Optimalisasi Keamanan Data Pada Sistem Operasi Windows Melalui Penerapan Teknologi Kriptografi Modern

by Rakhmadi Rahman

Submission date: 10-Jul-2024 10:24AM (UTC+0700)
Submission ID: 2414583377
File name: JUSIIK_Vol_2_no_3_Agust_2024_hal_146-166.pdf (1.21M)
Word count: 6185
Character count: 40956

Jurnal Sistem Informasi dan Ilmu Komputer
Volume. 2 No. 3 Agustus 2024
e-ISSN: 2986-4976; dan p-ISSN: 2986-5158, Hal. 146-166
DOI: https://doi.org/10.59581/jusiik-widyakarya.v2i2.3868
Available online: https://journal.widyakarya.ac.id/index.php/jusiik-widyakarya

Optimalisasi Keamanan Data Pada Sistem Operasi Windows Melalui Penerapan Teknologi Kriptografi Modern

Rakhmadi Rahman[1] , Mulyadi[2] , Alif Imran[3]
Sistem Informasi , Fakultas Teknik , Institut Teknologi Habibie Parepare, Indonesia
rakhmadi.rahman@ith.ac.id[1] ,adhimuhiddin101@gmail.com[2] ,imranalif015@gmail.com[3]

Abstract. *Data security is an important aspect of information systems, especially in the widely used windows operating system environment. Modern encryption technology offers a variety of ways to increase data protection from security threats. This method utilizes literature insights and comparative analysis of various cryptographic techniques applied to the Windows operating system. Data sources were obtained from academic journals, books and technical documents from Microsoft and cyber security institutions. This article describes various modern cryptographic techniques that can be applied to the Windows operating system, including symmetric and asymmetric algorithms and end-to-end encryption. Protocol implementation security. This research also examines the effectiveness of cryptographic techniques in overcoming cyber security threats and provides the best recommendations for improving data security. It also provides a comparative analysis of various cryptographic techniques implemented in Windows operating systems. This study shows that evaluating encryption techniques can help overcome cyber threats and provide optimal solutions to improve data security. Data sources were obtained from academic journals, books, and technical documents from Microsoft and cyber security.*

Keywords: *Data Decurity, Modern Cryptography, Windows Operating System, Cryptographic Algorithms, Security Protocols*

Abstrak. Keamanan data merupakan aspek penting dari sistem informasi, terutama di lingkungan sistem operasi Windows yang banyak digunakan. Teknologi enkripsi modern menawarkan berbagai cara untuk meningkatkan perlindungan data dari ancaman keamanan. Metode ini memanfaatkan tinjauan literatur dan analisis komparatif berbagai teknik kriptografi yang diterapkan pada sistem operasi Windows. Sumber data diperoleh dari jurnal akademis, buku, dan dokumen teknis dari Microsoft dan lembaga keamanan siber. Artikel ini menjelaskan berbagai teknik kriptografi modern yang dapat diterapkan pada sistem operasi Windows, termasuk algoritma simetris dan asimetris serta enkripsi ujung ke ujung. Keamanan implementasi protokol. Penelitian ini juga mengevaluasi efektivitas teknik kriptografi dalam mengatasi ancaman keamanan siber dan memberikan rekomendasi terbaik untuk meningkatkan keamanan data. Ini juga memberikan analisis komparatif berbagai teknik kriptografi yang diterapkan pada sistem operasi Windows. Studi ini menunjukkan bahwa evaluasi teknik enkripsi dapat membantu mengatasi ancaman dunia maya dan memberikan solusi optimal untuk meningkatkan keamanan data. Sumber data diperoleh dari jurnal akademis, buku, dan dokumen teknis dari Microsoft dan keamanan siber.

Kata kunci : Keamanan data, kriptografi modern, sistem operasi Windows,algoritma kriptografi, protokol keamanan.

1. PENDAHULUAN

Informasi berkembang sangat cepat dan semakin canggih saat ini.Kecanggihan perangkat teknologi informasi membuat pengguna banyak menggunakan perangkat teknologi informasi. Salah satu nya adalah perkembangan komputer. Banyak pengguna komputer memilih sistem operasi yang memiliki sistem keamanan yang baik, karena kemudahan penggunaan dan kenyamanan pengguna dalam menggunakan teknologi informasi salah satunya adalah dengan adanya jaminan privasi atau keamanan bagi penggunanya. Kemajuan teknologi informasi telah membawa dampak signifikan terhadap pengelolaan dan keamanan

Received: Juni 07, 2024; Revised: Juni 22, 2024 Accepted: Juli 08, 2024, 2024; Online available: Juli 10, 2024
* Rakhmadi Rahman , rakhmadi.rahman@ith.ac.id

data. Sistem operasi Windows, sebagai salah satu yang paling banyak digunakan di seluruh dunia, menjadi target utama serangan siber. Oleh karena itu, perlindungan data melalui penerapan teknologi kriptografi modern menjadi sangat penting. Artikel ini bertujuan untuk mengkaji berbagai teknik kriptografi yang dapat diterapkan dalam lingkungan Windows untuk meningkatkan keamanan data.

Kriptografi adalah salah satu metode untuk mencegah kebocoran data rahasia. Penggunaan aplikasi kriptografi dengan algoritma Blowfish untuk enkripsi dan dekripsi merupakan salah satu cara untuk mengamankan file dokumen. Dalam konteks ini, pengguna file dokumen memerlukan bantuan untuk memastikan keamanan file dokumen yang disimpan. Penerapan kriptografi dalam tesis ini difokuskan pada bagaimana kriptografi dapat menjaga keamanan file dokumen hingga saat file tersebut dibuka oleh pihak yang berwenang. Secara umum, terdapat dua jenis kriptografi, yaitu kriptografi klasik dan kriptografi modern.

Implementasi keamanan sangat penting untuk memastikan sistem tidak terganggu atau diinterupsi. Perlindungan dan keamanan terhadap perangkat keras dan sistem operasi sama-sama penting. Meskipun sistem operasi hanya merupakan satu bagian kecil dari keseluruhan perangkat lunak dalam suatu sistem, namun perannya sangat vital dalam menjaga keamanan sistem secara keseluruhan.

2. TINJAUAN PUSTAKA

2.1 Keamanan Data di Sistem Operasi Windows

a. keamanan data

Keamanan merupakan aspek yang sangat penting dalam sistem komputer. Sayangnya, seringkali masalah keamanan tidak mendapat perhatian yang cukup dari para pengelola sistem komputer. Keamanan seringkali ditempatkan pada urutan yang lebih rendah dalam daftar prioritas, bahkan diabaikan sama sekali. Meskipun konfigurasi keamanan sistem dapat mempengaruhi performansi sistem, namun seringkali keamanan diabaikan.

