JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 4, September Tahun 2024
ISSN 3025-0919 (media online)
Hal 597-601

Keamanan Bahasa Pemrograman Java Dengan Implementasi Kriptografi AES

Andika Bintang Ramadhan[1*], Faturohman[2], Rhaka Dirgantara[3], Muhammad Ramzi[4], Ines Heidiani Ikasari[5]

[1]Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Kota Tanggerang, Indonesia
Email: [1*]ramadhanandikabintang@email.com, [2]fathurree20022@email.com, [3]ramzi140205@gmail.com, [4]rakadirgantara@gmail.com, [5]inesheidianii@gmail.com
(* : coressponding author)

Abstrak − Keamanan adalah hak asasi bagi setiap individu. Setiap orang berhak mendapatkan perlindungan yang memadai, termasuk keamanan pribadi, identitas, dan lainnya. Demikian pula di dunia teknologi, setiap individu berhak memiliki keamanan yang terjamin di dunia internet, termasuk perlindungan data pribadi dan riwayat aktivitas online. Dalam hal pengiriman pesan, data pesan berhak dijaga kerahasiaannya melalui proses enkripsi dan dekripsi, yang merupakan langkah penting untuk melindungi informasi dari kebocoran. Penggunaan enkripsi dan dekripsi adalah solusi untuk mencegah akses oleh pihak yang tidak berwenang, dan Algoritma Kriptografi AES adalah salah satu metode yang aman untuk proses ini. Algoritma ini digunakan untuk enkripsi dan dekripsi data atau pesan. Penggunaan kriptografi diharapkan dapat menjaga kerahasiaan data yang sensitif. Implementasi ini akan dilakukan menggunakan bahasa pemrograman Java, dengan harapan dapat memberikan keamanan yang lebih baik untuk data atau pesan.

Kata Kunci: Kriptografi AES; Data/Pesan; Enkripsi dan Dekripsi; Pemograman Java

Abstract *− Security is a fundamental right for every individual. Every person deserves adequate protection, including personal security, identity security, and more. Similarly, in the realm of technology, individuals are entitled to secure experiences on the internet, including the protection of personal data and online activity history. In terms of messaging, message data deserves to be kept confidential through encryption and decryption processes, which are crucial steps to prevent data leakage. The use of encryption and decryption is a solution to protect confidential data/messages from unauthorized access, with the AES Cryptographic Algorithm being one of the secure algorithms for this purpose. This algorithm is used for the encryption and decryption of data/messages. The application of cryptography is expected to maintain the confidentiality of sensitive data. This implementation will use the Java programming language, aiming to provide better security for data/messages.*

Keywords*: AES Cryptography; Data/Message; Encryption and Decryption; Java Programming*

1. PENDAHULUAN

Dalam era di mana data memiliki nilai tinggi dan sering disimpan serta dikirim melalui jaringan yang rentan, melindungi data menjadi sangat penting. Keamanan data atau pesan yang bersifat rahasia merupakan layanan yang bertujuan untuk memastikan informasi tersebut tersimpan dengan aman dan tidak dapat diakses atau dibaca oleh pihak yang tidak berwenang. Keamanan data adalah hak dasar yang harus dimiliki oleh setiap individu.

Advanced Encryption Standard (AES) dikenal sebagai salah satu metode enkripsi yang sangat efektif, berkat kemampuannya memproses data dengan cepat dan ketahanannya yang luar biasa terhadap berbagai serangan kriptografi modern. Teknologi ini telah menjadi pilihan utama dalam berbagai aplikasi yang membutuhkan tingkat keamanan tinggi, baik dalam penyimpanan maupun transmisi data. Dengan menggunakan AES, kebutuhan akan perlindungan data yang kuat dan handal dapat terpenuhi, menjadikannya solusi ideal untuk menjaga kerahasiaan informasi dalam era digital yang semakin kompleks dan berisiko.

