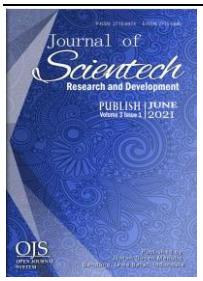

Journal of Scientech Research and Development
Volume 6, Issue 2, December 2024
P-ISSN 2715-6974
E-ISSN 2715-5846
Open Access at: https://idm.or.id/JSCR/index.php/JSCR

MELINDUNGI DATA DI DUNIA DIGITAL: PERAN STATEGIS ENKRIPSI DALAM KEAMANAN DATA

PROTECTING DATA IN THE DIGITAL WORLD: THE STRATEGIC ROLE OF ENCRYPTION IN DATA SECURITY

Alisa Almadira[1], Yogi Pratama[2], Fenny Purwani[3]
[1,2,3] *Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Raden Fatah*
E-mail: alisazn73@gmail.com[1], yogi87192@gmail.com[2], fennypurwani_uin@radenfatah.ac.id[3]

INFO ARTIKEL

Kata Kunci:
Enkripsi, Keamanan, Digital, Data.

ABSTRAK

Ancaman signifikan dalam lanskap digital saat ini, yang mengakibatkan risiko keamanan terhadap data pribadi dan informasi sensitif. Dalam upaya melindungi data digital, enkripsi mempunyai peran strategis sebagai alat utama yang menjaga kerahasiaan dan integritas informasi. Penelitian ini bertujuan untuk menguji efektivitas enkripsi, khususnya algoritma AES (Advanced Encryption Standard) dan RSA (Rivest-Shamir-Adleman), dalam mengamankan data yang disimpan dan dikirimkan di berbagai sektor, termasuk keuangan, kesehatan, dan pemerintahan. Dengan menggunakan metode studi literatur dari sumber ilmiah, laporan industri, dan publikasi terkini, penelitian ini mengidentifikasi manfaat, tantangan, dan keterbatasan penerapan enkripsi dalam menjaga keamanan data. Hasilnya menunjukkan bahwa kombinasi enkripsi simetris dan asimetris dapat meningkatkan keamanan data, namun menghadapi tantangan dalam manajemen kunci, kompatibilitas sistem, dan ancaman komputasi kuantum. Untuk menjamin perlindungan data di masa depan, diperlukan pengembangan lebih lanjut dari teknologi enkripsi, termasuk pendekatan kriptografi pasca-kuantum.

ARTICLE INFO

Keywords:
Encryption, Security, Digital, Data.

ABSTRACT

Data breaches and cyberattacks are significant threats in today's digital landscape, resulting in security risks for personal data and sensitive information. In an effort to protect digital data, encryption plays a strategic role as a primary tool that maintains the confidentiality and integrity of information. This study aims to examine the effectiveness of encryption, specifically the AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) algorithms, in securing data stored and transmitted in various sectors, including finance, healthcare, and government. Using a literature study method from scientific sources, industry reports, and recent publications, this study identifies the benefits, challenges, and limitations of implementing encryption in maintaining data security. The results show that the combination of symmetric and asymmetric encryption can improve data security, but faces challenges in key management, system compatibility, and quantum computing threats. To ensure data protection in the future, further development of encryption technology is needed, including post-quantum cryptography approaches.

PENDAHULUAN

Data bocor dan data bobol adalah fenomena yang kita saksikan beberapa tahun terakhir. Berbagai upaya sudah dilakukan untuk mencegah hal ini terjadi, namun sistem masih saja kecolongan yang mengakibatkan banyak data yang bocor. Sejak 2019 hingga 2024 terdapat 124 kasus pelanggaran perlindungan data pribadi dari data Kementrian Kominfo. Sebanyak 279 juta data penduduk Indonesia di BPJS Kesehatan diduga bocor. Hacker loliyta mencuri 17 juta data pelanggan PLN. Kemudian tidak lama ini data wajib pajak juga pernah mengalami kebocoran.

