CASE STUDY

Intel® Software Guard Extensions
Federated Learning
Artificial Intelligence

Break Down Data Silos with Hardware-enhanced Security Technology to Accelerate Federated Learning Practices

Intel® Software Guard Extensions Helps China's Ping An Technology Successfully Apply Federated Learning to Multi-source Data Collaboration for AI Training

平安科技
PING AN TECHNOLOGY

"The federated learning technology accelerates the advancement of artificial intelligence by helping ensure data security and privacy protection. Intel® Software Guard Extensions is ideal for building hardware trusted execution environments in federated learning solutions. Through processor instructions, it creates trusted zones in different data sources for data access. This helps us enhance the training effect of AI models with multi-source data through further improving data security."

Dr. Jianzong Wang
Deputy Chief Engineer,
Ping An Technology
Council Member, Guangdong Society of Artificial Intelligence and Robotics
Vice Chairman, China Artificial Intelligence Open Source Software Development League

High quality and a high volume of data has become crucial for businesses to build their core competitiveness in Artificial Intelligence (AI). And for China's Ping An Technology, their Federated Learning Technology Team is exploring ways of aggregating more-dimensional and higher-quality data from more sources using the federated learning approach in order to improve AI model training.

However, the exchange, transmission and aggregation of multi-source data also brings complex data security issues, especially in sensitive industries and sectors, where the risk of data breach is in the spotlight with attention of both authorities and the general public. This has resulted in the introduction of a series of laws and regulations on data protection. Without a secure, trusted multi-source data collaboration solution, it would be difficult to break these silos of multi-source data and the development and adoption of federated learning would undoubtedly be hindered.

A viable approach to address this problem is to create a Trusted Execution Environment (TEE) in specific hardware with the support of hardware-enhanced security technologies to protect sensitive data and applications from external access and attack. Through in-depth technical cooperation with Intel, the Federated Learning Team successfully introduced Intel® Software Guard Extensions (Intel® SGX) technology, a key pillar of the TEE solution, to its federated learning solutions. By doing so, the Federated Learning Team pioneers the implementation of AI training with a multi-source data collaboration solution, achieving noteworthy results in areas such as insurance, healthcare, intelligent voice and Internet of Vehicles (IoV) with much positive feedback from users.

Advantages of the Federated Learning Team's Solution:

- Through processor instructions, Intel SGX creates memory "enclaves" that better ensure data security on each node of federated learning for the exchange and transmission of intermediate parameters, helping to prevent internal and external attacks and providing more reliable security for implementation and exploration of federated learning in a multi-source data environment;
- The 1+N federated learning solution which integrates Intel SGX helps to accurately evaluate the contribution of data on each node to the AI model training and facilitates a user's ability to adjust the solution.

Federated Learning Practices Lend Weight to the AI Training Evolution

More mature algorithms and more plentiful computing power make large-scale and high-quality data an important factor affecting AI performance. However, in the process of AI adoption in various industries, insufficient training data has produced lackluster results in the training of AI models since data sources which belong to different businesses and departments are separated from each other. Traditionally, the system needs to integrate data to train models with data from multiple sources, but this approach does not guarantee the security of data exchange and increases the risk of data leakage.

As data security and privacy gain increasing attention, governments are increasing the protection of them through laws and regulations. For example, the “Guideline for Internet Personal Information Security Protection” officially released in China in April 2019 has clear provisions for personal information sharing and transferring, and further strengthens measures for personal information protection[1]. In May 2019, the Cyberspace Administration of China, together with relevant authorities, drafted the “Measures for Data Security Management (Consultation Paper)”, which provides clear opinions on and requirements for data processing and utilization as well as supervision and management of data security[2].

AI training therefore requires a safe data aggregation method to enhance multi-source data collaboration capabilities. With their sensibility to the development of AI and big data technologies, the Federated Learning Team proactively explores the increasingly mature federated learning approaches. Different from traditional data sharing methods, the data on each node in the federated learning approach is kept on premises for the training, so each data source is expected to participate in and promote optimization of the AI model and share optimization results on the basis that data privacy is guaranteed.

Based on this concept, the Federated Learning Team has now built a Hive Platform for Federated Learning to provide users with a one-stop solution to protect their data privacy and security. Whilst building the platform, the solution needs to resolve issues such as how to further enhance the security of multi-source data on premises, how to provide a more reliable security guarantee for the interim process of optimizing the AI model and how to effectively evaluate the contribution of each data source to the final optimization result. The Federated Learning Team and Intel have provided a better solution to these issues by introducing Intel SGX technology.

Hardware-enhanced Security Technology Empowers Federated Learning

In the process of aggregating multi-source data to implement the AI model training with the federated learning method, AI models or process parameters need to be transmitted and exchanged at various data nodes through the network. It is well known that the greater the data exposure is, the higher security risks that data faces. Therefore, no matter what hardware infrastructures or operating systems in each node, or which network devices such as routers and gateways are used, they could bring security risks like data leakage and tampering if they become "polluted".

