IET

Leveraging Federated Machine Learning to Improve Intrusion Detection in IoT

Mohammed Al-khafajiy

21st January 2025

Dr Mohammed Al-khafajiy

Senior Lecturer (Assistant Professor)
School of Computer Science
University of Lincoln

Contact

+447448822321

MAlkhafajiy@lincoln.ac.uk

Address

Office
University of Lincoln
Isaac Newton Building
Brayford Pool, Linocln

Who Am I?

IET

Dr Mohammed AL-KHAFAJIY

MAlkhafajiy@lincoln.ac.uk +447448822321

Linkedin.com/in/Mohammed-Alkhafajiy

SCAN ME

PROFESSIONAL EXPERIENCE

- Senior Lecturer (Assistant Professor) at University of Lincoln, Lincoln - UK
- ICT Instructor, **HUAWEI ICT ACADEMY UK** – *on demand*

Prior

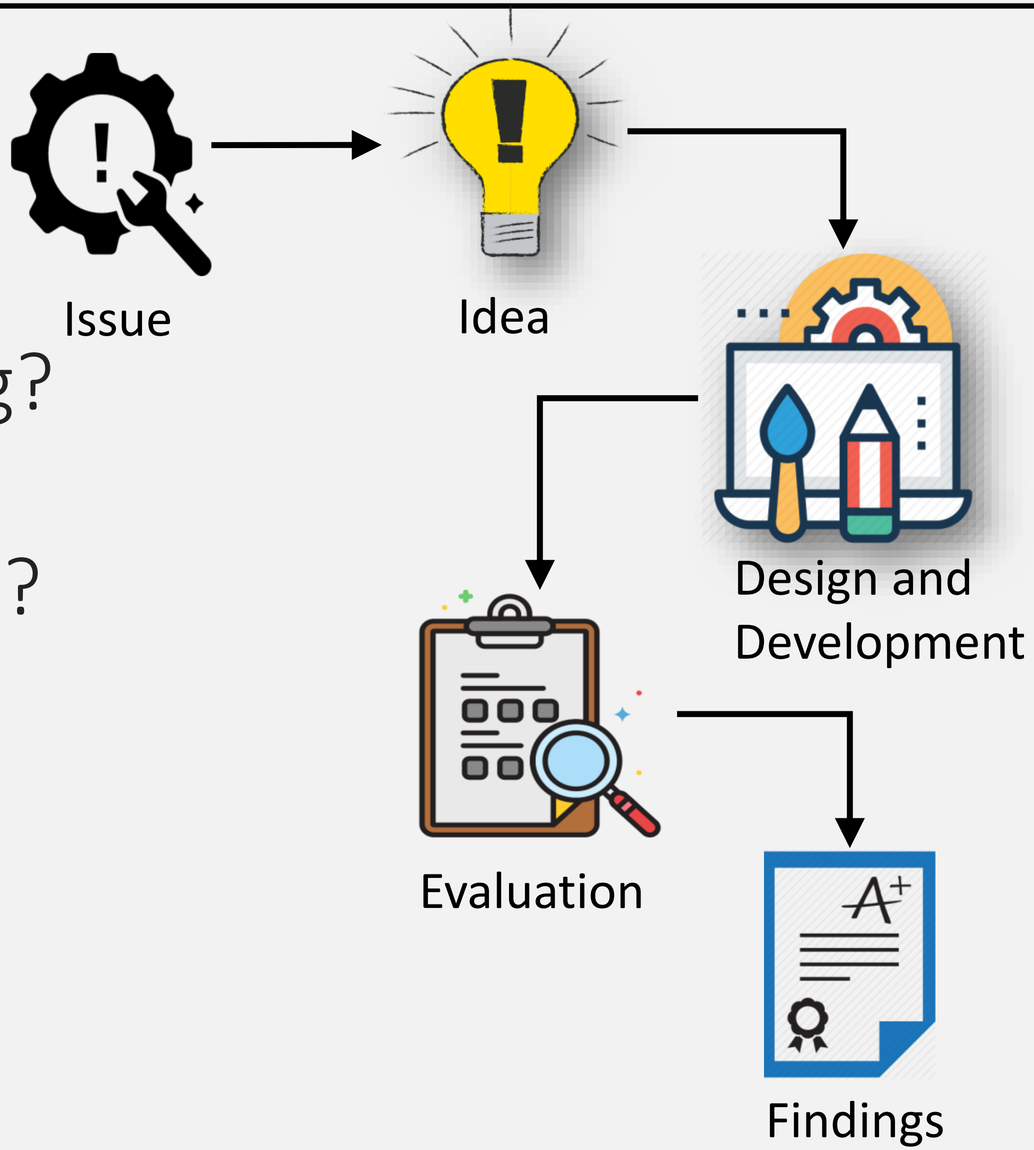
- **Lecturer**, University of **Reading**, Reading – UK
- **Senior Researcher**, Liverpool John Moores University, Liverpool - UK

EDUCATION

- PhD Liverpool John Moores University, PhD Computer Science - Distinction (Scholarship)
- MSc Liverpool John Moores University, MSc Software Engineering - Distinction (Scholarship)
- BSc University of Northampton, BSc Computing (Software Engineering) - 1st Class (Scholarship)

Outline

1. The IoT Security Landscape
2. What is Federated Machine Learning?
3. Traditional IDS vs. Federated IDS
4. Why FML for IoT Intrusion Detection?
5. Key Components of Federated ID
6. Challenges and Future Directions



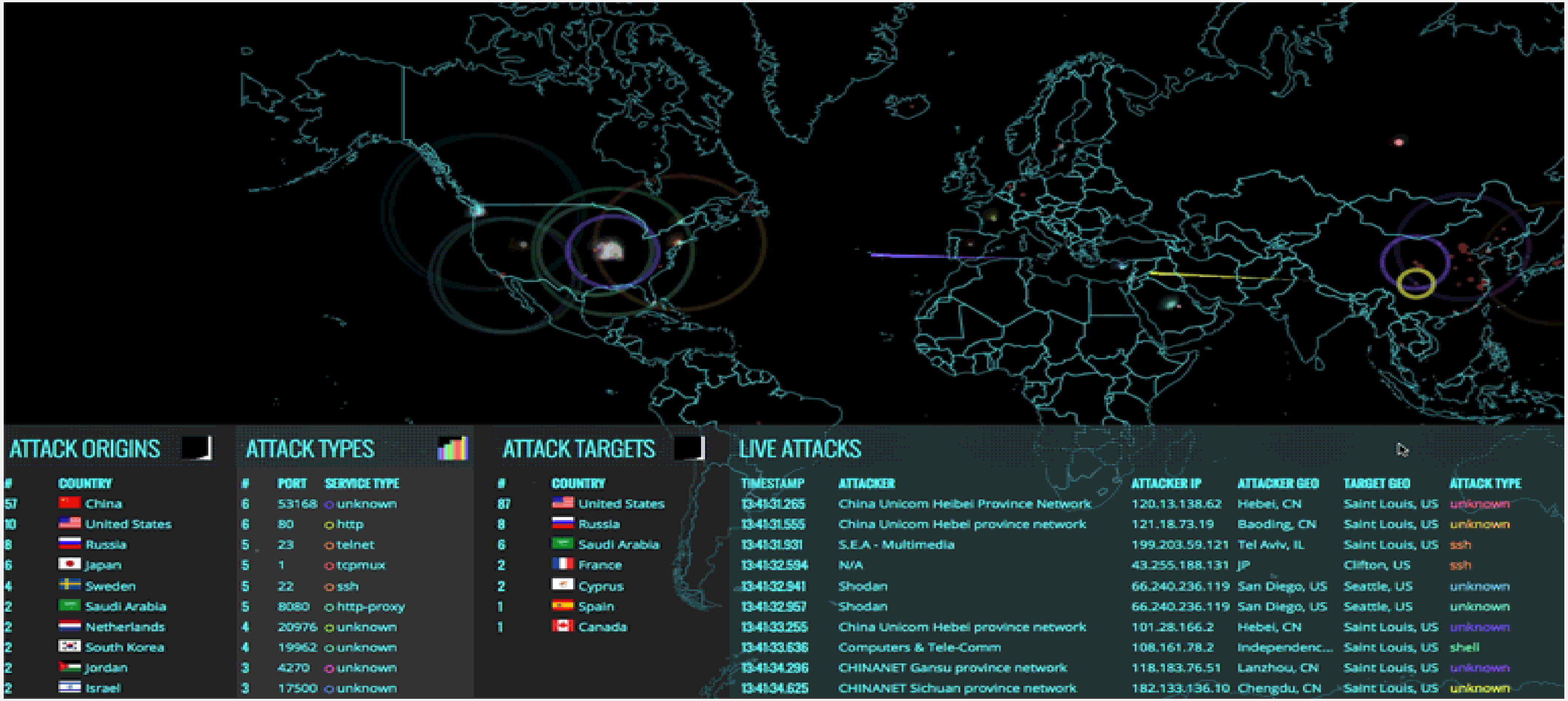
Introduction - IoT

- The **IoT** (Internet of Things) is the network of physical “*objects*” or “***things”*** embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.

