Hardware-Software Co-Design to Accelerate Garble Circuits

Technology

Novel in its approach, HAAC is a garbled circuit accelerator and compiler that enhances privacy-preserving computation, offering a practical solution to data privacy challenges without compromising system performance.

Background

In today's digital age, data privacy and security are paramount. Yet, ensuring these often comes at the cost of system performance. Enter HAAC - a revolutionary garbled circuit accelerator and compiler designed to enhance privacy-preserving computation. Through a unique hardware-software co-design approach, HAAC mitigates performance overheads, making privacy-preserving computation more practical and efficient. Whether you're a cybersecurity company, a cloud service provider, a government agency, or a financial institution, HAAC offers a promising solution to your data privacy challenges without compromising system performance. Embrace the future of secure computation with HAAC.

Applications

HAAC has many applications, particularly in sectors where data privacy and security are paramount.

- **Cybersecurity companies:** HAAC can enhance the security of systems by computing functions directly on encrypted data.
- **Cloud service providers:** HAAC can be used to offer more secure and efficient services to their clients.
- **Government agencies:** HAAC can be used to ensure the privacy and security of sensitive data in their systems.
- **Financial sector:** HAAC can be used to protect sensitive financial data and transactions.
- **Healthcare organizations:** HAAC can be used to secure patient data and other sensitive health information.

Advantages

Category

Software & IT/Cloud Computing

Software & IT/Cyber Security

Tarianna Stewart

Authors

Brandon Reagen, PhD

Learn more

- **Enhanced Data Privacy:** HAAC computes functions directly on encrypted data, providing a higher level of data privacy.
- **Improved System Performance:** By mitigating the performance overheads associated with garbled circuits, HAAC ensures efficient system performance.
- **Versatility:** HAAC supports arbitrary computation, making it adaptable to various applications and sectors.
- **Hardware Efficiency:** The hardware-software co-design approach of HAAC maximizes the area devoted to custom execution units and other essential circuits, ensuring hardware efficiency.
- **Programmable Interface:** HAAC offers a programmable interface via an ISA, providing flexibility and ease of use.
- **Potential for Speed:** In evaluations, HAAC has shown significant speedup potential, making it a promising solution for real-time applications.

Intellectual Property

US Provisional Application number 63/521,675