p-ISSN : 2598-0416 e-ISSN : 2615-689X

JURNAL ARMADA INFORMATIKA

STMIK Methodist Binjai

jurnal.stmikmethodistbinjai.ac.id/jai

Kriptografi

Proteksi Database dengan Algoritma Vernam Cipher

Murdani [1], Eferoni Ndururu [2], Muhammad Sayuthi [3], Abdul Halim Hasugian [5]

[1] *Program Studi Sistem Informasi, Universitas Budi Darma, Medan*
[2] *Program Studi Manajemen Informatika, Universitas Budi Darma, Medan*
[3] *Program Studi Teknik Informatika, Universitas Budi Darma, Medan*
[4] *Program Studi Ilmu Komputer, Universitas Islam Negeri Sumatera Utara, Medan*

INFORMASI ARTIKEL

Diterima Redaksi: 08 Agustus 2022
Revisi Akhir: 01 Oktober 2022
Diterbitkan *Online*: 01 Desember 2022

KATA KUNCI

Proteksi; Database; Algoritma Vernam Cipher

KORESPONDENSI

Phone: +62 852-9750-5332
E-mail: murdanibudidarma@gmail.com

A B S T R A K

Secara umum, sebagian besar pelanggaran keamanan terjadi karena administrasi keamanan yang buruk karena ekspektasi yang tidak realistis terhadap kemampuan alat keamanan membuat pengguna lengah. Satu-satunya cara untuk mencegah insiden tersebut adalah dengan meningkatkan kesadaran keamanan di seluruh kelompok pengguna. Sampai orang mendapatkan pemahaman yang memadai tentang keamanan dan menerima pelatihan dalam tata kelola keamanan, administrasi keamanan yang tepat dapat dilakukan. Banyak perusahaan atau organisasi ragu-ragu untuk mengimplementasikan enkripsi karena keyakinan bahwa memanfaatkan teknologi enkripsi akan memperlambat kinerja sistem. Bahkan untuk perusahaan yang menerapkan enkripsi, mereka percaya bahwa penurunan kinerja hanyalah pertukaran yang diperlukan – harga yang harus dibayar agar data mereka aman. Enkripsi harus diterapkan dengan tepat di ketiga lapisan sistem TI, yaitu lapisan aplikasi, sistem, dan jaringan. Dengan manajemen kunci yang aman, manajemen hak istimewa, dan kontrol akses, enkripsi yang solid dapat dicapai. Penelitian ini mencoba salah satu penanganan database dengan algoritma vernam cipher.

PENDAHULUAN

Proteksi database adalah tentang mencoba logika enkripsi secara sistematis melalui generalisasi dan proposisi, teknologi enkripsi, berdasarkan teori enkripsi, merupakan produk kebutuhan yang bertujuan untuk menciptakan hasil yang paling hemat biaya dan menguntungkan sejalan dengan prinsip ekonomi. Ini adalah hasil dari proses transformasi, pemurnian, dan penggabungan teori untuk aplikasi praktis. Menurut persyaratan bisnis, lokasi penerapan enkripsi dan karakteristik data dapat berbeda. Inilah mengapa teknologi enkripsi perlu dikualifikasikan dari nilai bisnisnya. Oleh karena itu, mempelajari teknologi enkripsi memerlukan pemahaman sistem dan bisnis yang luas dan menyeluruh. Ini adalah contoh terbaru dari sistem enkripsi aplikasi messenger seluler yang dirancang dan diimplementasikan. Pada tingkat paling dasar, enkripsi data diperlukan dalam DBMS (Database Management System). Hampir semua aplikasi membutuhkan database contohnya saja sosial media seperti facebook yang menggunakan database MySQL. Namun, mengingat tren umum dalam pelanggaran keamanan, konfigurasi di atas tidak mampu memberikan keamanan yang memadai. Pada kenyataannya, enkripsi aplikasi web perlu diimplementasikan proteksi database. Mirip dengan budaya, enkripsi memengaruhi semua aspek bisnis, termasuk desain, pengembangan, dan operasi. Bersamaan dengan kemajuan pengetahuan dan informasi, perlindungan data semakin penting. DBMS adalah modul inti yang mengelola input/output dan penyimpanan data di server DB. Sebagian besar produk DBMS menawarkan fitur enkripsi bawaan. Namun, sebagian besar produk enkripsi tipe TDE menyimpan data yang didekripsi dalam memori, yang menimbulkan risiko kebocoran informasi. Dengan mempertimbangkan praktik terbaik manajemen kunci, memiliki kunci enkripsi dan data yang disimpan dalam repositori yang sama akan membuat pencapaian keamanan yang lengkap menjadi tidak mungkin. Dengan pemahaman menyeluruh tentang seluruh sistem TIK dan lingkungan bisnis, teknologi dapat digunakan untuk memenuhi kebutuhan keamanan dan kinerja. Sebagai vendor enkripsi khusus, Penta Security menyediakan semua teknologi enkripsi yang diperlukan untuk perlindungan data. Penelitian ini mencoba melakukan enkripsi dan deskripsi diluar fungsi DBMS itu sendiri.