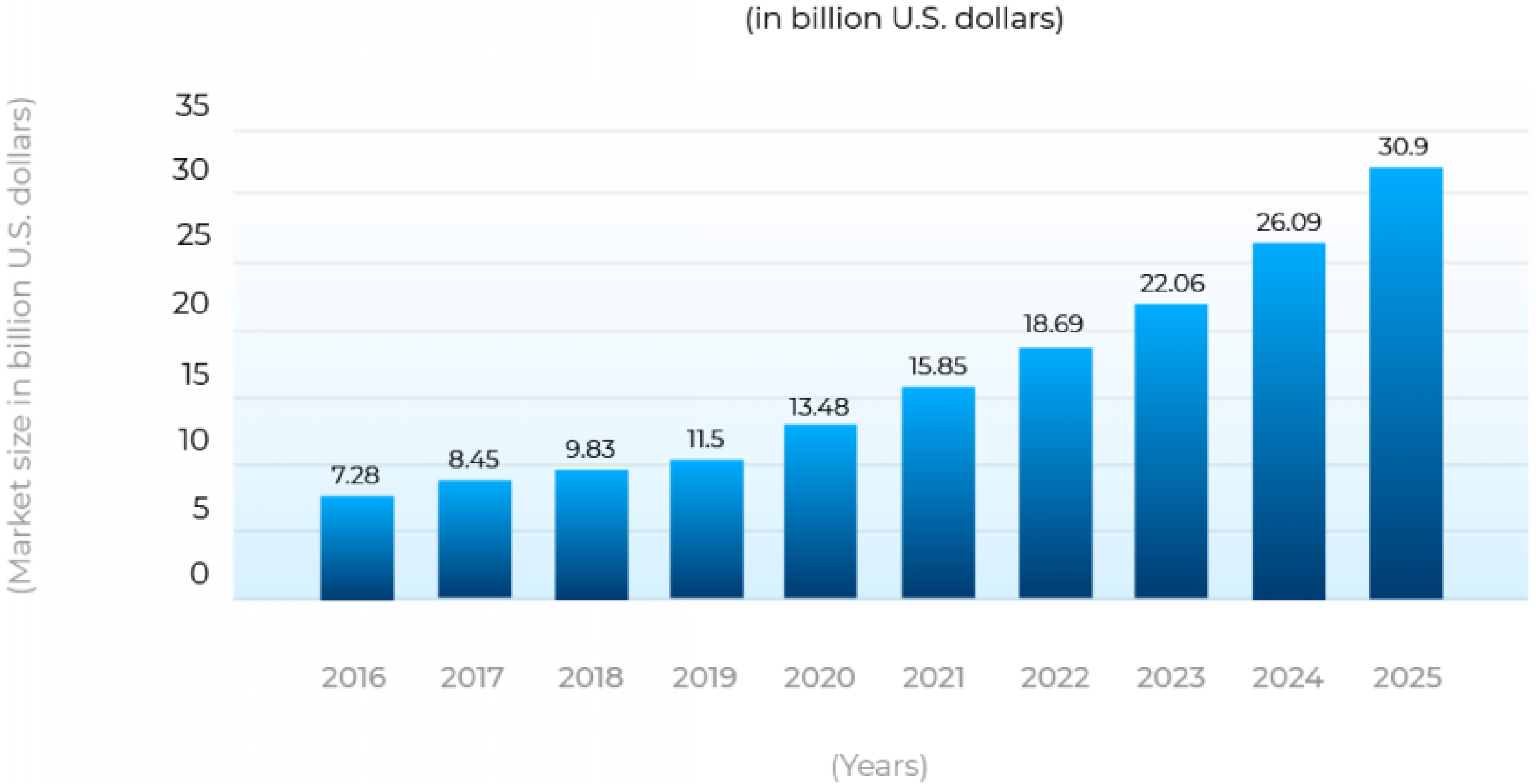
- Forming smart applications, homes, and cities.

Introduction - IoT Security

- Massive data exchange makes IoT networks vulnerable to intrusions such as malware, unauthorised access, and Distributed Denial of Service (DDoS) attacks.



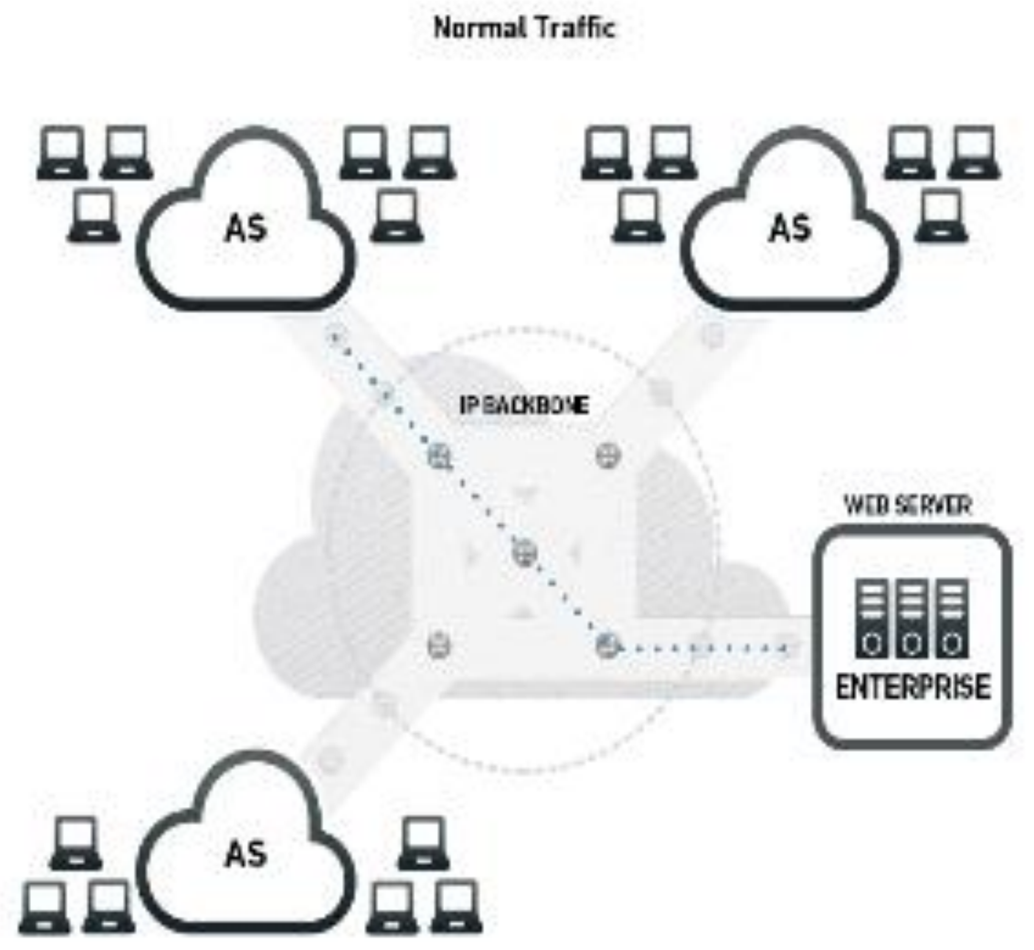
Size of the Internet of Things (IoT) security market worldwide from 2016 to 2025



The IoT Security Landscape

- **Challenges in IoT Security:**
  - **Heterogeneity:** Diverse devices with varying protocols.
  - **Resource Limitations:** Low power and memory in devices.
  - **Scalability:** Millions of devices in a single network.

- **Common Intrusion Threats:**
  - DDoS
  - Eavesdropping
  - Spoofing
  - Botnet attacks (e.g., Mirai botnet)



IoT Security

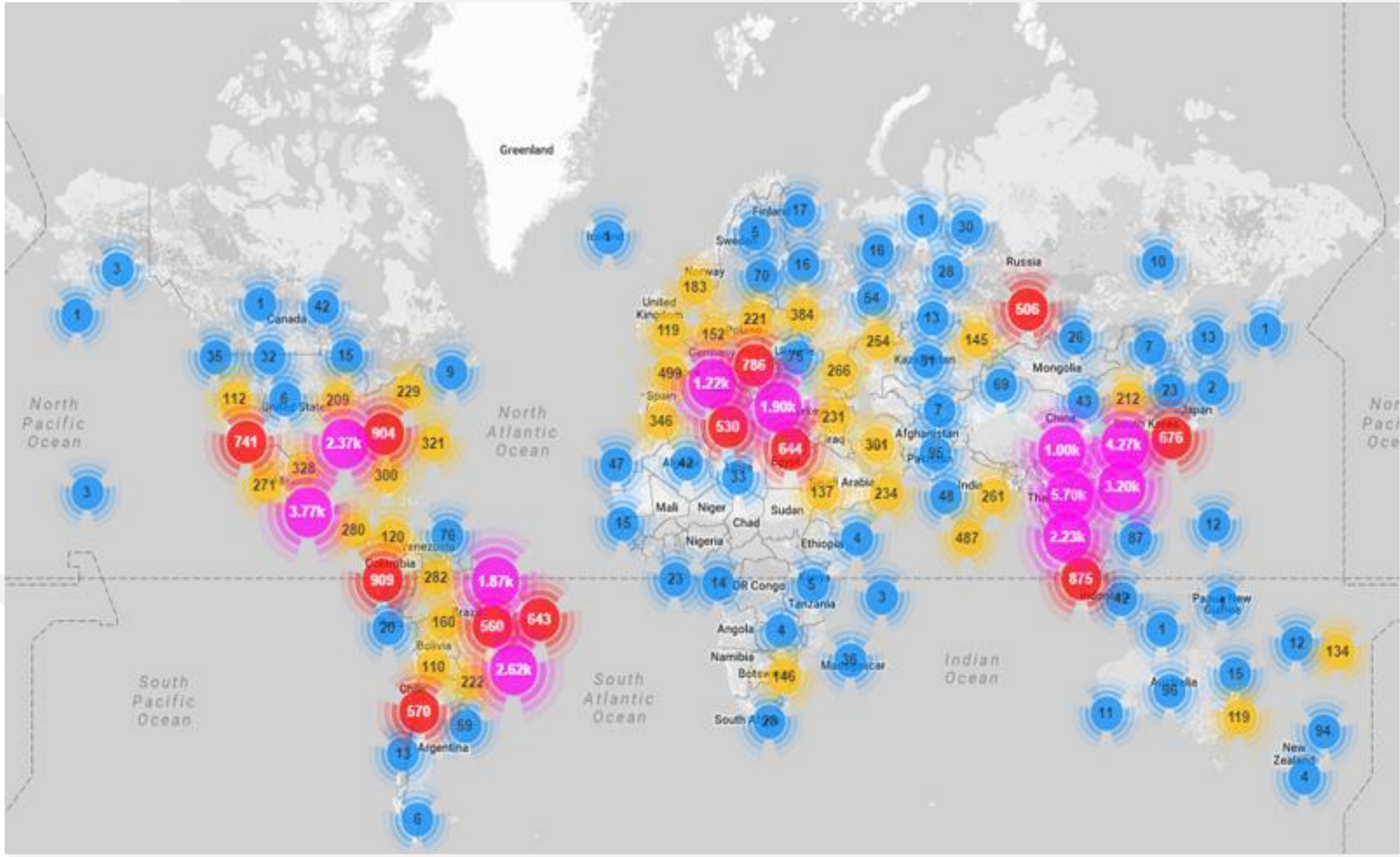
The three main security vulnerabilities in IoT are:

1. **Weak Authentication and Authorisation**
   Many IoT devices lack robust authentication mechanisms, this makes it easier for attackers to gain unauthorized access to devices and networks.

