ANALISA KEAMANAN E-COMMERCE MENGGUNAKAN METODE AES ALGORITMA

Luthfia Sodikin[1], Taufik Hidayat[2]
[1, 2] Department of Computer Engineering, Universitas Wiralora, Indonesia
[1]luthfiasodikin86903@gmail.com, [2] thidayat.ft@unwir.ac.id

ABSTRAK
E-Commerse yaitu kegiatan bertransaksi jasa atau barang dengan cara jarak jauh. Sarana ini digunakan menggunakan media internet. Berbagai manfaat yang kita dapatkan mulai dari lebih mudah dan lebih murah dibandingkan dengan pasar tradisional. Sistem E-Commerse memiliki beberapa aturan mencangkup sistem distribusi barang, sistem pembayaran, dan sistem informasi yang diterapkan. Agar semua data yang diberikan aman maka perlu memperhatikan asek keamanan. Kriptografi merupakan ilmu yang berhubungan dengan pengsadian yang mencangkup Enkripsi (plaintext) menjadi (ciphertext) dan Deskripsi (ciphertext) menjadi (plaintext). Ketiga hal itu berkaitan dengan metode yang saat ini kami gunakan dalam menganalisis Sistem keamanan E-Commerse. Metode AES (Advanced Encryption Standard) merupakan algoritma standar enkripsi kunci simetri yang dapat mengenkripsi dan mendekripsi.

Kata Kunci : E-Commerse, AES, Enkripsi, Deskripsi, Keamanan Jaringan.

ABSTRACT
E-Commerse, namely the activity of transacting services or goods by long distance. This facility is used using the internet media. The various benefits we get start from being easier and cheaper than traditional markets. The E-Commerse system has several regulations covering the goods distribution system, payment system, and information system applied. So that all the data provided is safe, it is necessary to pay attention to security aspects. Cryptography is a science that deals with sensing which includes encryption (plaintext) to (ciphertext) and description (ciphertext) to (plaintext). These three things relate to the methods we currently use in analyzing the E-Commerse security system. The AES (Advanced Encryption Standard) method is a standard symmetric key encryption algorithm that can encrypt and decrypt.

Keywords: E-Commerce, AES, Encryption, Description, Security Network.

PENDAHULUAN

Pada masa pandemik saat ini semua orang ditekankan untuk tetap dirumah saja dan menjaga jarak. Namun kebutuhan sehari-hari harus tetap tersedia dan tercukupi. E-Commerse merupakan bentuk transaksi perdagangan yang melibatkan Internet. Dengan E-Commerce pembeli bertransaksi dengan praktis dan biaya yang murah tanpa melalui proses tawar menawar, di mana pihak pembeli cukup mengakses internet kemudian mengetahui ketentuan-ketentuan yang berlaku oleh pihak penjual [1].

Sarana yang digunakan yakni bisa menggunakan marketplace online, website sendiri dan media sosial. Dengan begitu E-Commerse menjadi salah satu solusi untuk transaksi jual beli yang dilakukan dari jarak jauh. E-Commerce [2], [3]. Dalam transaksi E-Commerse terdapat 3 metode pembayaran yang bisa digunakan yakni: Online Processing Credit Card, Money Transfer Dan Cash On Delivery. Pada E-Commerse terdapat ketentuan-ketentuan yang perlu dipahami karena terdapat beberapa komponen yang terlibat yakni kosumen, Penjual, Produk, Front End, Infrastruktur, Back

End, Partner Bisnis, dan Support Service [4]. Sistem E-Commerse memiliki beberapa aturan mencangkup sistem distribusi barang, sistem pembayaran, dan sistem informasi yang diterapkan. Agar semua sistem tersebut berjalan sesuai dengan yang diharapkan maka perlu memperhatikan asek keamanan [5], [6].

Hal yang tidak diinginkan pada sistem keamanan E-Commerse ialah pencurian data costumer maupun kebocoran informasi rahasia dan berharga [7]. Kriptografi merupakan solusi untuk mengamankan informasi berupa melindungi kerahasiaan data dan melindungi pemalsuan dan pengubahan informasi data [8]. Saat ini perkembangan teknologi komputer semakin canggih, maka dari itu sistem keamanan membutuhkan algoritma kriptografi yang dapat dipercaya [9]. Dari penjelasan singkat tersebut penulis berupaya untuk menganilisis sistem keamanan E-Commerse yang digunakan marketplace dalam menjaga seluruh data dan informasi costumer seluruh Indonesia [10], [11].

