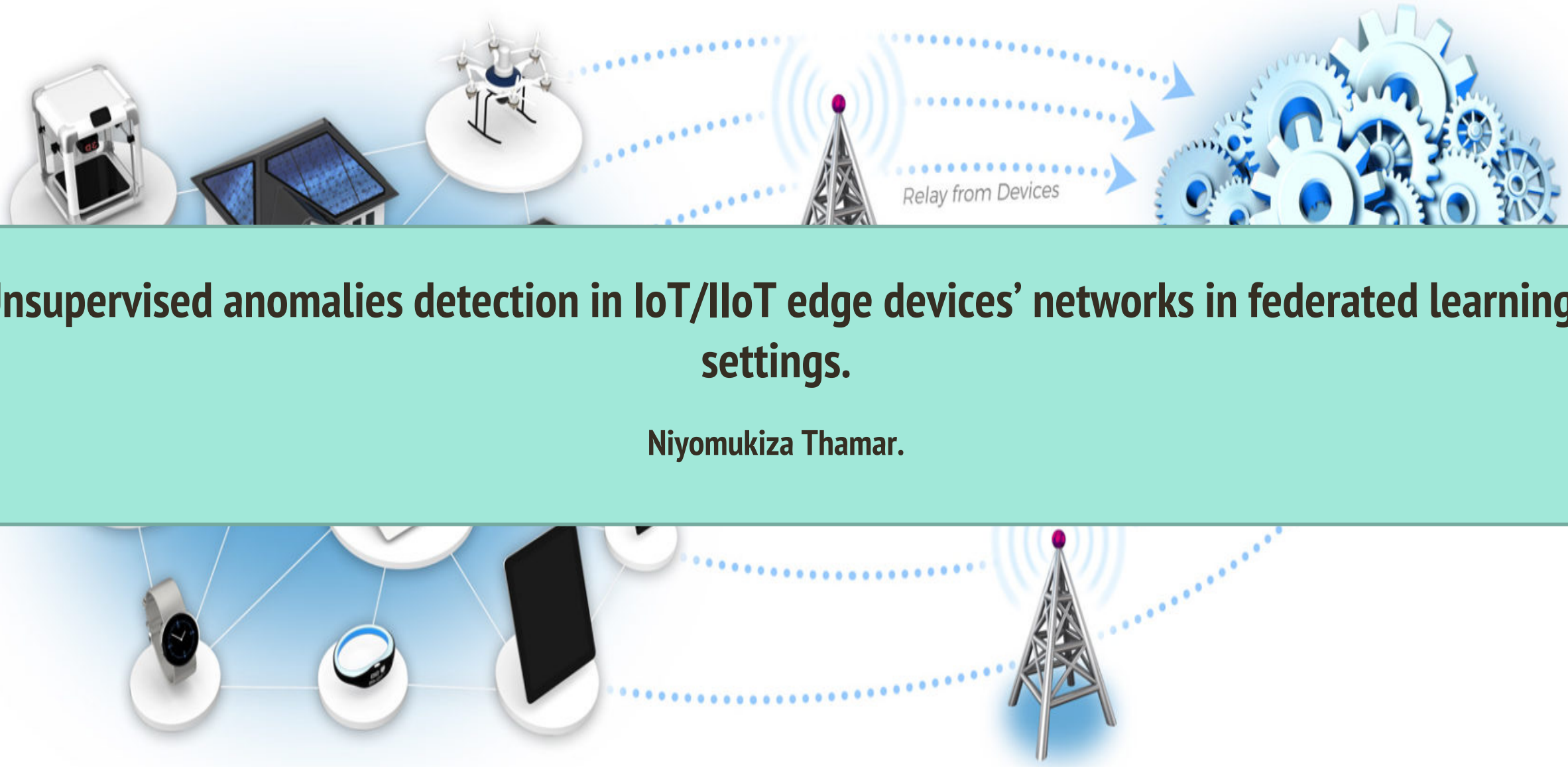


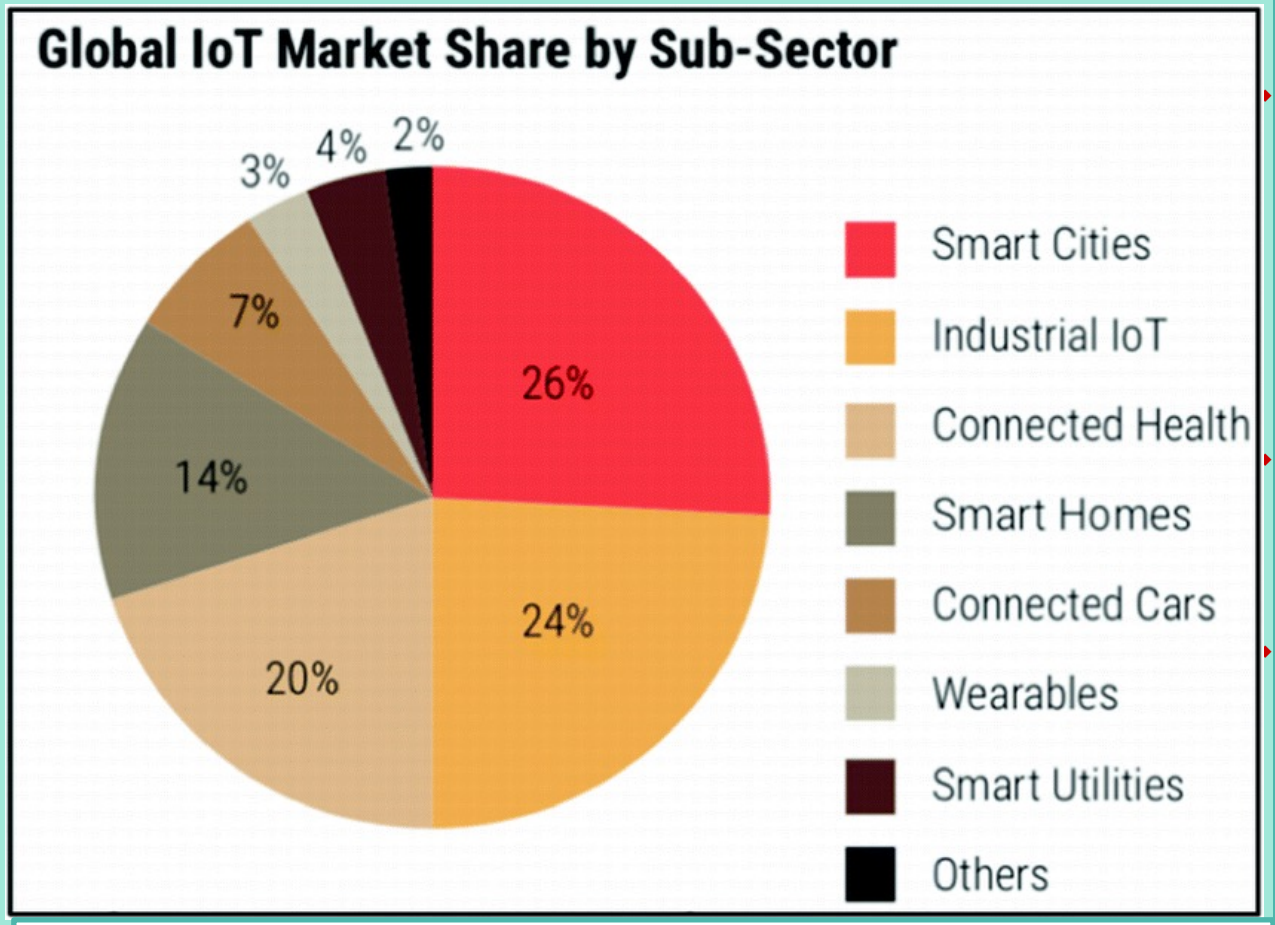
Unsupervised anomalies detection in IoT/IIoT edge devices' networks in federated learning settings.

Niyomukiza Thamar.

Outline

- Introduction
  - Anomaly detection approaches /Solutions
  - Motivation
  - The Project Objectives and goal
- Methodology
- Data Exploration
- Experiments and Results.
- Conclusion

Introduction



soure: growthenabler analysis

What is IoT :

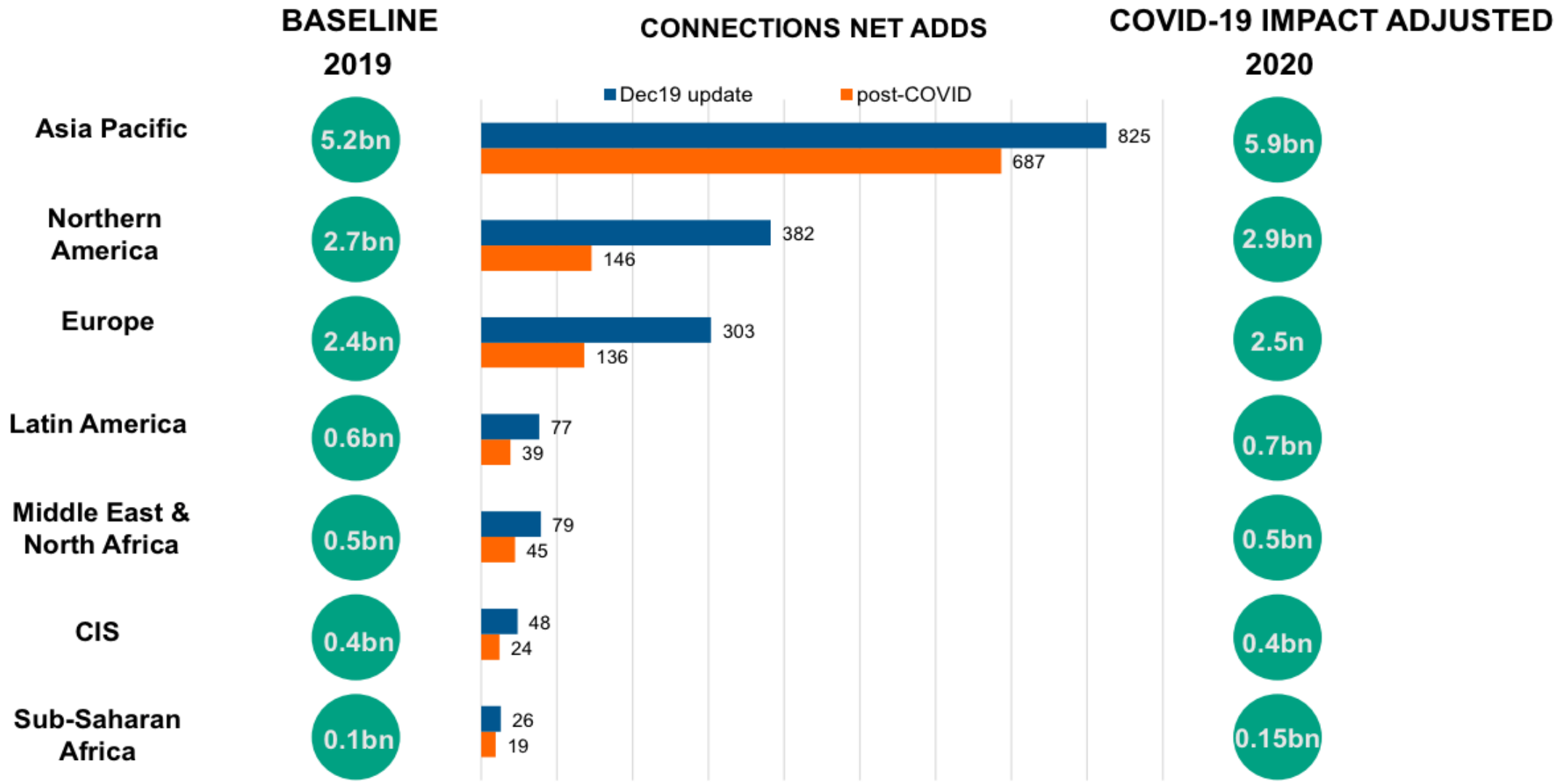
- The Internet of Things (IoT)
  - **physical objects that are embedded with sensors, processing ability, software, and other technologies,**
  - **connect and exchange data with other devices and systems over the Internet or other communications networks**

IoT devices have found their ways into every corner of humans' lives.

