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

The advancement of information and communication technology has brought significant changes in the e-commerce sector, including large platforms such as Tokopedia. With the increasing number of online transactions, user data security has become a very crucial aspect. Cyber threats, such as man-in-the-middle attacks, brute-force, and SQL injection, require the development of a more robust security system to protect sensitive user information. This study aims to analyze the application of modern cryptographic techniques, especially the AES-256 and RSA algorithms, in improving data security in e-commerce systems. By understanding the effectiveness of these algorithms, it is expected to provide useful recommendations for the development of security systems on e-commerce platforms. The method used in this study is descriptive qualitative with a case study approach on the XYZ e-commerce platform. Data were collected through interviews with the technical team, direct observation of the security system, and analysis of system documentation. This approach allows researchers to gain in-depth insight into the implementation and effectiveness of cryptographic techniques in a practical context. The results of the study show that the application of a combination of the AES-256 and RSA algorithms has succeeded in increasing the level of data security by up to 85%. AES-256 is able to encrypt user data with high efficiency, while RSA provides protection for the encryption key, thus minimizing the risk of data leakage. Penetration testing also confirmed that the system can withstand common cyber attacks. The study concluded that the combination of AES-256 and RSA algorithms is effective in enhancing data security on e-commerce platforms. The implementation of this cryptographic technique not only protects sensitive data but also maintains the user experience without sacrificing access speed. Recommendations for further development include the implementation of quantum-resistant cryptography technology and upgrading server infrastructure to overcome challenges when there is a traffic spike.

KATA KUNCI
keamanan komputer; kriptografi; *e-commerce;* AES-256; RSA.

ABSTRAK

Kemajuan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam sektor *e-commerce*, termasuk platform besar seperti Tokopedia. Dengan meningkatnya jumlah transaksi online, keamanan data pengguna menjadi aspek yang sangat krusial. Ancaman siber, seperti serangan *man-in-the-middle, brute-force*, dan SQL injection, menuntut pengembangan sistem keamanan yang lebih tangguh untuk melindungi informasi sensitif pengguna. Penelitian ini bertujuan untuk menganalisis penerapan teknik kriptografi modern, khususnya algoritma AES-256 dan RSA, dalam meningkatkan keamanan data pada sistem *e-commerce*. Dengan memahami efektivitas algoritma ini, diharapkan dapat memberikan rekomendasi yang bermanfaat untuk pengembangan sistem keamanan di platform *e-commerce*. Metode yang digunakan dalam penelitian ini adalah deskriptif kualitatif dengan pendekatan studi kasus pada platform *e-commerce* XYZ. Data dikumpulkan melalui wawancara dengan tim teknis, observasi langsung pada sistem keamanan, dan analisis dokumentasi sistem. Pendekatan ini memungkinkan peneliti untuk mendapatkan wawasan mendalam mengenai implementasi dan efektivitas teknik kriptografi dalam konteks praktis. Hasil penelitian menunjukkan bahwa penerapan kombinasi algoritma AES-256 dan RSA berhasil meningkatkan tingkat keamanan data hingga 85%. AES-256 mampu mengenkripsi data pengguna dengan efisiensi tinggi, sementara RSA memberikan perlindungan pada kunci enkripsi, sehingga meminimalkan risiko kebocoran data. Pengujian penetrasi juga mengkonfirmasi bahwa sistem dapat menahan serangan siber yang umum terjadi. Penelitian ini menyimpulkan bahwa kombinasi algoritma AES-256 dan RSA efektif dalam meningkatkan keamanan data pada platform *e-commerce*. Implementasi teknik kriptografi ini tidak hanya melindungi data sensitif, tetapi juga menjaga pengalaman pengguna tanpa mengorbankan kecepatan akses. Rekomendasi untuk pengembangan lebih lanjut termasuk penerapan teknologi quantum-resistant *cryptography* dan peningkatan infrastruktur server untuk mengatasi tantangan saat terjadi lonjakan trafik.

PENDAHULUAN

Kemajuan teknologi di sektor *e-commerce*, seperti Tokopedia, telah meningkatkan kebutuhan akan sistem keamanan yang andal (Beach et al., 2022). 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 (Boneh & Shoup, 2020). 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 (Stallings, 2019).

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 (Schneier, 1995).

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 (Katz & Lindell, 2020).

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 (Khounborine, 2023).

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 (Shahid et al., 2022).

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 system (Standardization, 2013).
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 (Ferguson et al., 2011).

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 (Alagic et al., 2019).

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 (Huth & Ryan, 2004).

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 (Almansoori et al., 2020).

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 (Mohamed & Mohamed, 2020).

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 (Mattioli & Malatras, 2024).

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 (Mishra & Bisoy, 2018)vv.

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

Alagic, G., Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.-K., Miller, C., Moody, D., & Peralta, R. (2019). *Status report on the first round of the NIST post-quantum cryptography standardization process*.

Almansoori, M., Lam, J., Fang, E., Mulligan, K., Soosai Raj, A. G., & Chatterjee, R. (2020). How secure are our computer systems courses? *Proceedings of the 2020 ACM Conference on International Computing Education Research*, 271–281.

Beach, P. M., Mailloux, L. O., Langhals, B. T., & Mills, R. F. (2022). Analysis of systems security engineering design principles for the development of secure and resilient systems. In *Handbook of Scholarly Publications from the Air Force Institute of Technology (AFIT), Volume 1, 2000-2020* (pp. 33–63). CRC Press.

Boneh, D., & Shoup, V. (2020). A graduate course in applied *cryptography*. *Draft 0.5*.

Ferguson, N., Schneier, B., & Kohno, T. (2011). *Cryptography engineering: design principles and practical applications*. John Wiley & Sons.

Huth, M., & Ryan, M. (2004). *Logic in Computer Science: Modelling and reasoning about systems*. Cambridge university press.

Katz, J., & Lindell, Y. (2020). *Introduction to modern cryptography crc press*. Taylor & Francis), Boca Raton, FL, USA.

Khounborine, C. (2023). *A Survey and Comparative Study on Vulnerability Scanning Tools*.

Mattioli, R., & Malatras, A. (2024). *Foresight cybersecurity threats for 2030: Update*.

Mishra, A., & Bisoy, S. K. (2018). Understanding the Aspect of *Cryptography* and Internet

Security: A Practical Approach. In *Handbook of e-Business Security* (pp. 31–49). Auerbach Publications.

Mohamed, K. S., & Mohamed, K. S. (2020). *Cryptography* concepts: Confidentiality. *New Frontiers in Cryptography: Quantum, Blockchain, Lightweight, Chaotic and DNA*, 13–39.

Schneier, B. (1995). Applied *cryptography* protocols. *Algorithms and Source Code in C*.

Shahid, J., Hameed, M. K., Javed, I. T., Qureshi, K. N., Ali, M., & Crespi, N. (2022). A comparative study of web application security parameters: Current trends and future directions. *Applied Sciences*, *12*(8), 4077.

Stallings, W. (2019). *Information privacy engineering and privacy by design: Understanding privacy threats, technology, and regulations based on standards and best practices*. Addison-Wesley Professional.

Standardization, I. O. for. (2013). *ISO/IEC 27001: 2013: Information Technology--Security Techniques--Information Security Management Systems--Requirements*. International Organization for Standardization.