JITKOM

Jurnal Ilmu Teknik dan Komputer
Vol. 07. No. 01, Januari 2023: 1-6
p-ISSN: 2548-740X e-ISSN: 2621-1491

Penerapan Algoritma AES 256 *Database Mysql* Pada Aplikasi Berbasis *Web*

Bimo Prakoso

Teknik Informatika, Universitas Mercu Buana, Jakarta
41519120033@mercubuana.ac.id

Seiring berkembangnya teknologi informasi dalam keseharian khususnya masyarakat Indonesia dan di dunia pada umumnya. Perubahan besar dan signifikan yang terjadi pada saat pandemi Covid-19 membuat perilaku masyarakat yang sering berinteraksi secara tatap muka kini lebih memilih untuk berkomunikasi secara virtual. Sejalan dengan dinamika tersebut, banyak instansi pemerintahan pun menerapkan layanan-layanan digital dimana pelayanan publik kini bisa dilakukan secara elektronik. Kebocoran data di Indonesia yang kerap terjadi tak luput dari semakin berkembangnya teknologi digital yang secara tidak langsung di pelopori oleh pandemi Covid-19 yang membuat banyak pihak ingin mendapatkan keuntungan dari data pengguna. Penelitian ini dimaksudkan untuk menambah keamanan dari segi basis data yang dienkripsi menggunakan metode algoritma AES 256 pada aplikasi web Penilaian Kinerja Pegawai. Perbedaan dengan penelitian terkait sebelumnya adalah terletak pada penggunaan metode AES. Jika pada penelitian sebelumnya dibuat enkripsi AES pada URL aplikasi web agar tidak dapat dibobol peretas dari URL yang terlihat di browser menggunakan software sniffer seperti wireshark, kemudian meletakkan algoritma AES pada sisi basis data agar saat terjadi kebocoran data, walaupun peretas bisa melihat isi basis data namun tetap tidak dapat menggunakan data pengguna karena telah ter-enkripsi. Hasil penelitian menunjukan waktu proses yang dibutuhkan untuk akses aplikasi pada saat diimplementasikan algoritma AES 256 ini meningkat sekitar 3-5% dari sebelum diimpementasikan algoritma tersebut.

Article History:
Received: Dec 22, 2023
Revised: Feb 25, 2023
Accepted:Feb 28, 2023
Published: Mar 29, 2023

Kata Kunci : Algoritma; AES 256; Database; Aplikasi.

DOI: 10.22441/jitkom.v7i1.001

I. PENDAHULUAN

Seiring berkembangnya teknologi informasi dalam keseharian khususnya masyarakat Indonesia dan di dunia pada umumnya. Perubahan besar dan signifikan yang terjadi pada saat pandemi Covid-19 membuat perilaku masyarakat yang sering berinteraksi secara tatap muka kini lebih memilih untuk berkomunikasi secara virtual. Sejalan dengan dinamika tersebut, banyak instansi pemerintahan pun menerapkan layanan-layanan digital dimana pelayanan publik kini bisa dilakukan secara elektronik. Pun dengan inovasi-inovasi yang bermunculan tak menutup kemungkinan adanya celah bagi para pelaku kejahatan untuk melancarkan aksinya. Banyak sudah terjadi kebocoran data pada instansi-instansi yang mengalihkan kegiatan pelayanannya ke pelayanan digital. Seperti contoh kebocoran data pengguna BPJS yang berisikan nama dan alamat valid para pengguna [3], juga ada kebocoran data E-HAC yang berisikan nama, nomor KTP, serta riwayat perjalanan [2]. Tak hanya itu e-commerce nomor satu di Indonesia Tokopedia pun turut tercoreng kredibilitas keamanan data penggunanya dimana data alamat, nama, dan password dapat diperoleh dengan mudah oleh hacker[3].

