sistem tabungan santri hanya menggunakan *online tools* yaitu CrackStation, pengujian tersebut tidak menggunakan tambahan *wordlist* , karena itu pada penelitian ini diterapkan *wordlist* dalam serangan *bruteforce* untuk menguji lebih dalam, namun hasilnya tetap sama, tidak bisa dipecahkan. Adapun besaran *resource* mengalami kenaikan pada tabel untuk menyimpan data warga dan tabel untuk menyimpan data kartu keluarga. *Resource* mengalami kenaikan yang signifikan seperti yang terlihat pada Gambar 10 dan Gambar 11, hal tersebut dikarenakan adanya penambahan karakter dari data pada tiap kolom yang dienkripsi, namun hal tersebut tidak mengganggu kinerja sistem maupun *server*. Data merupakan dari salinan kartu keluarga yang langsung didapatkan dari ketua rukun tetangga Desa Sukaharja Karawang atas izin Kepala Desa. Data tersebut dimasukan ke dalam sistem pelayanan Desa dengan validasi sistem, jika data tersebut memenuhi validasi maka data akan dienkripsi lalu dimasukan ke dalam *database*, dalam pengujian ketahanan Algoritma AES, menggunakan teknik serangan *Bruteforce* dengan ataupun tidak menggunakan *wordlist*, hasil dari pengujian tersebut, Hashcat atau perangkat lunak yang digunakan dalam pengujian ini tidak dapat memecahkan, bahkan tidak dapat mengenali *chiper text* meskipun sudah menggunakan model yang sesuai dengan Algoritma yang digunakan. Maka dari itu, penulis beranggapan bahwa data warga Desa Sukaharja lebih aman dari serangan *Bruteforce* baik itu menggunakan *wordlist* dengan isi yang sesuai kandidat nilai asli, maupun tidak.

KESIMPULAN

Upaya pengamanan dalam sistem pelayanan Desa Sukaharja Karawang berbasis web menggunakan Algoritma AES-128 merupakan langkah yang baik dalam meminimalisir terjadinya kebocoran data. Proses enkripsi dan dekripsi yang dilakukan tidak memakan resource besar, bahkan dalam menampilkan 100 data pertama juga tidak membutuhkan waktu lama. Ketahanan Algoritma AES-128 terbukti dalam pengujiannya menggunakan teknik *Bruteforce* dengan bantuan perangkat lunak Hashcat versi 6.2.5, Algoritma AES-128 tahan dari serangan tersebut. Algoritma AES yang diterapkan tidak mengganggu kinerja sistem pelayanan desa, seperti hasil yang dilampirkan di atas dalam menampilkan 100 data pertama pada data kartu keluarga, dibutuhkan 761.02 *millisecond* setelah data terenkripsi dan dibutuhkan waktu 522 *millisecond* sebelum data terenkripsi. Sedangkan dalam menampilkan 100 data pertama data warga, dibutuhkan waktu 2.38 detik setelah data terenkripsi, dan dibutuhkan waktu 462.97 *millisecond* sebelum data terenkripsi. Pada basis data walaupun kenaikan resource terlihat jauh berbeda ketika data sudah dienkripsi, namun hal tersebut tidak mempengaruhi kepada kinerja *server* yang digunakan. Algoritma *Advanced Encryption Standard* dengan panjang 128 bit sangat direkomendasikan dalam upaya pengamanan data pada basis data berdasarkan hasil dari analisis yang telah dilakukan dan dilampirkan pada penelitian ini.

DAFTAR PUSTAKA

[1] A. Susilo, Y. Irawan, A. R. Pratama, and R. Antono, "Journal of Sisfotek Global RC4 Cryptography Implementation Analysis on Text Data ARTICLE HISTORY," *Issn*, vol. 11, no. 2, pp. 115–120, 2021, [Online]. Available: http://journal.stmikglobal.ac.id/index.php/sisfotek

[2] S. Al Busafi and B. Kumar, "Review and Analysis of Cryptography Techniques," *Int. Conf. Syst. Model. Adv. Res. Trends SMART(SMART)*, pp. 2–6, 2020, doi: 10.1109.

[3] D. Kr, V. K. R. Dwivedi, and M. C. Trivedi, "Encryption algorithm in cloud computing," *ScienceDirect*, vol. 37, no. 2, pp. 1869–1875, 2021, doi: 10.1016/j.matpr.2020.07.452.

[4] F. Tawfiq, A. Hussien, A. M. S. Rahma, H. Bahjat, and A. Wahab, "A Secure Environment Using a New Lightweight AES Algorithm for E-Commerce Websites," *Secur. Commun. Networks*, vol. 2021, p. 15, 2023, doi: https://doi.org/10.1155/2021/9961172.

[5] F. Fathurrahmad, "Development And Implementation Of The Rijndael Algorithm And Base-64 Advanced Encryption Standard (AES) For Website Data Security," *Int. J. Sci. Technol. Res.*, vol. 9, no. November, pp. 7–11, 2020.

[6] M. Farras, I. J. Volume, M. F. Muttaqin, S. Dian, and H. Permana, "Implementation of AES-128 and Token-Base64 to Prevent SQL Injection Attacks via HTTP," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, pp. 2876–2882, 2020, doi: https://doi.org/10.30534/ijatcse/2020/60932020.

[7] M. Al-Mashhadani and M. Shujaa, "IoT Security Using AES Encryption Technology based ESP32 Platform," *Int. Arab J. Inf. Technol.*, vol. 19, no. 2, pp. 214–223, 2022, doi: 10.34028/iajit/19/2/8.