Penelitian ini bertujuan untuk mengembangkan aplikasi yang sangat aman dari serangan peretas yang sering mencuri data melalui internet. Aplikasi ini akan menggunakan algoritma kriptografi AES untuk melindungi data dengan cara mengenkripsi dan mendekripsi informasi sensitif, sehingga mencegah akses yang tidak sah dan memastikan keamanan selama data tersebut berada dalam berada dalam perjalanan melalui jaringan.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 4, September Tahun 2024
ISSN 3025-0919 (media online)
Hal 597-601

Bahasa Pemrograman Java

Java adalah bahasa pemrograman yang dapat dijalankan di berbagai perangkat komputer. Biasanya, Java digunakan untuk membuat dan menjalankan perangkat lunak baik secara standalone maupun dalam lingkungan jaringan. Selain itu, Java sering dimanfaatkan untuk mengembangkan bagian back-end dari perangkat lunak, aplikasi Android, serta berbagai situs web.

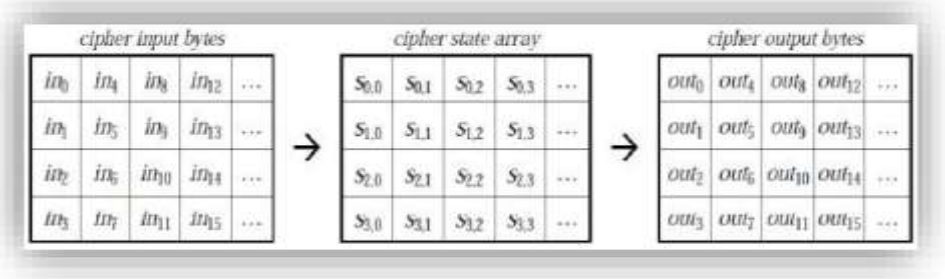
Cryptography AES (*Advance Encryption Standard*)

Kriptografi adalah proses mengubah pesan untuk menjaga kerahasiaannya. Tujuan dari kriptografi adalah menyembunyikan pesan atau data sehingga informasi tetap rahasia. Pesan yang telah diubah ini tidak dapat dibaca oleh pihak yang tidak berwenang, sehingga informasi pesan atau data tetap aman. Ada empat tujuan utama kriptografi, yaitu kerahasiaan (*confidentiality*), tidak dapat dipungkiri (*non-repudiation*), otentikasi (*authentication*), dan integritas (*integrity*). Dalam penelitian ini, penulis menggunakan Algoritma Kriptografi AES, yang merupakan salah satu algoritma block cipher dan menggunakan kunci simetri dalam proses enkripsi dan dekripsi pesan. Algoritma AES memiliki berbagai ukuran kunci, yaitu 128-bit, 192-bit, dan 256-bit. Perbedaan dari ketiga ukuran kunci tersebut terletak pada panjang kunci dan jumlah putaran (*round*).

Tabel 1. Jumlah *Round* AES

Tipe	Jumlah Key (Nk)	Besar Blok (Nb)	Jumlah Round (Nr)
AES-128	4	4	10
AES-192	6	4	12
AS-256	8	4	14

Operasi AES melibatkan manipulasi data pada sebuah array dua dimensi yang dikenal sebagai state. State ini memiliki ukuran Nrows x Ncols. Proses enkripsi dimulai dengan penyalinan data in0, in2, in3, in4, in5, in6, in7, in8, in9, in10, in11, in12, in13, in14, in15 ke dalam array state. Data yang terdapat dalam state ini kemudian mengalami serangkaian transformasi kriptografis sesuai dengan algoritma AES selama proses enkripsi dan dekripsi. Ilustrasi visual dari proses ini dapat ditemukan pada gambar berikut.



Gambar 1. Proses Input Dan Output Bytes

2. METODE

2.1 Mencari Referensi Jurnal Yang Relevan

Dalam metode penelitian ini, peneliti mengadopsi pendekatan yang didasarkan pada pengumpulan referensi jurnal yang relevan dengan topik kriptografi AES dalam konteks bahasa pemrograman Java. Referensi jurnal dipilih dengan teliti untuk memastikan keakuratan dan kedalaman informasi yang diperlukan. Setelah referensi jurnal yang tepat diidentifikasi, peneliti melakukan pembacaan mendalam terhadap setiap artikel, mengeksplorasi berbagai aspek dari proses

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 4, September Tahun 2024
ISSN 3025-0919 (media online)
Hal 597-601

enkripsi dan dekripsi, penggunaan kunci simetris, hingga implementasi algoritma AES dalam konteks pemrograman Java.