Kebocoran data di Indonesia yang kerap terjadi tak luput dari semakin berkembangnya teknologi digital yang secara tidak langsung di pelopori oleh pandemi Covid-19 yang membuat banyak pihak ingin mendapatkan keuntungan dari data pengguna. Beberapa penelitian telah mengangkat tema ini seperti yang dilakukan oleh Muhammad Fathur [2] yang membahas tanggung jawab pihak Tokopedia atas kebocoran data tersebut dan Nadhif Ikbar Wibowo, Tri Andika Maulana, Hamzah Muhammad, Nur tAini Rakhmawati [4] Aplikasi Web Penilaian Kinerja Pegawai yang kini sedang berjalan sudah tertata rapi namun dari sisi keamanan ada kerentanan yang cukup besar dimana jika ada kebocoran data maka peretas akan dapat melihat data tersebut secara keseluruhan.

Penelitian ini dimaksudkan untuk menambah keamanan dari segi basis data yang dienkripsi menggunakan metode algoritma AES 256 pada aplikasi web Penilaian Kinerja Pegawai. Perbedaan dengan penelitian terkait sebelumnya adalah terletak pada penggunaan metode AES. [5][6][7] Jika pada penelitian sebelumnya dibuat enkripsi AES pada URL aplikasi web agar tidak dapat dibobol peretas dari URL yang terlihat di browser menggunakan software sniffer seperti wireshark, kemudian meletakkan algoritma AES pada sisi basis data agar saat terjadi kebocoran data, walaupun peretas bisa melihat isi basis data namun tetap tidak dapat menggunakan data pengguna karena telah ter-enkripsi. [8][9][10]

Peneliti akan menggandakan aplikasi yang tengah berjalan di server kantor ke dalam server pribadi dengan data dummy lalu dipasang di domain pribadi agar kerahasiaan dan privasi data sensitif terkait kepegawaian instansi dapat terjaga. Peneliti akan memasang algoritma AES pada proses transaksi GET dan POST di dalam transaksi CRUD (Create, Read, Update dan Delete)

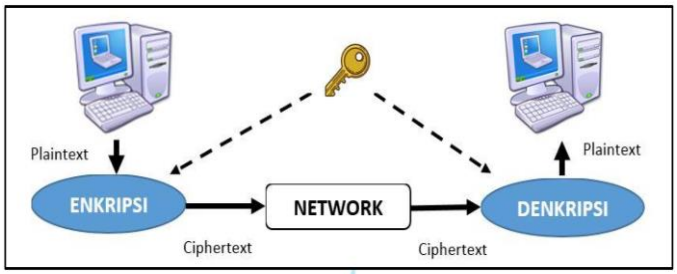
pada aplikasi, lalu membandingkannya dengan kondisi sebelum dipasangnya algoritma AES pada arus lalu lintas data pada aplikasi.[11]

II. LITERATURE REVIEW

Berbagai perkembangan telah banyak dilakukan oleh para programmer di seluruh dunia terkait mengamankan data yang ada pada database aplikasi berbasis web yang seringkali dibuat dengan bahasa pemrograman MySQL yang memiliki enkripsi sebesar 128 bit. Namun peretasan kerap terjadi karena metode yang digunakan belum dapat mencegah 100% serangan yang terjadi setiap menitnya. Untuk itu dipilih metode AES 256 dalam enkripsi database MySQL pada aplikasi berbasis web agar keamanan data lebih terjamin walaupun tidak 100%, tapi setidaknya dapat meminimalisir terjadinya kebocoran data pada database. [12][13] [14]

Kriptografi Berasal dari bahasa Yunani yang terdiri dari 2 (dua) suku kata yaitu kripto dengan arti menyembunyikan dan grafi dengan arti tulisan. Kriptografi memiliki arti ilmu yang mempelajari teknik-teknik sistematika yang berhubungan dengan aspek keamana informasi, kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [3]. Tetapi tidak semua aspek dapat diselesaikan dengan kriptografi. Kriptografi juga dapat di artikan sebagai ilmu atau seni untuk menjaga keamanan dari sebuah pesan [15].

Enkripsi merupakan sebuah proses dari pesan yang dapat dibaca (plaintext) menjadi pesan yang sudah dirubah susunannya menjadi tidak dapat dibaca (ciphertext) [15].



