Tensor Decomposition Methods for Cybersecurity

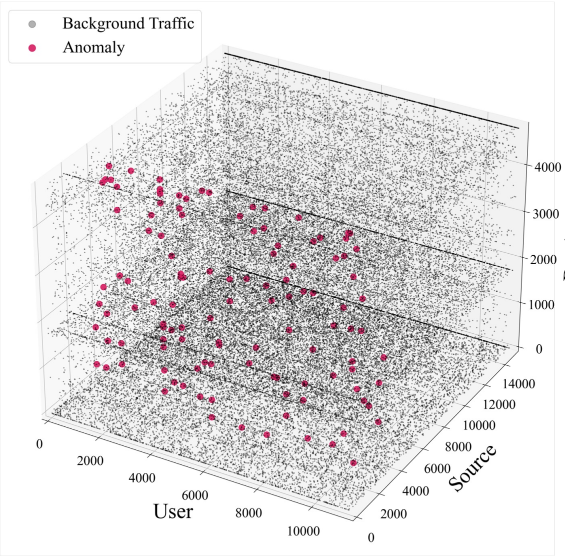
Maksim E. Eren
Advanced Research in Cyber Systems (A-4)
& **CSEE, UMBC**

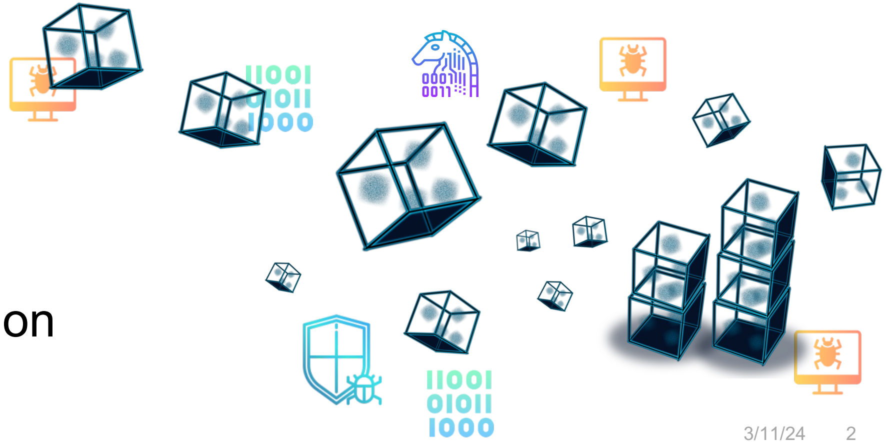
March 12, 24

LA-UR-23-32504

AI4Sec, Auburn University

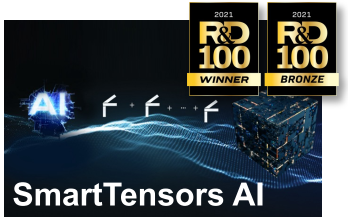
- Network Anomaly Detection
- User Behavior Analysis
- SPAM E-Mail Detection
- Credit Card Fraud Detection
- Malware/Benign-ware Identification
- Malware Family Classification
- Novel Malware Detection
- Federated Learning for Data Privacy
- Power Grid/SCADA Anomaly Detection





Multi-Dimensional Anomalous Entity Detection via Poisson Tensor Factorization [1]

MTEM '21: *Random Forest of Tensors* [5]



[2,3]

MTEM '22: *Malware Antivirus Scan Pattern Mining via Tensor Decomposition* [4]

IEEE MILCOM

Electrical Grid Anomaly Detection via Tensor Decomposition [6]

General-Purpose Unsupervised Cyber Anomaly Detection via Non-Negative Tensor Factorization [18]

Catch'em all: Classification of Rare, Prominent, and Novel Malware Families [36]

One-Shot Federated Group Collaborative Filtering [7]

Los Alamos NATIONAL LABORATORY

Malware Technical Exchange Meeting
Lawrence Livermore National Laboratory
JULY 25-27, 2023

Malware-DNA: Machine Learning for Malware Analysis that Treats Malware as Mutations in the Software Genome [8]

Malware-DNA: Machine Learning for Malware Analysis that Treats Malware as Mutations in the Software Genome

World record

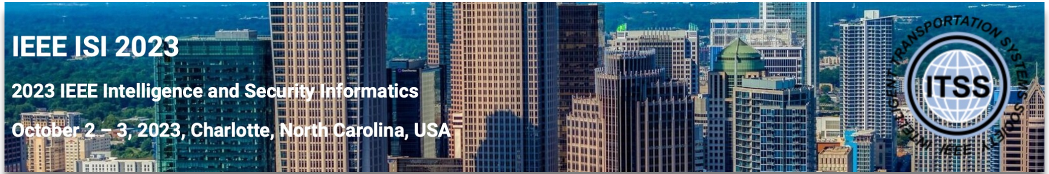
Semi-supervised Classification of Malware Families Under Extreme Class Imbalance via Hierarchical Non-Negative Matrix Factorization with Automatic Model Selection [9]

Patent

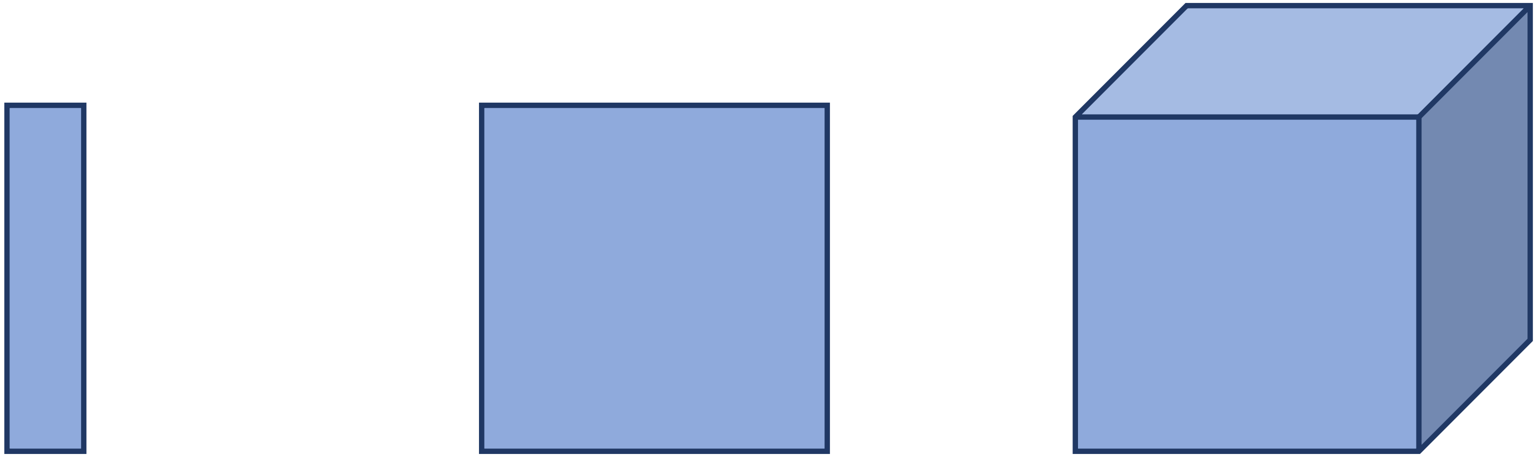
Data Identification and Classification Method, Apparatus, and System, US, Provisional Patent 63/472,188 [10]

SPRINGER NATURE

Classifying Malware Using Tensor Decomposition. Malware - Handbook of Prevention and Detection [37]



MalwareDNA: Simultaneous Classification of Malware, Malware Families, and Novel Malware [11]



Vector
d = 1

Matrix
d = 2

3-Dimensional Tensor
d = 3

$\mathbf{x} \in \mathbb{R}^{N_1}$

$\mathbf{X} \in \mathbb{R}^{N_1 \,\mathrm{x}\, N_2}$

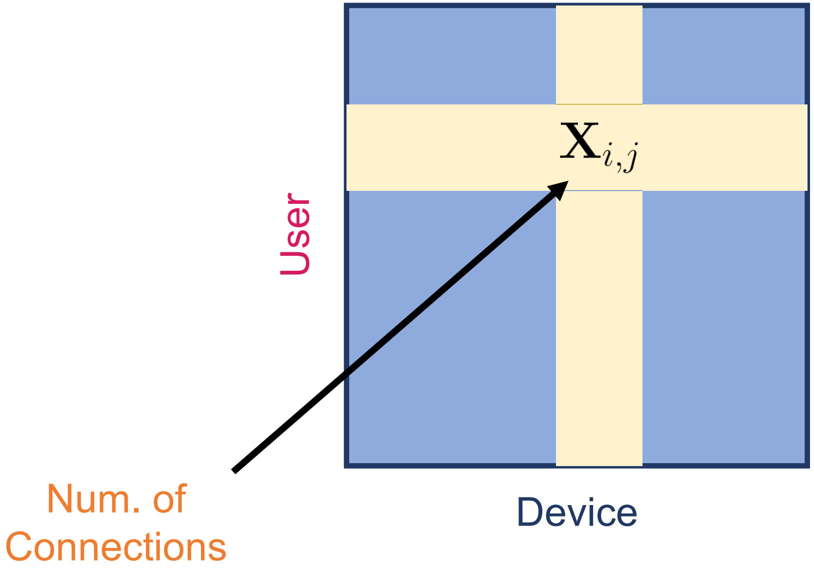
$\boldsymbol{\mathcal{X}} \in \mathbb{R}^{N_1 \,\mathrm{x}\, N_2 \mathrm{x}\, N_3}$

Matrices (2-Dimensional Tensor)

Dimensions: User x Device

Entry: Number of Connections

$$\mathbf{X} \in \mathbb{R}^{N_1 \times N_2}$$



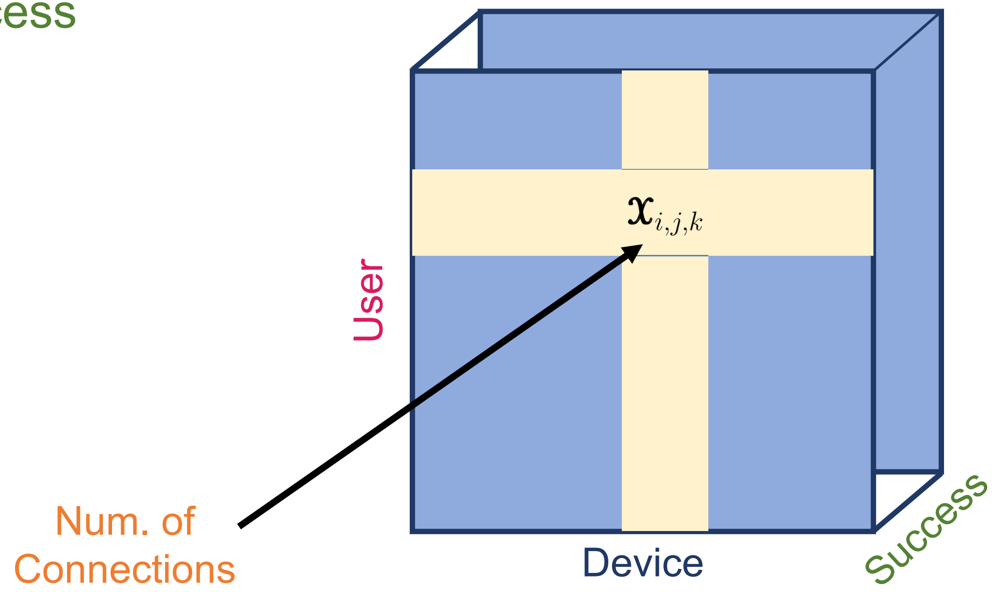
Tensors (3+ Dimensions)

Num. Dimensions (d) **=** 3

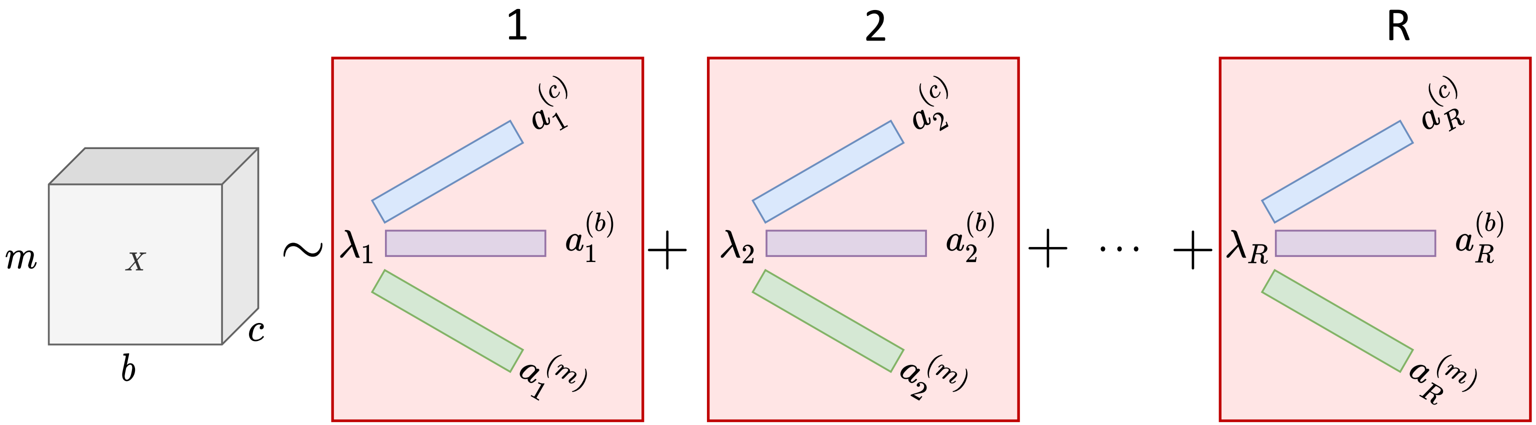
Dimensions: User x Device x Success

Entry: Number of Connections

$$\mathcal{X} \in \mathbb{R}^{N_1 \times N_2 \times N_3}$$



CANDECOMP/PARAFAC Decomposition (CPD)

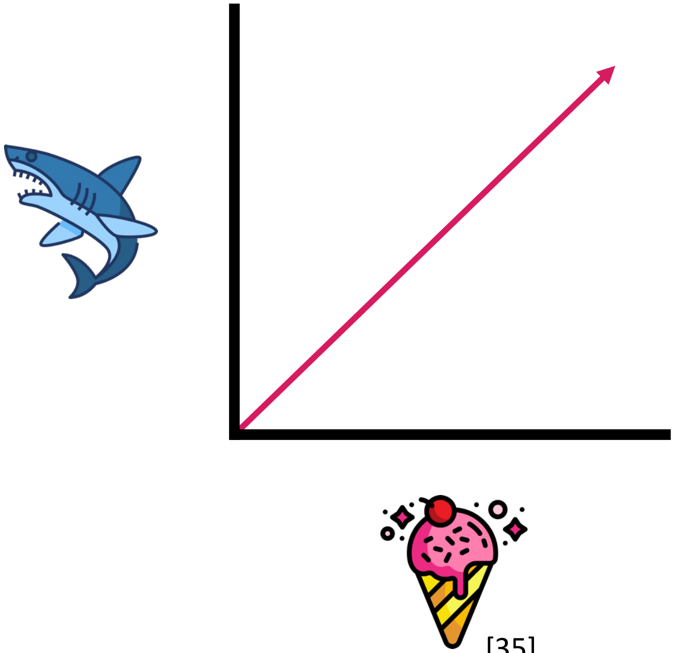


$$\mathfrak{X} \approx \sum_{r=1}^{R} \boxed{\lambda_r \cdot \mathbf{a}_r^{(m)} \circ \mathbf{a}_r^{(b)} \circ \mathbf{a}_r^{(c)}}$$

$$\mathfrak{X} \approx \mathfrak{M} \equiv [\![\lambda \,;\, \mathbf{A}^{(m)}, \mathbf{A}^{(b)}, \mathbf{A}^{(c)}]\!]$$

$$\mathbf{A}^{(d)} = [\mathbf{a}_1^{(d)}, \mathbf{a}_2^{(d)}, \ldots, \mathbf{a}_R^{(d)}]$$

Hidden Patterns?



