IBM Newsroom

IBM Helps Prepare Clients for Next Generation Encryption Technology

• New IBM Security Homomorphic Encryption Services will offer education, expert support, and testing environment to build prototype applications using emerging encryption schemes

• Fully homomorphic encryption could allow sensitive data to remain encrypted, even while being analyzed in cloud or third-party environments

ARMONK, N.Y., December 17, 2020 – Today, IBM (NYSE: IBM) Security launched a new service that allows companies to experiment with fully homomorphic encryption (FHE) – an emerging technology designed to allow data to remain encrypted even while being processed or analyzed in cloud or third-party environments. The new IBM Security Homomorphic Encryption Services provide companies with education, expert support, and a testing environment for clients to develop prototype applications that can take advantage of FHE.

With the growth of hybrid cloud, sensitive data will be even more broadly stored, shared and analyzed across platforms and parties, exposing it to varying security controls and risks. While current encryption techniques allow data to be protected during storage and in transit, data must be decrypted while it is being processed or analyzed – creating a window of opportunity where data is more vulnerable to theft or exposure. FHE is an emerging and advanced encryption technology that allows data to remain encrypted even while it's being processed, potentially closing this critical gap in current encryption solutions being used today.

"Fully homomorphic encryption holds tremendous potential for the future of privacy and cloud computing, but businesses must begin learning about and experimenting with FHE before they can take full advantage of what it has to offer," said Sridhar Muppidi, Chief Technology Officer, IBM Security. "By bringing IBM's cryptography expertise and resources to our clients that are driving innovation in their unique industries, we can work together to create a new generation of applications that leverage sensitive data, without compromising its privacy."

Building on groundwork and tools developed IBM Research and IBM Z, the new IBM Security Homomorphic Encryption Services provide a scalable hosting environment on IBM Cloud, along with consulting and managed services to help clients begin learning about and designing prototype solutions which can take advantage of FHE.

As FHE technology advances, these solutions can allow companies to apply functions like search, analytics and AI to their sensitive data in an environment, without revealing that data to the underlying service – helping them to maintain existing compliance and privacy controls as part of a "zero trust" security strategy. Additionally, FHE is based on lattice cryptography which is considered "quantum safe" – or resistant to breakage by future quantum-computing speeds.

Bridging Gap between Research and Early Adoption

The algorithms behind FHE have been under development by IBM and the broader research community for more than a decade, but FHE computations were originally too slow for everyday usage – taking days or weeks for calculations that take seconds without encryption. As industry compute power has grown exponentially, and the algorithms behind FHE have advanced, testing has shown that FHE is now capable of being performed at seconds per bit,[1] making it fast enough for many types of real-world use cases and early trials with businesses.

Gartner estimates that by 2025, at least 20% of companies will have a budget for projects that include fully homomorphic encryption (FHE), up from less than 1% today.[2]

Early this year, IBM released tools and educational materials for developers, and have been working with select clients on early pilot programs for FHE. IBM Security is now taking the next pivotal step in bringing FHE to a broader audience, launching a first-of-its-kind service offering to help companies get started with Fully Homomorphic Encryption.

Available today, the new IBM Security Homomorphic Encryption Services are designed to help educate and prepare clients to build and deploy FHE-enabled applications as the technology reaches maturity in the near future. The service includes access to both the tools and expertise needed to get started with FHE, including:

- FHE tools developed by IBM Research, which provide templates for common FHE use cases, such as encrypted search, AI and machine learning.
- Guidance, consulting and education support from IBM cryptography experts, helping companies build the skills needed to design and work with FHE-enabled applications.
- A scalable hosting environment on IBM Cloud for developers to begin experimenting and building prototypes for their own FHE-enabled applications.

As part of this service, IBM will work closely with clients to further develop new prototype solutions and use

cases that can take advantage of FHE technology – with the initial offering focused on developers and crypto engineers. Some of the initial use cases include performing analytics on encrypted data, conducting encrypted searches while concealing search query and content and training AI and machine learning models while maintaining existing privacy and confidentiality controls.

[1]FHE has been demonstrated at speeds of seconds per bit in select research/field trials.

[2]Gartner, "Emerging Technologies: Homomorphic Encryption for Data Sharing With Privacy," Mark Driver, 23 April 2020.

Additional Resources and Multi-Media:

- Media Kit: For images, videos, and additional content on Fully Homomorphic Encryption (FHE,) how it works, and potential use-cases, visit: https://newsroom.ibm.com/Homomorphic-Encryption-Services
- To learn more about the new IBM Security Fully Homomorphic Encryption Services, visit: ibm.com/security/services/homomorphic-encryption
- Register here for an IBM Security webinar on FHE and the new offering, taking place January 21, 2021.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Media Contact:

Cassy Lalan
Media Relations, IBM Security
(319) 230-2232
cllalan@us.ibm.com

Additional assets available online:  Photos

https://newsroom.ibm.com/2020-12-17-IBM-Helps-Prepare-Clients-for-Next-Generation-Encryption-Technology