A Key-Policy Attribute-Based Temporary Keyword Search scheme for Secure Cloud Storage

A. Suganya, Assistant Professor, Indra Ganesan College of Engineering

N. Deepika, Ug Student, Indra Ganesan College of Engineering

S. Sivasankari, UG Student, Indra Ganesan College of Engineering

Abstract

The cloud enables users to access the same files and applications from almost any device, because the computing and storage takes place on servers in a data centre, instead of locally on the user device.The cloud providers are not fully trusted in the accept of temporary keyword search on confidential data. Hence this is the main focus of this research, it is necessary to outsource data in the encrypted format. In the attribute-based keyword search scheme the authorized users generate some tokens which were in encrypted format and send them to cloud for the search operation. These tokens can be used to extract all the cipher texts which are generated at any time and contain the search token which were generated by authorized users. Since this may lead to some information leakage, a new cryptographic primitive is introduced which is more secure to propose a scheme called key-policy attribute-based temporary keyword search (KPABTKS) which provide this property. To evaluate the security of our scheme, and formally prove that our proposed scheme achieves the keyword secrecy property and is secure against selectively chosen keyword attack (SCKA) both in the random oracle model and under the hardness of Decisional Bilinear Diffie-Hellman (DBDH) assumption. Furthermore, It show that the complexity of the encryption algorithm is linear with respect to the number of the involved attributes.