2. **Lack of Data Encryption**
   IoT devices often transmit data over networks without proper encryption. This exposes sensitive information, such as operational data, to interception or eavesdropping by malicious actors.

3. **Insecure Software and Firmware**
   IoT devices frequently run outdated or poorly designed software and firmware. Vulnerabilities in these systems can be exploited by attackers, especially when security patches and updates are not applied regularly.

Examples of IoT security breaches



- **Mirai Botnet Attack in 2016:** Hundreds of thousands of IoT devices were infected and used to create the Mirai botnet.

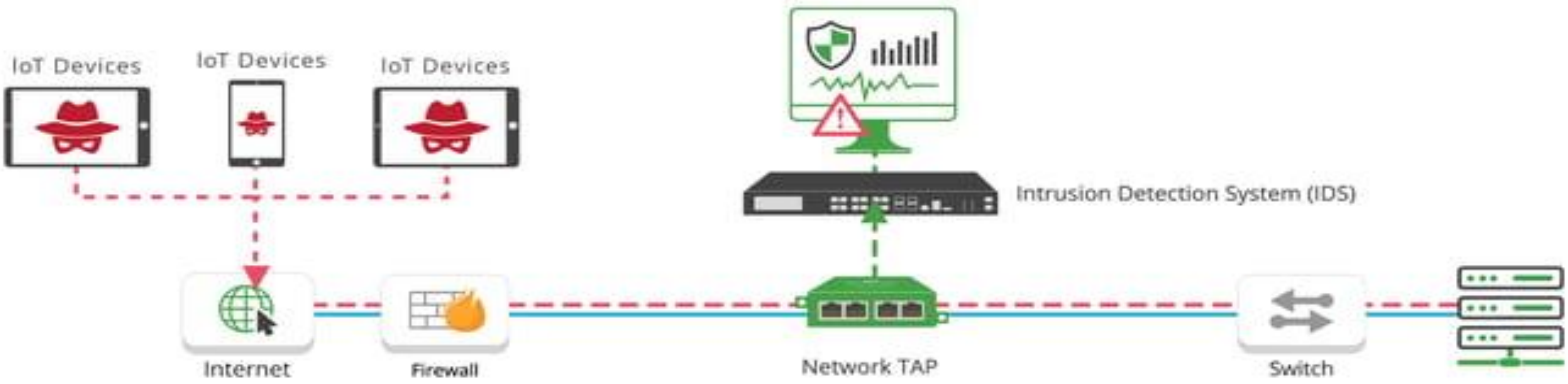
- This botnet launched DDoS attacks that temporarily shut down major services like **Spotify**, **Netflix**, and **PayPal**.

More examples of IoT security breaches

- **2018: VPNFilter Malware**
  - VPNFilter malware infected over 500,000 routers in 50+ countries. The malware intercepted data, blocked traffic, and stole sensitive information like passwords.
- **2020: Tesla Model X Hacked**
  - A cybersecurity expert exploited a Bluetooth vulnerability to hack a Tesla Model X, highlighting security risks with wireless key systems in cars.
- **2021: Verkada Camera Feeds Hacked**
  - Swiss hackers compromised 150,000 live camera feeds from Verkada, a security camera company. These cameras monitored locations like schools, hospitals, and prisons, raising privacy concerns.

Intrusion Detection in IoT

- **IoT Network Intrusion Detection Systems**
  - IoT IDS monitors the internet traffic across the devices in an IoT network. It acts as a defence line, which can identify risks and protect the network from intruders and malicious attacks.



Limitation of IoT IDS

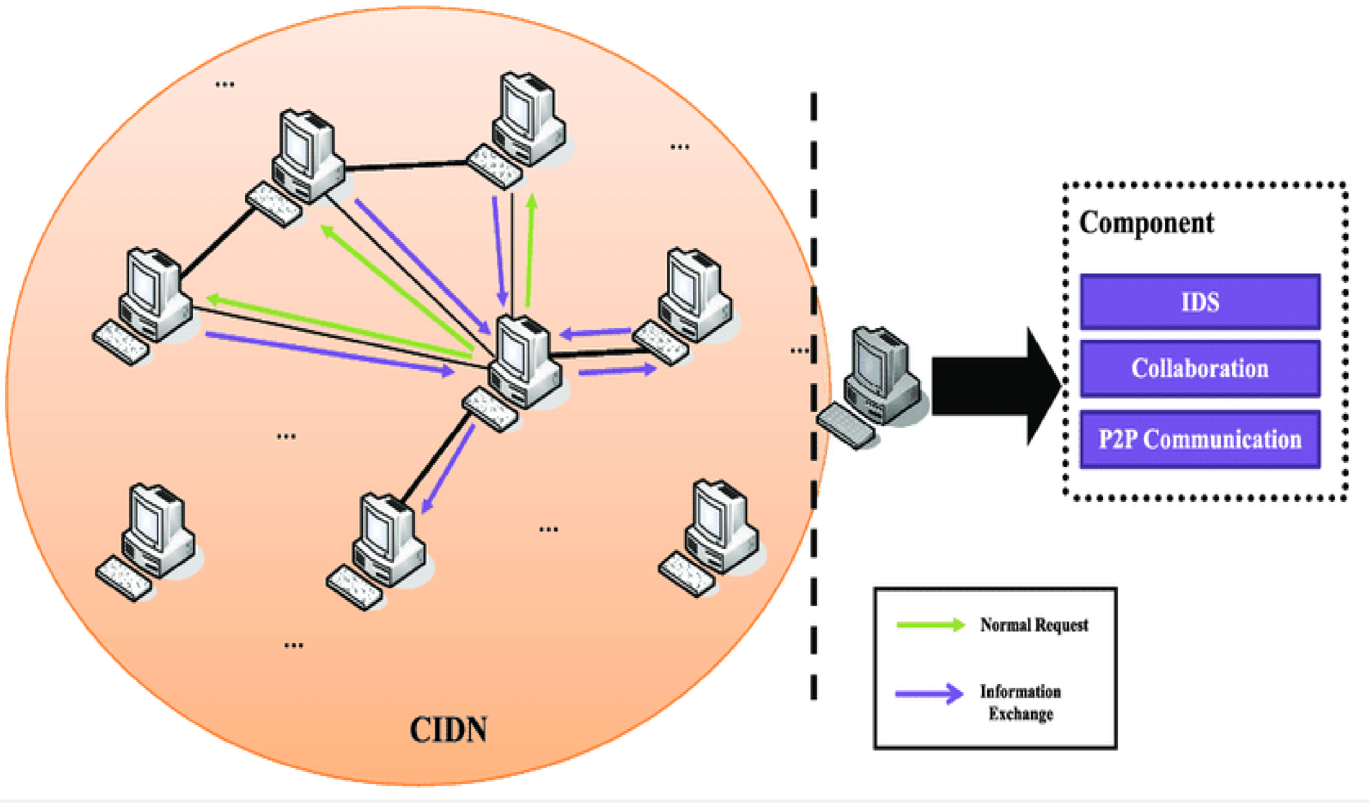
- **Traditional Intrusion Detection Systems (IDS):**
  - Inefficient against unknown attacks
  - ML IDS needs a lot of data to be accurate
  - Vulnerable to data breaches and network bottlenecks.

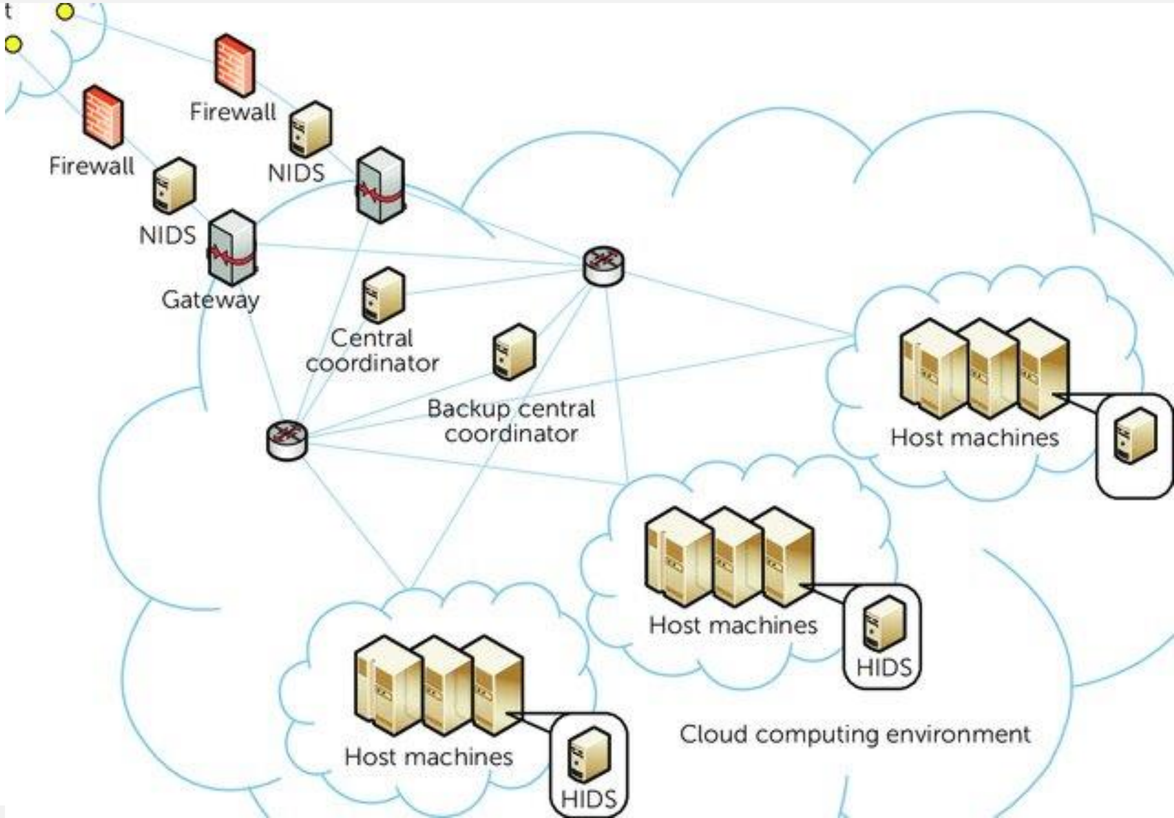
- **+ IoT limitation**
  - Resource restrictions (memory, desk, etc.) and execution time.
  - Centralised data collection and analysis.

