UNIVERSITAS
GADJAH MADA

Client Side Encryption in Dropbox Cloud Storage Using AES 128 Algorithm
IKVI A R, Dr.-Ing. Mhd. Reza M.I Pulungan, S,Si., M.Sc
Universitas Gadjah Mada, 2016 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

Client Side Encryption in Dropbox Cloud Storage using AES 128 Algorithm

by

Ikvi Auliaurrachmah
11/315568/PA/13774

In cloud computing systems, data are stored on remote servers accessed through the internet. The increasing volume of personal and vital data, brings up more focus on storing the data securely. Storing data in the cloud has many advantages such as reducing storage in local computer, can be accessed from anywhere because the files stored on the internet, and becoming a safe file backup.

Once users put a file on the internet, it does not guarantee the file will be safe from hackers. Therefore, this research focuses on client side encryption before the file is uploaded to the Dropbox. AES 128 algorithm is chosen because of the security level.

To provide an efficient and secure application, files to be uploaded to Dropbox is firstly encrypted using AES. However, the file can be accessed through Dropbox desktop client in an unencrypted form. The result shows that this application can be effective and secure. It stores encrypted files into Dropbox with running time process faster than running time of uploading through Dropbox website directly.

Keywords: AES encryption and decryption, cloud storage, data security, client side encryption.