



**IMPLEMENTASI KEAMANAN *FILE* PADA APLIKASI PENYIMPANAN
BERBASIS *CLOUD COMPUTING* DENGAN ALGORITMA *ADVANCED
ENCRYPTION STANDARD (AES)* DAN KOMPRESI *LEMPER ZIV WELCH
(LZW)***

SKRIPSI

DWI SETYO WIRATOMO

1810511124

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2022



**IMPLEMENTASI KEAMANAN *FILE* PADA APLIKASI PENYIMPANAN
BERBASIS *CLOUD COMPUTING* DENGAN ALGORITMA *ADVANCED
ENCRYPTION STANDARD (AES)* DAN KOMPRESI *LEMPER ZIV WELCH
(LZW)***

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana
Komputer**

DWI SETYO WIRATOMO

1810511124

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2022

PERNYATAAN ORISINALITAS

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

Nama : Dwi Setyo Wiratomo

NIM : 1810511124

Tanggal : 27 Juni 2022

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

Jakarta, 27 Juni 2022

Yang Menyatakan



(Dwi Setyo Wiratomo)

PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertandatangan di bawah ini:

Nama : Dwi Setyo Wiratomo

NIM : 1810511124

Fakultas : Ilmu Komputer

Program Studi : S1 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:

IMPLEMENTASI KEAMANAN *FILE* PADA APLIKASI PENYIMPANAN BERBASIS *CLOUD COMPUTING* DENGAN ALGORITMA *ADVANCED ENCRYPTION STANDARD (AES)* DAN KOMPRESI *LEMPER ZIV WELCH (LZW)*

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 kata (basis data), 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 : 27 Juni 2022

Yang Menyatakan,



(Dwi Setyo Wiratomo)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut:

Nama : Dwi Setyo Wiratomo
NIM : 1810511124
Program Studi : S1 Informatika
Judul : Implementasi Keamanan *File* Pada Aplikasi Penyimpanan Berbasis *Cloud Computing* Dengan Algoritma *Advanced Encryption Standard* (AES) dan Kompresi *Lempel Ziv Welch* (LZW)

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian dari persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S-1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Henki Bavu Seta, S.Kom., M.TI.

Penguji 1



Noor Falih, S.Kom., M.T.

Penguji 2



Bavu Hananto, S.Kom., M.Kom.

Pembimbing 1



I Wawan Widi P, S.Kom., M.TI.

Pembimbing 2



Dr. Ernawati, M.Kom.

Dekan Fakultas Ilmu Komputer



Desta Sandva Prasvita, S.Kom., M.Kom.

Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Persetujuan : 19 Juli 2022



**IMPLEMENTASI KEAMANAN *FILE* PADA APLIKASI PENYIMPANAN
BERBASIS *CLOUD COMPUTING* DENGAN ALGORITMA *ADVANCED
ENCRYPTION STANDARD (AES)* DAN KOMPRESI *LEMPER ZIV WELCH
(LZW)***

Dwi Setyo Wiratomo

ABSTRAK

Data *file* merupakan data yang digunakan tiap perusahaan, organisasi, maupun perseorangan. Apalagi data penting yang tersimpan dalam database. Supaya data itu bisa diakses fleksibel, maka bisa disimpan dalam *cloud storage*. Tetapi keamanan dalam *cloud storage* belum cukup untuk menghindari kebocoran data yang tersimpan dalam *cloud storage*. Dengan menggunakan Kriptografi, keamanan data yang tersimpan dalam *cloud storage* akan menjadi berlapis dan tidak mudah untuk diambil maupun dirusak oleh penyusup. Walaupun sangat mudah diakses, maka harus disiapkan juga untuk keamanan data dari pengguna *cloud*. Setiap layanan *cloud* harus menyediakan keamanan data yang aman untuk penggunanya supaya menghindari penyusup untuk mengambil dan merusak data pengguna *cloud*. *Cloud Storage* merupakan bagian dari sistem *cloud computing* yang menyediakan media penyimpanan yang dapat diakses hanya dengan memerlukan jaringan internet. Ada beberapa jenis media penyimpanan yang berkembang salah satunya adalah media penyimpanan berbasis *cloud*. Keamanan data merupakan hal yang penting dalam layanan *cloud*. Salah satunya adalah media penyimpanan yang bisa di akses dalam keadaan apapun dan dimanapun. Teknik Kriptografi adalah salah satu cara untuk mengamankan data yang tersimpan dalam layanan *cloud*. Salah satu teknik kriptografi yang digunakan adalah algoritma *Advanced Encryption Standard (AES)* yang akan menghasilkan enkripsi dan dekripsi data *file* tanpa merubah isi dari *file* tersebut serta melakukan kompresi *file* menggunakan algoritma *Lempel Ziv Welch (LZW)* untuk menurunkan ukuran *file* dan mempercepat pengiriman *file* ke *cloud storage*.

