e-ISSN 2962-0651
JURNAL KOMPUTER

Penggunaan Kriptografi Asimetris Dalam Pengamanan Komunikasi IOT

Dhika Alfatah[1)]
[1)]***STIA Bengkulu, Indonesia***
Email: [1)] dhika@gmail.com

Abstrak

Internet of Things (IoT) telah berkembang pesat dan menjadi bagian penting dalam berbagai sektor, mulai dari industri, kesehatan, hingga rumah tangga. Namun, pertumbuhan ini juga meningkatkan risiko keamanan, terutama terkait komunikasi data antar perangkat. Salah satu solusi yang menjanjikan adalah penerapan kriptografi asimetris, yang menawarkan mekanisme enkripsi dan dekripsi menggunakan pasangan kunci publik dan privat. Artikel ini membahas bagaimana kriptografi asimetris dapat diterapkan dalam sistem IoT untuk menjaga kerahasiaan, integritas, dan otentikasi data. Selain itu, dianalisis pula tantangan implementasi seperti keterbatasan daya komputasi dan konsumsi energi pada perangkat IoT, serta solusi yang dapat diterapkan untuk mengatasinya. Studi ini menunjukkan bahwa meskipun terdapat hambatan teknis, penggunaan kriptografi asimetris tetap relevan dan efektif sebagai lapisan perlindungan dalam ekosistem IoT yang semakin kompleks.

Kata kunci: *Internet Of Things, Kriptografi Asimetris, Keamanan Data, Komunikasi IOT, Enkripsi*

Use Of Asymmetric Cryptography In Securing IOT Communication

Abstract

The Internet of Things (IoT) has grown rapidly and become an important part of many sectors, from industry to healthcare to households. However, this growth also increases security risks, especially regarding data communication between devices. One promising solution is the implementation of asymmetric cryptography, which offers encryption and decryption mechanisms using public and private key pairs. This article discusses how asymmetric cryptography can be applied in IoT systems to maintain data confidentiality, integrity, and authentication. In addition, implementation challenges such as limited computing power and energy consumption in IoT devices are analysed, as well as solutions that can be applied to overcome them. This study shows that despite technical barriers, the use of asymmetric cryptography remains relevant and effective as a layer of protection in an increasingly complex IoT ecosystem.

Keywords: *Internet Of Things, Asymmetric Cryptography, Data Security, IOT Communication, Encryption*

PENDAHULUAN

Keamanan penting dalam penyimpanan dan pengiriman informasi atau pesan. Keamanan dapat didefinisikan sebagai proses, prosedur, dan kebijakan yang dipakai untuk menutup akses yang tidak sah. Memecahkan masalah, mengekspos, mengganggu, dan mengganti sumber daya jaringan komputer . Dalam hal ini perlu diperhatikan bahwa keamanan sistem informasi harus dijaga kerahasiaannya agar informasi siap diterima oleh penerima dan dapat dikirim dengan cara yang dirahasiakan oleh orang lain yang tidak berwenang . Ini hanya boleh dibaca oleh penerima dan dapat dirahasiakan oleh pengirim. Ada cabang ilmu yang mempelajari privasi data atau informasi, yaitu kriptografi. Ilmu yang digunakan untuk memanipulasi data atau informasi dengan cara yang tidak dapat diuraikan. Itu dapat direproduksi sebagai informasi atau data disebut kriptografi. Kriptografi sendiri terbagi menjadi dua jenis, kriptografi simetris dan kriptografi asimetris . Enkripsi kunci simetris yaitu memakai kunci enkripsi yang sama dengan kunci dekripsi]. Contohnya adalah algoritma DES (Data Encryption Standard), blowfish, twofish, MARS, IDEA,

3DES (DES diaplikasikan 3 kali), AES (Advanced Encryption Standard) yang bernama asli Rijndael [8], untuk enkripsi kunci asimetris yaitu memakai kunci enkripsi yang berbeda dengan kunci enkripsi. Contohnya adalah algoritma RSA (Riverst Shamir Adleman) dan ECC (Elliptic Curve Cryptography) [9]. Masing-masing jenis kriptografi ini memiliki kelebihan dan kelemahan yang berbeda dalam konteks meningkatkan keamanan sistem informasi.

