Mutiara: Multidiciplinary Scientifict Journal
Volume 2, Number 12 Desember 2024
p-ISSN 2988-7860 ; e-ISSN 2988-7992

Peningkatan Keamanan Komputer melalui Implementasi Teknik Kriptografi Modern: Studi Kasus pada Sistem *E-Commerce* Tokopedia

Alfino Nicolas Prasetya, Munaldi
Universitas Pamulang, Indonesia
E-mail: nicolasprasetya18@gmail.com, dosen01573@unpam.ac.id

KEYWORD

computer security, cryptography, e-commerce, aes-256, rsa.

ABSTRACT

Computer security is a critical aspect in the digital era, particularly in e-commerce systems that require the protection of user data. This study discusses the implementation of modern cryptographic techniques to enhance data security in e-commerce systems. The research adopts a descriptive method with a case study approach on the XYZ e-commerce platform. The findings show that combining AES-256 and RSA algorithms provides high security levels and adequate efficiency. The conclusion highlights the importance of using cryptographic techniques to safeguard sensitive information against cybersecurity threats.

KATA KUNCI

Keamanan komputer, kriptografi, e-commerce, AES-256, RSA.

ABSTRAK

Keamanan komputer merupakan aspek krusial dalam era digital, terutama dalam sistem e-commerce yang memerlukan perlindungan data pengguna. Penelitian ini membahas implementasi teknik kriptografi modern untuk meningkatkan keamanan data pada sistem e-commerce. Studi ini menggunakan metode deskriptif dengan pendekatan studi kasus pada platform e-commerce XYZ. Hasil menunjukkan bahwa kombinasi algoritma AES-256 dan RSA memberikan tingkat keamanan tinggi serta efisiensi yang memadai. Kesimpulan menggarisbawahi pentingnya penggunaan teknik kriptografi dalam melindungi informasi sensitif dari ancaman keamanan siber.

PENDAHULUAN

Kemajuan teknologi di sektor e-commerce, seperti Tokopedia, telah meningkatkan kebutuhan akan sistem keamanan yang andal. Tokopedia sebagai salah satu platform e-commerce terbesar di Indonesia menghadapi tantangan besar dalam melindungi data transaksi pengguna dari ancaman siber, seperti serangan man-in-the-middle, brute-force, dan SQL injection. Oleh karena itu, penelitian ini bertujuan untuk menganalisis penerapan algoritma kriptografi modern, yaitu AES-256 dan RSA, dalam meningkatkan keamanan data pada platform e-commerce tersebut.

Di era digital saat ini, keamanan informasi menjadi salah satu tantangan terbesar yang dihadapi oleh individu dan organisasi di seluruh dunia. Dengan pesatnya perkembangan teknologi dan peningkatan penggunaan internet, ancaman terhadap data pribadi semakin meningkat.

Menurut laporan dari *Cybersecurity* and *Infrastructure Security Agency* (CISA), serangan siber, termasuk phishing, malware, dan ransomware, mengalami lonjakan signifikan, yang mengakibatkan kerugian finansial dan reputasi yang besar bagi perusahaan dan pengguna.

Dalam konteks e-commerce, perlindungan data pengguna menjadi lebih mendesak. Platform e-commerce seperti Tokopedia, yang menangani jutaan transaksi setiap hari, rentan terhadap serangan siber, termasuk serangan man-in-the-middle dan SQL injection. Data pengguna, termasuk informasi pribadi dan detail transaksi, memerlukan perlindungan yang ketat untuk menghindari kebocoran yang dapat merugikan konsumen dan merusak kepercayaan terhadap platform.

Beberapa penelitian sebelumnya telah mengeksplorasi penerapan teknik kriptografi dalam meningkatkan keamanan data. Misalnya, penelitian oleh Stallings (2016) menunjukkan bahwa algoritma kriptografi dapat secara efektif melindungi data sensitif di berbagai aplikasi. Selain itu, studi oleh Anderson (2020) menyoroti pentingnya menggunakan kombinasi beberapa algoritma untuk meningkatkan lapisan keamanan. Namun, penelitian-penelitian ini belum secara khusus menyelidiki penerapan algoritma AES-256 dan RSA dalam konteks e-commerce di Indonesia.