METODE PENELITIAN

Metode penelitian menggunakan Metode AES (Advanced Encryption Standard) karena Kecepatan operasi pada algoritma ini lebih tinggi daripada algoritma asimetrik, dalam operasi matematis lebih kompleks contohnya pada bilangan prima. Algoritma ini tahan terhadap serangan exhaustive key search serta dapat digunakan pada sistem real-time contohnya GSM. Sebelum membahas Algoritma AES, lebih dulu kita membahas Kriptografi.

Kriptografi ilmu yang mencangkup menjaga kerahasiaan informasi berupa sandi-sandi yang harus diterjemahkan. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi [12], [13]. Tujuan dari Kriptografi sendiri memiliki aspek-aspek berikut ini:

1. Kerahasiaan (*Confidentiality*) yakni layanan untuk menjaga data agar tidak dapat dibaca oleh pihak yang tidak berkepentingan.
2. Integritas Data (Data Integrity) yakni layanan untuk menjamin bahwa data masih asli dan belum pernah diubah.
3. Otentikasi (Authentication) yakni layanan untuk mengidentifikasi kebenaran pihak-pihak yang bersangkutan.
4. Non-Repudiation yakni layanan agar seseorang tidak dapat menyangkal terkait sebuah transaksi yang dilakukannya . [17]

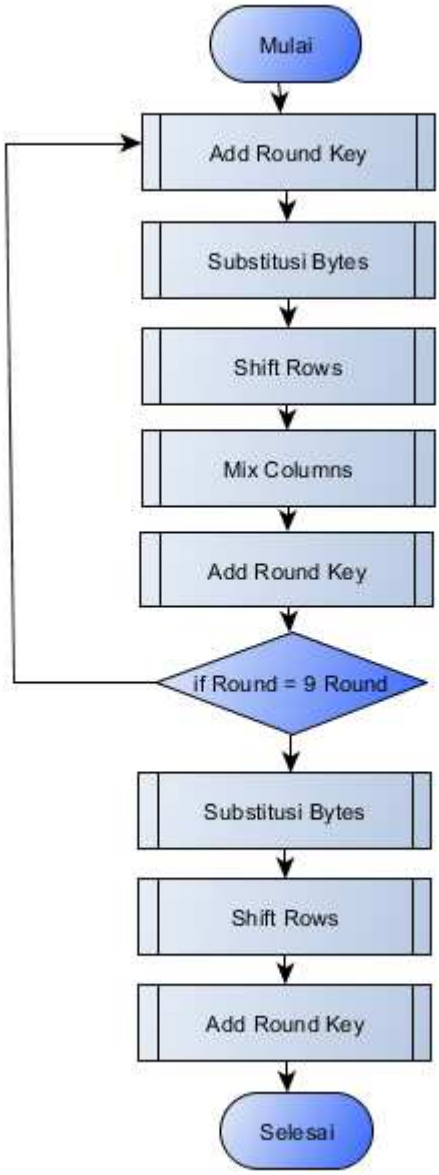
Metode AES (Advanced Encryption Standard) merupakan algoritma standar enkripsi kunci simetri yang dapat mengenkripsi dan mendekripsi. AES Algoritma memiliki 3 kunci kriptografi [14] untuk mengenkripsi dan mendekripsi informasi yakni 128 bit, 192 bit dan 256 bit. Ketiga kunci yang sudah terbentuk menjadi blok 128 bit atau plaintext. Perbedaan yang mempengaruhi jumlah putaran saat diaplikasikan pada AES Algoritma ialah panjang kunci [15], [16]. Berikut ini adalah tabel jumlah putaran (Nr) yang diaplikasikan pada masing masing panjang [17] kunci bisa dilihat pada tabel 1.

Tabel. 1 Perbandingan Jumlah Round dan Key

	Jumlah Key (Nk)	Ukuan Block (Nb)	Jumlah Putaran (Nr)
AES - 128	4	4	10
AES - 192	6	4	12
AES - 256	8	4	14

A. Proses Kriptografi Algoritma AES

Pada proses kriptografi engan menggunakan AES sebagai algoritmanya, ada bebrapa langkah yag harus dilalui pengirim sebelum mendapatkan hasil pesan yang telah disandikan, berikut ini flowchartnya:



