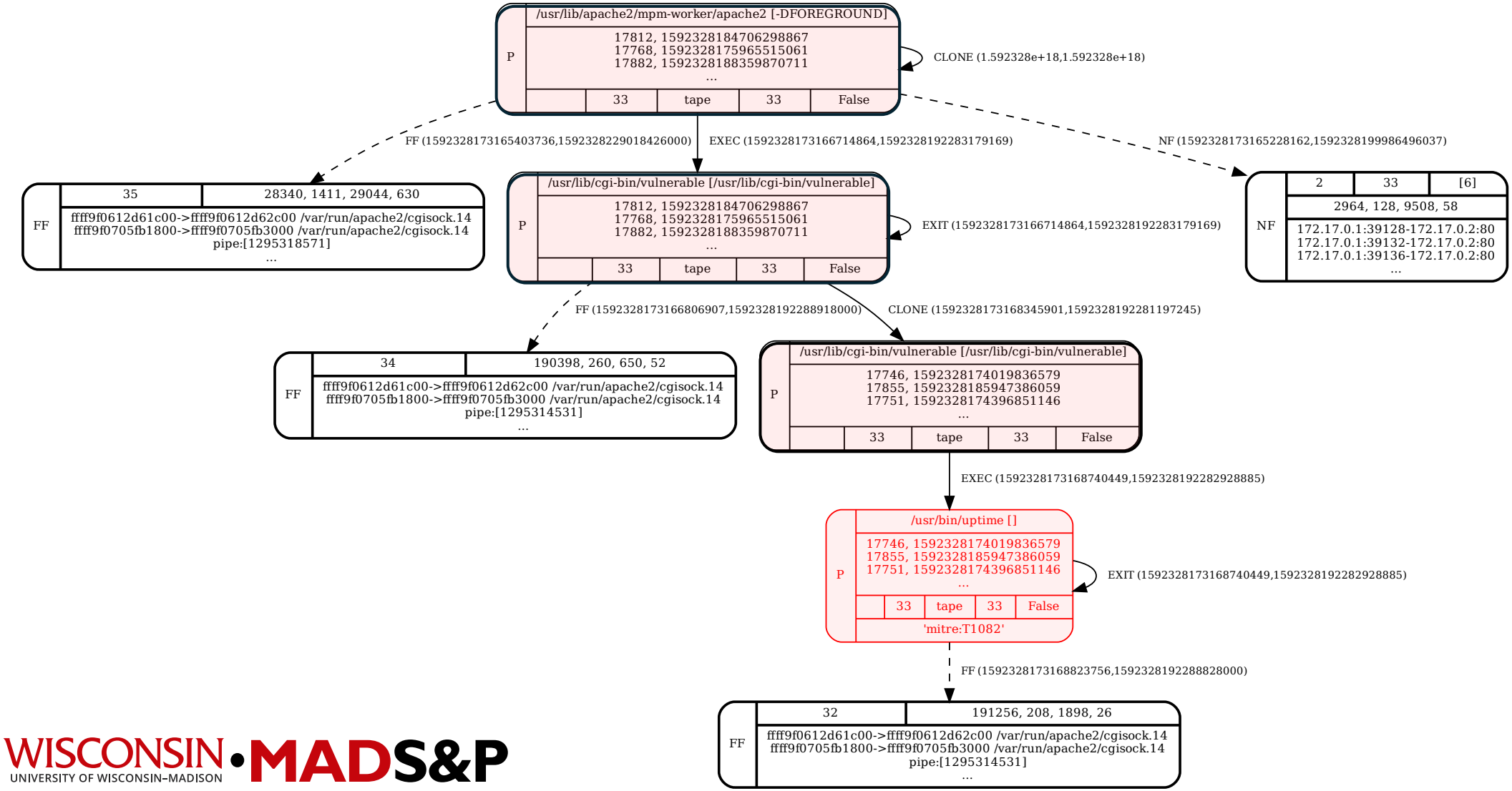


Subgraph with tagged nodes represents attack signature

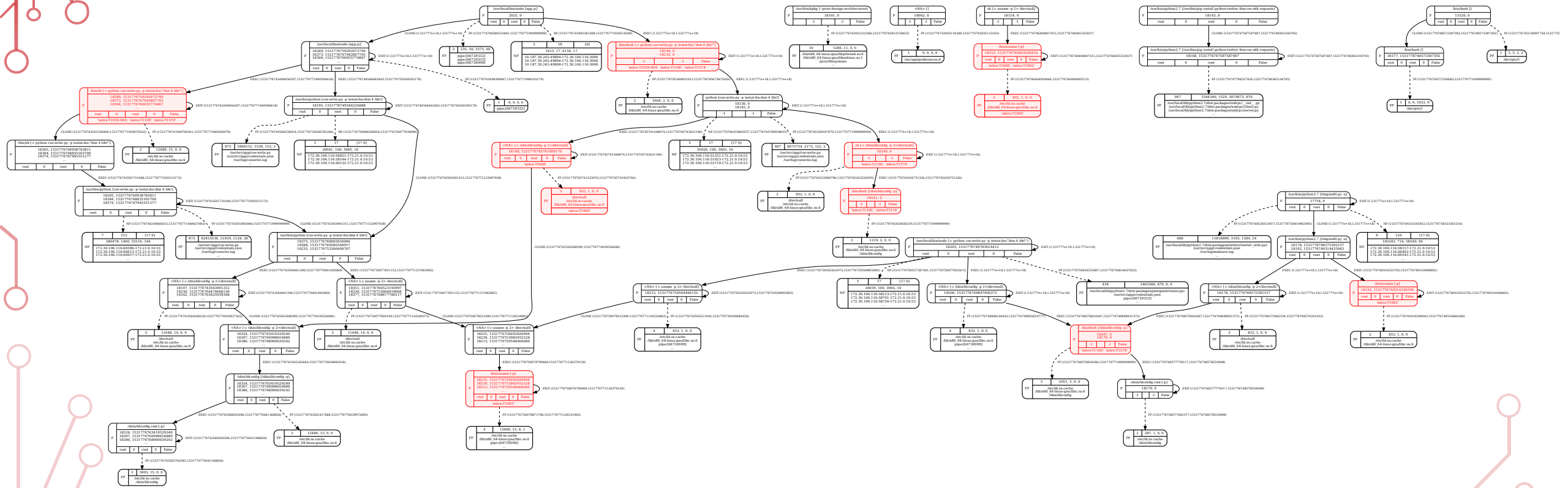