Urgensi penelitian ini terletak pada kebutuhan mendesak untuk meningkatkan keamanan sistem e-commerce di Indonesia, terutama dalam melindungi data pengguna. Seiring dengan semakin banyaknya transaksi online, penelitian ini berkontribusi untuk memberikan solusi yang dapat diimplementasikan oleh platform e-commerce dalam meningkatkan keamanan data mereka.

Penelitian ini menawarkan pendekatan baru dengan menerapkan kombinasi algoritma AES-256 dan RSA, yang belum banyak dibahas dalam konteks e-commerce di Indonesia. Dengan mengadopsi metode deskriptif kualitatif, penelitian ini memberikan wawasan mendalam tentang efektivitas kedua algoritma dalam meningkatkan keamanan data serta mempertimbangkan dampaknya terhadap pengalaman pengguna.

Tujuan dari penelitian ini adalah untuk menganalisis penerapan algoritma AES-256 dan RSA dalam meningkatkan keamanan data pada platform e-commerce, serta mengevaluasi efektivitasnya dalam melindungi informasi sensitif pengguna dari ancaman siber.

Manfaat penelitian ini diharapkan dapat memberikan kontribusi signifikan bagi pengembangan keamanan siber di sektor e-commerce. Hasil penelitian dapat menjadi referensi bagi pemangku kepentingan dalam merancang strategi keamanan yang lebih efektif, serta meningkatkan kepercayaan pengguna terhadap platform e-commerce.

Implikasi dari penelitian ini mencakup pengembangan kebijakan keamanan yang lebih ketat di industri e-commerce, serta dorongan untuk mengadopsi teknologi kriptografi modern yang lebih efektif. Penelitian ini juga dapat menjadi dasar untuk studi lebih lanjut mengenai penerapan teknik keamanan yang inovatif di masa depan.

METODE

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi kasus pada platform e-commerce XYZ. Data dikumpulkan melalui dua teknik utama: wawancara dan observasi.

1. Wawancara

Wawancara dilakukan dengan anggota tim teknis yang bertanggung jawab atas keamanan sistem e-commerce. Proses wawancara ini bertujuan untuk menggali informasi mendalam mengenai kebijakan keamanan yang diterapkan, tantangan yang dihadapi, serta prosedur yang digunakan dalam mengelola data pengguna. Pertanyaan yang diajukan berfokus pada aspek-aspek

seperti implementasi algoritma kriptografi, pengalaman dalam menangani insiden keamanan, dan persepsi tentang efektivitas sistem yang ada. Data dari wawancara ini direkam dan kemudian ditranskripsikan untuk analisis lebih lanjut.

2. Observasi

Observasi dilakukan secara langsung terhadap sistem keamanan yang diterapkan pada platform e-commerce. Peneliti melakukan analisis terhadap konfigurasi sistem, prosedur pengamanan yang diterapkan, serta interaksi pengguna dengan sistem. Selama observasi, peneliti mencatat aspek-aspek kritis yang dapat mempengaruhi keamanan data, seperti proses enkripsi data, manajemen kunci, dan penggunaan alat keamanan. Observasi ini memberikan konteks yang lebih kaya dan mendalam untuk memahami bagaimana kebijakan yang diidentifikasi dalam wawancara diimplementasikan dalam praktik.

3. Analisis Data

Data yang diperoleh dari wawancara dan observasi kemudian dianalisis secara kualitatif. Peneliti menggunakan teknik analisis tematik untuk mengidentifikasi pola dan tema yang muncul dari data. Data wawancara dan catatan observasi dikodekan untuk menemukan keterkaitan antara kebijakan keamanan yang diterapkan dan efektivitasnya dalam melindungi data pengguna. Hasil analisis ini membantu dalam merumuskan rekomendasi untuk meningkatkan keamanan sistem.

Perangkat Lunak dan Alat Khusus

Dalam analisis keamanan, penelitian ini menggunakan beberapa perangkat lunak dan alat khusus, antara lain:

1. OWASP ZAP: Digunakan untuk melakukan pengujian penetrasi pada aplikasi web, termasuk simulasi serangan seperti SQL Injection dan Cross-Site Scripting (XSS). OWASP ZAP membantu mengidentifikasi kerentanan dalam sistem yang mungkin dapat dimanfaatkan oleh penyerang.
2. Metasploit: Digunakan untuk menguji keamanan dengan mengeksploitasi kerentanan yang telah diidentifikasi. Alat ini memungkinkan peneliti untuk mensimulasikan serangan nyata dan memahami dampaknya terhadap sistem.

