Fully Homomorphic Encryption - Why it Matters

0:01 Our private information and data are being shared more widely than ever before

0:04 And often, we're the ones sharing it.

0:07 We share our data in exchange for convenience and improved services.

0:11 As long as our personal accounts remain untouched, we think nothing of it.

0:14 And for most, giving up our personal information is required to interact in the digital world - both at work, and to utilize basic everyday services.

0:23 So how do we know our data is safe?

0:25 Well, most of the sensitive data we share is encrypted.

0:28 Encrypted data is useless to hackers and thieves, as it's translated into complex code, or ciphertext, that can't be read by humans. That's a good thing.

0:37 But while encryption safeguards our data as it's being stored or transferred, the data must be decrypted - or translated back into a clear text - to be processed.

0:46 This provides a window of opportunity where your data is exposed, making it vulnerable to cyber criminals, privacy violations, and other misuse.

0:55 IBM is combating this problem with Fully Homomorphic Encryption - or FHE - which is changing the paradigm of security.

1:02 It's a technique that enables computers to process sensitive data while it's still encrypted.

1:08 For example, every time you hop in the car and fire up your phone's navigation app, the app needs to know where you are, where you're going, and any stops along the way in order to give you the best route.

1:19 With FHE, the app could still provide those same directions without the service behind it needing to see or save that information about you.

1:26 Maybe you don't care about an app knowing your location, maybe the convenience outweighs the risks.

1:32 But what if this data was much more sensitive? Like, say, health care records? Or your personal banking data?

1:39 Suddenly, the stakes are much higher.

1:41 The ability to apply AI, machine learning, and other computing functions to data without exposing more private information is the essence of what Fully Homomorphic Encryption enables.

© Copyright International Business Machines Corporation 2021

1:52 First envisioned in the 1970s, an IBM researcher pioneered the mathematical framework to make FHE possible in 2009.

1:58 But FHE was too slow for everyday usage because of the enormous computing power required.

2:04 Back in 2011, it took 30 minutes to process a single bit using FHE.

2:09 But by 2015, we could compare two human genomes with FHE in less than an hour.

2:15 And now, through software and hardware advances, the time has come for companies to start experimenting with FHE.

2:22 FHE will be a game changer for security in the hybrid cloud era, unlocking new business opportunities.

2:27 With its ability to process regulated and sensitive data, FHE will drive wider enterprise adoption of hybrid cloud platforms, especially in highly regulated industries like financial services and health care.

2:39 FHE could also impact mergers and acquisitions, where due diligence could be performed without violating the privacy of account holders, shareholders, and clients.

2:47 Even airlines, hotels, and restaurants could utilize FHE to offer packages and promotions without giving their partners access to details of closely held customer data sets.

2:57 But first things first - companies need to get their hands on this technology to begin developing real world usages for FHE within their unique industries.

3:05 With the launch of IBM Security's Homomorphic Encryption Services, clients will gain access to both the tools and cryptography expertise needed to start building prototypes for their own FHE-enabled applications.

3:17 Pushing forward on this new frontier of security is part of what positions IBM as the leader in hybrid cloud - all the while protecting the privacy and trust of clients, and keeping your data safe.

© Copyright International Business Machines Corporation 2021