A FRAMEWORK FOR SECURE DATA EXCHANGE IN MOBILE CLOUD COMPUTING

Ardi Benusi[1], Dolantina hyka[2]

[1]Faculty of Natural Sciences, University of Tirana, Albania,
E mail: ardi.benusi@fshn.edu.al
[2]Faculty of Natural Sciences, University of Tirana, Albania,
E mail: dolantina.hyka@fshn.edu.al

Abstract

Cloud computing optimizes usage of IT resources such as CPU, storage and network. Network access technologies like 2G, 3G, Wi-Fi, Wi-Max etc. have made possible emerging of a new derivate of Cloud Computing known as Mobile Cloud Computing (MCC) where the related processing of data happens in the cloud and can be accessed through mobile devices. In this paper we address issue of a secured data service for file exchange between two end users, one the owner of the file and other the authorized receiver. The cloud mobile is used for storing encrypted files without disclosing any information to the cloud provider. The proxy re-encryption and identity based encryption schemes are used based on bilinear mapping. The security scheme is considered strong based on the hardness of Decisional Bilinear Diffie-Hellman assumption and its related inversion.

Keywords: *Cloud Computing, Mobile Cloud Computing, Cryptography, proxy re-encryption, bilinear maps, Algorithmic, identity based encryption, Diffie-Hellman.*