PENERAPAN ENKRIPSI END TO END PADA KEAMANAN SURAT ELEKTRONIK DI INSTANSI MILITER

Desyderius Minggu[1)], Irfan Agung Nugroho[2)], Yohanes Dwi Cahyono[3)]
Jl. Raya Anggrek No. 1 Junrejo, Batu, Indonesia[1)2)3)]
Jurusan Teknik Telekomunikasi, Politeknik Angkatan Darat[1)2)3)]
E-mail: desyderius07@gmail.com[1)], irfannugroho0796@gmail.com[2)], yohanes@poltekad.ac.id [3)]

ARTICLE TITLE (IMPLEMENTATION OF END TO END ENCRYPTION FOR SECURING ELECTRONIC MAIL IN MILITARY INSTITUTIONS)

Abstract: *The exchange of electronic mail within military institutions requires a high level of security due to the confidential nature of the information transmitted. This research focuses on applying end-to-end encryption (E2EE) technology to enhance the security of electronic mail used in military environments. The applied method includes system design, encryption process implementation, and performance testing to assess encryption reliability and message delivery accuracy. The results indicate that E2EE implementation successfully ensures that messages can only be accessed by the intended recipient, thus preventing unauthorized access during transmission. This study concludes that applying E2EE can effectively improve the confidentiality and security of electronic mail communications within military institutions.*

Keywords: *end-to-end encryption, email security, military communication, cybersecurity*

Abstrak: *Pertukaran surat elektronik di lingkungan instansi militer memerlukan tingkat keamanan yang tinggi mengingat sifat informasi yang bersifat rahasia. Penelitian ini berfokus pada penerapan teknologi enkripsi end-to-end (E2EE) untuk meningkatkan keamanan surat elektronik yang digunakan di lingkungan militer. Metode yang diterapkan meliputi perancangan sistem, implementasi proses enkripsi, serta pengujian kinerja guna menilai keandalan enkripsi dan ketepatan pengiriman pesan. Hasil penelitian menunjukkan bahwa penerapan E2EE berhasil memastikan bahwa pesan hanya dapat diakses oleh penerima yang dituju, sehingga mencegah akses tidak sah selama proses transmisi. Penelitian ini menyimpulkan bahwa penerapan E2EE efektif meningkatkan kerahasiaan dan keamanan komunikasi surat elektronik di instansi militer.*

Kata kunci: *enkripsi end-to-end, keamanan email, komunikasi militer, keamanan siber*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa perubahan signifikan dalam pola komunikasi, termasuk di lingkungan militer. Surat elektronik (email) menjadi salah satu sarana komunikasi utama dalam menyampaikan informasi strategis dan rahasia secara cepat dan efisien. Namun, tingginya ketergantungan terhadap sistem digital juga membuka peluang terjadinya kebocoran data dan serangan siber, terutama jika sistem keamanan yang digunakan tidak mampu mengimbangi kompleksitas ancaman yang berkembang.

Komunikasi elektronik di lingkungan militer tidak hanya menuntut kecepatan, tetapi juga integritas, otentikasi, dan kerahasiaan informasi. Sistem pengamanan yang selama ini diterapkan masih rentan terhadap penyadapan, modifikasi isi pesan, maupun pemalsuan identitas pengirim atau penerima. Oleh karena itu, diperlukan solusi pengamanan yang menyeluruh, tidak hanya terbatas pada sisi server, melainkan juga mencakup proses transmisi dan penerimaan pesan itu sendiri.

Salah satu pendekatan yang menjanjikan adalah penerapan **enkripsi end-to-end (E2EE)**, yakni metode di mana pesan dienkripsi di sisi pengirim dan hanya dapat didekripsi oleh penerima yang sah. Sistem ini memastikan bahwa tidak ada pihak ketiga, termasuk server email, yang dapat membaca isi pesan selama dalam proses pengiriman. Namun, untuk mencapai tingkat keamanan maksimal, E2EE perlu dilengkapi dengan **mekanisme otentikasi pengguna yang kuat**.