Kata kunci : kriptografi, *cloud computing*, *cloud storage*, Algoritma *Advanced Encryption Standard (AES)*, *Lempel Ziv Welch (LZW)*.

**IMPLEMENTASI KEAMANAN *FILE* PADA APLIKASI PENYIMPANAN
BERBASIS *CLOUD COMPUTING* DENGAN ALGORITMA *ADVANCED
ENCRYPTION STANDARD* (AES) DAN KOMPRESI *LEMPER ZIV WELCH*
(LZW)**

Dwi Setyo Wiratomo

ABSTRACT

Data *files* are data used by every company, organization, or individual. Moreover, important data is stored in the database. So that the data can be accessed flexibly, it can be stored in cloud storage. But security in cloud storage is not enough to avoid leaking data stored in cloud storage. By using Cryptography, the security of data stored in cloud storage will be layered and not easily retrieved or damaged by intruders. Although it is very easy to access, it must also be prepared for data security from cloud users. Every cloud service must provide secure data security for its users in order to avoid intruders to retrieve and destroy cloud user data. Cloud Storage is part of a cloud computing system that provides storage media that can be accessed only by requiring an internet network. There are several types of storage media that are developing, one of which is cloud-based storage media. Data security is important in cloud services. One of them is storage media that can be accessed under any circumstances and anywhere. Cryptographic techniques are one way to secure data stored in cloud services. One of the cryptographic techniques used is the Advanced Encryption Standard (AES) algorithm which will result in encryption and decryption of *file* data without changing the contents of the *file* and compressing *files* using the Lempel Ziv Welch (LZW) algorithm to reduce *file* size and speed up *file* delivery to the cloud storage.

Keyword : cryptography, cloud computing, cloud storage, Advanced Encryption Standard (AES) Algorithm, Lempel Ziv Welch (LZW).

KATA PENGANTAR

Puji dan syukur penulis panjatkan atas berkat, rahmat dan karunia-Nya kepada Allah SWT, penulis dapat menyelesaikan Tugas Akhir/skripsi yang berjudul **“Implementasi Keamanan *File* Pada Aplikasi Penyimpanan Berbasis Cloud Computing Dengan Algoritma Advanced Encryption Standard (AES) dan Kompresi Lempel Ziv Welch (LZW)”** dengan baik.

Dalam penyelesaian tugas akhir ini, penulis tidak lupa mengucapkan terima kasih kepada pihak-pihak yang telah memberikan dukungan dan masukan kepada penulis, serta membantu penulis dalam merealisasikan tugas akhir ini, pihak-pihak tersebut adalah:

1. Kedua orang tua penulis beserta keluarga yang selalu memberi dukungan dan doa sehingga dapat menyelesaikan proposal ini.
2. Bapak Bayu Hananto, S.Kom., M.Kom. dan Bapak I Wayan Widi P, S.Kom., MTI., selaku dosen pembimbing yang telah memberikan saran dan masukan yang sangat bermanfaat.
3. Bapak/Ibu dosen Informatika Universitas Pembangunan Nasional Veteran Jakarta, terima kasih atas ilmu-ilmu yang selama ini sudah diajarkan.
4. Kepada teman saya Hanif, Ilmi, Rheina dan teman-teman terdekat saya yang tiada henti memberikan dukungan dan membantu dalam setiap proses penulisan tugas akhir/skripsi.
5. Seluruh pihak yang terlibat dalam kelancaran pembuatan tugas akhir ini dan yang belum disebutkan di atas, penulis ucapkan terima kasih.