Signature Generation



Signature Generation

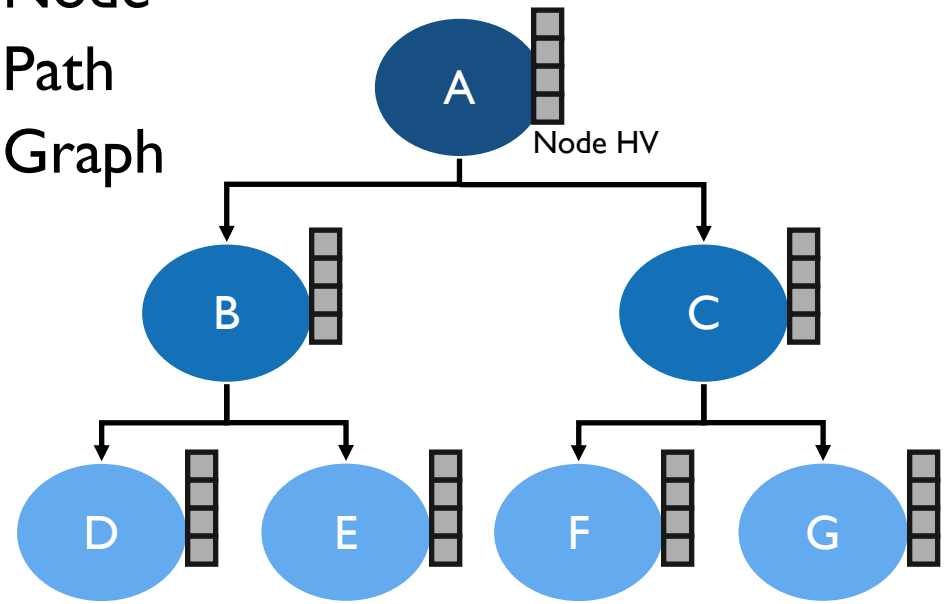


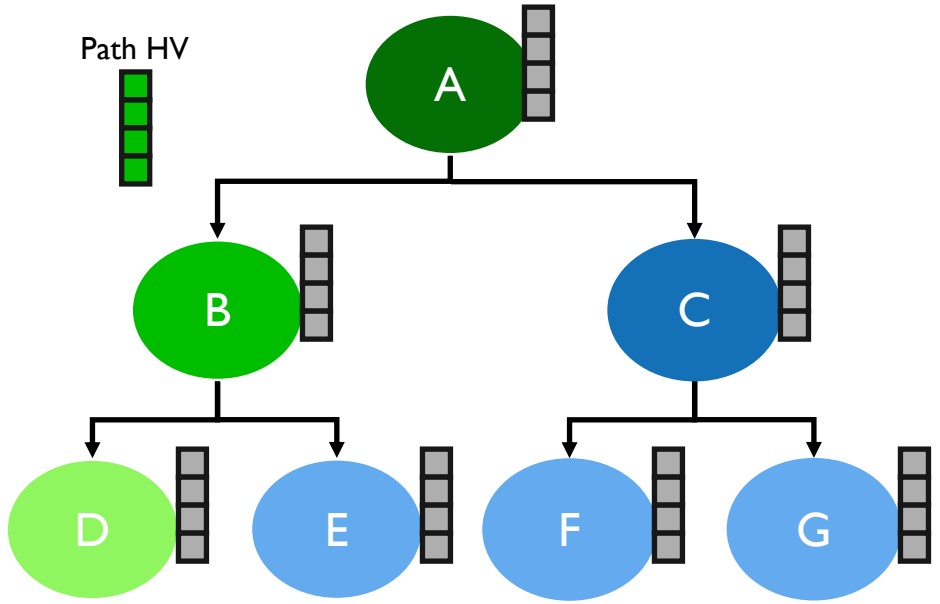
Signature Generation