They are interconnected to collect and exchange sensitive information.

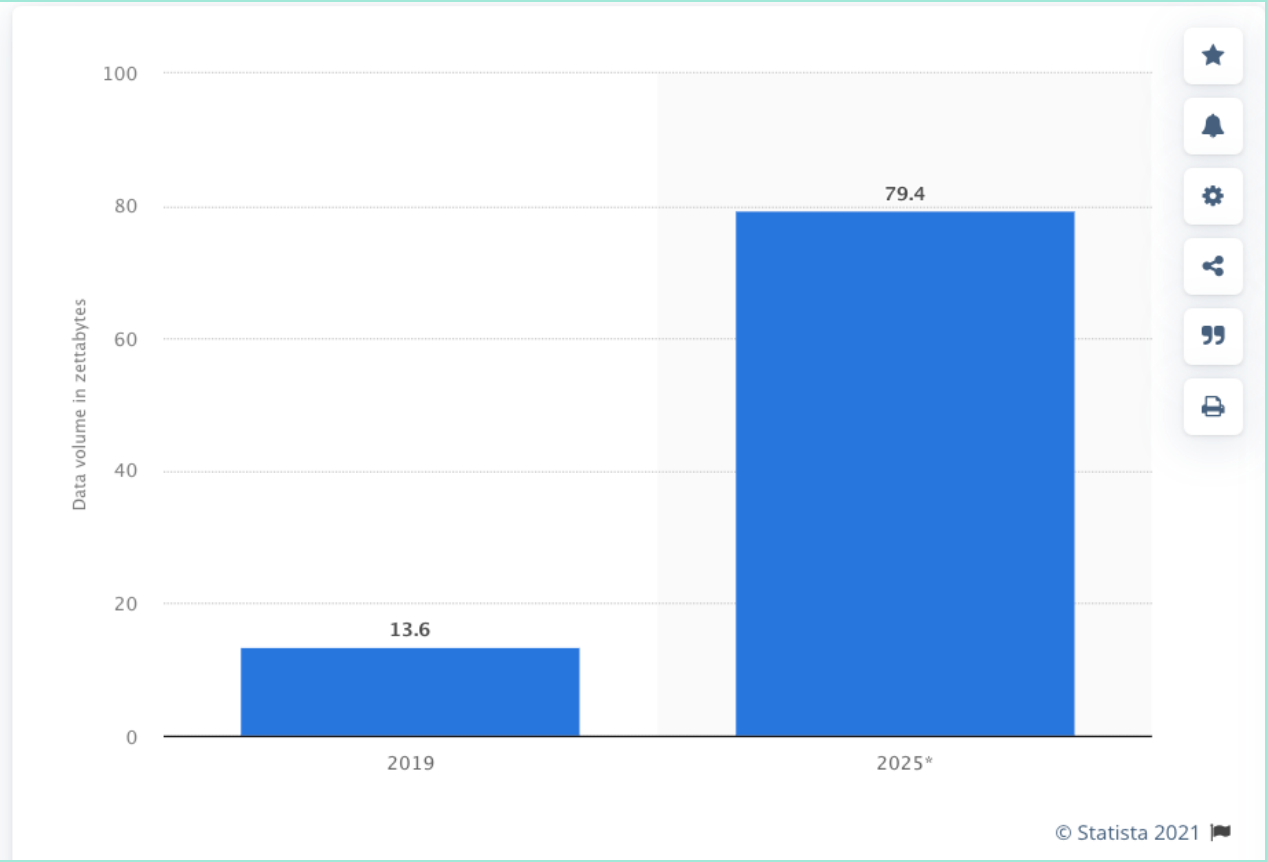
Covid impact on the growth of IOT devices market

IoT connections by region, 2019 – 2020 (pre and post COVID-19)



Source: GSMA Intelligence IoT Forecast, May 2020

Implications



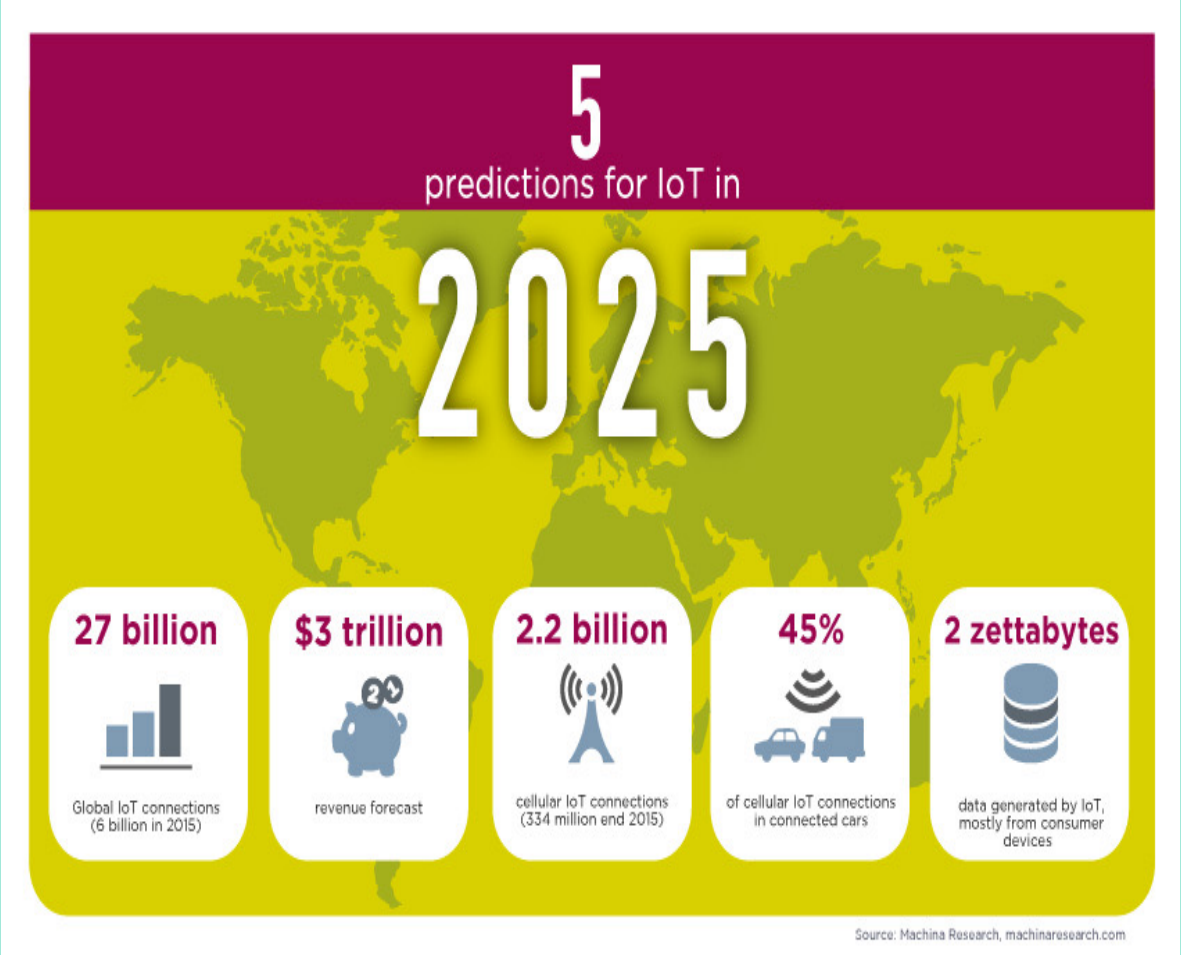
- **We must manage billions of connected devices.**

A storm of data:

By 2025 the amount of data produced by IoT devices will be 79.4 zettabytes [3]

- **IoT devices hold sensitive data**

Overview

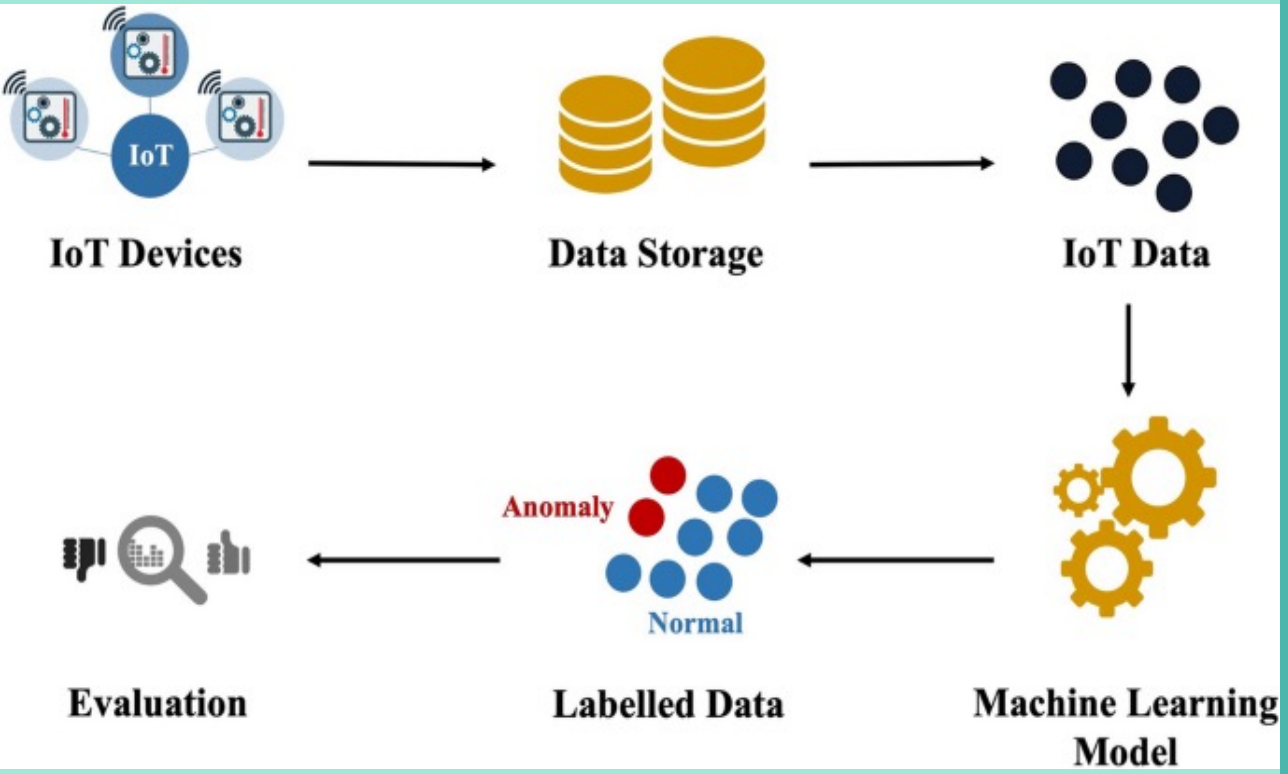


Their wide adoption and marked demand are leading to many many challenges.

