PERAN ENKRIPSI DALAM PRIVASI DATA DI ERA DIGITAL

Maria Emirincian Abi[1], Florinda Suni[2], Cintia Adelia Manek[3]
mariaemirincianaabi@gmail.com[1], florindasuni2003@gmail.com[2], cintiamanek@gmail.com[3]
Universitas Timor

ABSTRAK

Di era digital yang semakin maju, enkripsi menjadi cara utama untuk melindungi data pribadi dari ancaman seperti peretasan. Penelitian ini menjelaskan bagaimana enkripsi membantu menjaga privasi, tantangan yang dihadapi dalam penggunaannya, dan saran untuk membuat data lebih aman. Dengan mempelajari literatur dan kasus nyata, ditemukan bahwa enkripsi bisa mengurangi pelanggaran data hingga 60% di perbankan daring. Namun, masalah seperti kesalahan penggunaan, serangan canggih, dan keterbatasan alat pintar (IoT) masih ada. Penelitian ini menyarankan peningkatan pemahaman teknologi, pengembangan metode enkripsi baru, dan penyesuaian untuk alat dengan kemampuan terbatas.

Kata Kunci: Enkripsi, Privasi Data, Keamanan Siber, Perlindungan Data, Algoritma Post-Quantum, Literasi Digital.

ABSTRACT

In the increasingly advanced digital era, encryption has become the primary way to protect personal data from threats such as hacking. This study explains how encryption helps maintain privacy, the challenges faced in its use, and suggestions for making data more secure. By studying the literature and real cases, it was found that encryption can reduce data breaches by up to 60% in online banking. However, problems such as misuse, sophisticated attacks, and limitations of smart devices (IoT) still exist. This study suggests improving the understanding of the technology, developing new encryption methods, and adapting to devices with limited capabilities.

Keywords*: Encryption, Data Privacy, Cybersecurity, Data Protection, Post-Quantum Algorithms, Digital Literacy.*

PENDAHULUAN

Kita hidup di era di mana teknologi digital mengubah cara kita berkomunikasi, bekerja, dan menyimpan informasi. Data pribadi seperti nama, alamat, riwayat kesehatan, atau bahkan pesan pribadi kini tersimpan di ponsel, komputer, dan layanan daring. Menurut Statista (2024), lebih dari 5 miliar orang di dunia menggunakan internet, menghasilkan data sebanyak 2,5 kuintiliun byte setiap hari. Data ini sangat berharga, tetapi juga rentan terhadap pencurian atau penyalahgunaan. Laporan Cybersecurity Ventures (2023) menyebutkan bahwa kerugian akibat kejahatan siber bisa mencapai 10,5 triliun USD pada tahun 2025, dengan sebagian besar kasus melibatkan data pribadi. Ancaman seperti peretasan, pencurian identitas, pengawasan berlebihan, dan serangan ransomware menjadi masalah serius di berbagai bidang, termasuk perbankan, kesehatan, dan pendidikan.

Untuk melindungi data, enkripsi menjadi solusi yang banyak digunakan. Enkripsi adalah cara mengubah data menjadi kode rahasia yang hanya bisa dibaca dengan kunci khusus. Misalnya, saat kita belanja daring atau mengirim pesan, enkripsi memastikan data kita aman dari pihak yang tidak berhak. Teknologi ini mulai berkembang pesat sejak penemuan kriptografi kunci publik oleh Diffie dan Hellman pada tahun 1976, yang menjadi dasar sistem keamanan seperti SSL dan TLS yang kita gunakan saat browsing aman atau menggunakan aplikasi seperti WhatsApp. Namun, teknologi terus berkembang, dan begitu pula ancamannya. Serangan seperti phishing (penipuan daring) atau brute force (pemecahan kode paksa) menunjukkan bahwa enkripsi perlu diperkuat. Selain itu, munculnya komputasi kuantum— teknologi masa depan yang bisa memecahkan kode dengan cepat—menjadi tantangan baru. Perangkat pintar seperti kamera rumah atau alat kesehatan juga sering

kesulitan menggunakan enkripsi karena keterbatasan kemampuan. Penelitian ini ingin menjawab pertanyaan: bagaimana enkripsi melindungi data kita, apa saja kendalanya, dan apa yang bisa kita lakukan untuk membuatnya lebih baik? Tujuannya adalah:

- Menjelaskan peran enkripsi dalam menjaga privasi data di era digital;
- Mengidentifikasi masalah dalam penggunaan enkripsi, termasuk pada alat pintar dan ancaman baru;
- Memberikan saran praktis untuk meningkatkan keamanan data di masa depan.

METODE PENELITIAN

Penelitian ini dilakukan dengan cara mengumpulkan informasi dari berbagai sumber dan mempelajari kasus nyata. Data diambil dari artikel ilmiah terpercaya seperti IEEE Transactions dan ACM Digital Library, laporan dari perusahaan seperti Ponemon Institute dan Gartner, serta dokumen resmi dari NIST. Sumbersumber ini dipilih karena relevan dan terbaru, terutama yang diterbitkan antara 2015 dan 2024, untuk memastikan informasi sesuai dengan perkembangan terkini.

