NORSK REGNESENTRAL
NORWEGIAN COMPUTING CENTER

AI-Driven Anomaly Detection in 5G Systems: Addressing IT/OT Integration and GDPR Compliance with Healthcare Scenario

Dr. Sandeep Pirbhulal, PhD & Postdoc

Senior Research Scientist and Project Manger

Norwegian Computing Center, Norway

Goethe University Frankfurt

08.07.2025

Agenda

- Introduction
- Significance of Privacy and Data Protection
- Secure Data Management in IT-OT Convergence
- GDPR in 5G-IoT Networks
- AI-Based Tool for Anomaly Detection in 5G Systems
- Healthcare Scenarios

CybAlliance Introduction

CybAlliance
Healthcare Security & Privacy

- **CybAlliance** (International Alliance for Strengthening Cybersecurity and Privacy in Healthcare): Norway, Germany, France and USA Partnership
- **Project Manger:** Sandeep Pirbhulal, Senior Researcher, NR
- **Duration:** 01.03.2023-29.02.2028
- **Project Owner:** Norwegian Computing Center/ Norsk Regnesentral
- **Total Project Amount:** 12.5 MNoK
- **Partner Countries:** Norway, Germany, France and USA

CybAlliance
Healthcare Security & Privacy

CybAlliance Partners

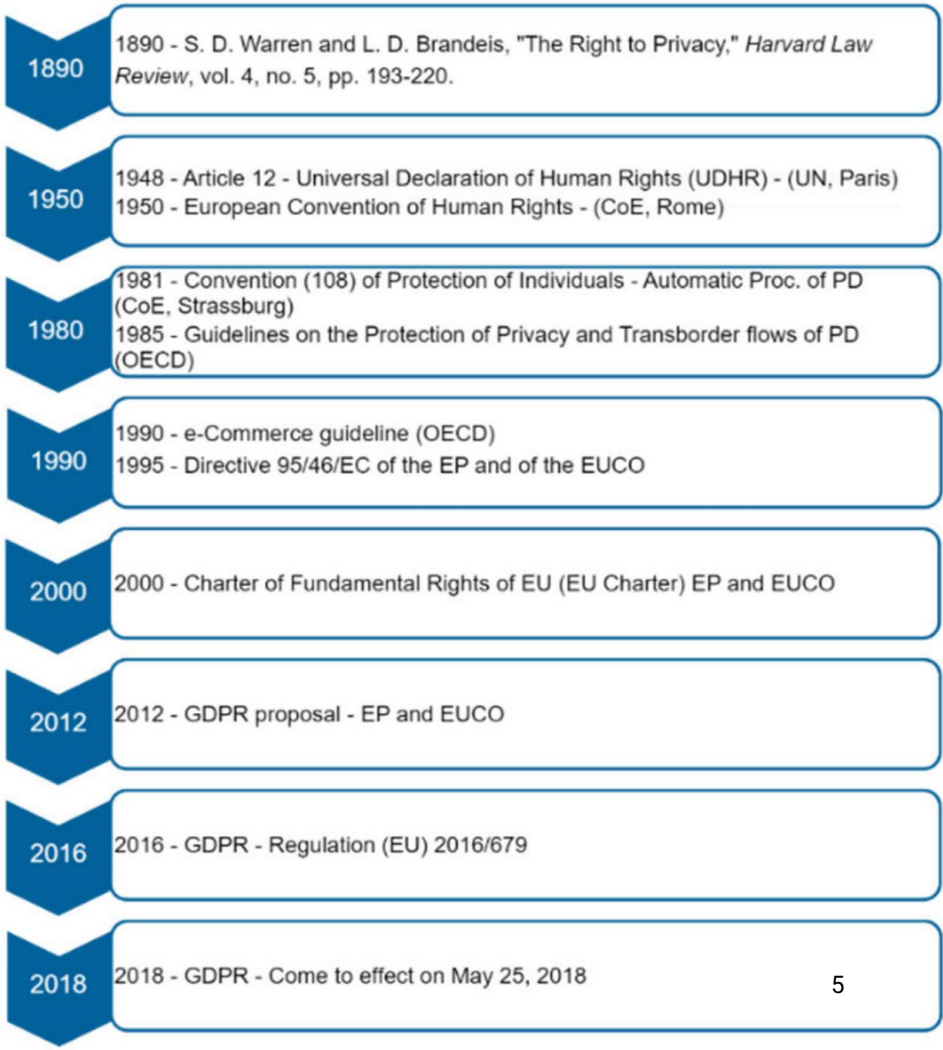
- Norwegian Computing Center (NR, Norway)
- Norwegian University of Science and Technology (NTNU, Norway)
- Oslo University Hospital (OUS, Norway)
- University of Colorado Springs (UCCS, USA)
- Telecom SudParis (IMT, France)
- Goethe University Frankfurt (GUF, Germany)
- University of Oslo (UiO, Norway) Associate Partner
- Institute for Energy Technology (IFE, Norway) Associate Partner

