



**SISTEM KEAMANAN DATA MENGGUNAKAN ALGORITMA AES DAN
RSA PADA CLOUD STORAGE**

SKRIPSI

GADING NOVA ARDANA

1710511056

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2021



**SISTEM KEAMANAN DATA MENGGUNAKAN ALGORITMA AES DAN
RSA PADA CLOUD STORAGE**

SKRIPSI

Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar

Sarjana Komputer

GADING NOVA ARDANA

1710511056

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2021

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Gading Nova Ardana

NIM : 1710511056

Tanggal : 25 Juli 2021

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 25 Juli 2021

Yang Menyatakan,



(Gading Nova Ardana)

**PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan dibawah ini:

Nama : Gading Nova Ardana

NIM 1710511056

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non-Eksklusif (*Non-Exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

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

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Jakarta

Pada tanggal: 25 Juli 2021

Yang Menyatakan,



(Gading Nova Ardana)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Tugas Akhir berikut :

Nama : Gading Nova Ardana

NIM : 1710511056

Program Studi : Informatika

Judul : SISTEM KEAMANAN DATA
MENGUNAKAN ALGORITMA AES DAN RSA
PADA CLOUD STORAGE

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Hengki Bayu Seta, S.kom., M.TI.

Penguji I



Ing. Artambo B. Pangaribuan.,B.Sc

Penguji II



Dr. Ermatita, M.Kom.

Pembimbing I



Nurul Chamidah, S.Kom., M.Kom.

Pembimbing II



Dr. Ermatita, M.Kom.

Dekan



Yuni Widiastiwi, S.Kom., Msi.

Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Persetujuan : 19 Juli 2021



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)

KATA PENGANTAR

Pertama-tama penulis panjatkan puji dan syukur atas kehadiran Allah SWT atas rahmat dan karunia yang diberikan kepada penulis sehingga diberikan kesehatan dan dapat menyelesaikan Skripsi tugas akhir dengan judul: “Sistem Keamanan Enkripsi Data Menggunakan Algoritma AES dan RSA Pada *Cloud Storage*” yang ditujukan untuk menjadi syarat kelulusan untuk menyelesaikan studi Sarjana Pendidikan Strata Satu program studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Jakarta. Kemudian tidak lupa penulis ingin berterima kasih atas dukungan, doa, dan bimbingan dari berbagai pihak yaitu kepada:

1. Orang tua saya yang telah mendukung dan memberikan semangat dan doa sehingga Skripsi tugas akhir ini dapat diselesaikan.
2. Ibu Dr. Ermatita, M.Kom. selaku Dosen Pembimbing Satu yang telah membimbing penulis dalam Menyusun dan menulis Skripsi tugas akhir ini.
3. Ibu Nurul Chamidah, S.Kom., M.Kom selaku Dosen Pembimbing Dua yang telah membimbing penulis dalam Menyusun dan menulis Skripsi tugas akhir ini.
4. Bapak/Ibu dosen Informatika Universitas Pembangunan Nasional “Veteran” Jakarta yang telah memberikan ilmu kepada penulis sehingga mendapatkan ilmu yang bermanfaat.
5. Teman -teman penulis yang telah menyediakan waktu untuk berdiskusi dengan saya mengenai Skripsi tugas akhir.

Semoga Skripsi tugas akhir ini dapat bermanfaat terutama untuk penelitian yang akan dilakukan selanjutnya.

Jakarta, 25 Juli 2021



(Gading Nova Ardana)

DAFTAR ISI

PERNYATAAN ORISIONALITAS	iii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS.....	iv
LEMBAR PENGESAHAN.....	v
ABSTRAK.....	vi
ABSTRACT	vii
KATA PENGANTAR.....	viii
DAFTAR ISI	ix
DAFTAR TABEL	xiii
DAFTAR GAMBAR.....	xiv
BAB 1 PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	3
1.6 Luaran yang Diharapkan	3
1.7 Sistematika Penulisan	4
BAB 2 TINJAUAN PUSTAKA	5
2.1 Sistem	5
2.2 <i>Cloud Computing</i>.....	5

2.3	<i>Cloud Storage</i>	7
2.4	Keamanan Data	7
2.5	Kriptografi	7
2.6	Algoritma Kriptografi Modern	8
2.6.1	Algoritma Simetris	8
2.6.2	Algoritma Asimetris	8
2.7	Enkripsi dan Dekripsi	9
2.8	AES	9
2.8.1	Pengertian AES	9
2.8.2	Cara Kerja AES	10
2.8.3	Ekspansi Kunci AES	12
2.8.4	Proses Enkripsi AES	13
2.8.5	Proses Dekripsi AES	15
2.8.6	Metode Operasi Cipher Blok	17
2.9	RSA	19
2.9.1	Pengertian RSA	19
2.9.2	Cara Kerja RSA	19
2.10	Penelitian Terkait	21
BAB 3 METODOLOGI PENELITIAN		22
3.1	Tahapan Penelitian	22
3.1.1	Identifikasi Masalah	23
3.1.2	Studi Pustaka	23
3.1.3	Perancangan Sistem	23
3.1.4	Implementasi Sistem	26
3.1.5	Pengujian Sistem	26

