Journal of Information Technology and Computer Science (INTECOMS)
Volume 6 Nomor 2, Desember 2023
e-ISSN : 2614-1574
p-ISSN : 2621-3249

IMPLEMENTASI ALGORITMA AES-256 DALAM PERANCANGAN APLIKASI PENGAMANAN DOKUMEN DIGITAL PERUSAHAAN BERBASIS ANDROID

IMPLEMENTATION OF AES-256 ALGORITHM IN THE DESIGN OF COMPANY-BASED DIGITAL DOCUMENT SECURITY APPLICATION

Tasya Diah Ayu Pramesthi Wardhani[1], Yuli Asriningtias[2]
[1,2]Program Studi Informatika Fakultas Sains dan Teknologi Universitas Teknologi Yogyakarta
tasyadiahayuu@gmail.com[1], yuli_asriningtias@uty.ac.id[2]

ABSTRACT

Advanced Encryption Standard (AES) is a cryptographic algorithm that can be used to secure data. The AES algorithm is a symmetric ciphertext block that can encrypt (encipher) and decrypt (decipher) information. Data collection techniques are the most strategic steps in a research. By using the correct data collection technique, the researcher will get data that meets the standards, then a data collection technique is carried out, namely, document study. This research produces an android application system for securing corporate digital documents by utilizing AES-256 as its cryptographic algorithm. The resulting application is designed using the Node js framework based on the JavaScript programming language on the backend side, while on the frontend side it uses the Kotlin programming language which was built using the Android Studio IDE. The database used in this application is MySql. The process of encrypting digital document data using the AES-256 algorithm is carried out on the backend by utilizing the library on Node js, namely the Node.js Crypto Module. Document data that has been successfully encrypted is stored in the MySql database. The resulting application uses the API as a communication intermediary between the client part and the server part. Based on the results of this study, it can be concluded that a corporate digital document security application has been created using the AES-256 algorithm. The application has managed to properly secure company digital document files in the format docx, pdf, csv/xlxs, png/jpg. Document files that have been successfully encrypted cannot be opened except by using this application based on the appropriate key and token.

Keywords: *Document Security, AES-256 Algorithm, Encryption, Decryption.*

ABSTRAK

Advanced Encryption Standard (AES) merupakan algoritma cryptographic yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Teknik pengumpulan data merupakan langkah yang paling strategis dalam sebuah penelitian. Dengan menggunakan teknik pengumpulan data yang benar maka peneliti akan mendapatkan data-data yang memenuhi standar, maka dilakukan teknik pengumpulan data yaitu, studi dokumen. Penelitian ini menghasilkan sebuah sistem aplikasi android untuk pengamanan dokumen digital perusahaan dengan memanfaatkan AES-256 sebagai algoritma kriptografinya. Aplikasi yang dihasilkan dirancang dengan menggunakan framework Node js berbasis bahasa pemrograman javascript pada sisi backendnya, sedangkan pada sisi frontendnya menggunakan bahasa pemrograman kotlin yang dibuild menggunakan IDE android studio. Database yang digunakan pada aplikasi ini adalah dengan menggunakan MySql. Proses enkripsi data dokumen digital menggunakan algoritma AES-256 dilakukan pada bagian backend dengan memanfaatkan library pada Node js yaitu yaitu Node.js Crypto Module. Data dokumen yang sudah berhasil dienkripsi, disimpan di dalam database MySql. Aplikasi yang dihasilkan menggunakan API sebagai perantara komunikasi antara bagian client dengan bagian server. Berdasarkan hasil penelitian ini dapat disimpulkan bahwa telah terciptanya aplikasi pengamanan dokumen digital perusahaan dengan menggunakan algoritma AES-256. Aplikasi tersebut telah berhasil mengamankan dengan baik file dokumen digital perusahaan yang berfomat docx, pdf, csv/xlxs, png/jpg. File dokumen yang berhasil dienkripsi berhasil tidak dapat dibuka kecuali dengan menggunakan aplikasi ini berdasarkan kunci dan token yang sesuai.

Kata Kunci: Pengamanan Dokumen, Algoritma AES-256, Enkripsi, Dekripsi.

