IMPLEMENTING HOMOMORPHIC ENCRYPTION AND DECRYPTIONS FOR SECURELY SHARING IMPORTANT DATA

Objective: The aim of my project was to implement the most recently published fully homomorphic encryption scheme. The idea behind this is to protect the data which needs to be shared with others in order for them to work on it without knowing the details of it.

Introduction: Homomorphic encryption – encryption that supports operations on encrypted data – has a wide range of applications in cryptography. The concept was first introduced in 1978 by Rivest et al. shortly after the discovery of public key cryptography [1], and many popular cryptosystems, such as unpadded RSA or ElGamal, support either addition or multiplication of encrypted data. It was only in 2009 however, that Craig Gentry discovered the first plausible construction of a fully homomorphic encryption system supporting both operations [2].

Note : Call for Final year engineering project ask for detailed synopsis for CSE students

Shield Technologies

#2232, 3rd floor, 16th B cross, Yelahanka new town, Bangalore-64

Phone: 9972364704 / 08073744810