Perancangan Infrastruktur Enkripsi End to End pada Aplikasi Penyimpanan File Berbasis Website

Ni Putu Sri Agnita Samyami Wiraputri[a1], Cokorda Pramartha[a2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Udayana, Bali
Jln. Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, 08261, Bali, Indonesia
[1]sriagnita111@student.unud.ac.id
[2]cokorda@unud.ac.id (Corresponding Author)

Abstract

The rapid evolution of information and communication technology has revolutionized how we communicate and share information. Despite the numerous benefits, these advancements have introduced challenges, particularly concerning data security and privacy. Issues like data interception and escalating file sizes necessitate effective solutions. Cryptography emerges as a pivotal tool in addressing these concerns, offering a means to bolster data security while mitigating file size. This field encompasses the science and techniques of information security, converting data into unreadable ciphertext through encryption algorithms and keys. Encryption, particularly end-to-end encryption, plays a crucial role in maintaining confidentiality during file storage and exchange. The RSA cryptographic algorithm exemplifies an asymmetric approach, utilizing distinct keys for encryption and decryption. Public and private keys ensure secure communication, with the public key encrypting messages and the private key decrypting them. This widely adopted algorithm fortifies data security across various applications. Complementing this, the Caesar Cipher, a simple substitution cryptographic technique, adds an additional layer to the encryption process. By replacing each character with another at a specified shift in alphabetical order, the Caesar Cipher offers a basic yet effective safeguard. Combining the robust RSA algorithm with the simplicity of Caesar Cipher enhances file storage security. Employing Caesar Cipher as the initial step in encryption, followed by RSA to encrypt its output, ensures double-layered encryption. This dual process guarantees that only the corresponding private key can decrypt the file, reinforcing the overall security of data storage and exchange.

Keywords: *Algorima RSA, Algoritma Caesar Cipher, Keamanan Jaringan.*

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah mengalami kemajuan dan mengubah cara kita berkomunikasi maupun bertukar informasi. Teknologi informasi juga berpengaruh negatif, salah satu dampak negatifnya yaitu penyadapan data dan ukuran file semakin meningkat. Masalah keamanan dan privasi adalah salah satu aspek penting dari data, pesan dan informasi. Data Dapat berupa dokumen digital seperti word, pdf, excel, dan lain-lain. Jika ada pihak yang tak berkepentingan mengakses data tersebut, maka dikhawatirkan akan terjadi hal-hal yang tidak diinginkan. Oleh karena itu diperlukan sebuah aplikasi yang dapat menjamin keamanan dokumen dan mengurangi ukuran file agar lebih mudah disimpan di komputer [1].

Salah satu cara pengamanan pada penyimpanan file yaitu dengan ilmu kriptografi. Kriptografi adalah ilmu dan praktik keamanan informasi yang mecakup teknik untuk mengubah teks atau data menjadi bentuk yang tidak dapat dibaca yang disebut chipertext dengan menggunakan algoritma enkripsi dan kunci enkripsi. Tujuan utama enkripsi dalam keamanan yaitu untuk menjaga kerahasiaan informasi agar pihak yang berwenang saja yang dapat membaca atau mengaksesnya. Salah satu jenis enkripsi yang dapat digunakan untuk pengamanan pada penyimpanan file yaitu enkripsi end to end. Enkripsi end to end adalah jenis enkripsi yang dapat memastikan bahwa pesan dienkripsi pleh pengirim dan hanya dapat didekripsi oleh penerima yang dituju [2].

Algoritma kriptografi RSA merupakan algoritma yang termasuk dalam kategori algoritma asimetris. Juga disebut algorithm kunci publik. Mereka disebut algoritma asimetris karena algoritma yang digunakan dalam proses enkripsi dan dekripsi berbeda. Pria. Dalam kriptografi, Caesar cipher atau slide cipher, Caesar code atau Caesar shift adalah salah satu teknik kriptografi yang paling sederhana dan terkenal. Kode ini berisi kode pengganti yang menggantikan setiap karakter dalam plaintext dengan karakter lain dengan perbedaan posisi tertentu dalam alfabet. Dalam sandi Caesar, setiap huruf diganti dengan huruf ketiga berikutnya dalam urutan abjad yang sama [3].

Berdasarkan penelitian yang dilakukan Wahyu Pramusinto, Nugroho Wizaksono, Ari Saputro dengan judul Aplikasi Pengamanan File Berbasis Web Dengan Metode Kriptografi Aes 192, Rc4 Dan Metode Kompresi Huffman didapatkan hasil akhir dengan aplikasi keamanan file dokumen ini, Anda dapat menjaga kerahasiaan file penting Anda karena disimpan di server dan hanya dapat diakses melalui aplikasi ini. Metode algoritmik AES dan RC4 menghasilkan file ciphertext yang lebih besar dari plaintext. Menggunakan algoritma kompresi Huffman menghasilkan file yang lebih kecil. Kesimpulan lainnya adalah waktu yang dibutuhkan untuk menyelesaikan proses enkripsi dan dekripsi berbanding lurus dengan ukuran file yang sedang diproses. Juga, waktu tergantung pada spesifikasi perangkat keras dari perangkat yang digunakan.

Berdasarkan penelitian yang dilakukan Bimantoro dengan judul Enkripsi Data Menggunakan Rsa & Aes Pada Aplikasi Instant Messaging Berbasis Mobile didapatkan hasil akhir dengan kombinasi dua metode enkripsi memberikan kinerja yang baik, dapat memproses volume data yang besar dalam hitungan milidetik. Kinerja proses enkripsi dan dekripsi ini mengikuti spesifikasi perangkat yang digunakan, semakin baik spesifikasinya maka semakin baik kinerjanya. Dari segi keamanan, kombinasi ini sangat memadai, misalnya jika kunci publik pengguna atau pesan terkirim berhasil diretas, pihak ketiga tetap tidak dapat mengirim atau membaca pesan.