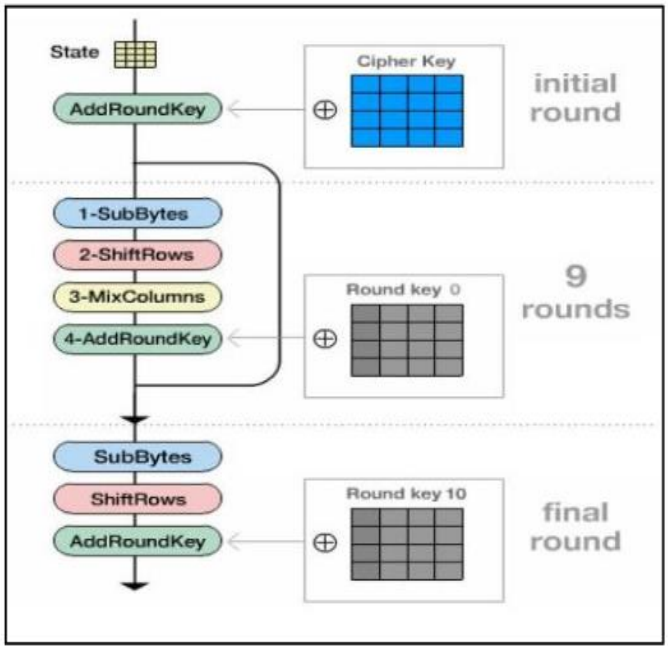
Gambar 1. Metode Enkripsi

Enkripsi yang digunakan dalam penelitian ini adalah enkripsi AES (Advanced Enkription Standard) yang menurut pakar dinilai lebih baik dibandingkan dengan metode enkripsi AES yang lainnya [1]. Enkripsi AES ini diperkenalkan oleh Rijndael (Vincent Rijmen dan Joan Daemen – Belgia) pada saat sayembara NIST (National Institute of Standards and Technology). Rijndael di pilih karena keamanan algoritma, efisien, fleksibelitas dan kebutuhan memory yang sedikit [15].

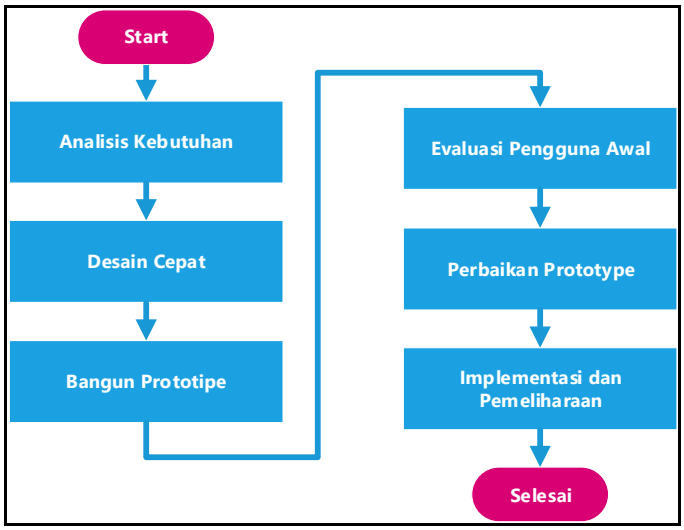
III. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode kuantitatif deskriptif, yang bertujuan membuat deskripsi yang akurat, faktual, dan sistematis pada fakta tertentu. Metode ini difokuskan untuk membuat gambar atau deskriptif tentang suatu keadaan secara objektif yang menggunakan angka, mulai dari pengumpulan data, penafsiran terhadap data tersebut serta penampilan dan hasilnya.

Penelitian yang dilakukan adalah pengembangan perangkat lunak menggunakan metode prototipe yang merupakan teknik pengembangan sistem yang menggunakan prototipe untuk menggambarkan sistem sehingga klien atau pemilik sistem mempunyai gambaran jelas pada sistem yang akan dibangun oleh tim pengembang dengan tahapan pada Gambar 3.