- pressures the development teams.
  - re-using unverified code snippets [2],
  - insecure third-party libraries [3], and not following secure software development practices [4]
  - leading to producing inherently vulnerable IoT devices for consumer markets [5].

Thus, as interconnect devices grows on the network, attacks targeting them increases [2-5, 20].

Anomaly detection approaches



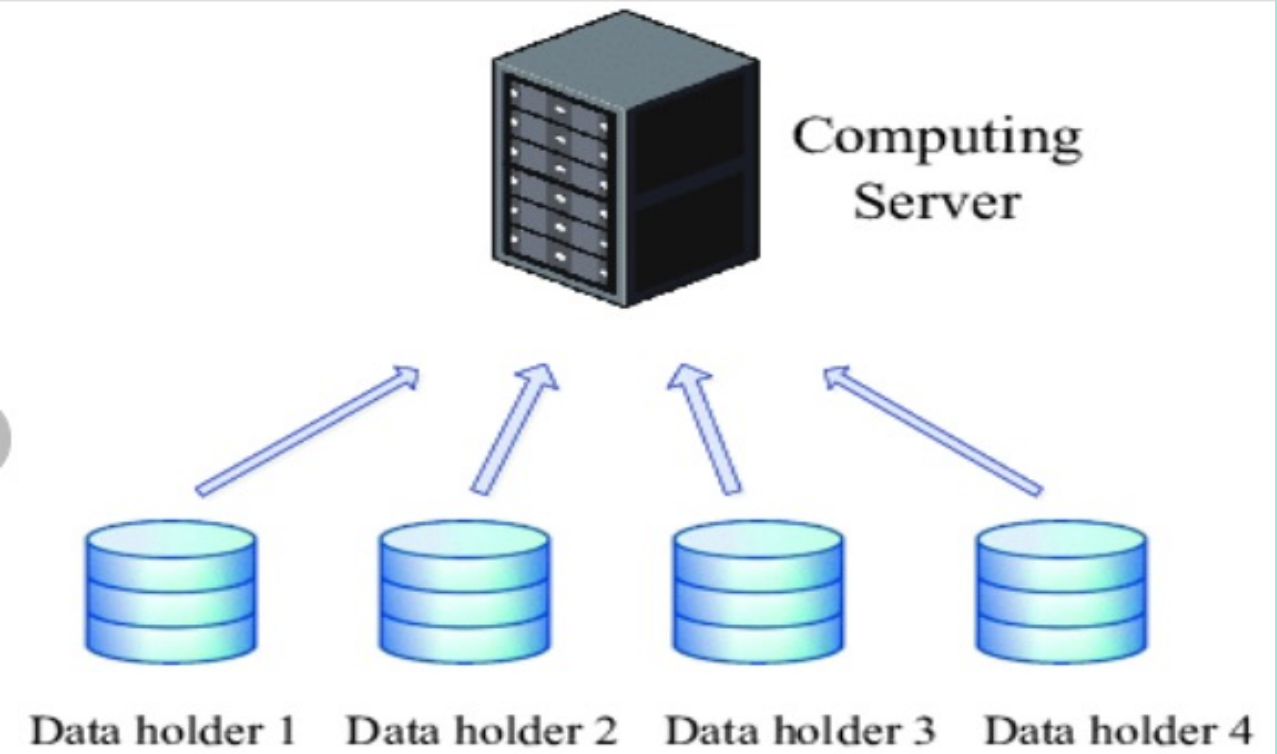
Source: https://link.springer.com/article/10.1007/s11277-021-08994-z

- **Centralized approaches**

  - ML/DL techniques have been adopted for the IoT security field for cyber-attacks as shown in [9,11,13,15,16]

  - Intrusion Detection Systems (IDS) has been the preferred approach. IDS studies the behavior of the normal samples through their features, and any deviation can be detected as suspicious action on the device.

Solutions cont'd



Centralized Multi-party Learning (Master-Worker Learning

Centralized approaches

- Intrusion detection solutions:

  - most of existing ML/DL approached depend on a central server, which gathers data from various IoT devices, and then trains global models. After this step, produced models are sent to each client that is concerned.

    - these clients transmit their live sensitive data to the server for behavior evaluation and intrusion detection [23].

Centralized approach issues for IoT devices anomaly detection.

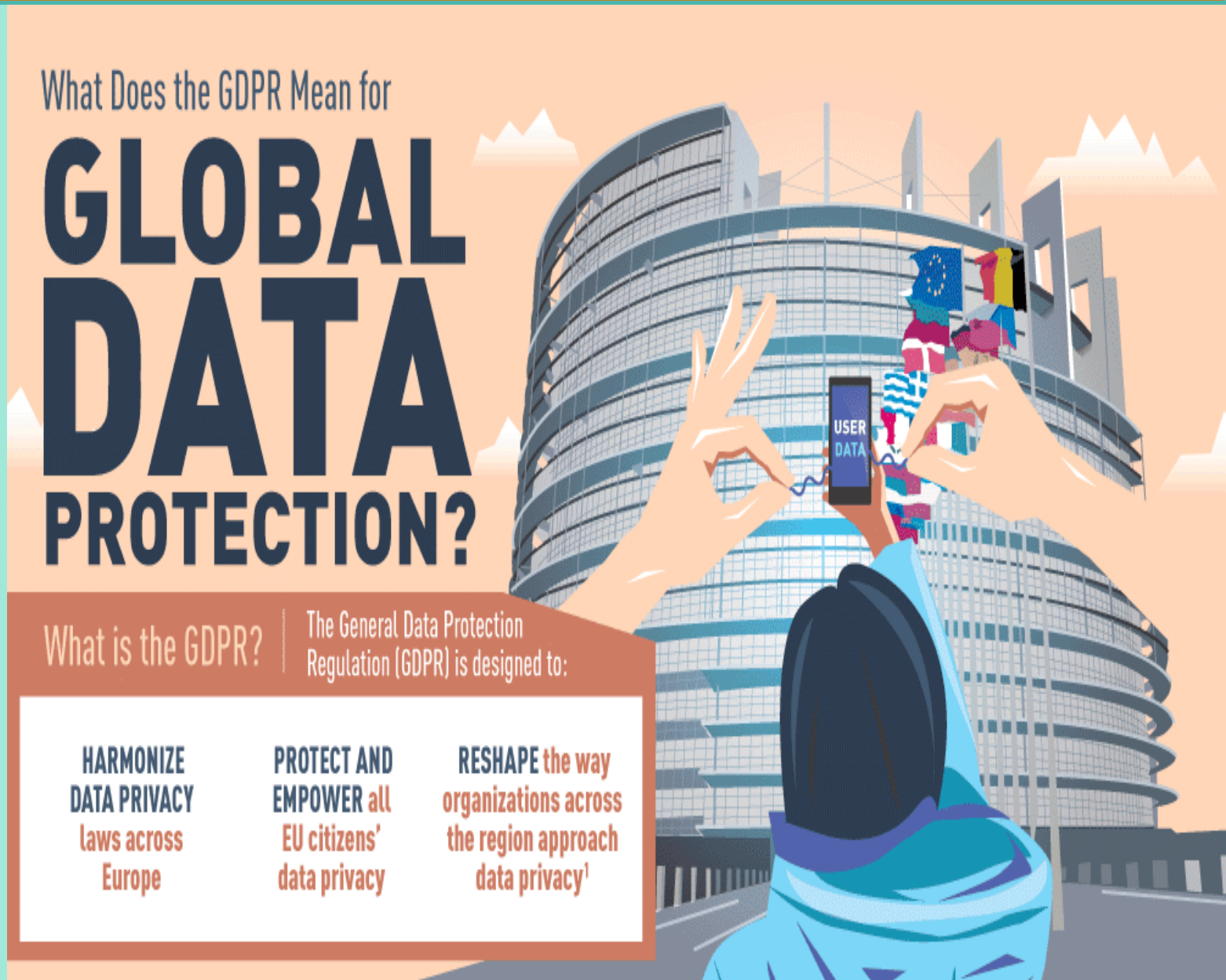
- **Communication overheads**
  - the communication protocol scale is much smaller due to restrictions of packets size.
  - The centralized ML/DL techniques requires to send huge data over the network,
    - will cause the communication overheads because of limited communication resources.

- **Privacy concern.**
  - **Data leakage**
    - **for scenarios where IoT device's behavior include confidential data that would impact the security and privacy of owners when captured by attackers, owners are reluctant to provide their data to be used for training.**

Centralized approach issues for IoT devices anomaly detection

Data regulatory

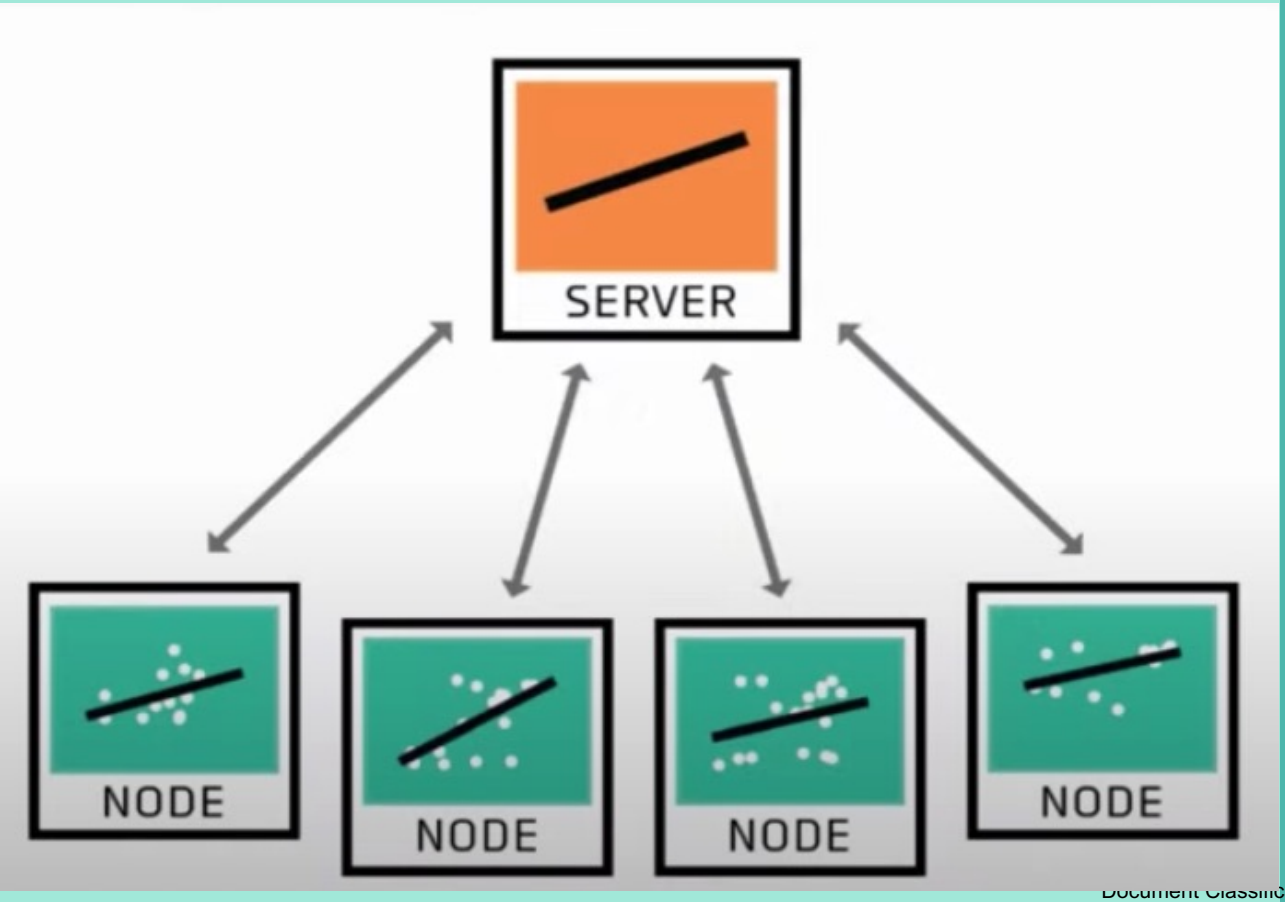
The General Data Protection Regulation (GDPR)



What could be the solution?

