Jurnal Riset Multidisiplin Edukasi
https://journal.hasbaedukasi.co.id/index.php/jurmie
Halaman : 181-198

IMPLEMENTASI ALGORITMA DIFFIE-HELLMAN KEY EXCHANGE (DHE) DAN AES DALAM ENKRIPSI PESAN END-TO-END

M. Khairi Nasution[1], Rachmat Aulia[2], Antoni[3]
Program Studi Teknik Informatika Fakultas Teknik Universitas Islam Sumatera Utara Medan[1,2,3]
Email: khairinasty@gmail.com

Informasi

Volume : 2
Nomor : 10
Bulan : Oktober
Tahun : 2025
E-ISSN : 3062-9624

Abstract

Digital communication security is a crucial aspect in the modern era of information technology. This study aims to implement a combination of the Diffie- Hellman Key Exchange (DHE) and Advanced Encryption Standard (AES) algorithms in an end- to-end encryption (E2EE) system to ensure data confidentiality and integrity. The method used includes a secure key exchange process via the DHE algorithm and message encryption using AES-256, ensuring secure communication between two users. The research process began with the design of a web-based communication system that allows users to securely exchange messages. The initial stage involves the exchange of public keys between two parties using DHE, which then generates a shared secret key. This key is subsequently used in the encryption and decryption of messages using AES, strengthened by the use of an Initialization Vector (IV) to enhance security. An example of implementation is demonstrated through a communication simulation between Alice and Bob, where values of p = 23 and g = 2 are used as public parameters, while a = 6 and b = 15 serve as private values. Both parties successfully establish a shared key of 4, which is then used to encrypt a message such as "Hello, Bob!" into ciphertext. This message can only be decrypted by the recipient using the same key and the included IV. With this system, users can securely send and receive text messages through a simple yet functional interface.

Keyword: *Cryptography, Diffie-Hellman Key Exchange, Advanced Encryption Standard, End-to-End Encryption, Data Security.*

Abstrak

Keamanan komunikasi digital menjadi aspek penting dalam era teknologi informasi modern. Penelitian ini bertujuan untuk mengimplementasikan kombinasi algoritma Diffie-Hellman Key Exchange (DHE) dan Advanced Encryption Standard (AES) dalam sistem enkripsi pesan end-to-end (E2EE) guna menjamin kerahasiaan dan integritas data. Metode yang digunakan meliputi proses pertukaran kunci secara aman melalui algoritma DHE serta enkripsi pesan menggunakan AES-256, yang memastikan keamanan komunikasi antara dua pengguna. Proses penelitian dimulai dengan merancang sistem komunikasi berbasis web yang memungkinkan pengguna bertukar pesan secara aman. Tahapan dimulai dari pertukaran kunci publik antara dua pihak menggunakan DHE, yang kemudian menghasilkan kunci rahasia bersama. Kunci ini selanjutnya digunakan dalam proses enkripsi dan dekripsi pesan menggunakan AES, yang diperkuat dengan penggunaan Initialization Vector (IV) untuk menambah tingkat keamanan. Contoh penerapan ditunjukkan melalui simulasi komunikasi antara Alice dan Bob, di mana nilai p = 23 dan g = 2 digunakan sebagai parameter publik, sementara a = 6 dan b = 15 sebagai nilai rahasia. Kedua pihak berhasil membentuk kunci bersama sebesar 4 yang kemudian digunakan untuk mengenkripsi pesan seperti "Halo, Bob!" menjadi ciphertext. Pesan ini hanya dapat didekripsi oleh penerima menggunakan kunci yang sama dan IV yang disertakan. Dengan sistem ini, pengguna dapat mengirim dan menerima pesan teks secara aman melalui antarmuka yang sederhana namun fungsional.

Kata Kunci: *Kriptografi, Diffie-Hellman Key Exchange, Advanced Encryption Standard, Enkripsi End-to-End, Keamanan Data.*

A. PENDAHULUAN

Keamanan informasi merupakan aspek yang sangat penting dalam komunikasi digital. Seiring dengan pesatnya perkembangan teknologi dan meningkatnya ketergantungan masyarakat pada layanan berbasis internet, ancaman terhadap data pribadi dan informasi sensitif juga semakin besar. Serangan siber seperti penyadapan, peretasan, dan pencurian data sering kali terjadi, mengakibatkan kebocoran informasi yang dapat merugikan individu maupun organisasi. Oleh karena itu, diperlukan metode enkripsi yang kuat untuk melindungi data selama proses transmisi.

Dalam era digital yang semakin berkembang, keamanan informasi menjadi aspek yang sangat krusial, terutama dalam komunikasi berbasis jaringan yang rawan terhadap ancaman seperti penyadapan dan peretasan. Algoritma Advanced Encryption Standard (AES) sebagai metode enkripsi simetris memiliki efisiensi tinggi dalam mengamankan data. Di sisi lain, algoritma Diffie-Hellman Key Exchange (DHE) menawarkan pertukaran kunci secara aman di jaringan publik, namun perlu diuji efektivitas dan keamanannya saat diintegrasikan dalam sistem end-to-end encryption. Permasalahan utama yang ingin dipecahkan dalam penelitian ini adalah bagaimana mengimplementasikan dan mengombinasikan algoritma DHE dan AES secara efektif dalam sistem enkripsi pesan end-to-end agar dapat menjamin keamanan dan efisiensi proses komunikasi digital, khususnya dalam pengamanan pertukaran kunci dan perlindungan terhadap isi pesan dari akses pihak yang tidak berwenang.

