IBM Security

IBM Security Homomorphic Encryption Services

What if you could unlock the value of your sensitive data without ever having to decrypt it?

With Fully Homomorphic Encryption (FHE), you can compute upon sensitive data while helping to maintain your privacy and compliance controls.

IBM Security now is offering a first-of-a-kind security services for FHE in the industry, pioneered by IBM Research® with over a decade of innovations.

IBM

Unlock value of sensitive data without decryption

Your business data is likely hosted and stored across hybrid multicloud environments, whether owned and managed by your organization or third-party providers. This setup can expose data to various risks and vulnerabilities. To mitigate this risk, security leaders of most enterprises encrypt their business data.

While encryption allows data to be protected both during transit and at rest, the data typically must be decrypted while being accessed for computing and business-critical operations. Under these conditions, you're potentially violating the privacy of your confidential data.

With FHE, the data is always encrypted and can be shared, even on untrusted domains in the cloud, while remaining unreadable by those doing the computation. In short, one can now do high-value analytics and data processing – by internal or external parties – without requiring that data to be exposed.

What we provide

IBM Security Homomorphic Encryption Services can help deliver what you need to get started, including the following solutions:

- Education and consulting on FHE concepts and constraints from IBM Data and Application Security Services advisors
- The FHE Toolkit with sample code and demonstrations to assist in learning and exploration
- A built-in Integrated Development Environment (IDE) for rapid development with minimal setup
- A managed computational environment on IBM Cloud® tailored to FHE use cases

Benefits of FHE

Data monetization

Can generate measurable economic benefits since organizations can compute and collaborate on sensitive business data while preserving data privacy.

Data privacy

Improves privacy since data can now be processed by third parties without divulging the data itself.

Regulatory compliance

Processes activities involving encrypted data without exposing sensitive information.

More secure use of cloud

Enables secure use of data computation in untrusted domains such as public cloud.

Talk to a trusted advisor: Take next steps today

IBM Security Homomorphic Encryption Services: Learn more

FHE use cases

Analytics over FHE encrypted data

Allow a third party to perform analytics on encrypted data with FHE without ever exposing it.

Marketing leaders can analyze a sensitive customer data set to run a campaign.

AI and machine learning

Train AI and machine learning models using a myriad of sensitive data without ever exposing the unencrypted data to the machine learning environment.

Developers can generate AI-driven insights from customers' personally identifiable information (PII) within their applications.

Search and data matching

Perform FHE encrypted searches without revealing the intent and contents of your search.

Users can perform point-of-interest searches on mobile devices without revealing the location.

Biometrics and behavioral Data

Authenticate to services providing only encrypted biometrics and behavioral information.

Customers can sign into applications without revealing their sensitive biometric data or usage patterns.