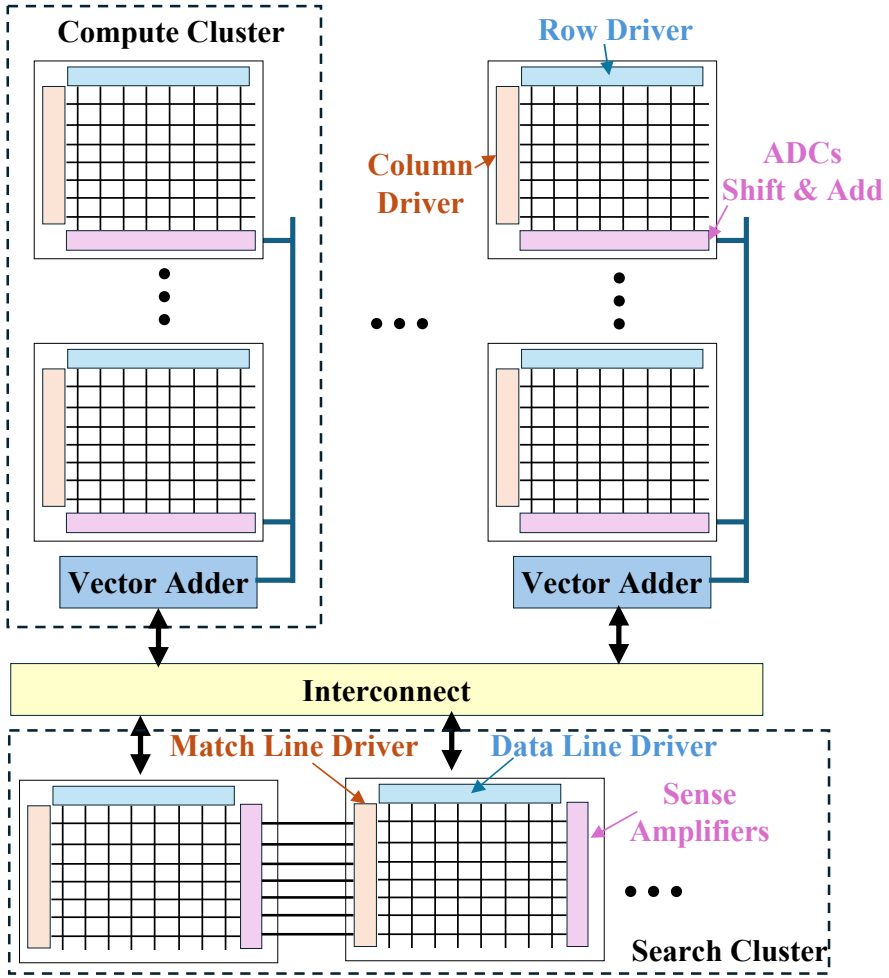
HDC Encoding

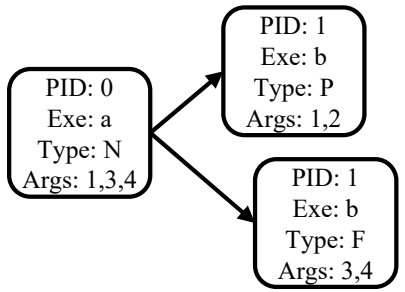
- Three stages of encoding:
  - Node
  - Path
  - Graph