Dalam implementasi enkripsi E2EE, algoritma kriptografi berperan penting dalam menjaga keamanan data. Advanced Encryption Standard (AES) merupakan salah satu algoritma enkripsi simetris yang telah menjadi standar global karena keamanannya yang tinggi dan efisiensinya dalam pemrosesan data. AES menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, yang membuatnya sangat cepat dan efisien dalam mengamankan pesan. Namun, karena AES menggunakan sistem kunci simetris, muncul tantangan dalam mendistribusikan kunci secara aman antara pengirim dan penerima.

Untuk mengatasi permasalahan pertukaran kunci pada algoritma enkripsi simetris, digunakan Diffie-Hellman Key Exchange (DHE). DHE adalah salah satu algoritma pertukaran kunci yang memungkinkan dua pihak untuk berbagi kunci enkripsi secara aman melalui jaringan yang tidak aman, tanpa harus mengirimkan kunci tersebut secara langsung. Dengan menggunakan prinsip matematika eksponensial modular, DHE memungkinkan pembentukan kunci rahasia bersama yang hanya dapat dihitung oleh kedua pihak yang berkomunikasi. Hal

ini membuat metode ini sangat efektif dalam melindungi proses pertukaran kunci dari serangan pihak ketiga.

Kombinasi antara Diffie-Hellman Key Exchange (DHE) dan Advanced Encryption Standard (AES) dalam enkripsi pesan end-to-end menjadi solusi yang efektif dalam meningkatkan keamanan komunikasi digital. DHE digunakan untuk mendistribusikan kunci secara aman, sedangkan AES digunakan untuk mengenkripsi pesan dengan efisiensi tinggi. Implementasi gabungan kedua algoritma ini dapat meningkatkan keamanan data dan mencegah akses tidak sah selama proses komunikasi berlangsung.

Penelitian ini bertujuan untuk mengimplementasikan algoritma Diffie-Hellman Key Exchange (DHE) dan AES dalam enkripsi pesan end-to-end serta menganalisis kinerja dan keamanannya. Melalui penelitian ini, diharapkan dapat diperoleh pemahaman yang lebih dalam mengenai efektivitas kombinasi kedua algoritma dalam menjaga kerahasiaan komunikasi digital. Selain itu, hasil penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem keamanan komunikasi yang lebih baik, terutama di era digital yang semakin rentan terhadap ancaman keamanan siber.

Berdasarkan latar belakang yang mendasari penelitian ini, penulis merumuskan beberapa rumusan masalah, yaitu: (1) bagaimana cara merancang mekanisme pertukaran kunci yang aman antara pengirim dan penerima pesan dengan menggunakan algoritma Diffie-Hellman Key Exchange (DHE); (2) bagaimana menerapkan algoritma AES untuk melakukan enkripsi dan dekripsi pesan setelah kunci berhasil dibentuk melalui DHE; (3) bagaimana mengintegrasikan algoritma DHE dan AES agar dapat membentuk sistem enkripsi pesan end-to-end yang efektif dan efisien; serta (4) bagaimana tingkat efisiensi kombinasi algoritma DHE dan AES dalam menjaga keamanan komunikasi digital dari berbagai ancaman. Agar penelitian tidak melebar dan tetap fokus, batasan masalah yang ditetapkan meliputi: penelitian hanya membahas implementasi algoritma DHE sebagai metode pertukaran kunci dan AES sebagai metode enkripsi pesan, pengujian dilakukan pada komunikasi berbasis teks, penerapan algoritma menggunakan AES 128 bit dan DHE 2048 bit, sistem hanya berfokus pada aspek keamanan enkripsi dan pertukaran kunci tanpa membahas autentikasi pengguna atau manajemen sesi, serta pemodelan data menggunakan UML.

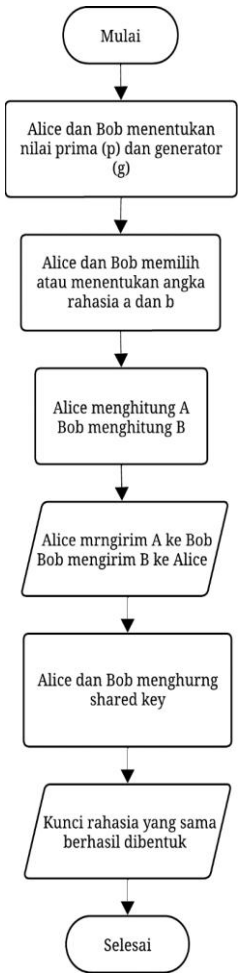
Tujuan penelitian ini antara lain untuk merancang mekanisme pertukaran kunci aman menggunakan algoritma Diffie-Hellman Key Exchange (DHE), menerapkan algoritma AES untuk melakukan proses enkripsi dan dekripsi pesan, serta mengintegrasikan algoritma DHE dan AES dalam satu sistem agar menghasilkan enkripsi pesan end-to-end yang optimal. Selain

itu, penelitian ini juga bertujuan untuk menguji dan menganalisis tingkat keamanan yang dihasilkan oleh kombinasi kedua algoritma tersebut dalam menjaga kerahasiaan pesan selama proses komunikasi berlangsung.

