Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Autonomous adaptive security and privacy for Internet of sustainable waste management

Internet of Sustainable waste MAnagement and sorting (iSMART)

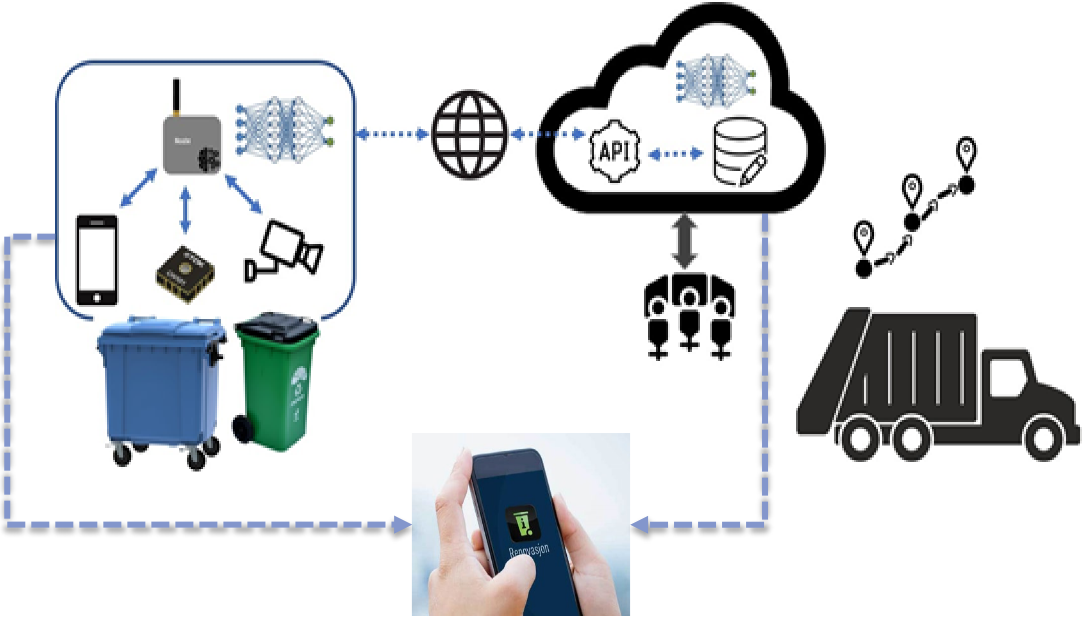
Habtamu Abie and Wolfgang Leister

Kjeller

10/03-2022

Internet of Sustainable waste MAnagement and soRTing (iSMART)

- Mobile app design for sustainable behavior
- Sorting-based incentive program to enhance recycling
- Low-power/Low-energy/low-bandwidth IoT-based machine learning for level/sorting detection and prediction
- Cloud-based multi-objective routing optimization
- Near real-time Collection-on-Demand (CoD) performance



NTNU: AI-powered IoT platform for sustainable waste management

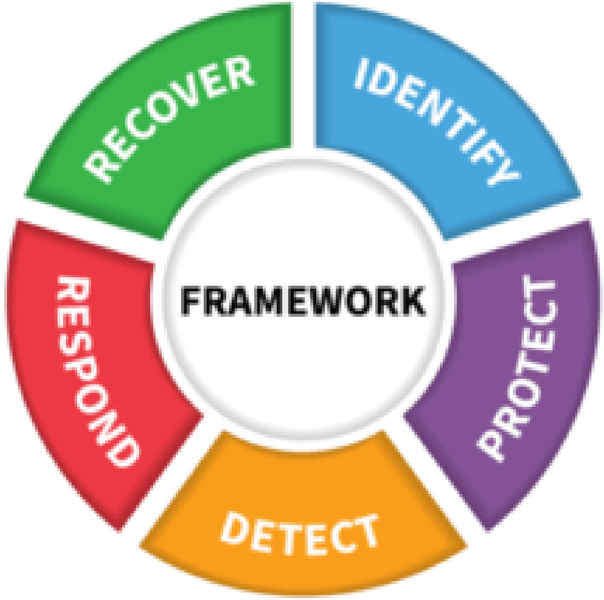
Autonomous adaptive security and privacy for Internet of sustainable waste management