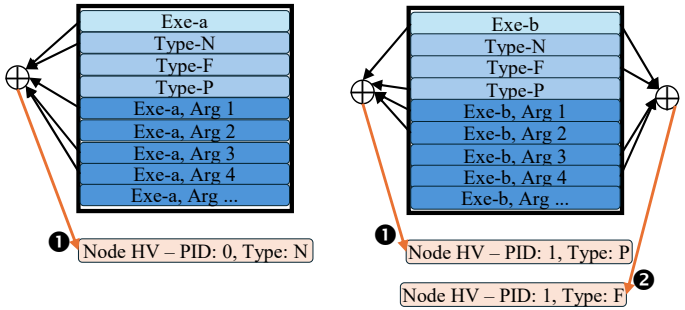


Hardware Acceleration

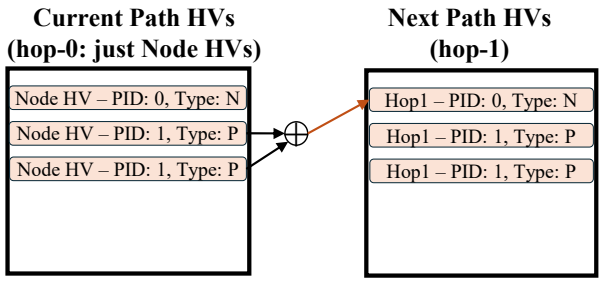




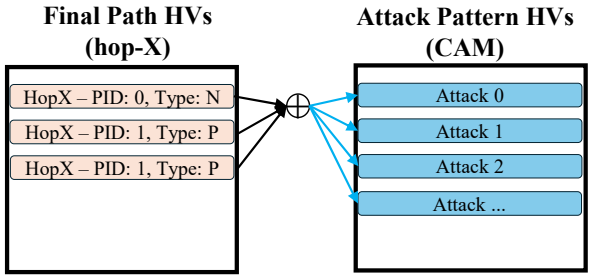
(a) Example graph



(b) Node encoding: all HVs are generated/placed offline



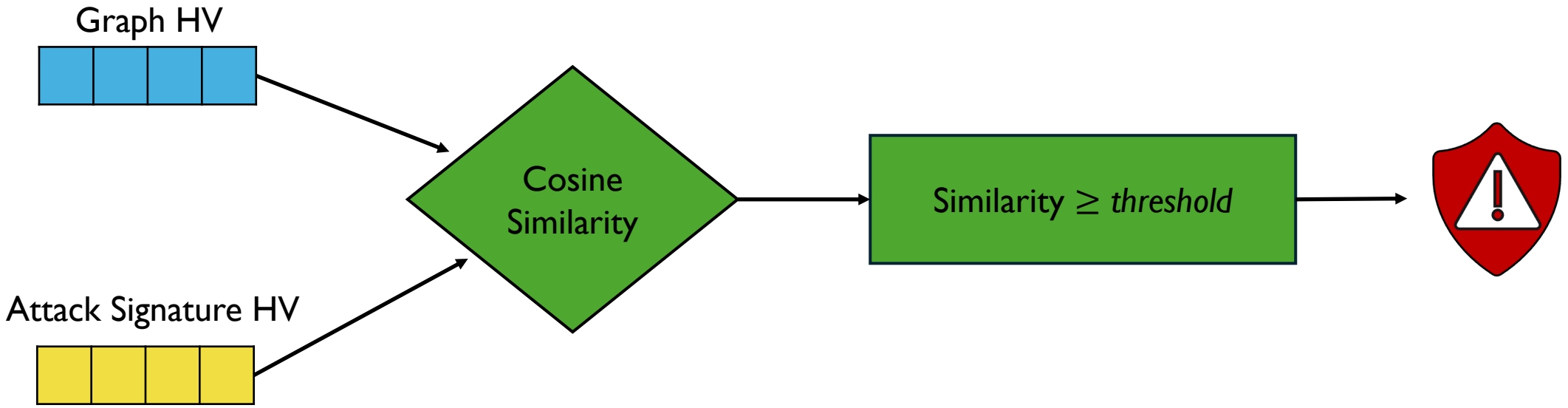
