Enabling Multi keyword Search on Secure Encrypted Data using Multi Cloud Approach

Dr. Mamatha G[1], Dr. Ramesh Hegde[2], Shilpitha Swarna[3], Lakshmikanthaiah SM[4]
[1]Professor, Department of ISE, Acharya Institute of Technology, Bangalore
[2]Professor & Head, Department of MCA, Acharya Institute of Technology, Bangalore
3Assistant Professor, Department of MCA, Acharya Institute of Technology
[4]Senior Software Engineer,

Abstract—

Cloud computing provides lot of benefits to enterprises to offload their data and software services to cloud saving them lot of money that has to be spent on infrastructure setup cost. Enterprises wanted to offload their data to cloud and save on their infrastructure cost. But when offloading the data security and privacy is a important concern. When the data offloaded to cloud by a enterprise is compromised, the enterprise will lose its business. Similarly when the hospitals and health care organization upload their patients details to cloud and when the data is comprised, it will affect the privacy of the patients. So privacy is a important concern when offloading the data to cloud. Most of solutions for privacy is based on encryption and data to be offloaded is encrypted and stored in cloud. Algorithms like AES, DES etc are used for encrypting the data before offloading to cloud. But the side effect in this encryption mechanism is that, the encrypted data is not order preserving and it is not suitable for searching and ranking. To solve it in work [1], author has proposed homomorphic encryption based mechanism. But the solution suffers from capture attack and relies on semi trust model on cloud. In this paper, we discuss the capture attack in detail and propose a solution based on multi cloud to avoid the same.