Perlindungan data merupakan hal terpenting dalam lanskap digital saat ini, khususnya terkait dengan integrasi berbagai sistem dan aplikasi. Di era digital, data sering kali menjadi target serangan siber, pencurian, dan manipulasi oleh pihak tidak sah, terutama karena banyaknya aktivitas online seperti transaksi finansial, komunikasi pribadi, dan penyimpanan informasi penting. Banyak penyebab data-data di atas bisa tidak aman mulai dari dibobok hacker, password admin yang mudah ditebak, lemahnya keamanan server ataupun hole pada webserver. Di era digital modern, memastikan keamanan dan integritas data telah menjadi hal yang sangat penting. Dengan informasi sensitif yang terus-menerus dikirim dan disimpan, sangat penting untuk memahami konsep dasar enkripsi

Enkripsi adalah proses canggih yang mengubah data menjadi bentuk yang tidak dapat dibaca, sehingga tidak dapat dipahami oleh individu yang tidak berwenang. Proses ini melibatkan pemanfaatan algoritma enkripsi dan kunci rahasia untuk mengubah data asli, yang dikenal sebagai teks biasa, menjadi bentuk terenkripsi yang disebut teks sandi. Enkripsi berfungsi sebagai alat yang ampuh dalam melindungi informasi sensitif dari akses yang tidak sah, memastikan kerahasiaan dan privasi. Dalam hal keamanan data, enkripsi menjadi pusat perhatian. Bayangkan mengamankan barang

berharga di dalam brankas yang terkunci. Enkripsi berfungsi sebagai kunci, mengubah item menjadi kode yang tidak dapat dipahami yang hanya dapat dibuka dengan kunci yang benar.

Enkripsi dan keamanan data saling berhubungan erat. Dengan mengimplementasikan enkripsi, data yang dikirim dan disimpan dapat terlindungi dari akses yang tidak sah. Meskipun terjadi kebocoran data, informasi yang terenkripsi akan sulit dimanfaatkan tanpa kunci yang benar, sehingga enkripsi menjadi inti dalam setiap kebijakan keamanan data digital. Enkripsi bukan hanya alat, tetapi bagian integral dari sistem keamanan data yang lebih besar.

Selain itu, perkembangan teknologi telah memunculkan algoritma enkripsi yang lebih canggih seperti AES (Advanced Encryption Standard) dan RSA (Rivest-Shamir-Adleman), yang sering digunakan dalam sistem keamanan digital saat ini. Implementasi kombinasi algoritma seperti ini membuat data lebih sulit diakses oleh pihak tidak berwenang, karena mereka harus melewati beberapa lapisan keamanan untuk dapat membuka data yang dienkripsi. Dengan demikian, enkripsi menjadi solusi utama dalam menjaga kerahasiaan dan integritas data, sekaligus meminimalkan risiko penyalahgunaan data jika terjadi kebocoran.

METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur yang terkait dengan topik keamanan data menggunakan enkripsi sumber-sumber relevan yang digunakan untuk menganalisis berbagai sumber referensi, termasuk jurnal ilmiah, buku, serta laporan penelitian terkait dalam kurung waktu 5 tahun terakhir. Studi literatur dilakukan dengan tujuan mengumpulkan dan mengkaji teori, konsep, serta temuan sebelumnya yang relevan dengan topik yang dibahas, guna membangun landasan teoritis yang kuat dan mengidentifikasi gap penelitian yang ada. Dengan metode ini, penulis dapat memperoleh pemahaman yang mendalam mengenai peran enkripsi dalam keamanan data. Penelitian ini berfokus pada studi kasus yang menggambarkan cara enkripsi digunakan untuk melindungi data sensitif dalam aplikasi atau sistem pada sektor-sektor tersebut, serta tantangan dan risiko yang mungkin dihadapi terkait perkembangan teknologi.

