Homomorphic Encryption

Next-Generation Encryption Technology

Edited by **MOHAN DAS VISWAM**

Organisations handle a variety of sensitive information such as personally identifiable information (PII), Health care data, financial data etc. Privacy of such data is a prevalent issue. Traditional encryption schemes protect data at rest and data in transit. The problem with encrypting data is that, to perform computations or operations, data needs to be decrypted first, which makes it vulnerable to hackers. Protecting data integrity and privacy while processing 'data in use' is a major challenge. Sharing data in an untrusted environment is unavoidable in the digital world.

Homomorphic Encryption is an emerging Privacy Enhancing Technology which responds to the above challenges and enables data sharing for computing without compromising privacy. It allows direct mathematical operations on encrypted data without requiring decryption during the process. After computation, the results are returned directly in encrypted format, ensuring that only the owner of the data can see the processed results by decrypting it. The confidentiality of data is maintained in Homomorphic Encryption even when the computations are performed on data residing in an untrusted environment.

> Data security is extremely important in today's data driven world. The Homomorphic Encryption (HE) is a Privacy Enhancing Technology (PET) which enables data sharing and collaboration stored in silos, while preserving the privacy of data throughout its processing life cycle.

K.P. Pariselvan
Dy. Director General & SIO
kpp.pari@nic.in

Savita Bhatnagar
Sr. Technical Director
savita.bhatnagar@nic.in

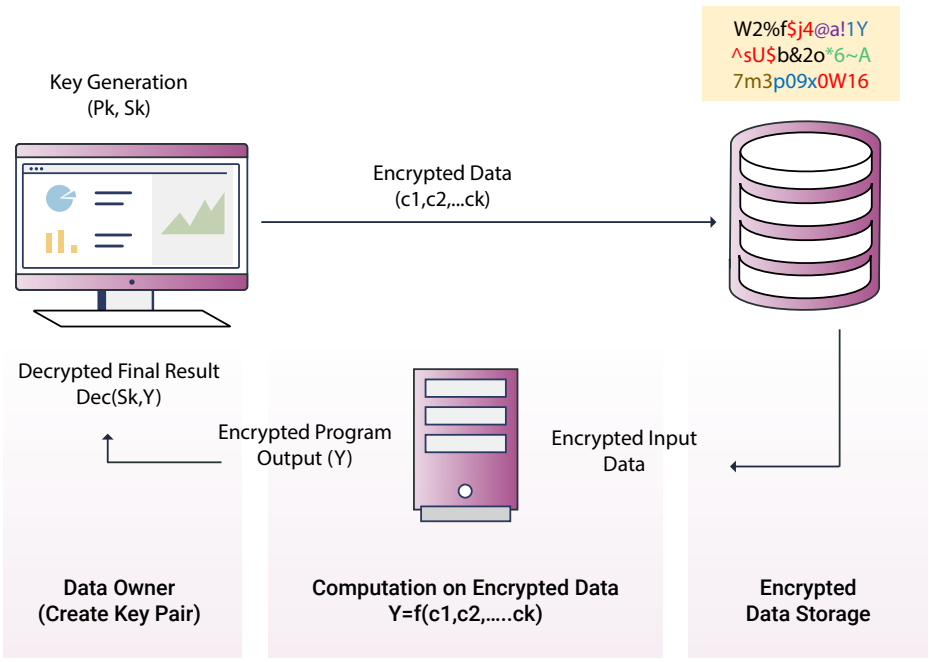
Homomorphic Encryption is widely defined as "A form of encryption allowing one to perform calculations on encrypted data without decrypting it first".

Traditional encryption schemes contain three-step algorithms: Key Generation, Encryption and Decryption. Homomorphic Encryption schemes involve one more algorithm which is called evaluation. Homomorphic evaluator f takes encryptions of $m1, ..., mk$, which is $(c1, c2, ..., ck)$ as inputs and output a ciphertext that decrypts to $f(m1, ..., mk)$.

Types of Homomorphic Encryption

There are three types of Homomorphic Encryption schemes. The primary difference between them is based on the types and frequency of mathematical operations that can be performed on the ciphertext.

- **Partially Homomorphic Encryption (PHE):** Allows only one operation either addition or multiplication on encrypted data, but not both. Selected operations can be performed an unlimited number of times on the ciphertext. The most popular PHE methods available are ElGamal encryption (a multiplication scheme) and Paillier encryption (an addition scheme).
- **Somewhat Homomorphic Encryption (SHE):** Allows more than one operation to be performed on encrypted data but only a limited number of times. The Boneh-Goh-Nissim (BGN) method is one of Somewhat Homomorphic Encryption schemes. This method allows an unlimited number of additions but only one multiplication to be performed on data.
- **Fully Homomorphic Encryption (FHE):** It allows an unlimited number of different types of evaluation operations on the encrypted data and the resulting output is within the ciphertext space. The first fully Homomorphic Encryption algorithm was invented in 2009, which allows performing arbitrary secure computations over encrypted data. Since then, many algorithms have been developed that improve on the original FHE algorithm. Brakerski-Gentry-Vaikuntanathan (BGV), Cheon-Kim-Kim-Song (CKKS) are some of FHE schemes.



▲ Fig. 8.1: Homomorphic Encryption Scheme

Applications of Homomorphic Encryption

Organisations are taking greater interest in Homomorphic Encryption because it is expected to play an important role in protecting data privacy in cloud platforms while allowing collaborative projects. Companies like IBM, Google, Microsoft are working on Homomorphic Encryption. Eventually, Homomorphic Encryption is moving from theoretical cryptography research area to applied cryptography research. Tools & libraries are available for organisations to experiment with Homomorphic Encryption and start designing prototype solutions. Some of the applications are discussed below:

- **Secure Data in the Cloud:** There are many debates about data residency, data ownership, and data privacy on the cloud. Homomorphic Encryption allows organisations to leverage cloud services securely. Data can be kept in the cloud in encrypted form while retaining the ability to perform calculations and search on ciphered information.
- **Data Analytics as Service:** Homomorphic Encryption allows us to utilise the services of analytics service providers without putting data privacy at risk. Service providers never see the client's private data. Homomorphic Encryption makes it possible for the service provider to perform analytics and draw insights from encrypted user data without compromising the confidentiality of user information.
- **Enhance Collaboration:** Homomorphic Encryption allows organisations to share sensitive data in encrypted form for computation. This can accelerate collaboration and innovation without the risk of sensitive information getting compromised.
- **Outsourcing of Research and Analytics in Regulated Industries:** Homomorphic Encryption allows heavily regulated industries, such as healthcare and finance, to get outsourcing services for research and analytical purposes without the risk of non-compliance. There is no need to mask or drop any features in order to preserve the privacy of data. All features may be used in an analysis without compromising privacy.

Conclusion

Homomorphic Encryption is an emerging, cutting-edge, privacy-preserving computation technology that offers collaborative and secure computing in an untrusted environment. Gartner has also listed Privacy-Enhancing Computation as one of the 12 top strategic technology trends for 2022. Considering the volume of data and requirement for round-the-clock availability, it is unavoidable for industries and organisations to keep the data on a third party cloud environment.

This ground-breaking technology will enable governments and industries to utilise outsourced storage and computation services securely.

Contact for more details

State Informatics Officer
NIC Maharashtra State Centre
11th Floor, New Administrative Building
Madam Cama Road, Mumbai, Maharashtra - 400032
Email: siomsu@nic.in, Phone: 022-22024552 / 22046934