View on Web

Homomorphic Encryption- A Game-Changer for Data Privacy

7th Mar,2022

In this digital-first world, we are drowned by a deluge of data. The frenzied manner in which data is being shared seamlessly has flagged concerns about its privacy. You or me as individuals are growing cagey about our personal data. How well guarded is our data? And, what if some creepy nerd steals your data by stealth? This is a nagging fear. Not just private data, the growing instances of breach of enterprise data has stoked concerns too.

Today, big tech companies like Google, Microsoft, Amazon and Meta (formerly Facebook) are grappling with mounting data privacy concerns. Regulations around data protection are also getting tighter with recurring cases of data breaches. The General Data Protection Regulation (GDPR), which applies to any EU citizen regardless of where they live, requires privacy by design and respect for user privacy**. Cisco's 2021 Data Privacy Benchmark**

Study found that 79 per cent of organizations believe such regulations are having a positive effect.

According to the Tech Republic, Microsoft spends over $1 billion a year on data security and protection. But is that enough?

A secure solution in Homomorphic Encryption

For highly regulated industries, securely transferring data to cloud environments or data-sharing partners is challenging. Homomorphic encryption might change that since it would allow data to be analyzed without compromising privacy.

This super niche tech is one of the pillars of Privacy Enhancing Technologies (PETs), offering the Encryption-as-a-Service model. When the world is obsessed with data privacy, homomorphic encryption could be the game-changer. With this technology, you can process encrypted data without decrypting it. So, there is no loss of data at rest or in transit.

Understanding the tech and its scope

With current forms of encryption, you have to decrypt data to work with it. By doing so, you expose data to the high risks you were trying to avoid. **With homomorphic encryption, you can manipulate and analyze data without compromising security. Companies can save time and money by not having to transfer data between networks or worry about it being copied.** Dr Craig Gentry, an independent researcher and an acclaimed expert, has demystified the technology. He says homomorphic encryption is like a glove box. Anybody can get their hands into the glove box and manipulate what's inside. Still, they are prevented from extracting anything from the glove box.

Not a booming market yet… but has the potential to grow

The market for Fully Homomorphic Encryption (FHE) is in its infancy now. Nonetheless, it has the potential to grow. **Market research firm The Insight Partners predicts it will increase from $120.12 million in 2019 to $246.29 million by 2027, an average of 9.7 per cent**

growth a year. Figures by Gartner say that currently, less than one per cent of the companies have the budget for FHE adoption but forecasts that the share will be more than 20 per cent by 2025.

Getting over barriers for adoption at scale

As of now, homomorphic encryption is extremely slow to process data-so slow that it isn't feasible to use for many applications. The other barrier to onboarding this technology is that it needs enormous compute power, making it expensive to use. Also, the use of this technology needs proven expertise in cryptography. However, the value that it brings outweighs the challenges to be navigated. The use cases of homomorphic encryption can range from spartan to the sophisticated- from spell checkers to an email and medical records analysis to things like photo filters or genomic research. Over to the future, where this tech will set the new gold standard for data privacy.

AUTHOR:

Jayajit Dash

Senior Manager- Corporate Communications (Marketing)