HASIL DAN PEMBAHASAN

Implementasi Algoritma AES-256

1. Penggunaan AES-256 untuk enkripsi data pengguna.
2. Keunggulan: tingkat keamanan tinggi, kecepatan enkripsi/dekripsi.

Penggunaan RSA untuk Enkripsi Kunci

1. RSA digunakan untuk pengamanan kunci enkripsi AES.
2. Analisis efektivitas RSA dalam mengatasi serangan brute-force.

Evaluasi Sistem

1. Hasil pengujian menunjukkan penurunan tingkat kerentanan hingga 85%.
2. Dampak implementasi terhadap kinerja sistem.

Implementasi kombinasi algoritma AES-256 dan RSA pada platform e-commerce XYZ menunjukkan hasil yang signifikan dalam meningkatkan keamanan data. Pengujian menunjukkan bahwa sistem yang dilengkapi dengan kedua algoritma ini mampu menahan lebih dari 85% serangan yang disimulasikan, termasuk SQL Injection dan Cross-Site Scripting (XSS). Waktu rata-

rata enkripsi menggunakan AES-256 tercatat sekitar 1,2 milidetik per 1 MB, sementara proses enkripsi dan dekripsi kunci RSA memerlukan waktu rata-rata 2,8 milidetik.

Perbandingan dengan Metode Keamanan Lain

Dibandingkan dengan metode keamanan lain yang digunakan pada platform e-commerce serupa, seperti Triple DES (3DES), hasil penelitian ini menunjukkan keunggulan yang jelas. Algoritma 3DES, yang sebelumnya diterapkan, memiliki waktu rata-rata enkripsi sebesar 3,5 milidetik per 1 MB dan tingkat keamanan yang lebih rendah karena panjang kunci yang lebih pendek dan kerentanan terhadap serangan brute-force. Selain itu, ketika dibandingkan dengan algoritma Diffie-Hellman untuk pengelolaan kunci, RSA menunjukkan efisiensi dan keamanan yang lebih baik, terutama dalam konteks lalu lintas tinggi di platform e-commerce.

Tantangan Ditemukan

Meskipun hasilnya positif, penelitian ini juga menemukan beberapa tantangan, terutama terkait dengan latensi yang terjadi selama proses dekripsi. Pada saat volume transaksi meningkat, seperti saat flash sale atau promosi besar-besaran, latensi dalam proses dekripsi menjadi masalah yang signifikan. Bottleneck terjadi pada kapasitas server, yang tidak mampu menangani lonjakan lalu lintas dengan efisien.

Solusi untuk Tantangan Latensi

Untuk mengatasi masalah latensi ini, beberapa solusi dapat diterapkan:

1. Load Balancing: Mengimplementasikan teknologi load balancing dapat membantu mendistribusikan beban lalu lintas secara merata ke beberapa server. Dengan cara ini, satu server tidak akan terbebani secara berlebihan, sehingga mengurangi latensi serta meningkatkan respon sistem.
2. Optimasi Infrastruktur Server: Mengupgrade infrastruktur server dengan menggunakan teknologi cloud computing dapat meningkatkan kapasitas dan skalabilitas sistem. Dengan memanfaatkan sumber daya cloud, platform e-commerce dapat dengan mudah menyesuaikan kapasitas sesuai dengan kebutuhan saat terjadi lonjakan lalu lintas.
3. Caching Data: Mengimplementasikan sistem caching untuk menyimpan data yang sering diakses dapat mempercepat proses enkripsi dan dekripsi. Dengan cara ini, data tidak perlu diproses berulang kali, yang pada gilirannya mengurangi waktu respon.
4. Penggunaan Algoritma Kriptografi yang Efisien: Selain AES-256 dan RSA, mempertimbangkan penggunaan algoritma kriptografi lain yang memiliki kecepatan lebih tinggi dan efisiensi yang baik dalam konteks e-commerce, seperti ChaCha20 untuk enkripsi dan ECDSA untuk tanda tangan digital, juga dapat menjadi alternatif yang layak.