- Enhance the security and privacy of Internet of sustainable waste management through security and privacy by design
- Integrate autonomous authentication, access control, objects validation, and privacy preservation in the entire development lifecycle systematically
- Adapt to dynamic changing conditions of internet of waste management systems (mobile App, IoT devices, edge servers and cloud), including threats, attacks, suspicious behaviours, and diversity/heterogeneity, autonomously

Advanced AI methods and mechanisms

- Use advanced AI to build autonomous adaptive security and privacy for real-time detection and prediction of attacks against systems
  - IoT devices (single hidden layer), mobile App/edge servers (more hidden layers), cloud (deep hidden layers), and communication among them
- Specifically, construct monitor-analyze-adapt control feedback loop models that consider these with increasing complexity

Building autonomous adaptive model



Source: NIST Cybersecurity Framework

- Adaptive model uses distributed learning
  - federated learning in each component to predict, detect and mitigate privacy breaches and security attacks based on the contextual information extracted from input data
  - with an objective of achieving high detection accuracy and low detection delay simultaneously

Adaptive model training

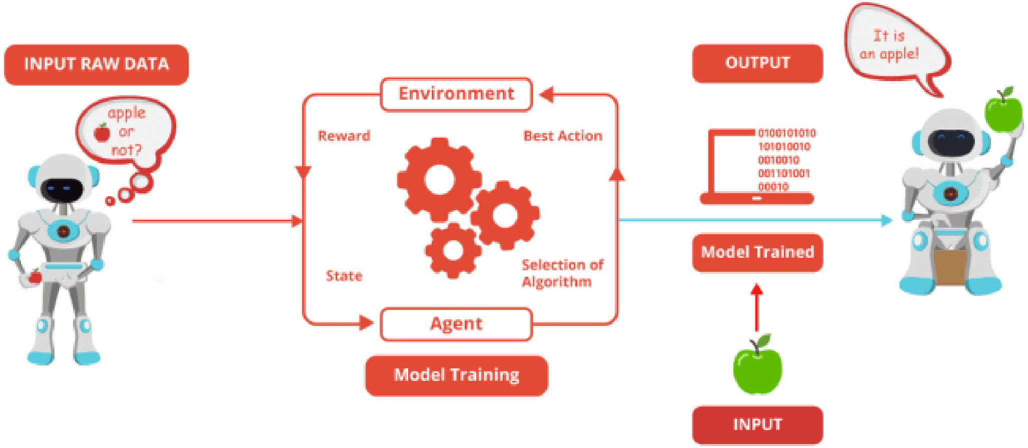
Train models in a decentralized manner on various

- IoT devices, edge devices, mobile, and cloud using their local data and thus the local data are not shared with any other participating devices

Improves scalability, allows for lower latency and less power consumption, and helps to preserve privacy

Poisoned/adversarial attacks

- Adversaries can exploit vulnerabilities in learned models and thus deceive the models via malicious input



Source: https://miro.medium.com/max/1360/1*_i0uyPboDhrYjqTsnQ8bsA.png

Combining evolutionary game with ML

- Adversarial attacks can be described as an evolutionary game (EG) between the machine learning system and the adversary
  - Players evolve by adapting their strategies to maximize their utilities
- Combining evolutionary game theory with ML training
  - enhance the models to specifically address adversarial attacks
- Evolutionary game theory and federated learning
  - adapt security intelligence features based on the changing context both within IoT, edge, cloud, mApp systems and their environments
  - ML models are used to detect and predict threats and attacks
  - EG is used to explore the space of defensive strategies for security intelligence

Advantage of the adaptive model: key takeaways

- Uses federated learning (FL)
  - with the ability to deal with unbalanced, sparse, and non-representative data at local nodes
- Provides better privacy by splitting the machine learning model architecture between devices
  - amalgamating FL and split learning eliminates their inherent drawbacks
- Enables training of devices with low computing resources
  - as they can train only the first “few layers” of the split ML network model to better adapt to their local threats
- Embeds autonomy and intelligence into networks, connected objects and services (NGI)