IMPLEMENTASI ENKRIPSI AES-256 UNTUK PROTEKSI FILE DI CLOUD STORAGE

Mariana Dewi Santi Lou[1], Edwardy Tkela[2], Servasius Tenis[3], Fadelio Putra Knaofmone[4], Siprianus Septian Manek[5]
dewylou049@gmail.com[1], edwarditkela@gmail.com[2], servasiustenis9@gmail.com[3], fadelsky991@gmail.com[4], septian16@mhs.if.its.ac.id[5]
Universitas Negeri Timor

ABSTRAK

Pertumbuhan eksponensial layanan cloud storage telah membawa kemudahan besar bagi pengguna dalam menyimpan, berbagi, dan mengakses data secara daring. Namun, seiring dengan kemudahan tersebut, muncul pula tantangan besar terkait keamanan data. Data yang tersimpan di cloud sering kali berada di bawah pengelolaan penyedia layanan, sehingga menimbulkan kekhawatiran terkait privasi dan kerahasiaan. Oleh karena itu, metode enkripsi yang kuat dan efisien menjadi sangat penting. Artikel ini membahas implementasi algoritma Advanced Encryption Standard (AES) dengan panjang kunci 256-bit (AES-256) sebagai solusi untuk melindungi file sebelum diunggah ke cloud storage. Melalui eksperimen menggunakan file dengan ukuran bervariasi, dilakukan evaluasi terhadap kinerja enkripsi serta dampaknya terhadap waktu proses dan integritas data. Hasil pengujian menunjukkan bahwa AES-256 memberikan tingkat keamanan tinggi dengan performa yang masih dapat diterima untuk berbagai ukuran file.

Kata Kunci: Enkripsi, AES-256, Cloud Storage, Keamanan Informasi, Kriptografi Simetris.

ABSTRACT

The exponential growth of cloud storage services has brought significant convenience for users in storing, sharing, and accessing data online. However, alongside this convenience comes a major challenge in ensuring data security. Data stored in the cloud is often managed by third-party service providers, raising concerns about privacy and confidentiality. Therefore, strong and efficient encryption methods are crucial. This paper discusses the implementation of the Advanced Encryption Standard (AES) algorithm with a 256-bit key (AES-256) as a solution to protect files before uploading them to cloud storage. Through experiments using files of varying sizes, the study evaluates encryption performance in terms of processing time and data integrity. The results show that AES-256 provides a high level of security with acceptable performance across different file sizes.

Keywords*: Encryption, AES-256, Cloud Storage, Data Security, Symmetric Cryptography.*

PENDAHULUAN

Cloud storage kini telah menjadi bagian tak terpisahkan dari aktivitas digital masyarakat modern. Layanan seperti Google Drive, Dropbox, iCloud, dan OneDrive memungkinkan pengguna untuk menyimpan data secara daring dan mengaksesnya kapan saja dan dari mana saja. Namun, meskipun menawarkan fleksibilitas dan efisiensi, penyimpanan data di cloud juga membawa risiko besar terhadap keamanan dan privasi.

Data sensitif seperti dokumen legal, informasi keuangan, hingga catatan medis seringkali disimpan dalam cloud. Apabila data tersebut tidak dilindungi dengan baik, maka dapat menjadi sasaran empuk bagi peretas (hacker), penyalahgunaan oleh pihak ketiga, atau bahkan eksploitasi internal dari penyedia layanan cloud itu sendiri. Dalam konteks ini, enkripsi data menjadi solusi utama yang mampu memberikan perlindungan menyeluruh terhadap konten file yang disimpan di cloud.

Salah satu algoritma enkripsi yang diakui secara global karena kekuatannya adalah Advanced Encryption Standard (AES), khususnya varian dengan panjang kunci 256-bit

(AES-256). AES-256 merupakan algoritma kriptografi simetris yang digunakan secara luas oleh institusi pemerintahan, militer, dan industri untuk melindungi data penting.

Artikel ini bertujuan untuk mengeksplorasi implementasi enkripsi AES-256 pada sistem penyimpanan cloud dengan pendekatan jika data berhasil diakses oleh pihak tidak di server cloud, mereka tetap tidak mengenkripsi dapat membaca isi file tanpa kunci enkripsi sesuai.

TINJAUAN PUSTAKA

A. Advanced Encryption Standard (AES)

AES adalah algoritma blok kriptografi simetris yang dikembangkan untuk menggantikan Data Encryption Standard (DES). AES menggunakan panjang blok tetap 128-bit, tetapi mendukung tiga panjang kunci: 128, 192, dan 256-bit. AES-256 adalah varian terkuat yang digunakan saat ini, terdiri dari 14 putaran enkripsi dan dianggap sangat tahan terhadap serangan brute force.

B. Keamanan Cloud Storage

Penyimpanan data di cloud melibatkan transfer data melalui jaringan internet dan penyimpanan di server yang dikendalikan oleh penyedia layanan pihak ketiga. Oleh karena itu, model keamanan tradisional yang hanya bergantung pada otentikasi pengguna dan izin akses menjadi tidak cukup. Enkripsi sisi klien (client-side encryption) menawarkan perlindungan tambahan karena data sudah dalam bentuk terenkripsi sebelum dikirim ke server.

C. Client-side Encryption

Dengan pendekatan ini, proses enkripsi dan dekripsi dilakukan sepenuhnya di sisi pengguna. Kunci enkripsi tidak pernah dikirim ke penyedia layanan, sehingga sekalipun server cloud diretas, data tetap tidak bisa dibaca oleh penyerang. AES-256 sangat cocok untuk model ini karena performanya efisien dan keamanannya terbukti.