Akhir kata, semoga tugas akhir/skripsi ini dapat bermanfaat bagi para pembacanya.

Jakarta, 27 Juni 2022

Penulis



Dwi Setyo Wiratomo

DAFTAR ISI

PERNYATAAN ORISINALITAS	i
PERNYATAAN PERSETUJUAN PUBLIKASI	ii
LEMBAR PENGESAHAN	iii
ABSTRAK	iv
ABSTRACT	v
KATA PENGANTAR	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan dan Manfaat Penelitian.....	2
1.4 Ruang Lingkup.....	2
1.5 Luaran Yang Diharapkan	2
1.6 Sistematika Penulisan	3
BAB 2 LANDASAN TEORI	4
2.1 Cloud Computing	4
2.1.1 Karakteristik Cloud	7
2.1.2 Model Penerapan Cloud	7
2.1.3 <i>Cloud storage</i>	8
2.2 Kriptografi	9
2.2.1 Tujuan Kriptografi	10
2.2.2 Jenis Algoritma Kriptografi.....	10
2.3 Advanced Encryption Standard (AES)	11
2.4 Algoritma Kompresi Lempel-ziv-welch (LZW)	12
2.5 Konsep Dasar <i>Website</i>	13
2.4.1 PHP	13
2.4.2 HTML.....	13
2.4.3 CSS.....	14
2.4.4 Javascript.....	14

2.4.5	<i>Database</i>	14
2.5	Penelitian Sejenis	14
BAB 3 METODE PENELITIAN		18
3.1	Kerangka Pikir	18
3.1.1	Identifikasi Masalah	18
3.1.2	Studi Literatur	19
3.1.3	Perancangan Aplikasi	19
3.1.4	Implementasi Aplikasi	20
3.1.5	Pengujian Aplikasi	20
3.1.6	Dokumentasi	21
3.2	Perangkat Penelitian	21
3.3	Jadwal Penelitian	21
BAB 4 HASIL DAN PEMBAHASAN		23
4.1	Analisis Sistem	23
4.2	Analisis Proses Perhitungan Metode AES dan LZW	24
4.2.1	Perhitungan Advanced Encryption Standard (AES)	24
4.2.2	Perhitungan Lempel-Ziv-Welch (LZW)	33
4.3	Perancangan Aplikasi	36
4.3.1	<i>Flowchart</i> Aplikasi	37
4.3.2	Use Case Diagram Aplikasi	41
4.3.2.1	Use Case Diagram <i>User</i>	42
4.3.3	Activity Diagram	43
4.3.4	Sequence Diagram Aplikasi	48
4.4	Tampilan Desain Aplikasi	55
4.4.1	Desain Aplikasi Admin	55
4.4.2	Desain Aplikasi <i>User</i>	57
4.5	Integrasi Penyimpanan <i>cloud storage</i>	59
4.5.1	Integrasi dari AWS	59
4.5.2	Integrasi ke Laravel	63
4.6	Pengujian	64
4.6.1	Pengujian Ukuran <i>file</i>	64
4.6.2	Pengujian Waktu Penyimpanan <i>file</i>	65
4.6.3	Pengujian Nilai Checksum <i>file</i>	66
BAB 5 PENUTUP		72

