Intel SGX in the real world

Confidential computing has the power to transform a data-driven world

Intel SGX technology is a game-changer for data sovereignty, security and privacy, enabling organisations to protect data not just when it's in transit or at rest, but also when it's in use. It splits applications into a non-secure part and a secure part that runs inside an enclave: a protected, private region of system memory. What goes on inside the enclave is invisible to other applications, the OS or the hypervisor, ensuring that even someone who has access to the hardware can't read any data exposed within it.

What's more, a process of attestation ensures that applications writing to and reading from the enclave can be sure that it is a specific enclave and that all the appropriate security protections are in place. Attestation guarantees that any data written out from the enclave is legitimate and unmodified – that it can be trusted.

Yet the exciting thing about Intel SGX isn't how it works, but what it enables and empowers. From fighting viruses and improving healthcare to delivering secure compute capabilities at the edge, SGX is a technology with transformative potential.

Guaranteeing data sovereignty in public cloud

Many organisations want to take advantage of the cost efficiencies of public cloud. Faced with an explosion of useful data and the need for more compute power, the financial arguments for doing so are compelling. Yet businesses in finance, healthcare and public services face regulatory barriers that can stop them taking advantage, while other organisations will be dissuaded by the risks of a data breach or IP loss. In the words of Richard Curran, Security Officer for the Datacenter Group at Intel, unprotected data in use always creates "an element of insider threat, because that data is exposed." While data in use is vulnerable to someone with access to the operating system or the hardware, there's always the possibility that IP, PII (Personally Identifiable Information) or other sensitive data could be exposed – or even the application or algorithm being used.

This and the fear of side channel attacks in public cloud causes too many sleepless nights for CIOs or CSOs, but this is where Intel SGX comes to the rescue. What goes on in the enclave stays in the enclave, which means platforms using SGX within their compute resources can protect data while in use, at rest or in transit, even when it's on a cloud platform in a container or virtual machine.

Microsoft is already delivering this capability through Microsoft Azure Confidential Computing. "With Microsoft Azure, you own your data, and you control it, whether it's at rest or in transit," says Mark Russinovich, CTO for Microsoft Azure. "Confidential computing is a breakthrough technology that extends that control by encrypting data in use." And this is just the beginning. "Microsoft is really excited about the new Intel SGX capabilities coming in 2021," he adds. "They'll unlock even more scenarios and allow more applications to become confidential."

Confidential computing at the edge

Between self-driving cars, IoT devices, health sensors built into wearables and the need to deliver low-latency, high-bandwidth services to businesses and consumers, there's a growing need to secure and process more data near the edge. The problem here is that, for many applications, there's a need to guarantee the integrity of that data and ensure it can't be inspected, stolen or modified while it's in use. Think of telemetry data from self-driving cars, sensor data from smart cities, or data from military drones, fighter planes or new mobile and wearable devices being used by modern

infantry and security forces. This isn't data that the organisations involved want tampered with, let alone released by any breach.

For performance and bandwidth reasons, it makes sense to process this data near the edge, but the security risks are high. With Intel SGX, the enclave can protect the most sensitive data while in use, and any results that come out can be cleaned, encrypted and deidentified by the application to meet any relevant security and regulatory requirements. Meanwhile, attestation confirms the integrity of the data, creating a line of trust that runs right through.

Strengthening personal data privacy

Beyond strengthening security for large organisations, Intel SGX can also help ensure privacy for individuals. A recent project with AOK, one of the biggest health insurers in Germany, saw the implementation of the electronic patient record (ePA) in the country and is a prime example of the advantages of this approach. AOK and a group of eleven other regional health insurance organisations, chose Intel SGX technology to implement the TEE (trusted execution environment) to meet the stringent integrity and confidentiality requirements of ePA. The main task of Intel SGX is to protect the ePA file system. The file system combines authorisation, document management and an access gateway. It ensures that only authenticated and authorised users can interact with ePA.

Secure data transfer, optimised for confidentiality, also has its business applications, particularly where organisations may need to exchange information with customers or partners with the highest standards of integrity. For example, using SGX and technology from Secretarium, Swisscom has developed its Secure File Exchange platform that enables users to make confidential business documents available within seconds. Yet the party sharing the information still retains control over its security and access, so that only those authorised to see it can see it – and only for the period when they need to.

Shared analytics and federated learning

Perhaps the most exciting opportunities for confidential computing lie in shared analytics and federated learning. There are many sectors and use cases where it makes sense for multiple organisations to share their datasets. In healthcare, for example, combining datasets from multiple clinics and hospitals could help train better analytics models or machine learning algorithms, which in turn might help doctors develop improved diagnostic processes or approaches to treatment for COVID-19, cancer and a wide range of other conditions. Such algorithms themselves may need to be tested against several different datasets for regulatory approval, and medical research, like any other kind of research, which is often a collaborative endeavour.

Unfortunately, barriers stand in the way. Dr Bob Rogers is Expert in Residence for AI at the University of California, San Francisco's Centre for Digital Health Innovation. "Data is viewed as an organisational asset," he told a recent Fortanix Webinar." A health system that had a large amount of data relevant to algorithm development isn't inclined to just share that data into some shared repository. They lose control over it, and that has both financial and legal implications. "What's more," he explains, "data from different organisations will be unlikely to share the same architecture, format or infrastructure platform, meaning that to organise and optimise it can take months and cost hundreds of thousands or even millions of dollars. This holds crucial research back."

Dr Rogers and the team at USCF are addressing this through USCF's BeeKeeper AI platform. This uses Intel SGX technology and solutions from Fortanix to bring multiple datasets from different health organisations to bear when testing new healthcare machine learning algorithms and, as Rogers puts

it, allows “access [to] data and compute without exposing the underlying data and without exposing the underlying algorithm”.

This means algorithm developers can train and validate their algorithms at a lower cost in less time, without compromising their IP or patient data. That also means AI-enhanced improvements to clinical practice can reach patients faster and improve their outcomes. As Rogers says, “we believe that 1,000 times more clinically realistic and deployable algorithms will be developed per year as a result of using these technologies.”

Fighting financial crime

Healthcare is far from the only sector where federated learning could make a massive difference. Take, for example, the fight against fraud, money laundering and financial crime. One of the technology leaders in this field, Consilient, has built a new secure, federated learning platform powered by SGX, which allows multiple datasets from different firms, databases and even jurisdictions to be amalgamated and processed for patterns and insights. None of the parties involved can see all the underlying data or any of the sensitive customer information – just the results and insights derived from the machine learning platform. This enhances their ability to detect illicit activity more efficiently and accurately, but no personal financial data is exposed along the way. That’s bad news for criminals, and good news for legitimate investors, businesses and financial institutions.

These applications are only the beginning. As more and more businesses drive forwards into digitalisation, the need for secure and controlled data access and confidential computing will only increase. Intel SGX is here right now to support it – and evolving fast to meet future needs.

Learn more about Intel SGX and confidential computing