Dengan semakin banyaknya sistem komputer yang terhubung ke jaringan, sistem menjadi rentan terhadap kejahatan komputer yang mengancam keamanan data. Kini, masyarakat bergantung pada komputer untuk berbagai keperluan penting seperti menyimpan informasi keuangan, data pribadi, informasi perusahaan, dan lain sebagainya. Oleh karena itu, pengguna dan pengelola sistem komputer perlu menjaga keamanan komputer dan data

mereka agar tidak hilang, rusak, atau disalahgunakan. Ancaman keamanan terhadap informasi meliputi:

1. Interruption: Ancaman terhadap ketersediaan informasi, di mana data dalam sistem komputer dapat dirusak atau dihapus sehingga informasi yang dibutuhkan tidak lagi tersedia.
2. Interception: Ancaman terhadap kerahasiaan informasi, di mana informasi dapat disadap atau diakses oleh pihak yang tidak berhak.
3. Modifikasi: Ancaman terhadap integritas informasi, di mana informasi yang sedang dikirim dapat disadap dan diubah oleh pihak yang tidak berhak.
4. Fabrication: Ancaman terhadap integritas informasi, di mana informasi dapat dipalsukan sehingga penerima informasi mengira informasi tersebut berasal dari sumber yang sebenarnya tidak benar.

Tujuan dari keamanan data adalah sebagai berikut:

1. Integritas Data: Memastikan bahwa pengguna yang tidak memiliki otorisasi untuk mengakses data tidak dapat mengubah atau memodifikasi data yang ada.
2. Kerahasiaan Data: Menjamin bahwa data yang telah ditentukan atau disimpan tidak dapat dibaca oleh pengguna lain dalam sistem, sehingga data tetap aman dan rahasia.
3. Ketersediaan Akses ke Sistem: Memastikan bahwa tidak ada individu yang, meskipun memiliki akses ke sistem, dapat menyebabkan sistem tidak dapat digunakan. Sebagai contoh, melalui serangan denial of service melalui internet.

b. Sistem operasi

Secara umum, sistem operasi memiliki tiga tujuan dasar:

1. Efisiensi: Memungkinkan penggunaan sumber daya sistem komputer secara efisien.
2. Kemudahan: Membuat penggunaan komputer menjadi lebih mudah.
3. Kemampuan berevolusi: memungkinkan pengembangan, pengujian, dan implementasi fungsi-fungsi baru tanpa mengganggu layanan yang sudah ada.

Fungsi dasar sistem operasi meliputi:

1. Menjembatani hubungan antara perangkat keras dan program aplikasi yang digunakan oleh pengguna.
2. Mengatur dan mengawasi penggunaan perangkat keras serta program aplikasi sebagai pengelola sumber daya (Resource Allocator).
3. Berperan sebagai pengendali untuk mencegah kesalahan (error) dan penggunaan komputer yang tidak efisien, menjaga komputer dari berbagai potensi kerusakan.
4. Mengelola sumber daya hardware seperti memori, printer, CD ROM, dll.

Keamanan komputer mencakup aspek berikut:

1. Authentication: Memastikan bahwa penerima informasi dapat memverifikasi bahwa pesan berasal dari orang yang seharusnya, sehingga informasi tersebut benar-benar dari sumber yang diinginkan.
2. Integrity: Menjamin keaslian pesan yang dikirim melalui jaringan, sehingga dapat dipastikan bahwa informasi tidak dimodifikasi oleh pihak yang tidak berhak selama perjalanan.
3. Nonrepudiation: Mencegah pengirim informasi untuk menyangkal bahwa dialah yang mengirim informasi tersebut.
4. Authority: Mencegah informasi dalam sistem jaringan dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
5. Confidentiality: Melindungi informasi dari akses oleh pihak yang tidak berhak, terutama terkait dengan informasi yang dibagikan dengan pihak lain.
6. Privacy: Menjaga kerahasiaan data pribadi.
7. Availability: Memastikan ketersediaan informasi saat diperlukan, sehingga serangan atau penetrasi sistem tidak menghambat atau menghalangi akses ke informasi.
8. Access Control: Mengatur cara akses informasi, seringkali melalui kombinasi ID pengguna dan kata sandi atau mekanisme keamanan lainnya.

2.2 Fitur keamanan windows seperti Windows Defender, BitLocker, dan mekanisme User Account Control (UAC).

a. Windows Defender

Windows Defender adalah perangkat lunak Antispyware yang disertakan dalam paket Windows dan berjalan secara otomatis saat komputer dinyalakan. Fungsinya adalah melindungi komputer dari spyware dan perangkat lunak tidak diinginkan. Spyware dapat menginstal dirinya tanpa sepengetahuan pengguna setiap kali terhubung ke Internet, atau saat menginstal program melalui CD, DVD, atau media removable lainnya. Selain itu, spyware dapat diprogram untuk berjalan pada waktu yang tidak terduga, bukan hanya karena sudah terinstal.

Cara mengaktifkan windows defender:

a. Silahkan klik pada logo start Windows pada taskbar kemudian pilih logo icon setting berbentuk gear diatas tombol power. Untuk lebih jelasnya silahkan lihat gambar dibawah ini.

b. Selanjutnya akan terbuka dashboard Windows Settings, geser pada bagian pojok bawah dan temukan menu "Update & Security", klik menu tersebut.
c. Pada saat terbuka dashboard Update & Security, silahkan pilih menu "Windows Security" yang memiliki logo perisai, kemudian pilih menu "Virus & threat protection".
d. Saat sudah terbuka dashboard Virus & threat protection, silahkan cari menu Virus & threat protection settings, kemudian pilih menu "Manage settings".
e. Untuk mengaktifkan Windows Defender pastikan semuanya setting "On" seperti pada Real-time protection, Cloud-delivered protection, Automatic sample submission danTamper protection.
f. Selamat Windows Defender sudah berhasil diaktifkan.

Kelebihan windows defender

1. Real-time protection: Windows Defender memberikan perlindungan secara real-time dengan memberi peringatan ketika spyware mencoba untuk menginstal dirinya atau mengubah pengaturan penting pada sistem Windows.
2. Scanning options: Pengguna dapat menggunakan Windows Defender untuk memindai dan menghapus spyware yang terdeteksi pada komputer, dengan opsi penjadwalan scan yang dapat diatur.
3. Otomatis: Windows Defender berjalan secara otomatis saat komputer dihidupkan, sehingga memberikan perlindungan tanpa perlu intervensi pengguna.
4. Database spyware: Windows Defender menggunakan database spyware yang terus diperbarui untuk mendeteksi dan menghapus program malware yang mungkin ada pada sistem komputer.