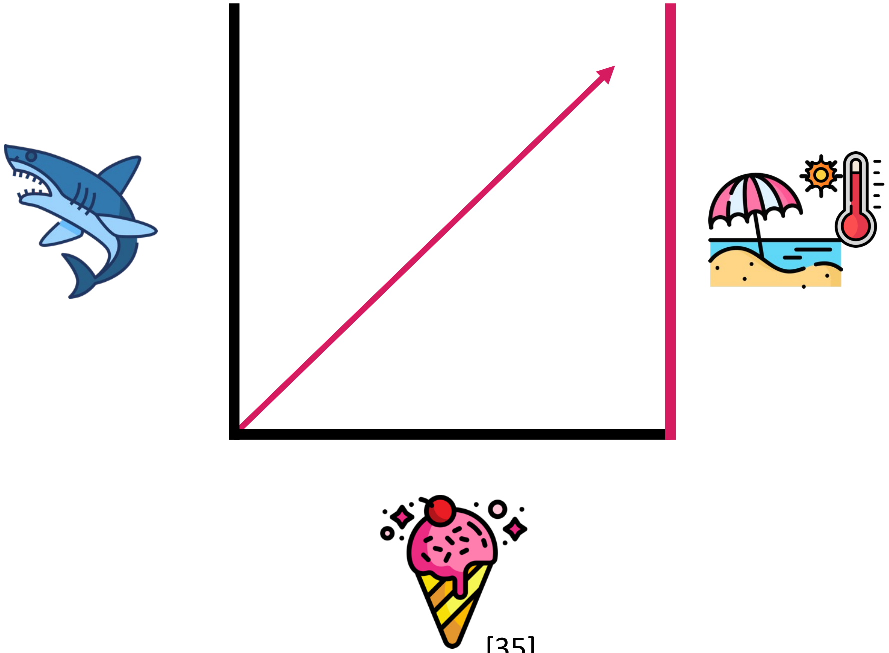
[35]

- Observable variables are often not that useful

Increase in ice cream consumption → Increase in shark attacks

Huh?

Hidden Patterns?



[35]

- Hidden patterns and correlations

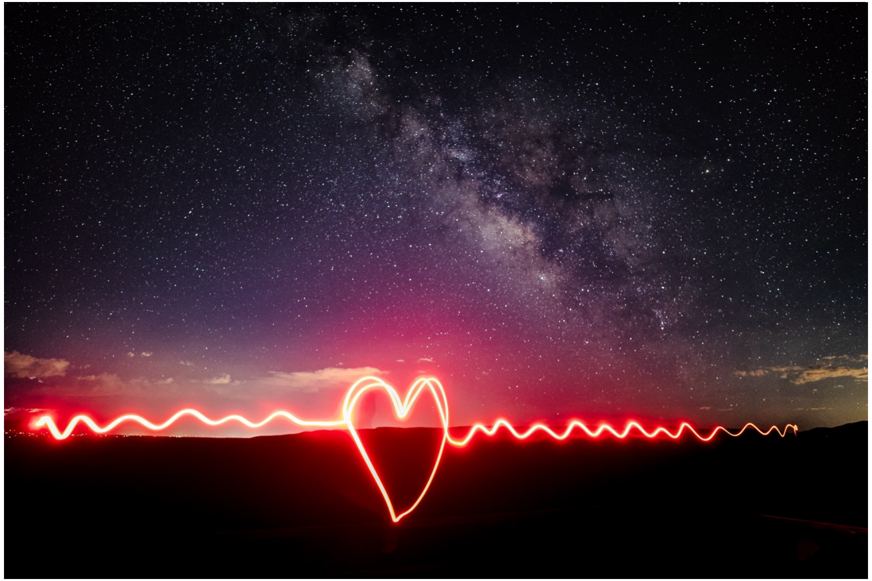
Useful for actionable results

Modeling data

Decision making

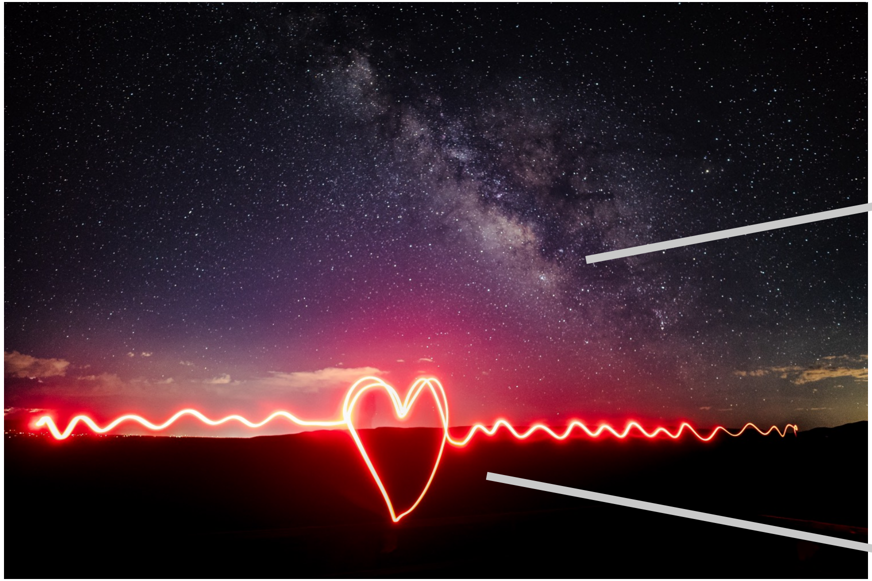
Accurate Data Modeling

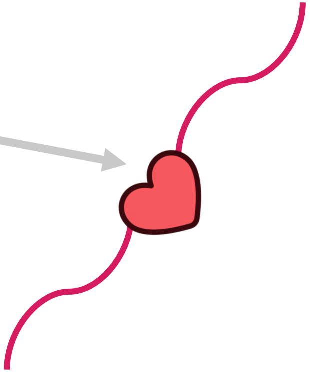
Nikon Z5, ISO 2500, f1.8, 15s - White Rock, Overlook, NM



Accurate Data Modeling

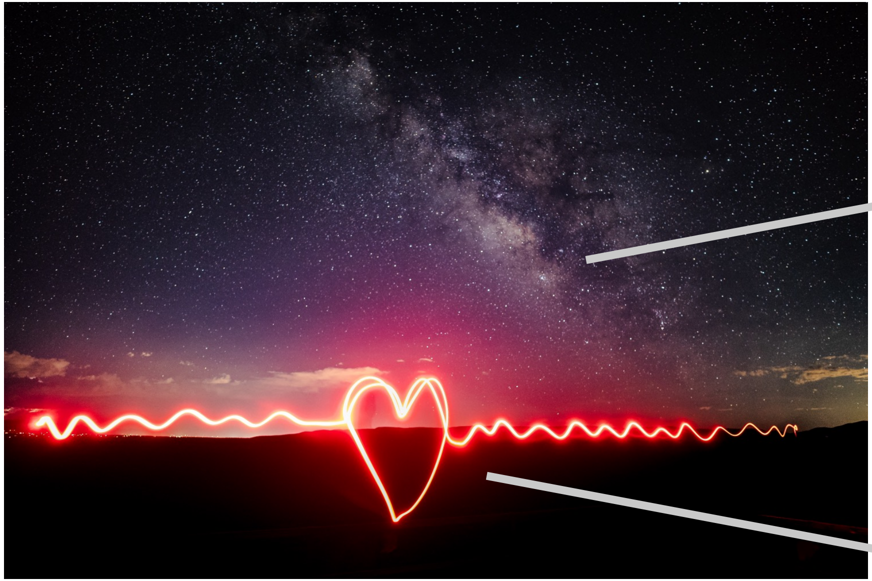
Nikon Z5, ISO 2500, f1.8, 15s - White Rock, Overlook, NM

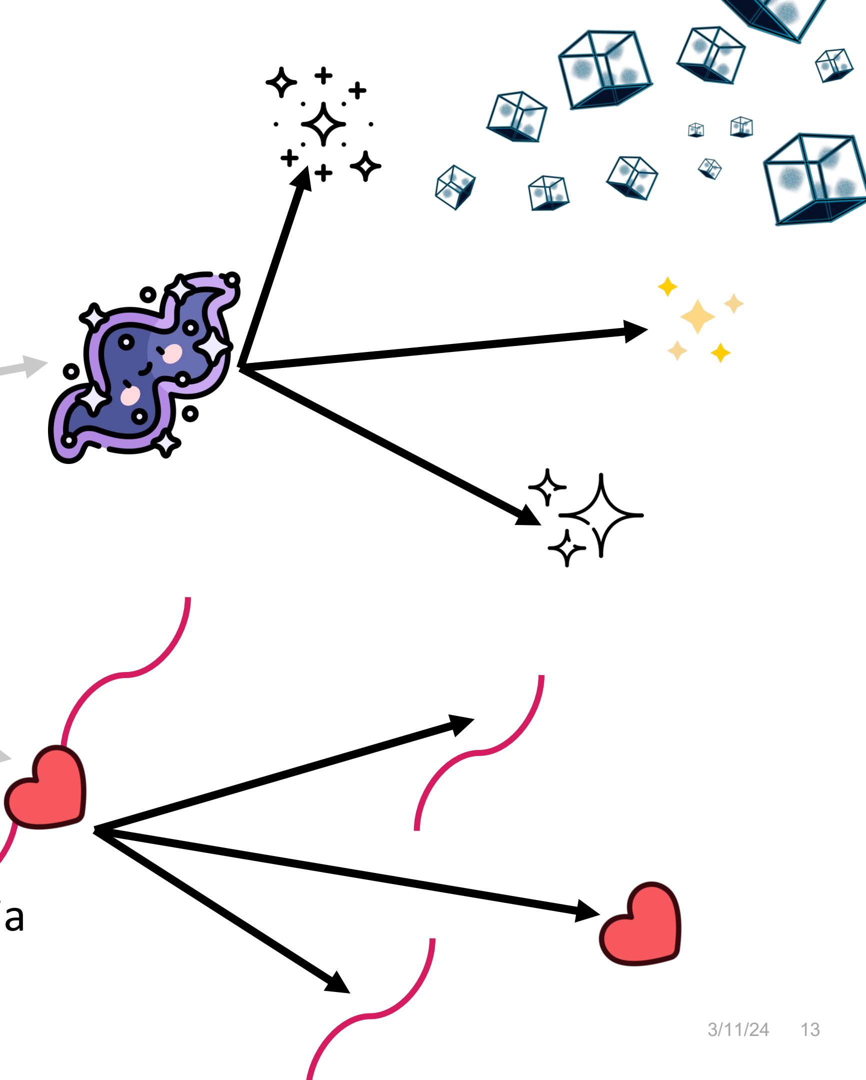




Accurate Data Modeling

Nikon Z5, ISO 2500, f1.8, 15s - White Rock, Overlook, NM





Automatic Model Determination:
Estimates the number of latent features using the **stability and accuracy** of the solutions via a **bootstrap approach**

Unsupervised Anomaly Detection

Detecting malicious anomalies is a significant challenge

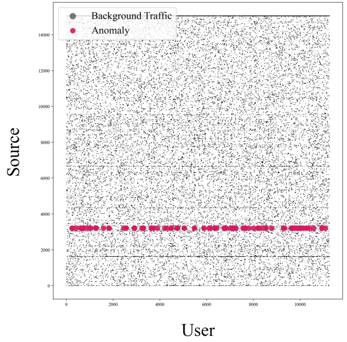
81%
of the cyber espionage breaches involved phishing
[12]

$3.86 million
average cost of a single security breach
[13]

80%
of data breaches involved compromised credentials
[14]

9%
of the attacks generated alerts
[15]

Motivation

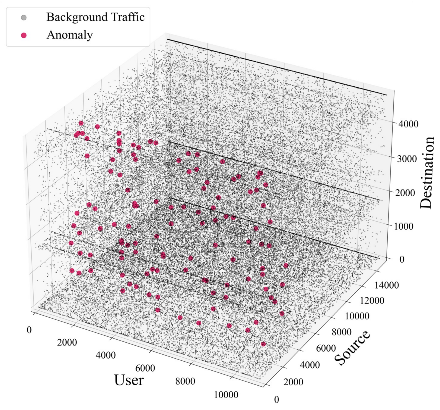


Traditional anomaly detection methods:

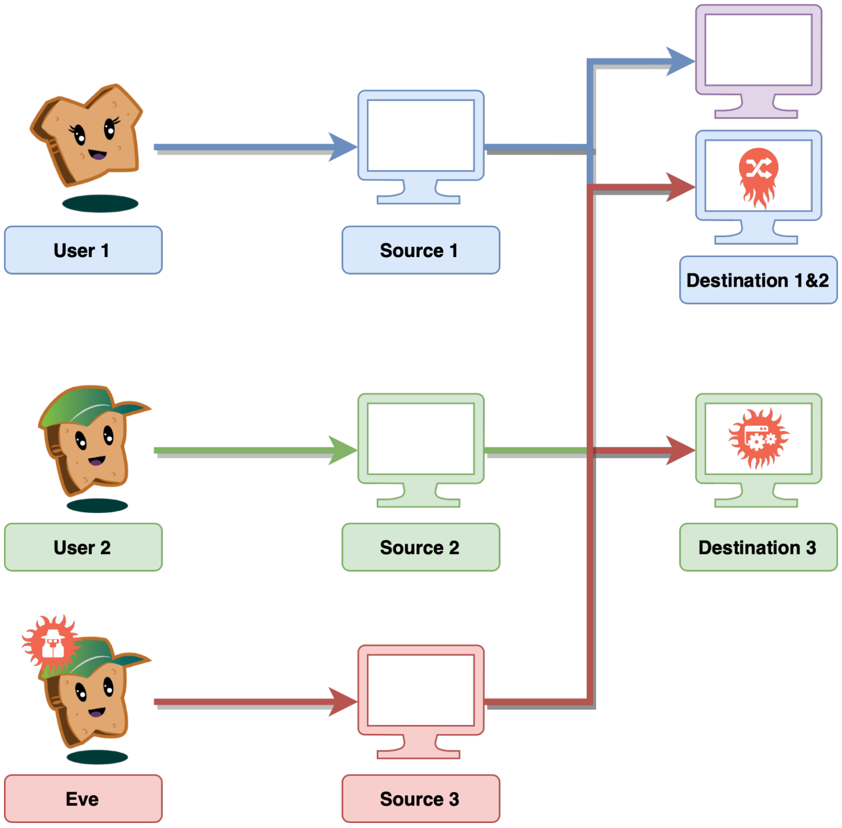
- User Behavior Analysis based on **matrix factorization is limited to 2 dimensions**
- Popular **Machine Learning models are black-box**
- **Rule-based indicators can fail** to detect zero day attacks
- Supervised solutions need **immense amount of labeled data**

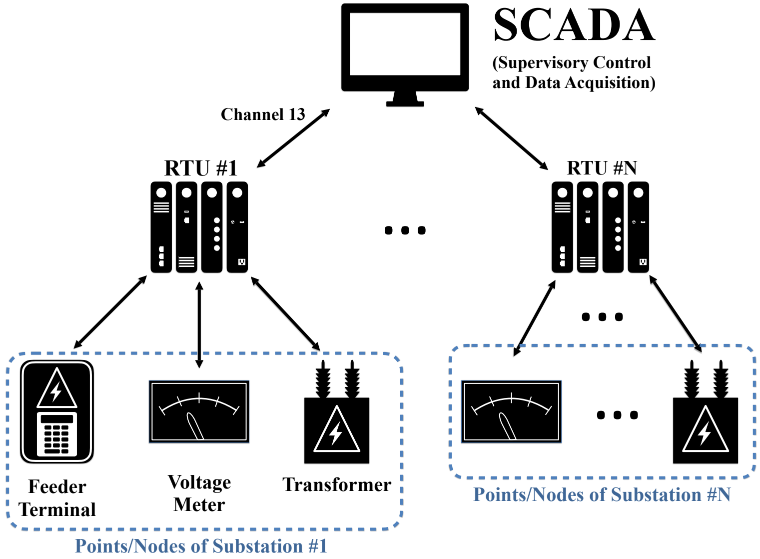
Non-negative Tensor decomposition for anomaly detection:

- **Model multi-dimensional activity profile** of the network events
- Produces **interpretable results**
- Detects a **few anomalies hidden in a large REAL world data**
- **Generalize to unseen types of attacks** that are out of the norm



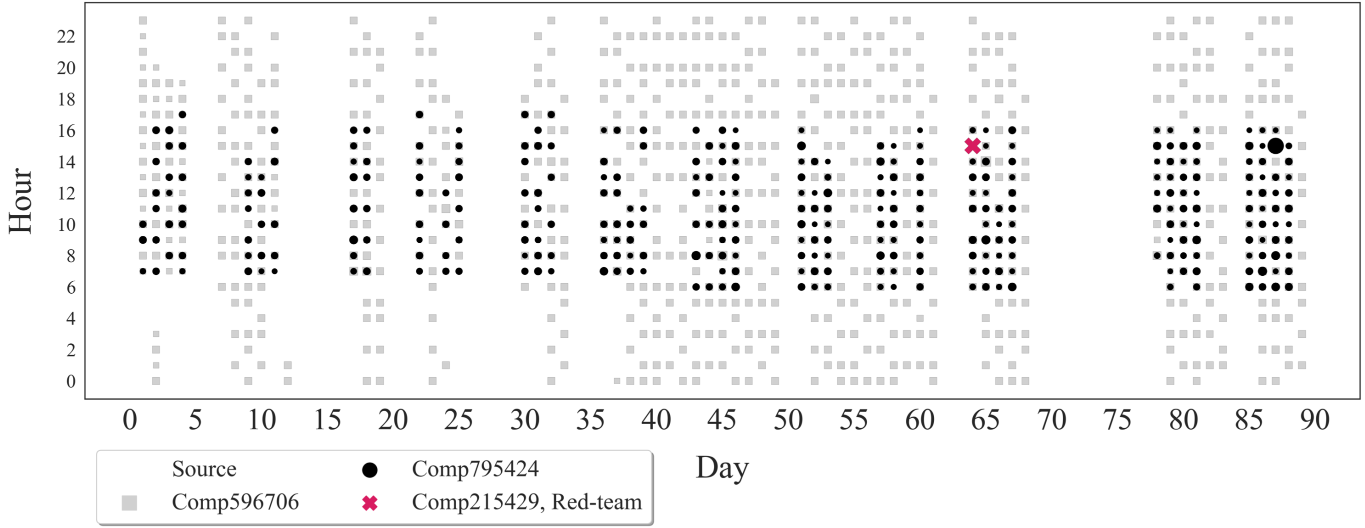
What do we want to detect?



