Enhancing IoT Security: Intrusion Detection System Using Machine Learning for Cross-Environment Attack Identification

CSE509 : System Security Project Presentation

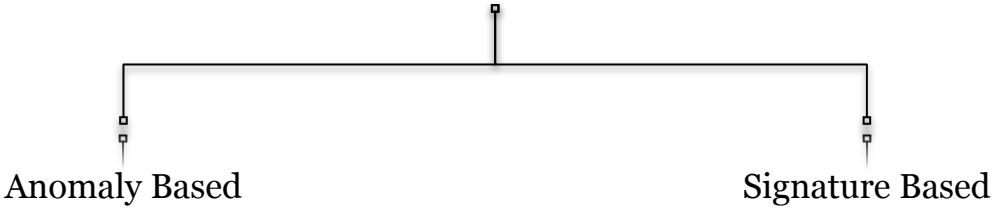
Priscilla Kyei Danso, P.A.C. Abisheka, Sagor Sikdar, G M Tasnim Alam

As of 2023, there are approximately 15.14 billion connected Internet of Things (IoT) devices

- IoT devices play a crucial role in our life, but how do we know if our device communications are tampered with or not?

- Network monitoring and anomaly detection using IDS
- Secure protocols and encryption
- Device authentication and authorization
- Etc

Let's talk about **Intrusion Detection Systems**



Research Problem

- Due to the diverse nature of networks and network devices and the lack of security measures builtin, it is challenging to identify compromised devices.
- Misclassifications commonly arise during the development of artificial intelligence models intended for testing such devices, primarily due to the variation between model training and testing environments.
- A gap exists in the availability of a robust intrusion detection system capable of effectively operating across multiple diverse environments.

Current State

Anomaly Detection

- Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review by Fahim et al.
  - Involve training models on normal behavior and identifying anomalies
  - More precise techniques are imperative for dealing with complex, real-world datasets.

https://www.flaticon.com/free-icon/intrusion_11313734

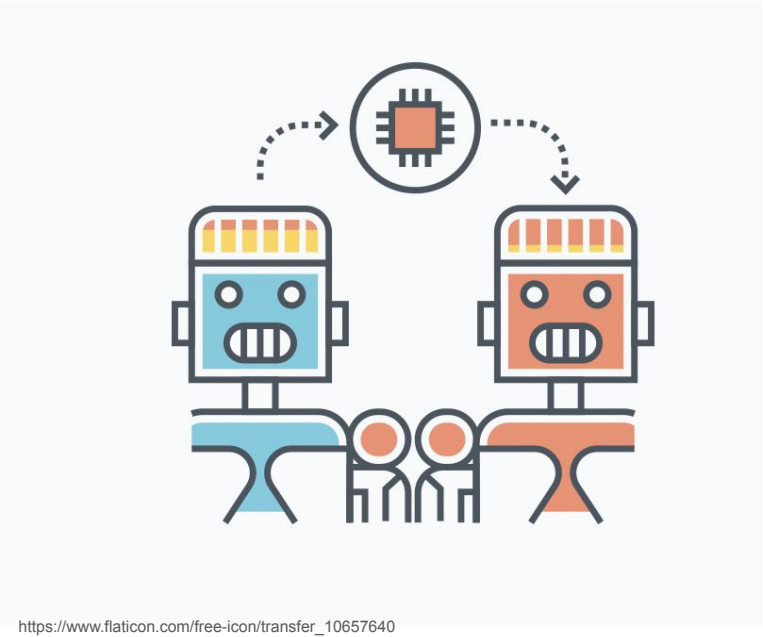
Malware Traffic Classification

- Malware Traffic Classification Using Domain Adaptation and Ladder Network for Secure Industrial Internet of Things by Jinhui Ning et al.
  - Innovative machine learning techniques to classify malwares
  - The ladder network adds an unsupervised component to the supervised learning objective of a deep forward network

