Abstract

Cloud computing is an arising computational model, where data and its several services associated with its scalable data centers in the cloud and can be obtained from the Internet. Computing gives an added amount of risk as vital services which are usually deployed to any third party, which creates the difficulty to enable data security, privacy factor, confidentiality, integrity, and authentication. Most of the users prefer to store their data inside the cloud in an encrypted/unoriginal format to decrease the security concerns. However, to perform any operation on data at server, cloud needs to first decrypt the data. This operation might cause the challenging issues like - confidentiality along with privacy of confidential data, stored inside the cloud. Here, This paper presents state of the art in this Homomorphic Encryption (HE) domain, and solve the problems of confidentiality and privacy of stored data in a cloud. HE is a kind of encryption mechanism that give ability to users for computations to be prosecuted on cipher text itself, thus producing an unoriginal/encrypted result when decrypted it shows similarity on the result of operations prosecuted on the plain text. Homomorphic Encryption is generally of two types i.e. Partial Homomorphic encryption (PHE) and Fully Homomorphic
Encryption (FHE). FHE considered to be as more secure and efficient in the form of third party computations, since it gains the advantage of both properties - Additive as well as multiplicative homomorphism. Based on the research done in past years, identification of the problem in the existing system is also presented in this paper and have given our future research directions.

References


18. Shafi Goldwasser, Yael Kalai, "Introduction to Homomorphic Encryption", (6.889), New
Developments in Cryptography, MIT CSAIL: February 1, 2011.

**Index Terms**

Computer Science               Security

**Keywords**

Cloud Environment, Data security, Homomorphic encryption, Privacy