Dalam konteks militer, pendekatan pengamanan berbasis biometrik dapat memberikan lapisan tambahan yang signifikan. Beberapa inovasi yang dapat diterapkan dalam sistem email militer antara lain:

- **Fingerprint authentication**: Penggunaan sidik jari untuk membuka atau mengenkripsi email. Sidik jari bersifat unik dan sulit dipalsukan, sehingga sangat sesuai untuk memastikan bahwa hanya personel yang sah yang dapat mengakses informasi.
- **Facial recognition**: Verifikasi wajah dapat ditanamkan sebagai tahap autentikasi tambahan sebelum dekripsi pesan dilakukan, menambah pengamanan terutama saat perangkat digunakan oleh pihak tidak sah.
- **Digital signature (tanda tangan elektronik)**: Setiap pesan dapat disertai dengan tanda tangan digital yang diverifikasi secara kriptografi. Hal ini memastikan integritas dan keaslian pengirim pesan, serta mencegah pemalsuan dokumen.

Dengan menggabungkan E2EE dan metode otentikasi biometrik serta tanda tangan elektronik, sistem komunikasi militer akan memiliki struktur keamanan berlapis (layered security) yang sulit ditembus. Pendekatan ini sejalan dengan prinsip zero trust yang semakin diterapkan dalam keamanan siber modern, di mana setiap akses diverifikasi secara menyeluruh, meskipun berasal dari dalam jaringan terpercaya.

Rumusan masalah dalam penelitian ini adalah: *Bagaimana merancang dan mengimplementasikan sistem enkripsi end-to-end yang dilengkapi dengan autentikasi biometrik dan tanda tangan digital untuk meningkatkan keamanan surat elektronik di lingkungan instansi militer?*

Adapun tujuan dari penelitian ini adalah:

1. Merancang sistem email militer berbasis E2EE yang mengintegrasikan fingerprint, verifikasi wajah, dan tanda tangan digital.

2. Menguji efektivitas sistem dalam mencegah akses tidak sah dan menjamin kerahasiaan serta integritas pesan selama proses transmisi.
3. Memberikan kontribusi terhadap pengembangan teknologi komunikasi aman di lingkungan militer yang adaptif terhadap ancaman siber modern.

Melalui penelitian ini, diharapkan akan dihasilkan sebuah sistem komunikasi yang tidak hanya mengandalkan enkripsi data, tetapi juga memperkuat otorisasi dan autentikasi pengguna, sehingga mampu memenuhi standar keamanan tinggi yang dibutuhkan dalam sektor militer.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimen laboratorium untuk merancang, mengembangkan, dan menguji sistem keamanan surat elektronik berbasis enkripsi end-to-end (E2EE) yang diperkuat dengan autentikasi biometrik (sidik jari dan pengenalan wajah) serta tanda tangan digital. Tujuan utama adalah untuk membuktikan bahwa kombinasi teknologi ini mampu meningkatkan kerahasiaan, integritas, dan otentikasi dalam komunikasi militer.

A. Rancangan Penelitian

Tahapan dalam penelitian ini meliputi:

1. Studi literatur mengenai E2EE, biometrik, dan digital signature.
2. Perancangan sistem email militer yang terdiri dari:
    - Modul enkripsi dan dekripsi pesan menggunakan kombinasi RSA dan AES.
    - Modul otentikasi menggunakan fingerprint dan facial recognition.
    - Modul validasi pengirim dengan tanda tangan digital (digital signature).
3. Pengembangan prototipe berbasis Python (untuk backend) dan framework Flask, dengan integrasi library seperti OpenCV untuk verifikasi wajah, dan PyFingerprint untuk otentikasi sidik jari.
4. Simulasi pengiriman dan penerimaan pesan antar pengguna.
5. Evaluasi performa sistem dari sisi waktu proses, keberhasilan otentikasi, dan ketahanan terhadap akses tidak sah.

B. Populasi dan Sampel

Populasi dari penelitian ini adalah sistem komunikasi digital internal instansi militer. Sampel berupa email simulasi yang memuat informasi sensitif, dalam format teks dan dokumen PDF, yang dikirim antar akun dalam jaringan lokal tertutup.

C. Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui:

- Pencatatan log sistem saat proses enkripsi, dekripsi, dan otentikasi pengguna.
- Simulasi skenario serangan (akses ilegal, spoofing, penyadapan).
- Wawancara terbatas dengan pengguna untuk menilai kemudahan penggunaan sistem.

D. Instrumen Penelitian

Instrumen yang digunakan meliputi:

- Modul E2EE berbasis RSA-AES untuk konten email.
- Sistem biometrik: fingerprint scanner (USB) dan webcam (untuk facial recognition).
- Tanda tangan digital yang dibuat dan diverifikasi menggunakan OpenSSL.
- Server email simulasi untuk menguji transmisi dan penerimaan pesan secara terenkripsi.