For example, a hacker may intercept data messages by installing a sniffer in a transmitter on the network or use a cold boot attack to read data remanence after the server has been restarted, or even attack the data in memory directly by methods of memory bus snooping or memory tampering. With an assortment of attack methods possible, it is difficult to secure the system and build a bottom-up protection and prevention mechanism covering software and hardware as well as the operating system. Efforts to build such a mechanism are a drain on resources and will increase the Total Cost of Ownership (TCO) without necessarily providing satisfactory results in actual protection scenarios.

Building a TEE solution for trusted zones in hardware is a better option to solve these issues. As a key element in the implementation of this solution, Intel SGX enables creation of a trusted "enclave" in specific hardware (such as memory), with security boundaries of data and applications limited to the "enclave" itself and the processor as shown in Figure 1. At the same time, its operation does not rely on other hardware or software, meaning that data security and protection are independent of the operating system or hardware configuration so that even if hardware drivers, virtual machines or the operating system itself are attacked and destroyed, data leakage can be prevented more effectively.

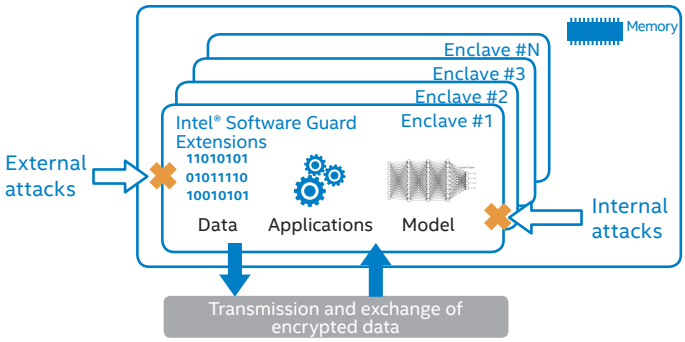

Figure 1. Intel SGX enhances data security with trusted “enclaves”

Based on the features of Intel SGX, the Federated Learning Team worked with Intel to design a 1+N multi-source data AI model training approach in its federated learning solution, resolving data security and training effect assessment issues better.

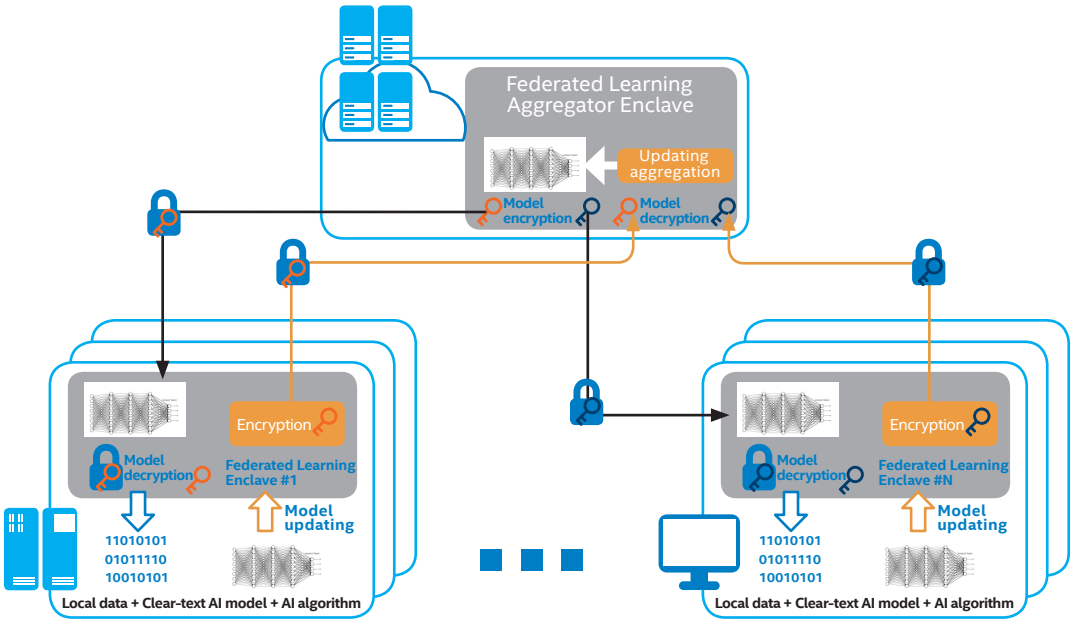

Figure 2. Federated learning solution using Intel SGX

The new 1+N solution architecture is shown in Figure 2. In it, an aggregator "enclave" located at the center and N edge "enclaves" deployed elsewhere comprise a network. “Enclaves” in the aggregator and data source systems are all trusted zones created in the memory through processor instructions provided by Intel SGX.