(c) Path encoding



(d) Graph encoding and search

Threat Detection

- Evaluate using cosine similarity



Evaluation

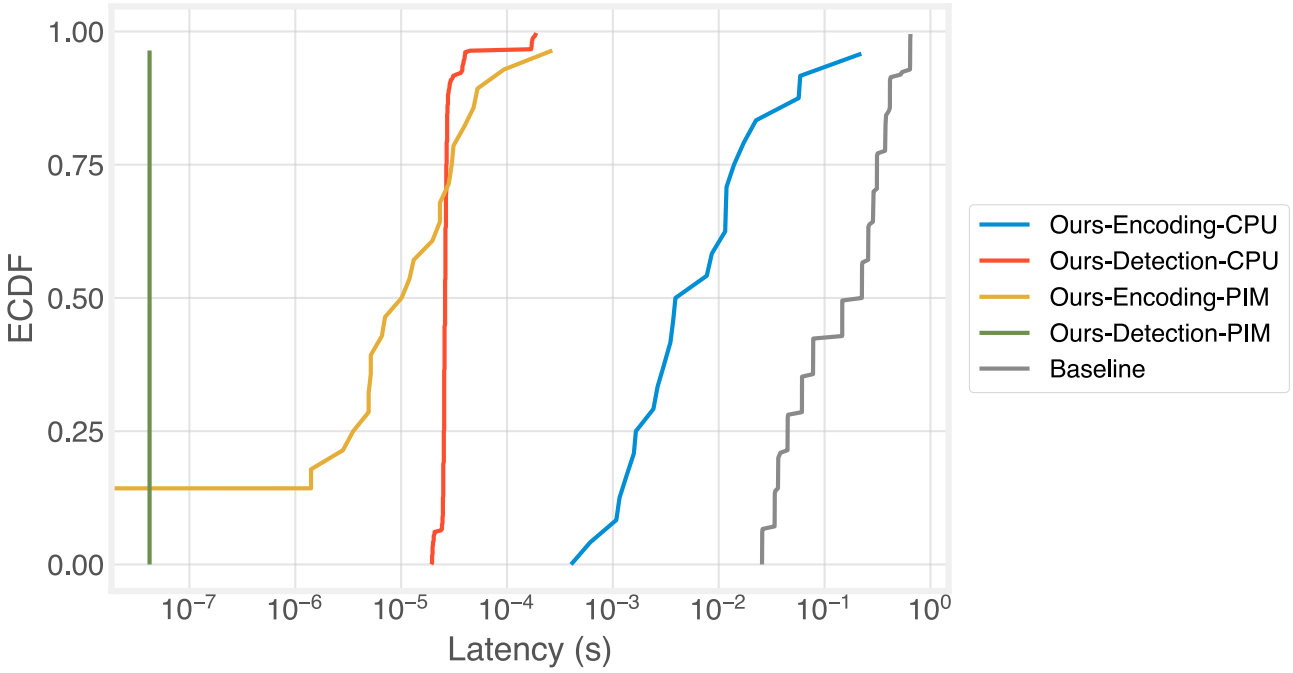
Research Questions:

- (1) What is the latency of our HDC approach?
- (2) How accurate is our HDC approach at detecting threats?