The Research Council of Norway

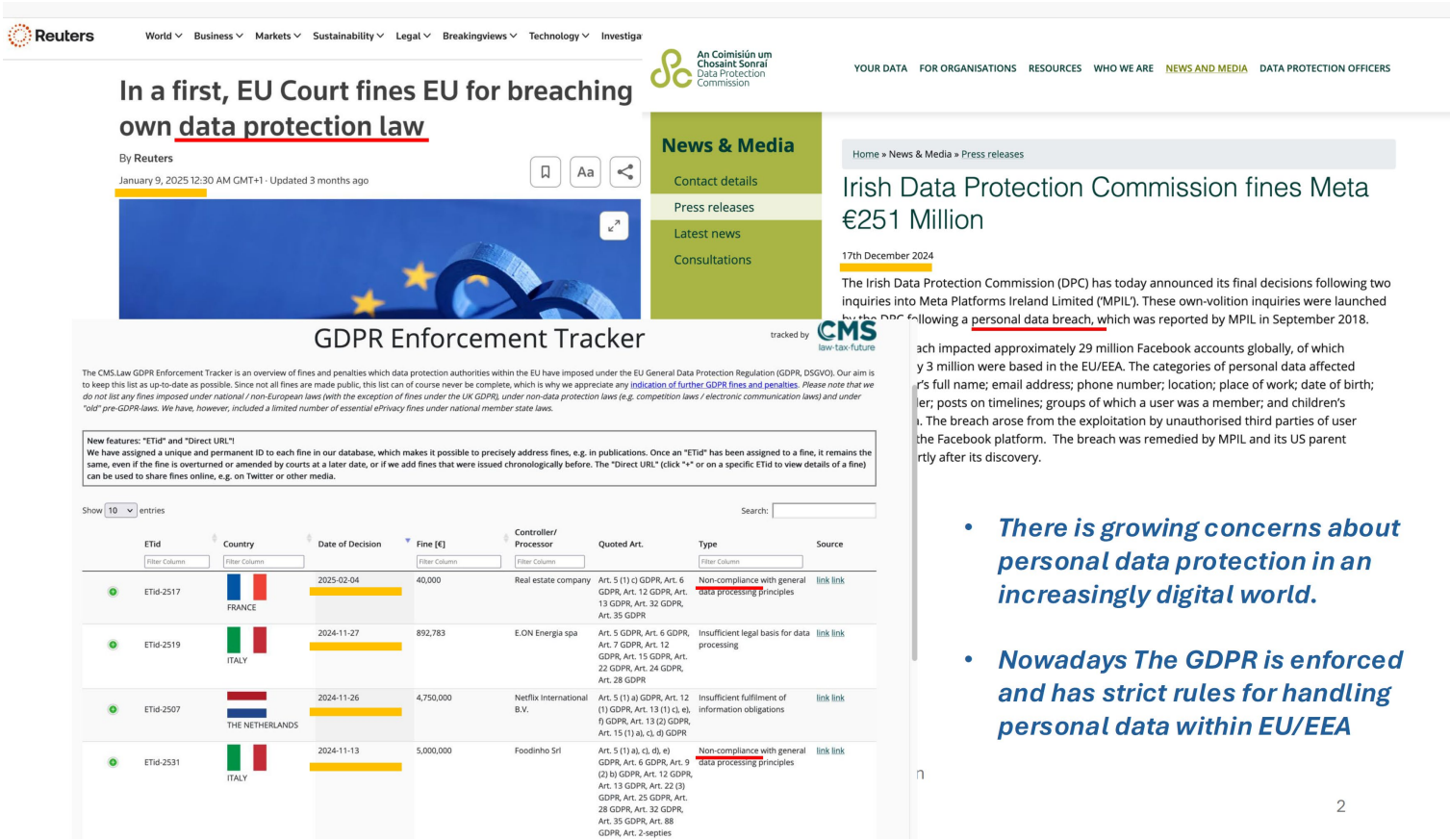
CybAlliance
Healthcare Security & Privacy

Timeline of privacy and data protection events

- **The General Data Protection Regulation (GDPR)**
- **Requires transparency** in how personal data is processed and upholds individuals' rights to control their data through informed consent.
- **Establishes a legal framework** to ensure organizations follow strict privacy and data security standards.
- **Provides general guidelines** for technical and organizational measures to protect data but does not prescribe specific solutions.
- **Leaves the responsibility of implementation to organizations**, allowing them to tailor their approach based on context, risk, and industry best practices.