- Distributed learning approaches.

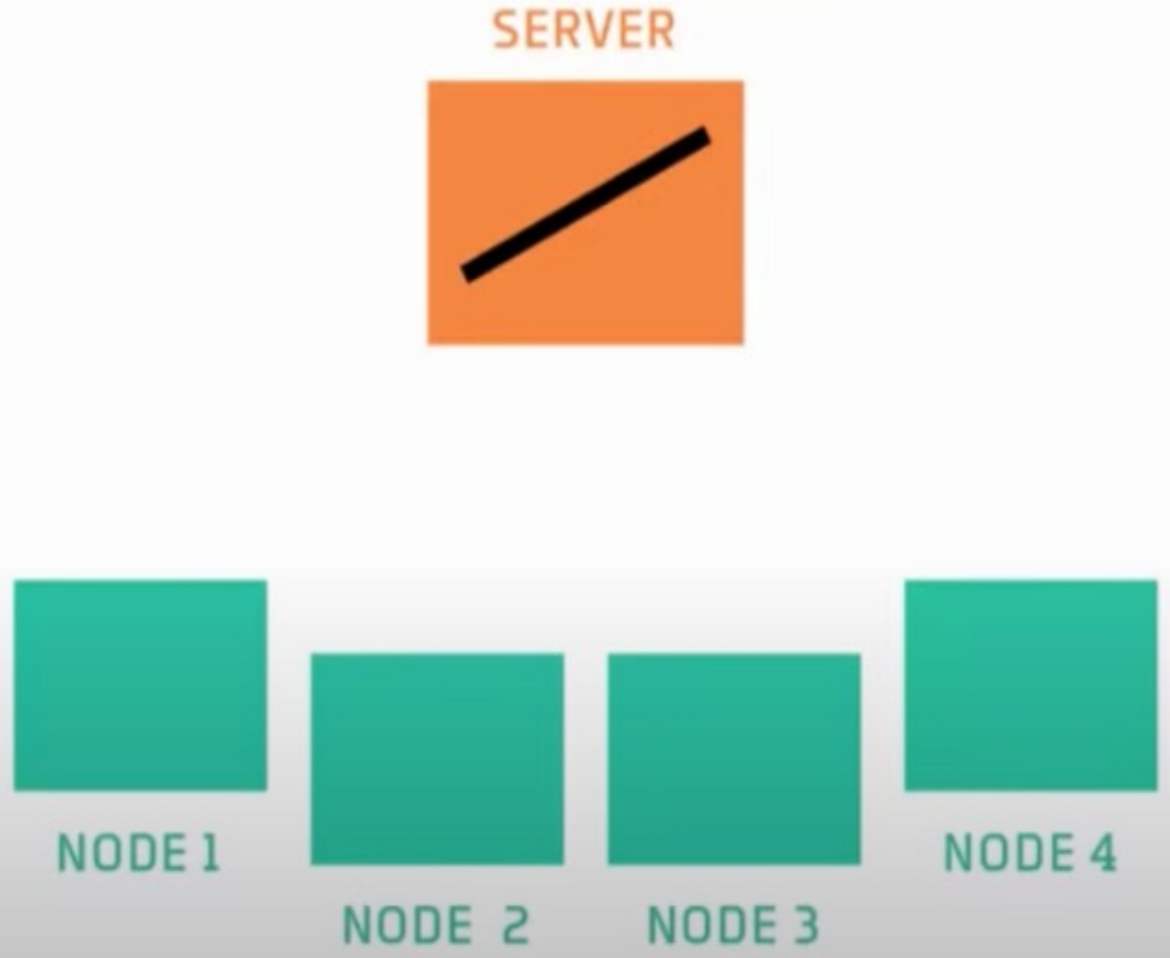
Distributed ML.



- **Federated Learning**
  - **Machine learning on decentralized data**

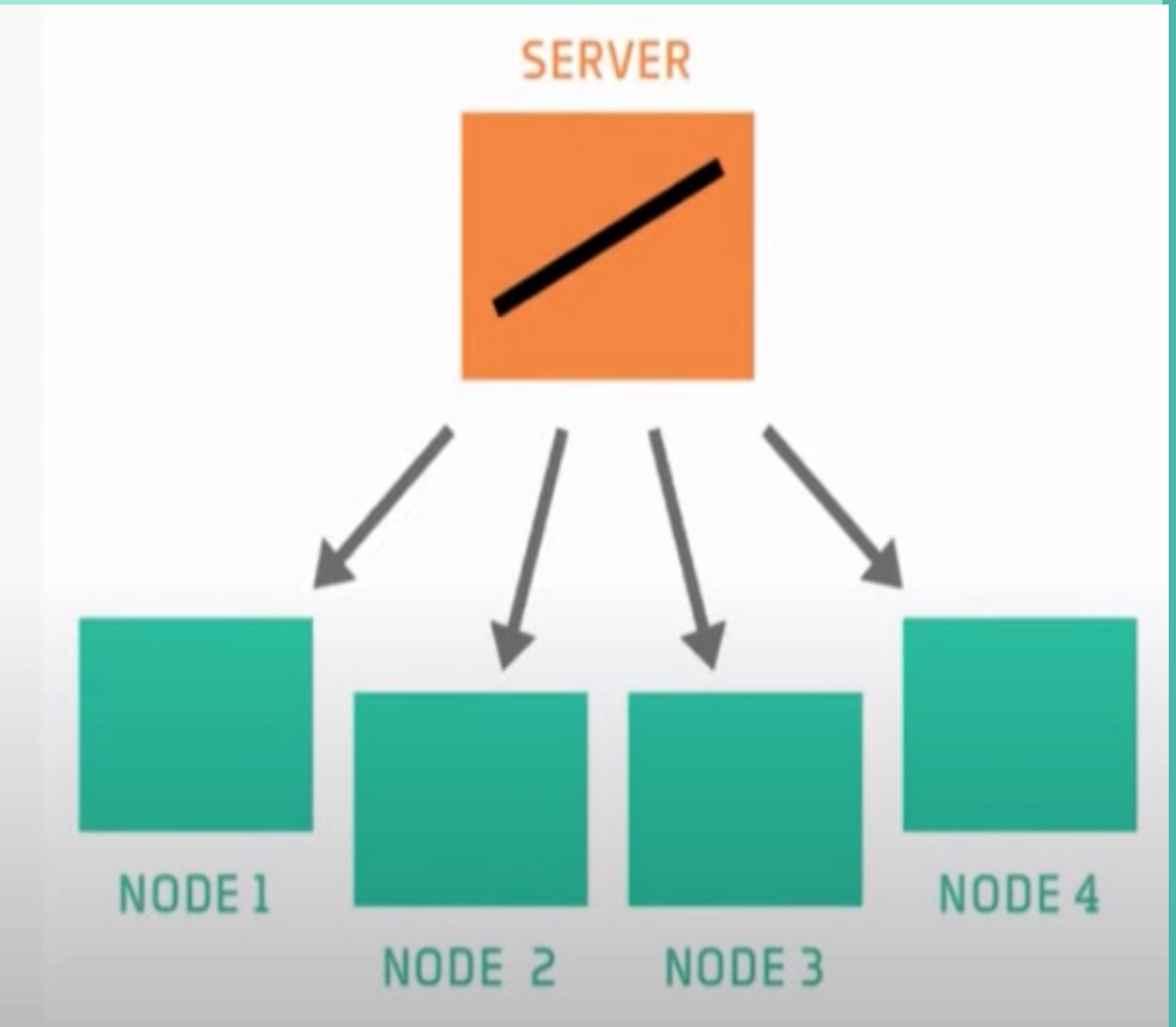
Enable **edges devices** to do **state of the art ML without centralized data** with **privacy** by default**. (Google I/O'19)**

Synchronous Federated learning



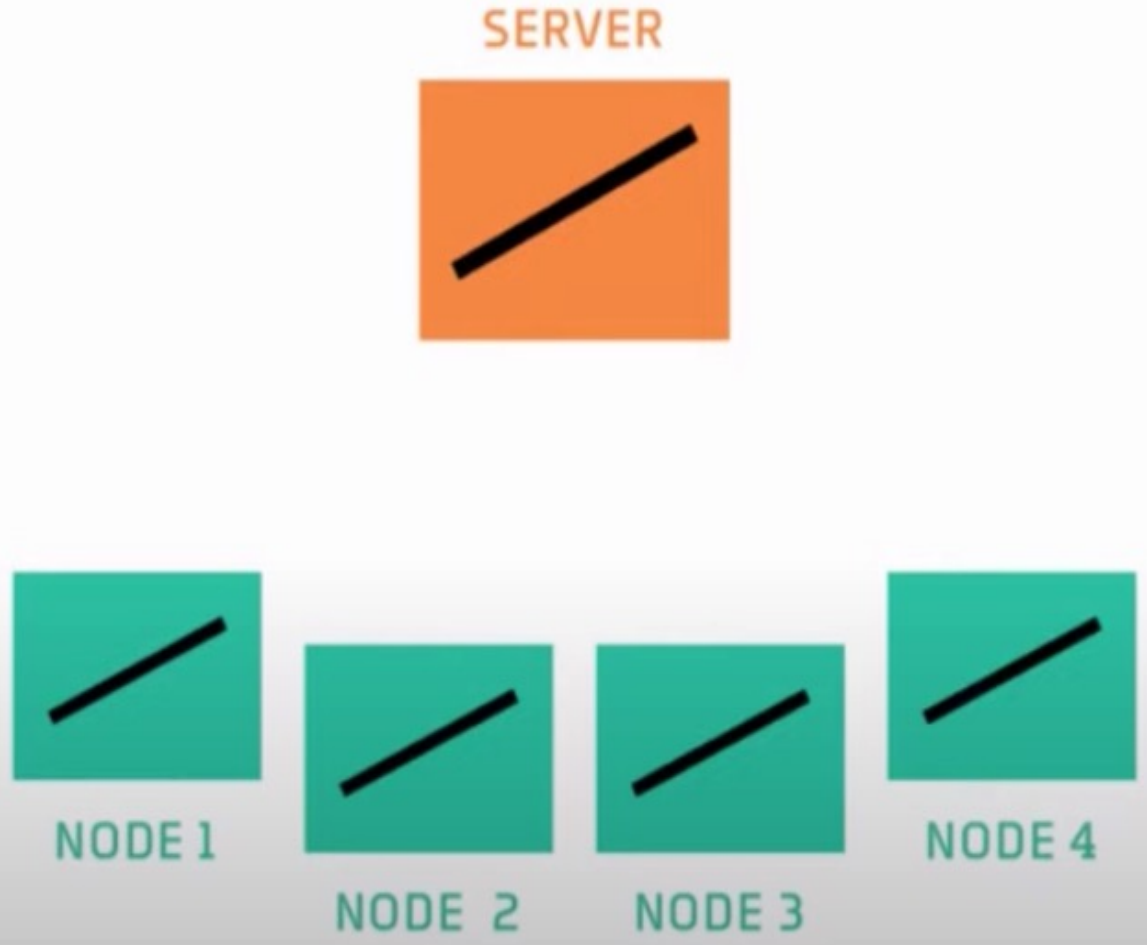
- **The server have a generic model**
  - **It initiates an untrained model**
  - **Wait all devices to send back the model.**

