6GFLAGSHIP.COM | #6GFLAGSHIP

Sec-EdgeAI: AI for Edge Security Vs Security for Edge AI

Pawani Porambage, Tanesh Kumar, Madhusanka Liyanage, Juha Partala, Lauri Lovén, Mika Ylianttila, and Tapio Seppänen

University of Oulu, Finland

Email: (firstname.lastname)@oulu.fi

INTRODUCTION

Fifth Generation (5G) wireless systems are expected to fully integrate telecommunication technologies with cloud computing and softwarized paradigms. They are expected to empower ultra reliability, low latency, massive scalability, and high capacity. 5G brings edge computing to offer customers more control of their data. 6G technologies may introduce extremely advanced technologies comprising of ambient intelligence [1].

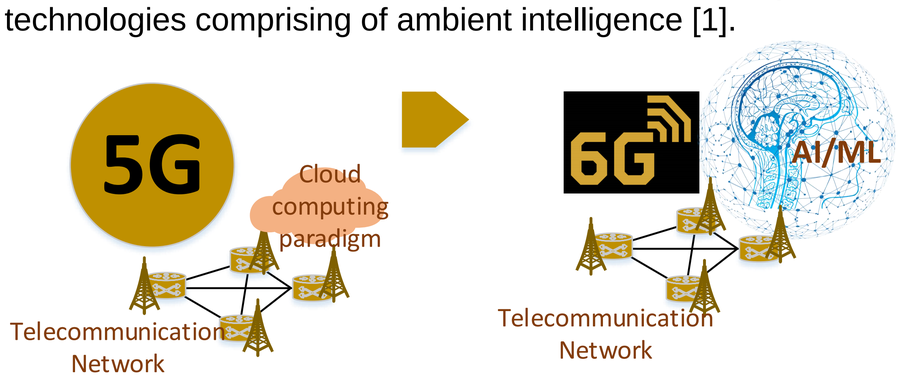

Fig 1. Evolution from 5G to 6G

SECURITY in 5G

– Potential security concerns in 5G systems may vary [2]:
  - From customer to service providers.
  - From network operators to device manufacturers.
  - From application developers to regulatory bodies.
– Most common security threats in edge paradigms:
  - Denial of Service (DoS) attacks.
  - Service or resource manipulation.
  - Privacy leakage.
  - Man-in-the-middle attacks, etc.
– Novel trends in edge security:
  - Artificial Intelligence (AI), Machine Learning (ML), data mining and deep learning techniques in static and dynamic malware analysis, and anomaly detection.
  - Leveraging novel advances in AI for network softwarization technologies such as MEC, SDN, NFV and Network Slicing to make intelligent decisions at the edge.

SECURITY in 6G

– Security of beyond 5G, **6G**, ecosystems will involve diverse users, infrastructure and technologies by making it even more crucial and complex than ever before:
  - **Intelligent** and **self-learning** security solutions are required.
  - AI at the edge can provide predictive based security opportunities to foresee the potential attacks.

AI in WIRELESS COMMUNICATION

– AI/ML applications enhance communication network operation and management [3] (***ML for Communication, MLC***).
– Novel communication network techniques support maximal AI operation (***Communication for ML, CML***).

SEC-EDGEAI VISION

AI for Edge Security: Exploit AI applications to identify and mitigate security vulnerabilities at Edge.

Security for Edge AI: Novel security mechanisms to make secure and robust Edge AI.

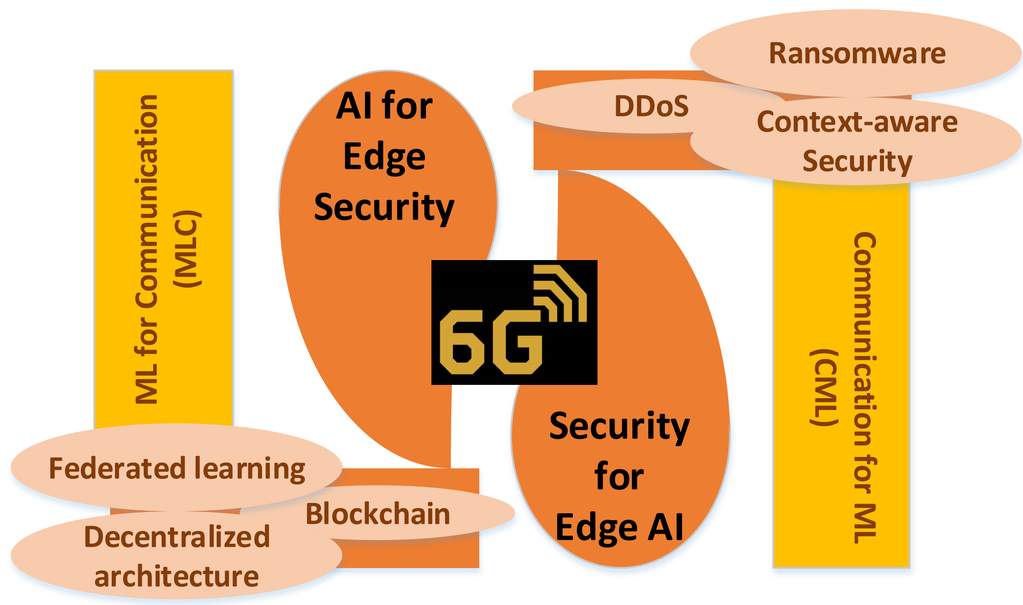

Fig 2. Our vision for SecEdgeAI

SECURITY THREATS

1. Opening up new attack vectors for malicious entities, targeting integration points and functionalities offered by CML and MLC, and their enabled applications.
2. Creating new incentive structures for malicious entities: Eg. integration of blockchain technologies or introduction of micro operators and pico cells in operator landscape.
3. Widening spectrum of potential malicious entities via increased intelligence of agents and distributed autonomous organizations.

IMPACT

– The proliferation of using AI/ML techniques are expected to improve the edge computing paradigms in 5G and 6G networks.
– Twofold security considerations:
  1) EdgeAI can be a platform that enable security solutions.
  2) Stand-alone EdgeAI solutions may impose their own security challenges.
– Security is important for instilling trust among those that use the solutions or are subject to their calculations and decisions.

REFERENCES

[1] T. Kumar et. al., “Securing the gadget-free digital services”, IEEE Computer, 2018.

[2] I. Ahmad et. al., “5G security: Analysis of threats and solutions”, in IEEE CSCN, 2017.

[3] J. Park et. al., “Wireless Network Intelligence at the Edge”, Submitted to PIEEE.