TINJAUAN PUSTAKA

Kriptografi

Kriptografi adalah cabang ilmu yang membahas mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi[1][2]. Pada dasarnya kriptografi sendiri sudah digunakan jauh sebelum konsep komputer dikenal[3]. Kriptografi, selama berabad-abad, telah menjadi seni yang dipraktekkan oleh banyak orang yang telah merancang teknik ad hoc untuk memenuhi beberapa persyaratan keamanan informasi[4][5]. Dua puluh tahun terakhir telah menjadi masa transisi bagi kriptografi dimana sebelumnya kriptografi hanyalah sebuah form atau bentuk dan sekarang telah pindah dari seni menjadi sebuah cabang ilmu[6][7].

Enkripsi dan Deskripsi

Enkripsi adalah hal yang sangat penting dalam kriptografi, enkripsi sendiri merupakan pengamanan data yang akan dikirimkan agar terjaga kerahasiaannya[4][8]. Proses enkripsi sendiri adalah sebuah perombakan suatu data menjadi bentuk data yang sama sekali tidak dapat dikaitkan dengan data awal sebelum di enkripsi.
Dekripsi juga memiliki porsi kepentingan yang sama dengan enkripsi dalam sebuah metode kriptografi, fungsi dekripsi yang mengembalikan data yang telah dienkripsi kembali ke bentuk awal sebelum proses enkripsi [4][9].

Keamanan

Keamanan Data atau *Data Security* pada awalnya adalah masalah utama dalam aplikasi militer[10][11] dan keamanan sebuah negara, namun sekarang perkembangan keamanan atau *security* pada umumnya telah di perkuat untuk sebagian besar komunikasi yang pada saat itu sudah mulai memasuki dunia internet[12]. Kriptografi sendiri adalah salah satu bidang ilmu yang dikembangkan untuk kepentingan pengamanan data baik pengirim maupun penerima dalam[13] mengirim ataupun menerima data melalui *chanel* ataupun jaringan yang kurang terpercaya dari segi keamanan[4].

Algoritma Viginere Cipher

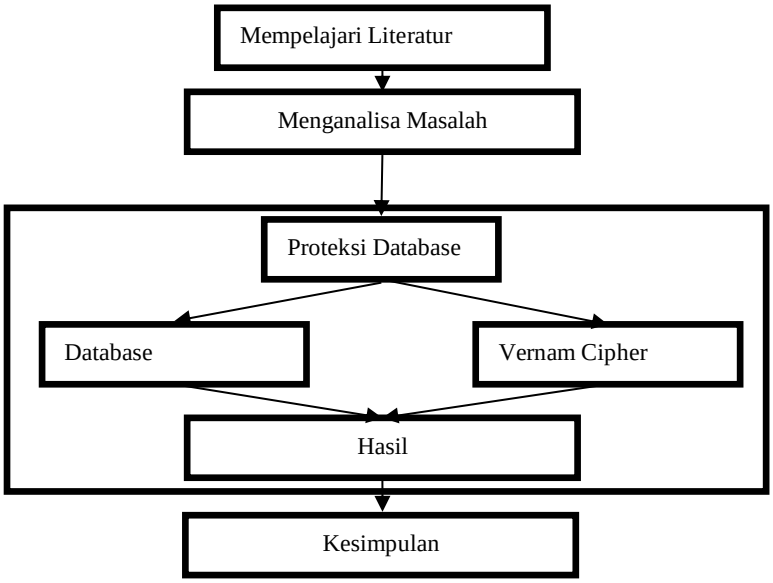
Algoritma vigener *cipher* adalah salah satu jenis kriptografi klasik yang pada dasarnya adalah melakukan substitusi *cipher* abjad majemuk (*polyalphabetic substitution*), yaitu mengubah *plaintext* dengan kunci tertentu biasanya berupa sebuah kata atau kalimat yang berulang sepanjang *plaintext* sehingga didapatkan *ciphertext*[14][15].

