DATA SECURITY IN CLOUD COMPUTING
USING ENCRYPTION AND OBfuscATION TECHNIQUES

Krunal Suthar

ABSTRACT

Cloud computing is now a day’s becomes the most attracted phenomena to use for large scale organization or for individual who need various network services with least cost. Normally individual’s information is stored on public Cloud which is available to everyone for access. This fundamental raises some issue opposite to flexible services provided by cloud providers, like Confidentiality, Integrity, Availability, Authorization and many more.

Recently, Lots of options are available to protect the data and most preferable ways is to use encryption. Encryption only can’t provide enough protection while considering lots of users’ sensitive information. It also consumes more time to perform encryption and decryption process for every single query. Secondly it’s not a good practice to think only about user centric because once user data is uploaded on Cloud premises, user doesn’t have direct control over this data. Considering this fact, we must need to think about the security of user’s valuable information on Cloud server. This becomes possible using the important techniques that’s obfuscation. To remove burden of Cloud server as well to provide adequate security to user’s information, we propose a methodology by combining both techniques wiz. Obfuscation and Encryption in this thesis.

The user data may be encrypted if it requires security for its files or document and the DaaS service of Cloud is secured using obfuscation techniques. Using these two way approach, we can say that the proposed scheme offers enough security towards anonymous access and preserve privacy even the information available on Cloud servers. Our aim is also to provide proper integrity checking mechanism, better access control mechanism, Group sharing mechanism etc. which lessen the burden and increase trust level between Client and Service Providers.