In the 1+N solution, what needs to be transmitted in an encrypted channel are the AI model to be trained and optimized and the related intermediate parameters, while training data, the clear-text AI model and the AI algorithm are kept in the node where each data source is located. In the initialization process, "enclaves" will generate public-private key pairs themselves, with the public key being registered to the aggregator and the private key stored in their own "enclaves" respectively. When training begins, the aggregator first establishes an encrypted connection with the target "enclave". The symmetric encrypted key for this connection is provided through negotiation using the asymmetric algorithm of the public-private key pairs, helping prevent a Man-in-the-Middle Attack. After the connection has been established, the aggregator first encrypts the AI model to be trained and pushes it to each “enclave” and then each “enclave” decrypts the model and transmits it to the local AI training environment to train the local data. After the training, the local AI training environment returns the intermediate parameters of the training to the local “enclave”.

In response to business needs, the Team has innovated federated learning: all “enclaves” in each local environment are trusted agents for the federation, and as the algorithm applied at later stages is able to run in the “enclave” directly, the trusted agents will be able to do more and more in the local environment. Next, the "enclave" will encrypt the intermediate parameters in the encrypted connection and transmit back to the aggregator "enclave" which will quickly aggregate the intermediate parameters it has received and optimize and adjust the AI model according to the results before proceeding to the next iteration.

As the above processes are all implemented in "enclaves", both the AI model and the intermediate parameters are transmitted and exchanged in the encrypted channels and the "enclaves" without any contact with external hardware or software throughout looping and iteration of the solution, resulting in a more secure and trusted "internal loop". Intel® Architecture Processors provide powerful computing support for the construction of the “enclave”, the laying of encrypted channels and the exchange and aggregation of intermediate parameters.

To evaluate each node’s contribution to the training effect, in the 1+N solution all nodes can first be trained to get the effect of total volume training when there are N data sources. Subsequently, the N-1 nodes other than the node to be evaluated are trained separately (for example, when evaluating Node 1, Nodes 2 to N are trained) and, after obtaining models with different training effects, the system will calculate the “contribution coefficient” of each data node in federated learning to get more accurate evaluation of the contribution of each data node in the joint training of AI and adjust the solution accordingly. These algorithms and scheduling may have an impact on the performance of federated learning and it still needs to be proven whether they work in practice. As to how to further use the "enclave" built on Intel technology, there is indeed much room for exploration and discovery.

Results from Leading Federated Learning Practices

Let's take the application of federated learning in the insurance industry as an example. Before federated learning, the salesperson would determine the premium amount on a Policy based only on basic information like the customer's age and gender. However, with continuous development of the information society, the amount and characteristics of user data have significantly increased. For example, in terms of health insurance, accuracy of the insured's health risk assessment will improve if the business system can make AI-enabled predictions using large amounts of data including medical records and family history data to obtain a more precise health assessment categorization.

However, medical records and medical history is the kind of data that healthcare institutions are required to keep absolutely private. It is not only impossible to disclose such data, but the security level to protect them actually needs to be enhanced. Now, with the introduction of a federated learning solution, insurers are able to conduct AI training on insurance pricing models without touching the user data. According to front-line feedback from some early, related projects, the federated learning 1+N solution can significantly improve the effect of personalized insurance pricing.

Outlook

With the value of data increasing and due to a lack of effective data protection in some industries, the phenomenon of data silos is increasingly becoming an issue. In response to some of these data challenges to AI development, Dr. Jianzong Wang, a pioneer of federated learning in China and head of Ping An Technology's Federated Learning Technology Team, has been leading his team to actively explore data safety and trusted collaborations in multi-data source environments. The Team uses advanced federated learning methods to cope with data challenges and have accumulated a wealth of experience for making breakthroughs in this field. They have made a lot of achievements, providing a useful reference for application of federated learning in different industrial sectors.

Currently the Team is using the federated learning method to develop a polymorphic and multi-tasking learning model for the financial industry, which is under strong supervision over data. This model is developed to meet the needs of banks and financial institutions in various application scenarios such as risk assessment, anti-money laundering, investment consulting, investment research, credit, insurance and supervision. By developing this model, the Team aims to help users leverage AI capabilities to build more effective risk control and marketing models as well as identifying potential financial risks such as credit card fraud, overdue loans, financial fraud etc. thus reducing the operational risks to financial businesses. At the same time, the federated learning method can help users utilize horizontal data for user profiling, to expand sales channels and optimize marketing strategies, providing an intelligent engine to improve sales capabilities.

In the future, the Federated Learning Team will further develop technological cooperation with Intel to drive secure operation and efficient transformation of data resources in federated learning with an increasing number of advanced technologies. And they will collaborate with more businesses and institutions to break down data barriers and promote the rapid development and application of federated learning in all walks of life.

[1] For details, see the link: http://www.beian.gov.cn/portal/topicDetail?id=88&token=cb6ad9ae-917f-4677-be49-3f682c718047

[2] For details, see the link: http://www.gov.cn/xinwen/2019-05/28/content_5395524.htm

Intel does not control or audit third-party data. You should review this content, consult other sources, and confirm whether referenced data are accurate.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

No product or component can be absolutely secure.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

Cost reduction scenarios described are intended as examples of how a given Intel- based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Intel, the Intel logo and other Intel trademarks are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

© Intel Corporation