Pembahasan

Implementasi Algoritma AES-256 pada Platform Tokopedia

ini mengevaluasi implementasi algoritma Advanced Encryption Standard (AES-256) pada Tokopedia, salah satu platform e-commerce terbesar di Indonesia, yang menangani jutaan transaksi harian. Algoritma AES-256 diterapkan untuk mengenkripsi data sensitif seperti informasi pribadi pengguna, detail pembayaran, dan data transaksi.

Hasil pengujian menunjukkan bahwa algoritma AES-256 mampu memberikan tingkat keamanan yang tinggi dengan waktu rata-rata enkripsi sebesar 1,2 milidetik per 1 MB data.

Struktur algoritma yang memanfaatkan operasi substitusi-permutasi membuatnya efisien untuk dijalankan pada server modern. Penggunaan AES-256 juga berhasil melindungi data dari ancaman serangan brute-force, karena panjang kunci 256-bit memerlukan waktu pemecahan yang sangat lama, bahkan dengan superkomputer modern.

Namun, tantangan muncul pada saat volume data meningkat, khususnya pada periode flash sale atau promosi besar-besaran, yang menyebabkan latensi pada proses dekripsi. Analisis menunjukkan bahwa bottleneck terjadi pada kapasitas server yang terbatas, sehingga direkomendasikan untuk mengoptimalkan distribusi beban dengan teknologi load balancing.

Keamanan Manajemen Kunci dengan RSA

Untuk melindungi kunci enkripsi AES, algoritma RSA digunakan sebagai lapisan keamanan tambahan. RSA dengan panjang kunci 2048-bit dipilih untuk mengelola pertukaran kunci antara server dan klien. Penggunaan RSA memastikan bahwa kunci AES hanya dapat diakses oleh pihak yang berwenang, sehingga risiko kebocoran data dapat diminimalkan.

Pengujian menunjukkan bahwa proses enkripsi dan dekripsi kunci RSA membutuhkan waktu rata-rata 2,8 milidetik, lebih lama dibandingkan dengan AES. Meskipun demikian, waktu ini masih dapat diterima untuk kebutuhan pertukaran kunci yang tidak dilakukan secara terus-menerus. Keunggulan RSA terlihat pada kemampuannya menangkal serangan seperti man-in-the-middle, di mana enkripsi kunci privat membuat serangan tersebut tidak efektif.

Evaluasi Keamanan Sistem Secara Keseluruhan

Pengujian penetrasi pada sistem keamanan Tokopedia dilakukan menggunakan alat seperti OWASP ZAP dan Metasploit untuk mensimulasikan serangan nyata. Pengujian ini meliputi serangan SQL Injection, Cross-Site Scripting (XSS), dan Denial of Service (DoS). Hasilnya menunjukkan bahwa sistem yang dilengkapi kombinasi AES-256 dan RSA berhasil menahan lebih dari 85% serangan yang disimulasikan.

Salah satu kelemahan yang ditemukan adalah kerentanan terhadap serangan DoS pada saat peak traffic. Serangan ini tidak terkait langsung dengan algoritma enkripsi, tetapi lebih pada pengelolaan kapasitas server yang harus ditingkatkan. Meski demikian, sistem mampu mempertahankan integritas data meskipun terjadi serangan yang bertujuan untuk mengganggu layanan.

Selain itu, implementasi kombinasi algoritma ini tidak memengaruhi pengalaman pengguna secara signifikan. Berdasarkan survei terhadap 100 pengguna aktif, 94% di antaranya menyatakan bahwa mereka tidak merasakan perbedaan dalam kecepatan akses atau proses pembayaran, meskipun terdapat peningkatan keamanan data. Hal ini menunjukkan bahwa solusi ini dapat diterapkan tanpa mengorbankan kenyamanan pengguna.

Perbandingan dengan Metode Keamanan Lain

Sebagai perbandingan, algoritma Triple DES (3DES) yang digunakan sebelumnya di platform ini memiliki waktu rata-rata enkripsi sebesar 3,5 milidetik per 1 MB data. Selain itu, tingkat keamanan 3DES lebih rendah karena panjang kunci yang lebih pendek dan kerentanan terhadap serangan brute-force. RSA juga dibandingkan dengan algoritma Diffie-Hellman, di mana RSA menunjukkan tingkat efisiensi dan keamanan yang lebih tinggi dalam konteks platform e-commerce dengan lalu lintas tinggi.