Gambar 2. Alur Enkripsi AES



Gambar 3. Diagram Alir Penelitian

Analisis Kebutuhan

Beberapa informasi didapatkan pada media internet untuk mengetahui mengapa masih banyak terjadi peretasan padahal di dalam database sudah melakukan metode enkripsi. Permasalahan yang sering muncul adalah peretas mampu menjebol enkripsi yang dipasang dengan metode brute force. Kebutuhan yang muncul pada tempat kerja mengharuskan adanya perubahan dari penggunaan metode AES 128 menjadi AES 256 agar data yang ter-enkripsi lebih sulit diretas.

Desain Cepat

Desain cepat yang dilakukan terhadap sistem yang sudah berjalan dilakukan dalam waktu singkat dan menghasilkan

konsep sederhana gambaran awal pengembangan perangkat lunak.

Bangun Prototipe

Konsep sederhana yang telah dibuat dan disetujui oleh user dibuatkan prototipenya sesuai dengan kesepakatan pada langkah 2.

Evaluasi Pengguna Awal

Setelah prototipe dibuat dan dicoba oleh user maka user bisa memberikan feedback terhadap prototipe tersebut apa kurang dan lebihnya yang ingin ditambahkan ke dalam perangkat lunak berbasis web tersebut.

Perbaikan Prototipe

Prototipe akan dilakukan perbaikan, baik dalam bentuk penambahan ataupun pengurangan fitur sesuai dengan feedback yang diberikan oleh pengguna pada tahap 4. Lalu akan kembali ke tahap 4 sampai dicapai kesepakatan bahwa perangkat lunak tersebut layak untuk dirilis sebagai pengembangan lanjutan.

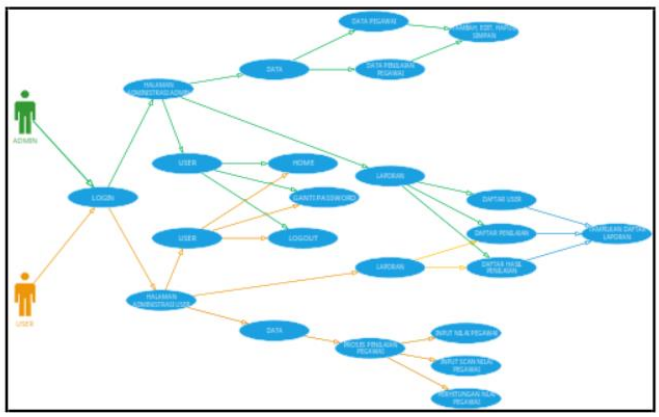
Implementasi dan Pemeliharaan.

Prototipe yang telah dilakukan pengujian dan perbaikan akan dirilis menjadi produk pengembangan sesuai dengan tujuan awal pengembangan perangkat lunak. Selanjutnya dilakukan pemeliharaan rutin agar perangkat lunak dapat berjalan dengan baik.

IV. HASIL DAN ANALISA

A. *Use Case Diagram*

Secara umum *Use Case Diagram* merupakan gambaran fungsional dari suatu sistem yang dibuat, sehingga pengguna mengerti kegunaan sistem yang akan dibangun. *Use Case Diagram* dalam aplikasi ini seperti dapat dilihat pada Gambar 4.