Data dalam penelitian ini diperoleh dari sumber sekunder, yaitu literatur ilmiah, laporan industri, dan publikasi dari berbagai institusi terkait. Analisis data dilakukan dengan memeriksa dokumentasi teknis dan praktik penerapan enkripsi, seperti penggunaan algoritma AES dan RSA. Data ini kemudian diorganisasikan berdasarkan sektor industri dan jenis enkripsi yang digunakan, lalu disimpulkan untuk menunjukkan efektivitas, kelemahan, dan solusi yang mungkin diadopsi guna menghadapi ancaman baru, termasuk tantangan dari teknologi komputasi kuantum.

Untuk memastikan validitas, penelitian ini menggunakan triangulasi data dari berbagai sumber agar interpretasi dan hasilnya konsisten. Dengan demikian, penelitian ini dapat memberikan gambaran menyeluruh mengenai peran enkripsi dalam menjaga keamanan data dan memitigasi risiko dalam dunia digital.

HASIL DAN PEMBAHASAN

Konsep Enkripsi End to end (E2EE)

Enkripsi End-to-End (E2EE) adalah metode untuk mengamankan data selama transmisi, di mana pesan atau data yang dikirim hanya bisa diakses oleh pengirim dan penerima. Dalam skema ini, data akan dikonversi menjadi kode terenkripsi (ciphertext) di perangkat pengirim sebelum dikirim, dan hanya dapat dikembalikan ke bentuk aslinya (plaintext) di perangkat penerima. Tujuannya adalah agar data tetap aman selama pengiriman, sehingga tidak dapat diakses oleh pihak ketiga.

Sistem ini menciptakan perlindungan berlapis untuk data pribadi, yang sangat diperlukan di dunia digital yang penuh risiko penyadapan. Aplikasi pesan, seperti WhatsApp, memanfaatkan E2EE dengan mengenkripsi pesan ketika dikirim, memastikan bahwa hanya penerima yang memiliki kunci dekripsi untuk mengubahnya kembali menjadi teks asli. Algoritma enkripsi seperti Advanced Encryption Standard dengan Galois Counter Mode (AES-GCM) juga digunakan dalam berbagai aplikasi komunikasi lainnya, termasuk konferensi video. Algoritma ini terkenal dengan kecepatan dan kemampuannya dalam menjaga keaslian data dan keamanan proses enkripsi, menjadikannya pilihan yang efisien untuk melindungi data sensitif.

Secara keseluruhan, konsep E2EE memainkan peran strategis dalam melindungi data dari akses tidak sah selama pengiriman, menjaga privasi, dan memastikan bahwa hanya pihak yang sah yang dapat membaca informasi tersebut.

Sistem ini menciptakan perlindungan berlapis untuk data pribadi, yang sangat diperlukan di dunia digital yang penuh risiko penyadapan. Aplikasi pesan, seperti WhatsApp, memanfaatkan E2EE dengan mengenkripsi pesan ketika dikirim, memastikan bahwa hanya penerima yang memiliki kunci dekripsi untuk mengubahnya kembali menjadi teks asli. Algoritma enkripsi seperti Advanced Encryption Standard dengan Galois Counter Mode (AES-GCM) juga digunakan dalam berbagai aplikasi komunikasi lainnya, termasuk konferensi video. Algoritma ini terkenal dengan kecepatan dan kemampuannya dalam menjaga keaslian data dan keamanan proses enkripsi, menjadikannya pilihan yang efisien untuk melindungi data sensitif.

Secara keseluruhan, konsep E2EE memainkan peran strategis dalam melindungi data dari akses tidak sah selama pengiriman, menjaga privasi, dan memastikan bahwa hanya pihak yang sah yang dapat membaca informasi tersebut.

Perlindungan Data dengan Enkripsi

Pada sistem keamanan informasi, perlindungan data memerlukan pendekatan khusus untuk menjaga kerahasiaan dan integritas data baik ketika data sedang disimpan maupun dalam proses pengiriman. Penelitian ini mengimplementasikan kombinasi algoritma AES (Advanced Encryption Standard) dan RSA (Rivest-Shamir-Adleman) untuk memberikan lapisan keamanan tambahan, sehingga data tetap terlindungi pada kedua kondisi tersebut.

