Data as an Asset

Enhancing Opportunities and Growth by Sharing Data
While Preserving Privacy in Highly Regulated Markets

Overview

The world produces 4.5 quintillion bytes of data a day. According to McKinsey, the cloud computing market is growing to a trillion dollars by 2030. Without question data analytics produces valuable Insights ……and it has become both a strategic and monetary asset.

Data is in high demand and organizations that can collect and curate high-quality data sets can monetize it and/or share it for greater benefits. The resulting analytics and insights contribute greatly to defining products and–enhancing current services such as personalized recommendations and/or marketing campaigns. Of course, most of these data sets contain sensitive information that should be protected and kept private to meet data compliance and regulations. For example, targeting the right audience without exposing personal and/or location-based confidential information delivers efficiency against marketing spend, generating a higher return while remaining compliant with regulations such as GDPR.

In addition to being a monetary asset, data is also a strategic asset that can help make better-informed decisions. By analyzing data, organizations can identify trends and patterns to improve predictions for future outcomes including the ability to make better decisions, gain a competitive advantage and generate new revenue streams.

Data-Based Insights Drives Value

Whether it is to make more informed decisions, optimize operations, or drive growth, the power of data insights to enterprises, industries, academics, countries, and global organizations cannot be understated.

For industries, data insights can help identify trends and patterns, forecasting, and improve the efficiency and effectiveness of business practices.
For academics, data insights can be used to drive research and innovation. By analyzing data, researchers can uncover new insights and knowledge that can lead to breakthroughs in fields such as healthcare, technology, and social science.
At national levels, data insights can be used to inform policy decisions and drive economic growth. Governments can use data to identify patterns that can be used to inform economic policy, improve healthcare systems, and enhance public safety.
Enterprises can access new markets and customers, and tailor their products and services to better meet the needs of both domestic and international customers.
And of course, data sharing across borders - Intelligent insights from secure collaboration across organizational and jurisdictional boundaries are vital to global organizations. One reason is that data sharing can help facilitate international trade and commerce while reducing fraud allowing, for example, financial institutions to share data with branches and corresponding banks.

The growth of the digital economy shows that sharing data between various stakeholders has become crucial for driving value in terms of enhancing these insights based on analyzing larger data pools. However, data processing and sharing also come with several challenges including data privacy and security in highly regulated markets.

Challenges

There are several challenges that organizations face when it comes to data sharing. These include data compliance and governance, cybersecurity, computing performance, and privacy regulations.

Regulatory: In most markets, there are increasing regulations that govern the collection, use, and sharing of data, particularly when it comes to personal and other confidential data. Data owners must comply with these laws and regulations or face large fines including market restrictions and legal challenges.
Compute Requirements for Predictive Analytics and Encrypted data sets: Data sets are exploding, and larger data pools can produce encrypted workloads that are compute-intensive and time-sensitive. An example is sharing sensitive data across multiple pharma companies and countries to develop life-saving treatments and drugs with a faster time to market while meeting regulatory requirements for data privacy.
Data Compliance and Governance: When data is shared across organizations, it is important to have clear policies and procedures in place to govern how the data will be used and shared. This can be particularly complex where organizations may be dealing with multiple policies across jurisdictions, that are subject to multiple layers of regulation and oversight.
Cybersecurity: Cybercrime continues to be a major threat to the confidentiality of data and produces a threat to the security and privacy of the data being shared. Organizations must implement privacy and security technologies to protect against cyber threats. Cybercrime continues to grow and according to Cyberventures, it is a trillion-dollar problem including monetary fines, business and reputation losses, along with legal lawsuits.

Solutions for Data Privacy, Security & Sharing such as Fully Homomorphic Encryption (FHE)

There are several approaches to address data privacy, security, and data sharing. Fully Homomorphic Encryption (FHE) is currently the only data privacy technique that promises "Zero-Trust". In a typical FHE scheme, data is encrypted, and can only be decrypted by someone who possesses the correct private key. With FHE, it is also possible to perform mathematical operations on the encrypted data and obtain an encrypted result that can only be decrypted only by the data owner's unique key. This allows multiple and independent parties to jointly perform computations on encrypted data without ever seeing the plaintext data. FHE also prevents cybercrime with quantum-secure privacy-preserving encrypted data sets. In other words, even if the data is hacked and stolen, it cannot be used by cyber-criminals.

Although highly desirable, FHE is extremely compute-intensive and requires 1 Million X higher performance over current processing technologies to deliver real-time results.

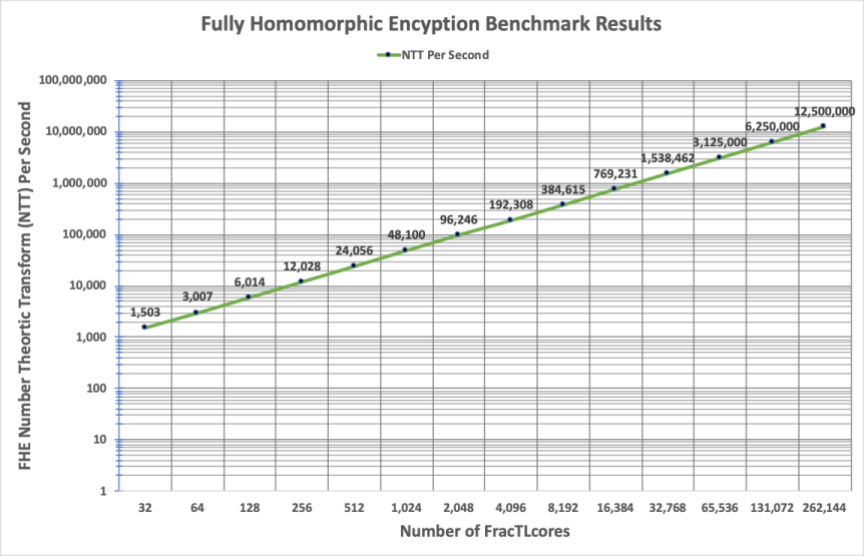
This is where Cornami comes in: Delivering a unique next-generation FracTLcore™ Computing fabric with unprecedented scale that dynamically addresses multiple application requirements in terms of performance, power, and cost in highly regulated industries. Most notably Cornami can meet the performance requirements of 10^6 for real-time FHE.

