Huorong Security and OpenVINO™ toolkit jointly build a new pattern of collaborative security with software and hardware

Background

In the modern network environment, network security faces increasingly complex challenges, including emerging ransomware, volatile Trojans and other advanced persistent threats. These threats are constantly evolving, requiring security solutions to not only react quickly, but also to accurately identify and block them at an unprecedented scale.

In response to the growing number of network attacks from various malicious programs, Huorong Security has established a multi-level active defense system to effectively respond. In terms of virus detection, it has achieved certain results based on traditional pattern matching and behavior analysis technologies. However, with the rapid advancement of malware technology, traditional methods face problems such as slow speed, high false alarm rate, and insufficient ability to adapt to new threats. To meet these challenges, Huorong Security uses an algorithm based on deep learning to enhance its virus detection capabilities and efficiency. The advantage of this method is that it can continuously learn and adapt to emerging malicious behaviors, greatly improving the accuracy and speed of detection.

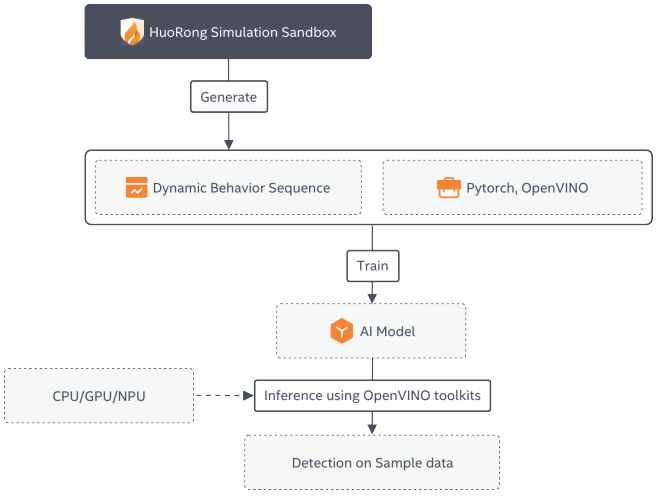
OpenVINO™ is an open source toolkit launched by Intel® for deep learning model optimization, inference acceleration, and rapid deployment. Using the OpenVINO™ toolkit, Huorong Security leveraged deep learning models for virus detection.

- Model optimization and inference acceleration. OpenVINO™ provides a series of model optimization tools that can effectively reduce model size and speed up inference, thereby more effectively achieving real-time threat detection on the user side.
- Rapid deployment of models across platforms and easy switching of inference loads. With the "write once, deploy anywhere" feature of OpenVINO™ , Huorong Security's deep learning model for virus detection can be easily deployed on multiple hardware devices, and inference loads can be quickly switched to different devices. By leveraging the Neural Processing Unit (NPU) in the Intel® Core™ Ultra platform, Huorong Security can migrate compute-intensive virus scanning tasks to this dedicated hardware. This not only reduces the burden on the main CPU, but also reduces the power consumption of the overall system, while maintaining high efficiency and low latency for scanning tasks.
- Faster and labor-saving software development. Currently, OpenVINO™ already supports both Intel® architecture and ARM architecture CPUs as hardware for running deep learning model inference. It also supports Intel's integrated graphics, discrete graphics, and model deployment on NPU and FPGA. Due to the support of cross-platform and multi-architecture hardware devices, Huorong Security can also use OpenVINO™ to shorten the development time of virus scanning and monitoring software on cross-platforms, while greatly reducing the development workload.

Huorong Security has teamed up with OpenVINO™ toolkit and Intel's new generation Core™ Ultra processors. The collaborative approach with hardware and software not only improves the efficiency of security, but also creates a more secure and efficient computing environment for users.