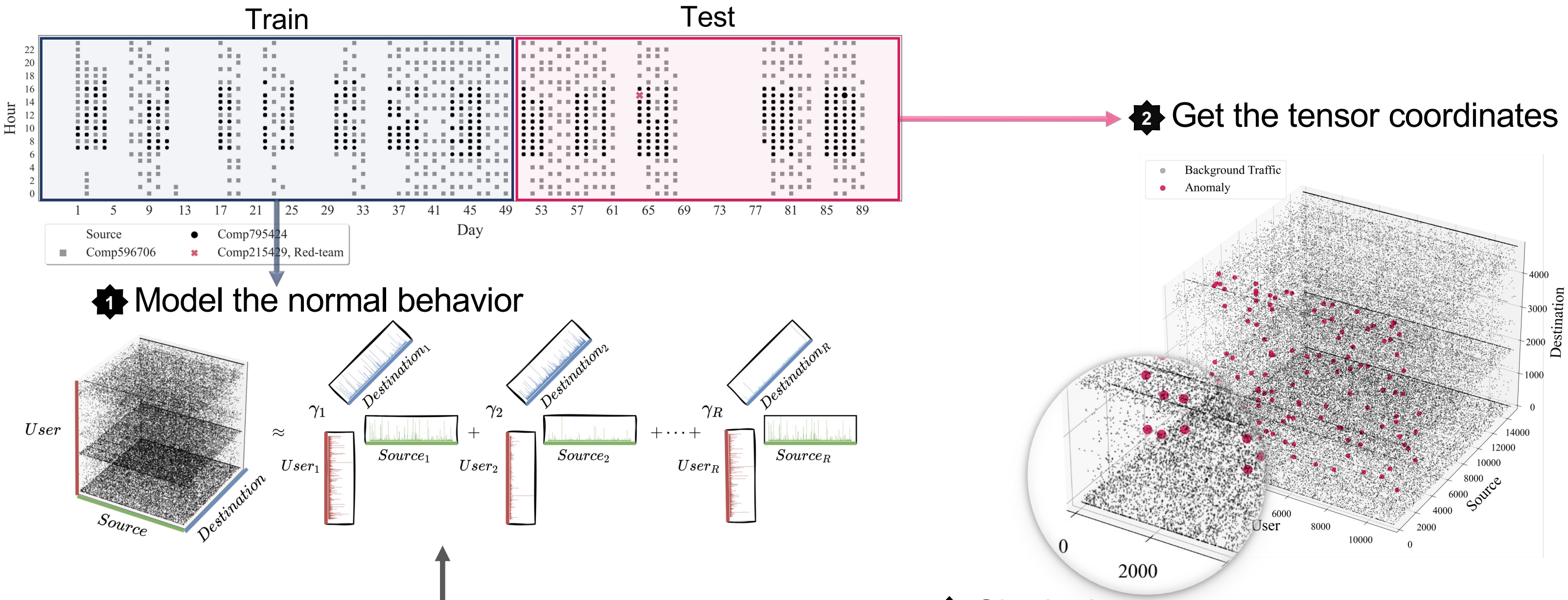


User Network Patterns

Users/devices create predictable patterns in time



General Unsupervised Anomaly Detection Framework



3 Obtain the anomaly scores

$$\mathcal{X}_{i_1,i_2,i_3} \sim \text{Poisson}(\lambda_{i_1,i_2,i_3})$$

$$\lambda_{i_1,i_2,i_3} = \sum_{r=1}^{R} \gamma_r \prod_{d=1}^{3} \theta^{(d)}_{r,i_d}$$

Los Alamos NATIONAL LABORATORY

Tensor Details

Table 1. Tensor details and test set p-value statistics for anomalous and benign events

	Tensor Details			**Anomaly p-value**			**Benign p-value**		
Dataset & Tensor	Dimensions Size	% Non-Zero	Decomposed Rank	Mean	Std	Count	Mean	Std	Count
LANL US	11260 x 15055	2.57×10^{-4}	20	.1993	.3253	76	.8945	.2421	31,241
LANL UD	11260 x 4796	1.51×10^{-3}	20	.6399	.3315	117	.9489	.1829	69,596
LANL USDs	11260 x 15055 x 4796 x 2	1.02×10^{-7}	4	.2721	.4090	119	.9575	.1677	125,166
LANL USDHs	11260 x 15055 x 4796 x 24 x 2	3.04×10^{-8}	5	.1062	.2621	137	.9801	.1215	955,808
LANL USDHDs	11260 x 15055 x 4796 x 24 x 7 x 2	1.60×10^{-8}	45	.0175	.0765	138	.9946	.0664	3,513,527
UGR'16 Neris 3&2 Octet Src&Dest IP Map	7453770 x 65536 x 24 x 7	7.32×10^{-7}	8	.0465	.1998	3,001	.9717	.1516	20,117,426
UGR'16 Neris 20-Bits IP Map	655360 x 522429 x 24 x 7	1.04×10^{-6}	10	.0262	.1425	6,381	.9659	.1478	23,383,989
UGR'16 Neris 24-Bits IP Map	3865526 x 848382 x 24 x 7	1.09×10^{-7}	7	.1464	.3008	2,369	.9822	.1034	21,847,564
UGR'16 Neris 4 Character IP Hash Map	65536 x 65536 x 24 x 7	8.04×10^{-5}	10	.0292	.1246	8,381	.9447	.2065	23,189,409
UGR'16 Neris 5 Character IP Hash Map	1048487 x 663889 x 24 x 7	5.16×10^{-7}	7	.0330	.1599	5,781	.9732	.1262	23,250,847
UGR'16 Neris 6 Character IP Hash Map	7477572 x 1019015 x 24 x 7	4.72×10^{-8}	6	.2813	.4315	495	.9857	.0922	19,481,318
UGR'16 Spam E-Mail	55287 x 65536 x 24 x 7	2.66×10^{-5}	20	.3814	.2165	2,495	.9791	.1220	1,909,544
PaySim Credit Card	100 x 5 x 24 x 7 x 100 x 100	9.00×10^{-6}	25	.6826	.4387	4,391	.9998	.0058	1,224

Tensor Details

Table 1. Tensor details and test set p-value statistics for anomalous and benign events

	Tensor Details			Anomaly p-value			Benign p-value		
Dataset & Tensor	Dimensions Size	% Non-Zero	Decomposed Rank	Mean	Std	Count	Mean	Std	Count
LANL US	11260 x 15055	2.57×10^{-4}	20	.1993	.3253	76	.8945	.2421	31,241
LANL UD	11260 x 4796	1.51×10^{-3}	20	.6399	.3315	117	.9489	.1829	69,596
LANL USDs	11260 x 15055 x 4796 x 2	1.02×10^{-7}	4	.2721	.4090	119	.9575	.1677	125,166
LANL USDHs	11260 x 15055 x 4796 x 24 x 2	3.04×10^{-8}	5	.1062	.2621	137	.9801	.1215	955,808
LANL USDHDs	11260 x 15055 x 4796 x 24 x 7 x 2	1.60×10^{-8}	45	.0175	.0765	138	.9946	.0664	3,513,527
UGR'16 Neris 3&2 Octet Src&Dest IP Map	7453770 x 65536 x 24 x 7	7.32×10^{-7}	8	.0465	.1998	3,001	.9717	.1516	20,117,426
UGR'16 Neris 20-Bits IP Map	655360 x 522429 x 24 x 7	1.04×10^{-6}	10	.0262	.1425	6,381	.9659	.1478	23,383,989
UGR'16 Neris 24-Bits IP Map	3865526 x 848382 x 24 x 7	1.09×10^{-7}	7	.1464	.3008	2,369	.9822	.1034	21,847,564
UGR'16 Neris 4 Character IP Hash Map	65536 x 65536 x 24 x 7	8.04×10^{-5}	10	.0292	.1246	8,381	.9447	.2065	23,189,409
UGR'16 Neris 5 Character IP Hash Map	1048487 x 663889 x 24 x 7	5.16×10^{-7}	7	.0330	.1599	5,781	.9732	.1262	23,250,847
UGR'16 Neris 6 Character IP Hash Map	7477572 x 1019015 x 24 x 7	4.72×10^{-8}	6	.2813	.4315	495	.9857	.0922	19,481,318
UGR'16 Spam E-Mail	55287 x 65536 x 24 x 7	2.66×10^{-5}	20	.3814	.2165	2,495	.9791	.1220	1,909,544
PaySim Credit Card	100 x 5 x 24 x 7 x 100 x 100	9.00×10^{-6}	25	.6826	.4387	4,391	.9998	.0058	1,224

Extremely Sparse

Large-scale analysis:
tensors with up to 6 dimensions

Tensor Details

Table 1. Tensor details and test set p-value statistics for anomalous and benign events

	Tensor Details			Anomaly p-value			Benign p-value		
Dataset & Tensor	Dimensions Size	% Non-Zero	Decomposed Rank	Mean	Std	Count	Mean	Std	Count
LANL US	11260 x 15055	2.57×10^{-4}	20	.1993	.3253	76	.8945	.2421	31,241
LANL UD	11260 x 4796	1.51×10^{-3}	20	.6399	.3315	117	.9489	.1829	69,596
LANL USDs	11260 x 15055 x 4796 x 2	1.02×10^{-7}	4	.2721	.4090	119	.9575	.1677	125,166
LANL USDHs	11260 x 15055 x 4796 x 24 x 2	3.04×10^{-8}	5	.1062	.2621	137	.9801	.1215	955,808
LANL USDHDs	11260 x 15055 x 4796 x 24 x 7 x 2	1.60×10^{-8}	45	.0175	.0765	138	.9946	.0664	3,513,527
UGR'16 Neris 3&2 Octet Src&Dest IP Map	7453770 x 65536 x 24 x 7	7.32×10^{-7}	8	.0465	.1998	3,001	.9717	.1516	20,117,426
UGR'16 Neris 20-Bits IP Map	655360 x 522429 x 24 x 7	1.04×10^{-6}	10	.0262	.1425	6,381	.9659	.1478	23,383,989
UGR'16 Neris 24-Bits IP Map	3865526 x 848382 x 24 x 7	1.09×10^{-7}	7	.1464	.3008	2,369	.9822	.1034	21,847,564
UGR'16 Neris 4 Character IP Hash Map	65536 x 65536 x 24 x 7	8.04×10^{-5}	10	.0292	.1246	8,381	.9447	.2065	23,189,409
UGR'16 Neris 5 Character IP Hash Map	1048487 x 663889 x 24 x 7	5.16×10^{-7}	7	.0330	.1599	5,781	.9732	.1262	23,250,847
UGR'16 Neris 6 Character IP Hash Map	7477572 x 1019015 x 24 x 7	4.72×10^{-8}	6	.2813	.4315	495	.9857	.0922	19,481,318
UGR'16 Spam E-Mail	55287 x 65536 x 24 x 7	2.66×10^{-5}	20	.3814	.2165	2,495	.9791	.1220	1,909,544
PaySim Credit Card	100 x 5 x 24 x 7 x 100 x 100	9.00×10^{-6}	25	.6826	.4387	4,391	.9998	.0058	1,224

Hunting for the needles
in a haystack

Tensor Details

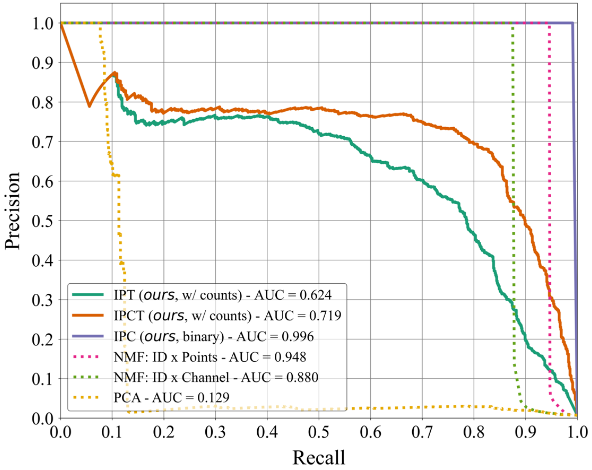
Table 1. Tensor details and test set p-value statistics for anomalous and benign events

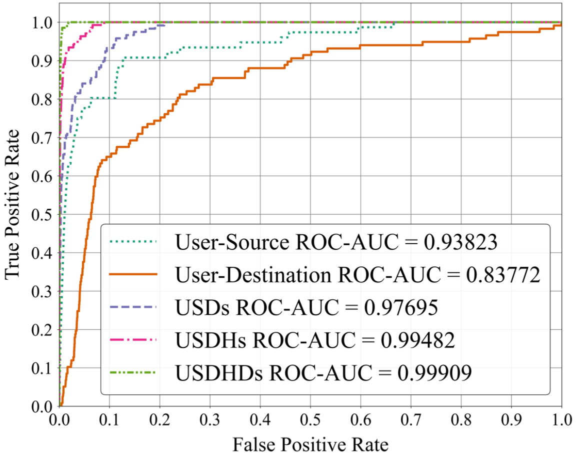
	Tensor Details			Anomaly p-value			Benign p-value		
Dataset & Tensor	Dimensions Size	% Non-Zero	Decomposed Rank	Mean	Std	Count	Mean	Std	Count
LANL US	11260 x 15055	2.57×10^{-4}	20	.1993	.3253	76	.8945	.2421	31,241
LANL UD	11260 x 4796	1.51×10^{-3}	20	.6399	.3315	117	.9489	.1829	69,596
LANL USDs	11260 x 15055 x 4796 x 2	1.02×10^{-7}	4	.2721	.4090	119	.9575	.1677	125,166
LANL USDHs	11260 x 15055 x 4796 x 24 x 2	3.04×10^{-8}	5	.1062	.2621	137	.9801	.1215	955,808
LANL USDHDs	11260 x 15055 x 4796 x 24 x 7 x 2	1.60×10^{-8}	45	.0175	.0765	138	.9946	.0664	3,513,527
UGR'16 Neris 3&2 Octet Src&Dest IP Map	7453770 x 65536 x 24 x 7	7.32×10^{-7}	8	.0465	.1998	3,001	.9717	.1516	20,117,426
UGR'16 Neris 20-Bits IP Map	655360 x 522429 x 24 x 7	1.04×10^{-6}	10	.0262	.1425	6,381	.9659	.1478	23,383,989
UGR'16 Neris 24-Bits IP Map	3865526 x 848382 x 24 x 7	1.09×10^{-7}	7	.1464	.3008	2,369	.9822	.1034	21,847,564
UGR'16 Neris 4 Character IP Hash Map	65536 x 65536 x 24 x 7	8.04×10^{-5}	10	.0292	.1246	8,381	.9447	.2065	23,189,409
UGR'16 Neris 5 Character IP Hash Map	1048487 x 663889 x 24 x 7	5.16×10^{-7}	7	.0330	.1599	5,781	.9732	.1262	23,250,847
UGR'16 Neris 6 Character IP Hash Map	7477572 x 1019015 x 24 x 7	4.72×10^{-8}	6	.2813	.4315	495	.9857	.0922	19,481,318
UGR'16 Spam E-Mail	55287 x 65536 x 24 x 7	2.66×10^{-5}	20	.3814	.2165	2,495	.9791	.1220	1,909,544
PaySim Credit Card	100 x 5 x 24 x 7 x 100 x 100	9.00×10^{-6}	25	.6826	.4387	4,391	.9998	.0058	1,224

