ID 167

Secure Data Transformation in Cloud Using Hybrid Cryptography

EBT Hansika[1#], RGC Upeksha[1] and TL Weerawardane[2]

[1]*Department of Computer Science, General Sir John Kotelawala Defence University, Sri Lanka*
[2]*Department of Computer Engineering, General Sir John Kotelawala Defence University, Sri Lanka*

[#]36-cs-0007@kdu.ac.lk

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. 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 unauthorised disclosure of data and lack of user privacy if the data is not properly protected. Many cryptographic algorithms are used to secure data transformation in the Cloud. The proposed system is designed to offer a method for properly securing data when transferring them to the Cloud, utilising various cryptographic techniques, and integrating them most innovatively and effectively considering the security, data integrity, speed and data confidentiality. The data is encrypted using a combination of three algorithms namely AES, ECC and RSA by increasing the security of the data. The keys generated by the ECC and RSA are combined using an Exclusive OR gate. The AES key is uploaded into the key management server after being encrypted by the newly generated key. The data encrypted by the AES key are uploaded into the Cloud storage. The proposed system is intended to distinguish the features and functionalities to overcome the drawbacks of the current systems.

Keywords: *RSA, Elliptic Curve Cryptography (ECC), AES, cloud, key management server*