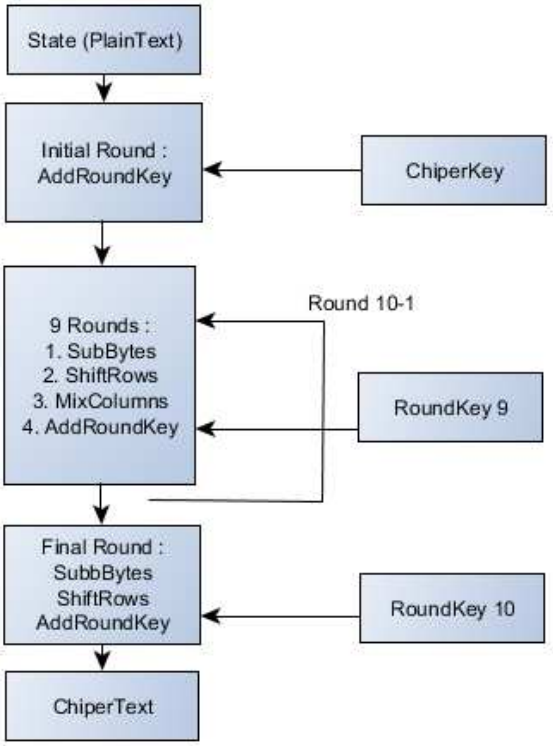
Gambar 1. Proses Algoritam AES [15]

B. Proses Enkripsi Alogritma AES

Enkripsi adalah proses pengubahan pesan asli (*plaintext*) menjadi pesan bersandi (*ciphertext*).

$$C = E(M) \quad (1)$$

Proses enkripsi dimulai dari input yang telah dimasukkan ke dalam state akan mengalami perubahan byte AddRoundKey [18]. Setelah itu, state akan mengalami perubahan SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak putaran [19]. Dibawah ini merupakan gambar diagram proses enkripsi seperti yang ditunjukkan pada Gambar 2.



Gambar 2. Diagram Proses Enkripsi AES

1. AddRoundKey: Melakukan XOR antara pesan asli dengan cipherkey.
2. Round: Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran yakni:
   a) SubBytes: Mensubstitusi byte dengan menggunakan tabel substitusi (S-box).
   b) ShiftRows: Pergeseran baris-baris array state secara wrapping.
   c) MixColumns: Mengalikan data di kolom-kolom array state.
   d) AddRoundKey: Melakukan XOR antara state sekarang dengan round key.
3. Final Round: Proses putaran terakhir yang meliputi
   A. SubBytes
   B. ShiftRows
   C. AddRoundKey [6]

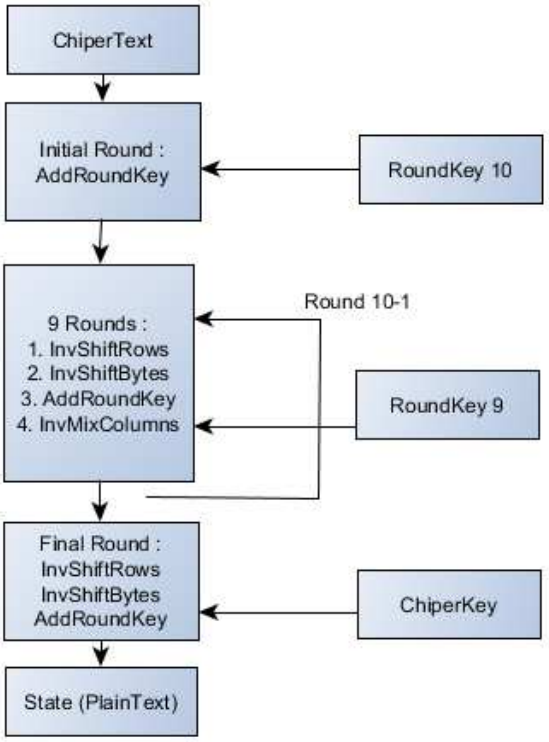
C. Proses Deskripsi Algoritma AES

Dekripsi proses pengubahan pesan bersandi (*ciphertext*) menjadi pesan asli (*plaintext*).

$$M = D(C) \quad (2)$$

Pada Deskripsi transformasi chipher dapat dibalikkan dan diaplikasikan dalam arah

yang berlawanan untuk menghasilkan inverse cipher yang mudah untuk dipahami [20]. Perubahan byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey [21], [22]. Dibawah ini merupakan gambar diagram proses deskripsi seperti yang ditunjukkan pada Gambar 3.



Gambar 3. Proses Deskripsi Algoritma AES

- InvShiftRows : Perubahan byte yang bergeser dari bit kiri ke kanan sedangkan pada ShiftRows dilakukan pergeseran bit kanan ke kiri.
- InvSubBytes : Perubahan bytes yang berkebalikan dengan transformasi SubBytes.
- InvMixColumns : Setiap kolom dalam state dikalikan dengan matrik perkalian dalam AES.

