appliedprivacy

CONFIDENTIAL COMPUTING AND THE FUTURE OF DATA PRIVACY

appliedblockchain.com

info@appliedblockchain.com

Table of contents

Overview

A new data privacy technology is becoming available in the mainstream, and we believe it opens up a wealth of opportunities. In this paper we explain secure enclaves and the breadth of new business applications they present.

The future of data privacy

Hardware secure enclaves (HSE's) enable computation to be conducted in a dedicated secure area of a computer chip that cannot be accessed by the operating system. This means that even the system administrator of a machine, or someone with physical access to the hardware is not able to gain access to the data being processed.

This new technology, initially developed by Intel, means that for the first time, companies can begin to offer cloud infrastructure and software services without having any access to the data that is processed.

We believe that this has profound implications on the software industry, where cyber security attacks and widespread abuse of customer data have forced regulators to intervene.

Hardware Manufacturers

Secure enclaves are implemented by chip manufacturers. Intel, AMD and Apple all include secure enclave capability in their new chipsets.

Cloud Providers

Microsoft Azure, Amazon AWS and Google Cloud have all launched Confidential Computing capabilities.

Adi Ben-Ari
Founder & CEO,
Applied Blockchain

Andrew Campbell
Solution Architect,
Applied Blockchain

Background

How did we arrive here?

Data privacy began with cryptography, a branch of computer science evolved from military encoding of messages through to advanced mathematical formulae.

Modern cryptography involving private and public key infrastructure (PKI) allows us to encrypt messages so that they cannot be inspected in transit, as well as to digitally sign data so that we prove its origin.

This technology is used throughout the internet, from encrypted text message on WhatsApp, through to secure browser identification of online banking websites, and digital signatures of documents.

Cryptography is also the technology that underpins the security of blockchain distributed ledgers, and this is where our own interest in the subject began.

The need to enable third parties to validate the transactions on a distributed ledger, without sharing the transaction details with them, accelerated advances in cryptography, with developments such as zero knowledge proofs (ZKP), secure multiparty computation (sMPC) and fully homomorphic encryption (FHE). Each of these methods deserves a dedicated paper in its own right, but suffice to say that they use only software-based cryptography, which means that they can run on any system.

The main drawbacks of these software based cryptography systems are:

- Extensive computation requirements, leading to relatively slow performance and scalability issues, especially on commodity hardware.
- Nascent custom cryptographic algorithms not yet matured, extensively tested, or endorsed by leading industry and government bodies such as NIST.
- Lack of depth in functionality, meaning that while simple functions are possible, complex functions are relatively difficult or very inefficient.

An alternative technical approach to data privacy, which has grown in popularity in recent years is use of hardware secure enclave environments.

Hardware secure enclaves are already used to store cryptographic private keys and secrets using Hardware Secure Modules (HSM's) in our mobile devices (e.g. Apply Pay) and cloud services (e.g. Azure Key Vault).

More recently secure enclave capability has been extended to run substantial computation and datasets.

Secure Enclaves

Hardware secure enclaves provide an environment where code can be executed in private, with no access given to the host computer or operating system.

The foundation for this new capability is a combination of hardware and software included in the latest chipsets from chip manufacturers including Intel, AMD and Apple. The early leader in the space is Intel with Secure Guard Extensions (SGX), a feature on a range of chips that supports running code and storing data in enclaves. These enclaves offer an execution and storage environment that is inaccessible to the operating system and user no matter what privileges the user has. The chip achieves this by encrypting data before storing it and only decrypting it at runtime within the enclave.

How does a user know that their data is stored and processed in an enclave?

Each enclave has its own identity, and Intel will provide an attestation that an enclave is indeed valid. The attestation also references the application code that has been initiated in the enclave, providing proof that only the specified code is executed in the enclave so that limitations on use of the data are transparent. In other words, the user can be presented with a valid enclave and an attestation from Intel prior to sending data. Any output produced by the enclave can be signed by the unique enclave key.

Considerations

Security

A number of vulnerabilities have been identified within the SGX architecture, including so called “side channel attacks” allowing a party to gain access to attestation keys. Intel has responded to these vulnerabilities and is patching them through microcode updates.

Performance

Unlike software based privacy solutions, the speed of execution of code in an SGX enclave is comparable with that of a regular CPU allowing for scalability and a high throughput of transactions. There is some overhead for encryption, but the technology does scale.

Portability

Because SGX is a CPU level innovation, applications built on top need to run on SGX enabled hardware.
However cloud providers including Microsoft Azure have launched SGX machines as a service.
Other chip manufacturers such as AMD have partnered with cloud providers such as Amazon AWS and Google.

Use Cases

The technology is already being incorporated into a number of use cases:

Application Use Cases

AI

Perform privacy-preserving NLP and machine learning to gain insights from fully encrypted sensitive data belonging to different parties.
The secure enclave provides assurance that the encrypted data provided by the parties is never revealed, even to the host.
By retaining the sensitive data inside an enclave, learning data can be built up over time, and insights can be gleaned within the privacy constraints defined in the enclave code.

GDPR & Data Minimisation

Hold personal identifiable information (PII) in a secure enclave environment. This increases GDPR data minimisation compliance and reduces cyber risk.
Sensitive customer data is never revealed to the host, and only computation enabled in the enclave can be performed.
This provides maximum compliance with GDPR and in particular the Data Minimisation principle, while still enabling value to be extracted from the personal data.

Dark Pools

Match fully encrypted transactions to prevent anyone, even the host, from seeing or accessing an order book.

Market Data

Generate data from private, sensitive, fully encrypted transactional data belonging to different parties, without providing the host with access to the data..

Cloud Hosting

The major cloud hosting providers have all launched confidential computing capabilities. Any application that is cloud hosted by a third party (e.g. Amazon AWS, Google Cloud, Microsoft Azure) carries a risk that the cloud provider, one of its employees, or an intruder, may access a device directly, and therefore gain access to data.

However, if the an application runs in a secure enclave, even if that enclave is hosted in the cloud by a third party, then the data in the application cannot be accessed, even by an intruder with physical access to the device. Proof that the application runs inside a secure enclave is provided independently by the chip manufacturer, and not the cloud hosting provider.

appliedprivacy

appliedblockchain.com info@appliedblockchain.com

WHO WE ARE

Applied Privacy builds enterprise grade secure enclave applications with increased trust and data privacy for global companies and startups

Our background

Applied Privacy is a group within Applied Blockchain focused on confidential computing and secure enclaves. The company was founded in 2015 with the vision of helping companies solve real world problems using blockchains and advanced encryption technologies.

Our experience

Over the past 5 years we've been selected by some of the largest global organisations in financial services, energy, trading, shipping, automotive, aviation, telecoms and government.

Notable recognition

Gartner recognised Applied Blockchain as a global leader in blockchain consulting in 2017-2020.

Forbes Bloomberg VentureBeat

"We did the first product derivative trade on blockchain together with our partner Applied Blockchain"

Ben van Beurden
CEO, Shell

Clients include:

Shell, Lloyd's Register, Bank of America, vodafone, SITA, KLM, TOYOTA, emsurge, nuggets, UNITED NATIONS, Travel Ledger

Notable partners:

Microsoft, r3, intel

AI & Machine Learning

GDPR & Data Minimisation

Market Data

Order Matching & Dark Pools

appliedblockchain applied-blockchain @AppBlockchain_ @appblockchain


appliedprivacy