PENDAHULUAN

Pengamanan data atau data protection merupakan salah satu hal penting untuk melindungi pesan dan informasi penting dari korupsi, kompromi atau kerugian supaya pesan dan informasi tersebut tetap aman. Banyak cara untuk mengamankan data, salah satunya adalah dengan menggunakan teknik kriptografi. Kriptografi merupakan sebuah seni untuk memanipulasi suatu pesan maupun data rahasia ke dalam bentuk yang tidak

diketahui oleh banyak orang dengan tujuan pesan atau data rahasia tersebut terlindungi dari orang yang tidak berhak mengetahuinya. Kriptografi menggunakan algoritma *Advanced Encryption Standard* (AES) memiliki ukuran blok dan kunci yang sama, yaitu 128 bit, 192 bit, dan 256 bit untuk proses enkripsi dan dekripsi. Sistem keamanan data ini dibangun untuk membantu melindungi data-data penting perusahaan, seperti data hasil laporan penelitian lapangan maupun data pribadi perusahaan. Advanced Encryption Standard (AES) merupakan algoritma cryptographic yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext; sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext.

Perusahaan adalah kegiatan yang diselenggarakan dengan peralatan atau dengan cara teratur dengan tujuan mencari keuntungan. Perusahaan juga didefinisikan sebagai organisasi berbadan hukum yang mengadakan transaksi atau usaha. Salah satu permasalahan yang sering terjadi pada suatu perusahaan yaitu, sering hilangnya data penting yang disebabkan oleh kurangnya keamanan terhadap data penting tersebut. Hilangnya data penting dapat terjadi melalui beberapa hal salah satunya yaitu berbagi file sembarangan. Penyimpanan data pada cloud melalui internet memungkinkan seseorang melakukan pencurian data di tengah pengiriman ataupun pada database.

Berdasarkan permasalahan yang ada maka diperlukan sebuah aplikasi untuk mengamankan dokumen perusahaan tersebut. Pada penelitian Aprijal Muhammad Yusup (2021) menyatakan bahwa cara kerja metode algoritma AES (*Advanced Encryption Standard*) ini untuk menjaga sebuah data yang bersifat rahasia tidak dapat diketahui oleh orang yang tidak bertanggung jawab. Oleh karena itu, peneliti ingin merancang sebuah aplikasi pengamanan dokumen perusahaan berbasis android dengan mengimplementasikan AES-256 sebagai algoritma kriptografinya.

METODE

Data yang diperoleh adalah segala sesuatu yang dapat memberikan informasi mengenai data. Data yang digunakan pada penelitian ini merupakan data sekunder yang diperoleh dari survei yang dilakukan tahun 2021 dari perusahaan keamanan siber Trend Micro yang bekerja sama dengan Ponemon Institute, Amerika Serikat yang menyatakan bahwa sebanyak 81% perusahaan di Indonesia kemungkinan bisa mengalami kebocoran data perusahaan. Data yang digunakan pada penelitian ini merupakan data sekunder berupa dokumen digital sebagai berikut :

1. Akta pendirian perusahaan
2. Nomor Pokok Wajib Pajak (NPWP)
3. Surat izin tempat usaha
4. Surat Izin Usaha Industri (SIUI)
5. Surat Keterangan Domisili Perusahaan (SKDP)
6. Tanda Daftar Perusahaan (TDP)

HASIL DAN PEMBAHASAN

Hasil

Perancangan struktur tabel penelitian ini menghasilkan sebuah sistem aplikasi android untuk pengamanan dokumen digital perusahaan dengan memanfaatkan AES-256 sebagai algoritma kriptografinya. Aplikasi yang dihasilkan dirancang dengan menggunakan framework Node js berbasis bahasa pemrograman javascript pada sisi backendnya, sedangkan pada sisi frontendnya menggunakan bahasa pemrograman kotlin yang dibuild menggunakan IDE android studio. Database yang digunakan pada aplikasi ini adalah dengan menggunakan MySql. Proses enkripsi data dokumen digital menggunakan algoritma AES-256 dilakukan pada bagian backend dengan memanfaatkan library pada Node js yaitu yaitu Node.js Crypto Module. Data dokumen yang sudah berhasil dienkripsi,

disimpan di dalam database MySql. Aplikasi yang dihasilkan menggunakan API sebagai perantara komunikasi antara bagian client dengan bagian server. Client yang dimaksud adalah pada sisi pengguna yang menggunakan aplikasi ini.