D. Ekspansi Kunci (Key Expansion)

AES Algoritma mengambil kunci primer dan melakukan rutin ekspansi kunci (key expansion) untuk menghasilkan key schedule. Kunci dipresentasikan menjadi word [wi]. SubWord merupakan fungsi yang mengambil 4 byte word input kemudian mengaplikasikan S-Box ke tiap-tiap data tersebt untuk menghasilkan word output. Fungsi RotWord mengambil word [a0, a1, a2, a3] sebagai input kemudian melakukan permutasi siklik, dan mengembalikan word [a1, a2, a3, a0]. Rcon[i] terdiri dari nilai-nilai yang diberikan oleh [xi-1, {00}, {00}, {00}], dengan xi-1 sebagai pangkat dari x (x dinotasikan sebagai {02} dalam field GF (28). Word ke Nk pertama pada ekspansi kunci berisi kunci cipher10.
Pada word berikutnya, w[i] = XOR dari word sebelumnya, w [i-1] dan word Nk yang ada pada posisi sebelumnya, w [i-Nk]. Untuk word pada posisi kelipatan Nk, sebuah perubahan diaplikasikan pada w [i-1] sebelum XOR, kemudian dilanjutkan oleh XOR dengan konstanta round, Rcon[i]. Perubahan ini meliputi pergeseran siklik dari byte data dalam suatu word RotWord, lalu diikuti aplikasi dari lookup Tabel untuk semua 4 byte data dari word SubWord.

HASIL DAN PEMBAHASAN

Berdasarkan analisis dari beberapa referensi yang kami dapatkan AES Algoritma memiliki memiliki kecepatan operasi lebih tinggi karena menggunakan jenis kunci simetri. AES Algoritma memiliki panjang kunci minimal 128 bit dengan perhitungan 2128 ≈ 3.4 x 1038 kemungkinan kunci. maka akan membutuhkan waktu 1010 tahun untuk mencoba seluruh kemungkinan kunci. AES Algoritma bersifat isomorphic karena memiliki medan GF (28) untuk setiap bilang prima yang selalu terdiri dari medan tunggal terbatas sehingga pemilihan polinomial biner berderajat 8m(x). Algoritma tersebut juga memiliki sifat irreducible yaitu pada medan selain 1 dan dirinya sendiri tidak dapat dibagi oleh bilangan lain. Kekuatan ini karena operasi matematis yang kompleks dan memerlukan sumber daya yang banyak untuk melakukan komputasi. Dengan begitu AES dapat dengan mudah dibuktikan keamanannya

KESIMPULAN

Hasil analisa yang dapat diperoleh dari Keamanan E-Commerce Menggunakan Metode AES Algoritma ialah dalam proses enkripsi dan deskripsi Algoritma ini terdapat medan tunggal terbatas yang unik untuk mengubah bilangan

prima dan pemilihan polynomial biner berderajat delapan.

AES Algoritma juga dapat bertahan menghadapi berbagai serangan. Terdapat 3 teknik yang dilakukan AES diantaranya : Differential Crytanalysis dan Linear Crynatalysis, Truncated Differentials, sertaThe Square Attacks dan Interpolation Attacks.

UCAPAN TERIMAKASIH

Penulis sangat sangat berterima kasih kepada seluruh pihak terutama kepada Department of Computer Engineering yang telah membantu kami menyelesaikan penulisan ini.

DAFTAR PUSTAKA

[1] B. Moriset, "e-Business and e-Commerce," in *International Encyclopedia of Human Geography*, Second Edi., vol. 4, Elsevier, 2020, pp. 1–10.

[2] C. Chiou-Wen and F. Chu, "The impact of internet finance in an open economy," *ACM International Conference Proceeding Series*, no. 2013, pp. 166–169, 2019, doi: 10.1145/3345035.3345055.

[3] T. V. Anh, H. T. T. Nguyen, and N. T. M. Linh, "Digital Transformation," in *Proceedings of the 2019 The World Symposium on Software Engineering - WSSE 2019*, 2019, no. 2017, pp. 119–124, doi: 10.1145/3362125.3362135.

[4] K. Konstantinos, M. Persefoni, F. Evangelia, M. Christos, and N. Mara, "Cloud computing and economic growth," *ACM International Conference Proceeding Series*, vol. 01–03–Octo, pp. 209–214, 2015, doi: 10.1145/2801948.2802000.

[5] T. R. Dillahunt, X. Wang, E. Wheeler, H. F. Cheng, B. Hecht, and H. Zhu, "The sharing economy in computing: A systematic literature review," *Proceedings of the ACM on Human-Computer Interaction*, vol. 1, no. CSCW, pp. 1–26, 2017, doi: 10.1145/3134673.