B. METODE PENELITIAN

Metodologi penelitian ini mencakup alat dan bahan yang digunakan serta teknik pengumpulan data. Dalam pembuatan penelitian skripsi ini, peneliti membutuhkan perangkat keras (hardware) dan perangkat lunak (software). Perangkat keras yang digunakan meliputi prosesor Intel Core i5-8000 series, RAM sebesar 16 GB, dan SSD berkapasitas 256 GB. Sementara itu, perangkat lunak yang digunakan terdiri dari sistem operasi Windows 11 Home Basic 64-bit, text editor Microsoft Visual Studio Code, web browser Google Chrome, bahasa pemrograman HTML, PHP, dan JavaScript, serta database MySQL. Adapun teknik pengumpulan data yang digunakan dalam penelitian ini adalah studi literatur, yaitu dengan mengumpulkan data dan informasi dari berbagai sumber seperti buku, jurnal, dan artikel yang berkaitan dengan teori serta langkah-langkah dalam pembuatan aplikasi. Hasil dari studi literatur ini digunakan sebagai dasar dalam penyusunan landasan teori dan perancangan aplikasi yang dikembangkan dalam penelitian ini.

Flowchart Algoritma Diffie-Hellman Key Exchange (DHE)

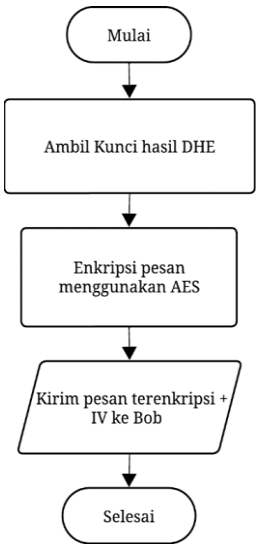


Gambar 1 Flowchart Algoritma Diffie-Hellman Key Exchange (DHE)

Keterangan pada Gambar 1 menjelaskan proses pertukaran kunci menggunakan algoritma Diffie-Hellman Key Exchange (DHE). Proses dimulai dengan langkah awal yaitu "Mulai", kemudian Alice dan Bob menentukan dua angka publik, yaitu p sebagai bilangan prima besar (misalnya 2048-bit) dan g sebagai generator (biasanya bernilai 2 atau 5). Nilai p dan g ini bersifat publik dan dapat diketahui oleh siapa pun. Selanjutnya, Alice memilih angka rahasia a sebagai private key yang hanya ia ketahui, sementara Bob juga memilih angka rahasia b yang hanya diketahui olehnya. Setelah itu, Alice menghitung nilai publik A dengan rumus A = (g^a) mod p, sedangkan Bob menghitung nilai publik B dengan rumus B = (g^b) mod p. Alice kemudian mengirimkan nilai A kepada Bob melalui kanal komunikasi, dan Bob mengirimkan nilai B kepada Alice. Setelah saling bertukar nilai publik, Alice menghitung kunci rahasia bersama dengan rumus kunci = (B^a) mod p, sementara Bob menghitung kunci rahasia dengan rumus kunci = (A^b) mod p. Hasil dari kedua perhitungan tersebut akan menghasilkan nilai kunci yang sama, yaitu shared secret key yang dapat digunakan untuk

komunikasi aman antara keduanya. Setelah kunci rahasia bersama berhasil dibentuk, proses pembangkitan kunci dinyatakan selesai.

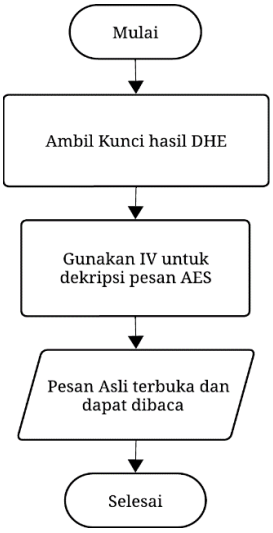
Flowchart Enkripsi Algoritma Advanced Encryption Standard (AES)



Gambar 2 Flowchart Enkripsi Algoritma Advanced Encryption Standard (AES)

Gambar 2 merupakan flowchart proses enkripsi menggunakan algoritma AES, di mana pada tahap ini penulis menjelaskan proses enkripsi pesan yang dilakukan oleh pengirim (Alice). Proses dimulai dengan langkah "Mulai Enkripsi", kemudian sistem mengambil kunci rahasia bersama yang telah dihasilkan melalui algoritma Diffie-Hellman Key Exchange (DHE). Kunci ini bersifat simetris dan digunakan untuk proses enkripsi pesan. Selanjutnya, pesan asli dienkripsi menggunakan algoritma AES dengan memanfaatkan kunci hasil DHE dan IV (Initialization Vector) yang dibuat secara acak untuk meningkatkan keamanan. Penggunaan IV ini bertujuan agar meskipun pesan dan kunci yang digunakan sama, hasil enkripsi tetap berbeda setiap kali proses dilakukan. Setelah pesan berhasil dienkripsi, pesan terenkripsi beserta IV dikirim kepada penerima (Bob), karena IV dibutuhkan agar Bob dapat melakukan dekripsi pesan dengan benar. Tahap terakhir adalah "Selesai", yang menandakan bahwa proses enkripsi dan pengiriman pesan telah berhasil diselesaikan.