- Enkripsi pada Data At Rest

  Data yang disimpan, atau Data At Rest, mencakup semua informasi yang tersimpan secara lokal maupun di server cloud, yang tetap rentan terhadap ancaman meskipun tidak sedang ditransmisikan. Dalam konteks ini, algoritma AES dipilih untuk mengenkripsi data yang akan disimpan. AES merupakan

algoritma enkripsi simetris yang terkenal efisien dan mampu mengenkripsi data dalam jumlah besar dengan tingkat keamanan yang tinggi. Dalam penerapannya, data mentah (plaintext) diubah menjadi ciphertext melalui proses enkripsi AES, sehingga hanya pengguna dengan kunci dekripsi yang benar dapat mengaksesnya. Hal ini membantu mencegah akses tidak sah ke data sensitif yang tersimpan dalam server, perangkat, atau media penyimpanan lainnya.

- Enkripsi pada Data In Transit

  Selain melindungi data yang tersimpan, penelitian ini juga mengupayakan perlindungan maksimal bagi Data In Transit, yaitu data yang sedang ditransmisikan melalui jaringan. Algoritma RSA digunakan dalam tahap ini untuk mengenkripsi kunci rahasia AES sebelum data dikirimkan. RSA, yang merupakan algoritma enkripsi asimetris, menggunakan dua kunci berbeda—kunci publik dan kunci privat. Dalam implementasinya, pengirim mengenkripsi kunci AES menggunakan kunci publik RSA penerima, memastikan bahwa kunci rahasia hanya dapat diakses oleh penerima yang memegang kunci privat RSA. Setelah kunci AES berhasil didekripsi oleh penerima, data tersebut dapat diakses dengan aman. Dengan demikian, enkripsi RSA pada kunci rahasia AES menjaga integritas dan keamanan data selama proses transmisi, bahkan di lingkungan jaringan terbuka yang rentan terhadap intersepsi.

Implementasi Enkripsi di Berbagai Sektor

Enkripsi adalah salah satu metode kriptografi yang berfungsi untuk menjaga kerahasiaan dan integritas data dengan cara mengubah informasi asli (plaintext) menjadi format yang tidak bisa dibaca oleh pihak yang tidak berwenang (ciphertext). Hanya pihak yang memiliki kunci dekripsi yang tepat yang dapat mengembalikan data tersebut ke bentuk aslinya. Seiring dengan perkembangan teknologi informasi, enkripsi semakin diperlukan, terutama pada sektor-sektor yang mengelola atau mentransmisikan data sensitif. Berbagai sektor industri seperti perbankan, kesehatan, perdagangan online, pemerintahan, dan lainnya, telah memanfaatkan enkripsi untuk menjaga keamanan data mereka.

1) Sektor Keuangan

   Dalam dunia perbankan dan layanan keuangan, enkripsi memainkan peran yang sangat penting untuk menjaga keamanan transaksi digital dan informasi pribadi nasabah. Lembaga keuangan mengandalkan enkripsi untuk melindungi data seperti detail akun dan transaksi pelanggan. Salah satu cara enkripsi diterapkan adalah melalui penggunaan protokol SSL/TLS yang digunakan pada transaksi online dan aplikasi perbankan mobile. Keamanan ini memastikan bahwa data yang dikirimkan antara nasabah dan bank terlindungi dari ancaman akses tidak sah. Selain itu, banyak bank dan platform keuangan lainnya yang juga menerapkan enkripsi end-to-end, memastikan hanya pihak yang sah yang dapat mengakses informasi sensitif.

2) Sektor Kesehatan

   Pada sektor kesehatan, enkripsi menjadi kunci untuk melindungi data pribadi pasien, termasuk riwayat medis, hasil pemeriksaan, dan informasi terkait lainnya yang sangat sensitif. Institusi medis wajib untuk mengenkripsi data tersebut untuk memenuhi standar yang ditetapkan oleh regulasi seperti Health Insurance Portability and Accountability Act (HIPAA) di Amerika Serikat.

