ERICSSON

AI/ML security in mobile telecommunication networks

Executive Summary

This paper explores the impact of AI/ML technologies on mobile telecommunication network security, particularly in 5G and beyond. While AI/ML technologies offer benefits like advanced network optimization and enhanced connectivity, they might also introduce security challenges that must be addressed to protect networks and sensitive information.

The paper assesses AI/ML in three primary contexts: as tools for attacking telecommunication networks, as tools for enhancing network security, and as potential targets for attackers. AI/ML can amplify existing offensive strategies and automate attacks. On the other hand, AI/ML can also enhance threat detection, support traditional security methods, identify potential new threats, and apply more dynamic and adaptable security measures. The paper emphasizes the importance of securing AI/ML components to ensure network availability and integrity, highlighting the potential vulnerability of these components to both conventional and AI/ML- specific threats.

The key ideas highlighted in the paper focus on the need for comprehensive security strategies that cover both traditional and AI/ML-specific security measures and the importance of conducting security risk assessments throughout the AI/ML development and operational lifecycle. Additionally, the paper underscores the need for compliance with security standards, proactive cybersecurity measures, and vulnerability management.

A holistic security approach, based on the Ericsson Trust Stack model, is recommended to effectively manage security challenges relevant to AI/ML to ensure the security posture of deployed mobile networks. This holistic security approach is addressing security at standards, product development, network deployment, and network operations levels.

The paper concludes with recommendations for policymakers, advocating for more research on AI/ML's role in enhancing threat detection, raising awareness of structured approaches to AI/ML-specific attacks, advancing security standards, promoting AI/ML security best practices, and supporting developments in confidential computing and privacy-enhancing technologies. Policymakers fostering collaboration between the public and the private sector stakeholders is key to ensuring that net benefits from AI/ML are maximized. A synergistic partnership between government and industry is the best way forward for effective cyber defenses to ensure the security of users and the resilience of mobile networks.

Contents

Introduction

In the mobile telecommunication network landscape, AI/ML has emerged as a pivotal force driving innovation and operational efficiency. It can facilitate advanced network optimization, enable dynamic resource allocation and predictive maintenance, and ensure seamless connectivity and reduced downtime. As mobile telecommunication infrastructures evolve towards advanced 5G and beyond, the utilization of AI/ML becomes increasingly important in addressing their complexities. While AI/ML technologies enhance the capabilities of mobile telecommunication networks, they also bring the need for robust security measures to secure the networks.

The primary goal of securing a mobile telecommunication network is to guarantee uninterrupted connectivity and prevent leakage of sensitive information for users such as consumers, enterprises, and public utilities. The network's security posture must provide a secure and reliable experience for all stakeholders, protecting both the network, data flows thorough it, as well as AI/ML components.

A holistic security approach based on the Ericsson trust stack and also recognized in OECD Digital Economy papers [1], identifies security across four integral layers: standards, development process, configuration, and operations [2]. This approach ensures comprehensive security considerations within and between each layer.

This paper examines AI/ML technology from a mobile telecommunication network security-centric perspective. The technologies are discussed in terms of:

- AI/ML as tools employed by threat actors to attack mobile telecommunication networks,
- AI/ML as tools to enhance mobile telecommunication network security, and
- AI/ML technologies integrated into mobile telecommunication networks as targets for atackers and how to protect them.

When adopting new technologies like AI/ML, there is always a balance between benefits and risks. It is essential to recognize that risks vary across different deployments, necessitating the selection of appropriate security controls tailored to each specific context. Therefore, this paper aims to assess the potential security risks AI/ML brings to mobile telecommunications and understand how current state-of-the-art security measures stand up against them. This approach seeks to create understanding and help suppliers of network equipment ensure that their products and services offer the best-in-class security.

AI/ML as attack tools

While AI/ML technologies offer promising advancements in security, they also amplify the effectiveness and reach of existing offensive strategies. This challenge is unlikely to be resolved by regulatory measures alone, and responsible stakeholders must consider the impact of AI/ML on cybersecurity risks since these technologies can substantially change both their type and scale. While they might not always introduce new types of attacks by themselves, they amplify the effectiveness and reach of existing attack methodologies. Ways in which AI/ML can be used for more effective attacks:

- Enhancing attack automation by enabling adversaries to find vulnerabilities, exploit them, and adapt to countermeasures. Such automation increases the speed and scalability of attacks. Unlike traditional methods that might require significant human intervention, AI/ML-driven attacks can operate autonomously, targeting multiple systems simultaneously and adjusting tactics as needed.
- Identifying the most vulnerable or valuable targets within a mobile telecommunication network by analyzing vast datasets. For example, critical servers that manage network traffic or specific cell sites serving high-profile customers might be identified as high-value assets to target.
- Adapting attacks more responsively and intelligently. Traditional security controls often rely on predefined signatures or known patterns to identify threats. However, AI/ML algorithms can evolve tactics in real time, making them difficult to detect and mitigate. For example, if a firewall blocks a particular type of malicious traffic, AI/ML algorithms might find an alternative route or method, effectively evading detection.
- Refinement of phishing algorithms and social engineering campaigns [3]. AI's capability to automate and personalize complex tasks, such as social engineering attacks, makes previously resource-intensive attacks accessible to less funded adversaries. Within the mobile telecommunication domain, engineers and operational staff can become targets for these advanced, AI-backed social engineering attacks.
- Using AI to attack AI. For example, if a mobile telecommunication system uses AI/ML for, mobility optimization, attackers could use AI-driven tools to automate its "poisoning." This can reduce the AI's decision-making confidence and lead to misjudging bandwidth distribution or mobile handoffs between base stations.
- Using AI models to convey malicious content. Researchers have explored how ML models can be used to deliver malware. A recent study showed that it is possible to embed malware into the model, enabling undetected data transfer past defensive systems [4]. For example, if a mobile telecommunication system uses pre-trained AI/ML models for later tailoring more specific tasks through transfer learning, without proper security controls the system might be infected with potentially persistent malware.
- Repurposing available AI tools. Attackers generally stay current on new technologies that they can leverage, including AI/ML. Following the release of ChatGPT and similar generative Large Language Models (LLMs), malicious actors have repurposed them for their benefit, using them to create malware, run phishing campaigns, or as a knowledge base for launching attacks. Some examples use open source LLMs to create specific malicious models like PoisonGPT.

While AI/ML can be leveraged as an attack instrument to disrupt the robustness, there are ways to use AI/ML on the other hand to improve security across mobile telecommunication networks as highlighted in the next section.

AI/ML for mobile telecommunication security

AI/ML technologies open new frontiers in cybersecurity defense. AI/ML can enhance threat detection in mobile telecommunication networks by supporting traditional methods and identifying potential new threats. AI/ML overcomes the limitations of traditional signature-based detection techniques, can identify new or complex threats, and apply more dynamic and adaptable security controls. Specialized AI-based security controls can employ advanced behavioral analysis and real-time adaptation, helping match the evolution of attacker techniques.

Also, the rise of offensive AI requires advanced countermeasures. Specialized AI-powered security controls, such as AI-driven intrusion detection systems, can serve as advanced mechanisms, designed to detect AI-driven attacks by identifying AI-specific anomalies [3]. Real time adaptation is particularly important against AI-based attacks, which can adapt themselves faster than humans can react. For example, if an AI-driven malware changes its signature to evade detection, a specialized security system can update its algorithms almost instantly to recognize this newly evolved threat.

Some example applications of AI for security include:

- Identifying abnormal patterns in network traffic and revealing potential security threats like Distributed Denial-of-Service (DDoS) attacks or unauthorized data access.
- Advancing security monitoring tasks such as the use of behavioral analysis to detect anomalies. These can extend beyond cyber threats to also include the detection of electromagnetic attacks, such as jamming against Radio Access Networks (RAN). Additionally, AI/ML can help analyze, detect, and prevent fraudulent activities, thereby protecting revenue generated from network-based services. AI/ML is also recognized as a tool to enhance security automation and orchestration, facilitating zero-touch network management and consequently reducing human-related risks.
- One notable application is false base station detection; utilizing advanced algorithms and ML models, the technology allows for much more accurate differentiation between legitimate and rogue base stations. This helps secure mobile telecommunication environments against deceptive entities like IMSI catchers and Stingrays, which impersonate genuine base stations for malicious activities [5].

AI/ML technologies are integral to the Network Data Analytics Function (NWDAF), particularly for enhancing the security measures within 5G networks. The scope of AI/ML within NWDAF is expansive, including providing mobility-related forecasts, predicting communication patterns, and offering congestion information. NWDAF leverages AI/ML to detect abnormal UE behavior, for instance, a UE transmitting unusual amounts of data in the middle of the night.

The emergence of Large Language Models (LLMs) has opened a new era in security automation. LLMs can be fine-tuned for security use cases to automatically analyze and interpret logs, thereby aiding in real-time threat detection. They can also be deployed in chat-based security systems to interact with security engineers and gather information on potential security incidents. This not only accelerates the incident response but also frees up human resources for more complex analysis and decision-making.

It is important to remember that while AI-powered security controls offer advanced capabilities for detecting and mitigating threats, the AI/ML components integrated into these systems are not invulnerable.

Securing AI/ML components in mobile telecommunication networks

AI/ML components in mobile telecommunication networks

While AI/ML adds capabilities and efficiencies in the mobile telecommunication domain, analyzing its security and trustworthiness is vital as it might introduce new vulnerabilities. The integrity of AI/ML models and the data they process is important, and a compromise, can result in consequences ranging from service disruptions to breaches of sensitive user information.