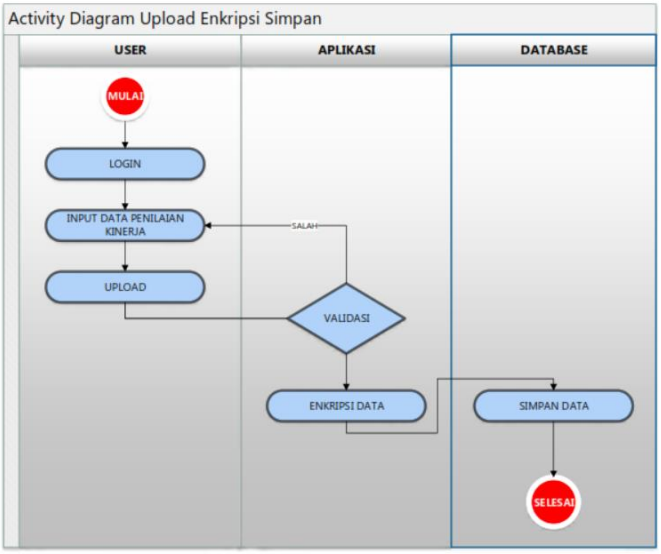
Gambar 4. *Use Case Diagram*

B. *Activity Diagram*

Alur kerja dari aplikasi Penilaian Kinerja Pegawai dapat lebih lanjut didetailkan pada Activity Diagram. Aktivitas ini akan dibagi menjadi beberapa ketegori berdasarkan kegiatan yang user dapat lakukan dengan sistem ini.

Activity Diagram Upload Enkripsi Simpan

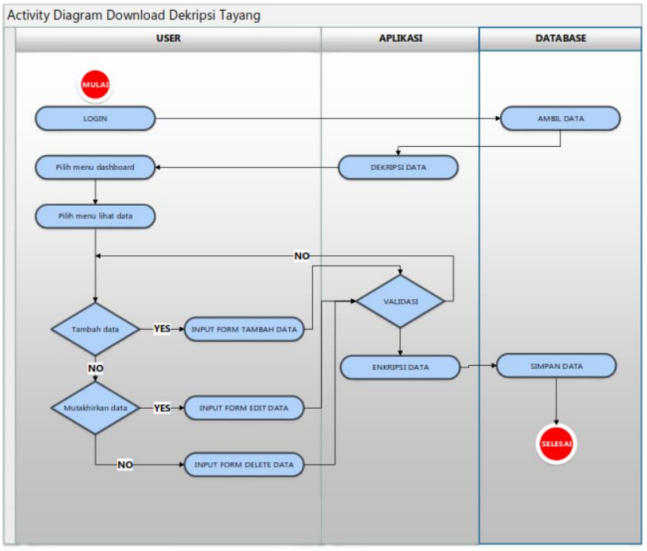
Activity diagram Upload Enkripsi Simpan digunakan untuk menggambarkan alur kerja user menjalankan aplikasi Penilaian Kinerja Pegawai, dengan terbih dahulu input username dan password masing- masing sesuai akun yang telah ditentukan. Jika username dan password yang diinputkan benar maka login berhasil dan akan menampilkan halaman utama. Proses enkripsi berada saat user menekan tombol upload, lalu aplikasi melakukan enkripsi terhadap semua file yang diupload, lalu disimpan di database dalam bentuk enkripsi seperti dapat dilihat pada Gambar 5.