*These led to the development of tools such as **TinyML**, which is designed to shrink ML down to IoT scale, however this comes at the cost of **performance**.*

Collaborative Intrusion Detection System

- A Collaborative Intrusion Detection System (CIDS) is a framework that uses multiple detectors to identify intrusions in distributed systems.





limitations of CIDS

1. **Privacy and Security Concerns:** Sharing sensitive data across systems can lead to potential exposure and security risks.

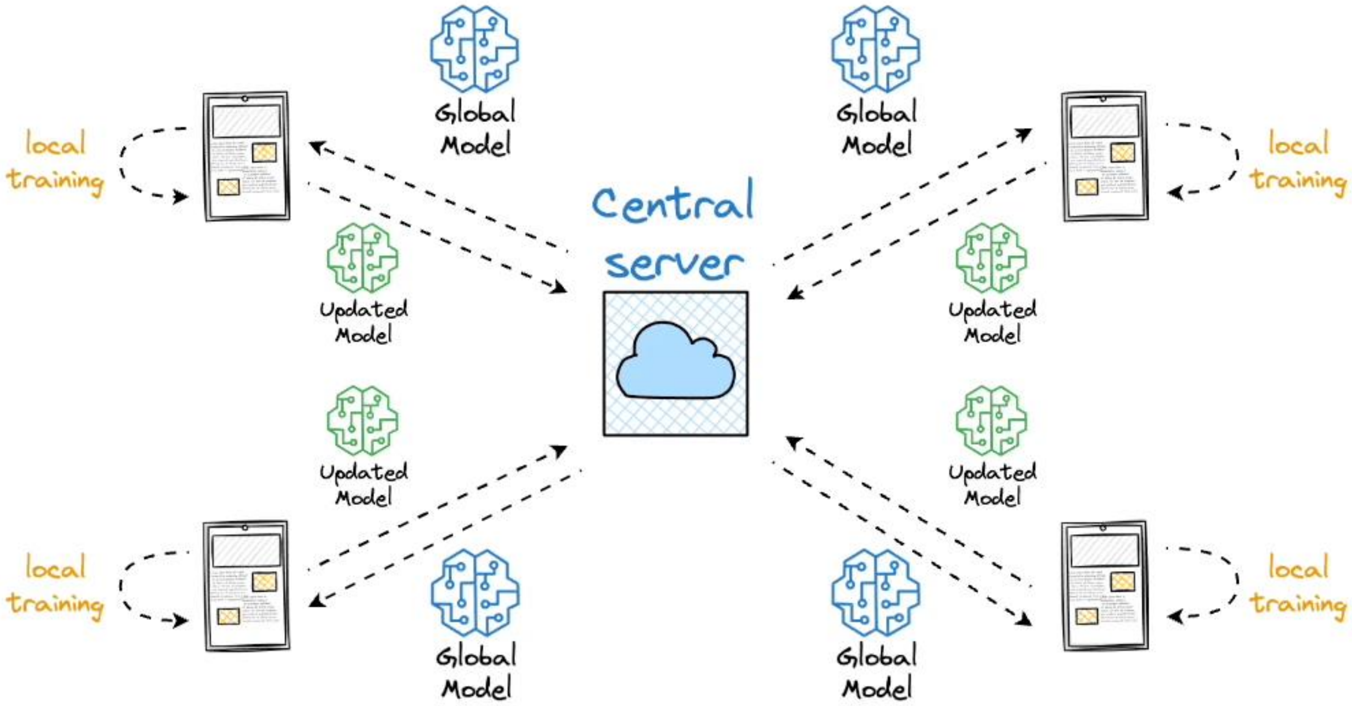
2. **Scalability Issues:** Managing a growing number of collaborating entities and large volumes of data can lead to performance problems.

3. **Data Overload:** High volumes of incoming data can overwhelm the system, making it difficult to identify real threats from false positives.

4. **Trust Issues:** Trusting all collaborators is difficult, especially if one participant is compromised, which could lead to false data being shared.

5. **Latency in Response:** Data exchange between multiple systems can introduce delays, allowing attackers more time to cause damage.

Federated IDS



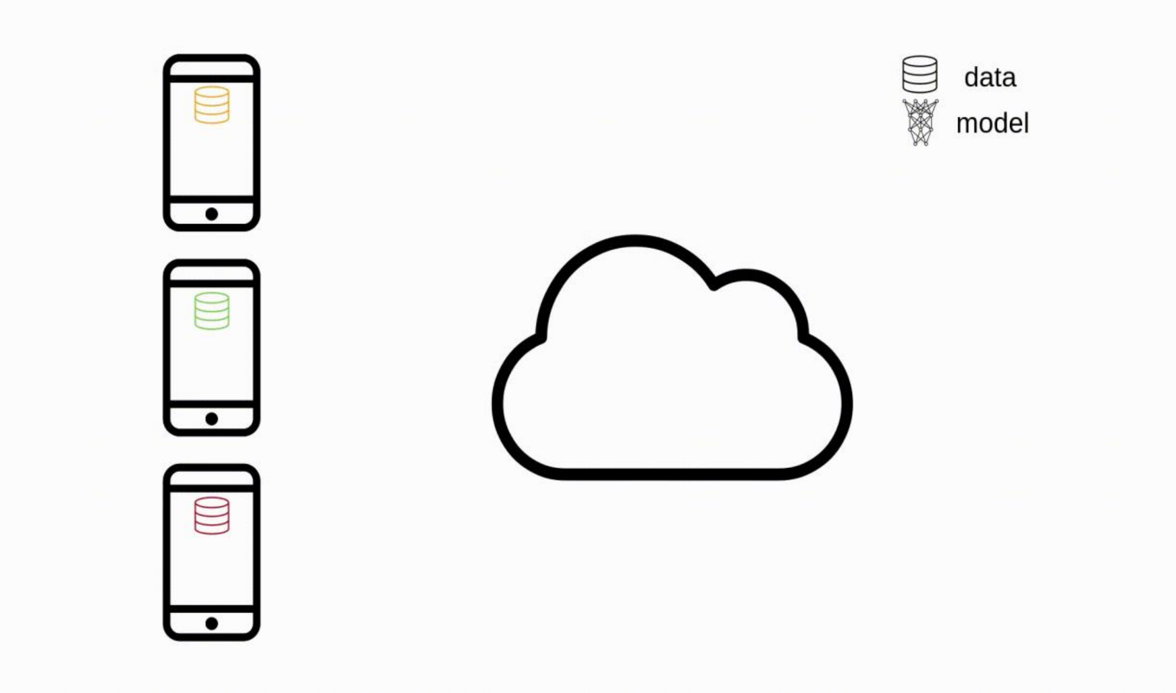
Federated Learning

- Federated Learning (FL) is a decentralized machine learning paradigm introduced by **Google** in **2016** to enhance data privacy.

- It uses a distributed environment where participating nodes complete analysis of their own data with no need of transfers. Nodes are then share trained model updates instead of raw data.

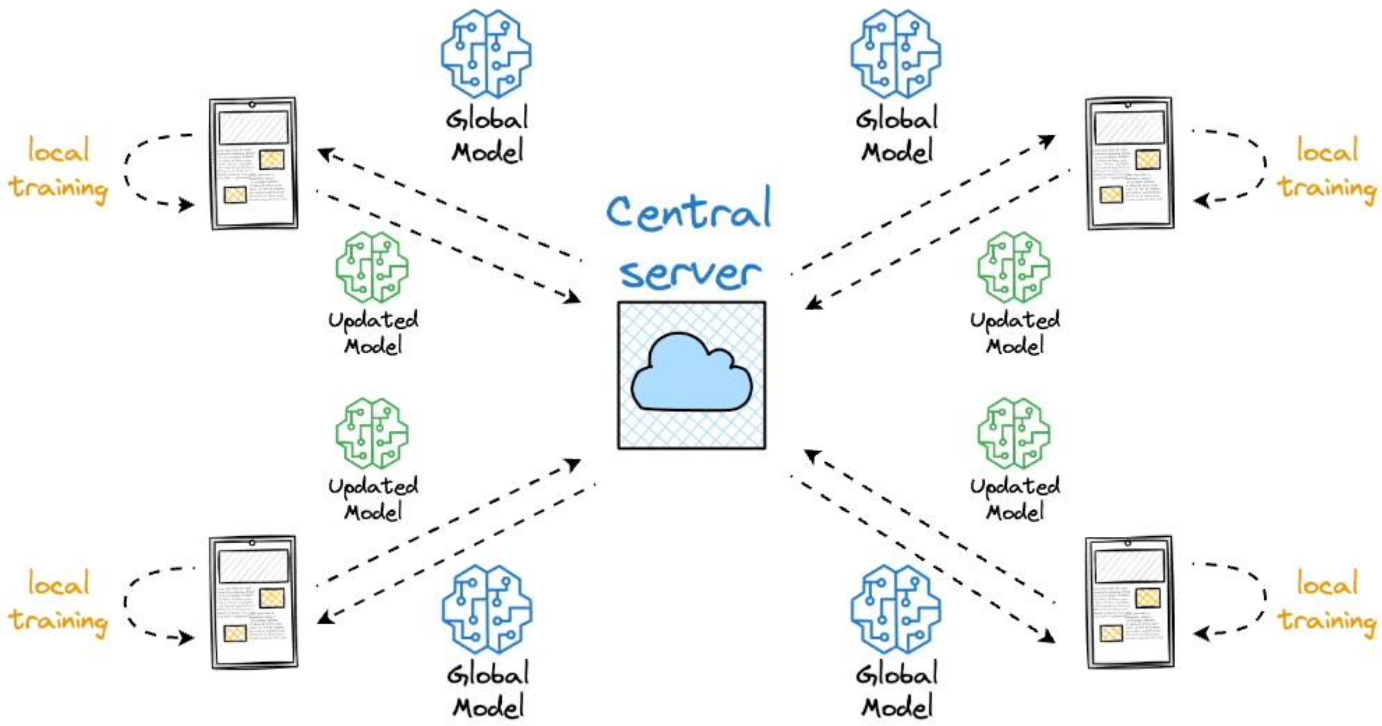
- A central server acts as an aggregator, coordinating the training process and combining model updates from clients.

