Implementasi Kriptografi pada Pemrograman Java Socket Menggunakan Mode ECB (Electronic Codebook)

Azi As'ari[1] Cut Muthia Ramadhani[2] Dini Berlian[3] Zatryandy Akbar[4] Linna Oktaviana Sari[5]
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Riau, Kota Pekanbaru, Provinsi Riau, Indonesia[1,2,3,4,5]
Email: azi.asari6364@student.unri.ac.id[1] cut.muthia0257@student.unri.ac.id[2]
dini.berlian4933@student.unri.ac.id[3] zatryandy.akbar4664@student.unri.ac.id[4]
linnaoasari@lecturer.unri.ac.id[5]

Abstrak
Kriptografi adalah salah satu metode penting dalam menjaga keamanan komunikasi data di lingkungan jaringan. Pemrograman socket Java merupakan teknologi yang sering digunakan untuk komunikasi jaringan, namun seringkali rentan terhadap serangan keamanan. Dalam jurnal ini, kami menginvestigasi dan mengimplementasikan teknik kriptografi pada pemrograman socket Java untuk meningkatkan tingkat keamanan komunikasi data. Kami memaparkan penggunaan algoritma kriptografi seperti AES (Advanced Encryption Standard) untuk mengenkripsi data yang dikirim melalui koneksi socket. Selain itu, juga dianalisis performa aplikasi setelah penerapan kriptografi dan dampaknya terhadap kecepatan dan keamanan komunikasi. Hasil eksperimen menunjukkan bahwa implementasi kriptografi pada pemrograman socket Java mampu meningkatkan keamanan komunikasi data tanpa mengorbankan performa yang signifikan. Temuan ini dapat menjadi panduan bagi pengembang yang ingin meningkatkan keamanan komunikasi data dalam aplikasi Java socket mereka.
Kata Kunci: Kriptografi, Pemrograman Java Socket, Keamanan Jaringan, Enkripsi Data, AES

PENDAHULUAN

Dalam era digital saat ini, keamanan informasi menjadi aspek yang sangat penting dalam mengamankan komunikasi dan pertukaran data melalui jaringan. Kriptografi, sebagai cabang ilmu yang berfokus pada pengamanan informasi, memegang peran krusial dalam upaya tersebut. Kriptografi memungkinkan kita untuk mengenkripsi data sehingga hanya pihak yang memiliki kunci rahasia yang dapat membacanya. Dalam konteks pengembangan perangkat lunak dan komunikasi jaringan, penggunaan socket pada bahasa pemrograman Java merupakan fondasi utama dalam memfasilitasi pertukaran data antar sistem. Namun, seringkali keamanan informasi yang dikirim melalui socket menjadi tantangan yang perlu diatasi. Pada titik inilah implementasi kriptografi pada pemrograman Java socket menjadi sangat relevan. Dengan mengintegrasikan teknik-teknik kriptografi, seperti enkripsi dan dekripsi, ke dalam penggunaan socket, kita dapat memastikan bahwa data yang dikirimkan antar sistem tetap terlindungi dari akses yang tidak sah. Dalam penelitian ini, kami akan menjelajahi konsep dan teknik implementasi kriptografi pada pemrograman Java socket. Kami akan membahas berbagai algoritma enkripsi yang dapat digunakan, serta memberikan contoh implementasi praktis untuk memperkuat keamanan komunikasi melalui socket.

METODE PENELITIAN

Penelitian ini bertujuan untuk memperkuat dan meningkatkan keamanan data antara Server dan Client, dengan tujuan utama mencegah kebocoran atau akses tidak sah oleh pihak yang tidak berwenang. Dalam rangka mencapai tujuan ini, penelitian ini mengadopsi

pendekatan gabungan antara Metode Eksperimental dan Metode Kualitatif. Metode Eksperimental dipilih untuk mengukur dan membandingkan kinerja implementasi kriptografi pada pemrograman Java Socket dengan mode operasi ECB. Pendekatan ini melibatkan perencanaan eksperimen yang cermat, pengumpulan data sistematis, dan analisis hasil secara statistik. Fokus utama dari eksperimen ini adalah mengevaluasi efektivitas kriptografi dalam melindungi data selama transmisi antara Server dan Client. Di samping Metode Eksperimental, Metode Kualitatif juga diadopsi untuk memahami perspektif pengembang atau pengguna terhadap implementasi kriptografi pada pemrograman Java Socket dengan mode operasi ECB. Pendekatan ini mencakup penggunaan wawancara dan analisis konten untuk mendapatkan wawasan yang lebih mendalam mengenai faktor-faktor kualitatif yang dapat mempengaruhi pengalaman dan persepsi terkait keamanan data. Dengan menggabungkan keduanya, penelitian ini diharapkan dapat memberikan pemahaman komprehensif tentang efektivitas kriptografi dalam konteks Java Socket dengan mode operasi ECB, tidak hanya dari segi kinerja teknis tetapi juga dari perspektif pengguna. Hasil penelitian ini diharapkan dapat memberikan panduan dan rekomendasi yang berharga untuk pengembangan sistem keamanan data yang lebih robust dan dapat diandalkan dalam lingkungan pemrograman Java Socket.

