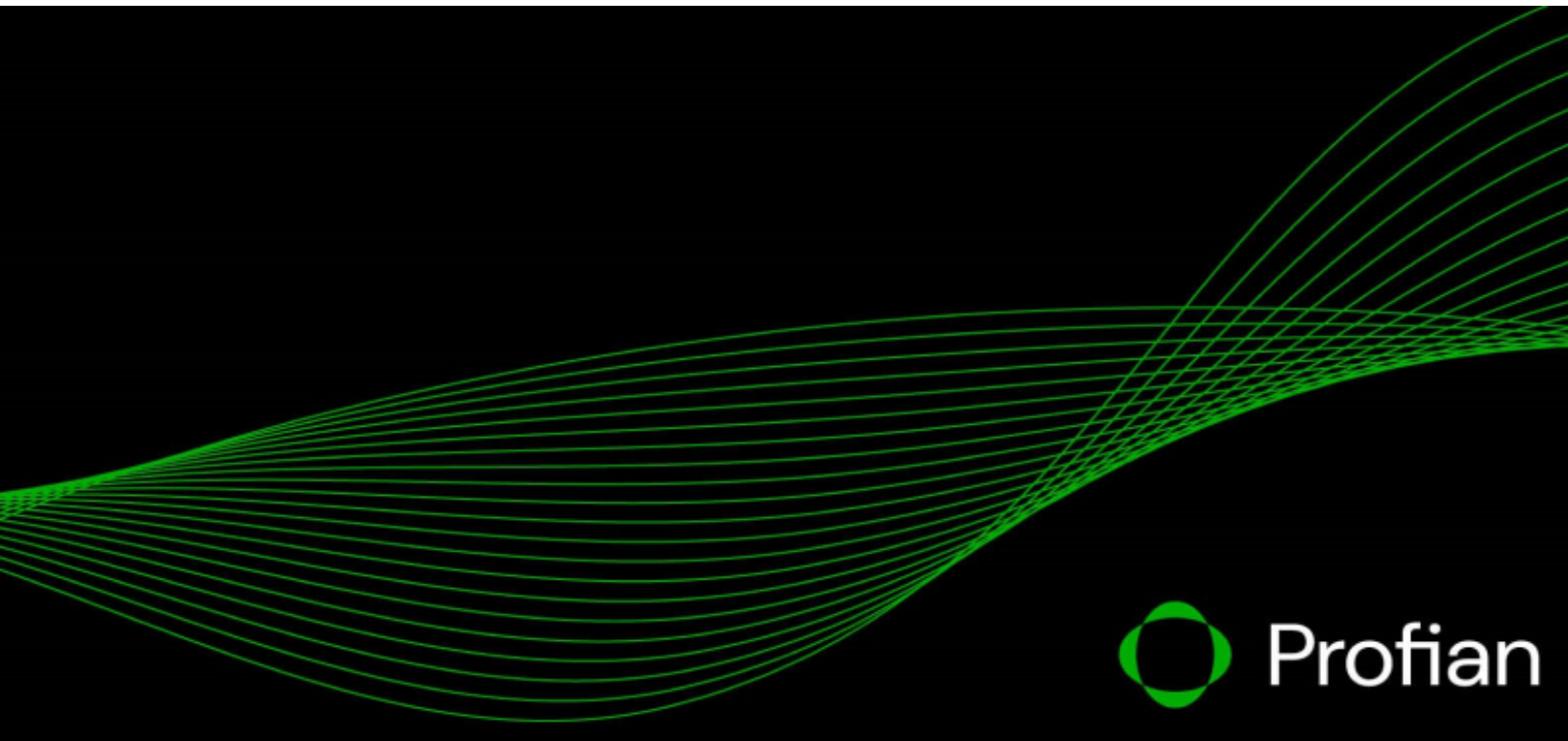
Profian

PETs AND CONFIDENTIAL COMPUTING COMPARED

Learn what are PETs and how they operate within Confidential Computing.