Berdasarkan latar belakang di atas, penulis ingin merancang sistem keamanan informasi pengguna dalam penyimpanan file dengan algoritma RSA dan Caesar Cipher. Penulis menggunakan metode algoritma tersebut untuk menilai sejauh mana dapat digunakan untuk mengamankan data. Dengan penggunaan metode tersebut, diharapkan dapat membantu pengguna aplikasi pesan teks untuk memastikan keamanan data dan semua informasi yang bersifat rahasia.

2. Metode Penelitian

Penelitian ini menggunakan model pengembangan sistem Waterfall. Model Waterfall adalah model pengembangan sistem yang bersifat sekuensial, di mana setiap tahap harus diselesaikan terlebih dahulu sebelum melanjutkan ke tahap berikutnya.

Tahapan dalam Model Waterfall:

1. Analisis Kebutuhan: Pada tahap ini, peneliti akan menganalisis kebutuhan pengguna dan sistem untuk menentukan fitur-fitur yang akan dibangun dalam aplikasi penyimpanan file berbasis website.

2. Perancangan Sistem: Pada tahap ini, peneliti akan merancang arsitektur sistem, database, dan antarmuka pengguna.

3. Implementasi Sistem: Pada tahap ini, peneliti akan membangun aplikasi penyimpanan file berbasis website sesuai dengan desain yang telah dibuat.

4. Pengujian Sistem: Pada tahap ini, peneliti akan menguji aplikasi penyimpanan file berbasis website untuk memastikan bahwa aplikasi tersebut berfungsi dengan baik dan sesuai dengan kebutuhan pengguna.

5. Pemeliharaan Sistem: Pada tahap ini, peneliti akan melakukan pemeliharaan aplikasi penyimpanan file berbasis website untuk memperbaiki bug dan menambahkan fitur-fitur baru.

Alur Algoritma:
Berikut adalah alur algoritma enkripsi end-to-end yang akan digunakan dalam aplikasi penyimpanan file berbasis website:

1. Pengirim:
   - Memasukkan file yang ingin disimpan.
   - Memilih algoritma enkripsi (RSA atau Caesar Cipher).
   - Memasukkan kunci enkripsi.
   - Mengenkripsi file menggunakan algoritma enkripsi yang dipilih.
   - Mengunggah file terenkripsi ke server.

2. Penerima:
   - Mengunduh file terenkripsi dari server.
   - Memilih algoritma dekripsi (RSA atau Caesar Cipher).
   - Memasukkan kunci dekripsi.
   - Mendekripsi file terenkripsi menggunakan algoritma dekripsi yang dipilih.
   - Mendapatkan file asli.

3. Hasil dan Pembahasan

Penelitian ini menghasilkan sebuah aplikasi penyimpanan file berbasis website dengan enkripsi end-to-end. Aplikasi ini memungkinkan pengguna untuk menyimpan file dengan aman dan terenkripsi, sehingga hanya pengguna yang memiliki kunci dekripsi yang dapat mengakses file tersebut. Aplikasi ini menggunakan dua algoritma enkripsi, yaitu RSA dan Caesar Cipher. Algoritma RSA digunakan untuk mengenkripsi kunci dekripsi, sedangkan algoritma Caesar Cipher digunakan untuk mengenkripsi file. Aplikasi ini telah diuji coba dengan menggunakan berbagai jenis file, dan hasilnya menunjukkan bahwa aplikasi ini dapat mengenkripsi dan mendekripsi file dengan baik.

Aplikasi penyimpanan file berbasis website dengan enkripsi end-to-end ini memiliki beberapa kelebihan, yaitu:

- Keamanan file terjamin karena file dienkripsi dengan dua algoritma enkripsi yang kuat.
- Privasi pengguna terjaga karena hanya pengguna yang memiliki kunci dekripsi yang dapat mengakses file.
- Mudah digunakan karena aplikasi ini memiliki antarmuka yang sederhana dan mudah dipahami.

Namun, aplikasi ini juga memiliki beberapa kekurangan, yaitu:

- Proses enkripsi dan dekripsi membutuhkan waktu yang relatif lama, terutama untuk file yang besar.
- Pengguna harus menyimpan kunci dekripsi dengan aman, karena jika kunci dekripsi hilang, maka file yang terenkripsi tidak akan dapat diakses.

Secara keseluruhan, aplikasi penyimpanan file berbasis website dengan enkripsi end-to-end ini merupakan solusi yang baik untuk menyimpan file dengan aman dan terenkripsi.

4. Kesimpulan

Penelitian ini telah berhasil mengembangkan aplikasi penyimpanan file berbasis website dengan enkripsi end-to-end. Aplikasi ini memiliki beberapa kelebihan, seperti keamanan file terjamin, privasi pengguna terjaga, dan mudah digunakan. Namun, aplikasi ini juga memiliki beberapa

kekurangan, seperti proses enkripsi dan dekripsi membutuhkan waktu yang relatif lama, dan pengguna harus menyimpan kunci dekripsi dengan aman.

Daftar Pustaka

[1] R. D. M. K. H. Aplikasi Pengamanan File Dengan Metode Kriptografi Aes 192, "Wahyu Pramusinto, Nugroho Wizaksono, Ari Saputro," *Jurnal Bit,* Vol. 16, Pp. 47-53, 2019.

[2] R. T. K. S. Yanuar Bimantoro, "Enkripsi Data Menggunakan Rsa & Aes Pada Aplikasi Instant Messaging Berbasis Mobile," *Jurnal Teknik Informatika,* Vol. 14, Pp. 135-144, 2021.