Flowchart Dekripsi Algoritma Advanced Encryption Standard (AES)

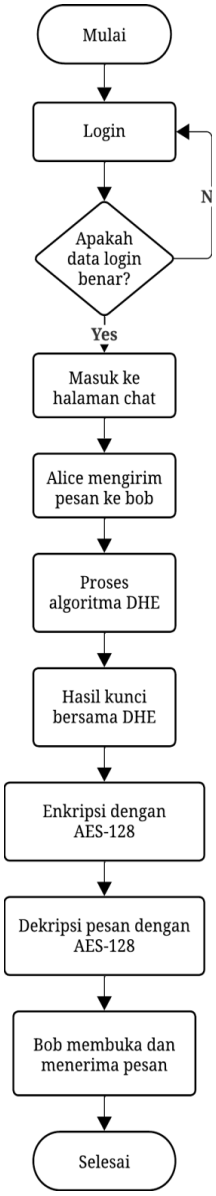


Gambar 3 Flowchart Dekripsi Algoritma Advanced Encryption Standard (AES)

Gambar 3 merupakan flowchart proses dekripsi menggunakan algoritma AES, di mana pada tahap ini penulis menjelaskan proses penerimaan dan pembacaan pesan terenkripsi oleh Bob. Proses dimulai dengan langkah "Mulai Dekripsi", kemudian penerima pesan mengambil kunci rahasia bersama yang sebelumnya telah dihasilkan melalui algoritma Diffie-Hellman (DHE). Kunci ini harus sama dengan kunci yang digunakan oleh pengirim (Alice) agar proses dekripsi dapat berhasil. Selanjutnya, Bob menggunakan IV (Initialization Vector) yang dikirim bersama ciphertext untuk mendekripsi pesan dengan algoritma AES. IV ini sangat penting karena digunakan juga pada saat enkripsi, sehingga memastikan pesan asli dapat dihasilkan dengan tepat. Setelah proses dekripsi selesai, Bob berhasil memperoleh pesan asli yang dikirim oleh Alice. Tahap terakhir adalah "Selesai", yang menandakan bahwa proses dekripsi telah berhasil dilakukan dan komunikasi antara pengirim dan penerima berlangsung dengan aman.

Perancangan Sistem

Flowchart Sistem



Gambar 4 Flowchart Sistem

Keterangan flowchart di atas menjelaskan proses pengiriman pesan terenkripsi antara dua pengguna, yaitu Alice dan Bob, dengan menggunakan kombinasi algoritma Diffie-Hellman Key Exchange (DHE) dan AES-128. Proses dimulai dari langkah "Mulai", di mana pengguna melakukan login ke dalam sistem dengan memasukkan username dan password. Sistem kemudian melakukan validasi terhadap data login tersebut. Jika data yang dimasukkan benar, pengguna akan diarahkan ke halaman utama aplikasi pesan (chat), namun jika salah, sistem akan mengembalikan pengguna ke form login. Setelah berhasil masuk ke halaman chat, pengguna bernama Alice dapat mengetik dan mengirim pesan kepada Bob. Sebelum pesan dikirim, sistem menjalankan proses algoritma DHE untuk menghasilkan kunci rahasia

bersama (shared key) antara Alice dan Bob tanpa harus saling mengirimkan kunci rahasia tersebut secara langsung.

Kunci hasil dari proses DHE tersebut kemudian digunakan sebagai kunci simetris untuk enkripsi dan dekripsi pesan menggunakan algoritma AES-128. Pesan yang diketik oleh Alice terlebih dahulu dienkripsi dengan AES-128 sebelum dikirim ke Bob. Setelah pesan terenkripsi diterima oleh Bob, sistem akan melakukan proses dekripsi menggunakan kunci yang sama hasil dari DHE sehingga pesan asli dapat dibaca dengan aman. Setelah pesan berhasil dibuka oleh Bob, proses komunikasi dianggap selesai. Flowchart ini menggambarkan bagaimana sistem menjaga keamanan pesan dengan memanfaatkan mekanisme pertukaran kunci rahasia yang aman melalui DHE dan enkripsi simetris AES-128, sehingga hanya pihak pengirim dan penerima yang dapat memahami isi pesan yang dikirimkan.

Penerapan Algoritma DHE

Tahapan penerapan algoritma DHE diawali dengan menentukan nilai publik p dan g. Dalam contoh ini, nilai p = 23 dan g = 2. Selanjutnya, Alice memilih angka rahasia a = 6, sedangkan Bob memilih angka rahasia b = 15. Setelah itu, Alice menghitung nilai publik A dengan rumus $A = g^a \bmod p = 2^6 \bmod 23 = 64 \bmod 23 = 18$. Bob juga menghitung nilai publik B dengan rumus $B = g^b \bmod p = 2^{15} \bmod 23 = 32768 \bmod 23 = 16$. Setelah mendapatkan nilai publik, keduanya saling menukar kunci publik. Alice menggunakan kunci publik Bob untuk menghitung kunci bersama dengan rumus $s_{ali}c_e = B^a \bmod p = 16^6 \bmod 23 = 16.777.216 \bmod 23 = 4$, sedangkan Bob menggunakan kunci publik Alice untuk menghitung $s\_bob = A^b \bmod p = 18^{15} \bmod 23 = 6.746.640.616.477.458.432 \bmod 23 = 4$. Hasilnya, baik Alice maupun Bob memperoleh kunci bersama yang sama, yaitu 4. Setelah kunci publik DHE diperoleh, proses dilanjutkan dengan penerapan algoritma AES untuk melakukan enkripsi dan dekripsi pesan. Dalam implementasinya, algoritma AES tidak menggunakan perhitungan manual, melainkan mengubah kunci bersama dari hasil DHE menjadi bilangan biner yang digunakan dalam proses enkripsi dan dekripsi.