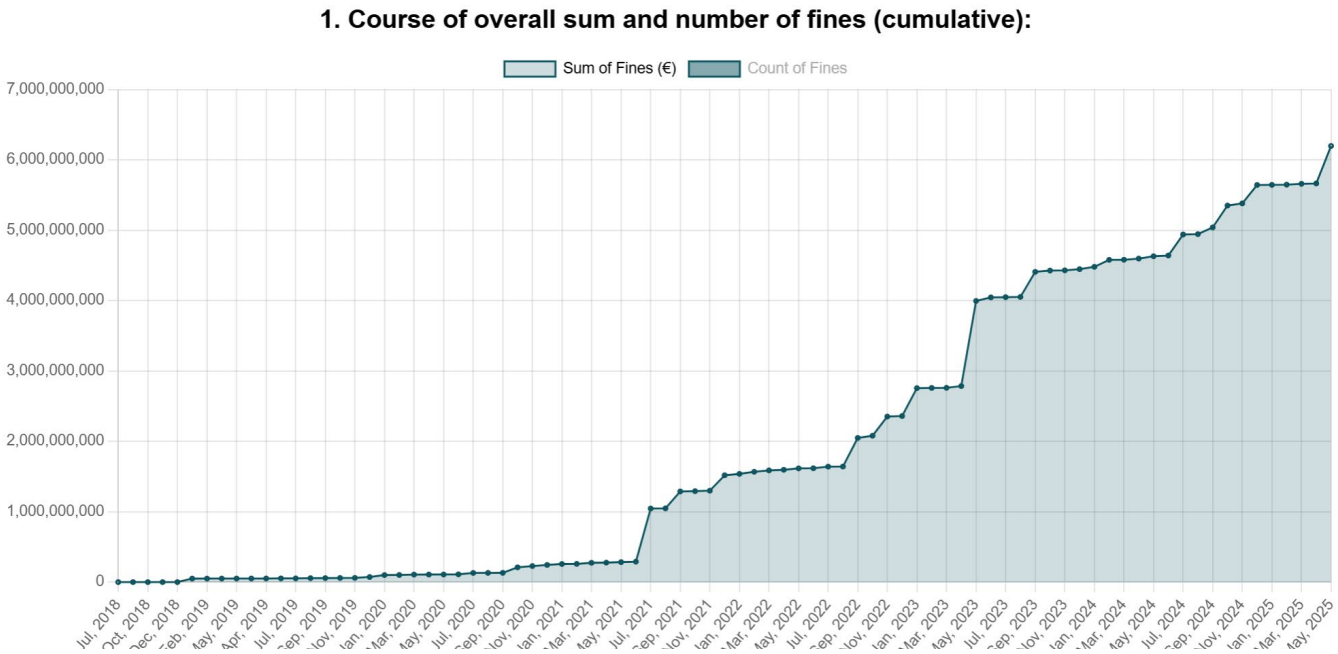
Zaguir, N. A., de Magalhães, G. H., & de Mesquita Spinola, M. (2024). Challenges and enablers for GDPR compliance: systematic literature review and future research directions. *IEEE Access*, *12*, 81608-81630.



- ***There is growing concerns about personal data protection in an increasingly digital world.***
- ***Nowadays The GDPR is enforced and has strict rules for handling personal data within EU/EEA***

2

As of May 2025, GDPR violations have resulted in over €6 billion in fines.



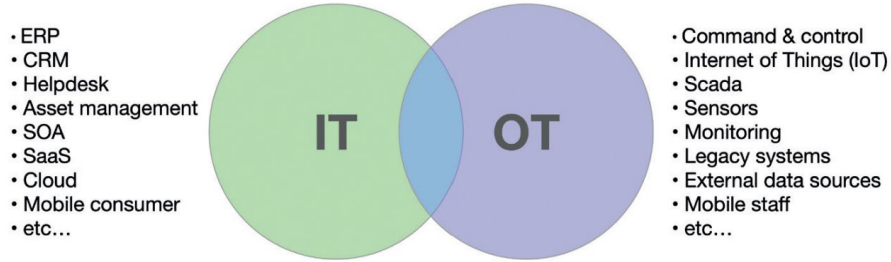
https://www.enforcement-tracker.com/chronological-statistic/