HASIL PENELITIAN DAN PEMBAHASAN

Kriptografi adalah bidang ilmu pengetahuan yang mempelajari pemakaian persamaan matematika untuk melakukan proses penyandian data (Onno, 2000). Kriptografi bertujuan untuk mengamankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak untuk mengetahui isi data tersebut. Dengan teknik atau algoritma tertentu yang disebut proses enkripsi (encrypt), data diubah menjadi data sandi yang bentuknya berbeda dengan data aslinya. Orang yang berhak menerima data akan mengetahui algoritma dan memiliki kunci untuk mengembalikan data sandi menjadi bentuk data aslinya, proses ini disebut dekripsi (decrypt). Bentuk data sandi diperlukan pada saat proses penyimpanan atau proses pengiriman data. Dalam Penelitian ini Membahas implementasi sistem keamanan pada komunikasi antara server dan klien menggunakan Java Socket Programming serta Java Cryptography Extension (JCE). Pada implementasi ini, digunakan algoritma Advanced Encryption Standard (AES) dalam mode *Electronic Codebook* (ECB) dengan padding PKCS5 untuk mengamankan data yang dikirimkan antara server dan klien.

Pertama-tama, pada sisi server, dibangun sebuah server socket yang mendengarkan koneksi pada port tertentu (di sini menggunakan port 12345). Setiap kali ada klien yang terhubung, server menghasilkan kunci acak menggunakan *KeyGenerator* dengan panjang kunci 128 bit. Kunci ini kemudian dikirimkan ke klien menggunakan ObjectOutputStream. Setelah itu, server dan klien menggunakan kunci yang sama untuk inisialisasi objek Cipher guna enkripsi dan dekripsi pesan yang dikirim. Pada sisi klien, setelah terhubung ke server, kunci rahasia diterima melalui ObjectInputStream. Kunci ini kemudian digunakan untuk inisialisasi Cipher pada klien. Selanjutnya, implementasi ini menggunakan dua thread terpisah untuk mengelola pembacaan (clientReadThread) dan pengiriman pesan (clientSendThread) agar dapat melakukan komunikasi secara simultan. Dalam implementasi ini, pesan yang dikirimkan antar klien dan server dienkripsi menggunakan kunci yang sama. Setiap pesan yang dikirim diubah menjadi byte array dan dienkripsi sebelum dikirim, dan setelah diterima oleh penerima, pesan tersebut didekripsi untuk mendapatkan kembali isi pesan asli. Selain itu, program juga mencakup fitur *EXIT*, yang memungkinkan klien untuk meminta keluar dari koneksi dengan server. Hal ini diimplementasikan dengan mengirimkan pesan terenkripsi "EXIT" kepada server, dan jika server menerima pesan ini, maka koneksi akan ditutup. Dengan implementasi ini, data yang dikirimkan antar klien dan server dapat dilindungi dari akses yang tidak sah

karena hanya pihak yang memiliki kunci rahasia yang dapat melakukan enkripsi dan dekripsi pesan. Meskipun demikian, perlu diperhatikan bahwa pada implementasi ini, mode ECB digunakan, yang memiliki beberapa kekurangan dalam konteks keamanan tertentu. Sebaiknya, mode operasi lain seperti Cipher Block Chaining (CBC) dapat diimplementasikan untuk meningkatkan keamanan komunikasi.

KESIMPULAN

Secara keseluruhan, penelitian ini telah berhasil mengimplementasikan sistem keamanan pada komunikasi antara server dan klien menggunakan Java Socket Programming dan Java Cryptography Extension (JCE). Melalui penggunaan algoritma Advanced Encryption Standard (AES) dalam mode Electronic Codebook (ECB) dengan padding PKCS5, data yang dikirimkan antara kedua entitas berhasil diamankan. Pada sisi server, sebuah server socket dibangun untuk mendengarkan koneksi pada port tertentu, dan setiap klien yang terhubung menerima kunci acak melalui ObjectOutputStream. Server dan klien selanjutnya menggunakan kunci yang sama untuk menginisialisasi objek Cipher guna proses enkripsi dan dekripsi pesan. Di sisi client, kunci rahasia diterima setelah terhubung ke server, dan dua thread terpisah diterapkan untuk mengelola pembacaan dan pengiriman pesan secara simultan. Selain itu, implementasi ini memasukkan fitur EXIT yang memungkinkan klien untuk keluar dari koneksi dengan mengirimkan pesan terenkripsi "EXIT" kepada server. Meskipun implementasi ini berhasil melindungi data dari akses yang tidak sah karena memerlukan kunci rahasia untuk enkripsi dan dekripsi, perlu dicatat bahwa mode ECB digunakan, yang memiliki kekurangan tertentu dalam konteks keamanan. Disarankan untuk mempertimbangkan penggunaan mode operasi lain seperti Cipher Block Chaining (CBC) guna meningkatkan tingkat keamanan komunikasi secara keseluruhan.

DAFTAR PUSTAKA

Ashari Arief. (2016). "Implementasi Algoritma Kriptografi Rsa-Crt Pada Aplikasi Instant Messaging". Universitas Diponegoro,6-7.

Badia Nommensen. (2020). "Pembangunan Aplikasi Pengiriman File Menggunakan Pemrograman Socket Pada Perusahaan Consulting Informatics Technology". Universitas Atma Jaya Yogyakarta,11-13.

Cahyadi, Tri. (2012). "Implementasi Steganografi. LSB dengan Enkripsi Vigenere Chiper pada Citra. Jpeg, Transient". ISSN: 2302-9927,44

Suhardi,03, Nomor 2, (2016). “Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-Or (XOR)”, *23*. https://media.neliti.com/media/publications/225742-aplikasi-kriptografi-data-sederhana- deng-6c1845f6.pdf

Yogi Adytia Marsal,Dr. Ir. Rinaldi Munir, M.T Pemanfaatan Konsep Kriptografi Visual untuk membangun Java API Pengamanan Perangkat Lunak, 2-4. informatika.stei.itb.ac.id/~rinaldi.munir/TA/Makalah_TA Yogi Aditya Marsal.pdf