enclaive

Accelerating Cloud Adoption in the FinTech Industry

www.enclaive.io

Confidential Containers in Action: How to Accelerate Cloud Adoption within the FinTech Industry

Cloud computing is driving digital transformation. Many businesses nowadays are in the process of moving workloads to the public cloud, knowing the cloud is the safest and most economical place to compute. Switching data centres from on-premise infrastructure to the cloud may reduce a lot of the historically grown complexities and also save businesses infrastructure costs.

The same transformation movement can be seen within the Financial Technology sector, abbreviated as FinTech. Within the last few years, consumers saw a massive shift in how their banks process and offer financial services such as insurance, lending, payments, and cash management.

ENCLAIVE GMBH
WWW.ENCLAIVE.IO
CHAUSSE ESTR. 40
101 15 BERLIN

The Challenges

Many companies within the FinTech industry are reshaping how financial services have been traditionally offered and consumed. With an overflood of regulatory audits of data security methods, organisations need to take legal and compliance regulations seriously to survive and stand above the rest. Furthermore, there has been a massive change within the industry, by focusing on a growing modularization of financial services. Third-party providers are becoming highly specialized and technically sophisticated with the specific services they are putting on the market, making it a lot more flexible and easy for banks to rely on different providers for specific financial services.

For example. you are having an account at bank A, but at the same time, you are using different services from third-party providers B and C, to which bank A outsourced its services. This means that B and C are also able to access all your customers' data.

- **How to prevent data breaches and ensure data privacy compliance?**
- **How to prevent insider/outsider threats and third parties**
- **How to ensure secure and untrusted collaboration with other institutions**

The Challenges

How to prevent data breaches and ensure data privacy compliance?

This is the obvious one. Your bank has access to a lot of highly sensitive data (your credit score, credit card details, and social security number). Trying to both leverage this volume of customers' data while adopting a cloud transformation and also meet all regulatory compliance requirements is a challenge in itself.

How to prevent insider/outsider threats and third parties

Especially in the context of the growing modularization of financial services, providing such services, while they are being outsourced to third-party providers, increases the risk of digital theft tenfolds. But this is not the only data-sharing financial institutions look to. In today's cloud-driven business world, institutions are working towards a cross-departmental data collaboration, leveraging both AI models and also machine learning technologies.
Realising the full potential of quality AI models is greatly interlinked with having access to quality data. Any development requires sufficient high-quality data for developing initiatives. While data sharing is greatly needed to better expand and offer services for customers worldwide, such a mechanism also means a lot of data security headaches. Working with different institutions and third-party providers signifies that all of them can access and process the users' information.

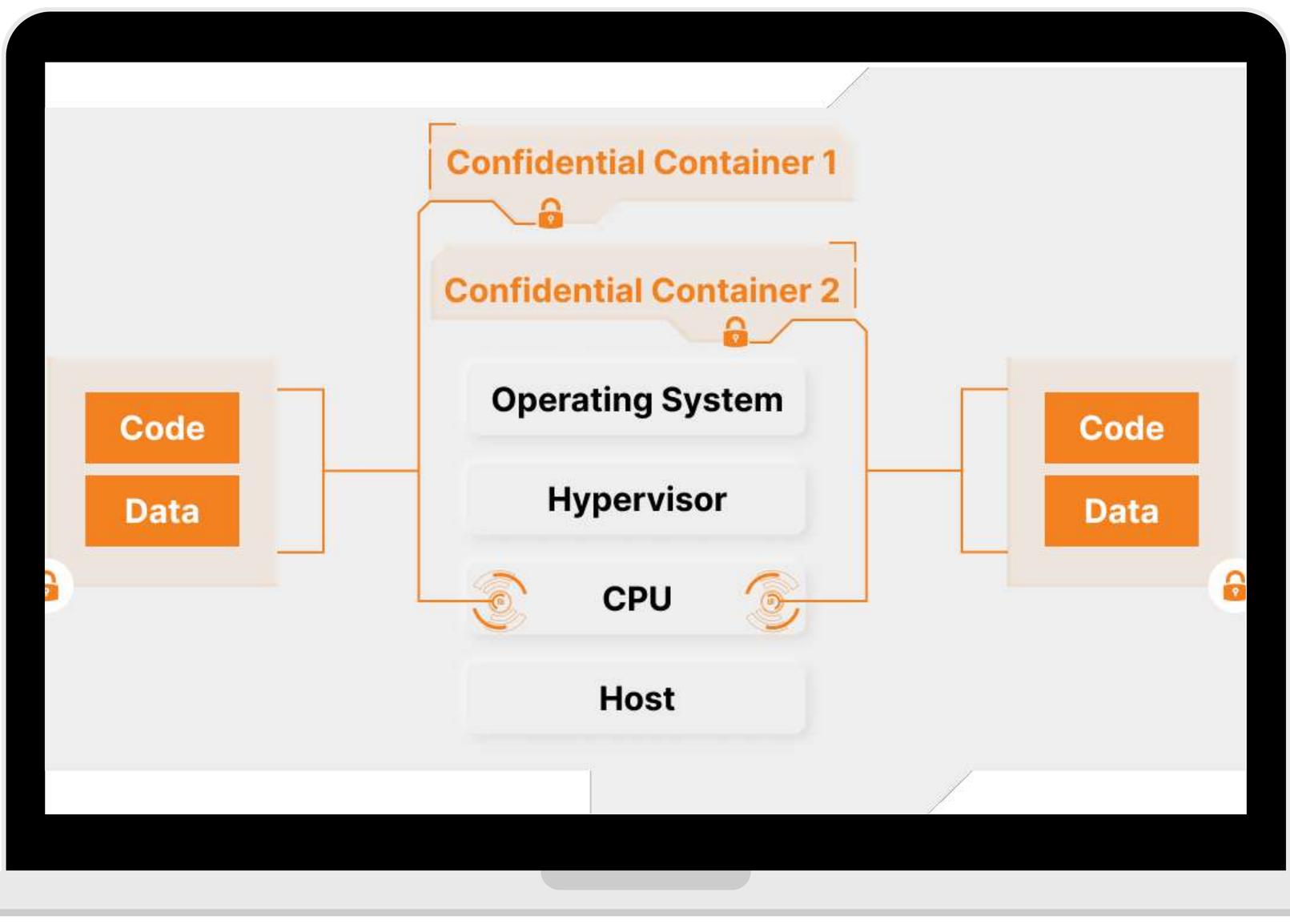
How to ensure secure and untrusted collaboration with other institutions