ETid	Country	Date	Fine [€]	Controller/ Processor	Quoted Article	Type	Link
ETid-2648	ITALY	2025-04-29	30,000	Ordine degli psicologi della Lombardia	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link link
ETid-2647	FINLAND	2025-05-27	1,100,000	Yliopiston Apteekin	Art. 5 (1) c), f) GDPR, Art. 32 (1), (2) GDPR	Non-compliance with general data processing principles	link link
ETid-2646	GERMANY	2025	45,000,000	Vodafone GmbH	Art. 28 (1) GDPR	Non-compliance with general data processing principles	link
ETid-2645	SPAIN	2025-03-24	2000	INDEPENDENTS DE VALLROMANES	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles	link

- The GDPR plays a crucial role in governing the handling of personal data across modern technologies, especially as reliance on 5G mobile communication, IT, and OT infrastructure grows.
- Since **5G often supports global operations** where data flows across regions, the GDPR offers a consistent framework to ensure that personal data remains protected, no matter where it is processed.

https://www.enforcement-tracker.com/chronological-statistic/

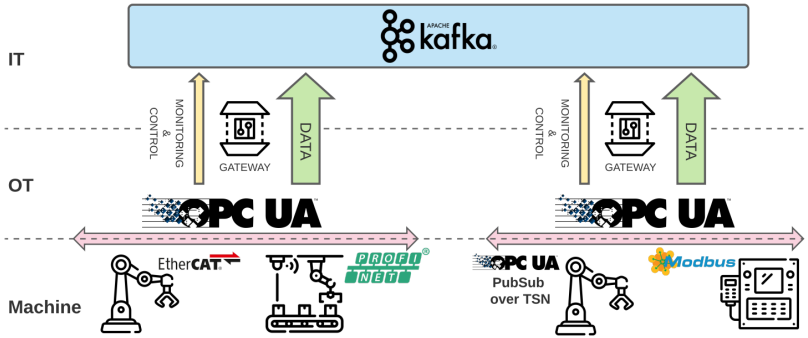
Why Secure Data Management in IT-OT Convergence?



Convergence between IT and OT

- Information and Operation Technology domains (OT-IT)
- **IT-OT Convergence** is needed for:
  - Better decision-making
  - Improved performance
  - Enhanced visibility
  - Resource optimization etc.

- **IT Technology** permits the handling of large volumes of **data in a secure and privacy-preserving manner**
- **OT Technology** deals with devices and other HW parts **to dynamically enable process control, maintenance, and manage key industrial functions** into the infrastructure
- **IT-OT convergence is one of significant drivers for Industry 5.0**



An Illustration of IT-OT Architecture Example

Yassine Maleh, IT/OT convergence and cyber security, Computer Fraud & Security, 2021
Lorenzo Patera et al., A Layered Middleware for OT/IT Convergence to Empower Industry 5.0 Applications, Sensors Journal, 2022

How 5G Increases the Security Threats in IT-OT?

Robust security approaches and continuous monitoring are essential to enable secure and privacy-preserving IT-OT convergence against evolving 5G-IoT anomalies

Expanding Device Ecosystem

5G connects a vast number of IoT devices, **dramatically increasing the potential attack surface**.

Conflicting Security and Privacy IT-OT Priorities

IT prioritizes data confidentiality, while **OT emphasizes availability** creating integration challenges.

New Hardware Attack Vectors

Emerging **5G hardware introduces** new entry points for **attackers in both IT and OT** environments.

Why is Anomaly Detection more Challenging in 5G-based Critical Sectors?

- Anomaly detection in 5G-IoT can improve the protection of critical sectors
- "The 5G-PPP consortium has identified a pool of Key Performance Indicators (KPI) [1] that have a high impact when analyzing and inspecting traffic network flows"
- " Four main KPI which can make anomaly detection procedures an even greater challenge in 5G mobile networks.
  - 1000 times higher mobile data volume per geographical area.
  - 10 to 100 times more connected devices.
  - 10 times to 100 times higher typical user data rate.
  - End-to-End latency of <1ms"[2]

As 5G links an increasing number of personal devices, the potential for misuse, surveillance, and data breaches rises. GDPR enforces privacy-by-design principles, enabling organizations to reduce these risks from the very beginning.