Pengguna dalam aplikasi ini adalah karyawan perusahaan di bagian eksekutif yang memiliki hak untuk mengakses dokumen-dokumen penting perusahaan. Pengguna perlu membuat akun terlebih dahulu untuk menggunakan aplikasi ini. Pada saat melakukan enkripsi, terlebih dahulu pengguna perlu menambahkan file dokumen berformat docx, pdf, csv/xlsx, atau png/jpg. Jika enkripsi berhasil maka pengguna akan mendapatkan kode token yang nantinya digunakan untuk proses mendekripsi. Token yang dihasilakan dapat berupa teks atau berupa gambar kode QR. Ada dua opsi yang bisa dilakukan pengguna untuk melakukan proses dekripsi, yaitu dengan memasukkan kode token secara langsung atau dengan memindai kode QR. Jika dekripsi berhasil, pengguna bisa langsung melihat file dokumennya atau pun mengunduh filenya agar tersimpan secara local pada memori internal smartphone.

Pembahasan

Pengujian *Blackbox* Testing

Blackbox testing adalah pengujian yang dilakukan untuk mengamati hasil input dan output dari perangkat lunak tanpa mengetahui struktur kode dari perangkat lunak. Pengujian ini dilakukan pada akhir pembuatan perangkat lunak untuk mengetahui apakah perangkat lunak dapat bekerja dengan baik. Adapun pengujian unit (black box testing) yang dilakukan pada laporan proyek profesional ini dapat dilihat pada Tabel 1.

Tabel 1. Pengujian unit (Blackbox testing)

Unit	Pengujian Sistem	Reaksi Sistem	Hasil Uji	Diuji Oleh
Daftar Akun	Mengisi semua kolom nama perusahaan, email, dan kata sandi	Akun terdaftar pada sistem	Berhasil	Karyawan
	Tidak mengisi semua kolom nama perusahaan,email, dan kata sandi	Akun tidak terdaftarpada sistem dan menampilkan pesan eror	Berhasil	Karyawan
Masuk Akun	Mengisi semua kolom email dan kata sandi	Masuk ke halaman utama	Berhasil	Karyawan
	Tidak mengisi salah satu kolom email dan kata sandi	Menampilkan pesan eror	Berhasil	Karyawan
Enkripsi File	Melakukan enkripsi file dengan mengisi semua kolom nama dokumen, dekripsi dokumen, dan menambahkan file yang akan dienkripsi	Menampilkan pemberitahuan enkripsi file berhasil	Berhasil	Karyawan
Dekripsi File	Melakukan dekripsi file dengan mengisi token yang sesuai	Menampilkan pemberitahuan dekripsi file berhasil	Berhasil	Karyawan
	Mengunduh file hasil dekripsi	Menampilkan hasil file yang berhasil	Berhasil	Karyawan

	diundu h			
	Melihat file hasil dekripsi	Mena mpilka n hasil file yang telah didekri psi	Berhasil	Karyawan
	Melakuk an enkripsi file dengan memind ai kode QR yang berusaha token	Mena mpilka n hasil pindai file berupa kode token	Berhasil	Karyawan
Detail File	Menamp ilkan detail file berupa nama dokume n, jenis dokume n, dan deskrips i dokume n	Mena mpilka n detail file	Berhasil	Karyawan
	Meneka n tombol dapatka n token	Mena mpilka n gamba r kode QR	Berhasil	Karyawan
	Menyalin kode token	Menyalin kode token berupa teks	Berhasil	Karyawan
Riwayat Enkripsi	Melihat riwayat enkripsifile	Menampilk an riwayat enkripsi file	Berhasil	Karyawan
Profil	Melihat data profil pengguna	Menampilk an profil pengguna	Berhasil	Karyawan
	Ubah profil pengguna	Menampilk an pemberitah uan ubah profil berhasil	Berhasil	Karyawan
Kirim File	Menampil kan form kirimfile	Menampil kan form kirim file	Berhasil	Karyawan
	Mengirim file dengan mengisi semua kolom nama dokumen, dekripsi dokumen, dan menambah kan file yang akan dikirim	Menampilk an pemberitah uan dokumen berhasil dikirim	Berhasil	Karyawan
Notifikasi	Melihat dokumen pada notifikasi kotak masuk	Menampilk an dokumen yang diterima dari perusahaan lain	Berhasil	Karyawan
	Mendekrip si file dokumen yang dikirim dari perusaahan lain	Menampilk an halaman verifikasi kode OTP	Berhasil	Karyawan
	Mengiri m Kode OTP pada email penggu na	Menampilk an kode OTP dengan 6 digit acak pada email	Berhasil	Karyawan
	Mengisi kode OTP pada ifikasi kodeOTP	Menampilk an pemberitah uan verifikasi berhasil	Berhasil	Karyawan
Keluar	Menekan tombol keluar	Mengeluarkan akunpengguna dan masuk ke halaman login	Berhasil	Karyawan

SIMPULAN

Berdasarkan hasil penelitian ini dapat disimpulkan bahwa telah terciptanya aplikasi pengamanan dokumen digital perusahaan dengan menggunakan algoritma AES-256. Aplikasi tersebut telah berhasil mengamankan dengan baik file dokumen digital perusahaan yang berfomat docx, pdf, csv/xlxs, png/jpg. File dokumen yang berhasil dienkripsi berhasil tidak dapat dibuka kecuali dengan menggunakan aplikasi ini berdasarkan kunci dan token yang sesuai.