For example:

Fig., (a):
Performance "increases" as more FracTLcores™ are allocated to the problem – showing the scaling ability of the FracTLcore Computing Fabric

- Cornami's numbers hold the Record **for the fastest NTT benchmark** performance.
- It is no longer about the peak performance of an individual "processor", but rather "*how fast do you want to run?*", which correlates to the number of cores to deliver real-time results.

fig. (a)



NTT Benchmark
- 64K Point Number Theoretic Transform
- 64 bit Coefficients
- Throughput in transforms per second (higher is better)

IC Performance:
- Clock Cycles measured from M-Class IC ASIC emulation system running final RTL
- Number of FracTLcores from Cornami toolchain
- NTT Topology created from Cornami toolchain
- Fabric Clock Frequency from ASIC Preliminary Physical Design
- Fabric FracTLcore Density from preliminary ASIC Physical Design

There are other Privacy Enhancing Technologies (PETs) approaches that can improve on data security but involve some level of trust. Data owners may feel more comfortable within organizations or across controlled ecosystems but at the minimum – they will require *some* trust even if it is employees and/or contractors. And of course, cybercrime risk still exists.

Cornami believes that many of these techniques will start to blend to meet requirements, and the company is already working with partners that want to process Privacy Preserving Machine Learning (PPML) and or take Multi-Party Computing approaches enhanced with FHE. Cornami's post-von Neumann architecture meets the need of the market offering a computing platform that can scale up or down while providing flexibility to migrate and support multiple approaches to meet performance, cost, and footprint requirements.

Cornami TruTrust™ - Privacy Computing Platform for Data Sharing

Meet Customer Performance, Power and Cost Requirements

- **Flexible and Scalable FracTLcore Computational Fabric**
- **Capable of Real Time FHE Performance**

* DARPA - Trust no one

Privacy-Preserving Techniques for Sharing Data

Fully Homomorphic Encryption: The Holy Grail* Data remains encrypted and can be analyzed and shared without ever exposing the underlying confidential data.

Privacy Preserving Machine Learning (PPML): bridge the gap between privacy while receiving the benefits of machine learning using FHE.

Zero Knowledge Proofs: Users can prove their knowledge of a value without revealing the value itself.

Differential Privacy: Noise is added to the dataset so that it is impossible to reverse engineer the original inputs.

Functional Encryption: Select users have a key that allows them to view some parts of the encrypted text.

Federated Analysis: Parties that share insights from their analysis without sharing the data itself.

Secure Multiparty Computation: Data analysis is spread across multiple parties such that no single party can see complete set of inputs.

Data Sharing

There are also a number of approaches that are currently being implemented to address data sharing, but many do not deploy available data privacy-preserving techniques which increases risk. One such approach is data-sharing platforms using Trusted Execution Environments (TEEs). These computing enclaves or TEEs often use software security and access control to protect the data being shared but have experienced breaches. They are often deployed as a data clean room to share data across multiple owners. The reality is that it is impossible to guarantee hack-proof firewalls, secure operating systems, processors without embedded trojans, or internal risk from employees in computing environments.

Another approach is data intermediaries. These are organizations that facilitate data sharing between different parties. Data intermediaries may offer services such as data vaults or clean rooms, data curation, data management, and data analytics, and they may use de-identification techniques for data privacy. Of course, they face the same risks and involve "trust" including using anonymized techniques that have been proven to be easily reverse-engineered using machine learning algorithms.

These types of approaches involve the need to "trust" and have been vulnerable to data breaches, however, adding FHE and/or other PETs will reduce this risk.

Database Schemes are Fundamental to Secure Data Management

There are many multiple database schemes for storing data and they are increasingly important as the market moves from not only data security but data privacy and data sharing. These need to be part of any data privacy approach and the data should remain encrypted – with the owner maintaining control of the key.

Summary

The role of PETs is important to building data as an asset while addressing privacy in regulated markets. Cornami's unique technology delivers a scalable and programmable PETs Computing Platform to support multiple privacy schemes including delivering 10^6 performance acceleration for real-time FHE. Its FracTLcore Computing fabric is highly scalable, meaning it can be expanded or contracted to meet the demands of any given task. This enables the handling of complex and compute-intensive tasks including the flexibility to address evolving markets while offering performance, latency, and cost advantages.

The digital economy can only reach its full potential if data remains encrypted and secure while processing to extract valuable data insights on sensitive data.

Cornami's scalable platform processes encrypted data sets while supporting data privacy for highly regulated markets.