Enkripsi juga diterapkan untuk melindungi komunikasi antara profesional medis dan pasien, seperti dalam layanan konsultasi jarak jauh atau aplikasi telemedicine. Hal ini penting untuk memastikan bahwa informasi medis tetap aman dan hanya dapat diakses oleh pihak yang berwenang, mengingat tingginya risiko terhadap kebocoran data pribadi dalam dunia digital.

3) Sektor E-commerce

Di dunia perdagangan elektronik, perlindungan terhadap data pelanggan adalah hal yang sangat krusial. E-commerce menggunakan berbagai teknik enkripsi untuk melindungi informasi pribadi dan data transaksi selama proses pembelian. Salah satu penerapan enkripsi yang umum adalah penggunaan protokol SSL/TLS pada situs web yang menangani pembayaran online, yang memastikan bahwa data pelanggan, termasuk nomor kartu kredit dan alamat pengiriman, terlindungi dari potensi ancaman pihak ketiga. Dengan mengimplementasikan enkripsi, platform e-commerce juga dapat menjaga agar data yang tersimpan di server mereka tetap aman dari pencurian, sehingga meningkatkan kepercayaan konsumen terhadap keamanan transaksi mereka.

4) Sektor Pemerintahan

Enkripsi juga memainkan peran penting dalam sektor pemerintahan, yang mengelola informasi sensitif terkait kebijakan publik, data pribadi warga negara, serta komunikasi internal antar lembaga. Untuk melindungi data tersebut dari potensi serangan siber atau kebocoran, banyak negara yang mengadopsi teknologi enkripsi canggih. Selain itu, dalam pengelolaan data publik seperti sistem perawatan kesehatan atau pendidikan, pemerintah juga menggunakan enkripsi untuk menjaga kerahasiaan dan privasi informasi pribadi warganya. Dengan demikian, enkripsi tidak hanya membantu melindungi data pemerintah, tetapi juga membangun kepercayaan masyarakat terhadap integritas sistem pemerintahan.

5) Sektor Teknologi dan Perangkat Lunak

Perusahaan teknologi yang mengembangkan perangkat lunak atau aplikasi digital juga menerapkan enkripsi sebagai bagian dari upaya perlindungan terhadap data pengguna. Data yang disimpan dalam sistem atau aplikasi, baik yang bersifat pribadi maupun sensitif, harus dilindungi agar tidak jatuh ke tangan yang salah. Misalnya, aplikasi perpesanan yang menggunakan enkripsi end-to-end untuk melindungi komunikasi antara pengirim dan penerima pesan. Selain itu, teknologi enkripsi juga digunakan untuk menjaga keamanan data yang dikirim melalui jaringan atau disimpan dalam cloud, sehingga informasi tetap aman meskipun terhubung dengan berbagai perangkat dan platform online.

Analisis Kasus Kebocoran dan Pencegahan dengan Enkripsi

Kebocoran data merupakan salah satu ancaman serius dalam dunia digital saat ini, mengingat banyaknya serangan dari pihak yang tidak berwenang. Dalam menghadapi masalah ini, penerapan enkripsi menjadi langkah penting untuk melindungi data sensitif yang disimpan dan dikirimkan melalui jaringan.

Penerapan Enkripsi:

1) Enkripsi Data dalam Transmisi: Menggunakan protokol seperti SSL/TLS dapat mengamankan komunikasi data yang melewati jaringan publik, menghindari potensi pencurian informasi seperti dalam transaksi online atau email.
2) Enkripsi End-to-End: Sistem komunikasi yang sangat sensitif membutuhkan enkripsi end-to-end, yang memastikan hanya pengirim dan penerima yang dapat mengakses data, bahkan jika data tersebut disadap selama perjalanan.
3) Enkripsi Data yang Disimpan: Mengamankan data yang disimpan di server juga penting, dengan menggunakan algoritma enkripsi kuat seperti AES, untuk melindungi data meskipun perangkat penyimpanan fisik dicuri atau diakses secara ilegal.
4) Integrasi IDS dengan Enkripsi: Menggabungkan Intrusion Detection System (IDS) dengan enkripsi memperkuat sistem keamanan. IDS berfungsi untuk mendeteksi penyusupan, sementara enkripsi memastikan bahwa data yang diakses oleh penyusup tetap tidak dapat dibaca tanpa kunci yang sesuai.