$$C_i = (P_i + K_i) \bmod 26 \qquad (1)$$
$$P_i = (P_i + K_i) \bmod 26 \qquad (2)$$

Dimana :
C_i = nilai desimal karakter *ciphertext* ke-i
P_i = nilai desimal karakter *plaintext* ke-i
K_i = nilai desimal karakter kunci ke-i

METODOLOGI

tahapan-tahapan didalam menyelesaikan penelitan dari awal penelitian sampai ahir yakni memulai dengan mempelajari literatur sampai menguji sistem :



Gambar 1. Metode Peneltian

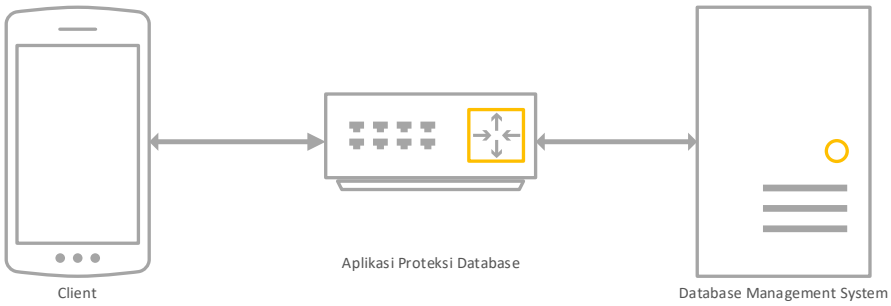
HASIL DAN PEMBAHASAN

Pertama ditemukan pada akhir abad ke-19 dan Vernam mendeskripsikannya pada tahun 1917. Sandi Vernam adalah sandi Vigenère, tetapi dengan kunci enkripsi yang harus memiliki jumlah huruf yang sama atau bahkan lebih besar dari jumlah karakter dalam pesan biasa. Kunci selama teks yang akan dienkripsi memungkinkan untuk menghindari upaya kriptanalisis Vigenère dan membuat pesan jauh lebih sulit untuk diuraikan tanpa mengetahui kuncinya. Untuk menjamin keamanan maksimum, kunci tidak boleh digunakan kembali, oleh karena itu nama lainnya: masker sekali pakai / one time pad. Vernam Chiffre menggunakan metode enkripsi Vigenere tetapi menggunakan kunci setidaknya sepanjang teks biasa.. Jika kuncinya tidak cukup panjang, itu akan diulangi, seperti dalam sandi Vigenere, tetapi ini menimbulkan kelemahan kriptografik dalam pesan. Dekripsi juga identik dengan metode dekripsi Vigenere. Pesan sandi Vernam memiliki indeks kebetulan yang mendekati teks acak. Jika panjang kunci sepanjang teks DAN kuncinya acak, maka tidak ada metode kriptanalisis yang dapat memecahkan Vernam. Jika kuncinya tidak acak, maka kemungkinan serangan kata teks biasa dapat memungkinkan untuk menebak bagian dari kunci (dan dapat menyimpulkan sisanya darinya), atau serangan dengan analisis frekuensi dapat memungkinkan untuk menemukan bahasa dari pesan dan mengurangi kemungkinan serangan brute force. Jika kunci digunakan kembali pada beberapa pesan, maka serangan Vigeneres dapat digunakan kembali.

1. Enkripsi

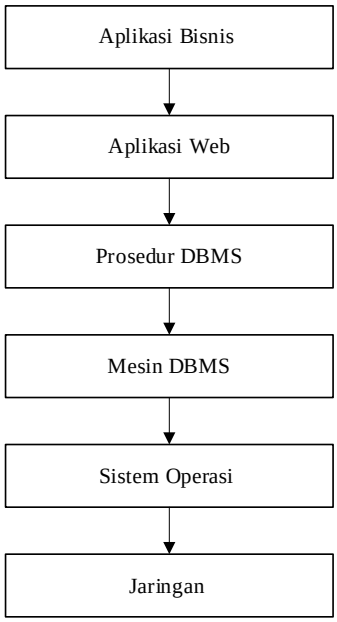
Deskripsi : PROTEKSI DATABASE DENGAN ALGORITMA VERNAM CIPHER
Kunci : DESTA
Enkripsi : SVGMENWAWAWETTSHHWGGDRSEGRVAMMDZWKNDQUBPKIJ

Berikut Konfigurasi meliputi enkripsi otentikasi pengguna, enkripsi bagian, enkripsi pesan, enkripsi file dan manajemen kunci.