FL



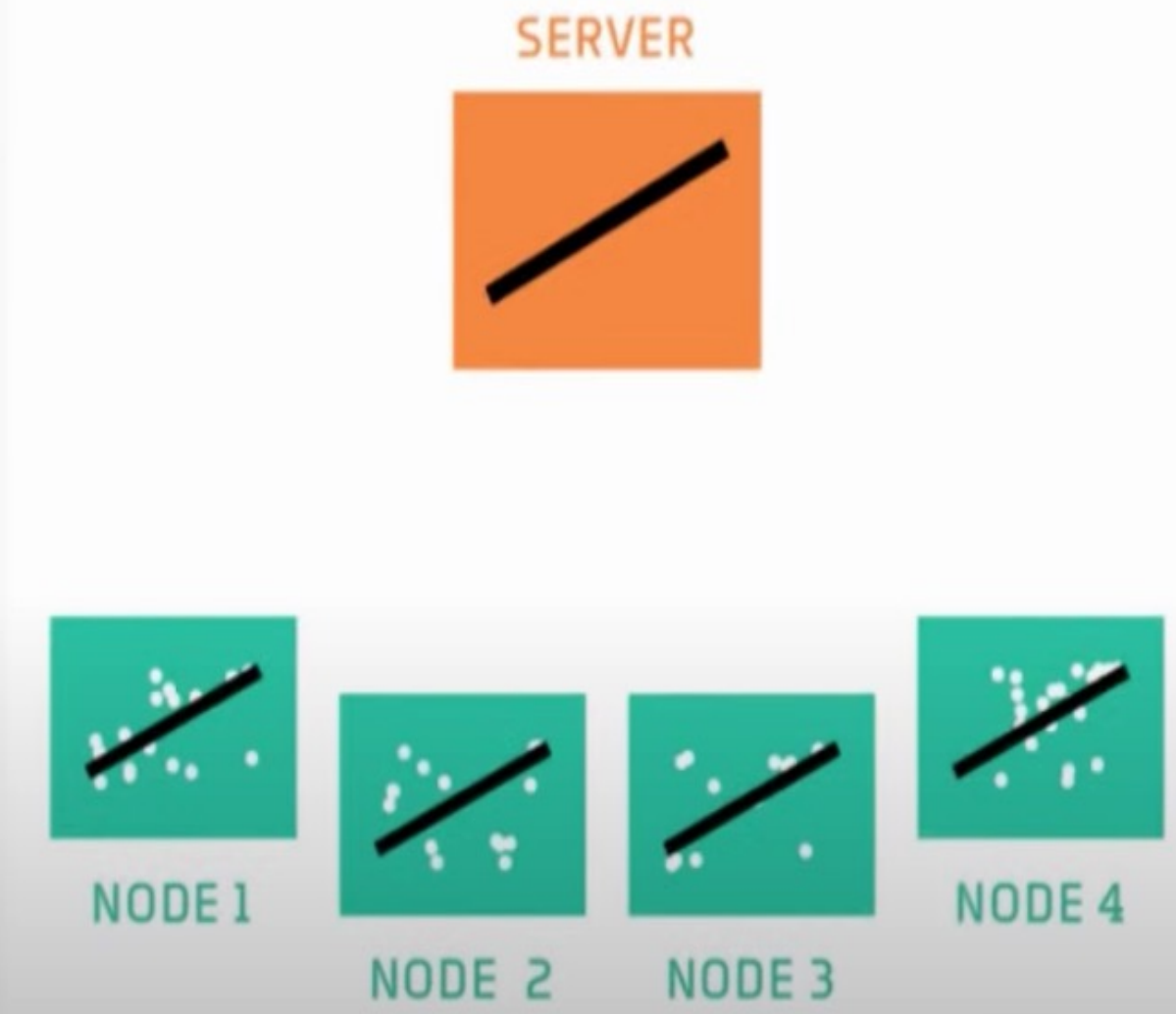
Sends the copy of the model to the edge nodes

FL



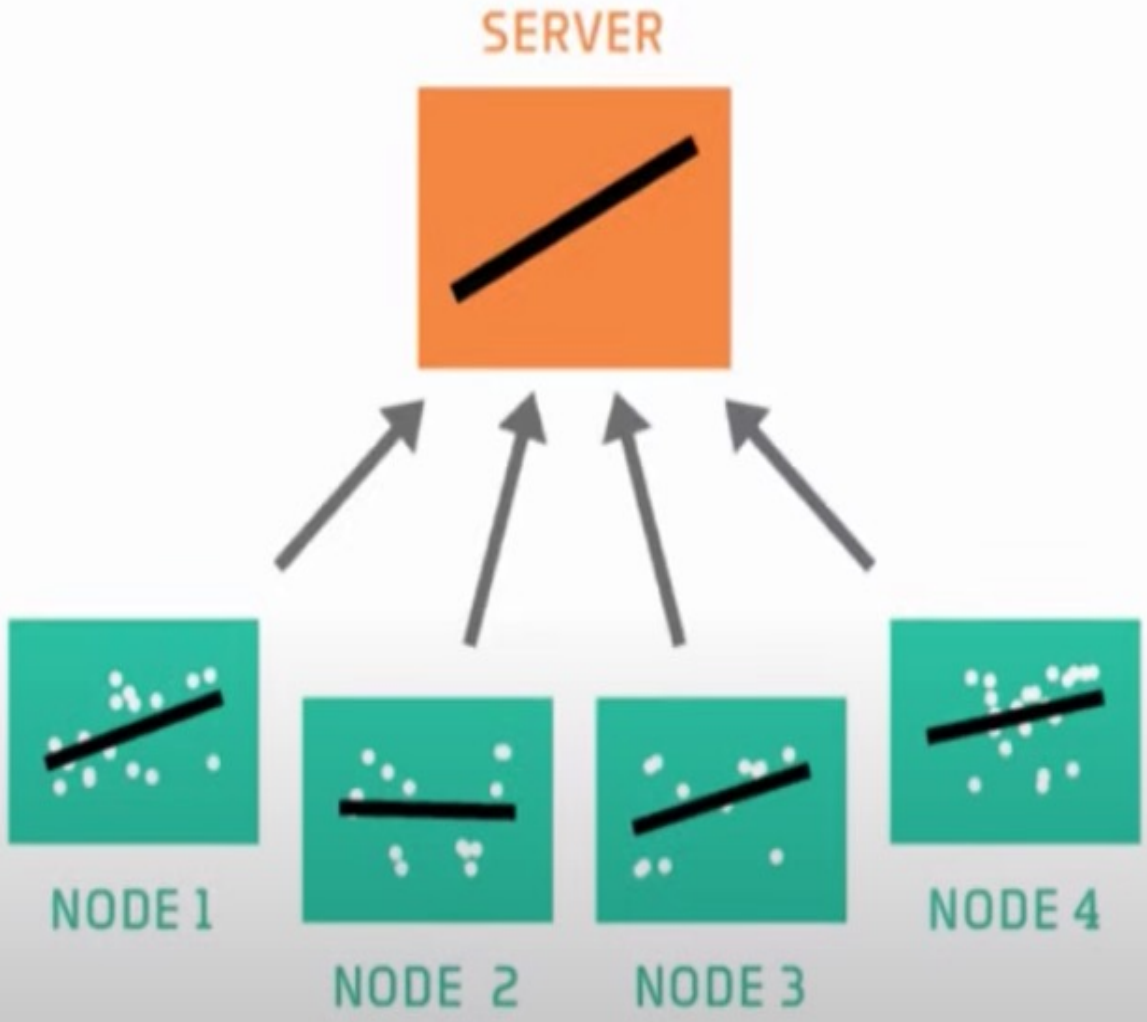
- Participants’ nodes have untrained model

FL



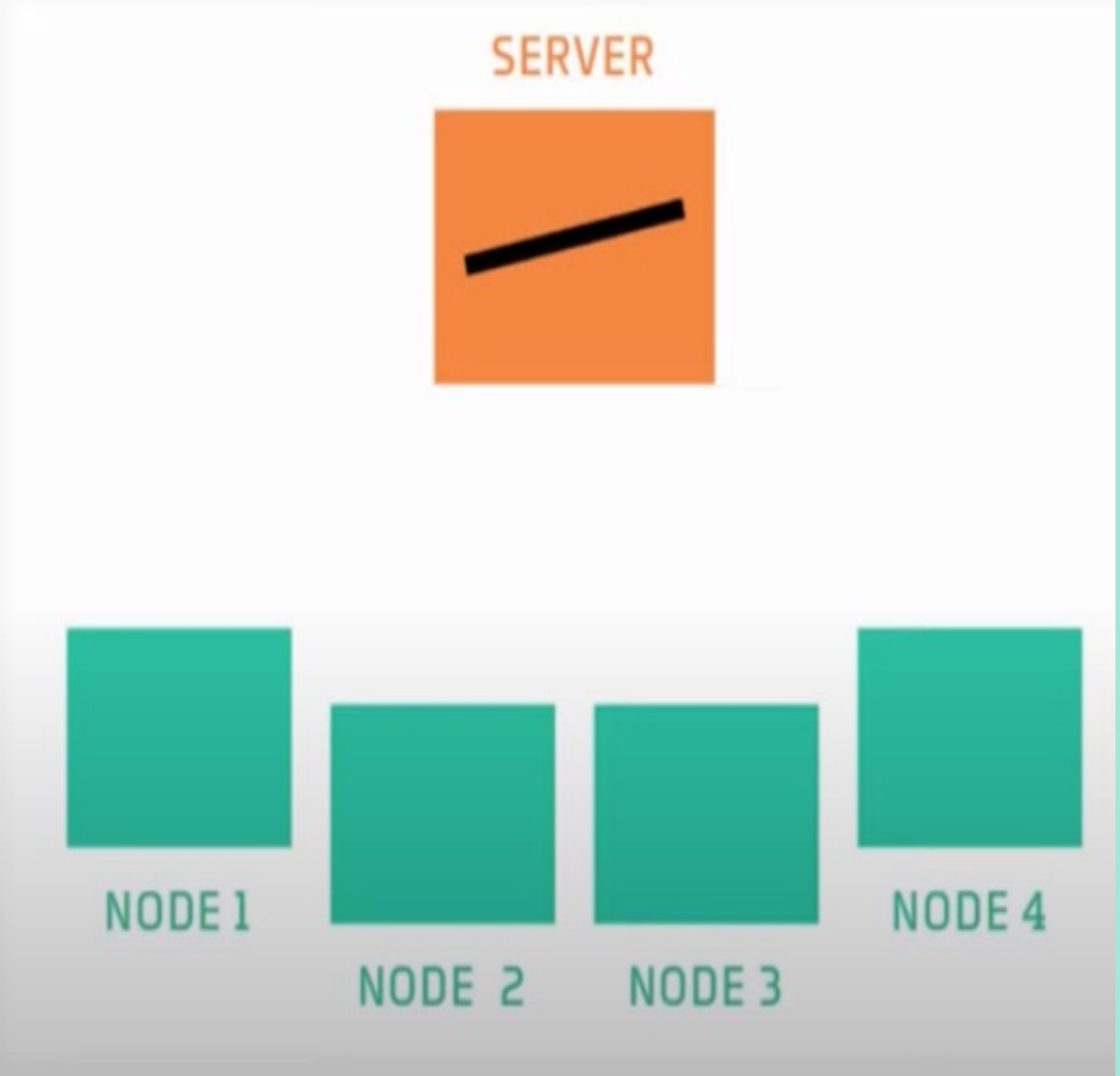
- Nodes have data on which to train the model
- Each node train the model to fit their unique data