[6] N. Mohammed and N. Ibrahim, "Implementation of new secure encryption technique for cloud computing," *ICCISTA 2019 - IEEE International Conference on Computing and Information Science and Technology and their Applications 2019*, pp. 1–5, 2019, doi: 10.1109/ICCISTA.2019.8830668.

[7] T. Hidayat and R. Mahardiko, "A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing," *International Journal of Artificial Intelligence Research*, vol. 4, no. 1, pp. 49–57, Apr. 2020, doi: 10.29099/ijair.v4i1.154.

[8] K. Hariss, H. Noura, and A. E. Samhat, "Fully Enhanced Homomorphic Encryption algorithm of MORE approach for real world applications," *Journal of Information Security and Applications*, vol. 34, pp. 233–242, Jun. 2017, doi: 10.1016/j.jisa.2017.02.001.

[9] T. Hidayat, D. Sianturi Tigor Franky, and R. Mahardiko, "Forecast Analysis of Research Chance on AES Algorithm to Encrypt during Data Transmission on Cloud Computing," in *2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP)*, Sep. 2020, pp. 163–166, doi: 10.1109/BCWSP50066.2020.9249478.

[10] G. Park, S. R. Shin, and M. Choy, "Early mover (dis)advantages and knowledge spillover effects on blockchain startups' funding and innovation performance," *Journal of Business Research*, vol. 109, no. April 2019, pp. 64–75, 2020, doi: 10.1016/j.jbusres.2019.11.068.

[11] BPS, "Berita Resmi Statistik Pertumbuhan Ekonomi Indonesia Triwulan III-2019," *Berita Resmi Statistik*, vol. No. 15/02/, no. 15, pp. 1–12, 2019.

[12] B.-H. Lee, E. K. Dewi, and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," in *2018 27th Wireless and Optical Communication Conference (WOCC)*,

Apr. 2018, pp. 1–5, doi: 10.1109/WOCC.2018.8372705.

[13] N. Shimbre and P. Deshpande, "Enhancing distributed data storage security for cloud computing using TPA and AES algorithm," *Proceedings - 1st International Conference on Computing, Communication, Control and Automation, ICCUBEA 2015*, pp. 35–39, 2015, doi: 10.1109/ICCUBEA.2015.16.

[14] P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security," *Optik*, vol. 127, no. 4, pp. 2341–2345, Feb. 2016, doi: 10.1016/j.ijleo.2015.11.188.

[15] M. I. S. Reddy and A. P. S. Kumar, "Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm," *Procedia Computer Science*, vol. 85, no. Cms, pp. 62–69, 2016, doi: 10.1016/j.procs.2016.05.177.

[16] S. Ojha and V. Rajput, "AES and MD5 based secure authentication in cloud computing," *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, pp. 856–860, 2017, doi: 10.1109/I-SMAC.2017.8058300.

[17] D. Nuñez, I. Agudo, and J. Lopez, "Proxy Re-Encryption: Analysis of constructions and its application to secure access delegation," *Journal of Network and Computer Applications*, vol. 87, pp. 193–209, Jun. 2017, doi: 10.1016/j.jnca.2017.03.005.

[18] R. Dowsley, A. Michalas, M. Nagel, and N. Paladi, "A survey on design and implementation of protected searchable data in the cloud," *Computer Science Review*, vol. 26, pp. 17–30, Nov. 2017, doi: 10.1016/j.cosrev.2017.08.001.

[19] J. Gong, Y. Xu, and X. Zhao, "A Privacy-preserving Image Retrieval Method Based on Improved BoVW Model in Cloud Environment," *IETE Technical Review*, vol. 35, no. sup1, pp. 76–84, Dec. 2018, doi: 10.1080/02564602.2018.1526654.

[20] J. Domingo-Ferrer, O. Farràs, J. Ribes-González, and D. Sánchez, "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges," *Computer Communications*, vol. 140–141, no. December 2018, pp. 38–60, May 2019, doi: 10.1016/j.comcom.2019.04.011.

[21] G. Jain and V. Sejwar, "Improving the security by using various cryptographic techniques in cloud computing," in *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, Jun. 2017, vol. 2018–Janua, pp. 23–28, doi: 10.1109/ICCONS.2017.8250721.

[22] B. Suzic, A. Reiter, F. Reimair, D. Venturi, and B. Kubo, "Secure Data Sharing and Processing in Heterogeneous Clouds," *Procedia Computer Science*, vol. 68, no. 316, pp. 116–126, 2015, doi: 10.1016/j.procs.2015.09.228.