5.1	Kesimpulan.....	72
5.2	Saran	72
	DAFTAR PUSTAKA	74
	DAFTAR RIWAYAT HIDUP	76
	LAMPIRAN.....	77

DAFTAR GAMBAR

Gambar 2. 1 Konsep Komputasi Awan (Herwanto, Purbo, & Aziz, 2020)	4
Gambar 2. 2 Perbedaan IaaS, PaaS, dan SaaS (Intermedia, 2020).....	6
Gambar 2. 3 Alur Kerja AES-128 (Mirsyah, Aksara, & Sajuah, 2019).....	11
Gambar 3. 1 Flowchart Tahapan Penelitian	18
Gambar 3. 2 Flowchart Mekanisme Program.....	20
Gambar 4. 1. Matriks <i>hexa</i> pada <i>file</i> dan kunci serta <i>chipertext</i>	25
Gambar 4. 2. Kolom matriks <i>chiperkey</i> melakukan proses <i>rotword</i>	25
Gambar 4. 3. Kolom <i>rotword</i> melakukan substitusi dengan S-Box.....	26
Gambar 4. 4. Perhitungan matriks <i>key schedule</i>	26
Gambar 4. 5. Proses <i>AddRoundKey</i>	29
Gambar 4. 6. Proses substitusi matriks <i>AddRoundKey</i> dengan S-Box.....	30
Gambar 4. 7. Proses <i>ShiftRows</i> dari matriks <i>SubBytes</i>	31
Gambar 4. 8. Proses <i>MixColumns</i> dari matriks <i>shiftrows</i> dengan matriks state..	31
Gambar 4. 9 Flowchart Aplikasi	37
Gambar 4. 10 Diagram Alir upload <i>file</i>	38
Gambar 4. 11 Diagram Alir download <i>file</i>	40
Gambar 4. 12 Use Case Diagram Admin	41
Gambar 4. 13 Use Case Diagram User.....	42
Gambar 4. 14 Activity Diagram Admin Login.....	43
Gambar 4. 15 Activity Diagram Admin Register User	44
Gambar 4. 16 Activity Diagram Admin Delete User	45
Gambar 4. 17 Activity Diagram User Login	46
Gambar 4. 18 Activity Diagram User upload <i>file</i>	47
Gambar 4. 19 Activity Diagram user download <i>file</i>	48
Gambar 4. 20 Sequence Diagram Admin Login	49
Gambar 4. 21 Sequence Diagram Admin Register User	50
Gambar 4. 22 Sequence Diagram Admin Delete User	51
Gambar 4. 23 Sequence Diagram User Login.....	52
Gambar 4. 24 Sequence Diagram User upload <i>file</i>	53
Gambar 4. 25 Sequence Diagram User download <i>file</i>	54
Gambar 4. 26 Desain Aplikasi Admin Login	55
Gambar 4. 27 Desain Aplikasi Register User.....	55
Gambar 4. 28 Desain Form Register User.....	56
Gambar 4. 29 Desain Aplikasi Delete User.....	57
Gambar 4. 30 Desain Aplikasi User Login	57
Gambar 4. 31 Desain Aplikasi upload <i>file</i>	58
Gambar 4. 32 Desain Form upload <i>file</i>	58
Gambar 4. 33 Desain Aplikasi download <i>file</i>	59
Gambar 4. 34 Alir Pembuatan IAM user.....	60
Gambar 4. 35 Policy Akun IAM	60
Gambar 4. 36 Detail Info IAM user	61

Gambar 4. 37	Pembuatan AWS S3 bucket.....	62
Gambar 4. 38	Detail Info AWS S3.....	62
Gambar 4. 39	Konfigurasi <i>filesystem.php</i>	63
Gambar 4. 40	Konfigurasi <i>.env file</i>	63
Gambar 4. 41	Tampilan Awal Md5Checker	67
Gambar 4. 42	Tampilan Nilai Checksum	68
Gambar 4. 43	Perbandingan Checksum sama	68
Gambar 4. 44	Perbandingan Checksum Berbeda	69
Gambar 4. 45	Perbandingan Checksum Asli Berhasil	69

DAFTAR TABEL

Table 2. 1 Penelitian Sejenis	15
Table 3. 1 Jadwal Penelitian.....	22
Table 4. 1. Round Constant (Rcon).....	26
Table 4. 2 <i>key schedule</i>	27
Table 4. 3 Tabel S-Box.....	30
Table 4. 4 Hasil Perhitungan Enkripsi AES	32
Table 4. 5 Tahapan Kompresi LZW	33
Table 4. 6 Hasil Kompresi LZW	34
Table 4. 7 Pengujian <i>file</i> Format .doc.....	64
Table 4. 8 Pengujian <i>file</i> Format .pdf.....	65
Table 4. 9 Pengujian <i>file</i> Format .doc.....	65
Table 4. 10 Pengujian <i>file</i> Format .pdf.....	66
Table 4. 11 Hasil checksum format .doc	70
Table 4. 12 Hasil checksum format .pdf	70