FL



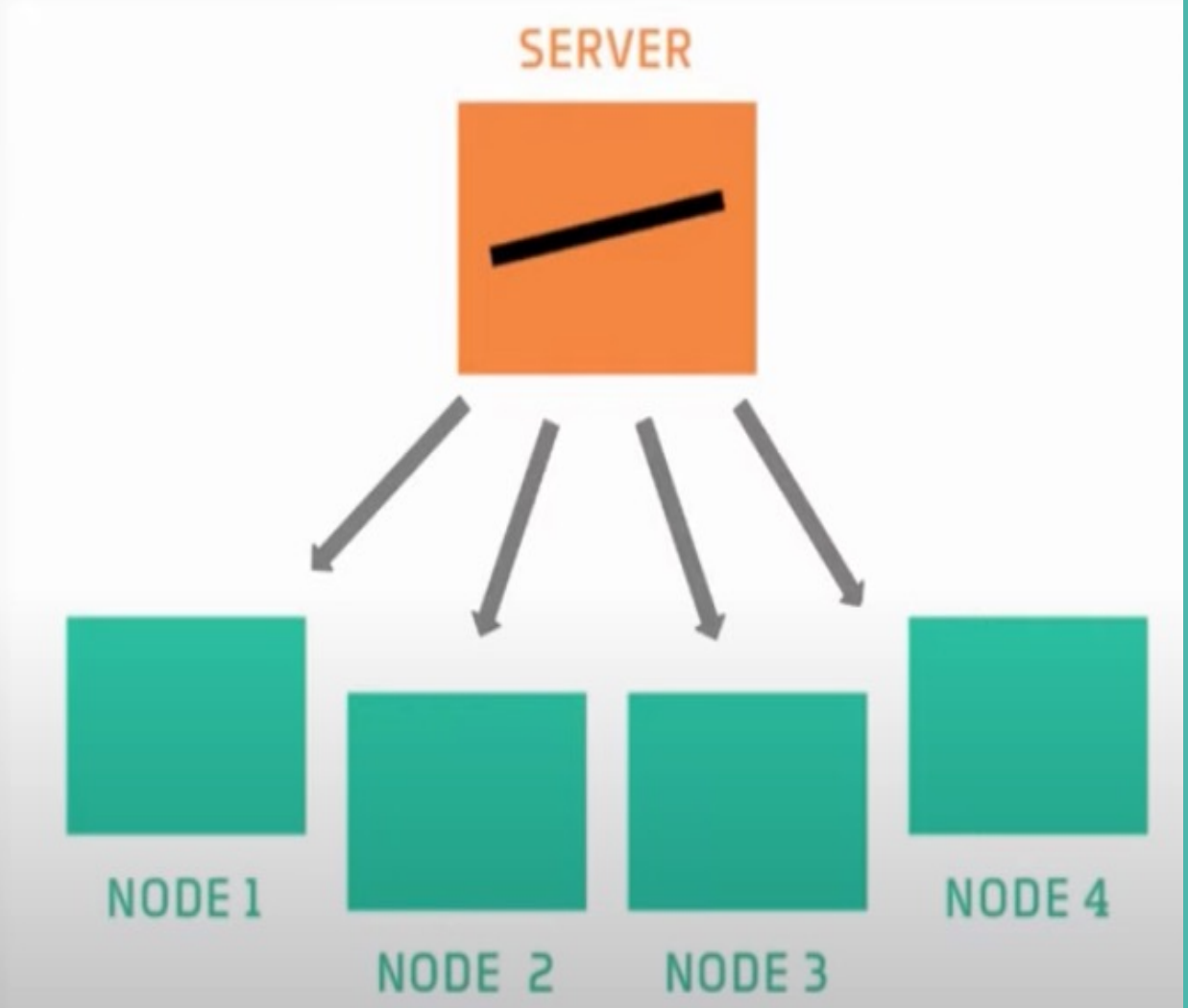
Each node sends a copy of its trained model and weights back to the server

FL



- The server combines these models and calculate the average

FedAvg algorithm



- At this step, the server has the model that captures the pattens in the training data of all participant nodes.
  - The steps are repeated in multiple rounds until a desirable accuracy is achieved.
  - Thus, FL can be an important distributed ML approach to secure IoT devices

FL – Malware detection in IoT networks

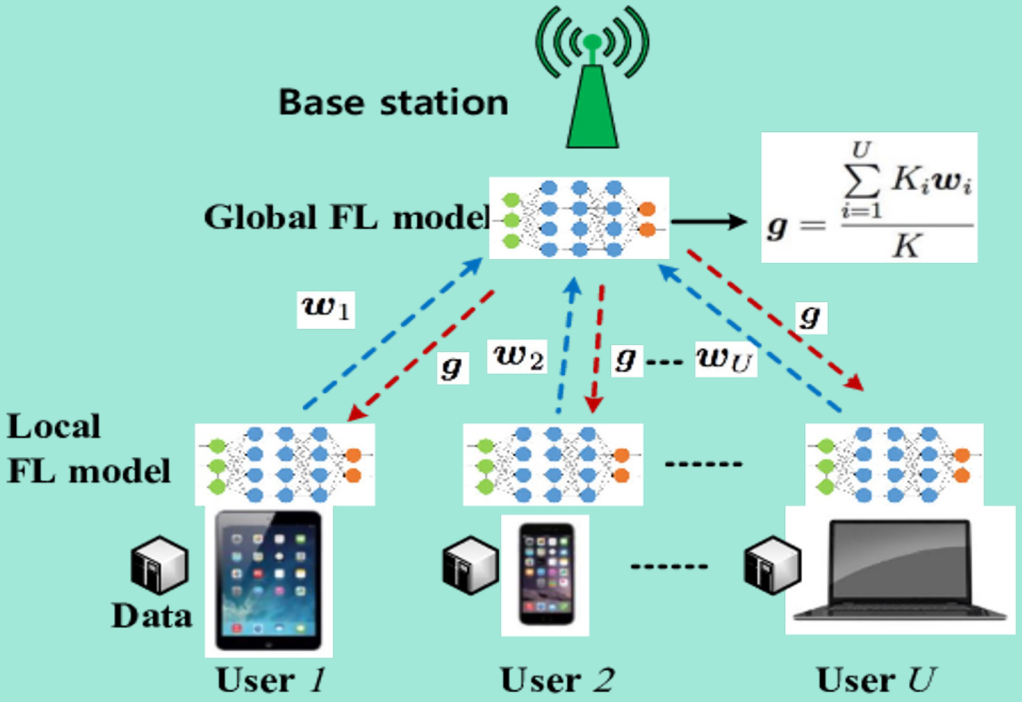
solutions cont'd

Enforcement from GDPR

- To ensure data privacy and securing IoT networks,
  federated learning have been designed [7, 17-21].
- Nguyen et al. [7] propose a synchronous FL Intrusion Detection System based on anomaly detection for IoT.
  - Different security gateways, each monitoring the traffic of one particular device type,
  - locally train Gated Recurrent Unit model were used.

Cont'd

Literature review



- K. Yadav et al. in [30] applied have applied the unsupervised synchronous Federated learning for detecting anomalies in IoT devices without compromising the data privacy,
- however, they used dataset that does not contain IoT and IIoT traffic to train and evaluate the model.

Statistical Heterogeneity

Issues

Challenge of IoT data anomaly detection:

- Non-IID - Non-independent and identically distributed (Non-IID) data

Motivation for the project

- data legislators and regulatory agencies have been putting a lot of effort into making sure that personal data is secured
  - data gathering even more difficult [3, 34, 35].
- Industries reluctant to share their data due to peer competition, privacy concerns, and other potential concerns [20]
  - gathering data from different reliable sources, especially for IoT devices that hold critical data for their owners, is almost impossible if not costly.
- For this reason,
  - the ML models built by utilizing distributed datasets are the possible solution
- Furthermore,
  - as the edge device architecture evolves, the attacks against them evolves making the network cyber-attack flow behaviors change leading to high false negatives if the intelligent intrusion detection systems used have been trained and tested on datasets that do not mirror modern attacks.
  - Thus, evaluating FL model, although it has the benefit of data privacy preserving needs to be performed on modern datasets that reflect modern IIoT attacks in an unsupervised manner.

Problem statement.

- To comply with data security, synchronous federated learning (FL) techniques for securing billions of vulnerable IoT/IIoT edge devices' network, has started to gain popularity.
- FL models for IoT/IIoT edge devices' network are trained and evaluate on old datasets .
  - most of those research has been tested on datasets that are not representing modern IoT/IIoT devices and these devices' architecture have been growing as the technology advances.
- Moreover, new attacks also evolve making it impossible to detect attacks that are specific to modern IIoT edge devices.
  - it is very important to use datasets that closely mirror real-world IoT/IIoT applications.
- datasets are generated across heterogenous edge devices and are unlabeled.
  - Unsupervised FL models trained and evaluated on modern datasets are needed

Project Objectives

- Explore the types of attacks targeting IIoT devices layers specially at the network layer.
- Investigate different approaches used for securing IoT devices at the network layer such as machine learning as well as deep learning approaches and their shortcomings as IoT devices' security is concerned.
- Investigate how Federated Learning (FL) has been adopted for intrusion detection in IoT/IIoT devices and explore the possibility of using its privacy enhanced feature to detect malware with improved training convergence and model accuracy that affecting the modern IoT devices due to the emerging technologies.
- Train and evaluate on a recent dataset that have recent IIoT attacks by using unsupervised federated learning setting for malicious network flows of IIoT devices.