- Aggregation is typically performed using algorithms like Federated Averaging (FedAvg).



Federated Learning Workflow

- Each device trains a local model using its data.
- Model updates (gradients) are sent to a central server.
- The server aggregates updates to create a global model.
- The global model is distributed back to devices.



Components of FID

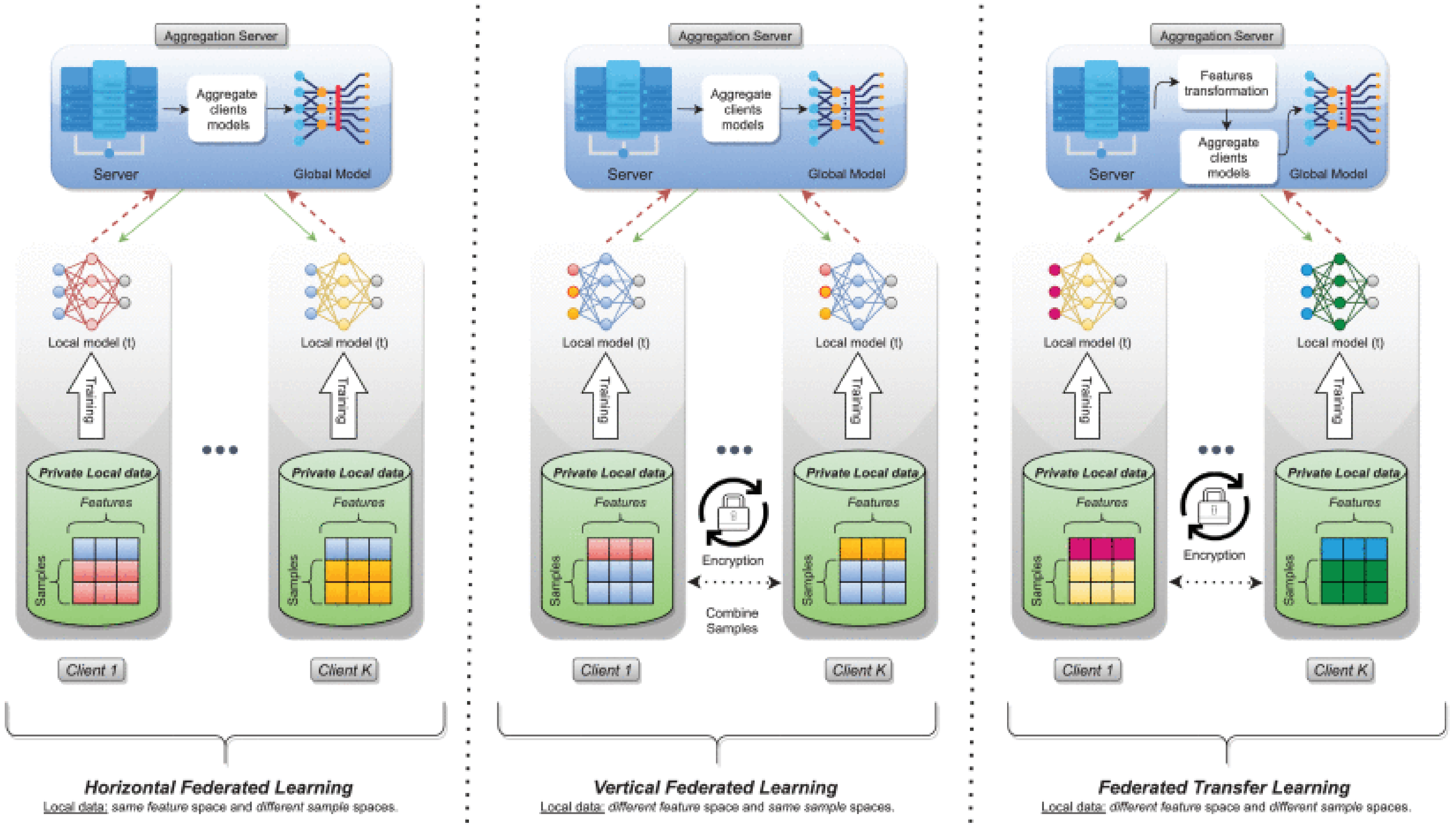
1. **Data Collection:**
   - Logs of network traffic and device activity.

2. **Local Model Training:**
   - Lightweight algorithms for resource-constrained devices.
   - Use of anomaly detection models like SVM, Autoencoders, etc.

3. **Federated Aggregation:**
   - Techniques like Federated Averaging (FedAvg) to combine model updates.

4. **Global Model Deployment:**
   - Models are optimized for diverse IoT architectures

Types of FID



Aggregation Server
Aggregate clients models
Server
Global Model
Local model (t)
Training
Private Local data
Features
Samples
Client 1
Client K
Horizontal Federated Learning
Local data: same feature space and different sample spaces.
Aggregation Server
Aggregate clients models
Server
Global Model
Local model (t)
Training
Private Local data
Features
Samples
Encryption
Combine Samples
Client 1
Client K
Vertical Federated Learning
Local data: different feature space and same sample spaces.
Aggregation Server
Features transformation
Aggregate clients models
Server
Global Model
Local model (t)
Training
Private Local data
Features
Samples
Encryption
Client 1
Client K
Federated Transfer Learning
Local data: different feature space and different sample spaces.

Proposed IoT FID

1. **Data:**
   - **CIC-IoT2023** - A real-time dataset and benchmark for large-scale attacks in IoT environment.
   - Approx 13GB - target DDoS attacks

2. **Local Model Training:**
   - Support Vector Machine (**SVM**) and One-Class SVM.
   - Complexity: $O(n{\cdot}d)$ per iteration, where:
     - n: number of training samples.
     - d: number of features (dimensionality).
   - Its *O(n · d)* space and time complexity makes it suitable for IoT devices training models

Proposed IoT FID

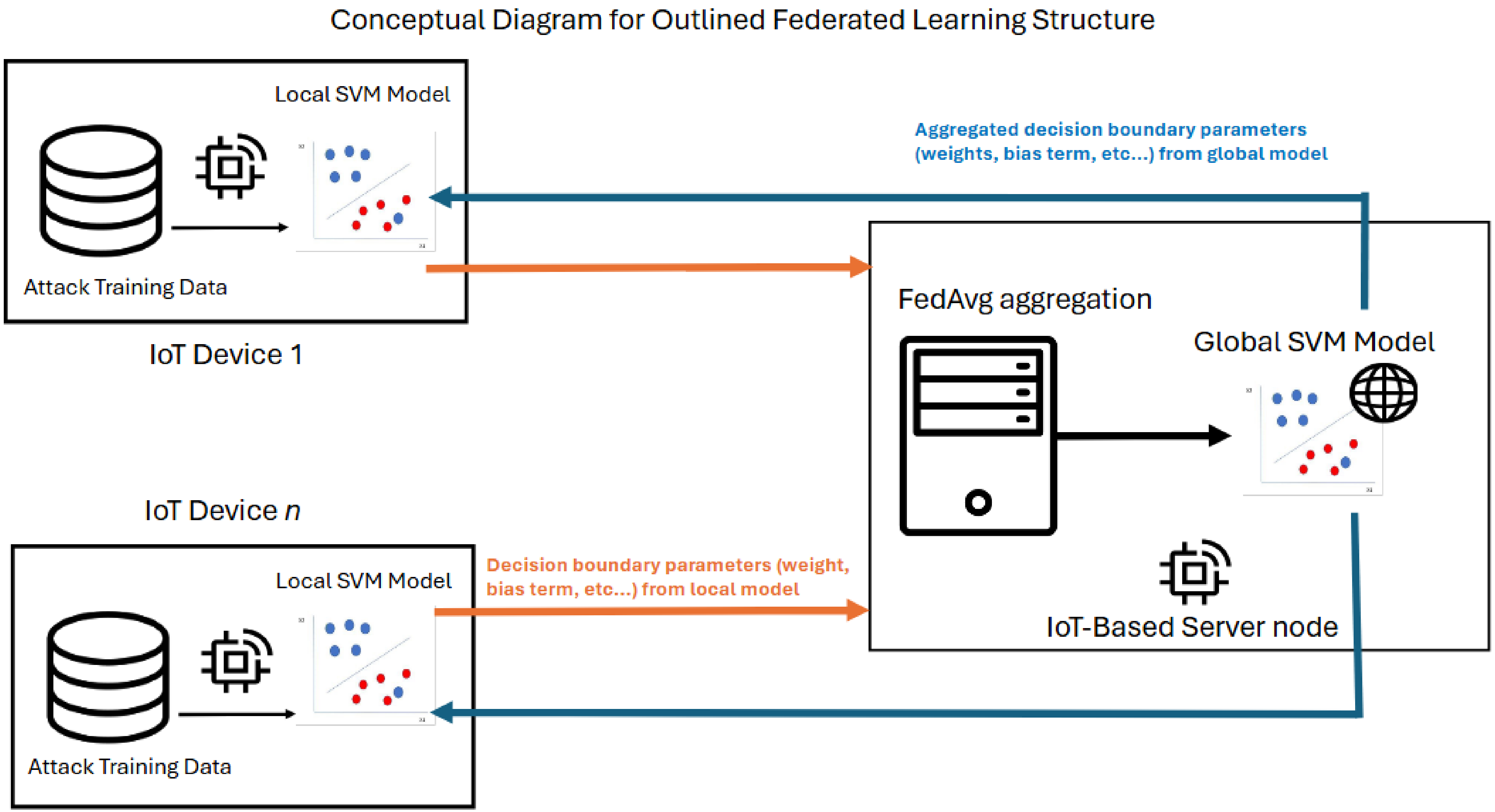
3. **Federated Aggregation:**
   - Federated Averaging (FedAvg) to combine model updates.

