Abstract

Cloud computing is a new era, attracting peoples for different services providing in cost effective manner. Privacy management is one of the critical issues in cloud when these services accessed through untrusted service provider or third party. There is risk with sending personal information to such parties. We proposed a strong privacy preserving scheme for processing of personal information at untrusted service provider or third party end in the cloud. With making use of homomorphic encryption function on personal information, the proposed scheme maintains confidentiality of personal information sent by the cloud users to untrusted service provider or third party. While registering to a cloud, the personal information sent by cloud user is encrypted by making use of homomorphic function. Cloud server receives this information in encrypted form and decrypts it by using homomorphic decryption function. The personal information of cloud user is stored at cloud server database and general information is created like registration ID. When it requires to access the services from untrusted service provider or third party, it need to login to cloud through such parties. In this, first, information sent by cloud user is encrypted using a homomorphic function and sent to the untrusted service provider or third party along with its general information. The service provider receives the encrypted information and request to cloud server for personal information by providing the received general information. Cloud server encrypts the personal information related to received general
information using another homomorphic function and sends it to the untrusted service provider or third party. Now, untrusted service provider or third party compares the personal information received from both, client and server in encrypted form. Moreover, the proposed scheme condenses computation at cloud server by eliminating process of authentication. Theoretical analysis and simulative evolution demonstrate the soundness and effectiveness of the proposed privacy management scheme in cloud computing.

References


Index Terms

Computer Science  Security

Keywords

Cloud computing  Homomorphic encryption  Privacy management  Third party in cloud