https://www.flaticon.com/free-icon/bulb_3058444

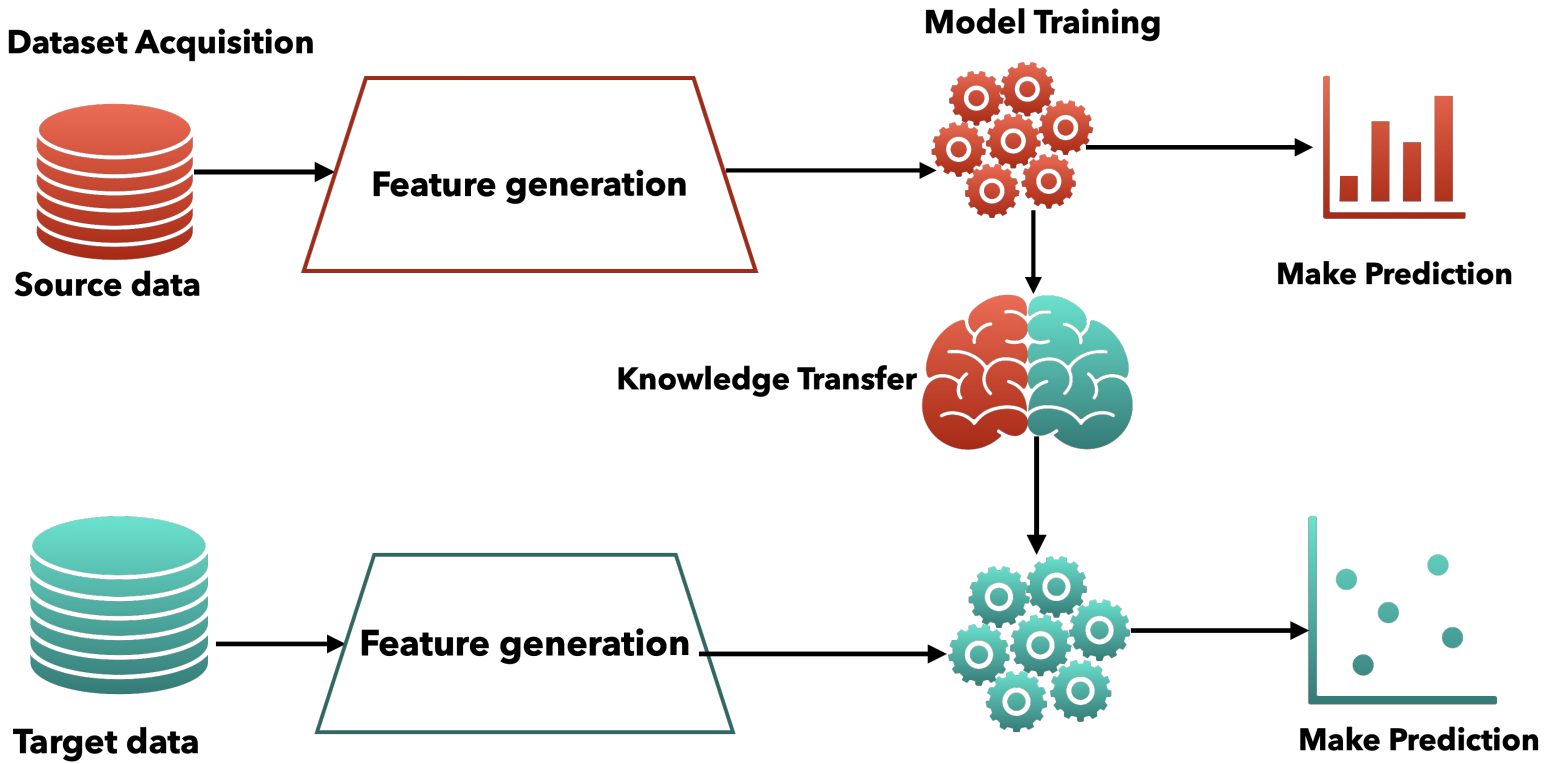
Transfer Learning and Adversarial DA

- Preparing Network Intrusion Detection Deep Learning Models with Minimal Data Using Adversarial Domain Adaptation by Ankush Singla et al.
    - Addressing the challenge of limited labeled samples in NID
    - Empowering organizations to identify new attack families by leveraging existing datasets

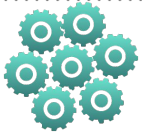
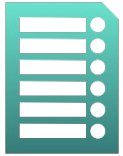


https://www.flaticon.com/free-icon/transfer_10657640

Our Approach



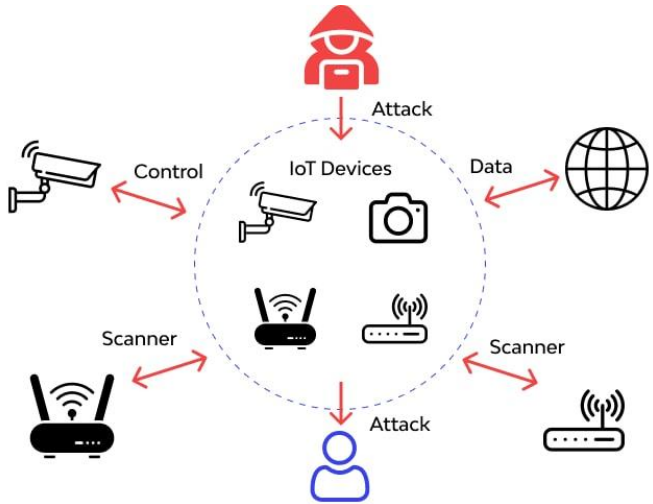
Our Approach - Underlying concept

Source		Target	
 D^{source}	Different but related	 D^{target}	*D = Data source* The data in both domains are considered different but related
 T^{source}	The same	 T^{target}	*T = Task* Task performed in both domains are equal
 $(X^{source}_{test}, Y^{source}_{test})$	No label in target	 $(X^{target}_{test}, ?)$	Target domain has no label during training
 $(X^{source}_{train}, Y^{source}_{train})$	Predict Target label	 (Y^{target}_{test})	Use trained model in source to predict the label in the target domain