Algoritma Enkripsi Populer dan Penggunaannya

Seiring dengan pesatnya perkembangan teknologi komputer, kebutuhan akan perlindungan data dan informasi menjadi semakin mendesak. Salah satu metode yang umum digunakan untuk melindungi data adalah kriptografi. Dua algoritma enkripsi yang banyak diterapkan dalam kriptografi adalah Advanced Encryption Standard (AES) dan Rivest–Shamir–Adleman (RSA). Kedua algoritma ini memainkan peran penting dalam menjaga kerahasiaan informasi yang ditransmisikan melalui jaringan yang mungkin rentan terhadap serangan.

- *Advanced Encryption Standard (AES)*

  AES adalah algoritma enkripsi simetris yang terkenal karena kecepatan dan tingkat keamanannya. Algoritma ini menggunakan kunci yang sama untuk kedua proses enkripsi dan dekripsi, yang membuatnya sangat efisien dalam pengolahan data dalam jumlah besar. AES telah diterima secara luas dalam berbagai aplikasi untuk melindungi data, seperti transaksi finansial, komunikasi yang aman, dan penyimpanan informasi penting. Dalam konteks penelitian ini, AES diterapkan untuk mengenkripsi pesan, menghasilkan ciphertext yang hanya dapat didekripsi dengan kunci yang sesuai, memberikan tingkat keamanan yang tinggi pada data yang dikirimkan.

- *Rivest–Shamir–Adleman (RSA)*

  RSA merupakan algoritma enkripsi asimetris yang bekerja menggunakan dua kunci berbeda, yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi. RSA sangat berguna dalam konteks yang membutuhkan tingkat perlindungan lebih tinggi, seperti pada tanda tangan digital atau pengamanan pertukaran kunci. Dalam penelitian ini, RSA digunakan untuk mengenkripsi kunci rahasia yang diperlukan dalam enkripsi AES. Dengan demikian, meskipun kunci publik dapat dibagikan secara luas, hanya penerima yang memiliki kunci privat yang dapat mendekripsi data tersebut dengan aman.

- Integrasi AES dan RSA

  Menggabungkan AES dengan RSA menghasilkan sistem enkripsi yang lebih tangguh dan sulit ditembus. Dalam penerapannya pada penelitian ini, RSA digunakan untuk mengenkripsi kunci rahasia yang kemudian dipakai untuk enkripsi pesan utama menggunakan AES. Pendekatan ini mengoptimalkan

keduanya: AES mengamankan data besar dengan efisiensi tinggi, sementara RSA menjamin keamanan kunci enkripsi yang digunakan. Dengan demikian, kombinasi kedua algoritma ini memberikan perlindungan yang lebih lengkap terhadap data yang sensitif.

Tantangan dan Keterbatasan Penggunaan Enkripsi

Meskipun enkripsi merupakan langkah yang krusial dalam melindungi data sensitif dalam dunia siber, penerapannya menghadapi beberapa kendala. Salah satunya adalah kompleksitas implementasi, yang seringkali mengurangi kinerja sistem, terutama pada perangkat dengan sumber daya terbatas. Pengelolaan kunci juga menjadi tantangan besar; kesalahan dalam mengatur kunci bisa mengarah pada kebocoran data atau ketidakmampuan untuk mengakses informasi yang telah dienkripsi. Masalah kompatibilitas antar sistem yang menggunakan standar enkripsi berbeda juga menjadi hambatan, menyebabkan kesulitan dalam integrasi antar platform.