Gambar 2. konfigurasi sistem keamanan

Metode enkripsi basis data dapat dibedakan berdasarkan target enkripsinya. Dalam enkripsi tingkat file , file basis data individu dienkripsi secara keseluruhan untuk membatasi akses yang tidak sah. Namun, enkripsi parsial database dapat dilakukan dengan target yang lebih spesifik sebagai berikut: Enkripsi tingkat sel : Sel individu dienkripsi secara terpisah, dengan kunci uniknya sendiri, Enkripsi tingkat kolom : Masing-masing kolom data dienkripsi secara terpisah, dengan setiap kolom memiliki kunci yang sama untuk mengakses, membaca, dan menulis data di dalam kolom, Enkripsi tingkat baris : Setiap baris data dienkripsi secara terpisah, dengan kunci uniknya sendiri untuk selnya, Enkripsi tingkat ruang tabel : Ruang tabel individual dienkripsi secara keseluruhan. Setiap tablespace memiliki kunci unik untuk semua isinya. Dengan mengizinkan enkripsi data selektif, seperti hanya mengenkripsi data sensitif, kinerja sangat ditingkatkan dibandingkan dengan enkripsi seluruh file database. Di antara berbagai metode enkripsi parsial ini, enkripsi tingkat kolom memberikan manfaat unik dengan memungkinkan fungsionalitas tertentu. Dengan enkripsi tingkat file, data harus didekripsi sepenuhnya untuk melakukan pencarian teks lengkap. Namun, jika enkripsi kolom indeks dimungkinkan, pencarian indeks dapat dilakukan dengan porsi data yang dibiarkan tidak terenkripsi. Ini memungkinkan fungsi pencarian dijalankan dengan lebih efisien. Enkripsi tingkat kolom dimungkinkan bahkan dengan data yang "sedang transit" atau "sedang digunakan", yang dikenal sebagai data aktif. Ini sangat penting untuk database yang terus-menerus diakses atau diperbarui. Administrator keamanan dapat mendelegasikan kunci enkripsi/dekripsi hanya kepada pengguna yang berwenang, untuk membatasi kolom data mana yang dapat diakses pengguna. Tidak seperti enkripsi tingkat file di mana hanya kontrol akses tingkat OS yang dapat diatur, enkripsi tingkat kolom memungkinkan pengguna menikmati akses tak terbatas ke data sensitif yang tidak perlu dienkripsi. Untuk menganalisis lingkungan data, struktur lapisan sistem TI harus dipahami sesuai dengan metode pemrosesan data. Sistem TI dapat dikonseptualisasikan sebagai terstruktur menurut lapisan virtual berikut:



Gambar 3. Lapisan Keamanan Proteksi Database

Pada Lapisan Jaringan, server dan klien saling berhubungan untuk transfer data. Ini termasuk komunikasi antara server aplikasi dan server DB, antara perangkat penyimpanan jaringan dan server, dan antara server dan terminal. Penyerang dapat mengumpulkan dan mencuri data yang ditransfer dengan mengetuk saluran komunikasi. Saat ini, untuk melindungi data, data yang ditransfer dienkripsi dengan cara berikut:

1. Aplikasi Bisnis : sistem informasi besar yang menggabungkan aplikasi kecil untuk membuat sistem aplikasi besar
2. Aplikasi Web : menyediakan konten kepada pengguna melalui web dengan bekerja sama dengan server DB
3. Prosedur DBMS : mengonfigurasi aplikasi yang menggunakan DB sebagai penyimpanan data dengan bekerja sama dengan server DB
4. Paket DBMS : menyediakan interworking untuk memproses data di server DB atau untuk menggunakan server DB secara eksternal
5. Mesin DBMS : fitur inti dari sistem basis data yang menyimpan atau mengambil data di dalam basis data, Sistem Operasi : menggerakkan server atau perangkat, dan secara fisik menyimpan file data
6. Jaringan : mentransmisikan data antar server atau antara server dan perangkat pengguna

Dengan mengenkripsi semua data, efisiensi dapat diturunkan; namun, karena pengiriman data itu sendiri dapat disembunyikan, metode ini sangat aman. Ini meningkatkan kinerja dengan hanya mengenkripsi informasi yang diinginkan. Itu membutuhkan teknologi enkripsi

selektif. Enkripsi pada lapisan jaringan secara fisik dapat memberikan enkripsi yang aman antara pengirim dan penerima. Kunci enkripsi harus dibuat dan dikelola dengan cara yang aman antara pengirim dan penerima untuk enkripsi yang aman.