Penerapan Algoritma AES

Setelah melakukan perhitungan untuk menentukan kunci publik pengamanan pesan pada algoritma DHE, tahap selanjutnya adalah melakukan penguncian pesan atau enkripsi dan pembukaan pesan atau dekripsi dengan menggunakan algoritma AES. Pada penerapan enkripsi dan dekripsi pada program penulis, tidak ada rumus atau perhitungan khusus untuk algoritma AES itu berjalan. Algoritma AES melakukan enkripsi dan dekripsi dengan mengubah kunci bersama yang didapat dari DHE menjadi bilangan biner.

Perancangan Tabel

Tabel 1 Perancangan Tabel User

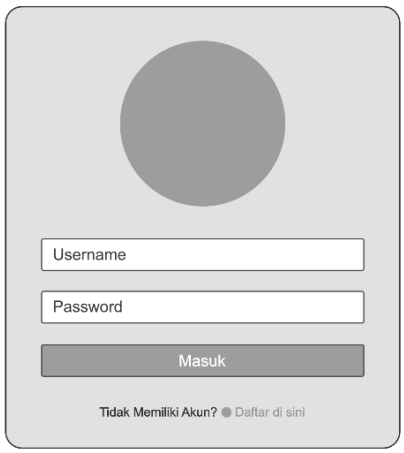
Nama Kolom	Tipe Data (Size)
Id	Int (2)
Username	Varchar (50)
Password	Varchar (255)
Foto_profil	Longbob
Dh_public_key	Text
Dh_private_key	Text
Dh_prime	Text
Dh_generator	Text
Created_at	datetime

Tabel 2 Perancangan Tabel Hasil Pesan

Nama Kolom	Tipe Data (Size)
Id	Int (2)
Sender_id	Int (2)
Receiver_id	Int (2)
Encrypted_message	Text
Iv	Text
Timestamp	Datetime

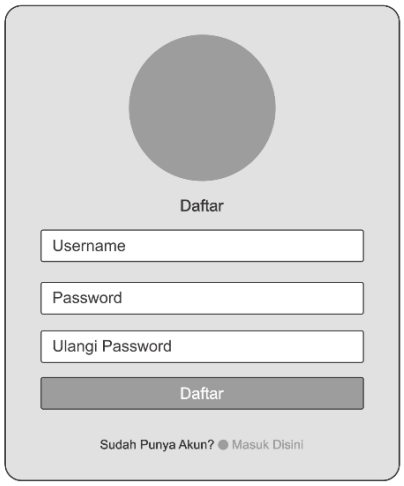
Perancangan Antarmuka

Perancangan Antarmuka Halaman Login Pengguna



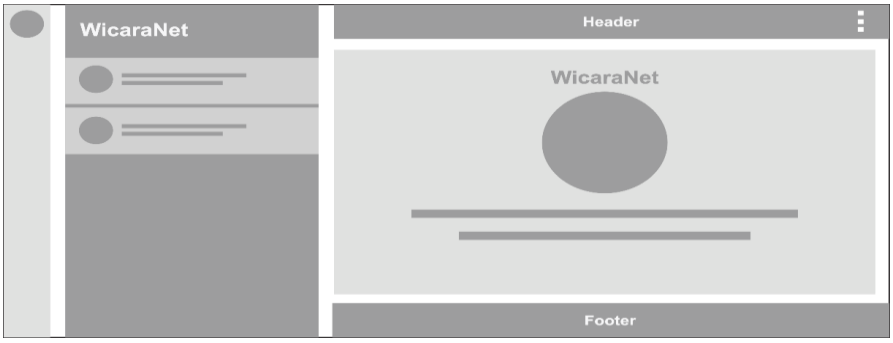
Gambar 5 Perancangan Antarmuka Halaman Login Pengguna

Perancangan Antarmuka Halaman Registrasi



Gambar 6 Perancangan Antarmuka Halaman Registrasi

Perancangan Antarmuka Halaman Fitur Chat



Gambar 7 Perancangan Antarmuka Halaman Fitur Chat

C. HASIL DAN PEMBAHASAN

Hasil Penelitian

Penelitian ini menghasilkan sebuah sistem komunikasi berbasis web yang mengintegrasikan algoritma Diffie-Hellman Key Exchange (DHE) dan Advanced Encryption Standard (AES) untuk mengamankan pertukaran pesan secara end-to- end (E2EE). Sistem ini memungkinkan dua pengguna untuk bertukar pesan teks secara aman tanpa harus khawatir pesan mereka disadap atau dimodifikasi oleh pihak ketiga. DHE berperan dalam menghasilkan kunci enkripsi secara aman melalui saluran publik, sementara AES digunakan untuk melakukan proses enkripsi dan dekripsi pesan dengan tingkat efisiensi dan keamanan yang tinggi.