Mobile telecommunication networks serve as the backbone for transmitting voice and data across the globe, enabling seamless connectivity for user devices like mobile phones [2]. These networks are structured into five main logical parts: The Radio Access Network, core network, transport network, management, and interconnect network. Those parts operate on three distinct planes—control, user, and management—responsible for signaling, payload, and network management traffic (Figure 1).

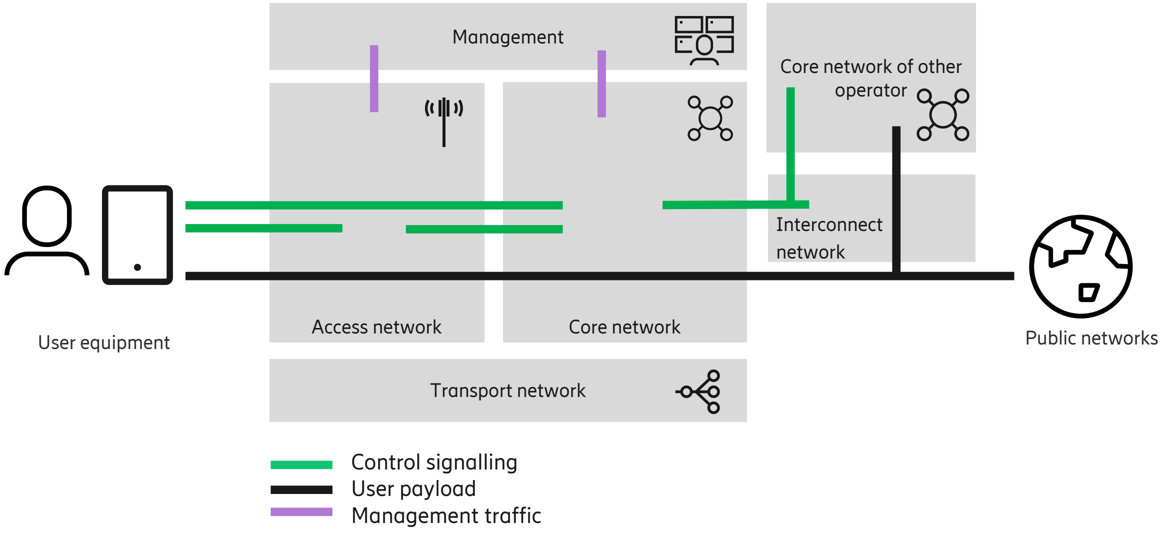


Figure 1. High-level architecture of a mobile telecommunication network

Security of AI/ML should focus on the following components containing AI/ML technologies: Next-Generation Radio Access Networks (NG-RAN), access networks based on the O-RAN architecture, NWDAF within 5G core network, AI-driven Operations/Business Support Systems (OSS/BSS), and security management tools. Integration of AI/ML there without appropriate security measures might elevate security risks in mobile telecommunication networks.

The adoption of AI/ML within NG-RAN significantly enhances network performance but introduces new security and privacy challenges, particularly in the management of user equipment (UE) data used for training AI/ML models. Mishandling such data could result in unauthorized access to sensitive information. Similarly, within the O-RAN framework, AI/ML optimizes and automates network operations through components like Near Real-Time RAN Intelligent Controller (Near-RT RIC) and Service Management and Orchestration (SMO), coupled with the Non-Real-Time RIC (Non-RT RIC). This otherwise beneficial integration might bring vulnerabilities, including the risk of data poisoning attacks that could compromise network performance and security.

AI/ML's role within NWDAF underscores its importance in adapting networks to dynamic conditions and user demands. Protecting NWDAF against poisoning and privacy attacks remains essential, especially in a multivendor environment. As 3GPP does not specify AI/ML-specific security controls, vendors must step in with appropriate measures.

Also, the automation capabilities provided by AI-driven OSS and BSS tools, while optimizing operations and customer experiences, might be exposed to evasion attacks.

A thorough understanding of the risks linked to AI/ML-powered components in mobile telecommunication networks and the implementation of effective mitigation strategies must be a strategic priority. Secure networks are essential for maintaining trust, protecting users, complying with regulations, and fostering innovation and growth in the mobile telecommunication industry.