Top-level FedAvg algorithm
$parameters \leftarrow [weight, bias]$
for $rounds$ **do**
Each node $\leftarrow$ $parameters$
Each node trains
$weight\_array \leftarrow weight$ FROM ALL nodes
$bias\_array \leftarrow bias$ FROM ALL nodes
$weight \leftarrow \frac{\sum weight_i}{N}$
$bias \leftarrow \frac{\sum bias_i}{N}$
$parameters \leftarrow [weight, bias]$
end for

4. **Model Deployment:**
   - Flower federated learning framework
   - It handle coordination and communication between worker nodes;

Flower
Framework

Proposed IOT FID



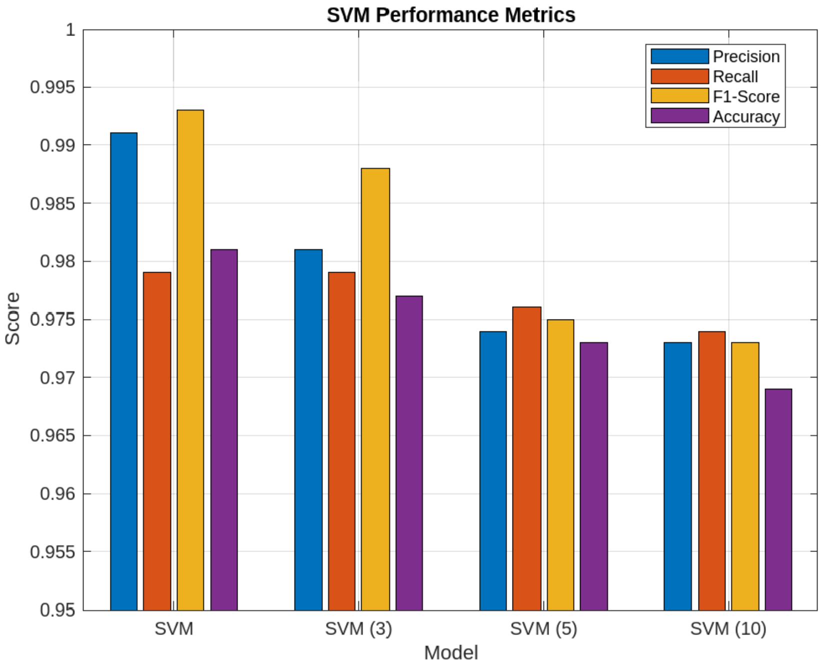
Results

Federated *vs* Non-Federated

Table 1. SVM compared with itself.

Model	Accuracy	Precision	Recall	F1 Score
SVM	0.991	0.979	0.993	0.981
SVM (3)	0.981	0.979	0.988	0.977
SVM (5)	0.974	0.976	0.975	0.973
SVM (10)	0.973	0.974	0.973	0.969

Table 1 shows steady performance decreases as the node count rises, due to the dataset becoming more fractured. The jump from **three** nodes to **five** nodes is much bigger than **five** to **ten**, suggesting that it has some **diminishing effects**.



Results

SVM *vs* Other Models

Table 2. SVM compared with other federated models.

Model	Accuracy	Precision	Recall	F1 Score
SVM (5)	0.974	0.976	0.975	0.981
IF (5)	0.732	0.741	0.741	0.742
RF (5)	0.981	0.982	0.982	0.981
ANN (5)	0.974	0.983	0.975	0.975

Table 2 shows that SVM fits in the top range of models, with the slight variances between ANN (Artificial Neural Network), RF (Random Forests), and SVM. Isolation Forest (IF) performs poorly here compared to other classifiers

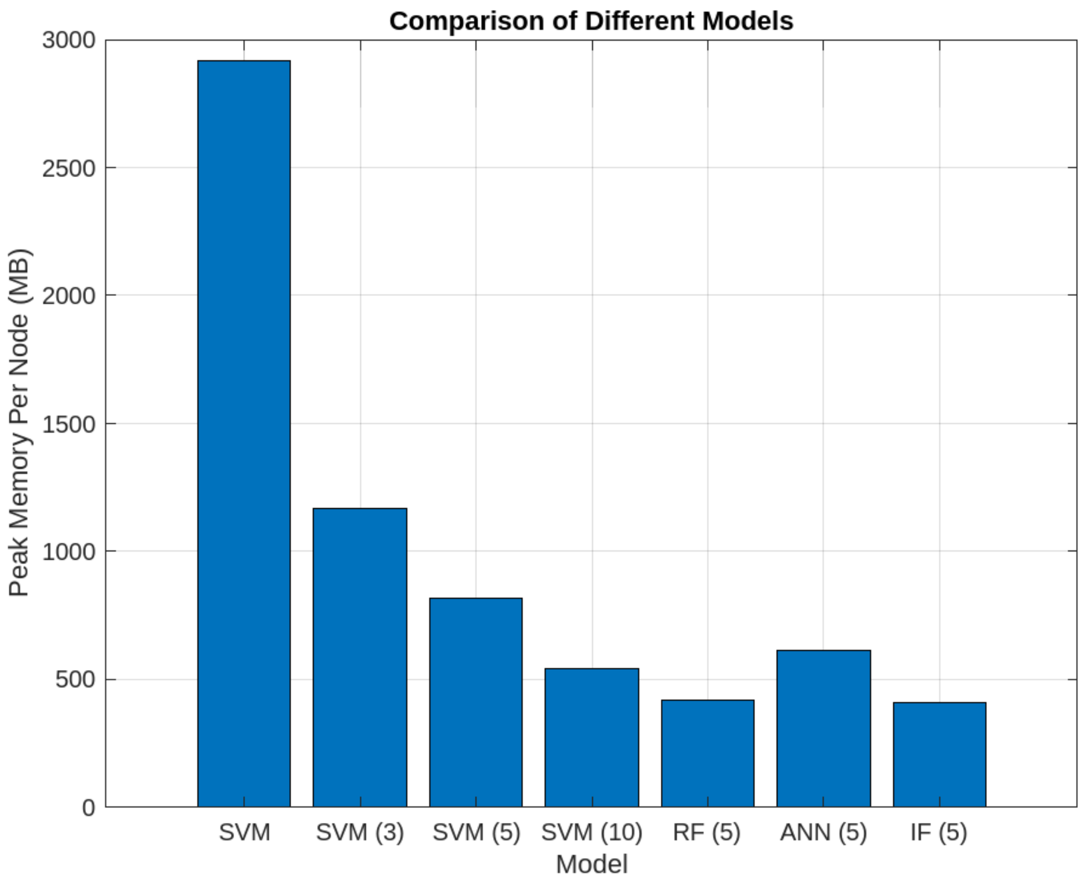
Results

Physical Metrics

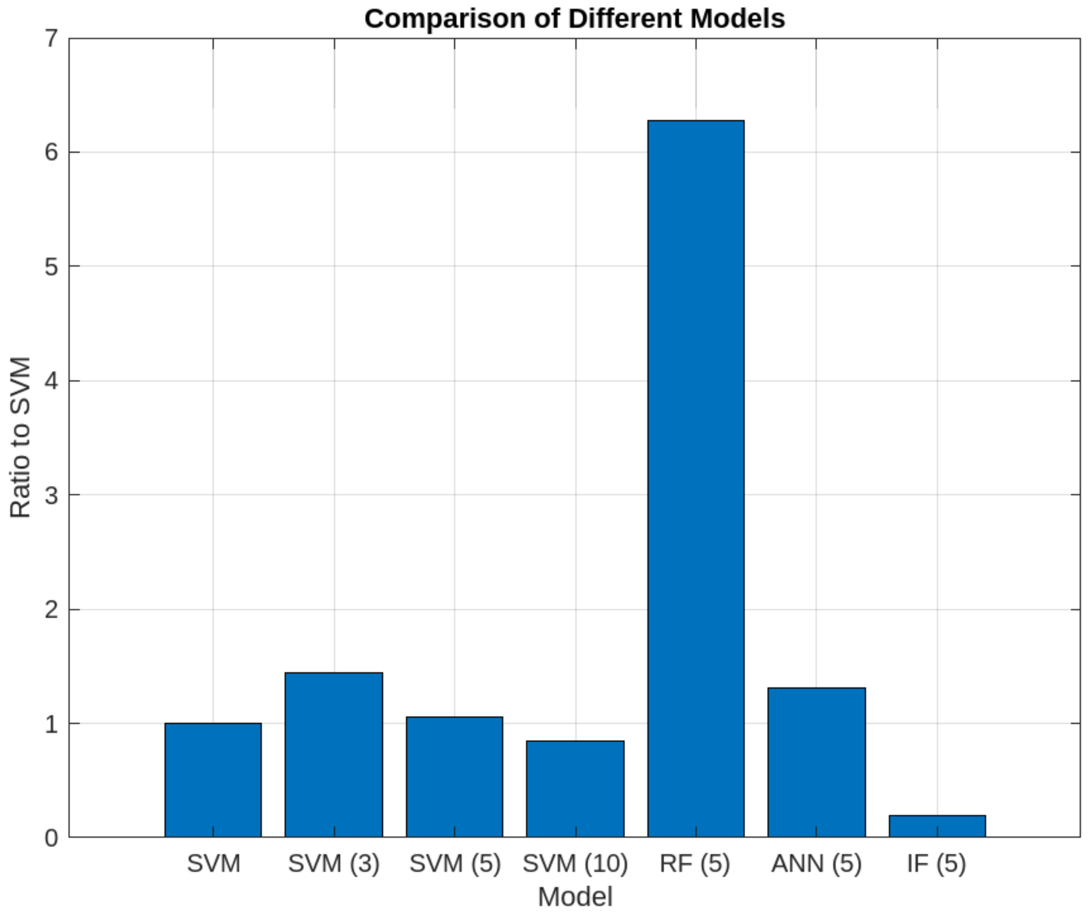
Table 3. SVM compared with other federated models.