Profian

Protecting sensitive apps and data

The public cloud

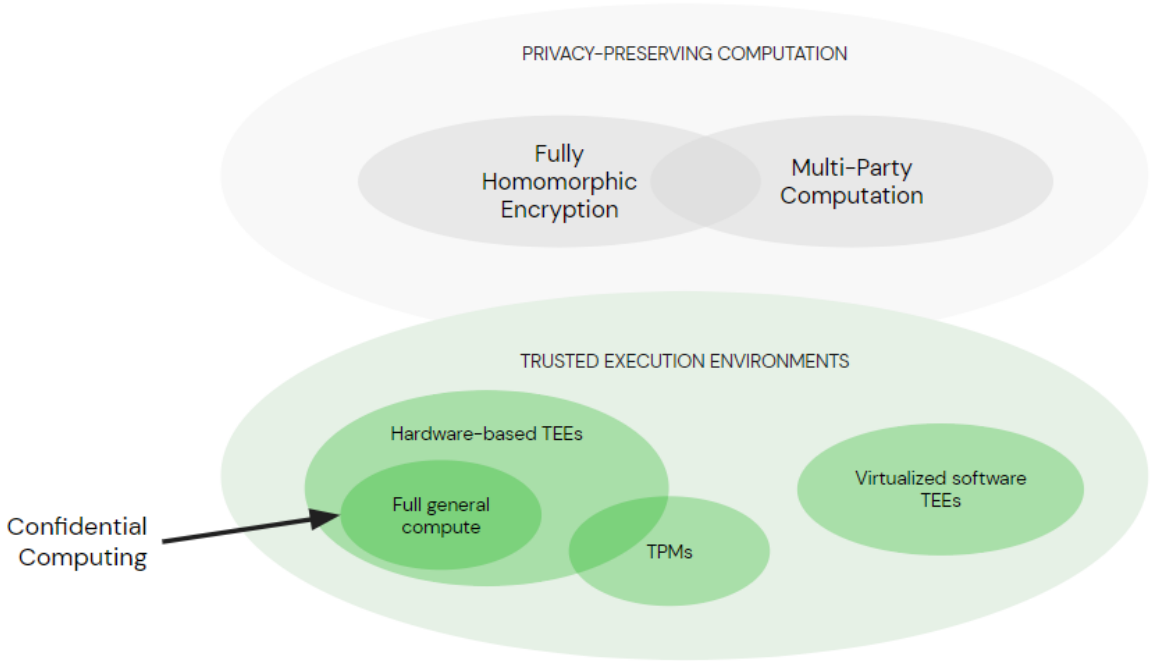
- **Has revolutionized organizations' computing deployments**
- **Presents challenges for sensitive data and applications**
- **Can be made safer for deployments with Privacy-Enhancing Technologies**

The ability to "rent" computing resources in the public cloud has revolutionized how organizations deploy applications, with Cloud Service Providers (CSPs) offering a variety of services, including bare metal hosts, Virtual Machines (VMs), Containers, Infrastructure as a Service (IaaS) and more. However, as organizations realized the benefits in terms of speed of scaling, cost management and ease of deployment they have also encountered a major issue: the confidentiality and integrity of the most sensitive data and applications. Almost all sectors collect or manipulate data which is in some way sensitive, and sometimes the applications performing computation on the data are themselves in need of protection. Examples of sensitive applications and data might include:

- Credit card or account details
- Customer address and tax information
- Patient records
- Merger and acquisition plans
- Cryptographic keys
- Logging data
- Investment decision engines
- AI/ML models for geographic surveys
- Crypto applications and wallets

© Profian 2022

Various technologies have been developed over the past few years to provide protection for use cases involving applications and data which are sensitive: these are typically referred to as Privacy-Enhancing Technologies, or PETs. This white paper lists the most relevant characteristics of three of these technologies – Fully Homomorphic Encryption (FHE), Multi-Party Computation (MPC) and Confidential Computing – to help organizations make information decisions about which approaches are the best fit to their requirements. Each of these technologies has several approaches and implementations, and the choice of a specific detailed description requires careful research and selection by an organization planning to adopt it.



The main approaches to computing with confidential data[1]

[1] Diagram is adapted from https://confidentialcomputing.io/wp-content/uploads/sites/85/2022/01/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.2.pdf

© Profian 2022

Fully Homomorphic Encryption

The industry body Homomorphic Encryption Standardization introduces FHE by explaining that "Fully homomorphic encryption, or simply homomorphic encryption … differs from typical encryption methods in that it allows computation to be performed directly on encrypted data without requiring access to a secret key. The result of such a computation remains in encrypted form, and can at a later point be revealed by the owner of the secret key[2]." FHE shares in common with other types of encryption that it comprises a set of mathematical operations which can be performed on almost any sufficiently powerful computer system. These mathematical operations need to be performed on carefully structured data implementing specific algorithms.