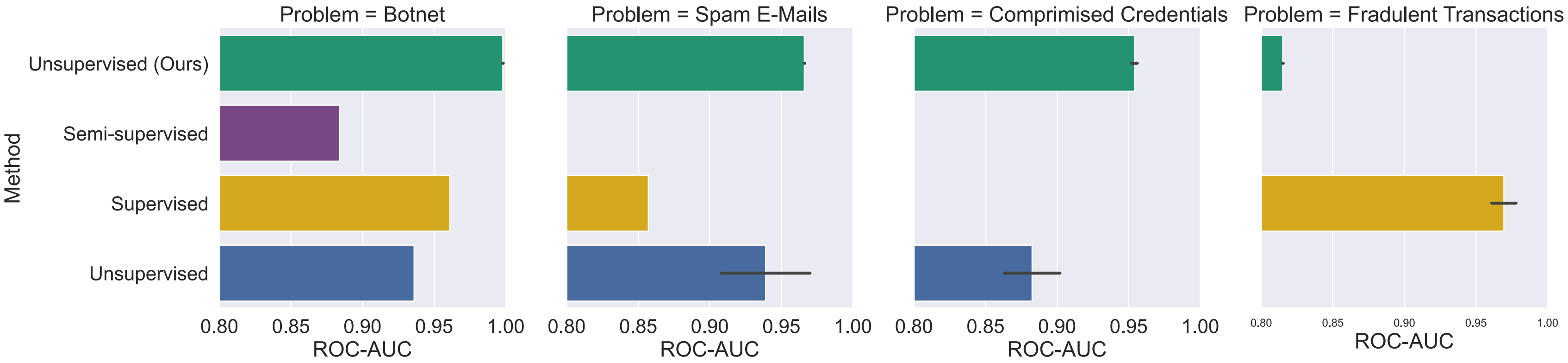
1) User – Source – Destination - status
2) User – Source – Destination – Hour - status
3) User – Source – Destination – Hour – Day - status

Adding temporal information to the tensor makes the model more certain

Performance

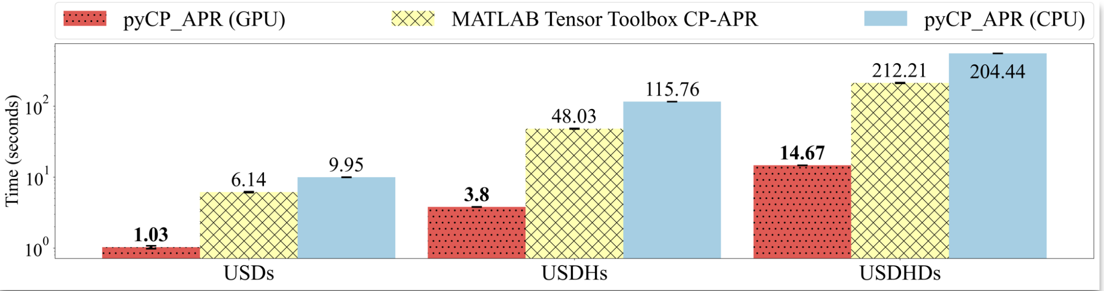






Public Dataset & Software

csr.lanl.gov/data/2017/



Chapter 1

Unified Host and Network Data Set

Melissa J. M. Turcotte*,‡, Alexander D. Kent* and Curtis Hash†

*Los Alamos National Laboratory, Los Alamos, NM 87545, USA
†Ernst & Young, New Mexico, USA
‡mturcotte@lanl.gov

The lack of data sets derived from operational enterprise networks continues to be a critical deficiency in the cyber-security research community. Unfortunately, releasing viable data sets to the larger community is challenging for a number of reasons, primarily the difficulty of balancing security and privacy concerns against the fidelity and utility of the data. This chapter discusses the importance of cyber-security research data sets and introduces a large data set derived from the operational network environment at Los Alamos National Laboratory (LANL). The hope is that this data set and associated discussion will act as a catalyst for both new research in cyber-security as well as motivation for other organisations to release similar data sets to the community.

GitHub

github.com/lanl/pyCP_APR

Data Privacy

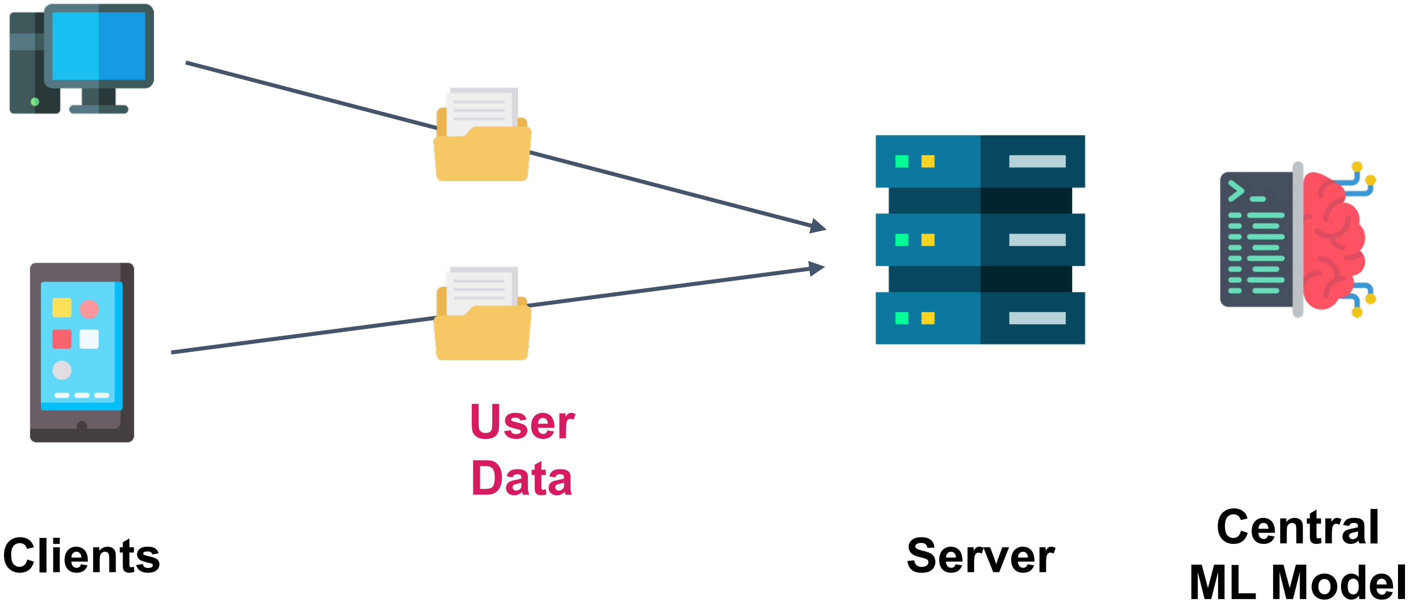
Motivation
ML and Recommender Systems

- ML has grown in popularity, including recommender systems
- Books, music, merchandise in e-commerce
- Companies gain customer loyalty and increase sales [16,17]

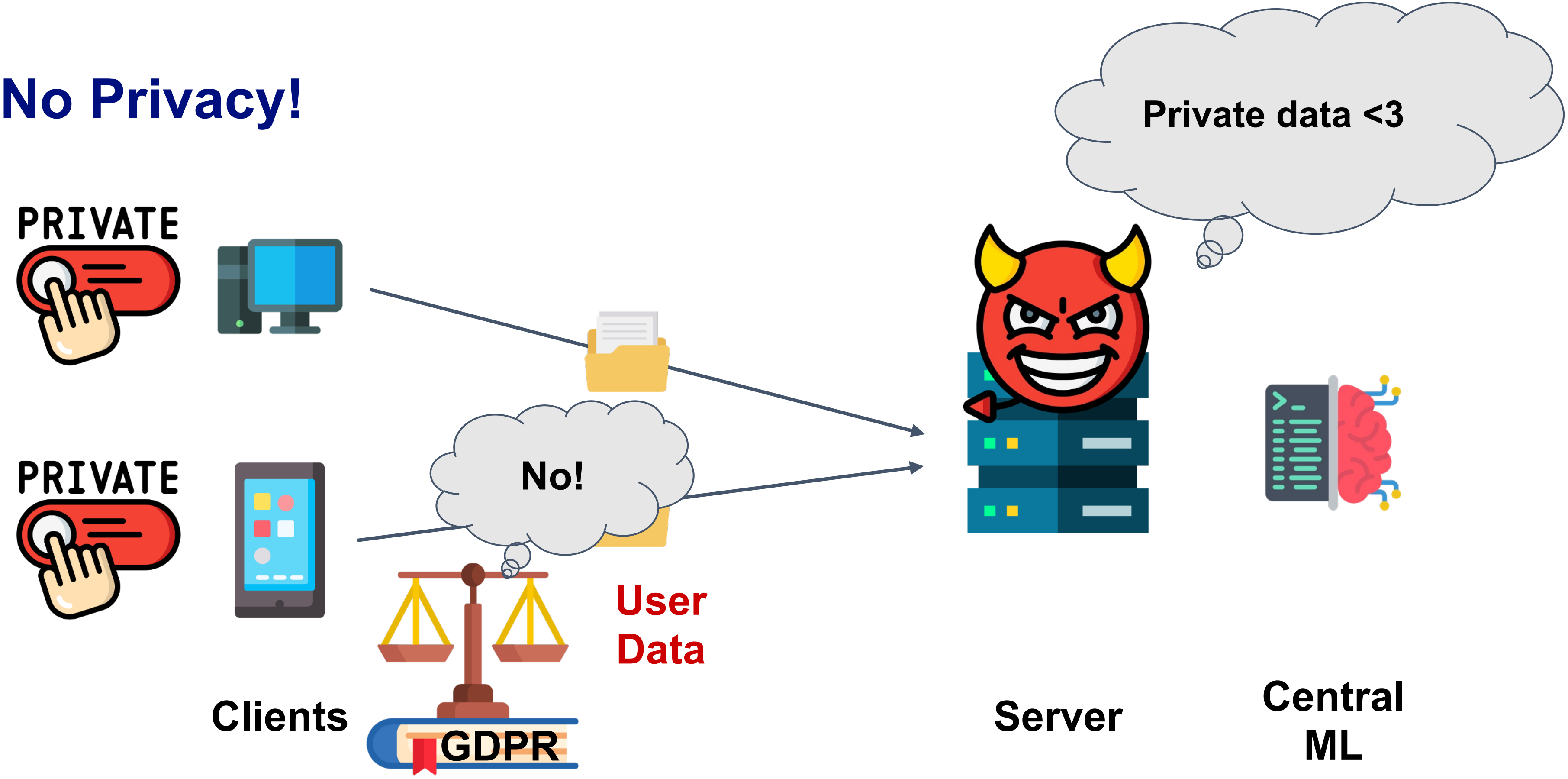





Traditional Collaborative Filtering

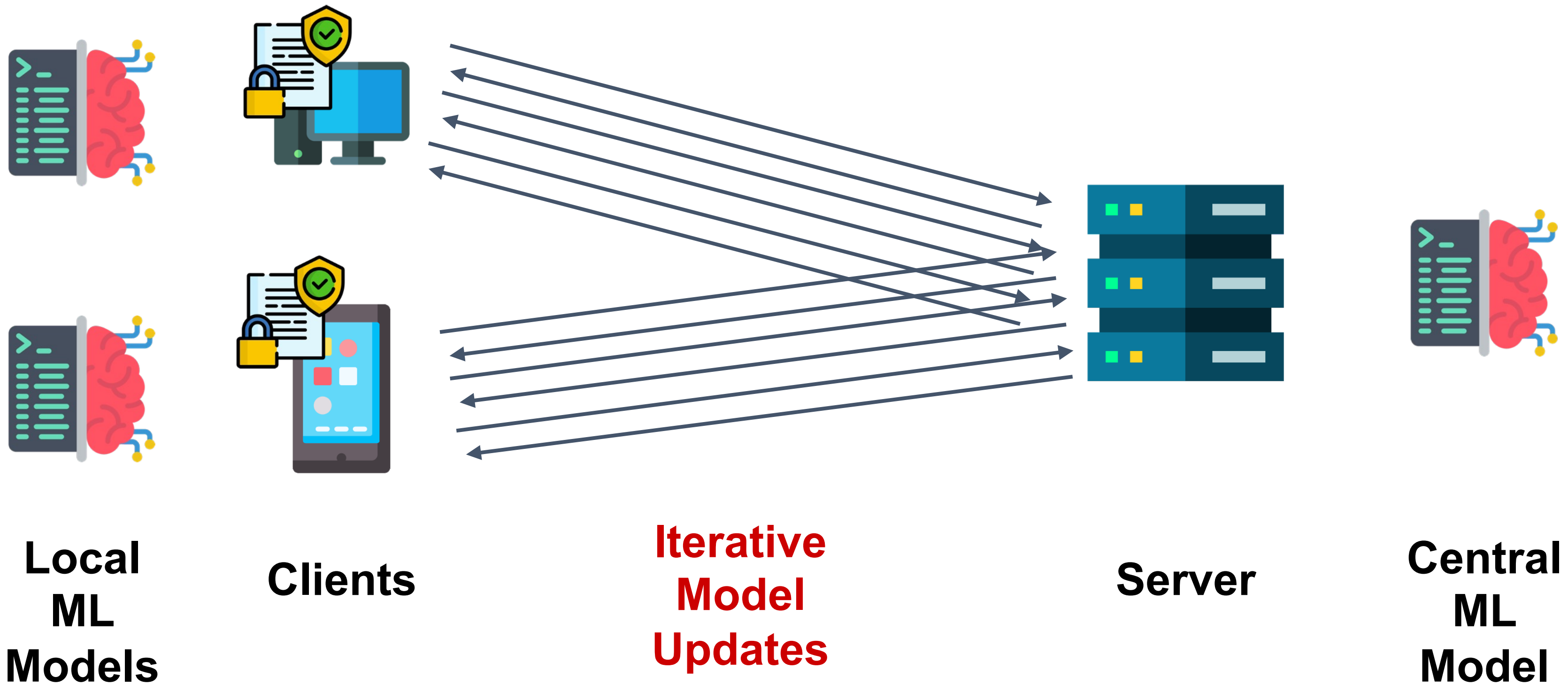


No Privacy!

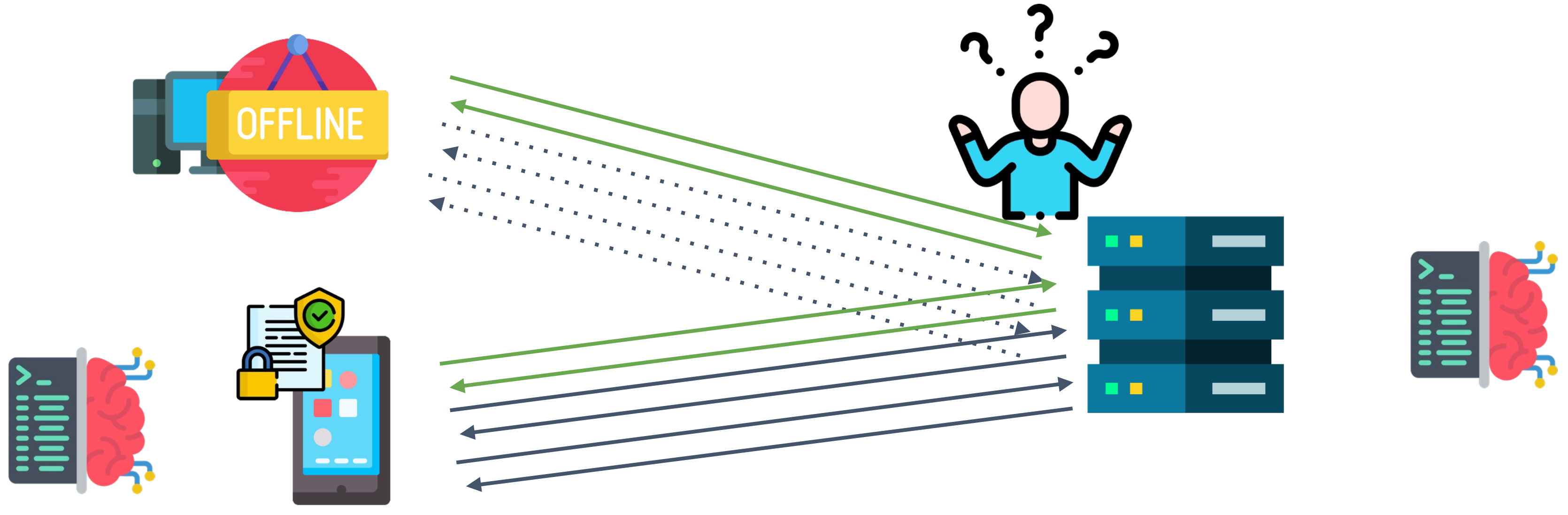


[18,19]