Sebagai contoh penerapan, sistem diuji dengan dua pengguna, yaitu Alice dan Bob. Dalam simulasi komunikasi, Alice dan Bob pertama-tama melakukan proses pertukaran kunci menggunakan algoritma DHE. Misalnya, Alice memilih bilangan rahasia a = 6 dan Bob memilih b = 15, dengan nilai publik p = 23 dan g = 2. Dari perhitungan ini, mereka masing-masing memperoleh nilai publik yang kemudian ditukar. Setelah proses pertukaran selesai, baik Alice maupun Bob menghasilkan kunci bersama yang sama, yaitu 18. Kunci ini kemudian digunakan oleh kedua belah pihak untuk proses enkripsi dan dekripsi pesan menggunakan algoritma AES. Dalam praktiknya, ketika Alice mengirimkan pesan seperti "Halo, Bob!",

Pesan ini tidak langsung dikirim dalam bentuk teks biasa, melainkan terlebih dahulu dienkripsi menggunakan AES-128 dengan kunci 18 yang dihasilkan dari DHE serta IV (Initialization Vector) acak. Hasilnya adalah ciphertext yang dikirim ke Bob melalui sistem. Saat Bob menerima pesan tersebut, sistem menggunakan IV dan kunci yang sama untuk mendekripsi pesan dan menampilkannya sebagai teks asli. Proses ini memastikan bahwa hanya Bob yang dapat membaca pesan tersebut, bahkan jika pihak ketiga berhasil menyadap data yang dikirimkan.

Selain proses komunikasi yang aman, sistem ini juga dilengkapi dengan antarmuka pengguna seperti halaman registrasi, login, dan fitur chat yang dirancang sederhana namun fungsional. Perancangan sistem ini didukung dengan diagram UML seperti use case, activity, class, dan sequence diagram untuk memastikan proses komunikasi dan keamanan berjalan sesuai desain.

Melalui penerapan dan pengujian sistem ini, dapat disimpulkan bahwa kombinasi algoritma DHE dan AES mampu mengamankan komunikasi berbasis teks. Sistem tidak hanya

berhasil menjamin kerahasiaan pesan, tetapi juga mencegah potensi serangan man-in-the-middle dan pengungkapan data oleh pihak yang tidak berwenang.

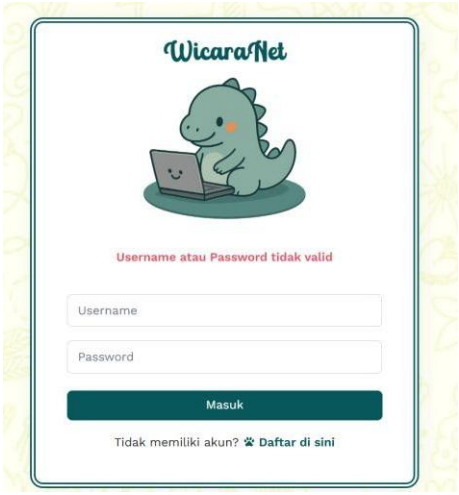
Implementasi Aplikasi

Tampilan Halaman Login

Gambar 8 Tampilan Halaman Login

Gambar 8 merupakan tampilan halaman login, halaman ini adalah halaman utama yang akan pengguna lihat ketika pertama kali membuka website. Pada halamanan ini penguna harus memasukkan data login yaitu username dan password dengan benar. Jika data sudah dimasukkan, pengguna dapat menekan tombol masuk untuk dapat masuk ke halaman selanjutnya.

Tampilan Halaman Login Gagal

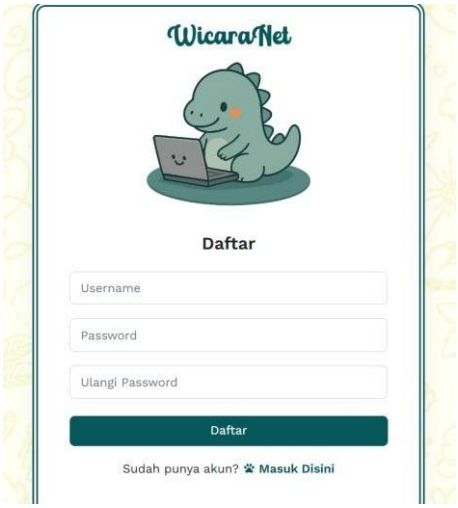


Gambar 9 Tampilan Halaman Login Gagal

Gambar 9 merupakan tampilan halaman login pengguna jika gagal. Pada halaman ini jika pengguna memasukkan username atau password yang salah, maka tampilan seperti gambar

4.2 ini akan keluar dengan manampilkan peringatan bahwa “Username atau Password tidak valid”.

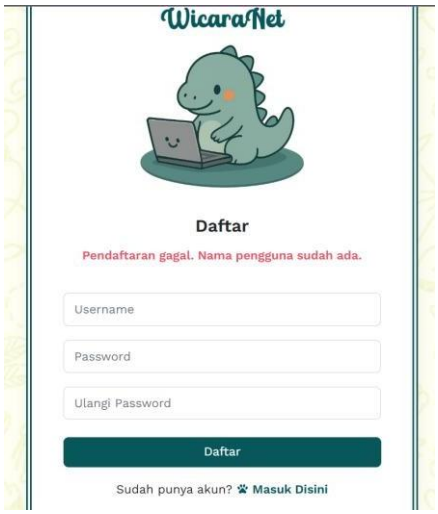
Tampilan Halaman Registrasi



Gambar 10 Tampilan Halaman Registrasi

Gambar 10 merupakan tampilan halaman Registrasi pengguna. Halaman ini adalah halaman untuk pengguna yang tidak atau belum memiliki akun chat, tetapi ingin memiliki akun. Pengguna akan diminta memasukkan username, password, dan ulangi password untuk melakukan registrasi atau pendaftaran. Jika data sudah selesai dimasukkan, pengguna dapat menekan tombol daftar untuk kemudia memasukkan kembali data yang sudah dibuat ke halaman login.

