

ABSTRAK

Pada saat ini, keamanan informasi menjadi isu penting dalam penyimpanan dan transmisi data. Penggunaan data citra semakin luas dalam berbagai bidang. Oleh karena itu, pengamanan data citra dari akses yang tidak berhak menjadi hal yang penting. Komputasi awan merupakan salah satu contoh perkembangan teknologi informasi. Salah satu layanan komputasi awan yang digunakan adalah *AWS S3*. Ruang penyimpanan pada *AWS S3* yang dapat digunakan paling kecil 5 GB, sehingga semakin besar ukuran *file* yang di unggah semakin besar pula ruang penyimpanan yang dibutuhkan. Oleh karena itu penulis membuat aplikasi enkripsi data dan kompresi data sebelum diunggah ke *Cloud Storage AWS S3* yang menggunakan algoritma kriptografi AES (*Advanced Encryption Standard*) dan LZW (*Lempel Ziv Welch*) untuk mengenkripsi dan kompresi berkas sebelum diunggah ke *AWS S3*. Hasil penelitian mengungkapkan bahwa proses enkripsi dan dekripsi memerlukan waktu kurang dari 0,5 detik untuk berkas berukuran 5 MB dan berkas terenkripsi juga tidak dapat diakses, dan juga proses kompresi menghemat ruang penyimpanan *AWS S3* dengan rasio pengkompersian 22,18% untuk berkas 4 MB dengan format **.txt*.

Kata Kunci: kriptografi, kompresi, LZW, AES, *AWS S3*, komputasi awan, keamanan

ABSTRACT

*At this time, information security is an important issue in data storage and transmission. The use of image data is increasingly widespread in various fields. Therefore, securing image data from unauthorized access is important. Cloud computing is one example of the development of information technology. One of the cloud computing services used is AWS S3. The minimum usable storage space on AWS S3 is 5 GB, so the larger the uploaded file size, the larger the storage space required. Therefore, the author creates a data encryption and data compression application before uploading to AWS S3 Cloud Storage that uses the AES (Advanced Encryption Standard) and LZW (Lempel Ziv Welch) cryptographic algorithms to encrypt and compress files before uploading them to AWS S3. The results reveal that the encryption and decryption process takes less than 0.5 seconds for a 5 MB file and the encrypted file is also inaccessible, and also the compression process saves AWS S3 storage space with a 22.18% compression ratio for a 4 MB file with *.txt format.*

keywords: cryptography, compression, LZW, AES, AWS S3, Cloud computing, security