[8] S. Fatima, T. Rehman, M. Fatima, S. Khan, and M. A. Ali, "Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing †," *Eng. Proc.*, vol. 20, no. 1, 2022, doi: 10.3390/engproc2022020014.

[9] H. B. Setiawan and F. U. Najicha, "Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data,"

J. Kewarganegaraan, vol. 6, no. 1, pp. 976–982, 2022.

[10] O. Maulida and H. Utomo, "Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan Atas Kebocoran Data Pribadi Pengguna dalam Perspektif Hukum Pidana," *Indones. J. Law Justice*, vol. 1, no. 2, p. 10, 2023, doi: 10.47134/ijlj.v1i2.2011.

[11] Muhammad Raihan, "Perlindungan Data Diri Konsumen Dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia)," *J. Inov. Penelit.*, vol. 3, no. 10, pp. 7847–7856, 2023.

[12] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy," *J. Tek. Inform.*, vol. 1, no. 2, pp. 69–77, 2020, doi: 10.20884/1.jutif.2020.1.2.21.

[13] B. A. Iswandari, "Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance," *J. Huk. Ius Quia Iustum*, vol. 28, no. 1, pp. 115–138, 2021, doi: 10.20885/iustum.vol28.iss1.art6.

[14] R. Luthfi, "Perlindungan Data Pribadi sebagai Perwujudan Perlindungan Hak Asasi Manusia," *J. Sos. Teknol.*, vol. 2, no. 5, pp. 431–436, 2022, doi: 10.59188/jurnalsostech.v2i5.336.

[15] Gatot Efrianto and Nia Tresnawaty, "Pengaruh Privasi, Keamanan, Kepercayaan Dan Pengalaman Terhadap Penggunaan Fintech Di Kalangan Masyarakat Kabupaten Tangerang Banten," *J. Liabilitas*, vol. 6, no. 1, pp. 53–72, 2021, doi: 10.54964/liabilitas.v6i1.71.

[16] B. E. Nino, "Perbandingan Performa Algoritma AES dan Twofish Menggunakan Metode Strict Avalanche Criterion pada Nomor Induk Kependudukan Indonesia," *J. Teknol. Inf.*, vol. 9, no. 1, pp. 19–29, 2023, doi: 10.52643/jti.v9i1.2994.

[17] D. Puspitasari, I. Izzatusholekha, and S. K. Haniandaresta, "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Mengatasi Masalah Keamanan Data Penduduk," *J. Adm. Sos. Sci.*, vol. 4, no. 2, pp. 195–205, 2023, doi: https://doi.org/10.55606/jass.v4i2.403.

[18] R. F. Anggitafani, "Perlindungan Hukum Data Pribadi Peminjam Pinjaman Online Perspektif Pojk No. 1/Pojk.07/2013 tentang Perlindungan Konsumen Sektor Keuangan dan Aspek Kemaslahatan," *J. Islam. Bus. Law*, vol. Vol. 2, no. No. 2, pp. 56–72, 2021.

[19] A. Abdalrahman, "A Cloud Database based on AES 256 GCM Encryption Through Devolving Web application of Accounting Information System," *Int. J. Recent Technol. Eng.*, vol. 9, no. 5, pp. 216–221, 2021, doi: 10.35940/ijrte.e5269.019521.

[20] A. Fadlil, I. Riadi, and A. Nugrahantoro, "Data Security for School Service Top-Up Transactions Based on AES Combination Blockchain Technology," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 11, no. 3, p. 155, 2020, doi: 10.24843/lkjiti.2020.v11.i03.p04.

[21] E. Fernando, H. Rohayani, and D. Irsan, Muhammad, Dine, Agustin, Sujana, "Performance Comparison of Symmetries Encryption Algorithm AES and DES With Raspberry Pi," *IEEE*, pp. 353–357, 2019, doi: 10.1109/SIET48054.2019.8986122.

[22] P. Gaur, "AES Image Encryption (Advanced Encryption Standard)," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 9, no. 12, pp. 1357–1363, 2021, doi: 10.22214/ijraset.2021.39542.

[23] J. Kaur, S. Lamba, and P. Saini, "Advanced Encryption Standard: Attacks and Current Research Trends," *2021 Int. Conf. Adv. Comput. Innov. Technol. Eng. ICACITE 2021*, vol. 7, pp. 112–116, 2021, doi: 10.1109/ICACITE51222.2021.9404716.

[24] K. Shahbazi, S. Ko, and S. Member, "Area-Efficient Nano-AES Implementation for Internet-of-Things Devices," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 29, pp. 136–148, 2020, doi: 10.1109/TVLSI.2020.3033928.

[25] S. M. Kareem and A. M. S. Rahma, "New method for improving add round key in the advanced encryption standard algorithm," *Inf. Secur. J.*, vol. 30, no. 6, pp. 371–383, 2021, doi: 10.1080/19393555.2020.1859654.

[26] T. M. Kumar, K. S. Reddy, S. Rinaldi, B. D. Parameshachari, and K. Arunachalam, "A low area high speed fpga implementation of aes architecture for cryptography application," *Electron.*, vol. 10, no. 16, 2021, doi: 10.3390/electronics10162023.

[27] M. Hasanudin and M. N. Dasaprawira, "Pengujian aplikasi tabungan santri berbasis web dengan menggunakan algoritma kriptografi advance encryption standard (aes) 256.," vol. 1, no. 1, pp. 11–18, 2022.