Yes Privacy! Federated Collaborative Filtering[20,21]



Problems: What if someone leaves?[22]



Local ML Models

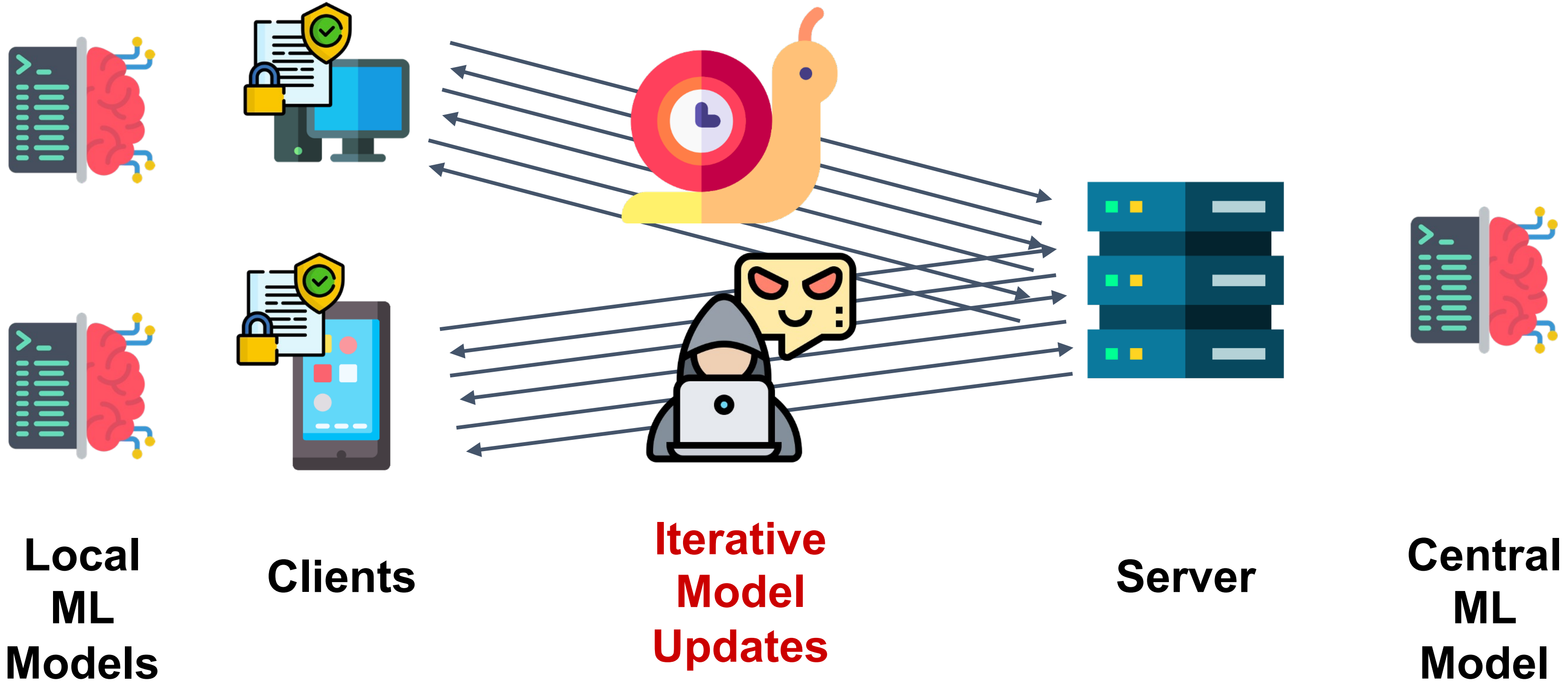
Clients

Iterative Model Updates

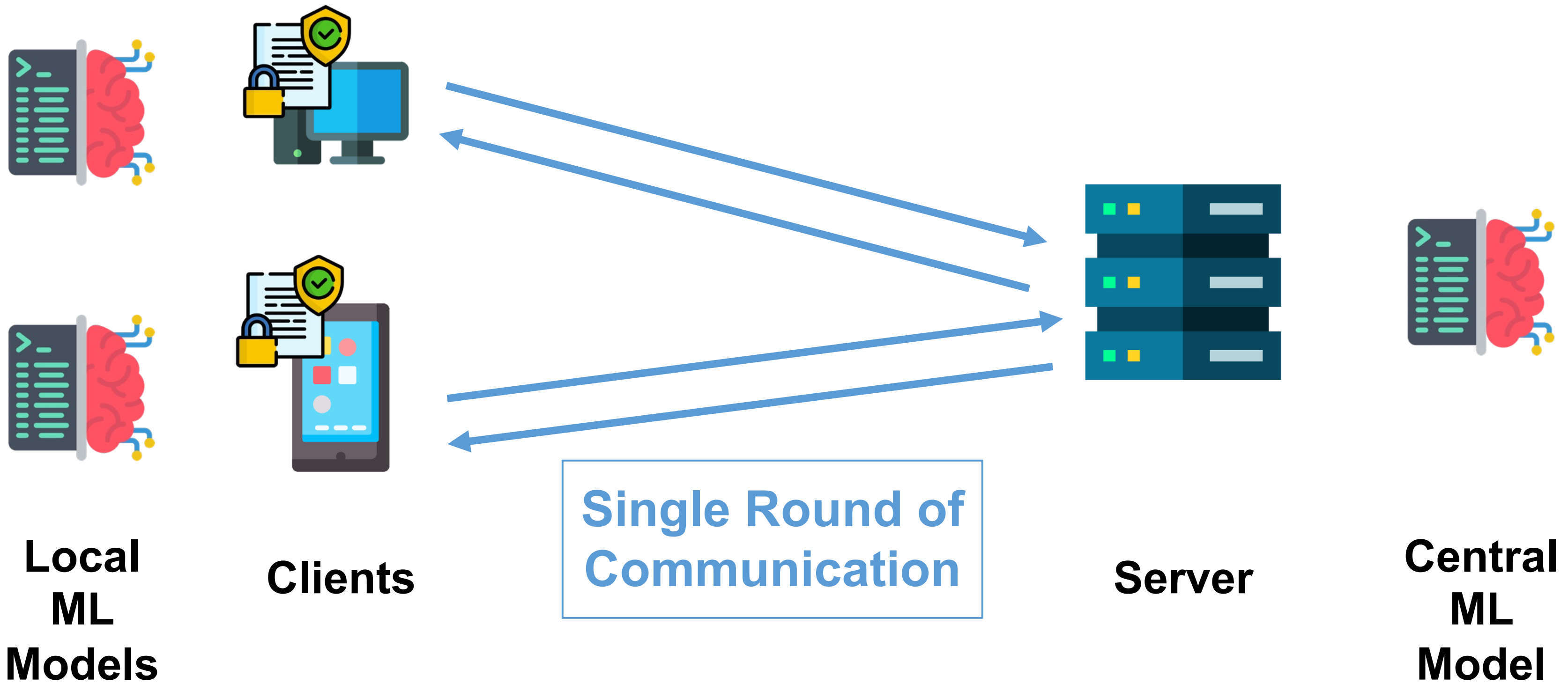
Server

Central ML Model

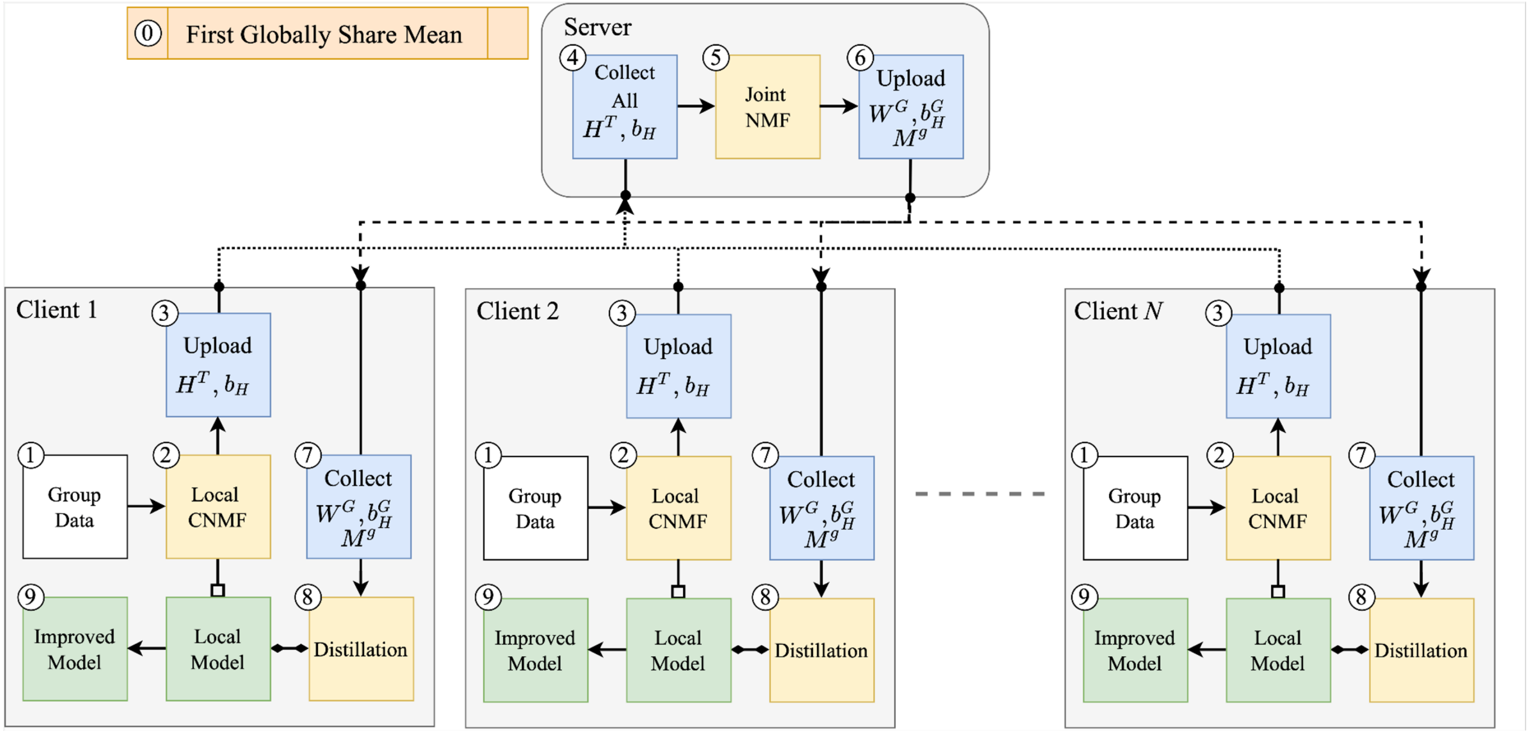
Problems: Too many to fit in this title [23, 24]



Solution = **One-shot** Federated Collaborative Filtering

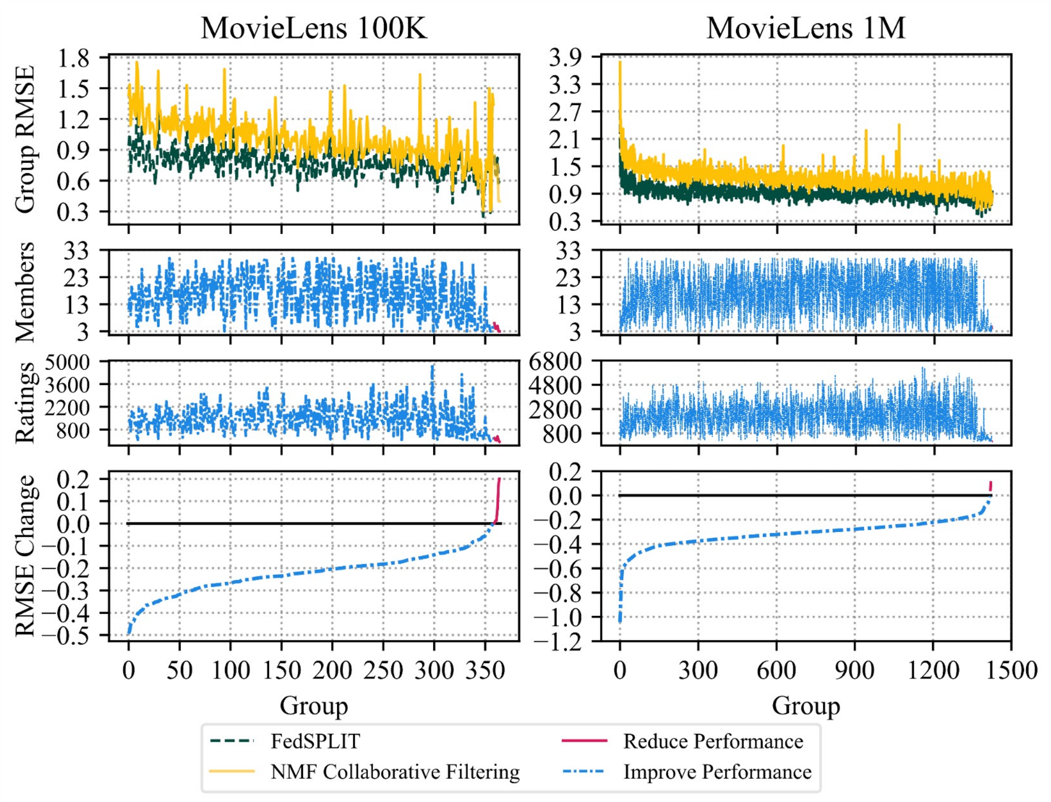


Method Summary



Performance

Dataset	Num. Groups	Num. Improved	RMSE Improve	RMSE Reduce	Members-RMSE Pearson	Ratings-RMSE Pearson
MovieLens 100K	365	359	-0.22 (± 0.008)	0.07 (± 0.092)	-0.06	-0.11
MovieLens 1M	1,422	1,420	-0.31 (± 0.005)	0.07 (± 0.381)	-0.12	-0.16



Performance

			RMSE Results on Datasets	
Method	**Reference**	**# of Comm. Rounds**	**MovieLens 100K**	**MovieLens 1M**
Standard CF				
Non-Private/Standard CF (CNMF)	-	-	**0.71 ($\pm$ 0.006)**	**0.76 ($\pm$ 0.006)**
Groups' Local CF (CNMF)	-	-	1.00 ($\pm$ 0.022)	1.22 ($\pm$ 0.013)
Iterative Federated Baselines				
CLFM-VFL	[9]	1–175	~3.80 (*NA*) – ~1.00 (*NA*)	*NA*
FedRec (SVD++)	[4]	10–100	~0.95 (*NA*) – **0.92 ($\pm$ 0.005)**	~0.90 (*NA*) – **0.84 ($\pm$ 0.001)**
Homomorphic Encryption	[3]	10–100	~3.40 (*NA*) – 1.03 (*NA*)	*NA*
FCMF	[7]	50	0.95 ($\pm$ 0.005)	0.88 ($\pm$ 0.001)
FedRecon	[5]	500	*NA*	0.90 (*NA*)
FedGNN	[6]	*NA* ($>$ 1)	**0.92 (*NA*)**	**0.84 (*NA*)**
Two-order FedMMF	[8]	*NA* ($>$ 1)	**0.92 ($\pm$ 0.003)**	*NA*
FedMF	[2, 6]	*NA* ($>$ 1)	0.94 (*NA*)	0.87 (*NA*)
FCF	[1, 6]	*NA* ($>$ 1)	0.95 (*NA*)	0.87 (*NA*)
One-shot Federated CF				
FedSPLIT	(ours)	**1**	**0.78 ($\pm$ 0.016)**	**0.91 ($\pm$ 0.016)**

[1] Muhammad Ammad-Ud-Din, Elena Ivannikova, Suleiman A Khan, Were Oyomno, Qiang Fu, Kuan Eeik Tan, and Adrian Flanagan. 2019. Federated collaborative filtering for privacy-preserving personalized recommendation system. arXiv preprint arXiv:1901.09888 (2019).

[2] Di Chai, Leye Wang, Kai Chen, and Qiang Yang. 2020. Secure federated matrix factorization. IEEE Intelligent Systems 36, 5 (2020), 11–20.

[3] Yongjie Du, Deyun Zhou, Yu Xie, Jiao Shi, and Maoguo Gong. 2021. Federated matrix factorization for privacy-preserving recommender systems. Applied Soft Computing 111 (2021), 107700.

[4] Guanyu Lin, Feng Liang, Weike Pan, and Zhong Ming. 2020. Fedrec: Federated recommendation with explicit feedback. IEEE Intelligent Systems 36, 5 (2020), 21–30.

[5] K. Singhal, Hakim Sidahmed, Zachary Garrett, Shanshan Wu, Keith Rush, and Sushant Prakash. 2021. Federated Reconstruction: Partially Local Federated Learning. ArXiv abs/2102.03448 (2021).