Rekomendasi untuk Pengembangan Selanjutnya

Berdasarkan hasil penelitian, direkomendasikan untuk mengintegrasikan teknologi quantum-resistant cryptography di masa depan. Komputasi kuantum, yang diperkirakan akan menjadi ancaman bagi algoritma RSA dalam beberapa dekade mendatang, dapat mengancam sistem keamanan jika tidak diantisipasi. Selain itu, peningkatan infrastruktur server, seperti penggunaan cloud computing dan teknologi kontainerisasi, dapat membantu menangani lonjakan lalu lintas selama periode promosi besar.

KESIMPULAN

Penelitian ini berhasil membuktikan bahwa kombinasi algoritma AES-256 dan RSA dapat meningkatkan keamanan data pada platform e-commerce Tokopedia secara signifikan. AES-256 memberikan efisiensi tinggi dalam proses enkripsi data sensitif, sedangkan RSA memastikan pengelolaan kunci enkripsi yang aman. Implementasi kombinasi algoritma ini mampu menahan lebih dari 85% serangan siber yang disimulasikan, seperti SQL Injection dan Cross-Site Scripting (XSS), tanpa mengorbankan pengalaman pengguna. Namun, penelitian juga mengidentifikasi tantangan, seperti penurunan performa saat terjadi lonjakan lalu lintas, yang memerlukan optimalisasi infrastruktur server. Rekomendasi pengembangan meliputi integrasi teknologi quantum-resistant cryptography untuk mengantisipasi ancaman di masa depan dan penerapan cloud computing untuk meningkatkan skalabilitas sistem. Dengan solusi ini, platform e-commerce dapat meningkatkan kepercayaan pengguna terhadap keamanan data mereka di era digital.

DAFTAR PUSTAKA

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

Stallings, W. (2016). *Cryptography and Network Security: Principles and Practice*. Pearson.

Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2), 120-126.

Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer.

National Institute of Standards and Technology (NIST). (2001). Advanced Encryption Standard (AES) (FIPS PUB 197). U.S. Department of Commerce.

OWASP Foundation. (2023). *OWASP ZAP – Zed Attack Proxy*. Retrieved from https://owasp.org/www-project-zap

Metasploit Project. (2023). *Metasploit Framework Documentation*. Retrieved from https://www.metasploit.com/

Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography*. CRC Press.

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

Goldreich, O. (2004). *Foundations of Cryptography: Basic Tools*. Cambridge University Press.

Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644-654.

Boneh, D., & Shoup, V. (2020). *A Graduate Course in Applied Cryptography*. Stanford University.

Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Fourth Estate.

Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

Shamir, A. (1979). How to Share a Secret. *Communications of the ACM*, 22(11), 612-613.

ISO/IEC 27001. (2013). *Information Security Management Systems — Requirements*. ISO.

Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.

Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177), 203-209.

Huth, M., & Ryan, M. (2019). *Logic in Computer Science: Modelling and Reasoning about Systems*. Cambridge University Press.

Bishop, M. (2018). *Introduction to Computer Security*. Addison-Wesley.

ENISA. (2022). *Threat Landscape 2022: Key Insights and Trends*. European Union Agency for *Cybersecurity*.

Chen, L., et al. (2016). *Report on Post-Quantum Cryptography*. NIST.

National Security Agency (NSA). (2016). *Commercial National Security Algorithm Suite*. NSA.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage Learning.

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley.

Hunt, T. (2023). *Have I Been Pwned? - Data Breach Notification Service*. Retrieved from https://haveibeenpwned.com

Arora, A., & Soni, P. (2021). Comparative Analysis of RSA and ECC Algorithms. *International Journal of Advanced Research in Computer Science*, 12(1), 1-7.

Zimmerman, P. R. (1995). *PGP Source Code and Internals*. MIT Press.

Kaspersky Lab. (2023). *Global Threat Report*. Retrieved from https://www.kaspersky.com

Cybersecurity and *Infrastructure Security Agency* (CISA). (2023). *Best Practices for Cybersecurity*. U.S. Department of Homeland Security.