The primary impediment to accessing more datasets is the increase in data privacy regulations within the FinTech sector and how to ensure that the data shared remains protected. Fintech firms have a legal obligation to prevent unwanted data access resulting in privacy breaches. Because of negative consequences, such as financial and reputational costs, FinTech institutions are highly hesitant to share or allow access to certain types of sensitive data/workloads due to data breaches.

Solution Overview

In this context, the emerging technology of Confidential Computing can be used to secure customers’ data, while also complying with data privacy regulations like GDPR. In a nutshell, confidential computing is a new computing paradigm safeguarding customers’ data and sensitive data at any moment in time, while it is stored, looked up, edited or processed, remains encrypted and shielded against data breaches. Only legitimate users may access the data.

By design, our data stored in any government institution is given the safest harbour. FinTech institutions can turn their applications into confidential applications with ease thanks to enclaive’s revolutionary confidential container technology.



Enclaive’ Confidential Containers leverage the Confidential Compute Technology and are designed to protect both data and the intellectual property contained in AI algorithms, even on untrusted infrastructure.
Throughout the algorithm’s runtime, data is always encrypted in memory and stays protected within the enclave while being processed. Fintech organisations would have complete sovereign control over all financial data at all times, while also ensuring a secure, quick and easy cross-departmental collaboration. This ultimately leads to improved outcomes for the customer and long-term services.

Enclaive reduces the legal and IT-compliance efforts by providing Confidential Container technology that meets GDPR regulations at all times. Hence, any attempt to hack this information is prevented by the privacy box, allowing for storing and processing of financial data in a privacy-enhanced way. Moreover, the container may be attested at any point in time to the integrity and confidentiality of the code and data.

For instance, two financial institutions can work on generating **credit qualifications** for customers by leveraging enclaive’s Confidential Container. They can combine their two separate datasets within a secure enclave. They could share the credit history of their customer to track and assess each credit score. Once the data is in this secure box, no unauthorized access is possible. But AI applications and algorithms can still access this new combined dataset. Based on this, they track and assess the transactional data and generate new conclusions. This will benefit both institutions with improved outcomes. And this all while remaining owners of the privacy of their sensitive data.

Another application of Confidential Containers could be when it comes to efforts against **money laundering**.

This approach also involves different organisations that work collaboratively to obtain a shared prediction model. Federated learning allows the data to be kept in local environments, such as banks' internal systems. They upload data to a centralized node where AI algorithms provide risk assessments, allowing banks and other financial institutions to spot potential risk candidates. Furthermore, banks could share and use each other's transaction data to build predictive models and create an anti-money laundering system.

Further application scenarios

Detect fraud and digital theft

Market-rate calculations

Access financial products more quickly

Analyse loan applications

Read enough? Click here to jump right in.

Why should you choose enclaive?

Give customers' IT the safest place

Make Data Privacy a friend - not foe

Frictionless deployment

Be ready for Compliance Audits

Testimonial:

> **Enclaive helped us to expand our business and increase in revenue. While optimizing the financial accounting, key to our customers is the protection of data during the analysis. Enclaive‘s confidential compute technology gives our platform the safest harbor trusted by numerous clients.**
> **David Weber, CEO Nooxit**

Why should you choose enclaive?

Give customers' data the safest place

Wrapping government IT with confidential containers means deploying the highest standard of security and privacy to protect sensitive data. It is so secure, that even the underlying infrastructure administrator may not access it.

Make Data Privacy a friend - not foe

By design, data while in use is fully encrypted. Only legitimate endpoints may access the data in cleartext. This way, Confidential Compute is a modern data anonymization technique, as no clear text data may be leaked.

Be ready for Compliance Audits

How can you prove that you have taken the best efforts to protect your IT? Running your IT shielded by confidential containers allows you to audit the containers and obtain a digital certificate that sensitive data runs in confidential containers.

Frictionless deployment

Our highly secure containers are built to work right out of the box. No changes to the application code or SDKs are required.

Want to know more?

Get in touch and let us walk you through a demonstration of how our Confidential Containers can accelerate the cloud transformation within your company.

>>> Watch a demo

>>> Try it out

If you want to get to know Enclaive:

>>> Product Portfolio

>>> In the Press

>>> About Us

EMAIL:
contact@enclaive.io

WEB:
enclaive.io