INTEL: PROTECTING DATA AND MODELS WITHIN EMERGING AI WORKFLOWS

EXECUTIVE SUMMARY

The rise of artificial intelligence (AI), fueled by the overwhelming popularity of AI-powered language models like ChatGPT, along with the broader generative AI applications, spotlights the importance of data security.

The large amount of data AI requires to train models makes data security paramount. Beyond securing the data used to build large language models (LLMs) — public and foundational — protecting the AI models themselves becomes equally important. This is true cross-domain, public and private, on-premises, in the cloud, and at the network edge.

In addition, ensuring the ease of deployment and ongoing management of AI operations is also key— and it all must easily integrate into developer operational processes and workflows, or it will risk adoption failure.

The looming threat of adversarial AI used by bad actors intending to compromise model integrity, access private data, and destroy reputation through model poisoning is real. Securing AI must, therefore, span all stages, from ingestion through preparation, model training, deployment, inferencing, and results. Some models also require a query engine that may have sensitive information that requires protection.

It is no surprise, then, that enterprises now demand AI security capabilities that protect the underlying data, models, workflows, and the corresponding operating environments.

4th Gen Intel® Xeon® Scalable processors, hardened with Intel Software Guard Extensions (SGX) or Trust Domain Extensions (TDX), provide deep, silicon-level protection for today's emerging AI workflows. Intel's contributions to confidential computing, buoyed by extensive partnerships with industry leaders, also have the potential to ensure both model and data integrity, as well as accelerate the AI developer journey. The potential value in Intel's offering is significant — allowing companies to maximize AI investments, gain deeper insights, meet compliance requirements, and provide transformational, innovative services.

Copyright ©2023 Moor Insights & Strategy

INTEL'S AI INVESTMENTS

Confidential computing offers hardware-based security on-premises, in the public cloud, and network edge, protecting workload data in use. Intel's approach aims to integrate security extensions into its x86 CPU architecture designed to deliver silicon root of trust. Intel SGX and TDX support the security of AI workflows with multi-domain protection and proof through attestation based on zero-trust principles.

Intel SGX is arguably the most deployed confidential computing technology in data centers today. It employs hardware-based memory encryption that isolates specific application code and data in memory. SGX facilitates this functionality by allocating private regions of memory, often called secure enclaves, that are protected from processes that run at higher privilege levels.

Intel TDX provides virtual machine (VM) isolation from virtual machine managers and hypervisors within public cloud deployments. This capability creates trust domains that have the potential to safeguard against a broad range of software. Intel TDX will soon be available on select 4th Gen Intel Xeon Scalable processors through four leading cloud providers. Intel TDX becomes generally available with 5th Gen Intel Xeon Scalable processors in the future.

Together, Intel SGX and TDX offer a complete, end-to-end AI model and data protection platform spanning on-premises, public cloud, and network edge. Given the hybrid, disaggregated nature of modern information and operational technology infrastructure deployments, Moor Insights & Strategy believes that Intel's vision and execution to support emerging AI workflows is compelling.

INTEL ECOSYSTEMS AND PARTNERSHIPS DRIVING AI VALUE

Beyond Intel SGX and TDX available in 4th Gen Intel Xeon Scalable processors, the company is active in a multitude of software and solution ecosystem activities through the Intel Partner Alliance (IPA) and Accelerated by Intel programs that support the broad adoption of its confidential computing platform. Intel is also engaged in several partnerships contributing to AI workflows. Four partnerships, in particular, warrant mention:

1. Fortanix is a data security company that provides solutions that scale across multiple domains and accelerate AI inference in the cloud. The company's Confidential AI platform leverages Intel SGX to enable general-purpose

computation on encrypted data without exposing the underlying application code and data to an operating system or any other runtime process. The ultimate value of Intel's contribution lies in its ability to protect sensitive data for analytics in highly regulated industries that might not otherwise take the risk to do so. It also facilitates improved usability and the flexibility to import AI models safely and securely.

2. HiddenLayer is an AI application security company that protects machine learning (ML) from inference, bypass, extraction attacks, and model theft through behavior analysis. The company's ML Model Scanner platform uses Intel SGX to enable the smallest trust boundary possible to deliver on the promise of confidential computing. Intel and HiddenLayer are also jointly engaged in ongoing research, customer education, and channel partner sales enablement designed to improve the offering and scale its availability.
3. BeeKeeper AI provides a clinical AI platform designed to create secure data access in supporting high-quality, impactful algorithm validation and development in the healthcare industry. The company is leveraging Intel SGX to reduce the validation time of AI algorithms by half, significantly mitigating costs and accelerating time to market. Some examples of BeeKeeper AI clinical models that incorporate Intel SGX include diabetic retinopathy treatment tools and the training and validation of an algorithm that allows Novartis scientists to predict instances of a rare childhood condition with actual patient data.
4. Decentriq provides data clean room solutions that leverage AI-predicted insights and decision-making on first-party data sets with applicability across diverse industries, including life sciences and advertising technology platforms. The corresponding AI models can be deployed in secure Intel SGX-protected enclaves to enable bilateral collaboration that ensures data privacy and security.

CALL TO ACTION

AI will continue to disrupt enterprise processes and service delivery and accelerate positive business outcomes across multiple industries and domains. However, careful consideration must be paid to the protection of data and the underlying models. The task mandates securing the data that feeds AI across the entire lifecycle, including ingestion through preparation, model training, deployment, inferencing, query, and results.

Moor Insights & Strategy believes that 4th Gen Intel Xeon Scalable processors featuring Intel SGX and TDX, as well as the company's investment in ecosystem initiatives,

Copyright ©2023 Moor Insights & Strategy

partnerships and the creation of innovative trust services that support independent attestation such as Project Amber, can help organizations safeguard emerging AI workflows. Intel continues to demonstrate a consistent track record of accomplishments in broadening adoption of confidential computing at the silicon level, and this is translating to its emerging success in achieving the same with confidential AI through its support of AI-powered ecosystems, security, and compliance.

CONTRIBUTOR

Will Townsend, Vice President & Principal Analyst, Networking & Security Practices at Moor Insights & Strategy

PUBLISHER

Patrick Moorhead, Founder, President, & Chief Analyst at Moor Insights & Strategy

INQUIRIES

Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

This document, including any supporting materials, is owned by Moor Insights & Strategy. This publication may not be reproduced, distributed, or shared in any form without Moor Insights & Strategy's prior written permission.

DISCLOSURES

Intel commissioned this paper. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.

©2023 Moor Insights & Strategy. Company and product names are used for informational purposes only and may be trademarks of their respective owners.