The 5G Infrastructure Public Private Partnership, "Key Performance Indicators (KPI)," https://5g-ppp.eu/kpis
Maimó, Lorenzo Fernández, et al. "On the performance of a deep learning-based anomaly detection system for 5G networks." IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Examples of Personal Data in 5G, IT and OT

IT Personal Data:

- Device IDs
- Records
- Browsing history

OT Personal Data:

- Biometric data to access control
- Incident and accident reports
- Work Schedules

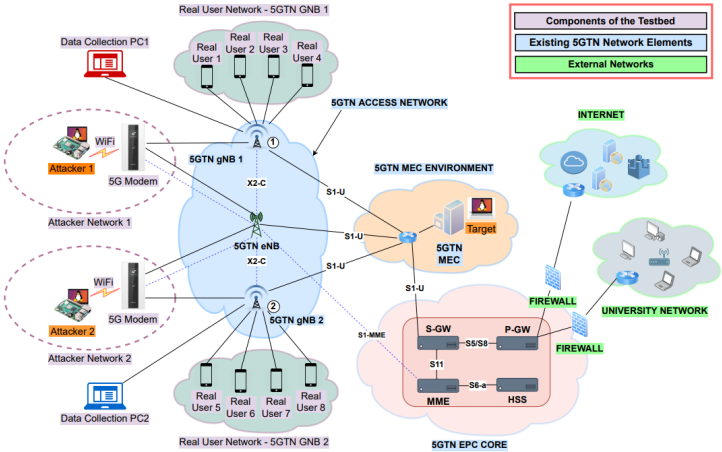
5G Personal Data:

- Subscriber Identity
- Location Data
- IoT Data

Why GDPR in 5G-IoT Networks

Scientific Problem: Due to the increased **softwarization and virtualization in 5G-enabled IoT systems**, security threats and anomalies have become major concerns.

In this context, **GDPR's emphasis on privacy and data protection** is crucial to ensure that such intelligent systems are designed to safeguard user information and maintain compliance with privacy regulations.

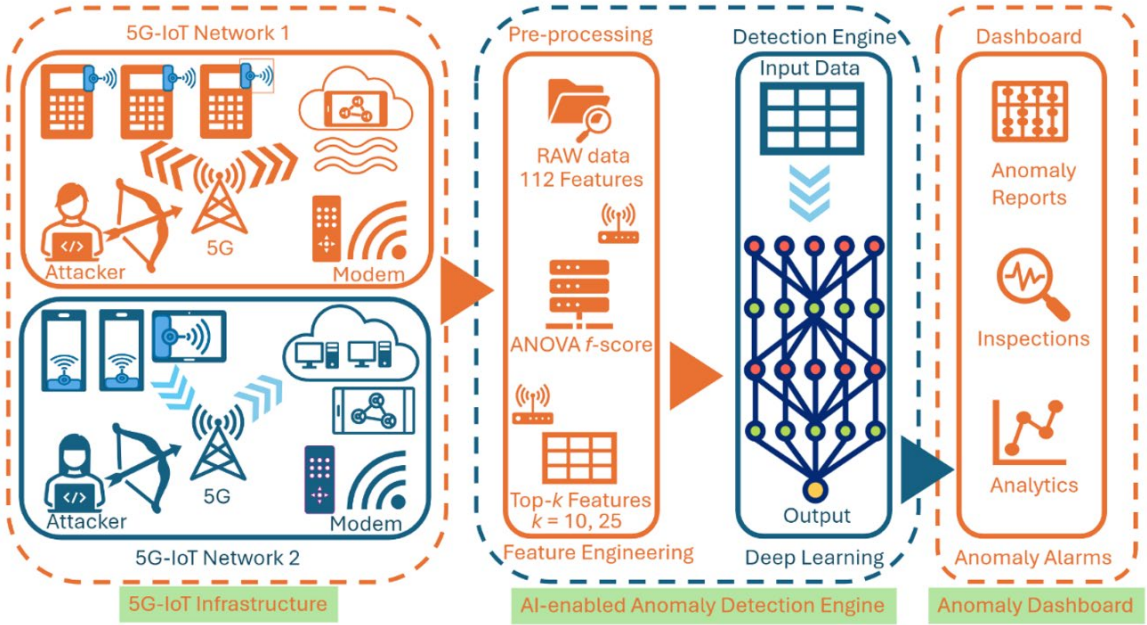


5G Test Network, University of Oulu

Device	Description
Attacker	Raspberry Pi 4 Model B with Ubuntu 21.10 - Impish
Victim	HP with Ubuntu 18.04.5 LTS - Bionic
Base Station	Nokia - Flexi Zone Indoor Pico Base Station
Modem	HUAWEI - E6878
Mobile devices	Motorola - Moto g50 5G
Switch	Dell - N1524