E. Teknik Analisis Data

Analisis dilakukan secara kuantitatif dan kualitatif:

- Rata-rata waktu enkripsi, dekripsi, dan otentikasi.
- Persentase keberhasilan autentikasi pengguna sah.
- Persentase deteksi dan penolakan terhadap percobaan akses ilegal.
- Evaluasi deskriptif terhadap pengalaman pengguna dan potensi integrasi di lingkungan militer.

HASIL PENELITIAN

Setelah sistem diimplementasikan, dilakukan pengujian terhadap beberapa skenario komunikasi email.

A. Efektivitas Enkripsi dan Dekripsi

Hasil pengujian menunjukkan bahwa sistem mampu melakukan enkripsi dan dekripsi pesan teks dengan rata-rata waktu 0,15 detik dan file berukuran 1-2 MB dalam waktu 0,35 detik.

Ukuran Filev	Waktu Enkripsi	Waktu Dekripsi
500 KB	0,10 s	0,08 s
1 MB	0,20 s	0,17 s
2 MB	0,35 s	0,30 s

B. Keamanan Akses

Sistem mampu menolak 100% akses tidak sah melalui simulasi penyadapan pada server. Karena enkripsi hanya dapat didekripsi oleh penerima dengan private key sah, pihak lain tidak dapat membuka isi pesan walau berhasil mencegat email.

C. Ketepatan Pengiriman

Dalam simulasi pengiriman 30 email antar akun uji coba, seluruh pesan diterima utuh dan dapat didekripsi dengan benar. Hal ini menunjukkan bahwa implementasi E2EE tidak mengganggu keakuratan transmisi pesan.

tangguh, cocok untuk diterapkan pada lingkungan operasional militer yang menuntut kerahasiaan tinggi, kecepatan proses, dan keterlacakan penuh terhadap akses data.

PEMBAHASAN

Integrasi enkripsi end-to-end dengan autentikasi biometrik dan tanda tangan digital membentuk sistem komunikasi yang sangat aman untuk keperluan militer.

A. Perlindungan Berlapis

E2EE menjaga kerahasiaan pesan selama transmisi, sementara biometrik memastikan hanya personel sah yang dapat mengakses pesan. Digital signature memastikan keaslian dan integritas pengirim serta isi pesan. Sistem ini mengikuti prinsip zero-trust yang semakin banyak diterapkan dalam keamanan militer modern.

B. Efisiensi Operasional

Proses autentikasi biometrik dan verifikasi tanda tangan tidak memberikan beban berarti terhadap waktu operasional. Hal ini penting untuk menjaga ritme kerja militer yang cepat namun tetap aman.

C. Perbandingan dengan Sistem Sebelumnya

Sistem komunikasi militer yang tidak menggunakan E2EE atau tanpa autentikasi biometrik mudah disusupi melalui spoofing atau penyadapan. Sistem ini menutup celah tersebut dengan kombinasi teknologi yang saling melengkapi.

D. Potensi Implementasi Nyata

Dengan perangkat biometrik yang kini semakin terjangkau dan dukungan open-source tools, sistem ini memungkinkan untuk diimplementasikan dalam jaringan email militer secara bertahap. Diperlukan pelatihan pengguna dan uji coba operasional untuk adopsi skala penuh.

PENUTUP

Penelitian ini berhasil merancang dan menguji sistem keamanan surat elektronik di

instansi militer dengan pendekatan berlapis: enkripsi end-to-end, autentikasi biometrik, dan tanda tangan digital. Hasilnya menunjukkan:

1. Proses enkripsi dan dekripsi berjalan efisien.
2. Sistem berhasil menolak seluruh akses tidak sah.
3. Autentikasi fingerprint dan wajah memberikan proteksi identitas yang kuat.
4. Tanda tangan digital memastikan integritas dan keaslian pesan.

Sistem ini sangat potensial untuk diadopsi dalam komunikasi militer guna menghadapi kompleksitas ancaman siber. Penelitian lanjutan dapat mengkaji integrasi dengan blockchain untuk manajemen kunci dan pengarsipan pesan yang aman.

DAFTAR PUSTAKA

Diffie, W., & Hellman, M. (1976). *New directions in cryptography*. IEEE Transactions on Information Theory, 22(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE International Congress on Big Data*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to Biometrics*. Springer.

Kumar, A., & Zhang, D. (2006). *Personal recognition using hand shape and texture*. IEEE Transactions on Image Processing, 15(8), 2454–2461.