Kekurangan windows defender

1. Performa scanning yang lambat: Windows Defender terkadang dapat memperlambat kinerja komputer saat melakukan proses scanning disk untuk mencari malware, terutama pada komputer dengan spesifikasi rendah.
2. Kurangnya fitur lanjutan: Windows Defender mungkin kurang memiliki fitur lanjutan yang tersedia di perangkat lunak keamanan lainnya, seperti firewall yang lebih canggih atau proteksi terhadap serangan yang lebih kompleks.
3. Rentan terhadap serangan baru: Karena Windows Defender bergantung pada database spyware yang diperbarui secara teratur, ada kemungkinan bahwa program malware baru yang belum terdeteksi dalam database dapat lolos dan menginfeksi sistem.

4. Tidak menyediakan perlindungan lengkap: Meskipun Windows Defender dapat memberikan perlindungan dasar terhadap spyware, namun untuk perlindungan yang lebih komprehensif, pengguna mungkin perlu menggunakan perangkat lunak keamanan tambahan.

b. BitLocker

BitLocker Drive Encryption adalah fitur keamanan dalam sistem operasi Windows yang menyediakan enkripsi untuk seluruh volume disk. Fitur ini membantu melindungi data pada komputer yang mungkin hilang atau dicuri.

Cara kerja bitlocker drive encryption bitLocker Drive Encryption bekerja dengan cara mengenkripsi seluruh volume hard disk, namun tidak mengenkripsi seluruh sektor pada drive hard disk. BitLocker menyisakan bagian kecil dari drive yang tidak dienkripsi, yang berisi informasi untuk melakukan booting ke sistem operasi yang terinstal pada komputer (boot manager). Hal ini penting karena boot manager harus dijalankan pertama kali ketika komputer dinyalakan. BitLocker menggunakan berbagai metode autentikasi, seperti menggunakan USB Flash Disk, nomor atau sandi privat (PIN), dan autentikasi secara transparan, untuk memungkinkan pengguna mengakses drive yang terenkripsi. Proses dekripsi BitLocker melibatkan pengambilan kunci dari media USB atau Recovery Key (RK), yang kemudian digunakan untuk mendekripsi Volume Master Key (VMK) dengan algoritma AES+CBC. Setelah VMK didapat, Full Volume Encryption Key (FVEK) didekripsi dan sistem operasi dapat di-boot.

Kelebihan bitlocker drive encryption

BitLocker Drive Encryption memiliki beberapa kelebihan, antara lain:

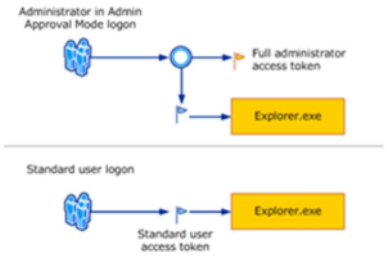
1. Menyediakan tingkat keamanan yang tinggi dengan enkripsi seluruh volume hard disk secara menyeluruh, sehingga sulit bagi pihak yang tidak sah untuk membongkar isi file yang terenkripsi.
2. Memiliki berbagai metode autentikasi yang berbeda, seperti menggunakan USB Flash Disk, PIN, atau autentikasi transparan, untuk memungkinkan pengguna mengakses drive terenkripsi.
3. Mencegah manipulasi environment sistem saat booting dilakukan melalui fasilitas Integrity Check, yang juga membantu mencegah kerja virus boot sector.

4. Menggunakan Trusted Platform Module (TPM) untuk mengamankan kunci enkripsi, serta dapat digunakan dengan USB key atau password tambahan untuk lapisan keamanan ekstra.

Kekurangan bitlocker drive encryption

1. Ketergantungan pada hardware tertentu: BitLocker memerlukan Trusted Platform Module (TPM) atau USB key sebagai metode autentikasi tambahan, sehingga pengguna perlu memastikan bahwa hardware yang diperlukan tersedia pada komputer mereka.
2. Tidak tersedia di semua edisi Windows: Fitur BitLocker Drive Encryption tidak tersedia di semua edisi Windows, seperti Windows 10 Home, sehingga pengguna dengan edisi tersebut tidak dapat menggunakan fitur ini tanpa upgrade ke edisi yang mendukung.
3. Risiko kehilangan kunci enkripsi: Jika pengguna kehilangan kunci enkripsi BitLocker, misalnya Recovery Key, maka data yang terenkripsi tidak dapat diakses lagi, kecuali pengguna memiliki cadangan kunci atau melakukan prosedur pemulihan yang rumit.
4. Performa: Proses enkripsi dan dekripsi data oleh BitLocker dapat mempengaruhi performa komputer, terutama pada komputer dengan spesifikasi rendah atau saat mengakses file yang besar.

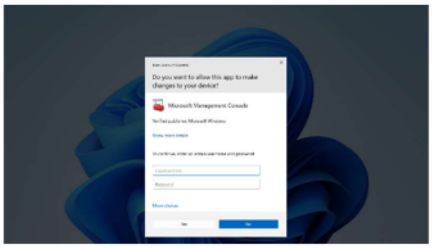
c. User Account Control (UAC



Gambar. 1. Proses masuk untuk admistrator

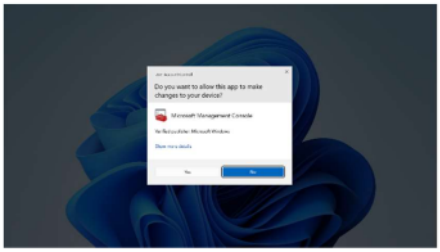
User Account Control (UAC) adalah fitur keamanan yang diperkenalkan oleh Windows untuk membantu mencegah perubahan tidak sah terhadap komputer. UAC bekerja dengan memberikan notifikasi atau permintaan izin ketika program atau pengguna mencoba melakukan tindakan yang memerlukan hak akses administrator, mekanisme kerja User Account Control (UAC) :

a. Notifikasi: Ketika pengguna atau program mencoba melakukan tindakan yang memerlukan hak akses administrator, UAC akan menampilkan notifikasi yang meminta konfirmasi atau izin dari pengguna.



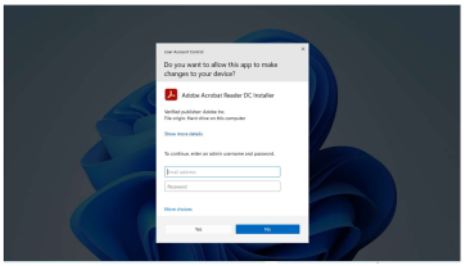
Gambar. 2. Permintaan kredensial.

b. Elevasi hak akses: Jika pengguna memberikan izin, UAC akan meningkatkan hak akses program atau tindakan tersebut ke level administrator untuk menjalankan tindakan yang diminta.



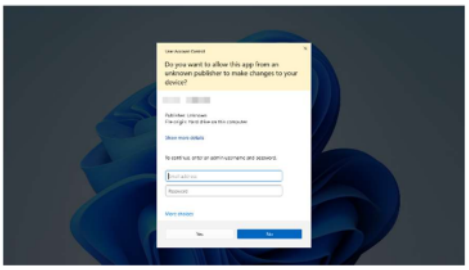
Gambar. 3. Permintaan persetujuan.

c. Password administrator: Untuk tindakan yang lebih sensitif atau berisiko, UAC dapat meminta pengguna untuk memasukkan password administrator sebagai langkah verifikasi tambahan sebelum tindakan tersebut dilakukan.