[6] Chuhan Wu, Fangzhao Wu, Yang Cao, Yongfeng Huang, and Xing Xie. 2021. Fedgnn: Federated graph neural network for privacy-preserving recommendation. arXiv preprint arXiv:2102.04925 (2021).

[7] Enyue Yang, Yunfeng Huang, Feng Liang, Weike Pan, and Zhong Ming. 2021. FCMF: Federated collective matrix factorization for heterogeneous collaborative filtering. Knowledge-Based Systems 220 (2021), 106946.

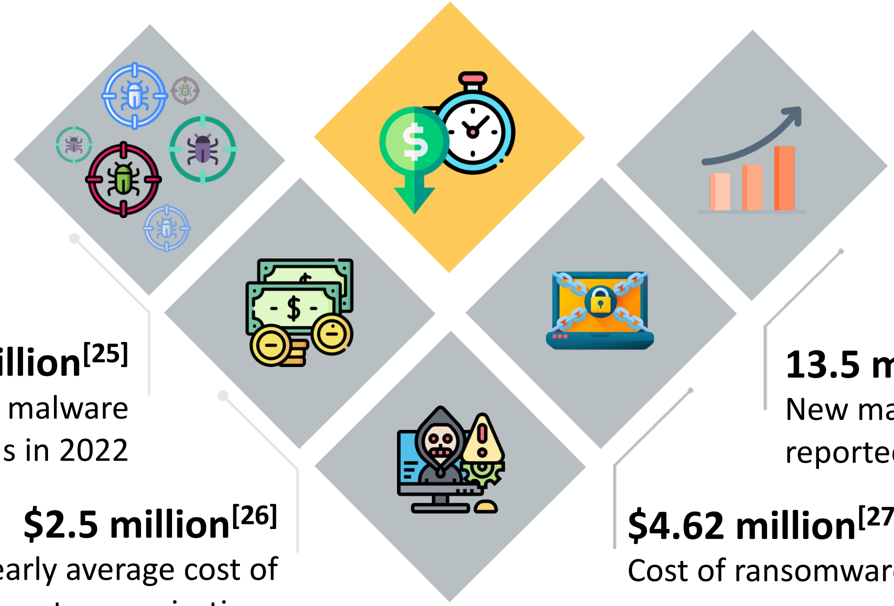
[8] Liu Yang, Ben Tan, Bo Liu, Vincent W Zheng, Kai Chen, and Qiang Yang. 2021. Practical and Secure Federated Recommendation with Personalized Masks. arXiv preprint arXiv:2109.02464 (2021).

[9] JianFei Zhang and YuChen Jiang. 2021. A vertical federation recommendation method based on clustering and latent factor model. In International Conference on Electronic Information Engineering and Computer Science (EIECS). 362–366.

Malware

Malware is a problem!

Save Time & Reduce Cost[30]
ML can reduce response and recovery time



1.3 billion[25]
Total reported malware malware specimens in 2022

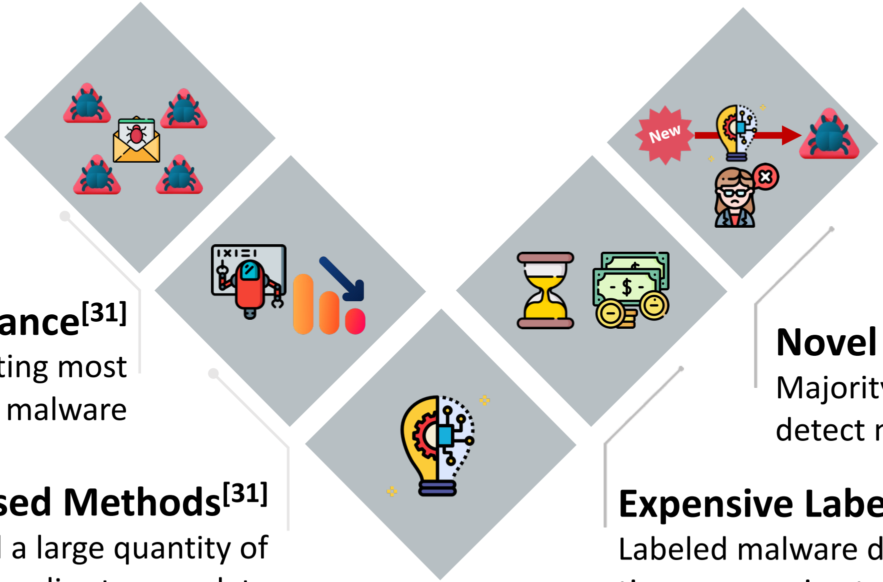
13.5 million[25]
New malware specimens reported monthly

$2.5 million[26]
Yearly average cost of malware to organizations

$4.62 million[27]
Cost of ransomware breach

Growing Sophistication[28,29]
Capabilities of malware in the wild grow

Machine learning can help, but…



Class Imbalance[31]
Many solutions focus on detecting most prominent malware

Popular Supervised Methods[31]
Supervised models need a large quantity of labeled data, poorly generalize to new data

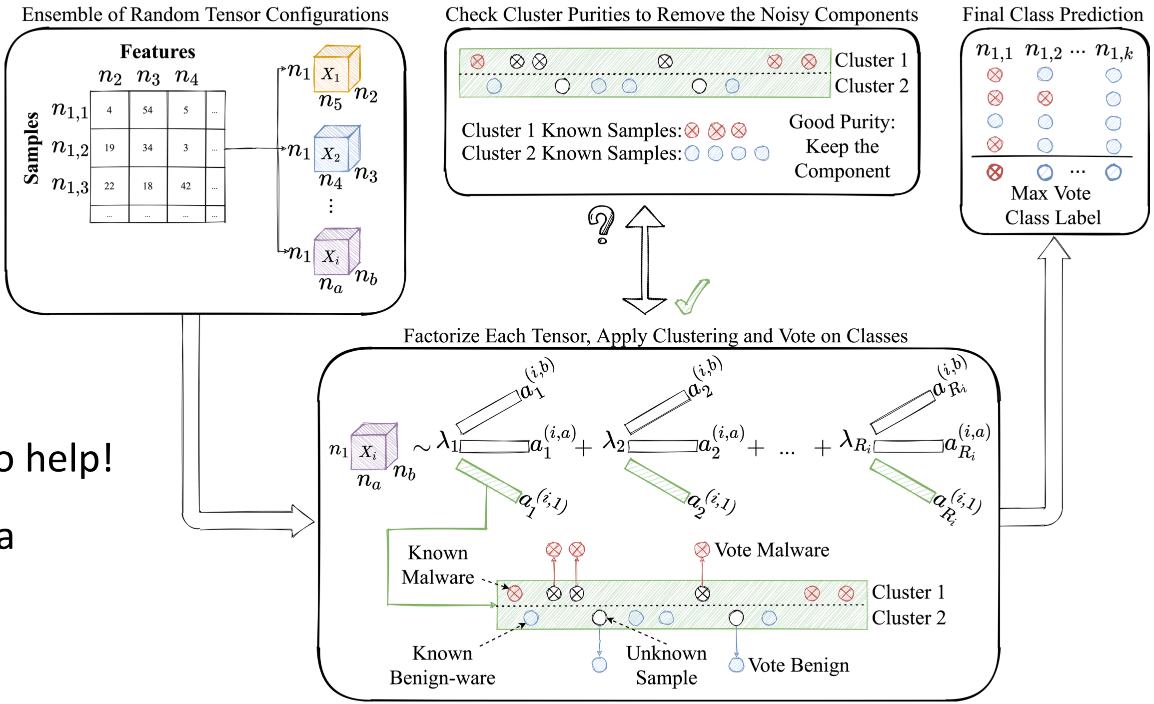
Semi-supervised Methods[31]
The research community had not widely explored the application of semi- supervised learning to Windows malware detection

Expensive Labels[31]
Labeled malware data is expensive and time-consuming to obtain

Novel Malware[31]
Majority of the solutions can not detect novel malware

Random Forest of Tensors (RFoT)

Bulk Semi-supervised Malware Family Classification

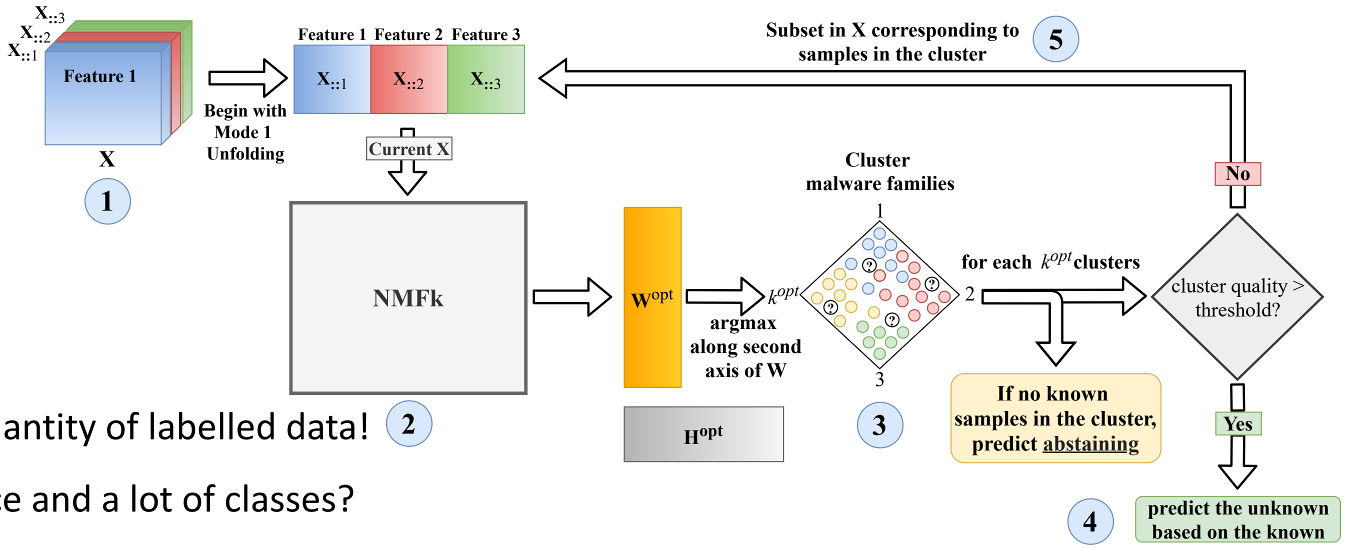


- Tensors are useful!
- Semi-supervised methods do help!
- Low quantity of labelled data

– no problem!

HNFMk Classifier

Bulk Semi-supervised Malware Family Classification



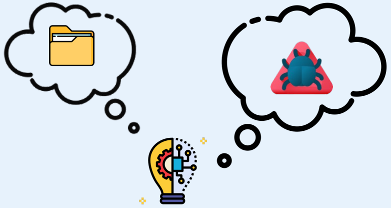
- Works well with low quantity of labelled data!
- Extreme class imbalance and a lot of classes?

  - no problem!
- **Somewhat detects novel malware**
- **World record 2.9k malware families**

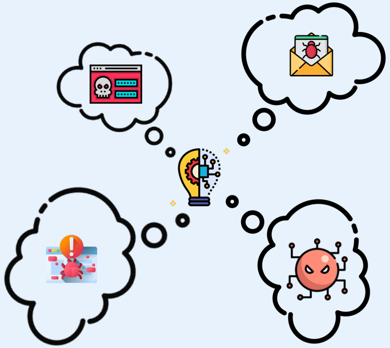
Address the shortcomings

Real-time semi-supervised malware characterization

Malware Detection



Malware Family Classification



Identification of Novel Families

Malware-DNA ✓

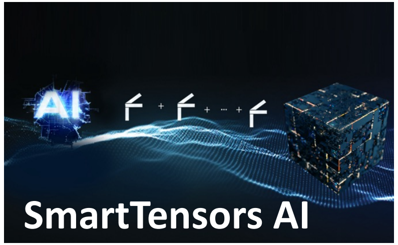
Malware-DNA ✓

Malware-DNA ✓

MalwareDNA[Patent: 10]

- Consider **software as genomic DNA**, and **malware as mutations in DNA** 

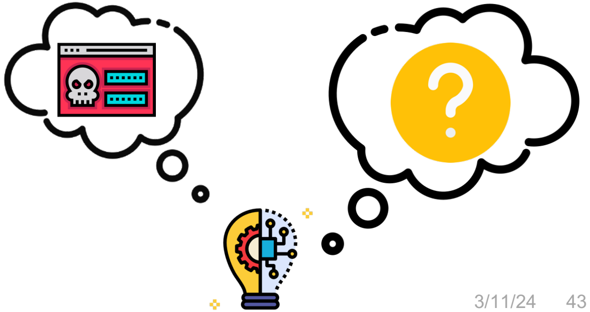
- Discover the hidden **hierarchical structure of malware** in the genome
- Extract identifying malware signatures using **tensor decomposition**

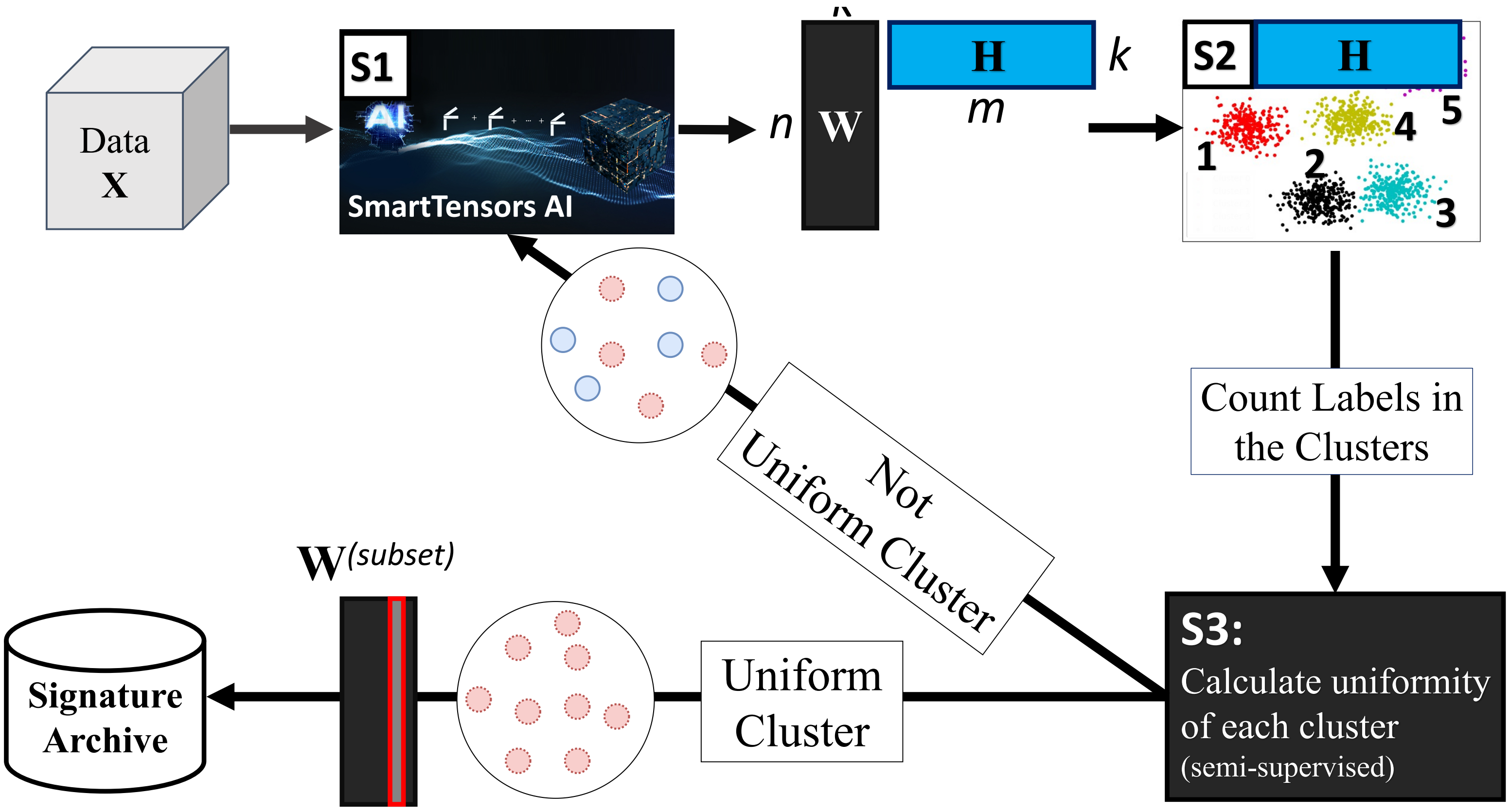


[2,3]

Reject-option[32]

