Secure data transformation in cloud using ECC and RSA - A review

EBT Hansika, URC Upeksha, TL Weerawardane

Department of Computer Science, Department of Computer Engineering, Faculty of Computing, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka

Abstract. Unlike traditional storage systems, the cloud is a very well-known and accepted data storage that provides many benefits to users with a pay-as-you-go pricing model, even providing storage solutions for massive amounts of data. Many users nowadays use different cloud services, mainly because the data can be accessed from anywhere via the internet. The cloud servers are located all over the world storing massive amounts of data. When a user uploads or downloads from the cloud server, the data is exposed to the internet. This can lead to security issues such as unauthorized disclosure of data and the privacy of users if the data is not properly protected. Many cryptographic algorithms are used to secure data transformation in the cloud. ECC (Elliptic Curve Cryptography) and RSA are asymmetric encryption algorithms that can secure data in the cloud, in which encryption and decryption are performed using different keys, one a private key and one a public key. RSA is a block cipher in which the plaintext and ciphertext are integers and it involves 3 steps as key generation, encryption, and decryption. Elliptic Curve Cryptography (ECC) is one of the public key cryptographic schemes which uses the characteristics of an elliptical curve to create Cryptographic calculations depending on the mathematical background. This paper focuses on the significance of both ECC and RSA as a review of the researches, compared with other asymmetric algorithms which have been used in the cloud to secure data transformation. It is intended to distinguish the features and functionalities to overcome drawbacks when implementing ECC and RSA for the data transformation in the cloud.

Keywords: *RSA, ECC (Elliptic Curve Cryptography), Cloud, Asymmetric algorithms*