World Standards Day

Technical Report

Artificial Intelligence and Big Data

Saharnaz DILMAGHANI

October 2019
Big Data, Machine Learning (ML), and Artificial Intelligence (AI)

- **Big Data**
  - Volume
  - Variety
  - Velocity

- **Machine Learning**
  - Supervised
  - Un-supervised
  - Reinforcement Learning
  - Deep Learning

- **Artificial Intelligence**
Data Privacy and Trustworthiness Threats

- Privacy breaches
- Data poisoning
- Data bias

Training Data ➔ Model learning

- Model extraction
- Inference attack

New Data ➔ Application ➔ Inference and Prediction

- Inference attack
- Privacy breaches

- Privacy breaches
- Adversarial inputs

Importance of Standardization

International standards, certifications, and regulations

• Ensure the degree of privacy, security, and trust against cyber attacks

• Protect individuals’ data
Gap Analysis

Identification

- Definitions and terminology
- Computational approaches
- Applications and use cases
- Privacy and security threats

✓ ISO/IEC 2382
✓ ISO/IEC WD 22989
✓ ISO/NP TR 23347
✓ ISO/IEC AWI 24372
✓ ISO/NP 3534-5
✓ ISO/IEC WD 23053
✓ ISO/IEC NP TR 24030
✓ ISO/IEC TR 20547-2
✓ ISO/IEC PDTR 24028
Gap Analysis

Measurements

- Metrics
- Mitigation Strategies
- Risk quantification

✓ ISO/IEC PDTR 24028
✓ ISO/IEC PDTR 24028
✓ ISO/IEC NP TR 24027
✓ ISO/IEC NP TR 24029-1
✓ ISO/IEC 20889
✓ ISO/IEC TR 27103
✓ ISO/IEC 18033-6
Gap Analysis

Implementation

- Tests and Evaluation
- Constraints
- Implementation

✓ ISO/IEC CD 20547-4
✓ ISO/IEC NP TR 24027
✓ ISO/IEC NP TR 24029-1
✓ ISO/IEC CD 20547-4
Thank You!

saharnaz.dilmaghani@uni.lu