Project Goal

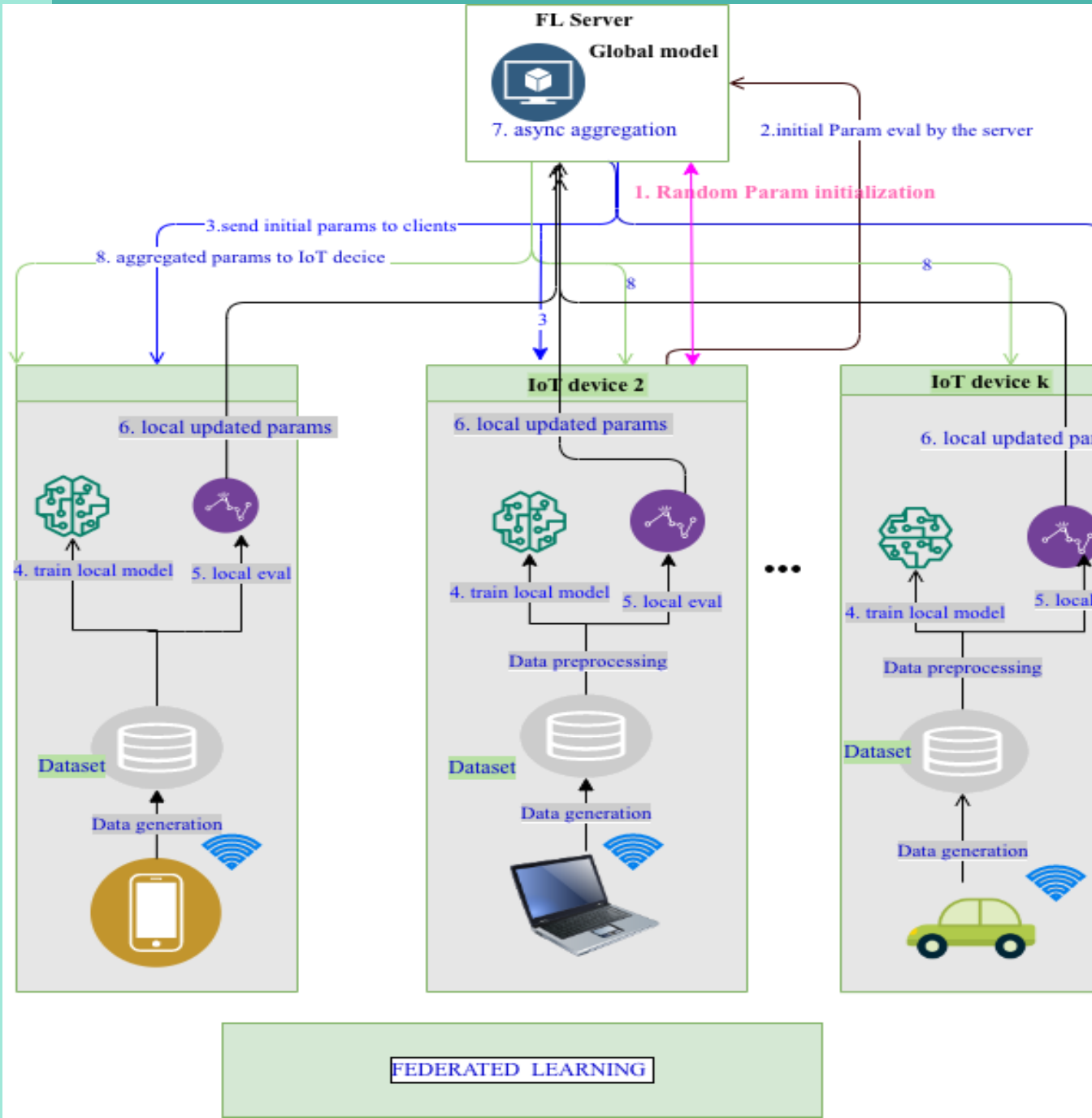
- Given that most prior research that have applied FL for intrusion detection in IoT networks, our project aim is planned as follows:
    - first, train and evaluate an unsupervised deep auto-encoder ML learning FedAvg on a modern IoT/IIoT dataset and assess its performance in regard of unsupervised centralized approach.
    - design, train and evaluate an unsupervised deep auto-encoder federated learning FedAvg on a modern IoT/IIoT dataset.
    - Finally, assess its performance in regard of unsupervised centralized approach on the recent real-world dataset. Model performance comparison with vanilla FedAvg model will be executed.

Architecture / Design

Detailed view of the client architecture during training and evaluation.

Illustration of federated learning from the step 0ne until step 8 where aggregated weights are sent back to the local devices for continuation of the process until the desired accuracy is achieved.

Note that from step one to step 8 is one round. The training is performed for many rounds depending on the problem at hand

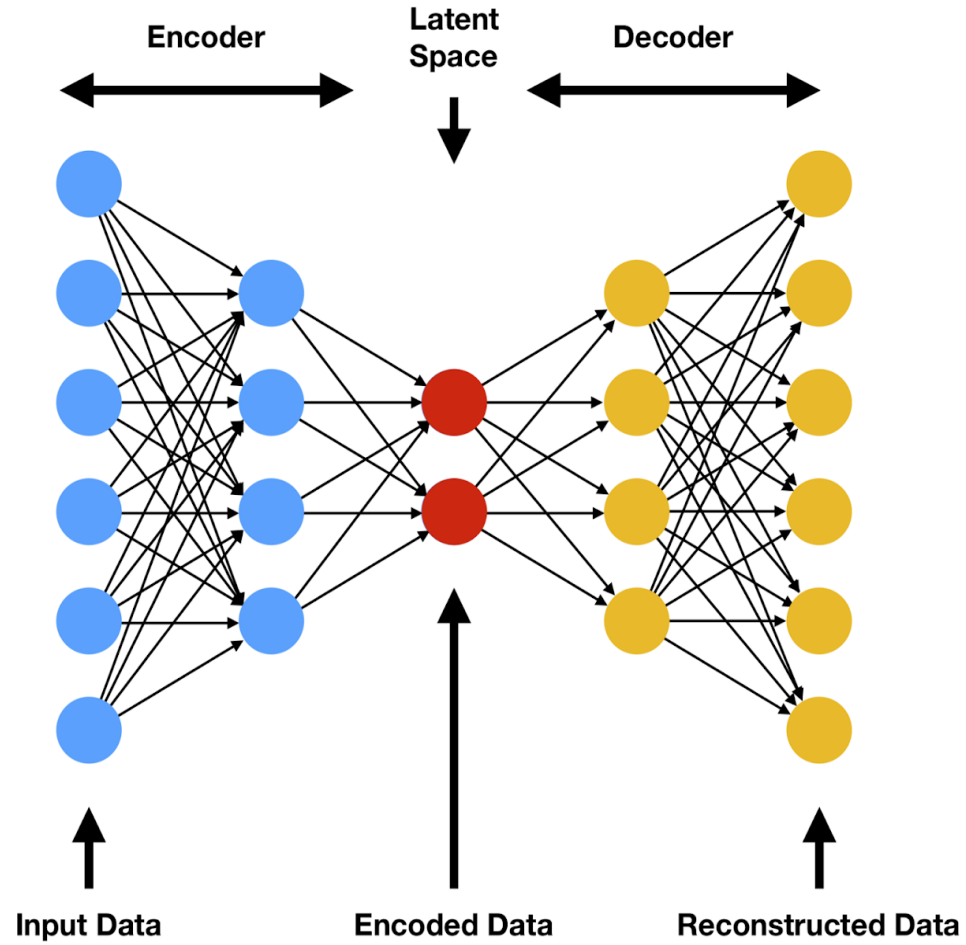


Technical Approach (methodology)

Implemented

- Design a deep autoencoder ML model for the unsupervised classification of cybersecurity attacks in IIOT Edge devices .
- Design a deep autoencoder FL model for the unsupervised classification of intrusion attacks in IIOT Edge devices .
- Train and evaluate the both deep autoencoder ML model AND FL on a modern dataset.

Auto Encoder For Anomaly Detection



- An autoencoder is a special form of feed-forward neural network made of two parts, the encoder and the decoder
- The encoder transforms the input by reducing its number of dimensions to a value defined as the coding dimension,
- and the decoder tries to map the encoded input back to the original input
- It is trained by minimizing the Mean Squared Error (MSE) between the reconstructed features and the input.

Technical Approach (methodology)

Implemented

- The model uses the deep auto encoder that classifies data to normal or malicious data.
- The deep autoencoder used for training and evaluation is composed by the input layers of 66 neurons, 3 hidden layers of 128, 64 and 32 neurons each
- followed by a dropout probability p set to 0.2, and the encoded layer(bottleneck) of 16 neurons.
- We have used the relu activations function in the hidden layer of autoencoder, whereas the Tahn activation function was used in the output layer of the decoder part of the deep autoencoder model.
- We set the threshold using the formula

Technical Approach (methodology)

Implemented

- We set the threshold using the formula

$$thr_k = mean(MSE(D_k^{Thr}; w_k) + std(MSE(D_k^{Thr}; w_k)$$

- This is based on computing mean and standard deviation of the reconstruction error of normal network flows.

- When testing, if a certain data sample mean squared reconstruction error is above the fixed threshold, it is classified as positive, otherwise it is considered as a normal network flow.

Candidate dataset(s) to be used

Dataset Edge_IIoTset description

a dataset modeling network traffic of several real IoT/IIOT EDGE devices while affected by malware

It was chosen based on the reason of being produced after involving several layers containing new emerging technologies

Those technologies fulfill the key requirements of IoT and IIoT applications:

1. **ThingsBoard IoT platform,**
2. **OPNFV platform,**
3. **Hyperledger Sawtooth, Digital twin,**
4. **ONOS SDN controller, Mosquitto MQTT brokers,**
5. **Modbus TCP/IP, …etc.**

It also is realistic for testing machine learning in federated learning manner.

Candidate dataset(s) to be used

Dataset Edge_IIoTset description

The data is generated from various IoT devices :

1. **temperature**
2. **humidity sensors,**
3. **Ultrasonic sensor,**
4. **Water level detection sensor,**
5. **pH Sensor Meter,**
6. **Soil Moisture sensor,**
7. **Heart Rate Sensor, Flame Sensor, etc.**

The dataset includes 14 types of attacks belonging to the following categories:

1. **DoS/DDoS attacks,**
2. **Information gathering,**
3. **Man in the middle attacks,**
4. **Injection attacks,**
5. **and Malware attacks.**