2.2 Analisis Poin-Poin Penting

Pada tahap berikutnya, poin-poin krusial yang ditemukan dari jurnal-jurnal tersebut diekstraksi dan diintegrasikan ke dalam kerangka studi penelitian ini. Penelitian ini tidak hanya mengandalkan pada pemahaman teoritis dari referensi jurnal, tetapi juga mempertimbangkan aplikasi praktis dari konsep-konsep yang dipelajari. Dengan demikian, pendekatan ini menyediakan landasan yang kokoh untuk membangun pemahaman yang holistik dan mendalam mengenai implementasi kriptografi AES dalam bahasa pemrograman Java.

3. ANALISA DAN PEMBAHASAN

3.1 Implementasi Dan Integrasi

Analisis masalah mengenai implementasi dan integrasi AES (*Advanced Encryption Standard*) dalam konteks penggunaan praktis dan integrasi sistem dapat mencakup beberapa aspek penting sebagai berikut:

a. Integrasi Dengan Aplikasi Java: AES harus diintegrasikan dengan baik ke dalam aplikasi java yang sudah ada atau sedang dikembangkan. Ini termasuk memastikan bahwa proses enkripsi dan dekripsi berjalan lancar, aman, dan tidak mempengaruhi kinerja aplikasi secara siginifikan.

b. Uji Coba Dan Validasi: sebelum menerapkan kedalam produksi, implementasi AES dalam Java perlu diuji coba secara menyeluruh untuk memastikan keamanan dan kehandalan. Uji coba mencakup pengujian terhadap serangan kriptoanalisis, uji keamanan kunci, dan pengujian integrasi dengan infrastruktur aplikasi yang lebih luas.

3.2 Performa Dan Efisiensi

Performa dan Efisiensi kriptografi AES dalam Java sangat penting untuk memastikan bahwa sistem dapat beroperasi secara efektif dan responsif. Berikut adalah aspek yang harus dipertimbangkan:

a. Optimalisasi Kode: Pengoptimalan implementasi AES dalam Java adalah penting untuk meningkatkan performa dan efisiensi. Hal ini mencakup penggunaan teknik_teknik pemrograman yang efisien, seperti penggunaan algoritma yang tepat, pengaturan buffer yang efektif, dan penggunaan struktur data yang sesuai.

b. Perbandingan Dengan Alternatif: Performa AES dalam Java perlu dibandingkan dengan alternatif kriptografi simestris lainnya untuk mengevaluasi keunggulan dan kelemahan relatif. Contohnya, *Bandwith* dan Overload enkripsi dapat mempengaruhi kinerja dalam hal penggunaan data.

3.3 Kelebihan Dan Kelemahan Kriptografi AES

Kriptografi AES (*Advance Encryption Standard)* dalam Java memiliki sejumlah kelebihan dan kelemahan yang perlu dipertimbangkan dalam implementasi aplikasi keamanan. Berikut adalah kelebihan dan kekurangan AES dalam Java:

a. Kelebihan AES:
   1. Keamanan yang tinggi
   2. Performa yang baik
   3. Standart Internasional
   4. Dukungan dan Integrasi

b. Kelemahan AES
   1. Kekhawatiran tentang keamanan sistem

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 4, September Tahun 2024
ISSN 3025-0919 (media online)
Hal 597-601

2. Pemrosesan Paralel
3. Kompleksitas Implementasi
4. Kebutuhan untuk manajemen kunci yang aktif

4. KESIMPULAN

Implementasi AES dalam aplikasi Java memerlukan integrasi yang cermat untuk memastikan bahwa proses enkripsi dan dekripsi beroperasi dengan lancar dan aman. Adalah penting untuk melakukan pengujian menyeluruh sebelum aplikasi dijalankan secara resmi guna menguji keamanan dan kehandalan sistem, termasuk uji terhadap serangan kriptoanalisis serta integrasi dengan infrastruktur aplikasi yang luas. Optimalisasi kode implementasi AES menjadi krusial untuk meningkatkan performa dan efisiensi, dengan menerapkan teknik-teknik pemrograman efisien seperti pemilihan algoritma yang tepat dan manajemen buffer yang efektif. Selain itu, perlu dilakukan perbandingan dengan alternatif kriptografi simetris lainnya untuk mengevaluasi keunggulan relatif dalam penggunaan bandwidth dan overhead enkripsi.