AI/ML threat landscape in mobile telecommunication networks

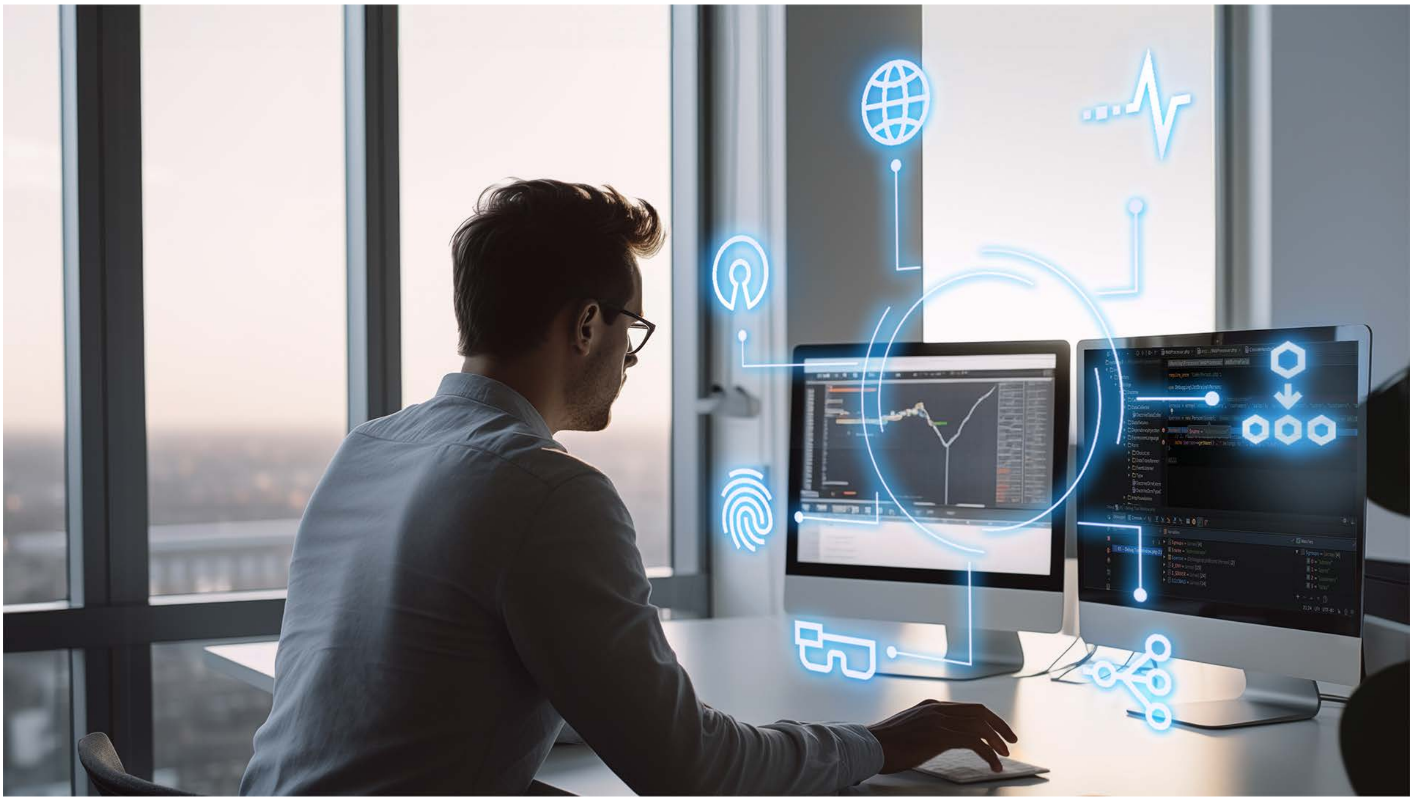
Even though AI/ML technologies bring a unique set of threats, they are not standalone units but are integrated into traditional mobile telecommunication systems. A comprehensive threat analysis should thoroughly assess the entire system, considering both threats to non-AI/ML entities and the environment in which AI/ML components run, as well as AI/ML-specific threats. This requires the development of defensive strategies that encompass both traditional and AI-specific security controls to maintain a robust security posture against a broad range of potential attacks.

AI/ML Environment threats are those that target vulnerabilities in components surrounding the AI/ML, such as the execution environment or data storage, rather than the model itself. These can be traditional forms of attacks, not specifically designed to exploit AI/ML vulnerabilities, but can still compromise the AI/ML system, especially if it automates existing processes. An attacker exploiting traditional vulnerabilities could even unknowingly compromise the AI/ML system, as well as the mobile telecommunication function it supports. Such attacks might also target the software development life cycle, deployment procedures, or communications and can result in compromised components or new exploitable vulnerabilities [6].

Threats relevant to the AI/ML environment include:

- Unauthorized access to training data or the model itself, to create a substitute model, steal model IP directly, or modify the model or its operation.
- Disruption of the operational environment, including DoS attacks. These can impact the availability of proper functioning of a model, particularly in client-server architectures.
- Supply chain attacks targeting critical components like the ML software stack or hardware elements.

