



# Chapter 10

## Homomorphic Encryption and Machine Learning in the Encrypted Domain


**Neethu Krishna**

 <https://orcid.org/0000-0002-6061-9193>  
SCMS School of Engineering and Technology,  
Karukutty, India

**Kommisetti Murthy Raju**

 <https://orcid.org/0000-0002-7576-4449>  
Shri Vishnu Engineering College For Women, India


**V. Dankan Gowda**

 <https://orcid.org/0000-0003-0724-0333>  
BMS Institute of Technology and Management, India

**G. Arun**

Erode Sengunthar Engineering College, India

**Sampathirao Suneetha**

 <https://orcid.org/0009-0005-2714-6442>  
Andhra University College of Engineering,  
Andhra University, India

### ABSTRACT

*In cryptography, performing computations on encrypted material without first decrypting it has long been an aspiration. This is exactly what homomorphic encryption (HE) accomplishes. By allowing computation on encrypted data, the associated privacy and security of sensitive information are beyond imagination to date. This chapter delves into the vast and intricate realm of HE, its fundamental theories, and far-reaching implications for machine learning. As a result of the sensitive nature of the data on which machine learning is based, privacy and security issues often arise. In this vein, homomorphic encryption, which allows algorithms to learn from and predict encrypted data, emerges as a possible panacea. The authors thus set out in this chapter to prepare the ground for a deeper understanding of that synergy, showing how it is there but also what lies ahead.*

DOI: 10.4018/979-8-3693-1642-9.ch010

## 1. INTRODUCTION TO HOMOMORPHIC ENCRYPTION

There exists a class of encryption, called HOMOMORPHIC Encryption (HE), that objects can be computed on directly in ciphertext. After being decrypted the results are identical to what would have been obtained if they had instead applied these operations to plain text. Because of this special property, HE becomes an effective instrument for secure data processing--sensitive information is encrypted even during computation. The principle of homomorphic HE means that the structure exists before and remains unchanged after in between encryption and computation. For instance, if you have two numbers in the clear--2 and 3 say--and wish to add them in encrypted form, HE would permit you first to transform these into ciphertexts then proceed with performing an addition operation on their respective encryptions. Decrypting the result will reveal 5, which is indeed equal to a sum of these original numbers. Historical Context and Development: The concept of Homomorphic Encryption goes back to the conception of RSA (invented in 1978) as an algorithm with homomorphic properties. But this was only for specific operations. The breakthrough came in 2009, when Craig Gentry--a student at Stanford working on his Ph.D. thesis--developed a fully homomorphic encryption scheme for the first time ever. This was a turning point, because it proved that one could perform arbitrary computations on encrypted data.

Its initial proposal for construction was lattice-based cryptography (Suryawanshi and Abhay Chaturvedi, 2022). It proposed an encryption scheme that could evaluate the circuit of its own decryption function homomorphically. This first scheme, though revolutionary, was unpractical in being too slow and complex. But it laid the groundwork for later research in that field.

Since then, HE has been a fast-developing field of research. Researchers have produced ever more effective and practical schemes. These technical breakthroughs have been brought about by the increasing importance of data privacy and security in areas from cloud computing to finance, healthcare, etc. Collaboration between cryptographers, mathematicians and computer scientists has characterized the development of HE.

Homomorphic Encryption now leads the way in search for secure data processing. In the age of big data and cloud computing, where privacy matters more than ever, this is seen as an essential technology (A. Singla, N. Sharma 2022). Later in the sections dealing with HE, we will see how this technology is not just a concept but can actually be something that people could use to radically change our handling and processing of information.

## 2. HOMOMORPHIC ENCRYPTION TECHNIQUES

The initial idea behind cryptography was to create a system that could guarantee safe communication between various entities. One side encrypts a message and sends it to the other, who can decode it (A. Singla, N. Sharma 2022). The idea of doing calculations on encrypted data was first proposed as a “privacy transformation” in 1978 by Rivest, Adleman, and Dertouzos. What is currently known as homomorphic encryption developed out of this idea over time. Homomorphic encryption, in a wide sense, allows us to compute on encrypted data. If a scheme has the following characteristics, we say that it is additively (or multiplicatively) homomorphic:

$$[x] \oplus [y] = [x + y] \text{ and } [x] \otimes [y] = [x \cdot y]$$

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:  
[www.igi-global.com/chapter/homomorphic-encryption-and-machine-learning-in-the-encrypted-domain/340979](http://www.igi-global.com/chapter/homomorphic-encryption-and-machine-learning-in-the-encrypted-domain/340979)

## Related Content

---

### Programming the Blockchain

(2017). *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities* (pp. 64-71).

[www.irma-international.org/chapter/programming-the-blockchain/176869](http://www.irma-international.org/chapter/programming-the-blockchain/176869)

### Supply Chain Governance Using DAO

Sujatha Gurunathan (2024). *Machine Learning and Cryptographic Solutions for Data Protection and Network Security* (pp. 444-456).

[www.irma-international.org/chapter/supply-chain-governance-using-dao/348623](http://www.irma-international.org/chapter/supply-chain-governance-using-dao/348623)

### Future Outlook: Synergies Between Advanced AI and Cryptographic Research

Dankan Gowda V., Joochi Garg, Shaifali Garg, K. D. V. Prasad and Sampathirao Suneetha (2024). *Innovative Machine Learning Applications for Cryptography* (pp. 27-46).

[www.irma-international.org/chapter/future-outlook/340971](http://www.irma-international.org/chapter/future-outlook/340971)

### Secret Communication Techniques

(2019). *Advanced Digital Image Steganography Using LSB, PVD, and EMD: Emerging Research and Opportunities* (pp. 1-19).

[www.irma-international.org/chapter/secret-communication-techniques/230055](http://www.irma-international.org/chapter/secret-communication-techniques/230055)

### Authentication of Smart Grid: The Case for Using Merkle Trees

Melesio Calderón Muñoz and Melody Moh (2020). *Cryptography: Breakthroughs in Research and Practice* (pp. 257-276).

[www.irma-international.org/chapter/authentication-of-smart-grid/244918](http://www.irma-international.org/chapter/authentication-of-smart-grid/244918)