Oleh karena itu, tujuan dari penelitian ini adalah untuk melakukan analisis perbandingan antara algoritma kriptografi simetris dan asimetris dalam upaya meningkatkan keamanan sistem informasi. Penelitian ini akan menjelajahi berbagai aspek, termasuk efisiensi, kecepatan, dan keamanan masing-masing jenis kriptografi, serta bagaimana mereka dapat diterapkan dalam berbagai skenario penggunaan. Hasil penelitian ini diharapkan akan memberikan pandangan yang lebih mendalam tentang peran dan relevansi kriptografi dalam melindungi informasi sensitif di dunia digital saat ini.

LANDASAN TEORI

Internet of Things (IoT)

Internet of Things (IoT) adalah konsep di mana objek fisik dilengkapi dengan sensor, perangkat lunak, dan konektivitas jaringan yang memungkinkan mereka mengumpulkan dan bertukar data. IoT telah banyak diterapkan di berbagai bidang seperti smart home, industri (IIoT), transportasi, dan kesehatan. Komunikasi antar perangkat dalam jaringan IoT bersifat otomatis dan berlangsung secara terus-menerus, sehingga sangat rentan terhadap ancaman keamanan seperti penyadapan, manipulasi data, dan akses tidak sah.

Keamanan Komunikasi IoT

Dalam sistem IoT, keamanan komunikasi menjadi aspek penting untuk menjaga **kerahasiaan (confidentiality)**, **integritas (integrity)**, dan **otentikasi (authentication)** data yang ditransmisikan antar perangkat. Kelemahan dalam sistem keamanan dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengakses, memodifikasi, atau bahkan menghancurkan data. Oleh karena itu, mekanisme pengamanan komunikasi yang kuat dan efisien sangat diperlukan dalam implementasi IoT .

Kriptografi

Kriptografi merupakan ilmu dan seni dalam menjaga keamanan informasi dengan cara mengubah data menjadi bentuk yang tidak dapat dipahami tanpa pengetahuan khusus, seperti kunci kriptografi. Tujuan utama kriptografi adalah untuk memastikan kerahasiaan, integritas, otentikasi, dan non-repudiation .

Kriptografi Asimetris

Kriptografi asimetris adalah salah satu jenis kriptografi yang menggunakan dua kunci berbeda namun saling terkait, yaitu kunci publik (public key) dan kunci privat (private key). Kunci publik digunakan untuk mengenkripsi pesan, sementara kunci privat digunakan untuk mendekripsi pesan tersebut . Contoh algoritma kriptografi asimetris yang umum digunakan adalah RSA (Rivest-Shamir-Adleman) dan ECC (Elliptic Curve Cryptography). Kelebihan kriptografi asimetris terletak pada kemampuannya untuk mendukung komunikasi yang aman tanpa perlu membagikan kunci secara langsung, sehingga sangat cocok untuk lingkungan seperti IoT yang melibatkan banyak perangkat dengan tingkat kepercayaan yang berbeda.

Tantangan Implementasi Kriptografi Asimetris dalam IoT

Meskipun kriptografi asimetris menawarkan keamanan yang tinggi, implementasinya dalam perangkat IoT memiliki tantangan tersendiri. Perangkat IoT umumnya memiliki keterbatasan dalam hal daya komputasi, kapasitas memori, dan konsumsi energi. Oleh karena itu, dibutuhkan algoritma yang ringan (lightweight) namun tetap aman agar dapat diterapkan secara efektif dalam lingkungan IoT. Penelitian dan pengembangan algoritma kriptografi asimetris yang efisien dan ramah terhadap perangkat dengan sumber daya terbatas menjadi hal yang sangat penting untuk mendukung pertumbuhan ekosistem IoT yang aman.