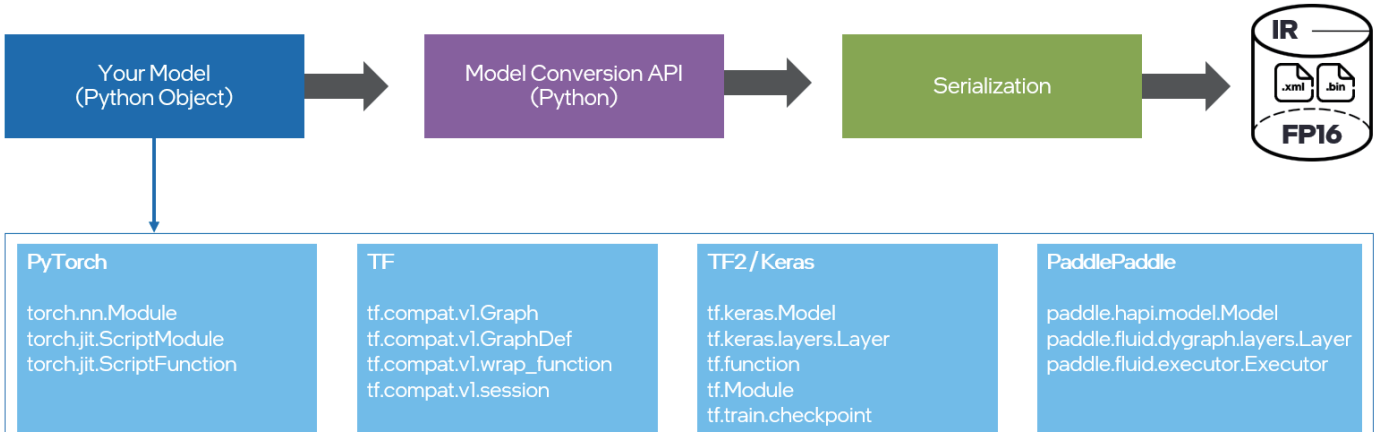
Optimization and Inference Acceleration of Virus Scanning Monitoring Model based on OpenVINO™

To meet the challenges from the rapid advancement of malware and virus technology, Huorong Security has adopted a deep learning-based algorithm to enhance its virus detection capabilities and detection efficiency. The flow chart is shown in the figure below:



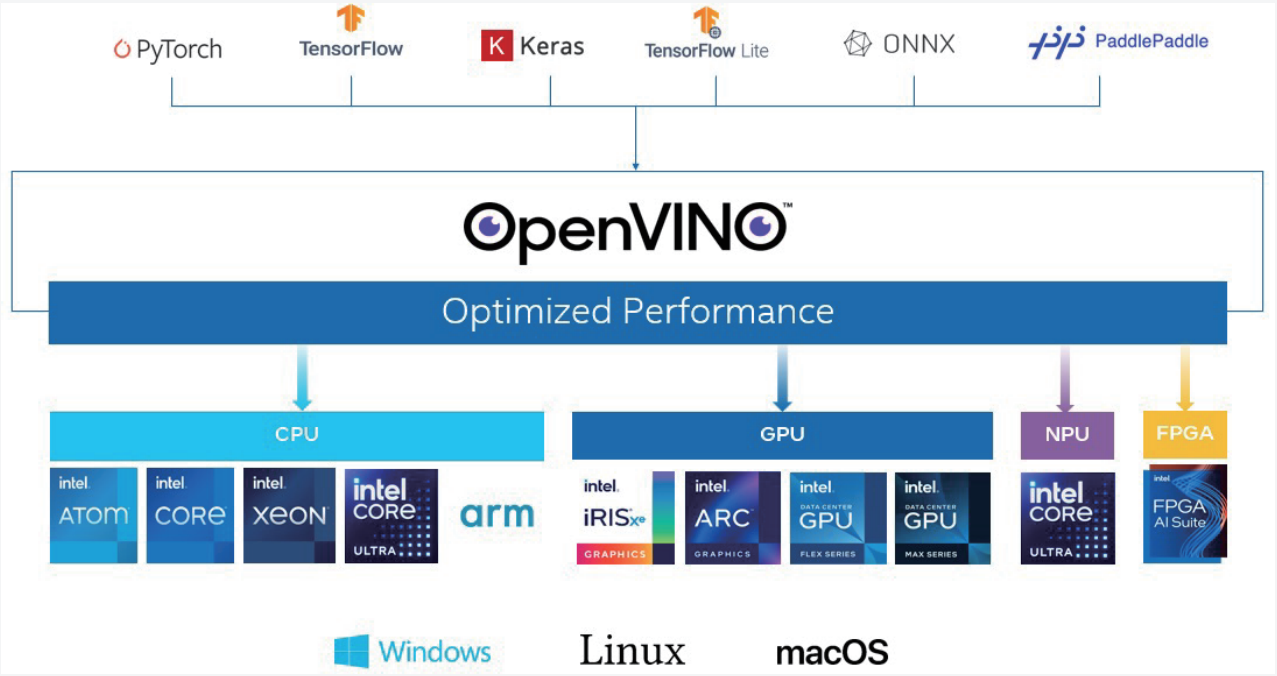
Using a dataset of dynamic behavior sequences collected from virus scanning in a simulation sandbox, Huorong Security trained the model based on the PyTorch deep learning framework and obtained an AI model that can detect viruses efficiently and accurately. Then, Huorong Security used the OpenVINO™ toolkit to optimize the model and deploy it simply and quickly based on the hardware platforms used by different users.