METODE PENELITIAN

A. Desain Sistem

Sistem proteksi file yang dikembangkan menggunakan skema client-side encryption. Proses enkripsi dilakukan pada sisi pengguna sebelum file dikirim ke cloud storage. Berikut tahapan utama:

1. Input File: Pengguna memilih file dari perangkat lokal.
2. Proses Enkripsi: File dienkripsi menggunakan algoritma AES-256 dengan kunci dan IV (Initialization Vector) acak.
3. Upload File: File yang telah terenkripsi dikirim ke layanan cloud (simulasi menggunakan folder lokal/Drive API).
4. Download dan Dekripsi: File yang diunduh dari cloud hanya bisa didekripsi menggunakan kunci yang sama dengan saat enkripsi.

B. Konfigurasi Implementasi

- Bahasa Pemrograman: Python 3.10
- Pustaka Kriptografi: pycryptodome
- Mode Enkripsi: AES-256 dengan mode CBC (Cipher Block Chaining)
- Sumber IV: Random 16-byte generator
- Penyimpanan IV dan Metadata: Disimpan bersama file dalam format JSON atau header terpisah
- Ukuran File Uji: 1 KB, 1 MB, 10 MB, 100 MB

C. Parameter Evaluasi

Untuk mengevaluasi kinerja sistem, digunakan beberapa metrik:

- Waktu Enkripsi dan Dekripsi: Diukur dalam detik
- Integritas File: Dicek menggunakan hash (SHA-256) sebelum dan sesudah enkripsi/dekripsi
- Kapasitas Penyimpanan: Mengukur penambahan ukuran akibat metadata
- Keamanan: Diuji secara konseptual terhadap brute force dan kebocoran IV

HASIL DAN PEMBAHASAN

A. Kinerja Enkripsi

Tabel berikut menunjukkan hasil pengujian waktu enkripsi untuk berbagai ukuran file:

Ukuran File	Waktu Enkripsi (detik)	Waktu Dekripsi (detik)
1 KB	**0.01**	**0.01**
1 MB	**0.26**	**0.24**
10 MB	**2.7**	**2.6**
100 MB	**25.1**	**24.9**

Analisis: Waktu proses meningkat secara linier terhadap ukuran file. Untuk file ukuran <10 MB, waktu enkripsi berada di bawah 3 detik, yang dianggap sangat efisien.

B. Keamanan

- **Brute Force**: AES-256 memiliki 2^{256} kemungkinan kunci, yang membuat brute force secara praktis mustahil dilakukan dalam waktu manusiawi dengan teknologi saat ini.
- **IV Acak**: IV baru dibuat untuk setiap proses enkripsi, sehingga meskipun file yang sama dienkripsi dua kali, hasil cipher akan berbeda.
- **Hash Integritas**: Tidak ditemukan perubahan pada file setelah proses dekripsi (hash SHA-256 cocok 100%).

C. Penyimpanan Tambahan

Penggunaan metadata (IV + ukuran blok) menyebabkan penambahan file sekitar 16–32 byte, tergantung struktur penyimpanan. Ini masih tergolong sangat ringan dan tidak berpengaruh signifikan terhadap efisiensi penyimpanan.

KESIMPULAN

Implementasi enkripsi AES-256 terbukti efektif dalam menjaga keamanan file yang disimpan di cloud storage. Dengan skema **client-side encryption**, file telah diamankan sebelum meninggalkan perangkat pengguna. Pengujian menunjukkan bahwa waktu enkripsi tergolong cepat, bahkan untuk file berukuran besar, dan file terenkripsi tetap menjaga integritas data sepenuhnya.

Beberapa poin utama yang dapat disimpulkan dari penelitian ini:

- **AES-256 memberikan keamanan tinggi** yang tahan terhadap brute force.
- **IV acak** mencegah analisis pola oleh penyerang.
- **Performa efisien** untuk file kecil hingga besar (hingga 100 MB).
- **Dekripsi hanya dapat dilakukan dengan kunci yang sama**, menjamin kerahasiaan penuh.

Rekomendasi untuk pengembangan selanjutnya adalah integrasi sistem manajemen kunci (key management system) berbasis biometrik atau multi-faktor otentikasi, serta penerapan dalam lingkungan mobile untuk pengguna akhir.

DAFTAR PUSTAKA

Bowers, K. D., Juels, A., & Oprea, A. (2009). HAIL: A High-Availability and Integrity Layer for Cloud Storage. Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 187–198.

Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer-Verlag.

Gruschka, N., & Iacono, L. L. (2009). Vulnerable Cloud: SOAP Message Security Validation Revisited. IEEE International Conference on Web Services (ICWS), 625–631.

Li, H., Dai, Y., Tian, L., & Yang, H. (2009). Identity-Based Authentication for Cloud Computing. CloudCom 2009: Cloud Computing, 157–166.

Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings. Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks, 89–106.

Liu, F., Tong, J., Mao, J., Bohn, R. B., Messina, J. V., Badger, L., & Leaf, D. (2011). NIST Cloud Computing Reference Architecture. NIST Special Publication 500-292.

National Institute of Standards and Technology (NIST). (2001). Specification for the Advanced Encryption Standard (AES). FIPS Publication 197.

Singh, A., & Shrivastava, K. (2012). Overview of Attacks on Cloud Computing. International Journal of Engineering and Innovative Technology (IJEIT), 1(4), 321–323.

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592.