METODE PENELITIAN

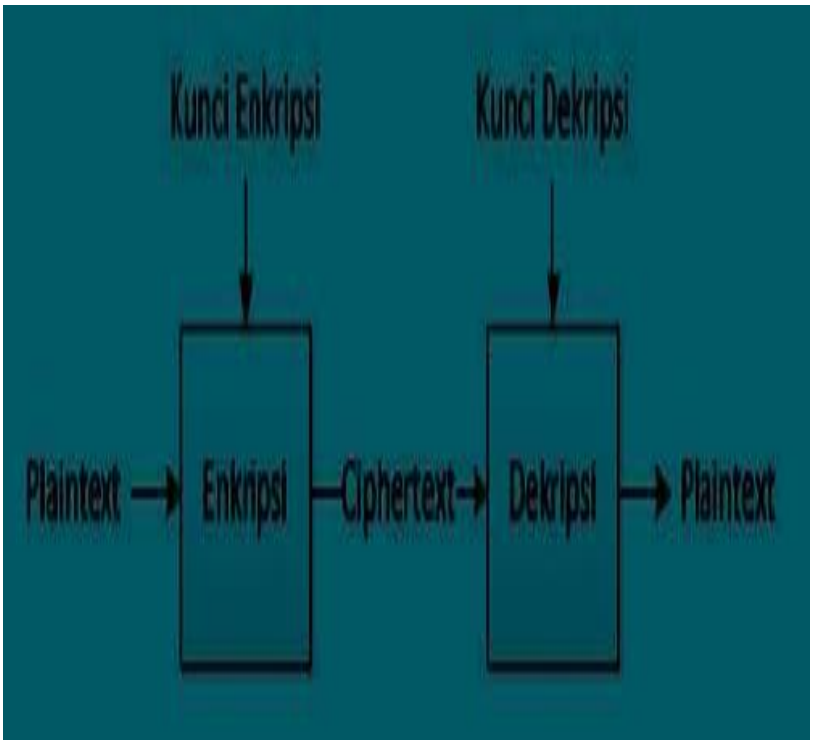
Pada penelitian jurnal ini, menggunakan metode internet searching yang merupakan teknik pengumpulan data melalui bantuan teknologi yang berupa alat atau mesin pencari di internet dimana segala informasi dari berbagai era tersedia didalamnya. Selain intenet searching, pengamatan tentang

e-ISSN 2962-0651
JURNAL KOMPUTER

kriptografi dan penerapannya terhadap keamanan data juga dilakukan dengan metode pendekatan Studi Pustaka. Studi Pustaka yaitu merupakan teknik pengumpulan data dengan mempelajari berbagai buku referensi serta hasil penelitian yang sudah ada sebelumnya yang sejenis, yang berguna untuk mendapatkan landasan teori mengenai masalah-masalah yang akan diteliti.

HASIL DAN PEMBAHASAN

Kata kriptografi (cryptography) berasal dari bahasa Yunani yaitu Kryptos (tersembunyi atau rahasia) dan Graphein (menulis atau tulisan). Sehingga dapat dijabarkan bahwa secara harfiah makna kriptografi adalah menulis secara tersembunyi untuk menyampaikan pesan-pesan yang perlu dijaga kerahasiaannya. Kriptografi memiliki arti lain, yaitu suatu ilmu yang mempelajari tentang teknik-teknik matematika yang berkaitan dengan aspek keamanan informasi data atau keamanan pesan dengan menggunakan dua proses dasar kriptografi yaitu enkripsi dan deskripsi. Enkripsi dapat diartikan sebagai cipher atau kode, merupakan proses penyembunyian sebuah data pesan, dengan cara mengubah plaintext (Pesan yang bisa dibaca) menjadi ciphertext (Pesan acak yang tidak bisa dibaca). Sedangkan Deskripsi merupakan kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.
Proses Enkripsi/Dekripsi :



Gambar 1. Proses Enkripsi/Dekripsi

Kriptografi Klasik

Merupakan kriptografi yang digunakan sebelum atau sesudah penemuan komputer, tapi tidak sepopuler saat ini.. Kriptografi ini hanya melakukan pengacakan pada huruf A – Z dan tidak disarankan untuk mengamankan informasi penting karena mudah dipecahkan dalam kurun waktu yang singkat, Penggunaan kriptografi klasik memberikan prinsip untuk menjaga keamanan kunci itu sendiri.
Ciri-ciri :

- Berbasis karakter
- Menggunakan pena dan kertas
- Termasuk kedalam kiptografi kunci simetris Algoritma kriptografi klasik :

Substitution Ciphers

Merupakan penggantian setiap karakter dari plaintext dengan karakter lain dalam susunan abjad (alfabet). Substitusi pertama kali ada dalam dunia persandian pada masa pemerintahan yulius caesar dan dikenal dengan sebutan caesar cipher.

Misalnya pada Caesar Chiper, setiap huruf di substitusi dengan tiga huruf berikutnya. Maka dalam hal ini, kuncinya adalah pergeseran tiga huruf (kunci = 3).

Agar kriptanalis menjadi lebih sulit, Cipherteks dapat dikelompokkan kedalam kelompok n-huruf, misal kelompok 4-huruf :

VWLN RPWX QDVE DQJV DSHP DWDQ JVLD QWDU

Atau dengan membuang semua spasi :

VWLNRPWXQDVEDQJVDSHPDWDQJVLDQWDU

Dan jika dilakukan dekripsi pesan, akan kembali ke pesan aslinya.