Traffic includes data from both IT and OT

Proposed AI-based Anomaly Detection in 5G System

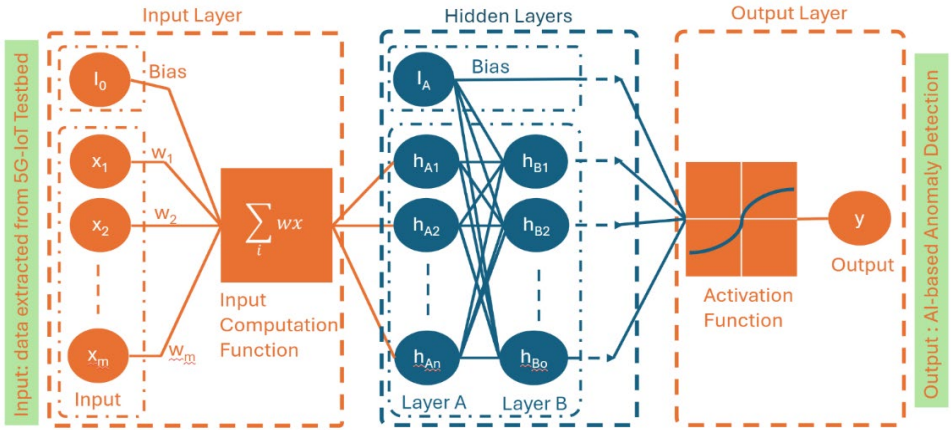


An overview of the proposed AI-based anomaly detection system for 5G-IoT networks

- There is an attacker node and devices generating benign traffic on two base stations in these networks.
- Data consists of 112 features in packet format
- We consider a range of visualizations for the dashboard:
  - line charts to track changes in the network traffic over time,
  - bar charts to display the frequency of detected anomalies

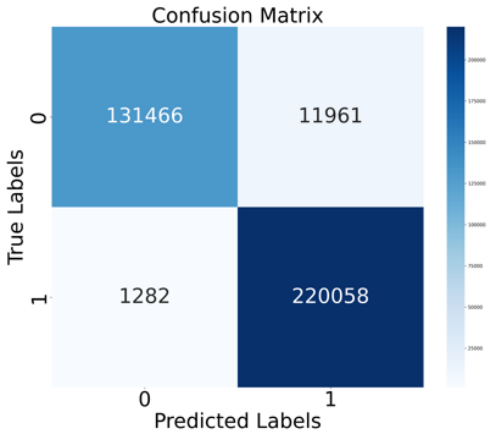
AI-based Anomaly detection: Binary10&25

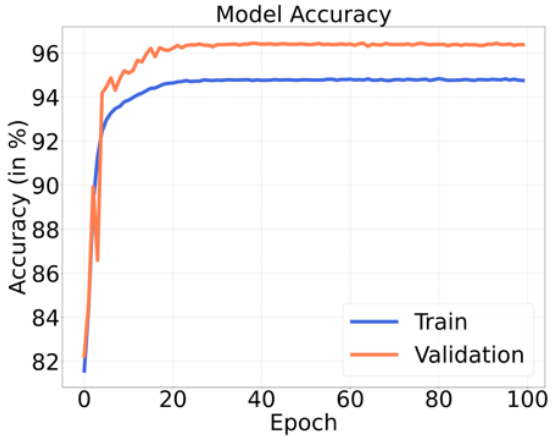
- Input data: 10 and 25 most important features (ANOVA)
- Deep Learning Models: GNN and CNN
- Epoch = 100; Batch size = 32; Learning rate = Adaptive;
- Results
  - More comprehensive and inclusive model
  - Higher training costs (CPU-based)

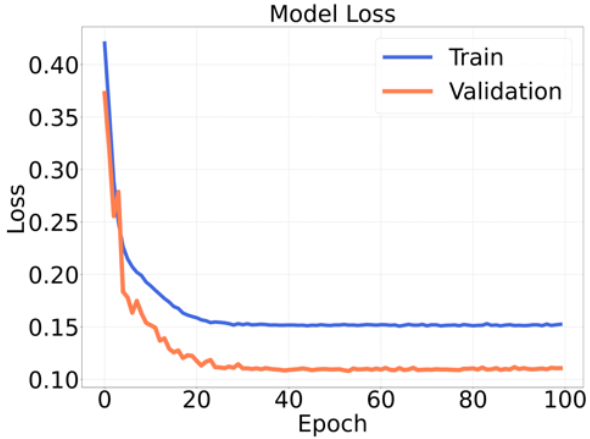


An illustration of the deep learning-based 5G-IoT Anomaly Detection Engine

Selected Experimental Results (1/2)