Gambar. 4. Perintah evalasi UAC terferivikasi.

d. Proteksi terhadap perubahan tidak sah: Dengan mekanisme ini, UAC membantu melindungi komputer dari perubahan tidak sah yang dapat memengaruhi keamanan sistem atau pengaturan komputer.



Gambar. 5. Perintah evalasi UAC tidak terferivikasi.

Kelebihan User Account Control (UAC):

1. Mencegah akses tidak sah: UAC membantu mencegah akses tidak sah ke sistem dengan meminta izin dari pengguna sebelum menjalankan tindakan yang memerlukan hak akses administrator.
2. Proteksi terhadap malware: Dengan meminta konfirmasi dari pengguna, UAC dapat membantu mengurangi risiko malware atau program berbahaya yang mencoba menjalankan tindakan tanpa izin.
3. Verifikasi tindakan sensitif: UAC meminta password administrator untuk tindakan yang lebih sensitif, sehingga memastikan bahwa hanya pengguna yang berwenang yang dapat menjalankan tindakan tersebut.
4. Notifikasi visual: Notifikasi UAC memberikan informasi visual kepada pengguna tentang tindakan yang akan dilakukan, sehingga pengguna dapat lebih waspada terhadap aktivitas yang memerlukan izin administrator.

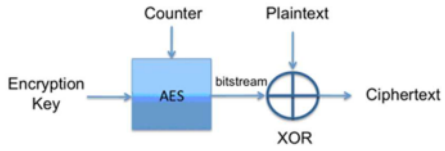
Kekurangan User Account Control (UAC):

1. Gangguan pengguna: Notifikasi UAC yang sering muncul dapat mengganggu pengguna, terutama jika pengguna sering menjalankan aplikasi atau tindakan yang memerlukan izin administrator.
2. Keterbatasan proteksi: Meskipun UAC dapat membantu mencegah akses tidak sah, namun tidak dapat memberikan perlindungan menyeluruh terhadap semua jenis serangan atau malware yang lebih canggih.
3. Keterlambatan proses: Proses meminta izin dari pengguna atau password administrator dapat memperlambat proses kerja, terutama jika pengguna harus sering mengonfirmasi tindakan.

4. Ketergantungan pada pengguna: Keefektifan UAC tergantung pada kesadaran dan kehati-hatian pengguna dalam memberikan izin atau password administrator, sehingga penggunaan yang tidak bijaksana dapat mengurangi keamanan sistem.

2.3 Teknologi Kriptografi Modern

a. Advanced Encryption Standard (AES)



Gambar. 6. Arsitektur AES

Advanced Encryption Standard (AES) adalah salah satu algoritma kriptografi simetris yang digunakan untuk enkripsi data. AES merupakan standar enkripsi yang digunakan secara luas di berbagai aplikasi dan sistem komputer karena keamanannya yang tinggi dan efisiensinya dalam melakukan enkripsi dan dekripsi data.

Keunggulan Advanced Encryption Standard (AES)

1. Keamanan Tinggi: AES menggunakan panjang kunci yang dapat mencapai 128, 192, atau 256 bit, sehingga memberikan tingkat keamanan yang tinggi terhadap serangan kriptanalisis.
2. Efisiensi: AES dirancang untuk memiliki kecepatan enkripsi dan dekripsi yang tinggi, sehingga cocok digunakan dalam aplikasi yang membutuhkan pengolahan data yang cepat.
3. Kekuatan Matematika: Algoritma AES didasarkan pada operasi matematika yang kompleks, seperti substitusi, pergeseran, dan pencampuran data, yang membuatnya sulit untuk dipecahkan tanpa kunci yang benar.

Teknik algoritma Advanced Encryption Standard (AES)

1. SubBytes: Pada tahap ini, setiap byte data diubah menggunakan sebuah tabel substitusi (S-box) yang menggantikan nilai byte dengan nilai yang berbeda. Hal ini membantu dalam mengacak data sebelum langkah-langkah enkripsi selanjutnya.
2. ShiftRows: Langkah ini melibatkan pergeseran baris dalam blok data. Setiap baris dari blok data diubah posisinya sesuai dengan aturan tertentu. Tujuannya adalah untuk memperkenalkan lebih banyak kompleksitas dan kekacauan dalam data.

3. MixColumns: Pada tahap ini, kolom-kolom dalam blok data diubah menggunakan operasi matematika tertentu. Setiap byte dalam kolom dioperasikan dengan matriks tertentu untuk mencampur data dengan cara yang tidak terbalik.
4. AddRoundKey: Langkah terakhir dalam setiap putaran enkripsi dan dekripsi melibatkan penambahan kunci rahasia ke blok data. Kunci ini dihasilkan dari kunci enkripsi utama dan berbeda untuk setiap putaran.
5. Invers Transformations: Proses dekripsi AES melibatkan invers dari transformasi yang dilakukan pada proses enkripsi. Misalnya, invers dari SubBytes, ShiftRows, dan MixColumns dilakukan untuk mendekripsi data.

b. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) adalah salah satu jenis algoritma kriptografi asimetris yang menggunakan kurva eliptik untuk melakukan proses enkripsi dan dekripsi data serta pertukaran kunci. ECC menawarkan tingkat keamanan yang tinggi dengan menggunakan kunci yang lebih pendek dibandingkan dengan algoritma kriptografi asimetris lainnya seperti RSA. Hal ini membuat ECC menjadi pilihan yang efisien untuk aplikasi yang membutuhkan keamanan data yang tinggi namun memiliki keterbatasan sumber daya, seperti pada perangkat mobile dan Internet of Things (IoT).

Algoritma ECC didasarkan pada sifat matematis dari kurva eliptik, yang memungkinkan operasi matematika yang kompleks untuk menghasilkan kunci-kunci kriptografi yang aman. ECC digunakan dalam berbagai protokol keamanan seperti Transport Layer Security (TLS), Secure Shell (SSH), dan PGP (Pretty Good Privacy) untuk melindungi data saat berkomunikasi melalui jaringan.

Keunggulan ECC antara lain efisiensi dalam penggunaan sumber daya, tingkat keamanan yang tinggi, dan ukuran kunci yang relatif kecil. Namun, implementasi ECC yang tidak benar dapat menyebabkan kerentanan keamanan, sehingga penting untuk mengikuti praktik terbaik dalam penggunaan dan konfigurasi ECC untuk memastikan keamanan sistem yang optimal.