Particular attention should be paid to AI/ML-specific threats. The assets at risk include AI/ML models and relevant data integrated into the mobile telecommunication system. Attackers might aim to compromise or manipulate these for various purposes, including disrupting operations or stealing IP. A structured approach to understanding AI/ML-specific threats is crucial and represented in NIST AML [7], MITRE ATLAS [6], OWASP ML Top 10 [8], and other relevant documents. Evasion attacks, for example, aim to alter ML model behavior with crafted queries, including prompt injection attacks on generative LLM models. Poisoning attacks contaminate training data or parameters, establishing backdoors and impacting deployment outcomes. Privacy attacks aim to extract information about the training data, targeting data (data privacy attacks), or the ML model (model privacy attacks). This includes scenarios where generative LLMs memorize and output training data verbatim.



AI/ML threat mitigation in mobile telecommunication networks

To mitigate attacks targeting the AI/ML systems, the first step is to identify threats to the AI/ML environment and AI/ML assets by performing a comprehensive security risk assessment [9]. Appropriate security controls, including both traditional and AI/ML-specific measures, are essential. The risk assessment, across the entire AI/ML development and operational lifecycle, helps identify and prioritize the necessary controls.

When there is a need to mitigate an identified threat, the first layer of defense involves implementing traditional security and privacy controls. These measures are effective against well-known threats and can also address some AI/ML-specific threats [6]. Factors to consider in implementing traditional controls are:

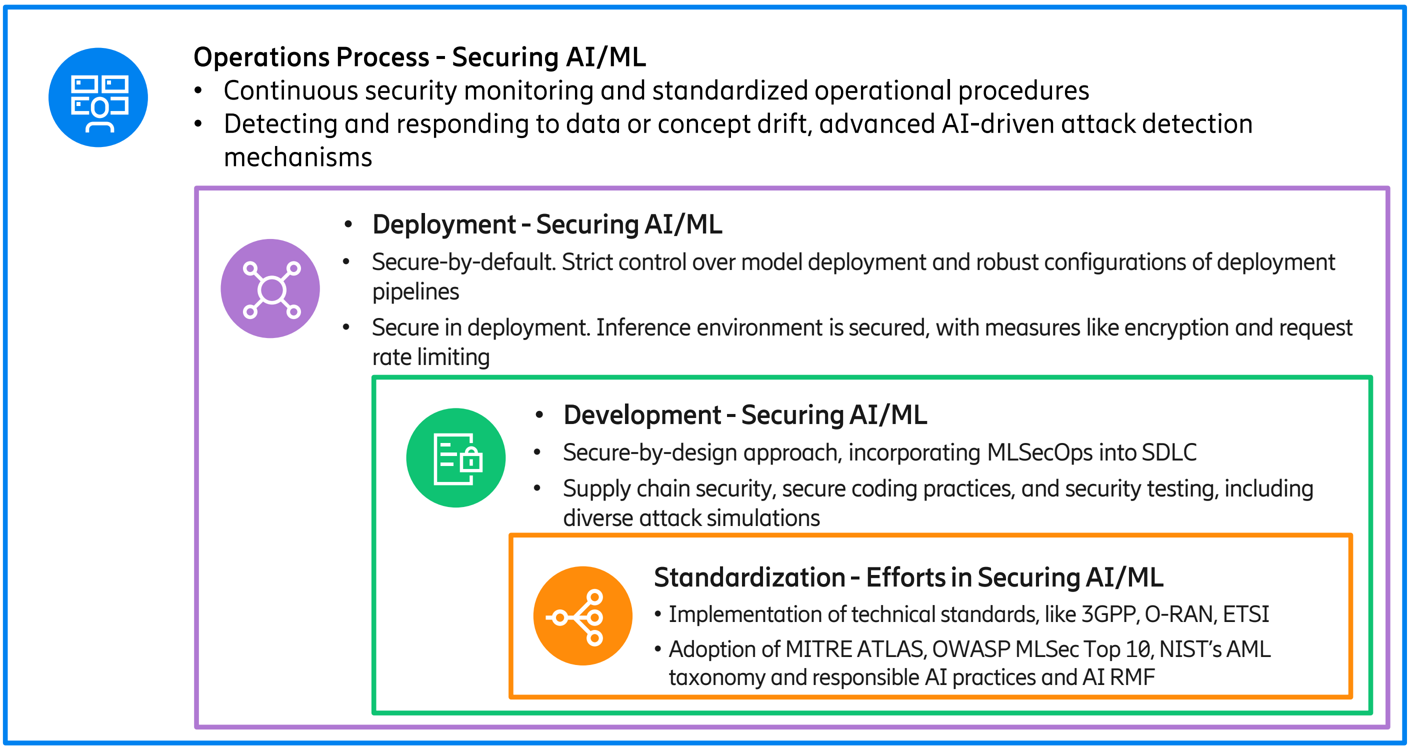
- Security measures must ensure confidentiality, integrity, availability, and authenticity. Allow only authorized access to data and ML models; prevent tampering; and verify data and model sources. Authentication and access control are crucial, limiting access and modifications to authorized entities and mitigating supply chain attacks.
- Security monitoring, regular auditing, and accountability practices help detect anomalies and ensure compliance with security standards.
- Data and model retention policies should define storage durations and conditions for deletion or archiving.
- Continual security training for ML teams is necessary to understand and uphold AI/ML system security.