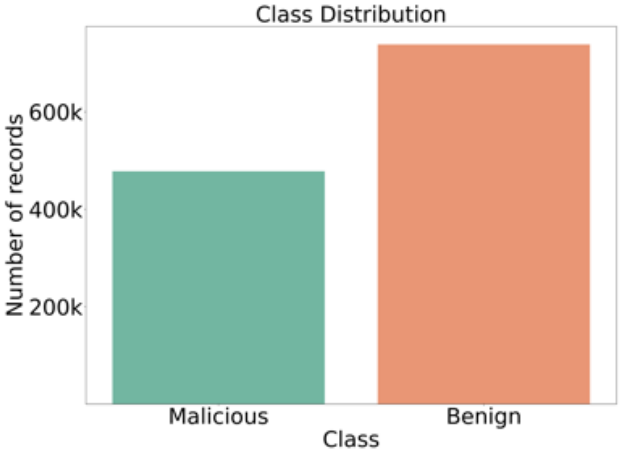


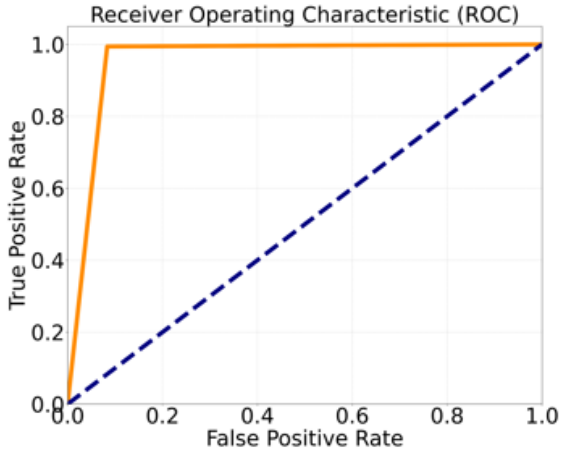


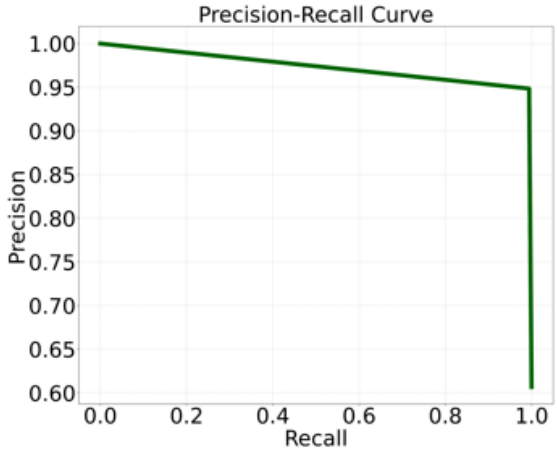


Training (right) and accuracy (left) results for 5G-IoT anomaly detection, ($k = 25$)

Selected Experimental Results (2/2)

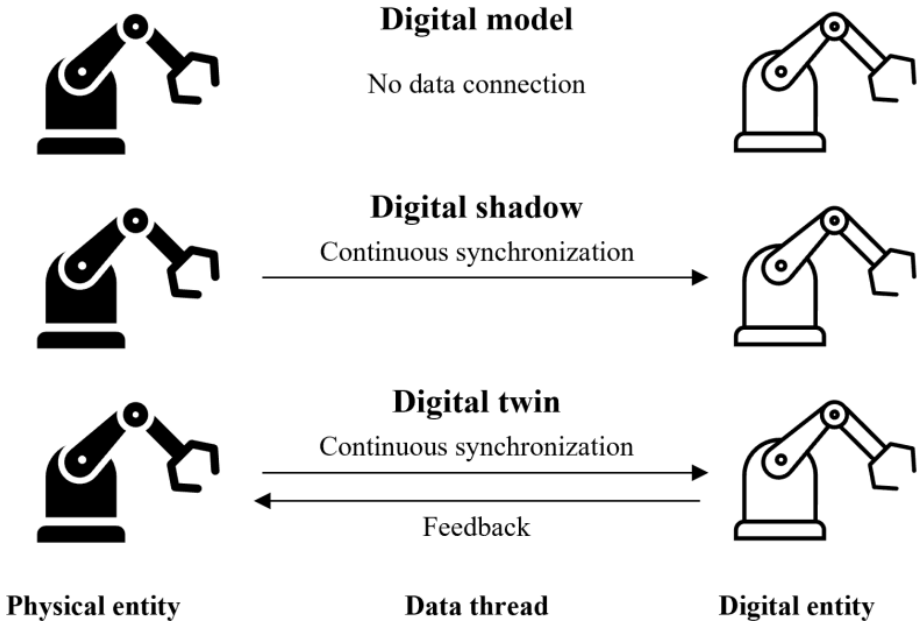






Dataset class distribution (left), ROC and Precision-Recall results (right), for (k =25)