Elliptic Curve Cryptography (ECC) menggunakan kurva eliptik untuk melakukan operasi kriptografi. Beberapa teknik yang digunakan dalam algoritma ECC meliputi:

1. Penghitungan Titik pada Kurva Eliptik: Operasi dasar dalam ECC adalah penjumlahan titik pada kurva eliptik. Titik-titik ini direpresentasikan dalam koordinat kartesian (x, y) dan operasi penjumlahan dilakukan sesuai dengan aturan matematika yang berlaku untuk kurva eliptik.

2. Pertukaran Kunci: ECC digunakan untuk pertukaran kunci rahasia antara dua entitas yang ingin berkomunikasi secara aman. Dengan menggunakan ECC, entitas dapat saling berbagi kunci publik mereka tanpa mengungkapkan kunci privat mereka.
3. Enkripsi dan Dekripsi: ECC digunakan untuk mengenkripsi dan mendekripsi data. Proses enkripsi melibatkan penggunaan kunci publik penerima untuk mengenkripsi data, sedangkan proses dekripsi melibatkan penggunaan kunci privat penerima untuk mendekripsi data yang telah dienkripsi.
4. Penandatanganan Digital: ECC juga digunakan untuk penandatanganan digital, di mana pesan ditandatangani dengan menggunakan kunci privat pengirim dan dapat diverifikasi oleh penerima menggunakan kunci publik pengirim.
5. Generasi Kunci: ECC melibatkan generasi kunci kriptografi yang aman. Kunci-kunci ini dihasilkan berdasarkan sifat matematis dari kurva eliptik dan memastikan keamanan data yang dienkripsi.

3. METODE PENELITIAN

ini menggunakan metode studi literatur dan analisis komparatif terhadap berbagai teknik kriptografi yang diterapkan pada sistem operasi Windows. Sumber data berasal dari jurnal ilmiah, buku, serta dokumentasi teknis dari Microsoft dan institusi keamanan siber.

4. HASIL DAN PEMBAHASAN

4.1 Algoritma Simetrik dan Asimetrik

a. Algoritma Simetrik

Algoritma simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi data. Kunci yang digunakan bersifat rahasia dan harus disimpan dengan aman oleh pihak yang terlibat dalam komunikasi.

Beberapa contoh algoritma simetris meliputi Data Encryption Standard (DES), Advanced Encryption Standard (AES), dan Triple Data Encryption Algorithm (TripleDES).

Keuntungan algoritma simetris

1. Kecepatan: Algoritma simetris cenderung lebih cepat dalam proses enkripsi dan dekripsi data d
2. ibandingkan dengan algoritma asimetris. Hal ini disebabkan oleh penggunaan kunci yang sama untuk kedua proses, sehingga mempercepat operasi kriptografi secara keseluruhan.

3. Efisiensi: Kunci yang digunakan dalam algoritma simetris relatif pendek dibandingkan dengan algoritma asimetris, sehingga membutuhkan penggunaan sumber daya yang lebih sedikit. Hal ini membuat algoritma simetris efisien dalam penggunaan memori dan CPU.
4. Implementasi yang Sederhana: Algoritma simetris umumnya memiliki implementasi yang lebih sederhana dibandingkan dengan algoritma asimetris. Hal ini memudahkan pengembang untuk mengimplementasikan algoritma simetris dalam berbagai aplikasi kriptografi.
5. Distribusi Kunci yang Mudah: Distribusi kunci rahasia dalam algoritma simetris relatif lebih mudah dibandingkan dengan algoritma asimetris. Pihak yang terlibat dalam komunikasi hanya perlu berbagi kunci rahasia yang sama untuk melakukan enkripsi dan dekripsi data.
6. Penggunaan dalam Enkripsi Massal: Algoritma simetris cocok digunakan untuk enkripsi data dalam jumlah besar, seperti pada proses enkripsi file atau komunikasi data yang membutuhkan kecepatan tinggi.

Kekurangan algoritma simetris

1. Distribusi Kunci yang Aman: Salah satu tantangan utama dalam penggunaan algoritma simetris adalah distribusi kunci rahasia yang aman antara pihak yang terlibat dalam komunikasi. Jika kunci rahasia jatuh ke tangan yang salah, data yang dienkripsi dengan algoritma simetris dapat terancam keamanannya.
2. Kunci Bersama: Karena algoritma simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi, pihak yang terlibat dalam komunikasi harus memiliki kunci bersama yang rahasia. Hal ini dapat menjadi masalah jika kunci tersebut terungkap atau disalahgunakan.
3. Kerentanan terhadap Serangan Brute Force: Beberapa algoritma simetris, terutama yang menggunakan kunci pendek, rentan terhadap serangan brute force di mana penyerang mencoba semua kemungkinan kunci untuk mendekripsi data yang dienkripsi.
4. Keterbatasan dalam Pertukaran Kunci: Algoritma simetris memiliki keterbatasan dalam pertukaran kunci yang aman antara pihak yang terlibat dalam komunikasi. Proses pertukaran kunci yang tidak aman dapat mengancam keamanan data yang dienkripsi.
5. Tidak Mendukung Penandatanganan Digital: Algoritma simetris tidak mendukung mekanisme penandatanganan digital yang diperlukan untuk memverifikasi keaslian dan integritas data. Untuk keperluan ini, seringkali digunakan algoritma asimetris.

b. Algoritma Asimetrik

Algoritma asimetris menggunakan sepasang kunci. Yaitu kunci publik digunakan untuk pengkodean data , sedangkan kunci privat digunakan untuk dekode data .

beberapa contoh algoritma simetris adalah Elliptic Curve Cryptography (ECC), Digital Signature Algorithm (DSA), dan Rivest-Shamir-Adleman (RSA).

Keuntungan Algoritma asimetris

1. Pertukaran Kunci yang Aman: Algoritma asimetris memungkinkan pertukaran kunci yang aman antara pihak yang terlibat dalam komunikasi tanpa perlu berbagi kunci rahasia. Kunci publik dapat disebarkan secara terbuka, sementara kunci privat tetap rahasia.
2. Tanda Tangan Digital: Algoritma asimetris mendukung mekanisme tanda tangan digital yang memungkinkan verifikasi keaslian dan integritas data. Hal ini penting dalam memastikan bahwa data tidak diubah oleh pihak yang tidak berwenang.
3. Keamanan yang Lebih Tinggi: Algoritma asimetris cenderung lebih aman daripada algoritma simetris karena penggunaan sepasang kunci yang berbeda untuk enkripsi dan dekripsi. Kunci privat hanya diketahui oleh pemiliknya, sehingga data yang dienkripsi dengan kunci publik hanya dapat didekripsi oleh kunci privat yang sesuai.
4. Pertukaran Kunci Rahasia yang Mudah: Algoritma asimetris memungkinkan pertukaran kunci rahasia antara pihak yang belum pernah bertemu sebelumnya dengan cara yang aman. Hal ini memudahkan implementasi keamanan dalam komunikasi jarak jauh.
5. Fleksibilitas dalam Penggunaan: Algoritma asimetris dapat digunakan untuk berbagai tujuan kriptografi, termasuk enkripsi data, tanda tangan digital, pertukaran kunci, dan otentikasi pengguna.

