PRAKTIK SISTEM KEAMANAN DATA

RESUME JURNAL AES

Disusun Oleh :

Diana Lathifa

V3922016/ TI D

Dosen

Yusuf Fadlila Rachman S.Kom.,M.Kom

PS D-III TEKNIK INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS SEBELAS MARET

2023

Resume jurnal

Jurnal 1

https://ejurnal.its.ac.id/index.php/teknik/article/viewFile/97042/7237

“Implementasi algoritma AES pada jaringan IoT untuk mendukung smart healthcare”

Merupakan sistem kesehatan cerdas yang menggunakan sensor, software, dan teknologi lain untuk menghubungkan dan menukarkan data antar divisi dan sistem lain menggunakan internet. Latar belakang masalah yang mendorong penelitian ini adalah adanya tantangan keamanan dan sumber daya yang harus dihadapi oleh IoT, seperti serangan sniffing yang dapat menyadap data yang dikirimkan melalui jaringan.

A. Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma AES pada jaringan IoT untuk mendukung smart healthcare, sehingga data yang dikirimkan dapat terenkripsi dan terhindar dari penyadapan. Penelitian ini juga bertujuan untuk menguji kinerja dan keamanan dari sistem yang dibangun.

B. Algoritma yang dipakai beserta alur penelitiannya

Algoritma yang dipakai dalam penelitian ini adalah AES-128, yaitu algoritma kriptografi kunci simetris yang menggunakan kunci sepanjang 128 bit untuk mengenkripsi dan mendekripsi data. Alur penelitiannya adalah sebagai berikut:

a. Merancang sistem IoT untuk smart healthcare yang terdiri dari sensor, Raspberry Pi, dan web server.
b. Mengimplementasikan algoritma AES-128 pada Raspberry Pi menggunakan bahasa PHP untuk mengenkripsi data yang dikirimkan oleh sensor dan mendekripsi data yang diterima dari web server.
c. Mengimplementasikan algoritma AES-128 pada web server menggunakan bahasa PHP untuk mendekripsi data yang diterima dari Raspberry Pi dan mengenkripsi data yang dikirimkan ke Raspberry Pi.
d. Mengintegrasikan seluruh bagian sistem dan melakukan pengujian kinerja dan keamanan.

C. Hasil penelitian dan kesimpulan

Hasil penelitian menunjukkan bahwa AES-128 yang diterapkan dapat berjalan baik dengan hasil waktu proses yang lebih lama dibandingkan sistem tanpa menggunakan algoritma AES 128 bit sebesar 0,560 detik untuk enkripsi dan 0,018 detik untuk dekripsi. Pengujian konektivitas jaringan wifi menunjukkan jarak maksimum sebesar 54 meter agar dapat terhubung. Pengujian keamanan dengan penetration testing menunjukkan bahwa database pada sistem ini aman dari hacker dan memenuhi unsur confidentiality atau kerahasiaan data. Kesimpulan dari penelitian ini adalah algoritma AES-128 dapat diimplementasikan pada jaringan IoT untuk mendukung smart healthcare dengan kinerja dan keamanan yang baik.

D. Kelebihan dan kekurangan jurnal

Kelebihan dari jurnal ini adalah memberikan solusi untuk mengatasi masalah keamanan pada jaringan IoT dengan menggunakan algoritma AES-128 yang memiliki konsumsi daya rendah dan ruang kunci yang besar. Jurnal ini juga memberikan hasil pengujian yang lengkap dan valid untuk menunjukkan kinerja dan keamanan dari sistem yang dibangun. Kekurangan dari jurnal ini adalah tidak memberikan perbandingan dengan algoritma kriptografi lain yang mungkin dapat digunakan pada jaringan IoT, seperti RC4, DES, atau RSA. Jurnal ini juga tidak memberikan analisis mengenai dampak dari penggunaan algoritma AES-128 terhadap aspek lain dari jaringan IoT, seperti bandwidth, latency, atau reliabilitas.

Jurnal 2

https://ejournal.unisba.ac.id/index.php/matematika/article/viewFile/4067/2398

“Implementasi algoritma AES untuk penyandian file dokumen”

Merupakan proses mengubah file dokumen menjadi bentuk yang tidak dapat dibaca atau dipahami oleh sembarang orang. Latar belakang masalah yang mendorong penelitian ini adalah adanya kebutuhan untuk melindungi file dokumen yang berisi informasi penting atau rahasia dari orang yang tidak berhak, seperti pencuri data, hacker, atau mata-mata.

A. Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma AES untuk penyandian file dokumen, sehingga file dokumen dapat terlindungi dari akses yang tidak sah. Penelitian ini juga bertujuan untuk menguji keamanan dan efektivitas dari algoritma AES untuk penyandian file dokumen.

B. Algoritma yang dipakai beserta alur penelitiannya

Algoritma yang dipakai dalam penelitian ini adalah AES 128, yaitu algoritma kriptografi kunci simetris yang menggunakan kunci sepanjang 128 bit untuk mengenkripsi dan mendekripsi file dokumen. Alur penelitiannya adalah sebagai berikut:

1. Merancang program penyandian file dokumen dengan menggunakan bahasa pemrograman C++.
2. Mengimplementasikan algoritma AES 128 pada program dengan menggunakan empat transformasi dasar, yaitu subbytes, shiftrows, mixcolumns, dan addroundkey untuk proses enkripsi, dan invers dari transformasi tersebut untuk proses dekripsi.
3. Melakukan proses penyandian file dokumen dengan menggunakan program yang telah dibuat dan menguji keamanan dan efektivitas dari algoritma AES 128.

C. Hasil penelitian dan kesimpulan

Hasil penelitian menunjukkan bahwa algoritma AES 128 dapat digunakan untuk penyandian file dokumen dengan hasil file yang terenkripsi dan tidak dapat dibaca oleh sembarang orang. Pengujian keamanan dengan menggunakan brute force attack menunjukkan bahwa algoritma AES 128 memiliki ruang kunci yang sangat besar, yaitu 2^128, yang membuatnya sulit untuk ditembus. Pengujian efektivitas dengan menggunakan ukuran file dan waktu proses menunjukkan bahwa algoritma AES 128 memiliki efektivitas yang tinggi, yaitu tidak mengubah ukuran file yang disandikan dan memiliki waktu proses yang cepat. Kesimpulan dari penelitian ini adalah algoritma AES 128 dapat diimplementasikan untuk penyandian file dokumen dengan keamanan dan efektivitas yang baik.

D. Kelebihan dan kekurangan jurnal

Kelebihan dari jurnal ini adalah memberikan solusi untuk mengatasi masalah penyandian file dokumen dengan menggunakan algoritma AES 128 yang memiliki keamanan dan efektivitas yang tinggi. Jurnal ini juga memberikan hasil pengujian yang lengkap dan valid untuk menunjukkan keamanan dan efektivitas dari algoritma AES 128. Kekurangan dari jurnal ini adalah tidak memberikan perbandingan dengan algoritma kriptografi lain yang mungkin dapat digunakan untuk penyandian file dokumen, seperti RC4, DES, atau RSA. Jurnal ini juga tidak memberikan analisis mengenai dampak dari penggunaan algoritma AES 128 terhadap aspek lain dari file dokumen, seperti kualitas, format, atau kompresi.