Mengkodekan setiap huruf abjad dengan bilangan bulat (integer) ; A = 0, B = 1, …, Z = 25.

Menyandikan Plainteks (P) menjadi Chiperteks (C) :

$$C = E(P) = (\mathrm{p}i + k) \bmod 26$$

Menyandikan Chiperteks (C) menjadi Plainteks (P) :

$$P = D(P) = (\mathrm{c}i - k) \bmod 26$$

* pi : karakter ke-i dari Plainteks (P)
* ci : karakter ke-i dari Chiperteks (C)

Jenis-jenis substitution ciphers :

a. Monoalphabetic Cipher
   Cipher yang mengubah tiap huruf nya pada plainteks dengan huruf yang bersesuaian. Jumlah kemungkinan susunan huruf yang dapat dibuat adalah 26! = 403.291.461.126.605.635.584.000.000
b. Homophonic Substitution Cipher
   Pada tiap huruf plainteks dihubungkan kedalam salah satu huruf cipherteks.
c. Polyalphabetic Substitusion Cipher
   Pensubstitusian setiap huruf menggunakan kunci yang berbeda.
d. Polygram Substitution Cipher

Blok karakter disubstitusikan dengan blok cipherteks.

Transpotition Chiper

Teknik ini menggunakan permutasi karakter, dimana teknik ini memungkinkan pesan yang asli tidak dapat dibaca kecuali memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula atau disebut deskripsi.

Kriptografi Modern

Merupakan kriptografi yang cukup rumit. Dibutuhkan pengetahuan matematika untuk menguasainya. Oleh karena itu kriptografi modern berkembang bersamaan dengan berkembangnya komputer hingga jaman sekarang.

KESIMPULAN DAN SARAN

Penggunaan kriptografi sudah mulai banyak di gunakan dalam kehidupan sehari-hari. Saat mengakses informasi di Internet, gunakan sistem enkripsi untuk memastikan keamanan data. Hasilnya, data lebih terlindungi dari spam dan peretas ilegal. Saat ini Kriptografi bukan hanya dipakai untuk menulis atau pun menyelesaikan kode, tetapi kriptografi sudah berkembang ke berbagai macam fungsi seperti enkripsi/dekripsi untuk pengamanan data, otentikasi identitas dan pesan, tanda tangan dan sertifikat digital, protokol pertukaran kunci, uang digital, dan lain sebagainya.

e-ISSN 2962-0651
JURNAL KOMPUTER

DAFTAR PUSTAKA

R. Dea Mustika, A. Zakir, and A. Rizmi, “IMPLEMENTASI ALGORITMA K-MEANS UNTUK CLUSTERING JUDUL SKRIPSI UNIVERSITAS HARAPAN MEDAN,” *J. Media Inform.*, vol. 4, no. 1, pp.

S. P. Lestari, H. N. Fadlan, R. Angelia Purba, and I. Gunawan, “REALISASI KRIPTOGRAFI PADA FITUR ENKRIPSI END-TO-END PESAN WHATSAPP,” *J. Media Inform.*, vol. 4, no. 1, pp. 1–8, Nov. 2022

J. H. Sinaga, M. Pangaribuan, I. Rivaldo, and I. Gunawan, “Penerapan Enkripsi Dan Deskripsi Menggunakan Algoritma Data Encryption Standart (DES) Dengan Pemograman Matlab,” vol. 4, 2022.

P. A. M. Z. R.W.P.P.Zer and I. Gunawan, “Penerapan Data Mining Naïve Bayes Dalam Klasifikasi Kepuasan Mahasiswa Berlangganan WiFi Indihome,” *J. Media Inform.*, vol. 3, no. 2, pp. 112–118, Jun. 2022, doi: 10.55338/jumin.v3i2.488.

N. D. Farhanah, “Optimalisasi Penentuan Kinerja Perawat Terbaik di Klinik Amanah dengan Sistem Pendukung Keputusan dan Metode Simple Additive Weighting,” vol. 2, 2023.B. Sapriatin and F. A. Sianturi, “Penerapan Teorema Bayes Mendeteksi Stunting pada Balita,” vol. 3, 2021.

A. Suaib and I. I. Tritosmoro, “Perbandingan Performa Metode Local Binary Pattern dan Random Forest dalam Identifikasi COVID-19 pada Citra X-ray Paru-paru.,” vol. 2, 2023.D. E. Frans, “Peningkatan Produksi Budidaya Perikanan dengan Penerapan Algoritma Apriori dan Association Rule,” vol. 2, 2023.