Kekurangan Algoritma asimetris

1. Kinerja yang Lambat: Algoritma asimetris cenderung lebih lambat dalam proses enkripsi dan dekripsi data dibandingkan dengan algoritma simetris. Hal ini disebabkan oleh kompleksitas matematika yang terlibat dalam operasi kunci publik dan privat.
2. Penggunaan Sumber Daya yang Lebih Besar: Algoritma asimetris membutuhkan penggunaan sumber daya yang lebih besar, seperti memori dan CPU, dibandingkan dengan algoritma simetris. Hal ini dapat mempengaruhi kinerja sistem terutama dalam aplikasi yang membutuhkan kecepatan tinggi.
3. Ketergantungan pada Infrastruktur Kunci Publik: Penggunaan algoritma asimetris seringkali bergantung pada infrastruktur kunci publik (PKI) yang memastikan keaslian kunci publik yang digunakan. Manajemen PKI yang kompleks dapat menjadi tantangan tersendiri.
4. Ukuran Kunci yang Lebih Besar: Kunci yang digunakan dalam algoritma asimetris umumnya memiliki ukuran yang lebih besar dibandingkan dengan kunci dalam algoritma simetris. Hal ini dapat mempengaruhi overhead komunikasi dan penyimpanan kunci.

5. Rentan terhadap Serangan Kuantum: Beberapa algoritma asimetris, seperti RSA, rentan terhadap serangan kuantum yang dapat mengancam keamanan sistem kriptografi. Hal ini mendorong pengembangan algoritma kriptografi yang tahan terhadap serangan kuantum.

4.2 Enkripsi End-to-End

Penerapan enkripsi end-to-end memastikan bahwa data tetap terenkripsi sepanjang perjalanan dari pengirim ke penerima, tanpa terdekripsi di sepanjang rute. Ini sangat efektif dalam melindungi data sensitif dari interceptors dan man-in-the-middle attacks. enkripsi end-to-end adalah sebuah sistem keamanan pada perangkat digital dengan mengubah kunci yang hanya diketahui oleh pemilik perangkat tersebut. Dengan kata lain, Setiap perangkat tentu akan memiliki kunci yang berbeda sehingga tidak bisa diakses oleh siapa pun kecuali pemilik bersangkutan yang mengizinkan.

Sistem ini biasa digunakan untuk aplikasi yang menghimpun data pribadi pengguna, seperti aplikasi pesan singkat, aplikasi e-commerce, aplikasi perusahaan, dan masih banyak lagi. Tujuan penggunaan sistem keamanan ini tidak lain adalah untuk mencegah kebocoran data pribadi serta menjaga privasi.

Perlu diingat bahwa sistem ini hanya bisa diakses oleh pemilik perangkat bersangkutan. Jadi, baik developer (pengembang aplikasi), pemerintah, atau bahkan hacker tidak memiliki akses untuk mendapatkan informasi di dalamnya. Apabila terjadi kebocoran data, berarti ada celah pada sistem keamanan yang perlu segera diperbaiki.

Cara Kerja Enkripsi End-to-End

Untuk mewujudkan keamanan perangkat yang mumpuni, cara kerja enkripsi end-to-end ini sendiri cukup kompleks. Ketika pengguna mengunduh sebuah aplikasi, pengguna akan diberikan dua kunci, yaitu kunci publik (public key) dan kunci pribadi (private key).

Ketika pengguna beraktivitas dalam aplikasi tersebut, kunci publik akan dikirimkan ke pusat server untuk dikelola. Tujuannya agar pengguna bisa tetap mengakses fitur-fitur yang ada di dalamnya. Kunci publik yang dikirim ini hanya berupa chipertext yang tidak bisa dibaca atau diakses oleh siapa pun.

Sementara itu, pengguna tetap menyimpan kunci pribadi untuk mengakses informasi tertentu, seperti pesan singkat, nomor PIN, password, dan sebagainya. Nah, kunci pribadi inilah yang nantinya akan membaca chipertext menjadi informasi yang jelas.

Perbedaan Enkripsi End-to-End dengan Jenis Enkripsi Lainnya

1. Peran Pengguna Sistem keamanan enkripsi end-to-end memungkinkan pengguna untuk memiliki kendali penuh atas data yang dimiliki. Dengan kata lain, pihak mana pun tidak bisa mengakses informasi dan membaca pesan yang dimiliki pengguna tanpa seizin

pemiliknya.Namun, jenis enkripsi lainnya masih memungkinkan pihak lain memiliki kunci deskripsi dan mengakses informasi di dalamnya. Hal ini biasanya disesuaikan lagi dengan kebutuhan pengguna atau perusahaan mengenai siapa saja yang berwenang untuk mengakses data tersebut.

2. Cakupan Keamanan Data Layaknya proses pengiriman barang, data yang dikirimkan dari satu perangkat ke perangkat lainnya hanya bisa dibuka oleh pihak yang dituju. Jadi, selama perjalanan data tersebut, pihak lain tidak memiliki wewenang untuk membuka apalagi mengambil data. Begitulah perbedaan enkripsi end-to-end dibandingkan jenis lainnya yang masih memungkinkan adanya pengambilan data selama perjalanan tersebut.

Manfaat Enkripsi End-to-End

1. Upaya Preventif Cegah Kebocoran Data

Maraknya kasus pengambilan data pribadi mengakibatkan perlunya peningkatan sistem keamanan perangkat dan aplikasi. Penerapan enkripsi end-to-end akan sangat bermanfaat bagi pengguna itu sendiri karena terhindar dari penggunaan data oleh pihak tidak bertanggung jawab.Anda dapat mengecek terjadinya kebocoran data melalui situs seperti Avast, Periksa Data, dan Have I Been Pwned. Jika memang terindikasi, dapat segera melaporkannya.

2. Memenuhi Standar Hukum Keamanan Perangkat dan Aplikasi Salah satu syarat sebuah aplikasi resmi dan aman digunakan oleh pengguna adalah sudah memenuhi standar hukum keamanan yang berlaku. Sistem keamanan ini menjadi dasar disahkannya sebuah aplikasi guna menjamin data pengguna akan aman dan tidak bocor. Oleh karena itu, terjadinya kebocoran data pada beberapa aplikasi perlu dipertanyakan lagi mengenai celah pada sistem keamanannya.
3. Menjaga Privasi Pengguna Segala aktivitas digital pengguna, seperti aktivitas keuangan, pesan singkat, dan sebagainya bisa terjaga berkat adanya enkripsi end-to-end. Sistem keamanan ini tentunya akan menjaga rasa aman dan kepuasan pengguna sehingga nyaman dalam beraktivitas.