In addition to these traditional controls, AI/ML systems might require specialized security controls to protect against unique types of attacks like evasion. Techniques for detecting and preventing AI/ML-specific attacks are outlined in NIST AML or OWASP ML Top 10 [10]. Since AI/ML attacks and mitigations are subject to ongoing research, the suitability of these methods requires further investigation and should be tailored to specific use cases. Good security practices to consider include:

- Resilient model design. Certain model designs, such as Ensemble Methods and Federated Learning, provide enhanced robustness against various attack types. Regularization Techniques also play a role in mitigating attacks by preventing overfitting and improving model generalizability.
- Model explainability, transparency, reproducibility, and auditability. A model's operating principles must be understandable (explainable), and its internal processes open to inspection (transparent) to mitigate risks such as evasion attacks. Ensuring that the outcomes generated by the model are reproducible and auditable is vital for consistent performance. Additionally, model design and development activities and processes should be well documented and recorded.
- Mitigations against evasion attacks. This can be challenging due to the prevalence of adversarial examples across AI/ML model architectures. These attacks can cause not only classification errors but also system malfunctions due to incorrect predictions. Methods to enhance system robustness include improving Robustness Against Evasion Samples, Adversarial Sample Detection, etcetera.
- Mitigations against data poisoning attacks. This helps maintain AI/ML model integrity, especially during training. Strategies like Training Data Sanitization and Training Data Distribution Monitoring help prevent corruption of training data or skewing of the model's learning process.
- Mitigations against privacy attacks. This protects the confidentiality of data used in AI/ML models. Strategies include Model Extraction Detection and using Synthetic Training Data. In collaborative ML environments, Privacy-Enhancing Technologies (PETs) are important for handling sensitive data, helping enable the extraction of valuable information through ML techniques while maintaining data privacy.

AI/ML-specific vulnerability analysis focuses on unique risks inherent to ML models and their data pipelines. The complexity of this analysis comes from the non-deterministic nature of AI/ML systems and the evolving nature of models, which complicates the assessment of test results. Tools like the Adversarial Robustness Toolbox (ART) and Counterfit can partly automate the AI/ML-specific vulnerability analysis process. Since AI/ML systems are data-driven, vulnerability analysis must encompass data handling, model training, and deployment stages.

Ericsson's holistic security approach depicted in Figure 2 is founded on the Ericsson trust stack model and designed to address and manage security challenges effectively [2]. This comprehensive approach, using the Ericsson Security Reliability Model (SRM) [10], includes key elements such as ensuring compliance with security standards as well as secure product development, deployment, and operations. It also emphasizes proactive cybersecurity measures, rigorous vulnerability management, and risk mitigation in the supply chain.



Operations Process - Securing AI/ML

- Continuous security monitoring and standardized operational procedures
- Detecting and responding to data or concept drift, advanced AI-driven attack detection mechanisms

Deployment - Securing AI/ML

- Secure-by-default. Strict control over model deployment and robust configurations of deployment pipelines
- Secure in deployment. Inference environment is secured, with measures like encryption and request rate limiting

Development - Securing AI/ML

- Secure-by-design approach, incorporating MLSecOps into SDLC
- Supply chain security, secure coding practices, and security testing, including diverse attack simulations

Standardization - Efforts in Securing AI/ML

- Implementation of technical standards, like 3GPP, O-RAN, ETSI
- Adoption of MITRE ATLAS, OWASP MLSec Top 10, NIST's AML taxonomy and responsible AI practices and AI RMF

Figure 2. Holistic security approach based on Ericsson trust stack to secure AI/ML components

The four layers in Ericsson's trust stack have been adapted to secure AI/ML components within mobile telecommunication networks. This adaptation incorporates findings and recommendations from academic research, industry insights, and cybersecurity authorities' knowledge about AI/ML risks and mitigations, as detailed in guidelines from respected bodies like the NCSC and CISA [11]. These findings have informed and shaped Ericsson's holistic security approach:

- Standardization Efforts in Securing AI/ML. Technical standards, like 3GPP, are key in developing AI/ML security frameworks for mobile telecommunication networks. Contributions such as AI Threat Ontology and Mitigation Strategy Reports from these bodies help unify AI security standards. NIST's efforts in taxonomy and responsible AI practices through its AI RMF also contribute significantly to the field.

- Securing AI/ML Development. Use a secure-by-design approach, incorporating MLSecOps into the SDLC. Consider supply chain security, secure coding practices, and comprehensive security testing, including diverse attack simulations.

