

DATA SECURITY SYSTEM AND METHOD FOR OPERATION THEREOF

ABSTRACT

There is provided a system and method for operating a data security system wherein attribute based encrypted ciphertext data is stored on a publicly accessible server, such as a public cloud hosting service. The system enables the decryption of the ciphertext to be outsourced to one or more third parties, whereby a substantial part the decryption will be conducted by such third parties, to alleviate the decrypting burden imposed on the computing devices of the users. The system further provides security features to prevent unauthorised decrypting of the ciphertext. This is achieved by having the public cloud use a public decryption key to partially decrypt the ciphertext to yield a partially decrypted ciphertext, transmitting this partially decrypted ciphertext to a private computer server that further partially decrypts the partially decrypted ciphertext to yield an intermediate decrypted ciphertext, and transmitting the intermediate decrypted ciphertext to a user who fully decrypts the intermediate decrypted ciphertext to yield unencrypted data. At both the public cloud and the private computer server the identity of the user is confirmed to ensure that the user is authorised to request decryption of the data.

(Figure 1)