Secure ML Model Deployment for Edge Devices

Update AI Systems with Security, Robustness, and Privacy ensured

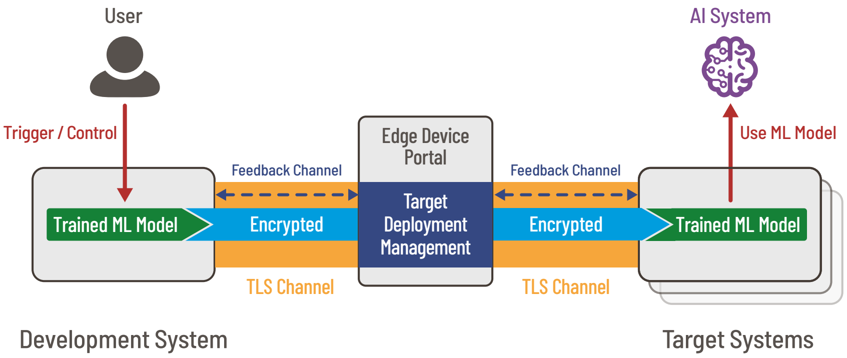
in cooperation with swissbit

/ Overview

Secure AI Update Solution by aicas and Swissbit

Updating AI systems involves significant security threats. aicas' edge-to-cloud solution for embedded systems provides a secure way to deploy AI applications and their components such as machine learning models to remote edge devices and vehicles.

It ensures seamless transfer of ML model updates, including transmission, installation, and operation. With encrypted, signed components and secure communication channels, the solution offers maximum security, robustness, and protection against unauthorized access, thus ensuring safe operation of edge AI systems.



/ The Challenge

Security Threats in Transferring ML Models to Edge Devices

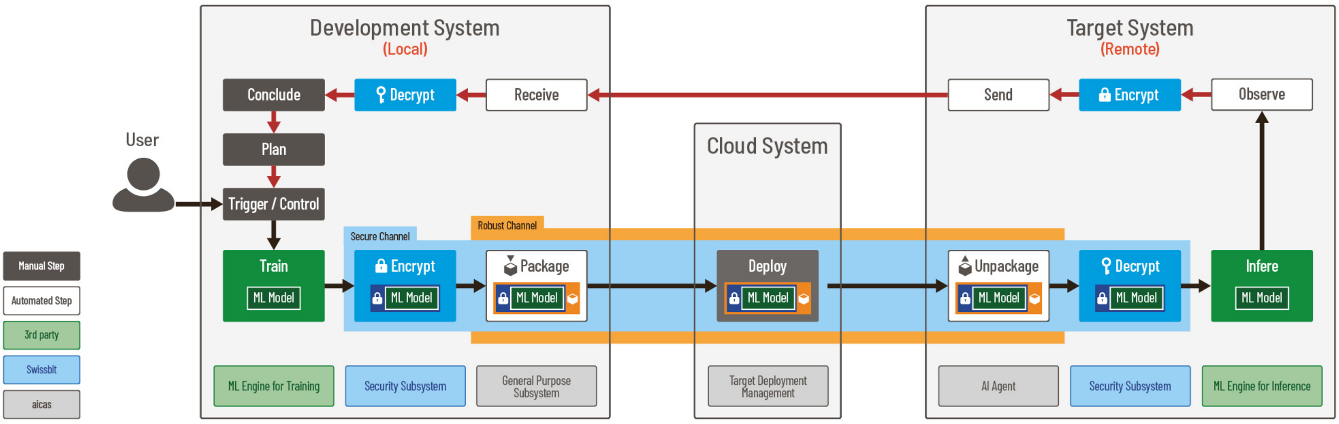
AI systems constantly evolve, leveraging data to enhance performance. Updating machine learning models and securely transmitting them to remote edge devices pose critical security challenges. These devices often operate in remote or heterogeneous environments, making them susceptible to unauthorized access, data leaks, theft, or manipulation. Failing to address these risks can lead to severe financial, legal, and reputational consequences, underscoring the need for robust security measures during AI system updates.

The AI update solution prevents risks and ensures

Robustness	Security	Privacy	Operational Integrity
Preventing model mis-matches, alterations, or execution errors.	Protecting models from theft, and tampering.	Protecting sensitive information encoded in models, both in transit and at rest.	Secure live reporting on AI application updates and execution.

/ The Solution

ML Model Lifecycle Workflow



The solution enables seamless transfer of ML models from development systems, via the cloud, to edge devices in an MLOps workflow:

1. Train a ML model (upstream process).
2. Securely deploy the model to devices at the edge (aicas' solution).
3. Use the model in edge applications.
4. Gather performance data.
5. Improve the model with enhanced data (downstream process).
6. Repeat.

/ Core Components

The Solution Components

aicas Edge Device Portal

Model Management:
Stores the packaged and encrypted ML models while "in motion."

Secure Connectivity:
Manages secure connections between the training system and target systems.

Distribution Oversight:
Supervises the ML model's distribution process.

Operator Feedback:
Provides visual feedback for human operators.

AI Agent on JamaicaAMS

Model Deployment:
Executes the distribution process, unpacks, triggers decryption, and installs the ML model in the inference engine. Supervises the ML application and provides feedback and data for training.

Swissbit Hardware Security

Enhanced Protection:
Provides the hardware anchor for advanced security in-system validation, encryption, and digital signatures—even plug-in for devices that do not yet have a dedicated security module.

SECURED BY
swissbit

/ Solution Details

Key Features of the Comprehensive Protection for Your Edge AI Systems

Key Feature	Benefit
Encrypted and Signed Model Updates	Secure and Reliable Model Transmission
Digital Signatures and Version Control	Reliable Model Authentication and Integrity
Centralized Management, OTA-Updates, and Device Health Monitoring	Simple Management of Diverse Edge Devices
End-to-End Encryption and Role-Based Access Control	Data Privacy

/ Key Benefits

Security Protection That Avoids Costs and Revenue Losses

- Prevention of Unauthorized Model Manipulation
- Data Protection and Privacy
- Ease-of-Use & Ease-of-Integration
- Resilience Against Attacks and Flaws
- Reputation Safeguard

/ Use Case Example

AI Systems Advanced by aicas‘ and Swissbit‘s Secure Solution

AI systems that benefit most from aicas‘ and Swissbist’s common solution operate edge devices in remote locations and require secure updates outside of a firewall. Examples:

IIoT: Industrial Automation

- Industrial devices such as sensors and actuators
- Building technologies like security cameras and presence detection systems
- Robotics for manufacturing and warehouse automation
- Predictive maintenance sensors on machines and equipment

Mobility and Automotive

- Autonomously controlled vehicles like drones and self-driving cars
- Smart traffic management systems
- Vehicle-to-everything (V2X) communication devices
- Fleet management systems for realtime monitoring of vehicles

Get in touch with us to learn more about the solution!

aicas GmbH
Emmy-Noether-Str. 9
76131 Karlsruhe, Germany

Web: www.aicas.com
Email: info@aicas.com
Phone: +49 721 663 968 0

Sign up for our Newsletter!