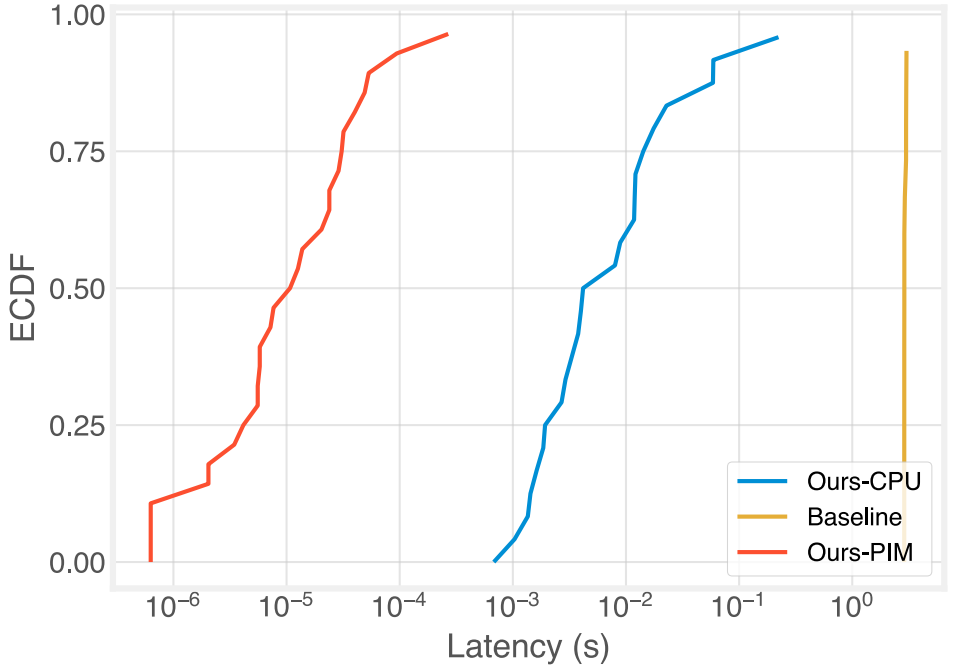
Experiment Setup:

- Dataset of 10 benign traces and 18 malicious traces with attacks from 15 known MITRE TTPs
- CPU: Intel Core i7-8700K processor and 64GB memory
- PIM: NeuroSim to model a FeFET memory with 32 clusters, each consisting of 2,048 memory blocks

Performance Results



Per Attack Latency



Total Latency

Accuracy Results

	Hop-Length			
TTP	0	1	2	3
T1020	1	1	1	1
T1033	0.952	0.984	1	1
T1059.004	1	1	1	0.979
T1068	0.926	0.916	0.853	0.832
T1069.001	1	0.783	0.957	1
T1072	1	1	1	1
T1082	0.828	0.898	0.891	0.891
T1083	0.955	1	1	1
T1087	1	1	1	1
T1087.001	0.87	0.87	0.87	0.898
T1105	0.926	0.726	0.768	0.758
T1106	0.886	0.757	0.771	0.786
T1222.002	0.952	0.984	0.984	0.937
T1552.003	0.825	0.794	0.81	0.825
T1574	0.886	0.757	0.771	0.786
Average	0.934	0.898	0.912	0.913

ROC-AUC scores for each attack and hop length.

Takeaways

We can improve performance of querying provenance graphs with HDC.

- Up to 4,242 times speedup with CPU compared to SotA.

We can achieve high detection accuracy using HDC-based querying.

- Greater than 90% detection accuracy across all attacks and hop lengths.

Thank you!