Digital Twins Technology (DTs): An Approach for Virtual Communications



Sources: Lauer-Schmaltz, M. W., Cash, P., Hansen, J. P., and Maier, A. (2024). Towards the Human Digital Twin: Definition and Design – A Survey. arXiv preprint arXiv:2402.07922.

Digital Twins in Tele-Healthcare

- Provide real-time secure monitoring of patients via physical twin (hospitals, and/or smart homes) and/or virtual twins
- Enable doctors to simulate treatments on virtual twins of patients to predict their responses, enhancing safety and care quality
- Establish feedback loops between virtual systems and healthcare providers for ongoing learning and improved diagnostic predictions for diseases like gastric issues, cancer, and cardiac conditions, among others
- Enable dynamic risk assessment with root cause analysis, cybersecurity prediction and evaluation with appropriate countermeasures using a closed feedback loop in healthcare infrastructures

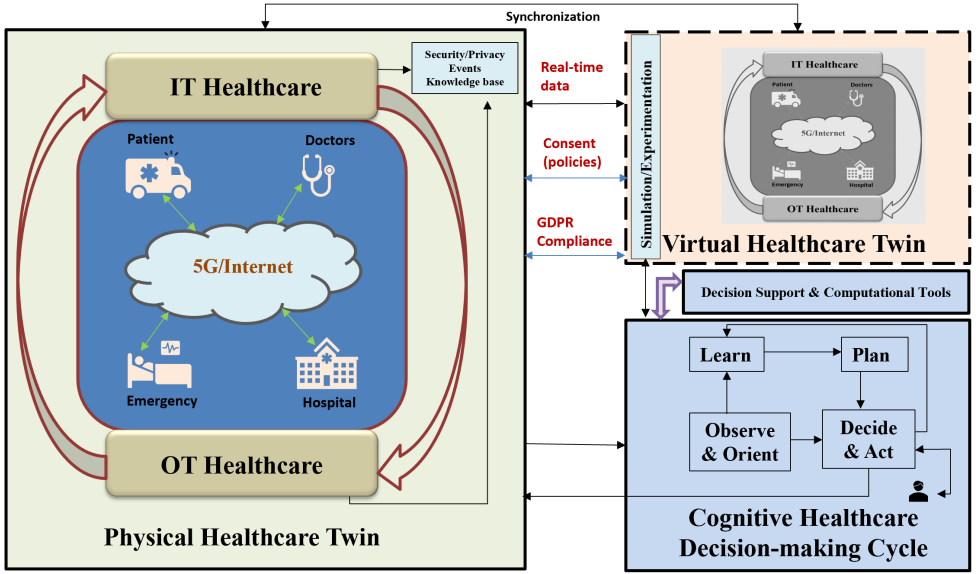
Embed Privacy by Design and Default into the architecture and lifecycle of digital twin systems.

Digital Twin-Driven Real-time Security for IT-OT based Healthcare Sectors

The digital twin is a virtual network that represents the components having **real mapping throughout life cycle** process by utilizing using **physical information**, **virtual information**, and **interaction between both data sources**.

Following features of Digital Twin are useful for enhancing cybersecurity

- Improves the understanding of cyber attacks
- Gives a continuous overview of vulnerabilities, threat landscape, attack space for IT-OT infrastructures, and mitigate them before they happen
- Allows the design of new prevention, detection, and response methods without disturbing physical IT-OT systems



- Adopt transparency-focused data policies that outline data use and access.
- Ensure comprehensive governance at every stage of the data lifecycle.

Thank You!

Any questions?

Sandeep Pirbhulal, Ph.D., Senior Research Scientist,
Norwegian Computing Center/Norsk Regnesentral,
P.O.Box 114 Blindern, N-0314 Oslo, Norway
Project Manager, CybAlliance
Email: sandeep@nr.no
Phone no. +47-41393687 or +47-22852582
Google Scholar:
https://scholar.google.com/citations?user=ecVXehQAAAAJ&hl=en
Researchgate: https://www.researchgate.net/profile/Sandeep-Pirbhulal
Linkedin:https://www.linkedin.com/in/sandeep-pirbhulal-4858a37a/?originalSubdomain=no