Tampilan Halaman Registrasi Gagal

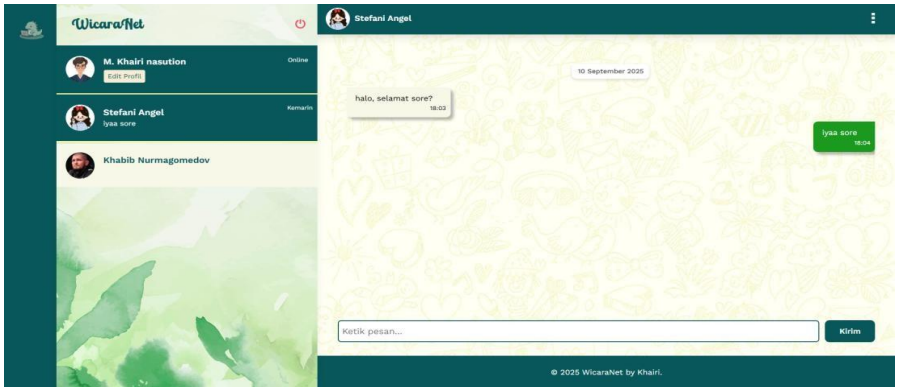


Gambar 11 Tampilan Halaman Registrasi Gagal

Gambar 11 merupakan tampilan halaman registrasi pengguna yang gagal. Pada halaman ini, jika pengguna memasukkan username yang sama dengan pengguna lain atau

memasukkan username yang sudah ada, maka registrasi atau pendaftaran akan gagal. Tampilan halaman registrasi akan mengeluarkan peringatan bahwa "Pendaftaran gagal. Nama pengguna sudah ada.".

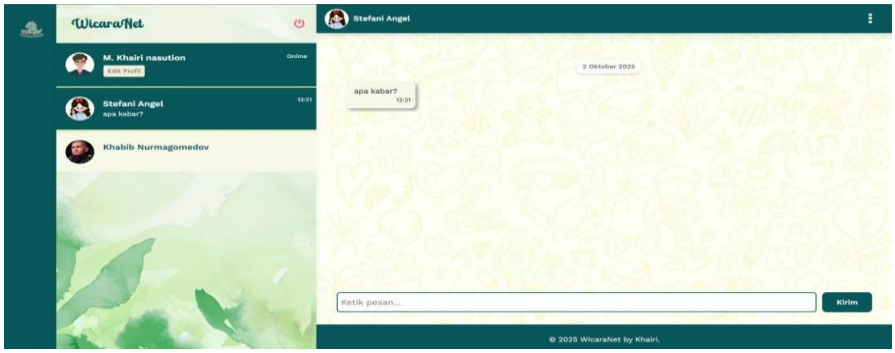
Tampilan Halaman Chat



Gambar 12 Tampilan Halaman Chat

Gambar 12 merupakan tampilan halaman chat pengguna. Pada halaman ini, pengguna yang sudah berhasil login akan langsung masuk ke halaman chat. Pada halaman ini pengguna dapat berkirim pesan kepada pengguna lainnya yang sudah terdaftar. Halaman chat ini memiliki dua algoritma enkripsi, yaitu DHE dan AES. Algoritma DHE dan AES akan berjalan pada halaman ini guna melakukan penguncian pesan teks antar pengguna. Pada halaman ini pengirim akan mengirimkan plaintext kepada penerima, lalu algoritma akan melakukan pengamanan pesan dengan algoritma DHE dan AES berupa sebuah chipertext, setelah itu penerima dapat melihat kembali isi pesan dari pengirim sebagai pleintext.

Tampilan Hasil Pesan



Gambar 13 Tampilan Hasil Pesan

Gambar 13 di atas merupakan tampilan hasil pesan yang dilakukan Stefani kepada Khairi. Pada tampilan pesan tersebut Stefani sebagai pengirim (sender) mengirimkan pesan kepada Khairi yang merupakan penerima (Receiver) berupa "apa kabar?". "apa kabar?" yang tampil pada halaman ini merupakan plaintext akhir yang sudah melawari proses end-to-end

atau proses enkripsi dan dekripsi pesan menggunakan AES dan DHE. Proses yang dilakukan adalah sender mengirim pesar plaintext berupa kalimat "apa kabar?", lalu DHE akan membuat kunci yang sebelumnya sender dan receiver sudah membuat kunci masing masing. Pada kaliman yang dikirimkan sender di atas, hasil shared key atau kunci bersamanya adalah 9c72f93056284dfc7221f4e1c0c0039456ecace2b...5b8e1ed07531728e4ee7546ad4 80f0ecaf6b057f8499a237dc64e4d135ab70. Setelah mendapatkan kunci bersama, tahap selanjutnya adalah AES akan melakukan proses enkripsi pesan yang akan menghasilkan chipertext berdasarkan kunci bersama yang sudah di ambil. Pada pesan di atas, chipertext yang sudah di ambil adalah f5a1b66f5ca117a8e73f7f422e066391. Setelah itu, AES akan melakukan dekripsi pesan yang berguna untuk menghasilkan kembali plaintext dan akan menampilkan pesan yang dikirim oleh sender kepada receiver. Plaintext akhir yang akan diterima oleh penerima akan sesuai dengan plaintext awal yang dikirim oleh pengeirim yaitu kalimat "apa kabar?".