Attack Types

We are working with 4 attack types

- Benign
- DOS (Syn Flood)
- Torii
- Mirai



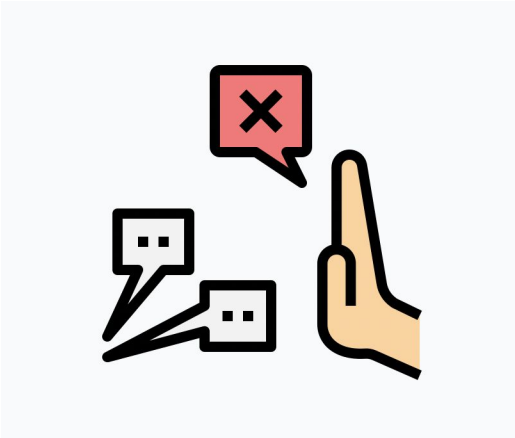
https://www.wallarm.com/what/iot-attack

Benign

- A benign cyber activity or entity refers to actions or elements that are **non-malicious** or pose **no threat** to a system or network.
- It encompasses normal, routine, or harmless activities within cyberspace that do not aim to cause harm or disruption.

DOS (Syn Flood)

- It is a type of cyber attack that targets the initiation of a TCP handshake.
- It involves overwhelming a server with a flood of connection requests (SYN packets)
- The attacker doesn't complete the handshake, leaving the server waiting for confirmation.
- This flood of half-open connections exhausts the server's resources



https://www.flaticon.com/free-icon/rejection_2191154

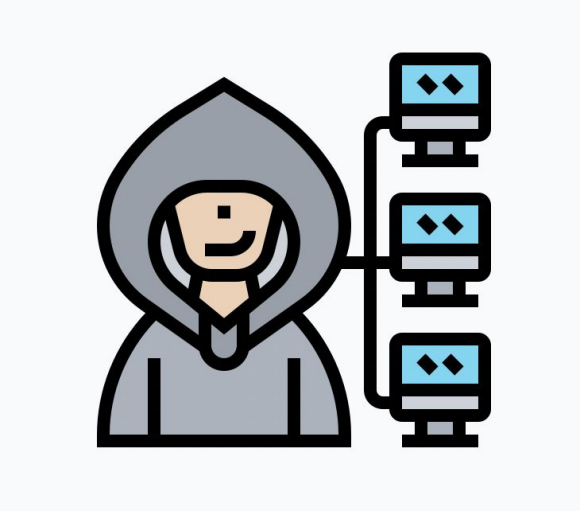
Torii

- It is a sophisticated and stealthy IoT botnet malware that targets various architectures, including **IoT devices** and enterprise servers
- It provides attackers with **remote control**, **data exfiltration**, and the ability to run **arbitrary commands** on infected devices

https://www.flaticon.com/free-icon/cyber-attack_9094815

Mirai

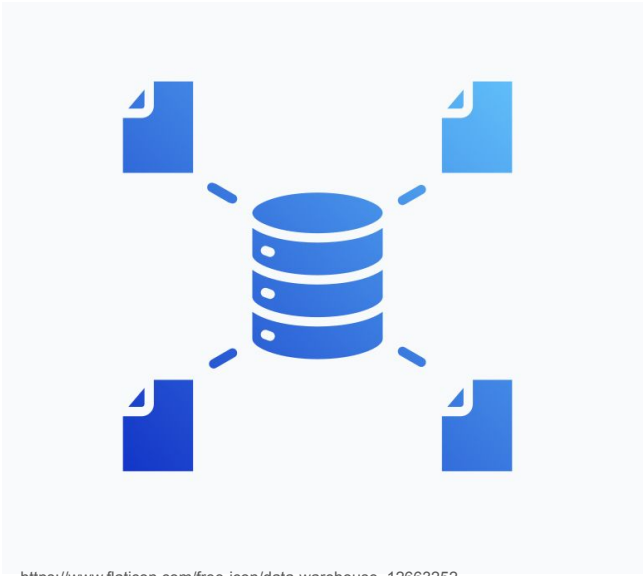
- Mirai is a type of malware that targets **IoT devices**
- It functions by exploiting weak security measures in these devices, infecting them to form a **botnet**.