Model	Total Delay (s)	Ratio to SVM	Peak Memory Usage (MB)	Peak Memory Per Node
SVM (C)	32	1	2,919	2,919
SVM (3)	46	1.44	3,503	1,168
SVM (5)	34	1.06	4,096	819
SVM (10)	27	0.843	5,420	542
ANN (5)	41	1.28	3056	613
RF (5)	201	6.28	2,059	418
IF (5)	6	0.19	2,050	410

Table 3 shows some interesting trends in both time and memory usage. The first quirk is that delay seems to go up before it eventually falls below centralised models, this is due to the fact that federated learning takes place in rounds



Comparison of Different Models
Peak Memory Per Node (MB)
0
500
1000
1500
2000
2500
3000
SVM
SVM (3)
SVM (5)
SVM (10)
RF (5)
ANN (5)
IF (5)
Model



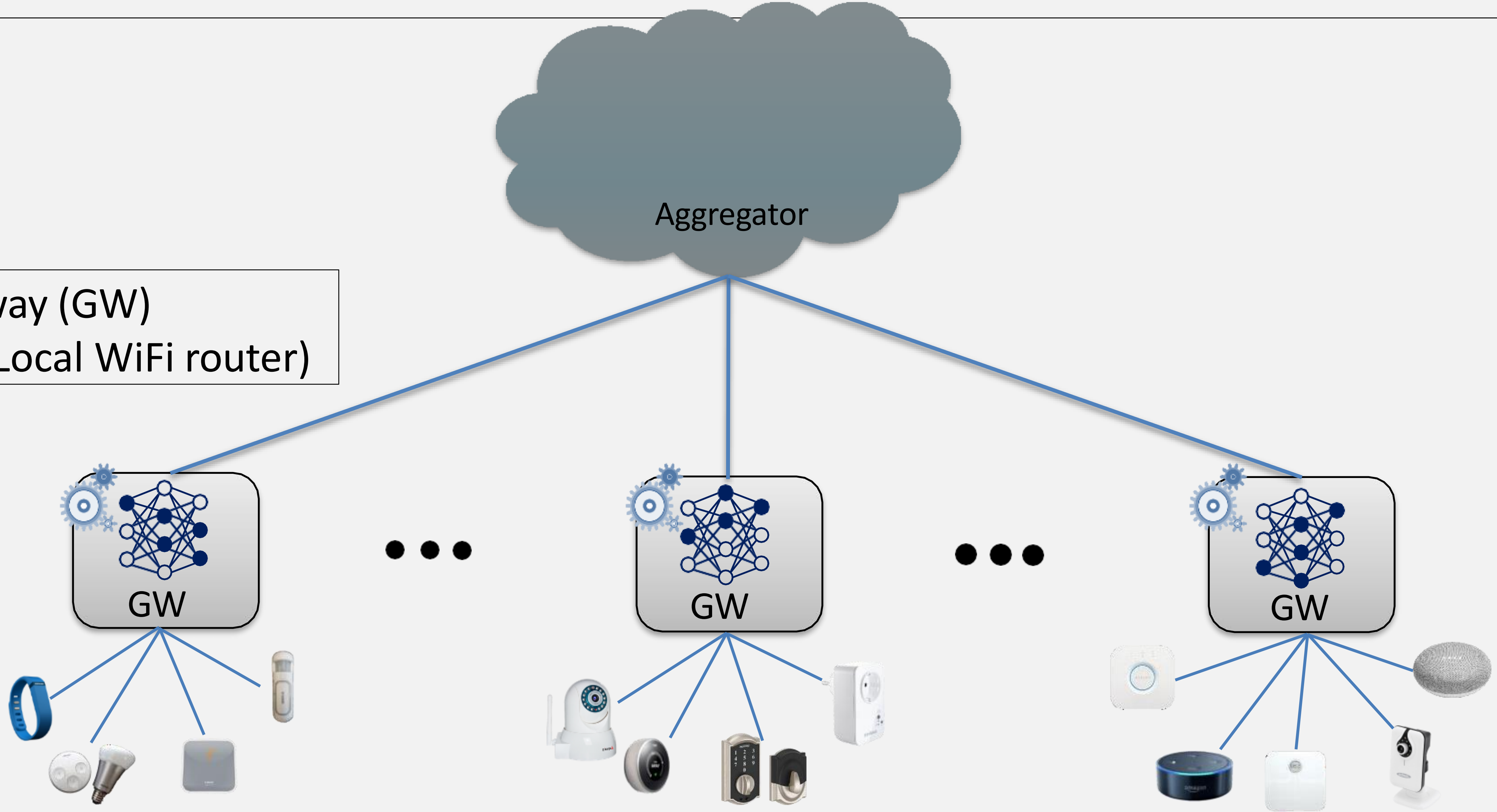
Comparison of Different Models
Ratio to SVM
0
1
2
3
4
5
6
7
SVM
SVM (3)
SVM (5)
SVM (10)
RF (5)
ANN (5)
IF (5)
Model

Conclusion

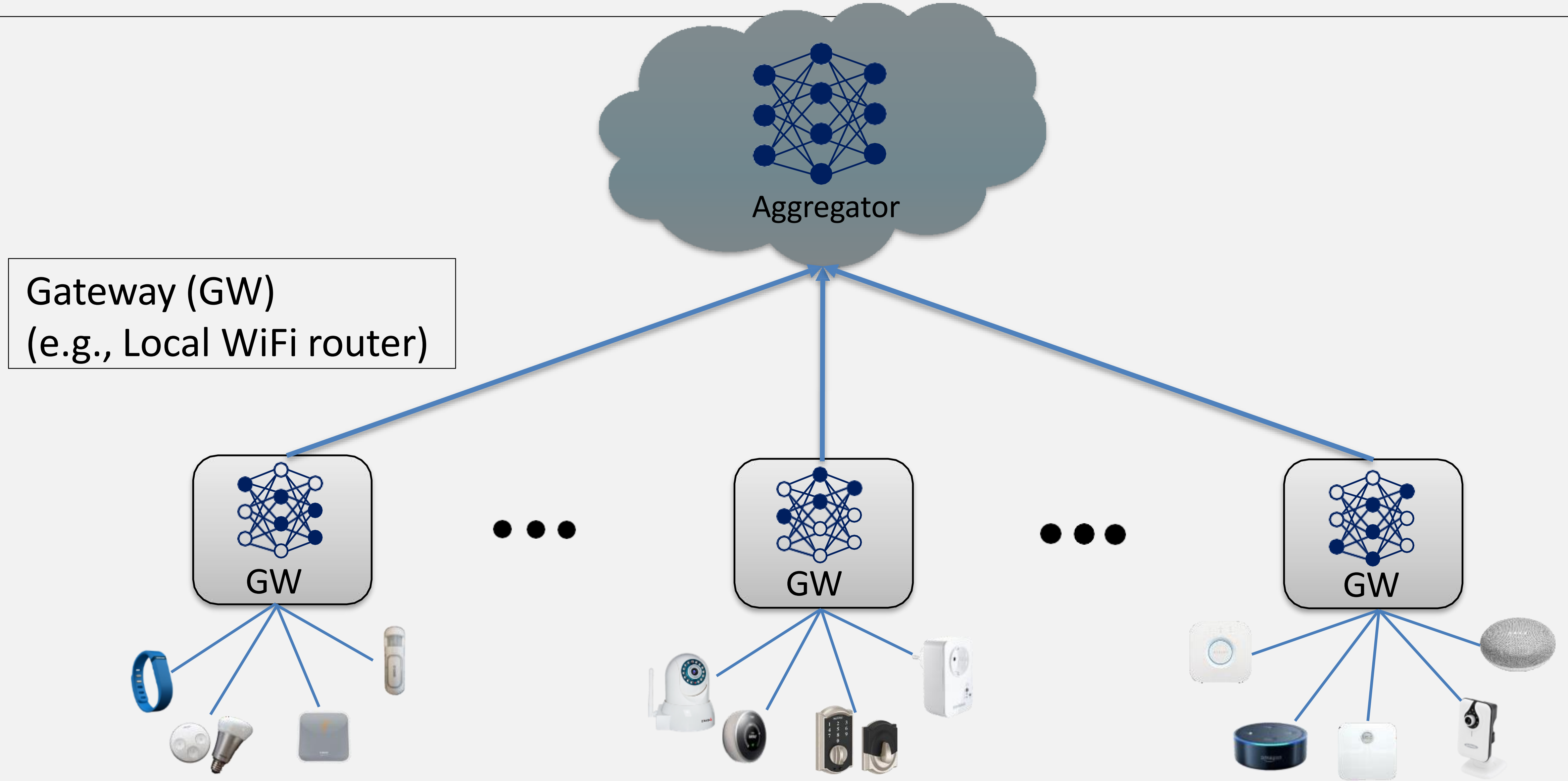
Feature	SVM	ANN
Decision Boundaries	Simple to moderately complex	Highly complex, non-linear
Data Requirements	**Performs well on small datasets**	Requires large datasets
Interpretability	**More interpretable**	Often a black box
Training Time	Slower for large datasets	Slower but scales better
Noise Handling	Sensitive to noise	Robust with regularization
Versatility	Limited to classification/regression	Extremely versatile
Scalability	Struggles with large-scale problems	Scales well with distributed systems
Real-Time Suitability	**Lightweight, fast prediction**	Can be resource-intensive