D. KESIMPULAN

Dari hasil penelitian ini dapat disimpulkan bahwa algoritma Diffie-Hellman Key Exchange (DHE) berhasil digunakan untuk menghasilkan kunci rahasia bersama antara dua pengguna (contoh: Alice dan Bob) melalui saluran publik secara aman, tanpa perlu mengirimkan kunci secara langsung. Setelah kunci bersama diperoleh melalui DHE, pesan teks berhasil dienkripsi dan didekripsi menggunakan algoritma AES-128. Proses enkripsi menggunakan Initialization Vector (IV) untuk meningkatkan keamanan, memastikan hasil enkripsi berbeda meskipun pesan dan kunci sama. Sistem berbasis web yang dibangun memungkinkan pengguna saling bertukar pesan dengan keamanan tinggi, mencegah akses tidak sah dari pihak ketiga (seperti serangan man-in-the-middle).

E. DAFTAR PUSTAKA

Adyan, A. Q., Susilo, B., & Andreswari, D. (2020). Sistem Pendukung Keputusan Penempatan Praktik Kerja Lapangan Berdasarkan Nilai Kompetensi Dasar Dan Nilai Sikap Siswa Menggunakan Metode Pembobotan Rank Order Centroid Dan Metode Profile Matching. Jurnal Rekursif, 8(1), 11–22.

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains Dan Komputer, 2(1), 163–171.

https://doi.org/10.47709/jpsk.v2i01.1390

Aziz, Nur. (2022). ANALISIS PERANCANGAN SISTEM INFORMASI. Edited by Wahyuni, Neneng S. Widina Media Utama. 1st ed. ed. Neneng Sri Wahuni. Bandung: Widina Bhakti Bandung.

Cristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (AES 128 Bit) untuk Mengamankan Data Keuangan. JIKOMSI (Jurnal Ilmu Komputer Dan Sistem Informasi), 4(2), 75–85. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181%0A

Gunawan, H., Budi, A. S., & Primananda, R. (2022). Penerapan Algoritma Diffie- Hellman Key Exchange dalam Komunikasi Data Antarnode pada Wireless Sensor Network. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer (J-PTIIK), 6(1), 197–203. Fakultas Ilmu Komputer, Universitas Brawijaya.

Haji, B. T. A. (2020). Pengertian Implementasi. LAPORAN AKHIR, 31. Hidayatulloh, N. W., dkk. (2023). Mengenal Advance Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data. Digital Transformation Technology (Digitech), 3(1), 1–10.

Kadir. 2021 . "Algoritma: Journal Of Mathematcs". Fakultas Ilmu Pendidikan UIN Syarif Hidayatullah Jakarta. Vol. III.

Lie, I. R., & Alamsyah, D. (2023). Penerapan Algoritma Diffie-Hellman pada Steganografi Least Significant Bit. MDP Student Conference 2023, Universitas Multi Data Palembang. E-ISSN: 2985-7406.

Mhatre, S., Khatode, O., Thakre, S., & Karche, S. (2024). Securing Text Files: A Comprehensive Study on AES and Diffie-Hellman Encryption. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 12(6), 2192–2199. https://doi.org/10.22214/ijraset.2024.63457

Rizka, M. (2021). Perpaduan Diffie Hellman dan Blowfish sebagai Sistem Keamanan Dokumen. Jurnal Infomedia: Teknik Informatika, Multimedia & Jaringan, 6(2), 86–90.

Sa'diyah, A. Z., Safitri, D., & Sujarwo. (2024). Implementasi pendidikan inklusif di SMP Negeri 259 Jakarta. Sindoro: Cendikia Pendidikan, 4(12), 51–60.

Sinambela, R. G., Fauzi, A., & Khair, H. (2024). Enhancing AES Key Generation Using Diffie-Hellman Method for Image Security. Journal of Artificial Intelligence and Engineering Applications, 3(3), 359–363. https://ioinformatic.org/

Sitepu, D. A., Nurhayati, & Khair, H. (2022). Implementasi Pengamanan Data Koperasi

Menggunakan Algoritma Advanced Encryption Standard (AES). Jurnal Ilmiah Kaputama (JIKA), 6(1), 49–58. https://citisee.amikompurwokerto.ac.id/assets/proceedings/paper/8 Amikom_Purwokerto_Implementasi _Pengamanan_Data_Koperasi_Menggunakan_Algoritma_Advanced_Encryption_Standard_(Aes).pdf

Tharisa amalia. (2020). Konsep dasar dalam mempelajari mata kuliah algoritma pemprograman. 1–23.

Ziliwu, K. B., Maslan, A., & Kremer, H. (2022). Implementasi Caesar Cipher pada Algoritma Kriptografi dalam Penyandian Pesan Whatsapp. Jurnal Comasie, 7(2), 117–125.