Selain itu, enkripsi tidak dapat menangkal serangan social engineering atau phishing, di mana penyerang bisa memperoleh informasi sensitif melalui trik psikologis. Oleh karena itu, meskipun enkripsi penting, penerapannya harus disertai dengan pendekatan keamanan lain, seperti pelatihan pengguna dan penerapan sistem manajemen risiko yang menyeluruh.

Masa Depan Enkripsi dan Teknologi *Zero-Knowledge Protocol*

Di masa depan, enkripsi akan berkembang untuk menghadapi tantangan baru, termasuk ancaman dari komputasi kuantum. Teknologi *Zero-Knowledge Protocol (ZKP)* muncul sebagai solusi inovatif untuk meningkatkan privasi dengan memungkinkan verifikasi data tanpa mengungkapkan informasi yang mendasarinya. ZKP diharapkan dapat memperkuat sistem keamanan di berbagai sektor, seperti transaksi digital dan identitas online, memberikan lapisan perlindungan tambahan, serta mendukung perkembangan sistem yang lebih aman dan efisien di dunia yang semakin tergantung pada data dan konektivitas.

Tren Teknologi yang Mempengaruhi Enkripsi

Komputasi kuantum berpotensi mengubah secara signifikan cara kita mengamankan data dan informasi melalui enkripsi. Sistem enkripsi tradisional, seperti RSA (Rivest-Shamir-Adleman) dan ECC (Elliptic Curve Cryptography), mengandalkan kesulitan dalam memecahkan masalah matematika yang kompleks, seperti faktorisasi bilangan besar atau logaritma diskrit. Namun, komputasi kuantum, dengan kemampuan untuk memproses informasi secara paralel melalui qubit, dapat menyelesaikan masalah tersebut dalam waktu yang jauh lebih cepat dibandingkan dengan komputer klasik. Hal ini akan memungkinkan komputer kuantum untuk dengan mudah memecahkan kunci enkripsi yang saat ini dianggap aman.

Akibatnya, teknologi enkripsi yang digunakan untuk melindungi informasi sensitif harus beradaptasi untuk menghadapi potensi ancaman ini. Salah satu solusi yang sedang dikembangkan adalah algoritma kriptografi pasca-kuantum (post-quantum cryptography), yang dirancang untuk tetap aman meskipun dihadapkan dengan kemampuan komputasi kuantum. Algoritma ini menggunakan pendekatan matematika yang berbeda, seperti lattice-based cryptography, yang lebih tahan terhadap serangan dari mesin kuantum. Pengembangan algoritma baru ini sangat penting untuk melindungi data di masa depan, terutama untuk aplikasi yang

memerlukan keamanan jangka panjang, seperti transaksi finansial, data pribadi, dan komunikasi sensitif.

Sementara itu, penelitian tentang komputer kuantum dan kriptografi pasca-kuantum masih dalam tahap awal, namun jelas bahwa masa depan keamanan siber akan sangat dipengaruhi oleh kemampuan teknologi kuantum. Organisasi dan lembaga penelitian di seluruh dunia mulai menginvestasikan sumber daya untuk memahami dampak komputasi kuantum terhadap enkripsi dan untuk merancang sistem perlindungan yang lebih kuat. Proses transisi menuju kriptografi pasca-kuantum membutuhkan waktu dan koordinasi antara sektor publik dan swasta, namun itu adalah langkah yang tak terhindarkan dalam menjaga integritas dan kerahasiaan data di masa depan.

SIMPULAN

Keamanan data merupakan tantangan yang semakin mendesak di dunia digital, terutama mengingat semakin seringnya terjadi kebocoran data dan serangan siber yang menargetkan informasi pribadi dan data sensitif lainnya. Dalam konteks ini, enkripsi berfungsi sebagai alat penting untuk melindungi data dari akses yang tidak sah. Proses enkripsi, yang mengubah data asli menjadi kode yang hanya dapat dibaca oleh pihak yang memiliki kunci dekripsi, memberikan jaminan kerahasiaan dan integritas data.