https://www.flaticon.com/free-icon/botnet_2974496

Data Set

- CIC IoT Dataset 2023
- MedBIoT Dataset
- IoT Dataset 2023
- IoT Network Intrusion Dataset 2019



https://www.flaticon.com/free-icon/data-warehouse_12663252

CIC IoT Dataset

- Created by Canadian Institute of Cyber Security
- **33 attacks are executed in an IoT topology composed of 105 devices. These attacks are classified into seven categories.**
- **PCAP:** Contains the original traffic captured during the attacks as .pcp files
- **CSV:** Contains features extracted from the original files to be used in the Machine Learning (ML) evaluation (.csv files)

MedBIoT

- Created by a research group in TALTech
- Combination of real and emulated IoT devices in a medium-sized network (i.e., 83 devices).
- Actual malware was deployed, providing real malware network data. Three prominent botnet malware were deployed: **Mirai**, **BashLite**, and **Torii**.
- This data set is suitable for **IoT botnet** research in general and **intrusion detection systems**

IoT Dataset

- This dataset was created as part of the Avast AIC laboratory with the funding of Avast Software
- It has **20 malware** captures executed in IoT devices, and **3 captures** for benign IoT devices traffic.
- We will be using this dataset as a source for Torii.

IoT NID

- Featuring **SKT NGU smart home** device and an **EZVIZ Wi-Fi camera.**
- The dataset consists of **42 raw** network packet files (pcap) at different time points.
- The IoTID20 dataset's development led to the final version comprising **83 network features** and three label features.
- We are going to use this dataset as a target dataset for **Mirai** and **DOS (Syn Flood)**

Source & Target

Attack Type	Source	Target
Benign	CIC IoT 2023	IoT 2023
DOS Syn Flood	CIC IoT 2023	IoT Network Intrusion 2019
Mirai	CIC IoT 2023	IoT Network Intrusion 2019
Torii	IoT 2023	MedBIoT

The baseline model utilized:

- 62 features
- 3000 records for each attack type

Experimental Results

	Accuracy (%)		Precision (%)		Recall (%)		F1-Score (%)	
	Source	Target	Source	Target	Source	Target	Source	Target
Algorithms								
KNN	64	25	64	25	64	25	63	24
SVC	66	25	64	25	66	25	64	24
NaiveBayes	75	25	79	25	75	25	75	24
LogisticRegression	68	25	67	25	68	25	67	24
DecisionTree	100	25	100	13	100	25	100	16
RandomForest	100	25	100	13	100	25	100	16
GradientBoosting	100	25	100	13	100	25	100	16
ExtraTree	100	25	100	13	100	25	100	16
AdaBoost	75	25	62	13	75	25	67	16

Deep Learning Approach

1. Train deep learning based methods on the source domain

2. Leverage this pretrained model on the target domain for few shot learning

3. Use PCA for strategic sampling of input from the target domain for few-shot learning

4. Fine-tune the pretrained model for the enhanced domain adaptation

Improved Experimental Results

Deep Learning Approaches	Accuracy(%)	Precision(%)	Recall(%)	F1 Score
LSTM	31.13	30.21	31.84	31
LSTM + CNN	33.47	32.63	33.17	32.88

For few shot learning, k = 5 was used.

Contribution and Novelty

- Analyze the application ML on when data (training and test) is drawn from the same or different distribution
- Employed transductive transfer learning of attack identification
- Employed multiple ML algorithms in our study
- Improved the results of our baseline model using deep learning

Future Work

- Improve classification results
- Employ boosting to find out specific information from each model
- Conduct experiments in real networks with simulated attacks

Any Questions?

TABLE II: Features extracted from pcaps used in evaluation

Time	Flow duration	Header Length	Protocol Type	Duration
Rate	Source Rate	Destination Rate	Fin flag number	Syn flag number
Rst flag number	Psh flag number	Ack flag number	Urg flag number	Ece flag number
Cwr flag number	Ack count	Syn count	Fin count	Urg count
Rst count	Max duration	Min duration	Sum duration	Average duration
std_duration	CoAP	HTTP	HTTPS	DNS
Telnet	SMTP	SSH	IRC	TCP
UDP	DHCP	ARP	ICMP	IGMP
IPv	LLC	Tot sum	Min	Max
AVG	Std	Tot size	IAT	Number
MAC	Magnitue	Radius	Covariance	Variance
Weight	DS status	Fragments	Sequence number	Protocol Version
Flow idle time	Flow active time			