23.June.2023

REBOTNIX

Secure authentication for edge computing.

Crypto Authentication

Written by
Gary Hilgemann

REBOTNIX AI HUB GERMANY

REBOTNIX

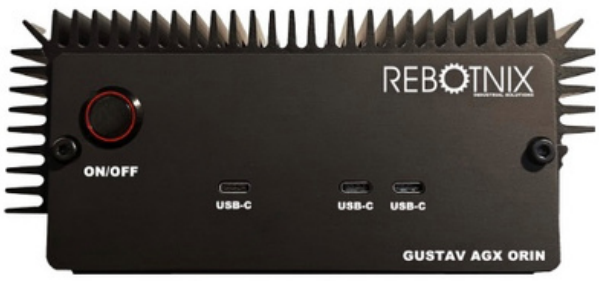
Why extra hardware for AI apps?

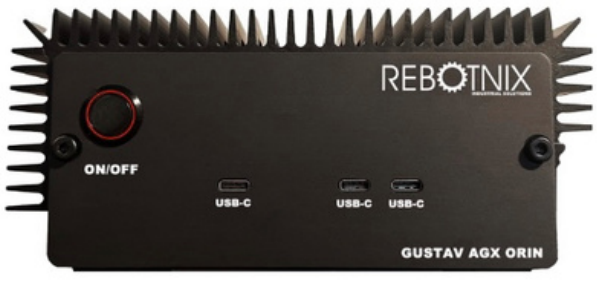
For the verifiability of AI applications as well as the European cybersecurity law and the upcoming AI ACT, proof of generated AI data of the liability issue is mandatory.

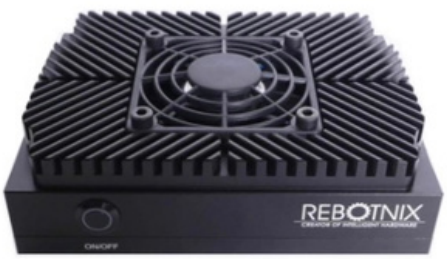
As of now, June 2023, all REBOTNIX edge systems include a hardware 256 bit based cryptochip on the mainboard. In combination with NVIDIA JETSON GPU, all addons, we can now create more secure AI applications.

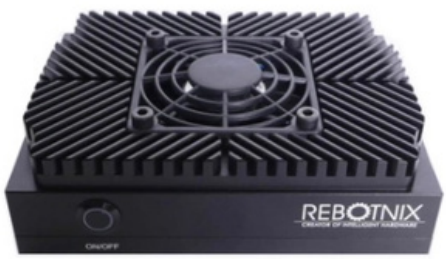
The new Crypto Element with Protected Hardware-based Key Storage.

Cryptochip now included in every GUSTAV edge device.









REBOTNIX

Features

- Crypto Element with Protected Hardware-based Key Storage
- Secure Symmetric Authentication Device Host and Client Operations.
- Superior SHA-256 Hash Algorithm with Message Authentication Code (MAC) and Hash-Based Message Authentication Code (HMAC) Options
- Best-in-class, 256-bit Key Length; Storage for Up to 16 Keys
- Guaranteed Unique 72-bit Serial Number
- Easy to use REBOTNIX free crypto programmer test and run application (only with hardware). Python, C++, JS bindings.

Physical Security

- An Active Shield Over the Part
- Internal Memory Encryption
- Glitch Protection
- Voltage Tamper Detection

REBOTNIX

Applications

Part One

Progress and Performance Report

Anti-counterfeiting

Validating that a removable, replaceable, or consumable Client is authentic. The device can also be used to validate (authenticate) a software/firmware module or memory storage element.

Protecting Firmware or Media

Validating code that is stored in flash memory at boot time to prevent unauthorized modifications (this is also known as secure boot), encrypt downloaded media files, and uniquely encrypt code images to be usable on a single system only.

REBOTNIX

Applications

Part Two

Progress and Performance Report

Exchanging Session Keys Securely and easily exchanging

Securely and easily exchanging stream encryption keys for use by an encryption/decryption engine in the GPU system, between AI Modells to manage a confidential communications channel, an encrypted download, and similar items.

Storing Data Securely

Storing secret keys for use by crypto accelerators in standard microprocessors. It can also be used to store small quantities of data necessary for configuration, calibration, ePurse value, consumption data, or other secrets. Programmable protection up through encrypted/authenticated reads and writes

Checking User Passwords

Validating user-entered passwords without letting the expected value become known, mapping simple passwords to complex ones, and securely exchanging password values with remote systems.

REBOTNIX

Question & Information

https://rebotnix.com