Candidate dataset(s) to be used

Statistics of the Edge_IIoTset deep learning dataset

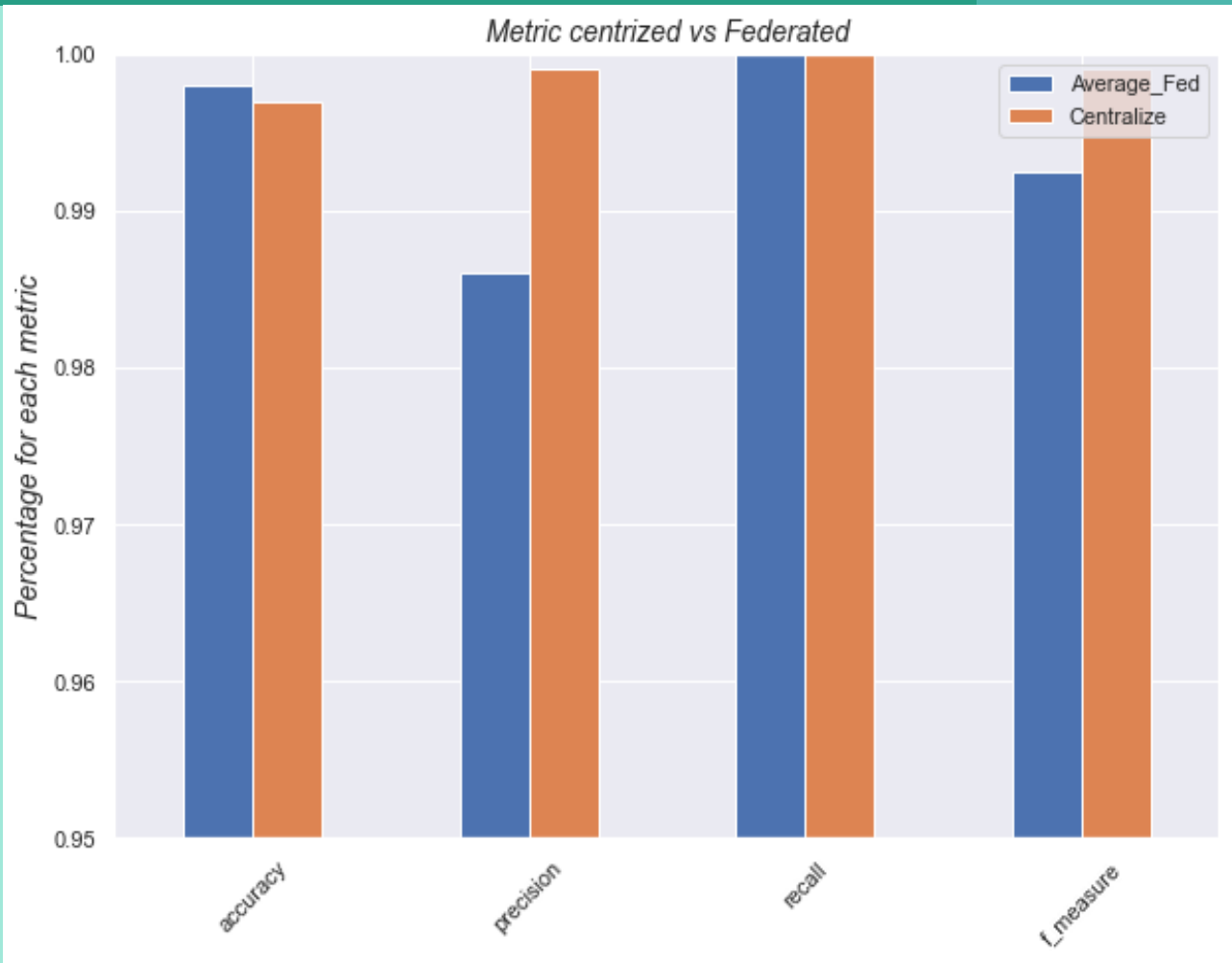
Number of normal records		300000
Number of attacks	ransomware	2000
	password	2000
	scanning	2000
	injection	2000
	xss	2000
	dos	2000
	backdoor	2000
	ddos	2000
	mitm	1043

Evaluation metrics

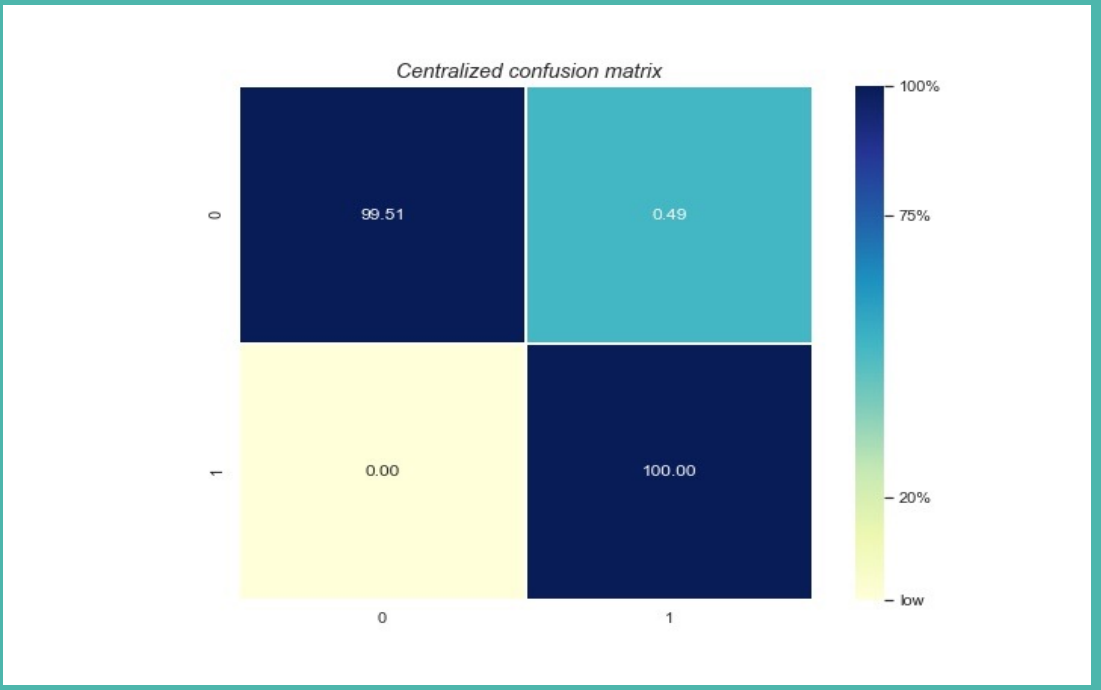
- Evaluation metrics will be used, such as TP, TN, FP, and FN standard values
- Threshold

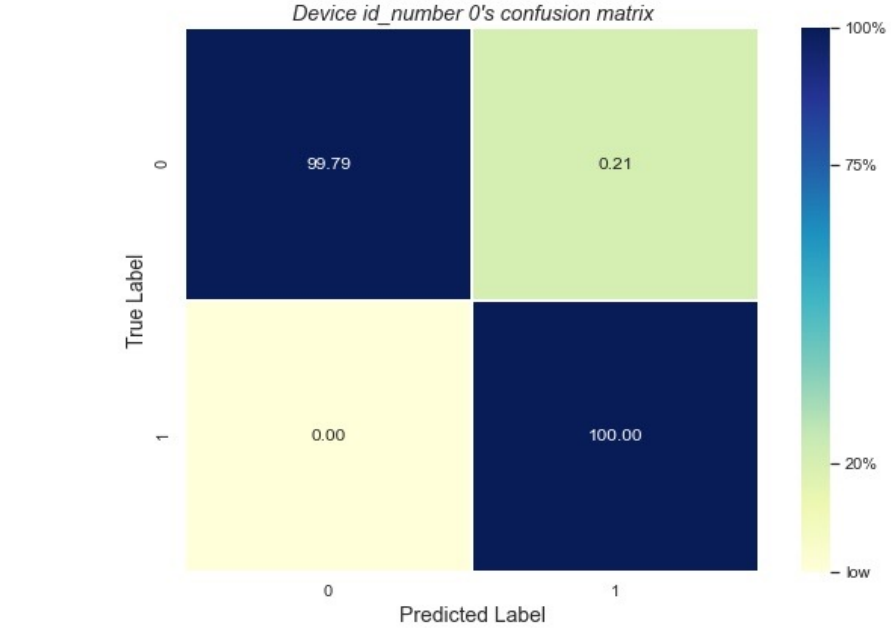
Model Comparison

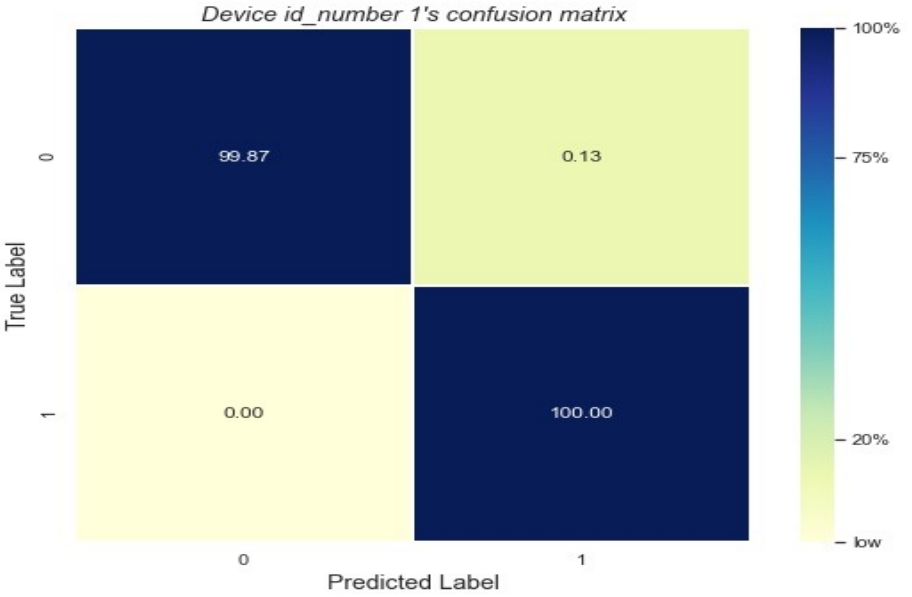
	Averaged Federated results	Centralized results
accuracy	99.8%	99.7%
precision	98.6	99.9%
recall	1	1
f_measure	99.2%	99.9%
false_rate	0.16%	0.49%



Model Comparison







Conclusion/ work in progress

- **With the online streaming of those devices' data, labeling data is almost impossible, and they have heterogeneous computing capabilities.**
- **For this reason, we applied an autoencoder-based unsupervised approach, and training and evaluating the model was done with the help of federated machine learning.**

- **Moreover, we are considering the issue of computation disparities among the devices participating for collaboratively training the global model.**

- **the next step is to continue developing and evaluating an Fair federated machine learning using the deep autoencoder with the same settings as centralized and vanilla FedAvg and perform comparisons.**

Reference

- **Horwitz, "The future of IoT miniguide: The burgeoning IoT market continues," *https://www.cisco.com/c/en/us/solutions/internet-of-things/future-of-iot.html*, 2019.**
- **D. Pauli. (2017). *414,949 D-Link Cameras, IoT Devices Can Be Hijacked Over the Net*. Accessed: Jul.21, 2018. [Online]. Available: https://www.theregister.co.uk/2016/07/08/414949_dlink_cameras_iot_devices_can_be_hijacked_over_the_net/**
- **Z. Zorz. (2017). *Exploitable GSOAP Flaw Exposes Thousands of IoT Devices to Attack*. [Online]. Available: https://www.helpnetsecurity.com/ 2017/07/19/exploitable-gsoap-flaw-iot-devices-exposed/**
- **M. W. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen, "Uninvited connections: A study of vulnerable devices on the Internet of Things (IoT)," in *Proc. IEEE Joint Intell. Security Inf. Conf.*, Sep. 2014, pp. 232–235.**
- **Hafeez, M. Antikainen, A. Y. Ding, and S. Tarkoma, "IoTKEEPER: Securing IoT Communications in Edge Networks," CoRR, vol. abs/1808.08415, 2018. [Online]. Available: https://arxiv.org/abs/ 1808.08415**
- **Liu L, Yang J, Meng W. Detecting malicious nodes via gradient descent and support vector machine in internet of things. Comput Electric Eng. 2019;77:339-353.**

Reference

- A. Kumar and T. J. Lim, “EDIMA: Early Detection of IoT Malware Network Activity Using Machine Learning Techniques,” in 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 289– 294.
- A. Sivanathan, “IoT Behavioral Monitoring via Network Traffic Analysis,” arXiv:2001.10632 [cs], Jan. 2020, arXiv: 2001.10632. [Online]. Available: http://arxiv.org/abs/2001.10632
- M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020, doi: 10.1109/COMST.2020.2988293.
- M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine Learning Techniques," in *IEEE Internet of Things Journal*, doi: 10.1109/JIOT.2020.3002255.
- T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan and A. Sadeghi, "DÏoT: A Federated Self-learning Anomaly Detection System for IoT," 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 2019, pp. 756-767, doi: 10.1109/ICDCS.2019.00080.
- J. Konecny, “Privacy-Preserving Collaborative Machine Learning without Centralized Training Data,” accessed: 2020-05-27; available: http://jakubkonecny:com/files/2018- 01 UW Federated Learning:pdf, 2018.

THANK YOU

COMMENTS & QUESTIONS