- Securing AI/ML in Deployment. A secure deployment strategy includes strict control over model deployment and robust configurations of deployment pipelines. The inference environment should be secured, with measures like encryption and request rate limiting, to protect against various AI/ML-specific threats.

- Securing AI/ML Operations Process. Continuous security monitoring and standardized operational procedures should be used in the operations stage. Detecting and responding to data or concept drift, along with advanced AI-driven attack detection mechanisms, help maintain the security and integrity of AI/ML systems.

Security policy recommendations to policymakers

Integrating AI/ML technologies into mobile telecommunication networks brings benefits and risks. This paper analyzes AI/ML's impact on mobile telecommunication network security, providing recommendations within this context.

As AI/ML technologies become integral to mobile telecommunication systems, the complexity of cyber-attacks and defenses is expected to rise. Security measures must be flexible, adaptive, and scalable as AI/ML models grow in complexity and data volume. Important activities include:

- Developing standardized secure protocols and frameworks for AI/ML.
- Collaborative efforts in academia, industry, and standards organizations to address AI/ML's unique security challenges, such as standardized risk management, security assurance and governance tools, processes, and methodologies.
- Open-source projects, tools, and shared research that contribute significantly to advancing AI/ML security.

Governments, aside from regulating the resilience and cyber security requirements applicable to the ICT sector, have also a pivotal role in protecting civil society, businesses, and critical infrastructure service providers from cyber threat actors. In the AI/ML security context, as is already the case more broadly in cybersecurity, attackers often have an advantage in resources and opportunities. In terms of resources, of them decreasing amount of them is required to execute a cyberattack while a corresponding amount of resources will have a marginal impact on strengthening resilience. In terms of opportunity, attackers only need to exploit one vulnerability, while defenders must secure all aspects of a system. Advancements during late 2022 and 2023 in generative LLMs have lowered the skill barrier for launching attacks, potentially giving attackers the upper hand in using AI tools for large-scale, low-cost attacks. In contrast, defenders face numerous interfaces and architectural components to protect, often incurring higher financial costs than attackers. This disparity demands increased government action to raise threat actors' costs and difficulty in launching attacks and to provide more support to defenders.

Mobile networks, as part of national infrastructures, are already subject to comprehensive regulations for security and privacy, which consequently will also influence the security requirements of AI/ML components used in mobile telecommunication networks. In addition, AI/ML- specific regulations will set requirements that will ensure the security of mobile telecommunication networks. The primary policy goal should be to continue to safeguard users of mobile networks, ensuring that AI/ML components used in networks align with security and privacy standards and requirements. Furthermore, policymakers should enable the industry to maximize benefits from AI/ML, including in the security domain, but do so in ways that do not slow innovation through over-regulation while avoiding compromising targeted security and resilience objectives. This can be achieved by considering the following recommended cybersecurity policy actions:

- Stimulate research on how AI/ML can be employed to enhance threat detection within mobile telecommunication networks and other critical IT and OT systems.
- Engage with the industry to continue to evolve a shared understanding of the telecom-specific threat landscape, including focusing on 5G evolution and future 6G systems.
- Promote increased awareness of structured approaches to AI/ML-specific attacks, such as those elaborated in the NIST AML.
- Work with industry to develop sector-specific best practices for mitigating AI/ML-enabled traditional and novel attacks.
- Stimulate research and foster a broad implementation of relevant security controls such as those identified by MITRE, OWASP, and NIST AML.
- Update security risk assessments in existing regulatory frameworks, through implementation guidelines that include relevant AI/ML security risk assessment practices, leveraging the NIST AI RMF.
- Promote standardization work, including:
  - Work with standardization, industry, and regulatory bodies to harmonize efforts in AI/ML security encompassing risk management, regulations, secure AI/ML operation, lifecycle management, tools, testbeds, and privacy-enhancing technologies [12].
  - Foster advancements of security standards such as the ISO and IEC that established a joint standardization committee on AI, namely ISO/IEC JTC 1/SC 42 to ensure that competent national agencies are involved in this process.
  - Engage competent authorities to share relevant security policy priorities in the ongoing work on AI/ML technical standards and specifications for mobile telecommunications such as through work in 3GPP, O-RAN Alliance, GSMA, ATIS/NGA, ISO, and ETSI.
- Promote AI/ML security best practices, and where appropriate support by public funding of open-source projects, including secure-by-design approaches, integrating AI/ML into software development and supply chain risk management frameworks, and integrating MLSecOps into the software development lifecycle.
- Promote advancements in confidential computing to ensure secure and trusted execution environments for virtualized AI/ML training and applications. In addition, other advancements in privacy-enhancing technologies to protect privacy and remove barriers to data sharing without violating privacy should be encouraged.

The unique challenges of securing AI/ML systems in the mobile telecommunication domain require specialized skills. Educational and training programs will need to update curricula to prepare the next generation for the challenges of this fast-changing field.