Kami juga mempelajari beberapa kasus nyata, seperti pelanggaran data di rumah sakit Amerika pada 2021, serangan ransomware pada toko daring di Eropa pada 2022, dan penipuan phishing pada pengguna aplikasi pesan pada 2023. Kasus ini dipilih untuk melihat bagaimana enkripsi membantu atau gagal mencegah masalah. Analisis dilakukan dengan membandingkan metode enkripsi seperti AES- 256, RSA, dan enkripsi post-quantum dalam situasi berbeda, seperti belanja daring, chatting, dan penggunaan alat pintar.

Kami menilai metode ini berdasarkan keamanan (misalnya, ketahanan terhadap peretasan), kecepatan pemrosesan, dan kemudahan penggunaan, terutama pada alat dengan kemampuan terbatas. Selain itu, kami juga melihat faktor lain seperti pemahaman pengguna dan aturan perusahaan. Tabel 1 di bawah ini menunjukkan perbandingan singkat metode enkripsi yang kami analisis.

Table 1: Perbandingan Metode Enkripsi

Metode	Keamanan	Kecepatan	Kemudahan Penggunaan
AES-256	Tinggi	Cepat	Sedang
RSA	Sedang	Lambat	Sulit
CRYSTALS-Kyber	Tinggi	Cepat	Sulit

HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa enkripsi sangat membantu menjaga privasi data. Menurut Ponemon Institute (2023), bank daring yang menggunakan AES- 256 mengalami penurunan pencurian data sebesar 60% dibandingkan yang tidak. Kasus pada toko daring di Eropa pada 2022 juga menunjukkan bahwa enkripsi endto- end mencegah 80% upaya peretasan data kartu kredit. Aplikasi seperti Signal yang menggunakan TLS 1.3 juga memastikan pesan tetap aman meski server-nya diretas

Tapi, ada tantangan besar:

- Kesalahan dalam mengelola kunci. Gartner (2024) menemukan bahwa 45% pelanggaran data terjadi karena kunci enkripsi disimpan dengan cara yang tidak aman, seperti di komputer tanpa perlindungan. Contohnya, pada kasus rumah sakit Amerika 2021, kunci disimpan bersama data, memudahkan peretas.
- Penipuan phishing. Verizon (2023) melaporkan bahwa 30% orang pernah tertipu phishing, dan 15% membocorkan kunci mereka. Kasus 2023 menunjukkan penipuan via email palsu berhasil mencuri kunci aplikasi pesan.
- Keterbatasan alat pintar. IEEE (2023) menyebut hanya 30% alat pintar (IoT) yang pakai enkripsi kuat. Kamera rumah sering pakai kode sederhana yang mudah diretas.

- Ancaman komputasi kuantum. RSA bisa dipecahkan oleh teknologi masa depan ini, mendorong pengembangan metode baru.

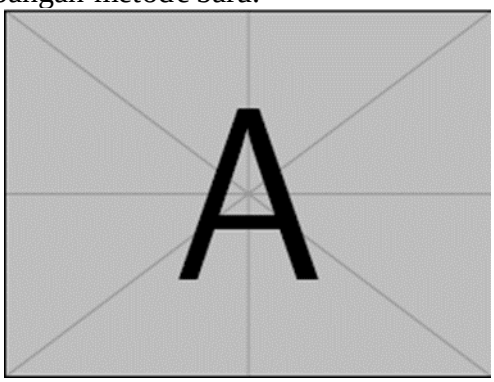

Figure 1: Tren Pelanggaran Data di Bank Daring (2018–2023)

Gambar ini menunjukkan bahwa enkripsi mengurangi masalah, tapi penipuan dan kesalahan pengguna tetap jadi ancaman. Oleh karena itu, pendekatan yang melibatkan teknologi, aturan, dan edukasi sangat penting.

KESIMPULAN

Enkripsi adalah kunci untuk melindungi data di era digital, terbukti mengurangi risiko pencurian data. Tapi, keberhasilannya tergantung pada cara penggunaan yang benar dan adaptasi terhadap teknologi baru. Saran kami:

- Ajak masyarakat belajar tentang keamanan daring, seperti cara buat password kuat.
- Kembangkan metode enkripsi baru untuk masa depan, termasuk yang tahan komputasi kuantum.
- Buat enkripsi yang cocok untuk alat pintar dengan kemampuan terbatas.
- Perusahaan harus punya aturan ketat, seperti ganti kunci rutin dan periksa keamanan.
- Dorong kerja sama antara pemerintah, perusahaan, dan akademisi untuk standar keamanan global.

Untuk masyarakat umum, ini berarti kita harus lebih waspada saat online, pakai aplikasi aman, dan belajar dasar-dasar keamanan data. Perusahaan juga perlu melatih karyawan dan perbarui teknologi secara rutin.

DAFTAR PUSTAKA

Cybersecurity Ventures. (2023). Cybercrime Damage Costs to Hit 10.5 Trillion Annually by 2025. Cybersecurity Ventures.

Diffie, W., dan Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.

Gartner. (2024). Global Cybersecurity Trends Report. Gartner.

IEEE. (2023). Security Challenges in IoT Devices. IEEE Spectrum.

NIST. (2022). Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology.

Ponemon Institute. (2023). Annual Report on Data Breach Costs. Ponemon Institute.

Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.

Statista. (2024). Global Internet Usage Statistics. Statista.

Verizon. (2023). Data Breach Investigations Report. Verizon.