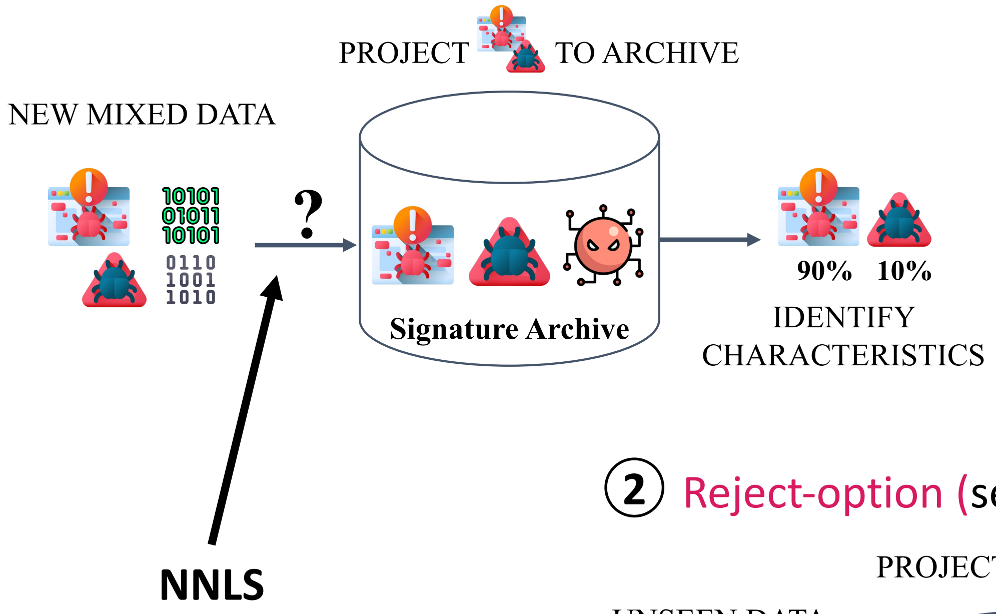
– Detects novel malware families



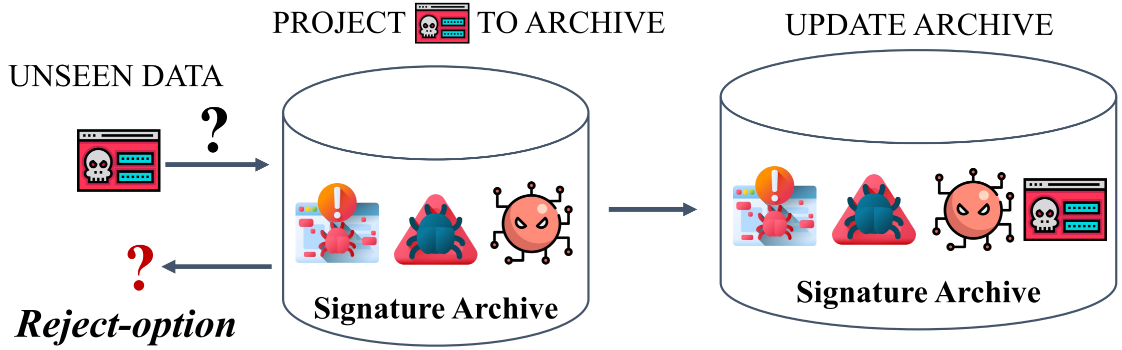


Data
X
S1
AI
SmartTensors AI
n
W
H
k
m
S2
H
1
2
3
4
5
Count Labels in the Clusters
Not Uniform Cluster
S3:
Calculate uniformity of each cluster
(semi-supervised)
Uniform Cluster
W(subset)
Signature Archive

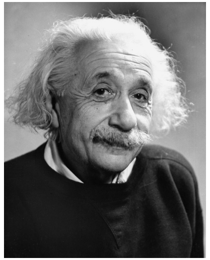
① Identifying new Samples



② Reject-option (selective classification)



Selective Classification (Reject-option)



Self-awareness for ML model to know when it does not know

"the more I learn, the more I realize how much I do not know." - Albert Einstein

"If knowledge is power, knowing what we do not know is wisdom" [32, 33]

Withdraw from making a decision for uncertain predictions using confidence

- Useful when a mistake is expensive

- Enable knowledge discovery: **novel malware families**

Distribute the Computation with HPC:
Scaling the experiments

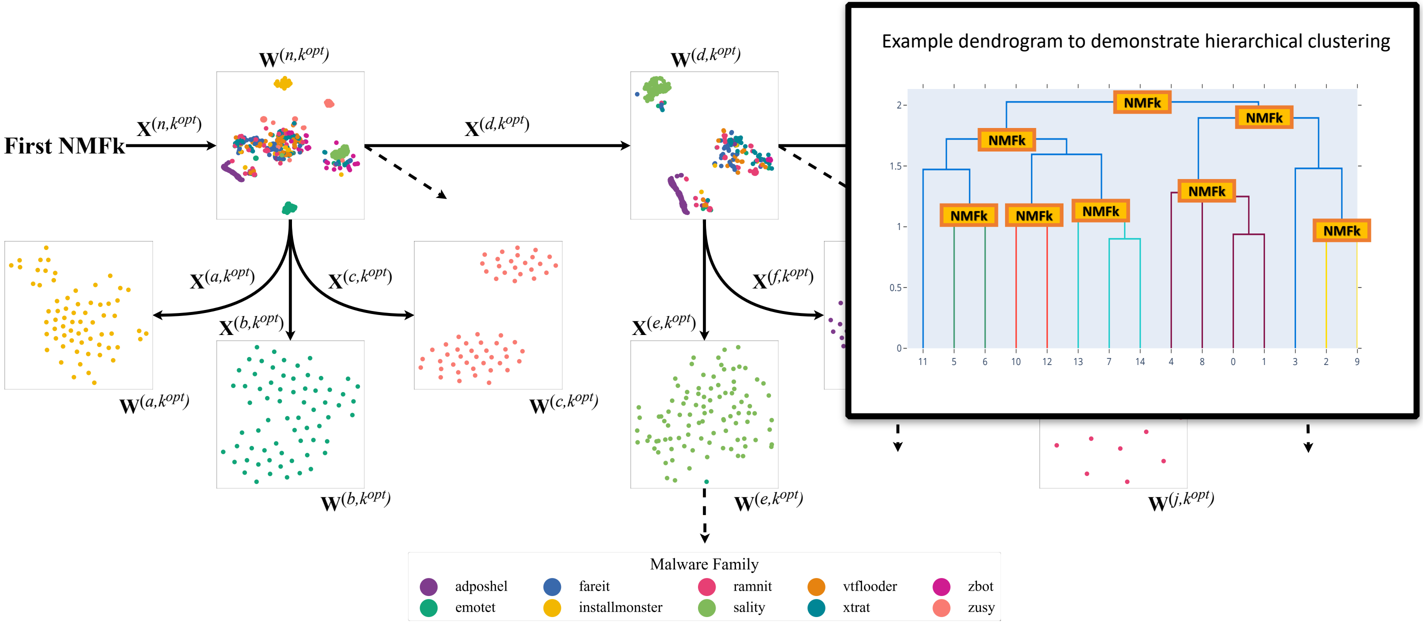
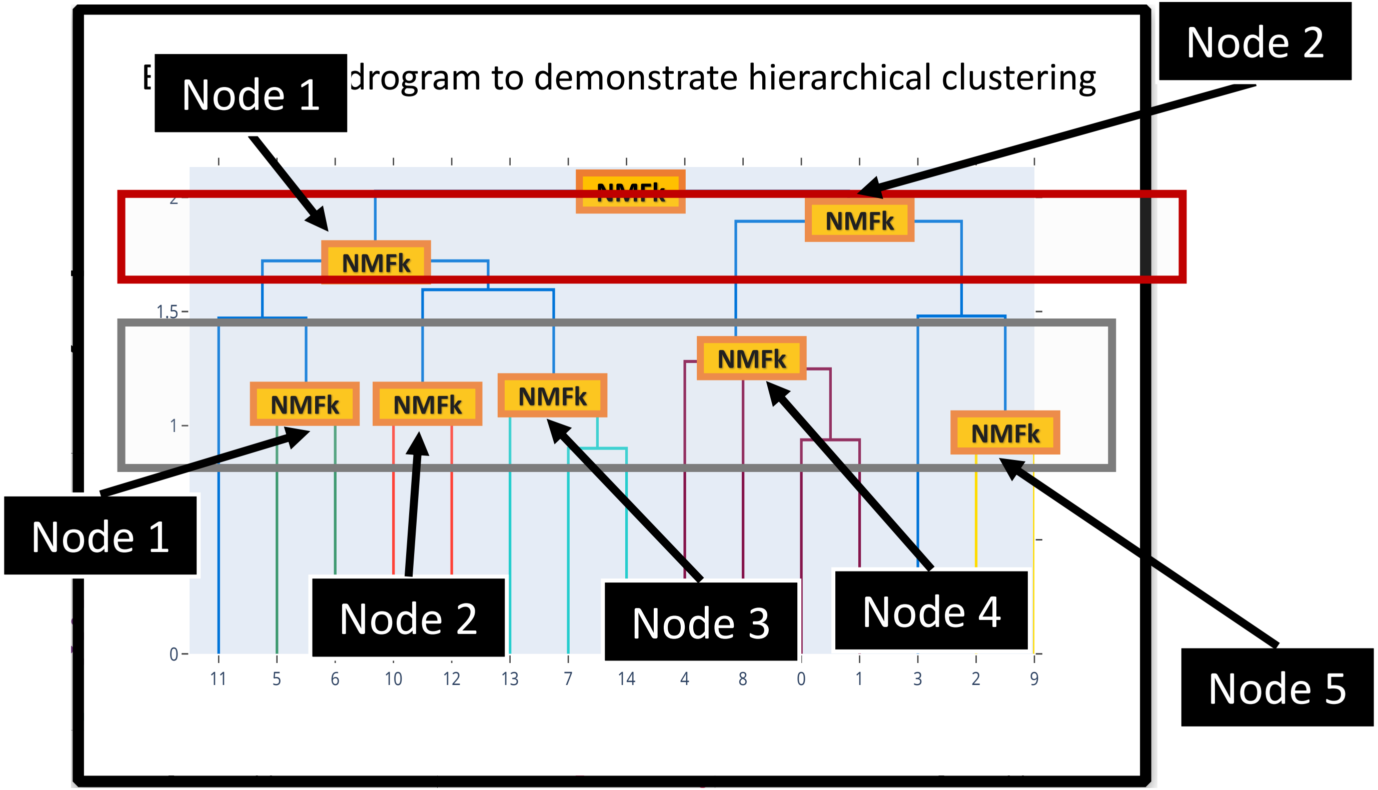


Fig 2. Demonstration of the hierarchical application of NMFk and clustering of malware.

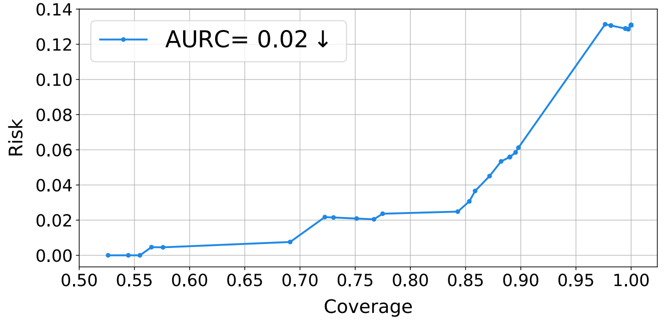
Distribute the Computation with HPC:
Scaling the experiments



Experiments

Using the EMBER-2018[34] dataset, we randomly sample **10,000 benign-ware, and malware specimens** from families:

- **Ramnit**, **Adposhel**, **Emotet**, **zusy**
- Select **Ramnit** to represent a novel family.



We achieve AURC* score of 0.02↓:

- **At ~84% coverage: ~0.975 F1**
- **Identify ~100% of Ramnit as novel**
- Surpasses supervised and semi-supervised baselines

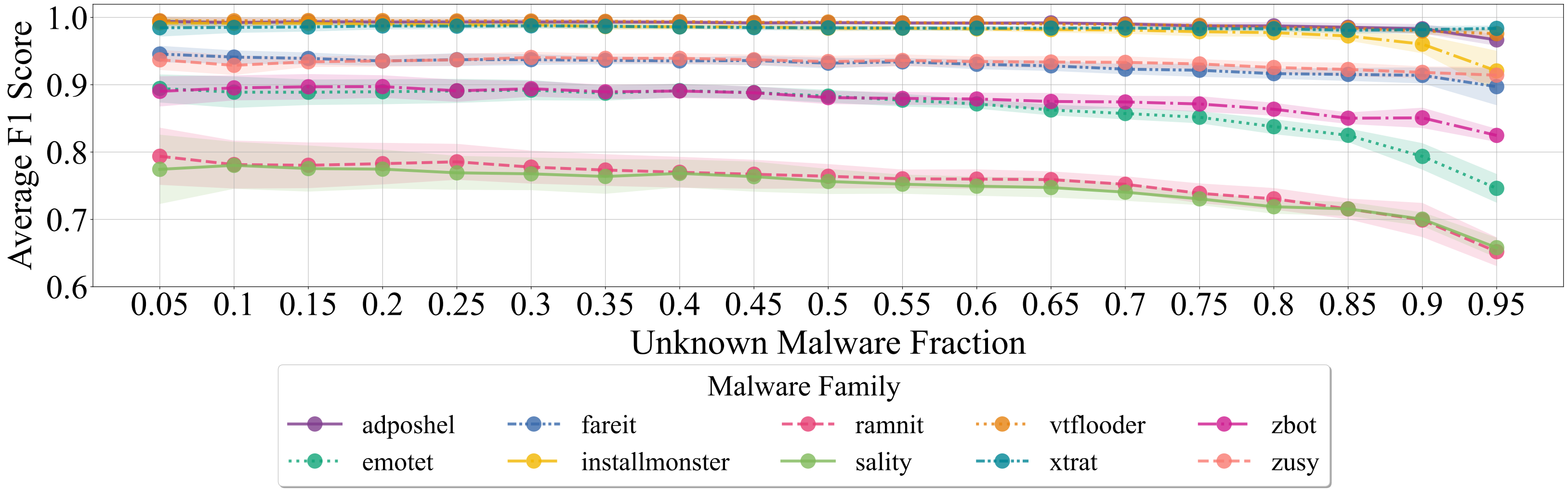
TABLE I
PERFORMANCE OF MALWAREDNA COMPARED TO BASELINES. REJECTION SEEN PROVIDES THE FALSE REJECTION PREDICTIONS FOR THE SAMPLES THAT BELONGS TO KNOWN CLASSES. REJECTION NOVEL IS THE TRUE REJECTION PREDICTIONS FOR THE SAMPLES THAT BELONGS TO A NOVEL MALWARE FAMILY. XGBOOST+SELFTRAIN AND LIGHTGBM+SELFTRAIN ACHIEVE AURC SCORE OF 0.654 AND 0.651.

