Privacy Preserving Cloud Computing

Indranil Thakur

Indian Institute of Technology Kanpur, India

indra@cse.iitk.ac.in

Abstract

Cloud computing is the backbone of the data-driven digital era. It has revolutionized digital storage and processing by delivering on-demand cloud services over the Internet. However, it poses data security and privacy concerns. Cloud clients have to blindly trust third-party cloud service providers. Fully Homomorphic Encryption (FHE) has emerged as an ideal technique for computing on encrypted data. However, current FHE schemes suffer from slow encryption speed and large ciphertext expansion. Practical implementation is hindered, especially when the client has limited bandwidth, memory, and computing power.

In this paper, we discuss how to mitigate these limitations. In particular, we explore Hybrid Homomorphic Encryption (HHE). It is a technique designed to address the drawbacks of FHE by incorporating symmetric cryptography. The field of HHE is a relatively new area of study that requires extensive research. We highlight gaps, open problems, and directions for future research.