Contoh Implementasi Enkripsi End-to-End

Salah satu contoh yang bisa ditemukan di tengah-tengah masyarakat. Salah satunya adalah pada aplikasi pesan singkat, seperti WhatsApp.Mungkin kita sudah tidak asing lagi ketika akan mengirim percakapan pesan ke nama kontak baru, akan muncul informasi seperti “Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them.”Selain pesan teks, WhatsApp juga memastikan bahwa semua foto, dokumen, catatan suara, serta panggilan suara dan video yang dikirimkan melalui aplikasinya telah dienkripsi end-to-end secara otomatis. Dengan fitur ini, WhatsApp menjamin bahwa pesan

yang disimpan pengguna pada layanan cloud mana pun akan tetap terlindungi dengan enkripsi end-to-end. Pesan-pesan tersebut akan diamankan oleh kunci enkripsi berupa 64 digit atau kata sandi yang tidak bisa diubah. Informasi tersebut bertujuan untuk menginformasikan kepada pengguna bahwa seluruh aktivitas online Anda akan terjamin kerahasiaan dan keamanannya. Tidak ada pihak mana pun yang bisa mengakses informasi tersebut, kecuali Anda mengizinkannya.Itulah mengapa aplikasi ini banyak digunakan oleh berbagai pihak untuk tujuan tertentu, seperti kepentingan pribadi, pendidikan, hingga bisnis. Selain karena mudah diaplikasikan, keamanan aplikasi ini pun terjamin berkat adanya sistem enkripsi end-to-end. Bagi kita yang banyak melakukan aktivitas online, seperti pengiriman dokumen, penandatangan dokumen, dsb, pastikan juga menggunakan aplikasi dengan sistem enkripsi yang aman. Salah satu contohnya adalah aplikasi Privy.

Aplikasi ini mengimplementasikan enkripsi jenis 2FA (Two-Factor Authentication) yang merupakan lapisan keamanan tambahan yang berfungsi untuk meminta verifikasi sebelum mengakses suatu akun atau layanan. Di Privy, Sistem ini diaplikasikan agar aktivitas penandatanganan dokumen, pengiriman dokumen, hingga mengecek keabsahan sebuah dokumen bisa aman dan nyaman dilakukan. Lalu, bagaimana cara kerjanya?Pada dasarnya, Privy ini adalah aplikasi bagi Anda yang ingin membuat tanda tangan digital. Tanda tangan yang sudah dibuat ini nantinya hanya bisa diakses oleh Anda dan tidak bisa digunakan oleh pihak tidak bertanggung jawab. Setiap TTd yang digunakan sembarangan akan muncul di notifikasi aplikasi Anda. Demikianlah beberapa informasi terkait enkripsi end-to-end mulai dari pengertian, cara kerja, hingga implementasinya dalam aplikasi. Akhir kata, dalam beraktivitas digital, pastikan Anda menggunakan aplikasi resmi dengan sistem keamanan mumpuni. Dengan begitu, data pribadi Anda pun bisa lebih aman dan terjaga.

4.3 Implementasi Protokol Keamanan SSL/STL

Secure Socket Layer (SSL) atau Secure Sockets Layer (SSL) adalah sebuah protokol keamanan yang digunakan untuk mengamankan komunikasi antara client dan server melalui internet. SSL bekerja dengan cara mengenkripsi data yang dikirim antara client dan server, sehingga informasi yang dikirimkan tidak dapat dibaca oleh pihak yang tidak berwenang. Protokol ini membantu menjaga keamanan dan integritas data yang dipertukarkan antara website dan web browser.

SSL memastikan bahwa data yang dikirimkan antara client dan server tetap terenkripsi dan tidak dapat diakses oleh pihak yang tidak sah. Dengan demikian, SSL membantu mencegah serangan seperti peretasan data (data breaches) dan pencurian informasi pribadi.

Implementasi SSL pada suatu sistem, seperti yang dilakukan pada Sistem Inventaris di Sanggar Tari Natya Lakshita, membantu meningkatkan keamanan data dan mencegah terjadinya serangan ilegal. Dengan menggunakan SSL, data yang dikirim antara client dan server menjadi sulit untuk dibaca karena telah dienkripsi secara aman.

Dalam konteks penelitian yang dilakukan, pengamatan dan analisis terhadap implementasi SSL dilakukan menggunakan perangkat lunak Wireshark. Wireshark digunakan untuk melakukan pemantauan lalu lintas paket data yang dikirim dan diterima oleh sistem, sehingga memungkinkan untuk memeriksa keamanan data sebelum dan sesudah penerapan SSL.

tujuan utama dari penggunaan SSL:

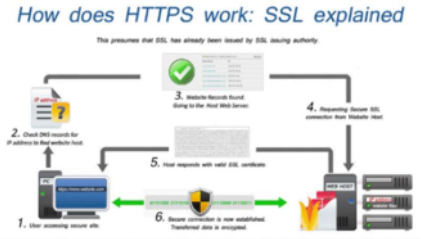
1. Enkripsi Data: SSL membantu mengenkripsi data yang dikirim antara client dan server, sehingga informasi yang dikirimkan menjadi tidak terbaca oleh pihak yang tidak berwenang. Hal ini membantu melindungi kerahasiaan data yang sensitif.
2. Integritas Data: SSL memastikan bahwa data yang dikirimkan antara client dan server tidak mengalami perubahan atau manipulasi selama proses transmisi. Dengan demikian, SSL membantu menjaga integritas data yang dikirimkan.
3. Autentikasi: SSL juga digunakan untuk memverifikasi identitas server dan kadang-kadang juga client. Dengan adanya autentikasi, pengguna dapat memastikan bahwa mereka terhubung ke server yang benar dan bukan server palsu yang berpotensi berbahaya.
4. Keamanan Transaksi Online: Implementasi SSL pada situs web e-commerce atau situs yang membutuhkan transaksi online membantu meningkatkan kepercayaan pengguna dalam melakukan transaksi secara online. SSL memberikan lapisan keamanan tambahan untuk melindungi data pembayaran dan informasi pribadi pengguna.
5. Mencegah Serangan: Dengan menggunakan SSL, sistem menjadi lebih tahan terhadap serangan cyber seperti peretasan data, pencurian informasi, dan serangan man-in-the-middle. SSL membantu mengurangi risiko serangan dengan mengenkripsi data yang dikirimkan.

Secure Socket Layer (SSL) atau Transport Layer Security (TLS) bekerja dengan cara:

1. Handshake: Proses dimulai dengan "handshake" antara client dan server. Pada tahap ini, server mengirim sertifikat digitalnya kepada client untuk memverifikasi identitasnya. Client kemudian memeriksa validitas sertifikat tersebut.
2. Enkripsi: Setelah verifikasi identitas selesai, client dan server saling bersepakat untuk menggunakan kunci enkripsi yang sama. Kunci ini digunakan untuk mengenkripsi data yang akan dikirimkan.