Berbagai metode enkripsi, seperti AES (Advanced Encryption Standard) untuk data yang disimpan (data at rest) dan RSA (Rivest-Shamir-Adleman) untuk data yang ditransmisikan (data in transit), telah terbukti efektif dalam menjaga keamanan data di berbagai sektor. Penggunaan enkripsi end-to-end (E2EE) pada aplikasi perpesanan dan protokol SSL/TLS pada transaksi online juga memperlihatkan bahwa enkripsi dapat meningkatkan keamanan dan kepercayaan pengguna terhadap sistem digital.

Namun, implementasi enkripsi tidak tanpa tantangan. Beberapa masalah utama yang dihadapi termasuk kompleksitas pengelolaan kunci, kompatibilitas antar sistem, serta keterbatasan dalam menangkal serangan berbasis sosial, seperti phishing. Terlebih lagi, dengan kemajuan komputasi kuantum, enkripsi konvensional akan menghadapi risiko yang lebih besar, mendorong kebutuhan untuk mengembangkan kriptografi pasca-kuantum yang lebih tangguh.

Secara keseluruhan, penelitian ini menekankan bahwa enkripsi tidak hanya menjadi solusi utama dalam perlindungan data saat ini, tetapi juga masa depan. Dengan mengadopsi teknologi seperti Zero-Knowledge Protocol dan berinvestasi dalam algoritma pasca-kuantum, organisasi dan pemerintah dapat membangun sistem keamanan yang lebih andal dan tahan terhadap ancaman di masa depan.

DAFTAR PUSTAKA

Aryani, A. P., & Susanti, L. E. (2022). Pentingnya Perlindungan Data Pribadi Konsumen Dalam Transaksi Online Pada Marketplace Terhadap Kepuasan Konsumen. Ahmad Dahlan Legal Perspective,2(1), 20–29. https://doi.org/10.12928/adlp.v2i1.5610

Witanti, W., Ghozali, M. A. M., & Abdillah, G. (2024). Pengamanan Data E-Mail MenggunakanEnkripsi Partially Homomorphic Encryption (PHE). Jurnal InformatikaPolinema, 10(4), 445–452. https://doi.org/10.33795/jip.v10i4.5420

Sarce Joel, A., Abdussalaam, F., & Yunengsih, Y. (2023). Tata Kelola Rekam Medis Berbasis Teknologi Informasi Dalam Penanganan Kerahasiaan Dan Keamanan Data Pasien Dengan MetodeKriptografi. Jurnal Indonesia: Manajemen Informatika dan Komunikasi, 4(3), 837–848. https://doi.org/10.35870/jimik.v4i3.287

Novianti, H. D., & Hidayat, A. T. (2023). Implementasi Kriptografi Advanced EncryptionStandard 128 Bit Dalam Pengamanan Data Keuangan Kas. Jurnal Komputer dan Teknologi. Retrieved from http://jurnal cahayapatriot.org/index.php/jukomtek/article/view/51

Yel, M. B., & Nasution, M. K. M. (2022). Keamanan Informasi Data Pribadi PadaMedia media sosial. Jurnal informatika kaputama (JIK), 6(1), 92–101. https://doi.org/10.59697/jik.v6i1.144

(Gunawan 2021) Gunawan, Hendro. 2021. "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Dalam Sosial Media." *Jurnal Muara Sains, Teknologi, Kedokteran dan Ilmu Kesehatan* 5(1): 1. doi:10.24912/jmstkik.v5i1.3456.

(Putra Rahmadi and Hilda Dwi Yunita 2020) Putra Rahmadi, and Hilda Dwi Yunita. 2020. "Implementasi Pengamanan Basis Data Dengan Teknik Enkripsi." *Jurnal Cendikia* 19(1):413–18.

(Lestari et al. 2022) Lestari, Sundari Putri, Harris Nur Fadlan, Ribka Angelia Purba, and IndraGunawan. 2022. "Realisasi Kriptografi Pada Fitur Enkripsi End-To-End Pesan Whatsapp." *Jurnal Media Informatika* 4(1): 1–8. doi:10.55338/jumin.v4i1.423