3.1.6	Evaluasi	26
3.1.7	Dokumentasi	26
3.2	Perangkat Penelitian.....	27
3.3	Jadwal Penelitian	28
BAB 4	PEMBAHASAN	29
4.1	Analisis Kebutuhan Sistem.....	29
4.1.1	Flowchart Sistem	31
4.2	Penerapan Algoritma AES (<i>Advanced Encryption Standard</i>).....	33
4.2.1	Ekspansi Kunci AES.....	33
4.2.2	Enkripsi File dengan AES	36
4.2.3	Dekripsi File dengan AES	41
4.3	Penerapan Algoritma RSA (<i>Rivest-Shamir-Addleman</i>)	47
4.3.1	Proses enkripsi kunci AES dengan RSA	47
4.4	Penerapan <i>Cloud Storage</i>	50
4.5	Perancangan Sistem.....	51
4.5.1	Use Case Diagram.....	51
4.5.2	Activity Diagram.....	53
4.5.3	Perancangan <i>User Interface</i> Sistem.....	58
4.6	Implementasi Sistem.....	60
4.7	Pengujian Sistem.....	65
4.7.1	Pengujian Fungsionalitas Sistem (<i>Blackbox Testing</i>)	65
4.7.2	Pengujian Waktu, Ukuran dan Integritas file	66
4.8	Evaluasi Sistem	70
Bab 5	PENUTUP.....	72
5.1	Kesimpulan	72

5.2	Saran	73
	DAFTAR PUSTAKA.....	74
	RIWAYAT HIDUP	
	LAMPIRAN	

DAFTAR TABEL

Tabel 2. 2 Jumlah Putaran	11
Tabel 2. 1 Tabel RCon	13
Tabel 3. 1 Jadwal Penelitian	27
Tabel 4. 1 Karakter ke ASCII.....	49
Tabel 4. 2 Enkripsi RSA	49
Tabel 4. 3 Dekripsi RSA.....	49
Tabel 4. 4 ASCII ke Karakter	50
Tabel 4. 5 Pengujian dengan Blackbox	65
Tabel 4. 6 Pengujian Enkripsi dan Dekripsi	66
Tabel 4. 7 Pengujian Waktu <i>Upload</i> Google Drive	67
Tabel 4. 8 Pengujian Waktu <i>Upload</i> Dropbox	68

DAFTAR GAMBAR

Gambar 2. 1 Proses Enkripsi dan Dekripsi	9
Gambar 2. 2 Cara Kerja AES	11
Gambar 2. 3 Proses Ekspansi Kunci.....	12
Gambar 2. 4 Operasi addRoundkey.....	13
Gambar 2. 5 Tabel S-box.....	14
Gambar 2. 6 Proses SubBytes.....	14
Gambar 2. 7 Proses ShiftRows	15
Gambar 2. 8 Pross MixColumns	15
Gambar 2. 9 Tabel Inverse S-box.....	16
Gambar 2. 10 Skema Cipher Blok.....	17
Gambar 2. 11 Proses Enkripsi AES-CBC.....	17
Gambar 2. 12 Proses Dekripsi AES-CBC	18
Gambar 3. 1 Kerangka Pikir	22
Gambar 3. 2 Alur Proses Enkripsi	24
gambar 3. 3 Proses Dekripsi	25
Gambar 4. 1 Flowchart Sistem.....	31
Gambar 4. 2 Proses AES.....	33
Gambar 4. 4 Enkripsi AES-CBC	36
Gambar 4. 5 Alur Enkripsi Pada Sistem.....	37
Gambar 4. 6 Dekripsi AES-CBC.....	41
Gambar 4. 7 Alur Dekripsi Pada Sistem.....	42
Gambar 4. 8 Penerapan Cloud Storage	50
Gambar 4. 9 Use Case Diagram Sistem	52
Gambar 4. 10 Activity Diagram Login.....	53
Gambar 4. 11 Activity Diagram Enkripsi	54
Gambar 4. 12 Activity Diagram Dekripsi	56

Gambar 4. 13 Activity Diagram Daftar File	57
Gambar 4. 14 Tampilan Awal	58
Gambar 4. 15 Tampilan Pilih Cloud Storage	58
Gambar 4. 16 Tampilan Upload File.....	59
Gambar 4. 17 Tampilan Daftar File.....	59
Gambar 4. 18 Tampilan Dekripsi File	60
Gambar 4. 19 Halaman Index	60
Gambar 4. 20 Halaman Pilih Cloud Storage	61
Gambar 4. 21 Login Google Drive	61
Gambar 4. 22 Login Dropbox.....	62
Gambar 4. 23 Halaman Upload Google Drive	63
Gambar 4. 24 Halaman Upload Dropbox	63
Gambar 4. 25 Halaman Daftar File.....	64
Gambar 4. 26 Halaman Dekrip File.....	64
Gambar 4. 27 File Asli Sebelum Enkripsi.....	69
Gambar 4. 28 File Terenkripsi di Cloud.....	69
Gambar 4. 29 File Hasil Dekripsi	69