Abstract

Mobile technology is proving to offer unprecedented advantage to health professionals by providing a more efficient transmission and access to health services. However, mobile devices are resource-constrained. This is setback whenever storage and computation are required on ehealth big data. To mitigate this drawback, mobile computing is integrated with scalable cloud computing. While this is an advantage on mobile user's side by enlarging the limited resources of the device, it also gives rise to security and privacy concerns. In order to overcome these challenges associated with security and privacy, the data owner (hospital) encrypts data using Attribute Based Encryption (ABE) primitive due to the fine-grained access control advantage it offers then sends ciphertext to the cloud. To realize fast data access, the resource-constrained device securely outsources heavy computations to resource abundant cloud server on its behalf with the guarantee that the server cannot learn anything about plaintext. In this paper, a survey of ABE with outsourced decryption of the existing works that is applicable to resource-constrained device for accessing eHealth big data is provided.