3. Enkripsi Data: Setelah kunci enkripsi disepakati, data yang dikirim antara client dan server akan dienkripsi sebelum dikirimkan melalui jaringan. Ini membuat data tidak dapat dibaca oleh pihak yang tidak berwenang.
4. Dekripsi Data: Di sisi penerima (client atau server), data yang diterima akan didekripsi menggunakan kunci yang sama yang telah disepakati sebelumnya. Hal ini memastikan bahwa data dapat dibaca dengan benar.
5. Integritas Data: Selama proses transmisi, SSL/TLS juga memastikan integritas data dengan menambahkan "message authentication code" (MAC) pada setiap paket data yang dikirim. Hal ini memungkinkan penerima untuk memverifikasi bahwa data tidak mengalami perubahan selama transmisi.
6. Terminasi Koneksi: Setelah komunikasi selesai, koneksi SSL/TLS dapat ditutup. Ini memastikan bahwa data sensitif tidak tersimpan dalam cache atau rentan terhadap serangan.

mengimplementasikan SSL/TLS di Windows:



Gambar. 7. Cara kerja SSL/TLS

1. Menghasilkan Sertifikat SSL:

   Kita dapat menggunakan alat seperti OpenSSL atau Microsoft Management Console (MMC) untuk membuat sertifikat SSL.Sertifikat SSL ini akan digunakan untuk mengenkripsi komunikasi antara client dan server.
2. Konfigurasi Server:

   Pada server Windows, Anda perlu mengonfigurasi layanan web server (misalnya IIS) untuk menggunakan sertifikat SSL yang telah dibuat.Aktifkan protokol SSL/TLS yang diinginkan (misalnya SSL 3.0, TLS 1.0, TLS 1.2) dan atur preferensi kriptografi.
3. Konfigurasi client:

   Pada sisi client Windows, pastikan bahwa browser atau aplikasi yang digunakan mendukung SSL/TLS.Pastikan bahwa sertifikat otoritas sertifikasi (CA) yang diperlukan untuk memverifikasi sertifikat SSL server telah diinstal di sistem.

4. Uji Coba Koneksi SSL:

   Setelah mengonfigurasi server dan client, lakukan uji coba koneksi SSL untuk memastikan bahwa komunikasi antara keduanya terenkripsi dengan benar.Gunakan alat seperti Wireshark untuk memantau lalu lintas data dan memverifikasi bahwa data terenkripsi.

5. Pemantauan dan Pemeliharaan:

   Secara teratur periksa dan perbarui sertifikat SSL untuk memastikan keamanan yang optimal.Pantau kinerja koneksi SSL/TLS untuk mendeteksi potensi masalah keamanan atau kinerja,

5. KESIMPULAN

Keamanan data memiliki signifikansi yang besar dalam lingkup sistem komputer, terutama dengan meningkatnya jumlah sistem yang terhubung ke jaringan dan rentan terhadap ancaman keamanan siber.Penerapan teknologi kriptografi modern dapat efektif meningkatkan keamanan data dengan memberikan perlindungan terhadap integritas, kerahasiaan, dan ketersediaan data.Fitur keamanan Windows seperti Windows Defender, BitLocker, dan User Account Control (UAC) memiliki peran krusial dalam menjaga keamanan sistem operasi Windows.Pentingnya memperhatikan aspek keamanan data dalam pengelolaan sistem komputer guna mencegah kerugian akibat kehilangan, kerusakan, atau penyalahgunaan data.Dalam pengelolaan keamanan data, penting untuk memperhatikan aspek seperti authentication, integrity, nonrepudiation, authority, confidentiality, privacy, availability, dan access control .

6. DAFTAR PUSTAKA

[7]Abdul, D. F., Ihsan Budiman, M., & Kurniawan, T. (n.d.). Analisis Sistem Keamanan Sistem Operasi (Windows, Linux, MacOS). Retrieved from 471-Article Text-920-1-10-20161208.

Aji, C. P., Hassanah, F. A., Auladhana, N. T., Waluyo, J. H. R., Timur, T., & Abstrak, B. J. (n.d.). STUDI ANALISA SISTEM KEAMANAN PADA SISTEM OPERASI WINDOWS STUDY OF ANALYSIS OF SECURITY SYSTEMS IN THE WINDOWS OPERATING SYSTEM. https://doi.org/10.33387/jiko

Azhari, M., Perwitosari, J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidik Sains dan Komputasi, 2*(1), 2809-476. https://doi.org/10.47709/jpsk.v2i1.1390

Choiri, E. O. (2020, May 13). Panduan Lengkap Menggunakan Windows Defender - Qwords. Qwords. Retrieved from https://qwords.com/blog/windows-defender/

Harun, M., & Mukhtar. (2018). *Kriptografi Untuk Keamanan Data*. Yogyakarta: CV BUDI UTAMA Group Penerbitan.

Mulyadi, K. (n.d.). Penerapan Keamanan Data Menggunakan Kriptografi Dengan Berbagai Metode.

Mufreni, S. L., Wijayanto, D., & Maryani, S. (2024). Implementasi SSL Untuk Keamanan Data Pada Sistem Inventaris (Studi Kasus: Sanggar Tari Natya Lakshita). *Vol 9*.

vinaypamnani-msft. (2024, March 26). How User Account Control works - Windows Security. Microsoft.com. Retrieved from https://learn.microsoft.com/en-us/windows/security/application-security/application-control/user-account-control/how-it-works

"Standard AE, Aes A, Aes A, et al." (2001). *Enkripsi Algoritma AES (Advanced Encryption Standard)*. Retrieved from [link not provided]

"Amelia, L." (2024). Enkripsi End-to-End: Pengertian, Manfaat, dan Cara Kerjanya. *Privy Blog*. Retrieved from https://blog.privy.id/enkripsi-end-to-end/

"DomaiNesia." (2023, April 10). Apa Itu SSL? Jenis dan Pentingnya Bagi Website! DomaiNesia. Retrieved from https://www.domainesia.com/panduan/apa-itu-ssl/

Optimalisasi Keamanan Data Pada Sistem Operasi Windows Melalui Penerapan Teknologi Kriptografi Modern

ORIGINALITY REPORT

10%	9%	1%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	journal.widyakarya.ac.id Internet Source	2%
2	qwords.com Internet Source	2%
3	www.coursehero.com Internet Source	1%
4	compu-techz.blogspot.com Internet Source	1%
5	webmail.informatika.org Internet Source	1%
6	kurniawan-bassist.blogspot.com Internet Source	1%
7	www.neliti.com Internet Source	1%
8	Submitted to Universitas Negeri Padang Student Paper	1%
9	maulidiyaah.blogspot.com Internet Source	1%

10	isaintek.polinef.ac.id Internet Source	1 %

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		