N. Hafizar, E. R. Syahputra, and D. Irwan, “Desain Dan Penerapan Sistem Informasi Untuk Pemasaran Biji Kopi Dan Bubuk Kopi Arabika Berbasis Android,” vol. 4, 2022.

A. Simangunsong, R. M. Simanjorang, and H. Fahmi, “Penerapan Metode Composite Performance Index Dalam Seleksi Penerimaan Calon Laboran,” vol. 1, 2022.

Y. Yusfrizal, “Rancang Bangun Aplikasi Kriptografi pada Teks Menggunakan Metode Reverse Chiper,” J. Tek. Inform. Kaputama, Vol. 3, No. 2, hlm. 29–37, 2019.

D. R. Saragi, J. M. Gultom, J. A. Tampubolon, dan I. Gunawan, “Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4,” J. Sist.Komput.dan Inform., Vol.1, No.2, hal. 114, 2020, doi: 10.30865/json.v1i2.1745.

M. I. Afandi dan N. Nurhayati, “Implementasi Algoritma Vigenere Cipher dan Atbash Cipher Untuk Keamanan Teks pada Aplikasi Catatan Berbasis Android,” It (Informatic Teknologi. J., Jil. 8, No. 1, hal. 30, 2021, doi: 10.22303/it.8.1.2020.30-41.

M.A.H. Septian Widiyanto, Govindo Adnan, Moh. Fatkuroji, Dwi Wahyu Handoyo, “Pengamanan Pesan Teks dengan menggunakan Kriptografi Klasik Metode Shift Chipper dan Metode Substitusi Chipper,”Riau J. Comput.Sci., Vol.7, No.01, pp.9– 17 Agustus 2021.

S. Ramadani, S. Sauda, K. Kunci, dan H. Criptosystem, “Penerapan Algoritma AES dan DSA Menggunakan Hybrid Cryptosystem untuk Keamanan Data,” J. Ris.Komputer), Jil. 7, No.4, hlm.2407–389, 2020, doi: 10.30865/jurikom.v7i4.2055.

S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, dan Srinjiwi, “Analisis Performa Kriptografi Hybrid Algoritma RSA,” Jurteksi, Vol.VI, No.1, pp.1–10, 2019.

A. Thahara dan I. T. Siregar, “Implementasi Kriptografi untuk Keamanan Data dan Jaringan Menggunakan Algoritma DES,” J. Rekayasa Teknol.Inf., Vol.5, No.1, p. 31, 2021, doi: 10.30872/jurti.v5i1.5657.

D. Adhar, “ImpleAdhar, D. (2019). Implementasi Algoritma Des (Enkripsi Data Standard) pada Enkripsi dan Deskripsi SMS Berbasis Android. Jurnal Teknik Informatika Kaputama (JTIK), 3(2), 53–60. https://jurnal.kaputama.ac.id/index.php/JTIK/article/view/185mentasi Alg,” J. Tek Memberitahukan. Kaputama, Vol. 3, No. 2, hlm. 53–60, 2019, [Online]. Tersedia: https://jurnal.kaputama.ac.id/index.php/JTIK/article/view/185.

M. H. T. A. Thoriq, A. I. H. Asep, dan P. N. S. Puspita, “Enkripsi Data pada FileVideo Menggunakan Algoritma Blowfish Berbasis Android,” Digit Informatika.Pakar, Jil. 4, No. 1, hlm. 33–39, 2022, doi: 10.36423/index.v4i1.880.

A. Rifa’i dan L.C. Sumartini, “Implementasi Kriptografi Menggunakan Metode Blowfish dan Base64 Untuk Mengamankan Database Informasi Akademik di Kampus Akademi Telekomunikasi Bogor Berbasis Berbasis Web,” J. E-Komtek, Vol.3, No.2, hal. 87–96, 2019, doi: 10.37339/e-komtek.v3i2.133.

K. A. Seputra dan G. A. J. Saskara, “Kriptografi Simetris RC4 pada Transaksi Online Booking Engine System,” J. Pendidik.Teknol.dan Kejuru., Vol.17, No.2, pp.286–295, 2020, [Online]. Tersedia: https://ejournal.undiksha.ac.id/index.php/JPTK/article/view/27096.

M. Azhari, D. I. Mulyana, F. J. Perwitosari, dan F. Ali, “Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standar (AES),” J. Pendidik.Sains dan Komput., Vol.2, No.01, hlm.163–171, 2022,doi: 10.47709/jpsk.v2i01.1390.