Mehr Licht!
More Photonics for Intelligence

#A06

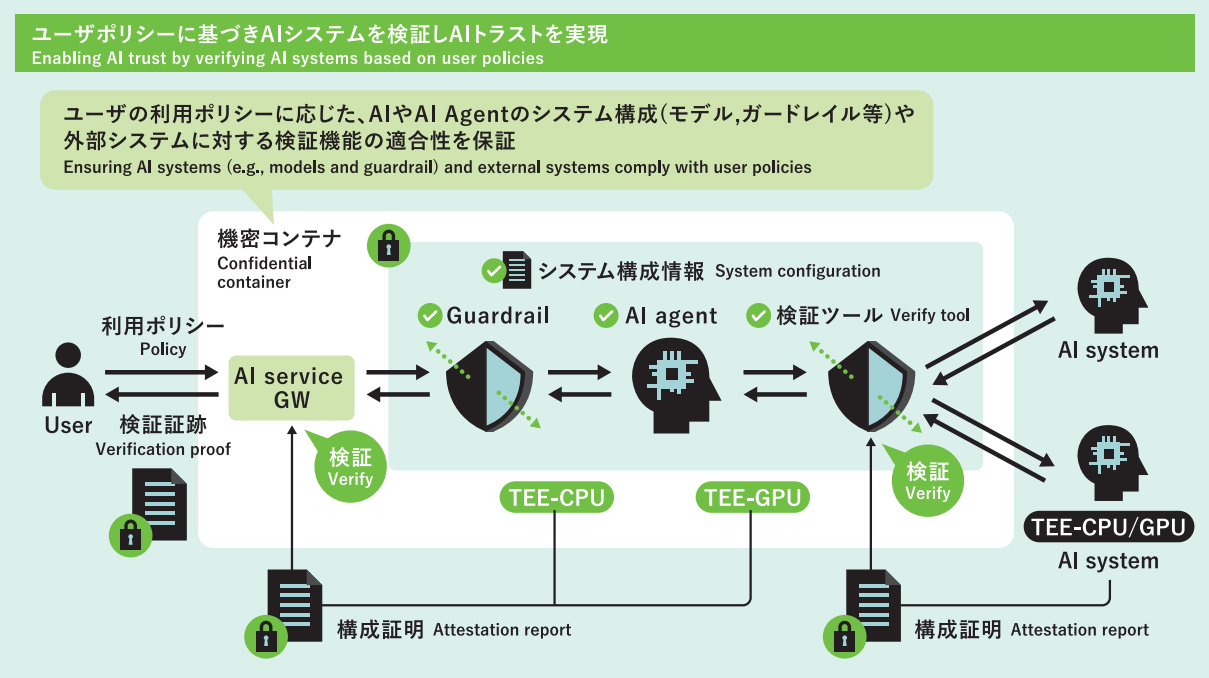
#AI & Quantum Infrastructure#Responsible AI#Safety and Security

Container Platform for Enabling AI Trust

Verify that your AI/agent is configured, behaves, and operates safely

Technical Challenges & Goals

As AI become widely used, users face concerns about misuse of personal data and unexpected behavior. We aim to enable users to verify AI's execution environment, model, data-use policies, and safeguards, enabling them to use AI and AI agents with confidence without blindly trusting service providers.



Key Technologies

Core Technologies

- TEE-CPU/GPU confidential containers ensuring AI/AI-agent data confidentiality and app integrity
- Generic platform supporting unmodified apps, multi-container setups, and secure data persistence

Key Differentiators

- User-verifiable AI and AI agent security without requiring implicit trust in service providers
- Generic verification applicable to any AI agent or LLM, independent of specific implementations

Use Cases

Communication Services

For personal AI agents handling sensitive data and tasks such as bookings and purchases, users can verify the environment, model, and safeguards, enabling them to confidently entrust their data and tasks to AI agents.

Exhibitors

NTT, Inc. Network Service Systems Laboratories

Related Links

https://www.rd.ntt/ns/inclusivecore.html

CONTACT:Network Architecture Project