First, using the model optimization tools provided by OpenVINO™, such as model conversion api, Neural Network Compression Framework (NNCF), etc., Huorong Security can convert the trained virus scanning monitoring model from the original PyTorch model format to OpenVINO™ Intermediate Representation format (IR format) to achieve optimized compression of the model. After OpenVINO™ model conversion and optimization compression, the model footprint can be reduced by about 50% compared to the model formats of PyTorch and ONNX. As a result, the inference speed of the model when running inference was also improved by more than 20%. This enables Huorong Security's virus detection algorithm to achieve faster response times and more efficient operations, significantly improving virus detection speed and maintaining accuracy.



Rapid Deployment of Virus Scanning Monitoring Model based on OpenVINO™

The other key feature of OpenVINO™ is the ability to support cross-platform model deployment. Without rewriting a lot of code, it can achieve seamless migration of deep learning models and achieve "write once, deploy anywhere", which is particularly important for quickly responding to emerging network threats. This is especially true to make it easy to run on the NPU (neural processing unit) in the new generation of Core™ Ultra processors. This allows Huorong Security to easily deploy optimized deep learning models on various hardware platforms, including but not limited to Intel and ARM architecture CPUs and Intel® GPUs. Since the version of OpenVINO™ 2024.0, deep learning models can be easily deployed on the NPU in the Intel Core™ Ultra platform. Due to the low power consumption of NPU, Huorong Security's deep learning model can continuously scan and monitor viruses using NPU and maintain low power consumption, providing higher energy efficiency utilization for user devices equipped with Core™ Ultra. At the same time, migrating deep learning model inferencing to NPU also releases the workload on the CPU, so that the CPU utilization rate remains at a low level during continuous virus scanning and monitoring, so that users are not aware of virus scanning and other workloads will not be affected.



Heterogeneous Architecture Support Saves Time and Effort in Software Development

OpenVINO™ supports multiple CPU architectures including Intel X86 and ARM, which provides great flexibility and convenience for developers. Support for heterogeneous architectures means that developers can write code once and then deploy it on multiple hardware platforms, whether on PCs, servers, or mobile devices. This capability not only simplifies the development process, but also allows Huorong Security to easily adapt to various hardware environments, ensuring wide compatibility and efficiency of the software. In addition, this support also enables Huorong Security to better utilize the specific hardware acceleration functions of different devices, further improving the performance and efficiency of its products.

Looking ahead, Huorong Security plans to continue to deepen its technical cooperation with Intel, aiming to provide users with more efficient and intelligent security solutions through technological research and innovation. With the continuous advancement of AI technology and the deepening of its application, Huorong Security's cooperation with Intel's software and hardware technologies, including OpenVINO™ toolkit and Intel® Core™ Ultra processors, not only improves the efficiency of virus scanning, but also provides end users with a safer, faster and more energy-efficient solution.

About Huorong Security

Founded in September 2011, Huorong Security is a company dedicated to security, committed to providing professional products and focused services in the field of endpoint security. The product features encompass "Malicious Code Protection," "System Protection," "Network Protection," "Identity Authentication," "Asset Control," "Intrusion Prevention," and so on. The company continually empowers the industry by sharing its independently developed technologies such as antivirus engines.

About Intel

Intel® (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.cn and intel.cn.

intel

火绒安全
www.huorong.cn

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex

Your costs and results may vary.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

No product or component can be absolutely secure.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

For more details
please scan the QR code and send an email to
guojun3.zhang@intel.com