Backdoor Attacks on FL

Gateway (GW)
(e.g., Local WiFi router)

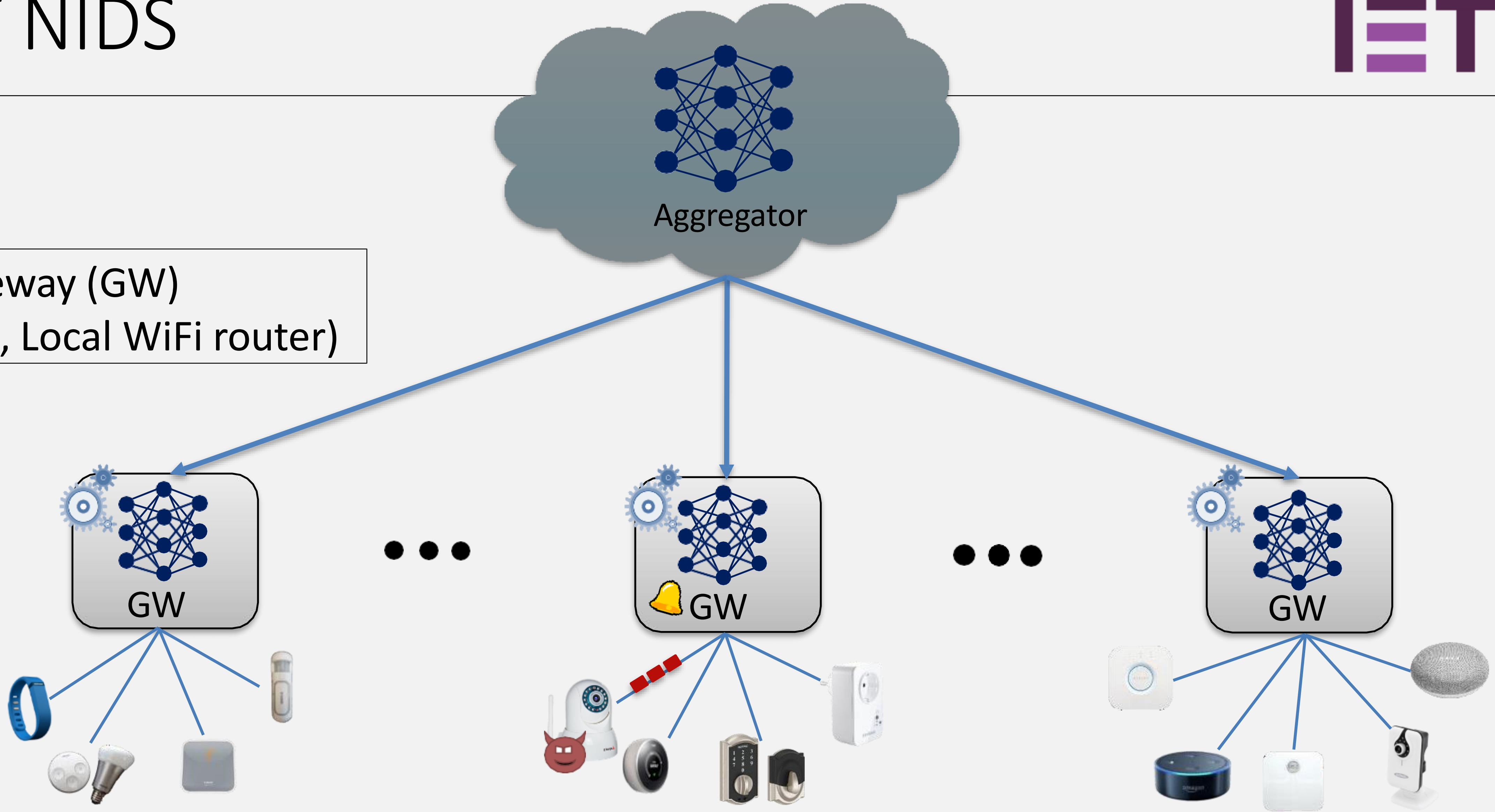


Backdoor Attacks on FL



IoT NIDS

Gateway (GW)
(e.g., Local WiFi router)



Backdoor Attacks on FL

Data label

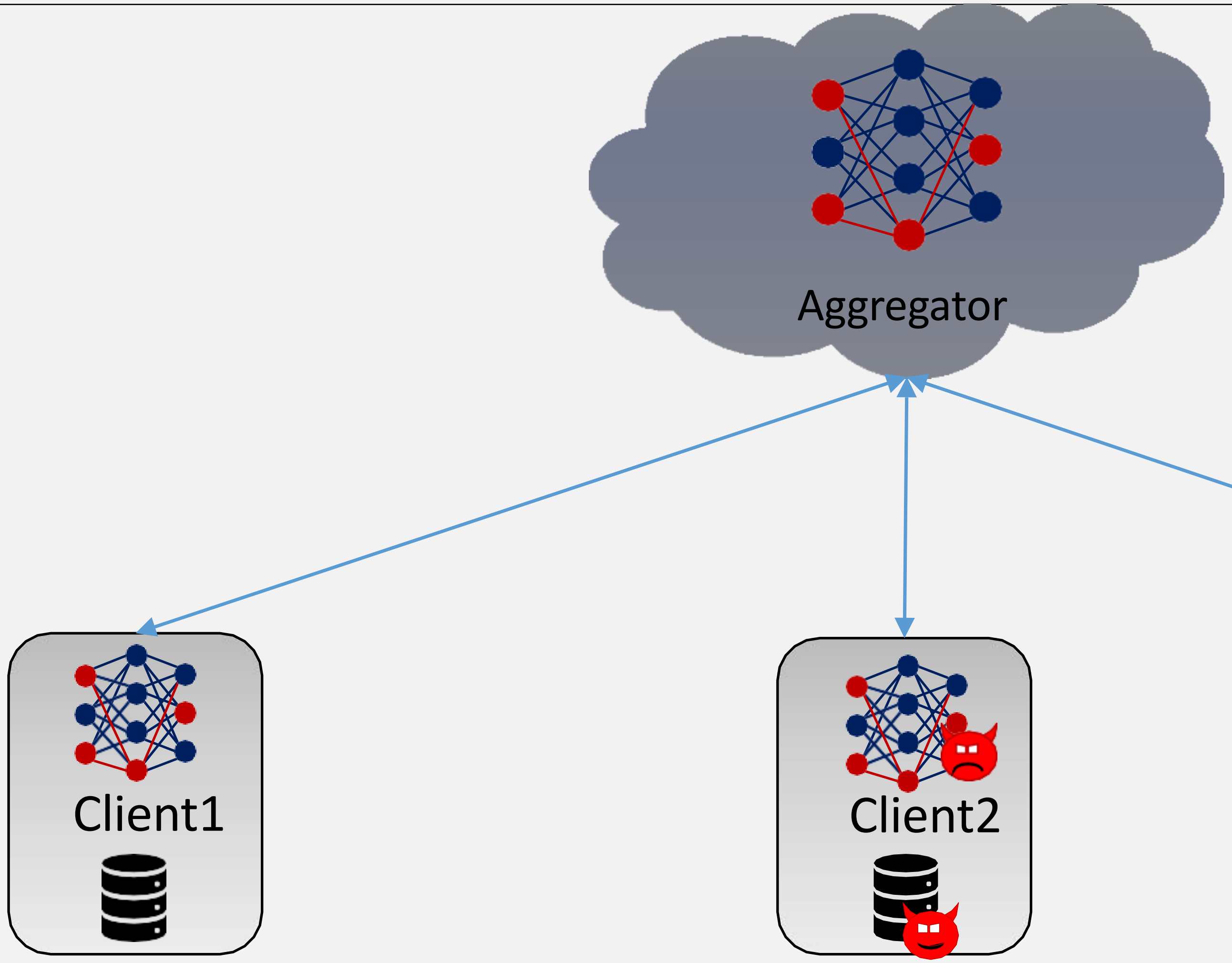
IoT malware detection

Inject malicious traffic, e.g.,
use compromised IoT devices

Image classification

Change labels, e.g., speed limit signs from 30kph to 80kph

Backdoor Attacks on FL



Attack Strategies:

1. Manipulate training data
2. Manipulate local models

Challenges and Future Directions

- **CHALLENGES:**
  - **Data Poisoning Attacks:** Adversaries may manipulate updates to disrupt the global model.
  - **Communication Overhead:** Frequent updates can strain networks.
  - **Device Constraints:** Ensuring compatibility with low-power devices.

- **FUTURE DIRECTIONS:**
  - **Federated Reinforcement Learning:** For adaptive and dynamic intrusion detection.
  - **Lightweight Models:** Development of models tailored for IoT constraints.

Thank you!

References

- Ferrag, M.A., Friha, O., Maglaras, L., Janicke, H. and Shu, L., 2021. Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis. IEEE Access, 9, pp.138509-138542.
- Nguyen, T.D., Rieger, P., Miettinen, M. and Sadeghi, A.R., 2020, February. Poisoning attacks on federated learning-based IoT intrusion detection system. In Proc. Workshop Decentralized IoT Syst. Secur.(DISS) (Vol. 79).
- Kaspersky (2021). Best Practices for IoT Security. [online] www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/preemptive-safety/best-practices-for-iot-security.
- Blog. (2016). Breaking Down Mirai: An IoT DDoS Botnet Analysis. [online] Available at: https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/?redirect=Incapsula.
- Intersog (2021). IoT Security Statistics: 6 Facts [Updated]. [online] Intersog. Available at: https://intersog.com/blog/development/iot-security-statistics/.