AES menawarkan tingkat keamanan tinggi, performa yang baik, serta merupakan standar internasional dengan dukungan dan integrasi yang solid dalam lingkungan Java. Namun, implementasi AES juga menimbulkan kekhawatiran terkait keamanan sistem, kompleksitas dalam implementasi, dan tantangan dalam pemrosesan paralel. Pengelolaan kunci yang efektif juga sangat penting untuk memastikan keamanan keseluruhan implementasi.

Dengan pemahaman yang mendalam terhadap kelebihan dan kelemahan ini, pengembang dapat mengambil langkah-langkah yang tepat untuk mengimplementasikan AES dengan efektif dan aman dalam aplikasi keamanan mereka.

REFERENCES

Ahmad Azis Iqbal Ramadhan, Ellena Zahrah Rivanti, Rizky Syahrial Zulva. (2023). Implementasi Kriptografi AES Menggunakan Bahasa Java Programming: Meningkatkan Keamanan Data Melalui Emkripsi & Dekripsi YangKuat.. TRIPLE A : Jurnal Pendidikan Teknologi Informasi, 2(1), 1-7. https://jurnal.umj.ac.id/index.php/TripleA/article/view/17513/9646

Nur Wachid Hidayatulloh, Muhlis Tahir, Husnul Amalia. (2023). Menegenal Advance Encryption Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data. Digital Transformation Technology (Digitech), 3(1), 1-6. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://jurnal.itscience.org/index.php/digitech/article/download/2293/1755/9486&ved=2ahUKEwjyyNfqk4GHAxUC7zgGHb9zAWMQFnoECB4QAQ&usg=AOvVaw1J4IfEfbjzmEi6glTVD9fy

Lilik Asih Indrayani, I Made Suartana. (2019). Implementasi Kriptografi Dengan Modifikasi Algoritma Advance Encryption Standard (AES) Untuk Pengamanan File Document. JINACS, 1(1), 1-6. https://ejournal.unesa.ac.id/index.php/jinacs/article/view/29450

Anggraeni Eka Putri, Aghistina Kartikadewi, Lina Audina Abdul Rosyid. (2020). Implementasi Kriptografi Dengan Algoritma *Advanced Encryption Standard* (AES) 128 Bit Dan Steganografi Menggunakan Metode End Of File (EOF) Berbasis Java Desktop Pada Dinas Pendidikan Kabupaten Tangerang. AISM, 3(2), 1-9. https://journal.uinjkt.ac.id/index.php/aism/article/view/14722/pdf

Niolinda Cristy, Friati Riandari. (2021). Implementasi Metode *Advanced Encryption Standard* (AES 128 Bit) Untuk Mengamankan Data Keuangan. JIKOMSI, 4(1), 1-11. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181

Muhammad Azhari, Dadang Iskandar Mulyana, Faisal Joko Perwitosari, Frihan Ali. (2022). Implementasi Pengamanan Data Pada Dokumen MenggunakanAlgoritma Kriptografi *Advanced Encryption Standard*(AES). Jurnal Pendidikan Sains Dan Komputer, 2(1), 1-9. https://jurnal.itscience.org/index.php/jpsk/article/view/1390

Eko Hartato, Indra Gunawan, Iin Parlina Solikhum. (2020). Analisis Algoritma AES Dalam Mengamankan Data Pada Kantor Walikota Pematangsiantar. Jurnal Ilmiah Informatika, 8(1), 1-7. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://ejournal.upbatam.ac.id/index.php/jif/article/download/1799/1030/6154&ved=2ahUKEwiQk4fPlYGHAxUExTgGHWLmB6EQFnoECCEQAQ&usg=AOvVaw0x88IAPVOFhAEB77CLPWQO

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 2, No. 4, September Tahun 2024
ISSN 3025-0919 (media online)
Hal 597-601

Dhiya Calista, Al Farissi, Mastura Diana Marieska. (2021). Sistem Pengamanan Data Menggunakan Kriptografi AESdan Blockchain Berbasis Android. Jurnal JUPITER, 13(2), 1-7. https://jurnal.polsri.ac.id/index.php/jupiter/article/download/3927/1674