KESIMPULAN DAN SARAN

Alat keamanan melindungi sistem dari penyusupan atau serangan, enkripsi adalah bentuk pertahanan mendasar yang berhubungan dengan keamanan data itu sendiri, salah satu tekniknya adalah dengan enkripsi data berdasarkan informasi yang diberikan oleh pengguna salah satunya disusupi dengan penerapan algoritma vernam cipher.

DAFTAR PUSTAKA

[1] J. Jamaludin, R. Romindo, and J. Simarmata, *Kriptografi: Teknik Hybrid Cryptosystem Menggunakan Kombinasi Vigenere Cipher dan RSA*. Yayasan Kita Menulis, 2020.

[2] T. S. Alasi, "Algoritma Hill Cipher Untuk Kebenaran Informasi pada Gambar dalam Media Sosial," *J. Inf. Komput. Log.*, vol. 2, no. 2, 2021.

[3] H. Mukhtar, *Kriptografi untuk Keamanan Data*. Deepublish, 2018.

[4] D. Ariyus, *Pengantar Ilmu Kriptografi: Teori Analisis \& Implementasi*. Penerbit Andi, 2008.

[5] E. Ndruru and T. S. Alasi, "ALGORITMA TRIPPLE DES DALAM PENGAMANAN FILE DENGAN USB FLASHDISK," *J. Inf. Komput. Log.*, vol. 2, no. 4, 2022.

[6] M. C. Sinaga, *Kriptografi Python*. Matius Celcius Sinaga, 2017.

[7] T. E. Panggabean, "Algoritma Idea Pada Keamanan Informasi," *J. Armada Inform.*, vol. 4, no. 2, 2020.

[8] T. S. Alasi, R. Wanto, and V. H. Sitanggang, "Implementasi Kriptografi Algoritma Idea Pada Keamanan Data Teks Berbasis Android," *J. Inf. Komput. Log.*, vol. 2, no. 1, 2020.

[9] P. Fitriani and T. S. Alasi, "Pengamanan Pesan Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit Pada Citra Digital," *J. Inf. Komput. Log.*, vol. 1, no. 2, 2019.

[10] Y. Yanti, M. Munawir, Z. Zulfan, E. Erdiwansyah, and others, "Implementasi Sistem Keamanan Database Menggunakan Metode Triangle Chain," *J. Serambi Eng.*, vol. 2, no. 4, 2017.

[11] B. Sugiantoro and J. E. Istiyanto, "Analisa Keamanan database Server Menggunakan Teknologi Virtual Private Database dan Notifikasi Database Server Menggunakan Agent Bergerak," in *Seminar Nasional Informatika (SEMNASIF)*, 2015, vol. 1, no. 3.

[12] S. P. Allwine, M. Kom, and A. O. D. Aritonang, "KEAMANAN JARINGAN TERPUSAT MENGUNAKAN INTRUSION DETECTION SYSTEM (IDS) DI STMIK METHODIST BINJAI," *J. Armada Inform.*, vol. 1, no. 2, 2020.

[13] T. E. Panggabean, "Perancangan Aplikasi Arsip STMIK Methodist Binjai Berbasis Web," *J. Armada Inform.*, vol. 4, no. 1, 2020.

[14] Jamaludin and Romindo, "Rancang Bangun Pengamanan Teks Menggunakan Kombinasi Vigenere Cipher dan RSA dalam Hybrid Cryptosystem," *Pros. Semin. Nas. Ris. Dan Inf. Sci.*, vol. 2, no. 0, pp. 105–116, 2020.

[15] T. S. Alasi and A. T. A. A. Siahaan, "Algoritma Vigenere Cipher Untuk Penyandian Record Informasi Pada Database," *J. Inf. Komput. Log.*, vol. 1, no. 4, 2020.