

# **Sistem Keamanan Data Menggunakan Algoritma AES dan RSA Pada Cloud Storage**

**Gading Nova Ardana**

## **ABSTRAK**

Pada zaman teknologi yang pesat seperti saat ini dokumen dan informasi lebih banyak berbentuk digital. Dokumen digital tersebut banyak yang disimpan di internet dengan memanfaatkan media penyimpanan cloud. Media penyimpanan *cloud* merupakan teknologi yang memanfaatkan server virtual untuk penyimpanannya. Keamanan data merupakan hal yang harus diperhatikan dalam menyimpan data di cloud. Salah satu cara dalam mengamankan data adalah dengan menggunakan kriptografi. Kriptografi bekerja dengan cara menyandikan isi teks menggunakan sebuah kunci, teknik penyandian ini disebut enkripsi. Selain melakukan enkripsi, penting juga mengetahui cara melakukan dekripsi agar isi teks bisa dibaca kembali. Proses dekripsi merupakan proses untuk mengubah teks yang sudah dienkripsi menggunakan kunci. Pada penelitian ini penulis membuat sistem untuk keamanan data yang terhubung ke *cloud storage*. *Cloud storage* yang digunakan dalam penelitian ini adalah Google Drive dan Dropbox. Metode kriptografi yang digunakan dalam penelitian ini adalah kriptografi asimetris RSA (*Rivest Shamir Adleman*) dan kriptografi simetris AES (*Advanced Encryption Standard*). Sistem ini dikembangkan menggunakan bahasa pemrograman PHP. Hasil akhir dari penelitian ini adalah sistem berbasis client-server yang dapat digunakan untuk mengunggah file yang otomatis terenkripsi ke *cloud storage* dan mendekripsi file enkripsi yang diunduh dari *cloud storage*.

**Kata Kunci:** Keamanan Data, *Cloud*, *Cloud Storage*, RSA, AES

# **Sistem Keamanan Data Menggunakan Algoritma AES dan RSA PadaCloud Storage**

**Gading Nova Ardana**

## **ABSTRACT**

In the era of rapid technology like today, documents and information are mostly in digital form. Many of these digital documents are stored on the internet by utilizing cloud storage. Cloud storage is a technology that utilizes virtual servers for storage. Data security is something that must be considered in storing data in the cloud. One way to secure data is to use cryptography. Cryptography works by encoding the contents of the text using a key, this encoding technique is called encryption. In addition to encrypting, it is also important to know how to decrypt so that the contents of the text can be read again. The decryption process is the process of changing the encrypted text using a key. In this study, the author makes a system for data security that is connected to cloud storage. Cloud storage used in this research is Google Drive and Dropbox. The cryptographic methods used in this research are asymmetric cryptography RSA (*Rivest Shamir Adleman*) and symmetric cryptography AES (*Advanced Encryption Standard*). This system was developed using the PHP programming language. The final result of this research is a client-server based system that can be used to upload encrypted files automatically to cloud storage and decrypt encrypted files downloaded from cloud storage.

**Keywords:** Data Security, *Cloud, Cloud Storage*, RSA, AES)