Saran

Adapun saran yang dapat peneliti sampaikan untuk dilakukan pengembangan

aplikasi ini agar lebih baik. Aplikasi yang telah dirancang belum bisa melakukan enkripsi dengan ukuran file yang besar. Hal itu dikarenakan terbatasnya penyimpanan pada bagian server. Sehingga kedepannya diharapkan aplikasi ini mampu mengenkripsi file dengan ukuran yang besar

DAFTAR PUSTAKA

Amin, S., dan Siahaan, K. (2016). Arsip Berbasis Web Pada Sekolah Tinggi Ilmu Tarbiyah. *Jurnal Manajemen Sistem Informasi*, Vol. 1(1), 1-10.

Ardiansyah, A., dan Kurniasih, M. (2019). Implementasi Algoritma AES-256 Untuk Pengamanan Layanan API Pada Restful Dengan Autentikasi JSon Web Tokens. *Seminar Nasional Inovasi Teknologi - SNITek*, Vol. 3(2), 315-326.

Arianto, A. (2018). Sistem Pakar Diagnosa Penyakit Ginjal Berbasis Android. *IJIEM: Kajian Teori dan Hasil Penelitian Pendidikan*, Vol.1(5), 43-67.

Clara, L. dan Budi, A. (2021). Implementasi Metode Algoritma AES Pada Perlindungan Data Sistem Login. *Jurnal Informatika dan Bisnis*, Vol. 10(2),121-133.

Didi, S. (2006). Algoritma Kriptografi AES Rijndael. *Jurnal Teknik Elektro*, Vol. 8 (2), 97-101.

Ega Shela Marsiani, E.S., Setiadi, I., dan Cahyo, A. . (2021). Implementasi Sistem Keamanan Aes 256-Bit Gcm Guna Mengamankan Data Pribadi. *JRKT (Jurnal Rekayasa Komputasi Terapan)*, Vol. 1(2), 108-114.

Fathurrozi, A. dan Selviyani. (2021). Penerapan Algoritma Advanced Encryption Standard (AES-256) Dengan Mode CBC DanSecure Hash Algorithm (SHA- 256) Untuk Pengamanan Data File. *Journal of Information and Information Security (JIFORTY)*, Vol. 2(2), 227-238.

Hidayah, M.A., Nugoho, N.B., dan Angin, M.I.P. . (2020). Penerapan Kriptografi Menggunakan Algoritma AES untuk Keamanan Data Penjualan P ada PT. Mestika Sakti. *Jurnal CyberTech*, Vol. 5(2), 111-114.

Murya, Y. (2014). *Pemrograman Android Black Box*. Jakarta: Jasakom.

Rohman, R.S., Firmansah, D.A., dan Ermawati, E. (2022). Sistem Informasi Decryptrespon Bridgingbpjs Kesehatan Dengan Algoritma Aes 256. *Jurnal Responsif*, Vol. 4(2), 142-151.

Rosa dan Shalahuddin. (2018). *Rekayasa Perangkat Lunak Terstruktur Dan Berorientasi Objek*. Bandung: Informatika.

Simangunsong, P. B. N., dan Fitri, K. (2018). Perancangan Aplikasi Pengamanan Citra Bewarna Dengan Algoritma RSA. *Jurnal Teknik Informatika*, Vol. 2(4), 99-107.

Singgih, S. (2017). *Menguasai Statistik Dengan SPSS 24*. Jakarta: PT Alex Media Komputindo.

Yusuf, A.M. (2019). *Metode Penelitian Kuantitatif, Kualitatif dan Penelitian Gabungan.* Jakarta: Pradamelia Group.

Yusup, A.M. (2021). *Pembangunan Sistem Keamanan Data File Arcgis Menggunakan Aes (Advanced Encryption Standard) Dan Hash Sha256 Pada Pt Baratim Info Bumi*. Bandung: Program Studi Teknik Informatika, Fakultas Teknik Dan Ilmu Komputer, Universitas Komputer Indonesia.