Multi-Party Computation

Multi-Party Computation, sometimes referred to as Secure Multi-Party Computation, is a set of techniques which, like FHE, provide mechanisms to perform calculations on particular types of data set using mathematical techniques which allow multiple parties to perform operations on data whilst keeping the initial data secret from each other. Some MPC techniques make use of FHE, while others use entirely different approaches. Like FHE, MPC can be performed on almost any sufficiently powerful computer system.

Confidential Computing

"Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment" as defined by the Confidential Computing Consortium[3]. Confidential Computing does not require the application of special mathematical techniques on data, but, unlike FHE and MPC, does require specific hardware which implements Trusted Execution Environments (TEEs),

[2] https://homomorphicencryption.org/introduction/
[3] Confidential Computing Consortium, 2021, A Technical Analysis of Confidential Computing, v1.2, https://confidentialcomputing.io/wp-content/uploads/sites/85/2022/01/CCC-A-Technical-Analysis-o f-Confidential-Computing-v1.2.pdf

© Profian 2022

such as include Intel® SGX and AMD® SEV technologies, which provide chip-based capabilities to allow the creation of applications which are protected from the host computer, including its administrators[4].

Characteristics of PETs

In this section, we look briefly at various characteristics of PETs that are relevant to considering their use for cloud computing deployments. A comparison table is provided at the end of the section, which includes standard cloud computing technologies as a baseline.

- Protection from other workloads - all the technologies discussed provide protection from other applications which may be running on the same host.
- Supported by all CPUs - Confidential Computing workloads require specific hardware available on the hosts on which they are running.
- General compute - FHE and MPC require applications to be redesigned to allow processing of data, whereas Confidential Computing allows the deployment of standard applications.
- Near-native performance - the algorithms required by FHE and MPC add significant overhead to any data processing, with FHE in particular often being 1,000 to 1,000,000 times slower than normal operation. Confidential Computing typically applications run with a slight overhead (e.g. 5-20%), providing near-native performance.
- Data confidentiality protection - all of the technologies discussed provide protection of the confidentiality of data processed by an application.
- Data integrity protection - FHE and MPC do not provide protection of the integrity of data processed by an application, whereas Confidential Computing does.
- Application confidentiality protection - a key benefit of Confidential Computing is that it protects the confidentiality not only of the data,

[4] Note that the AWS Nitro Enclaves® service does not meet this definition, as it does not provide sufficient protection from administrators and operators of the system to ensure that they cannot access data or applications.

© Profian 2022

but also of the application, allowing applications which are themselves sensitive to be deployed. FHE and MPC do not provide this protection

- Application integrity protection - Confidential Computing optionally allows for the protection of the integrity of applications, ensuring that they cannot be altered by a malicious party.
- Trusted attestation - attestation[5] is the measurement and validation of a runtime environment. When implemented fully, it allows cryptographic assurance of all of the various forms of protection described in this list. In order for this assurance to be useful, it must be performed by a third party, and not the CSP (who could provide "spoofed" assurances).

[5] See other white papers from Profian for an introduction to attestation.

© Profian 2022

Profian

	Cloud technologies	Fully Homomorphic Encryption	Multi-party Computation	Confidential Computing
Protection from other workloads	✓	✓	✓	✓
Supported by all CPUs	✓	✓	✓	✗
General compute	✓	✗	✗	✓
Near-native performance	✓	✗	✓[6]	✓
Data confidentiality protection	✗	✓	✓	✓
Data Integrity protection	✗	✗	✗	✓
Application confidentiality protection	✗	✗	✗	✓
Application integrity protection	✗	✗	✗	✓[7]
Trusted attestation	✗	✗	✗	✓

A comparison between run-time technologies

67

[6] Depends on specific mechanism
[7] Requires implementation - not part of Confidential Computing Consortium definition

© Profian 2022

Profian and Enarx

Profian is a security company providing products and services for Confidential Computing based on the open source Enarx project and is based in Raleigh, NC. It was founded in 2021 by the two co-founders of the Enarx project - Mike Bursell and Nathaniel McCallum - and acts as the custodian for the project, providing engineering and other resources and working to build a strong, welcoming and diverse community of developers and contributors. Profian is a member of both the Confidential Computing Consortium and the Bytecode Alliance. As well as contributing to the Enarx project, Profian is committed to the wider open source community and is involved with multiple upstream projects to improve the security and user experience associated with Enarx.

If you are interested in a demo or to learn more about our solutions, please contact us via http://profian.com.

© Profian 2022