Securing mobile communication infrastructure, including the AI/ML components within, requires a cooperative approach across all the organizations involved in standardizing, developing, implementing, and operating it. The cooperative approach also requires maintaining clarity on stakeholders' roles and responsibilities. Software developers and suppliers are responsible for the security and quality of the products that they develop. Network service providers are responsible for securing the configuration and implementation of discrete products into operational networks and for the day-to-day operation of these networks that they use to provide services. Policymakers have the overall responsibility for protecting society against cyber threat actors, including criminal and state actors. Ultimately the overarching policy objective should be to decrease cyber threats. Governments are also responsible for setting rules and requirements that define security and resilience objectives, facilitate cooperation between stakeholders, and provide incentives for research activities. A synergistic partnership between government and industry is the best path for effective cyber defenses to ensure the security of users and the resilience of mobile networks.

Glossary

3GPP - 3rd Generation Partnership Project

AI - Artificial Intelligence

AML — Adversarial Machine Learning, the process of extracting information about the behavior and characteristics of an ML system and/or learning how to manipulate the inputs into an ML system in order to obtain a preferred outcome.

ATIS/NGA — Alliance for Telecommunications Industry Solution/Next G (Generation) Alliance

BSS - Business Support Systems

ChatGPT — Open AI's Chat-based Generative Pre-trained Transformer

CISA — Cybersecurity and Infrastructure Security Agency of the United States

DDoS - Distributed Denial of Service

ETSI - European Telecommunications Standards Institute

GSMA - Global System for Mobile Communications Association

ICT - Information and communication technology

IEC - International Electrotechnical Commission

IMSI - International Mobile Subscriber Identity

ISO - International Organization for Standardization

LLM - Large Language Model

MITRE — MITRE corporation

ML - Machine Learning

MLSecOps - Machine Learning Secure Development and Operations

NCSC - National Cyber Security Center of the United Kingdom

Near-RT RIC - Near-Real Time RAN Intelligent Controller

Non-RT RIC - Non-Real Time RAN Intelligent Controller

NG-RAN - Next Generation Radio Access Network

NIST - National Institute of Standards and Technology

NWDAF - Network Data Analytics Function

OECD - Organization for Economic Co-operation and Development

O-RAN Alliance - Open Radio Access Network Alliance

OSS - Operations Support Systems

OT — Operational Technology

OWASP - The Open Worldwide Application Security Project

PoisonGPT — A generative AI model designed to stealthily spread disinformation.

RAN - Radio Access Network

Risk Management Framework

SDLC - Software Development Life Cycle

SMO - Service Management and Orchestration

UE — User Equipment

References

1. "OECD Digital Economy Papers, Enhancing the security of communication infrastructure," [Online]. Available: https://www.oecd-ilibrary.org/science-and-technology/enhancing-the-security-of-communication-infrastructure_bb608fe5-en.

2. "A guide to 5G network security 2.0," [Online]. Available: https://www.ericsson.com/en/security/a-guide-to-5g-network-security.

3. "How AI-Powered Cybersecurity Combats Growing AI Threats," [Online]. Available: https://www.sap.com/insights/viewpoints/ext-how-ai-powered-cybersecurity-combats-ai-threats.html#:~:text=AI,early%20alerts%2C%20signaling%20potential .

4. "StegoNet: Turn Deep Neural Network into a Stegomalware," [Online]. Available: https://dl.acm.org/doi/10.1145/3427228.3427268.

5. "Effective and explainable AI – a use case of false base station detection," [Online]. Available: https://www.ericsson.com/en/blog/2023/10/effective-and-explainable-ai.

6. "MITRE ATLAS," [Online]. Available: https://atlas.mitre.org/matrices/ATLAS/ .

7. "NIST AI 100-2 E2023, Adversarial Machine Learning," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf.

8. "OWASP Machine Learning Security Top Ten," [Online]. Available: https://owasp.org/www-project-machine-learning-security-top-10/.

9. "AI risk management framework," [Online]. Available: https://www.nist.gov/itl/ai-risk-management-framework.

10. "Our Security Reliability Model," [Online]. Available: https://www.ericsson.com/en/security/ericssons-security-reliability-model.

11. "Guidelines for secure AI system development," [Online]. Available: https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development.

12. "CISA Roadmap for Artificial Intelligence," [Online]. Available: https://www.cisa.gov/sites/default/files/2023-11/2023-2024_CISA-Roadmap-for-AI_508c.pdf.

Ericsson enables communications service providers, enterprises and the public sector to capture the full value of connectivity. The company's portfolio spans the following business areas: Networks, Cloud Software and Services, Enterprise Wireless Solutions, Global Communications Platform, and Technologies and New Businesses. It is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's innovation investments have delivered the benefits of mobility and mobile broadband to billions of people globally. Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.

ericsson.com

The content of this document is subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document

© Ericsson AB 2024