Model	F1	Precision	Recall	Rejection Seen	Rejection Novel
MalwareDNA (ours)	**0.975**	**0.975**	**0.977**	15.70 %	**100.00 %**
XGBoost	0.416	0.699	0.510	NA	NA
LightGBM	0.297	0.749	0.338	NA	NA
XGBoost+SelfTrain	0.096	0.258	0.108	4.34 %	18.09 %
LightGBM+SelfTrain	0.096	0.078	0.197	**2.89 %**	17.14 %

**Area Under the Curve of Risk-Coverage[32]*

Los Alamos NATIONAL LABORATORY

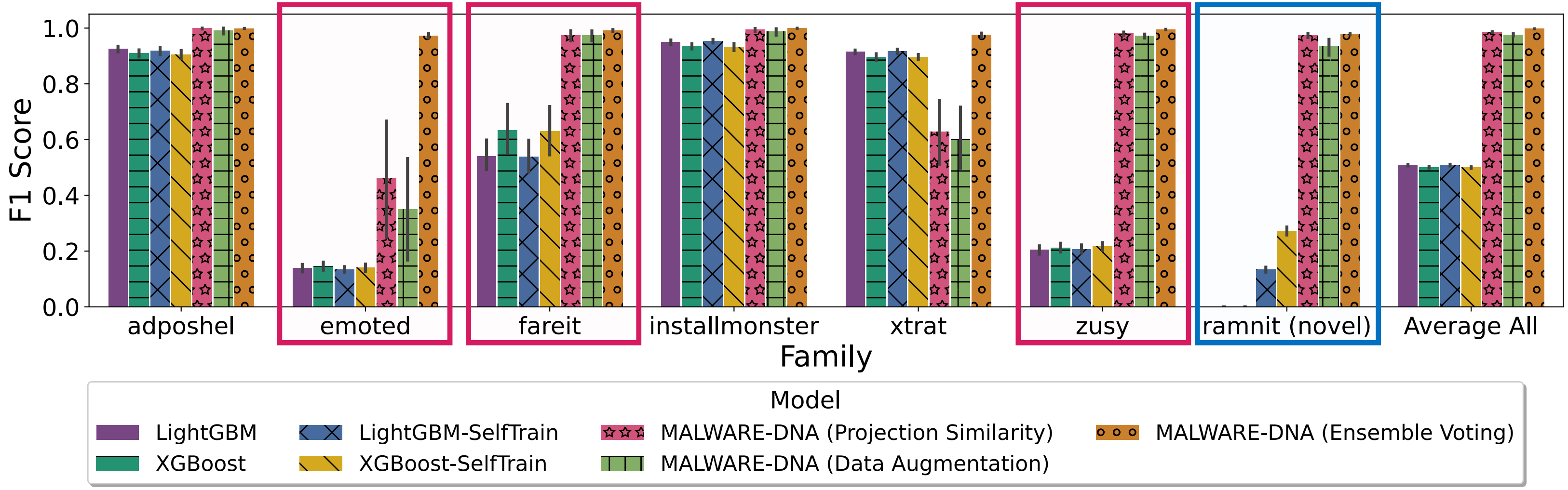
Experiments – Quantity of Labelled Data



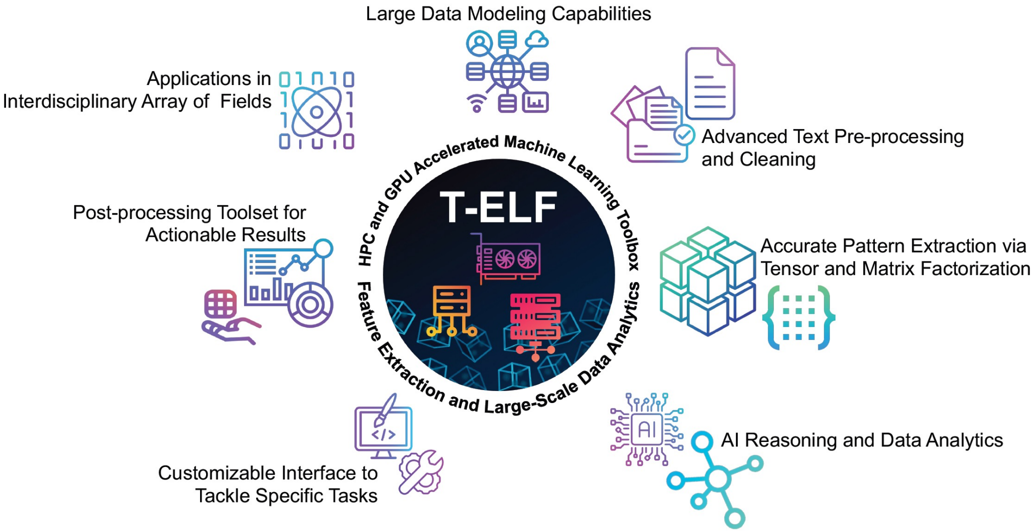
Experiments – Class Imbalance

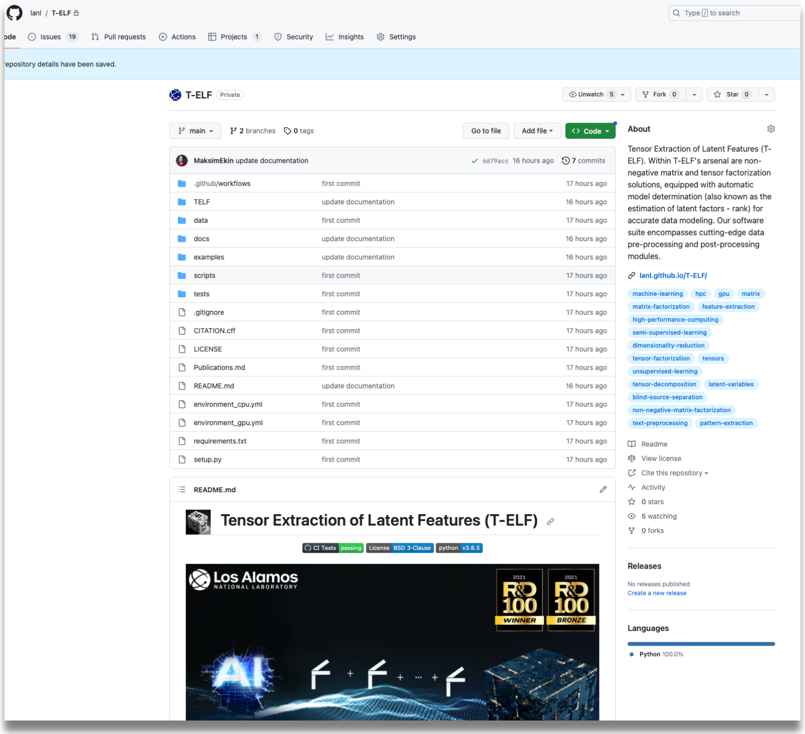
TABLE I
DISTRIBUTION OF MALWARE FAMILIES IN TRAINING AND TESTING SETS REPORTED WITH MEAN NUMBER OF INSTANCES AND THE CONFIDENCE INTERVAL OVER 10 SAMPLE TRIALS.

Malware Family	Training Set	Testing Set
xtrat	4853.9 (+- 12.6)	543.1 (+- 12.2)
installmonster	3750.3 (+- 10.2)	416.7 (+- 11.5)
adposhel	3216.4 (+- 6.6)	361.6 (+- 5.6)
zusy **(rare family)**	638.0 (+- 7.0)	67.0 (+- 6.9)
emoted **(rare family)**	232.2 (+- 3.8)	25.8 (+- 3.8)
farait **(rare family)**	97.2 (+- 1.9)	11.8 (+- 1.4)
ramnit **(novel family)**	0.0	1029.0 (+- 2.4)



Public Code:





github.com/lanl/T-ELF

Los Alamos NATIONAL LABORATORY

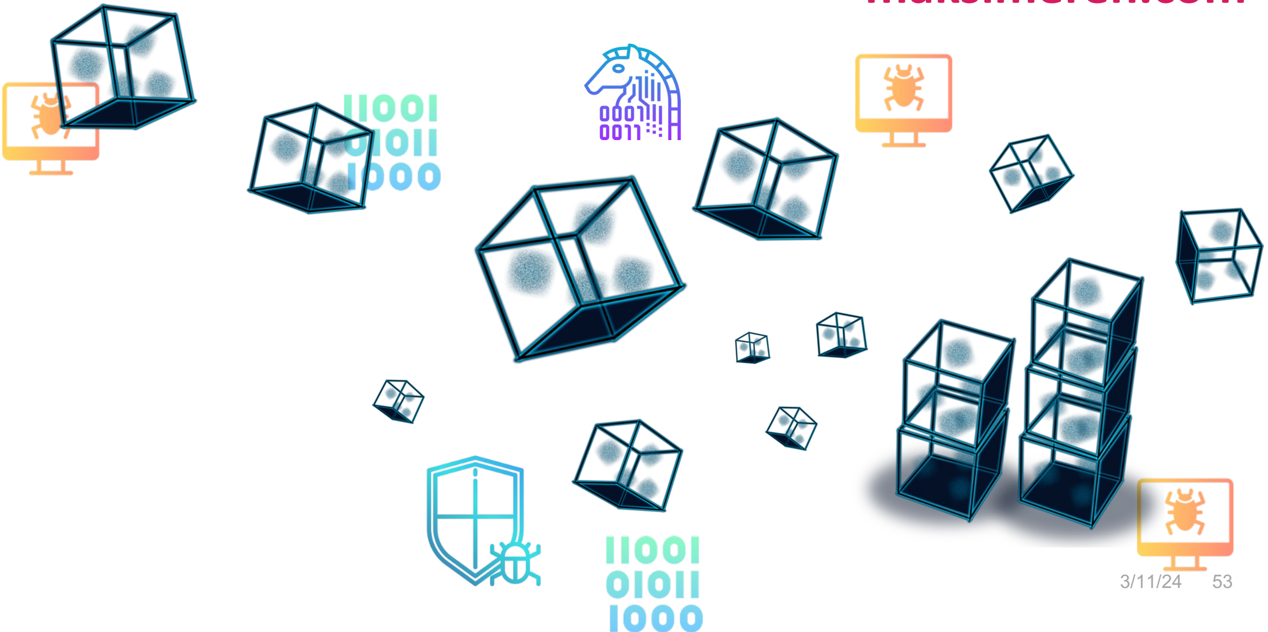
Thank you!

Questions?

Contact: maksim@lanl.gov

maksimeren.com

smart-tensors.lanl.gov



References

This slides has been designed using resources from Flaticon.com

[1] Eren, M.E., Moore, J.S., and Boian, A.S.. Multi-Dimensional Anomalous Entity Detection via Poisson Tensor Factorization. In ISI ’20: Proceedings of the 13th IEEE International Conference on Intelligence and Security Informatics, Nov. 9-10, 2020, Virtual Event, USA., 6 pages. DOI: 10.1109/ISI49825.2020.9280524

[2] Boian Alexandrov, Velimir Vesselinov, and Kim Orskov Rasmussen. SmartTensors Unsupervised AI platform for Big-Data Analytics. Technical Report, Los Alamos National Lab. (LANL), Los Alamos, NM (United States), 2021. LA-UR-21-25064.

[3] B. Alexandrov, L. Alexandrov, and V. S. et al., “Source identification by non-negative matrix factorization combined with semi-supervised clustering,” US Patent S10,776,718, 2020.

[4] Bhandary, P., Adetunji, I., Kiendrebeogo, A., Vieson, C., Joyce, R.J., Eren, M.E., and Nicholas, C.. Malware Antivirus Scan Pattern Mining via Tensor Decomposition. MTEM ’22: Malware Technical Exchange Meeting, July 26-28, 2021, Massachusetts Institute of Technology, Cambridge, MA, USA.

[5] Eren, M.E., Nicholas, C., McDonald, R., and Hamer, C.. Random Forest of Tensors. MTEM ’21: Malware Technical Exchange Meeting, July 13-15, 2021, Sandia National Laboratories, Virtual Event, USA.

[6] Most, A., Eren, M.E., Alexandrov, B., and Lawrence, N.. Electrical Grid Anomaly Detection via Tensor Decomposition. In MILCOM ’23: IEEE Military Communications Conference, Articial Intelligence for Cyber Workshop, Oct. 30 - Nov. 3, 2023, Boston, Massachusetts, USA. 7 pages.

[7] Eren, M.E., Bhattarai, M., Solovyev, N., Richards, L., Yus, R., Nicholas, C., and Alexandrov, B.. One-Shot Federated Group Collaborative Filtering. In ICMLA ’22: 21st IEEE International Conference on Machine Learning and Applications, Dec. 12-15, 2022, Nassau, The Bahamas. 6 pages. Awarded Best M.S. Research at 2023 UMBC CSEE Research Day. DOI: 10.1109/ICMLA55696.2022.00107

[8] Eren, M.E., Rasmussen, K.O., Nicholas, C., and Alexandrov, B.S.. Malware-DNA: Machine Learning for Malware Analysis that Treats Malware as Mutations in the Software Genome. MTEM ’23: Malware Technical Exchange Meeting, July 25-27, 2023, Lawrence Livermore National Laboratory, Livermore, California, USA.

[9] Eren, M.E., Bhattarai, M., Joyce, R.J., Raff, E., Nicholas, C. and Alexandrov, B.. 2023. Semi-supervised Classification of Malware Families Under Extreme Class Imbalance via Hierarchical Non-Negative Matrix Factorization with Automatic Model Selection. TOPS: ACM Transactions on Privacy and Security, 26 pages. DOI: 10.1145/3624567

[10] Eren, M.E., Bhattarai, M., Nicholas, C., Rasmussen K., and Alexandrov, B. (2023), Data Identification and Classification Method, Apparatus, and System, US, Provisional Patent 63/472,188.

[11] Eren, M.E., Bhattarai, M., Solovyev, N., Richards, L., Yus, R., Nicholas, C., and Alexandrov, B.. MalwareDNA: Simultaneous Classification of Malware, Malware Families, and Novel Malware. In ISI ’23: 20th Annual IEEE International Conference on Intelligence and Security Informatics, Oct. 2-3, 2023, Charlotte, North Carolina USA. 3 pages.

[12] 2020. Cyber Espionage Report. Technical Report. Verizon. Retrieved from https://www.verizon.com/business/resources/reports/cyber- espionage- report/.

[13] 2019. Cost of a Data Breach Report. Technical Report. IBM. Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture- 2019- Cost- of- Cybercrime- Study- Final.pdf .

[14] 2020. Data Breach Investigations Report 2020. Technical Report. Verizon. Retrieved from https://enterprise.verizon.com/resources/ reports/dbir/.

[15] 2020. Mandiant Security Effectiveness Report. Technical Report. FireEye. Retrieved from https://www.accenture.com/_acnmedia/PDF- 96/Accenture- 2019- Cost- of- Cybercrime- Study- Final.pdf.

[16] Pei-Yu Chen, Shin-yi Wu, and Jungsun Yoon. 2004. The impact of online recommendations and consumer feedback on sales. (2004).

[17] Linyuan Lü, Matúš Medo, Chi Ho Yeung, Yi-Cheng Zhang, Zi-Ke Zhang, and Tao Zhou. 2012. Recommender systems. Physics reports 519, 1 (2012), 1–49.

[18] Milano, S., Taddeo, M., & Floridi, L. (2020). Recommender systems and their ethical challenges. Ai & Society, 35(4), 957-967.

[19] Luciana Monteiro Krebs, Oscar Luis Alvarado Rodriguez, Pierre Dewitte, Jef Ausloos, David Geerts, Laurens Naudts, and Katrien Verbert. 2019. Tell me what you know: GDPR implications on designing transparency and accountability for news recommender systems. In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. 1–6.

[20] Muhammad Ammad-Ud-Din, Elena Ivannikova, Suleiman A Khan, Were Oyomno, Qiang Fu, Kuan Eeik Tan, and Adrian Flanagan. 2019. Federated collaborative filtering for privacy-preserving personalized recommendation system. arXiv preprint arXiv:1901.09888 (2019).

[21] Adrian Flanagan, Were Oyomno, Alexander Grigorievskiy, Kuan E Tan, Suleiman A Khan, and Muhammad Ammad-Ud-Din. 2020. Federated multi-view matrix factorization for personalized recommendations. In Joint European Conference on Machine Learning and Knowledge Discovery in Databases. 324–347.

References

[22] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. 2020. Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine 37, 3 (2020), 50–60.
[23] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. 2020. Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine 37, 3 (2020), 50–60.
[24] Neel Guha, Ameet S. Talwalkar, and Virginia Smith. 2019. One-Shot Federated Learning. ArXiv abs/1902.11175 (2019).
[25] The Independent IT Security Institute. Malware statistics & trends report: Av-test, Feb 2022.
[26] K. Bissell and L. Ponemon. The cost of cybercrime. Technical report, Accen- ture, Ponemon Institute, 2019.
[27] Cost of a data breach report. Technical report, IBM, 2019.
[28] State of malware report. Technical report, Malwarebytes Labs, February 2020.
[29] Data breach investigations report 2021. Technical report, Verizon, 2021.
[30] Cost of a data breach report. Technical report, IBM, 2019.
[31] Edward Raff and C. Nicholas. A survey of machine learning methods and challenges for windows malware classification. ArXiv, abs/2006.09271, 2020
[32] Zhang, X.-Y., Xie, G.-S., Li, X., Mei, T. & Liu, C.-L. A Survey on Learning to Reject. Proceedings of the IEEE (2023).
[33] A. Grant. (2021). Think Again: The Power Knowing What You Don't Know, Viking. [Online]. Available: https://www.amazon.com/Think-Again-Power- Knowing-What/dp/1984878107
[34] Anderson, Hyrum S., and Phil Roth. "Ember: an open dataset for training static PE malware machine learning models." arXiv preprint arXiv:1804.04637 (2018).
[35] Gilligan-Lee, Ciarán. "Causing trouble." New Scientist 246.3279 (2020): 32-35.
[36] Eren, M.E., Barron, R., Bhattarai, M., Wanna, S., Solovyev, N., Rasmussen, K., Alexandrov, B., and Nicholas, C.. Catch'em all: Classification of Rare, Prominent, and Novel Malware Families. In ISDFS '24: 12th IEEE International Symposium on Digital Forensics and Security (ISDFS), Apr. 29-30, 2024, San Antonio, Texas USA. 6 pages.
[37] Eren, M.E., Alexandrov, B., and Nicholas, C.. Classifying Malware Using Tensor Decomposition. Malware - Handbook of Prevention and Detection, Springer Nature. 2024.