Gambar 5. *Activity Diagram Upload Eknripsi* Simpan

Activity Diagram Download Dekripsi Tayang

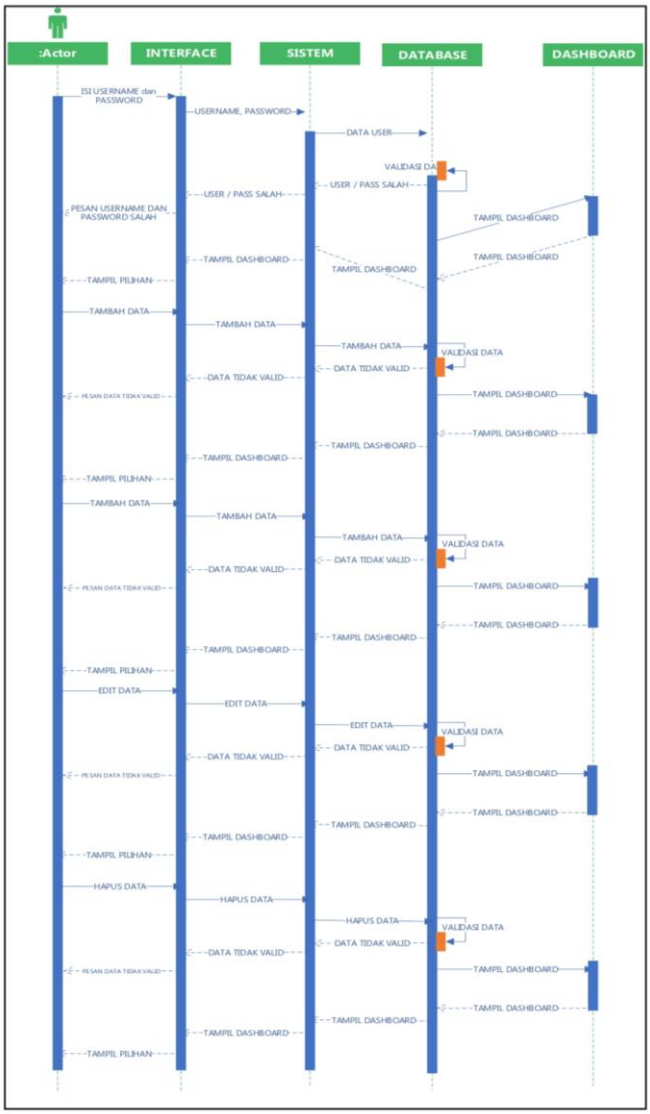
Activity diagram Download Dekripsi Tayang digunakan untuk menggambarkan alur kerja user dalam melakukan interaksi dengan aplikasi berupa penambahan data, pemutakhiran data, dan penghapusan data. Data yang terdapat di dalam database akan di dekripsi terlebih dahulu sebelum ditayangkan ke user interface, setelah itu baru user bisa melakukan keloa data yang terdaapt di dalam database. Berikut gambar activity diagram untuk kelola data penilaian kinerja. seperti dapat dilihat pada gambar 6.



Gambar 6. *Activity Diagram* Kelola Data Penilaian Kinerja

C. Sequence Diagram

Diagram sequence mendeskripsikan bagaimana entitas dalam sistem berinteraksi, termasuk pesan yang digunakan saat interaksi. Semua pesan dideskripsikan dalam urutan dari eksekusi. Diagram sequence berhubungan erat dengan diagram use case , dimana 1 use case akan menjadi 1 diagram sequence. seperti dapat dilihat pada gambar 7.



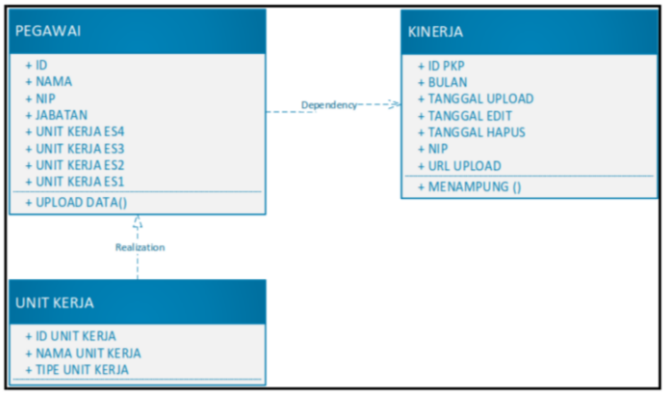
Gambar 8. *Sequence Diagram*

D. Class Diagram

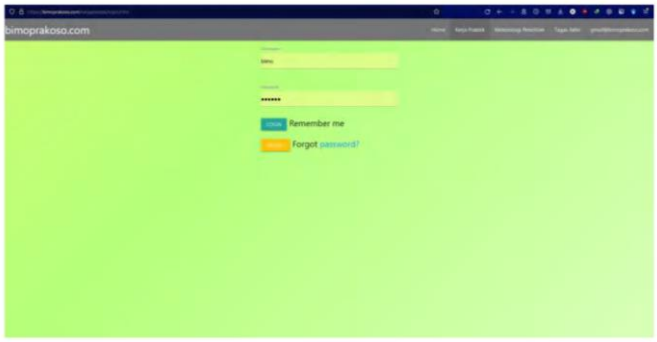
Class diagram merupakan spesifikasi dari pengembangan dan desain berorientasi objek yang menggambarkan struktur dan deskripsi class, package dan objek beserta hubungan satu sama lain seperti containment, pewarisan, asosiasi, dan lain-lain. seperti dapat dilihat pada gambar 9.

E. User Interface

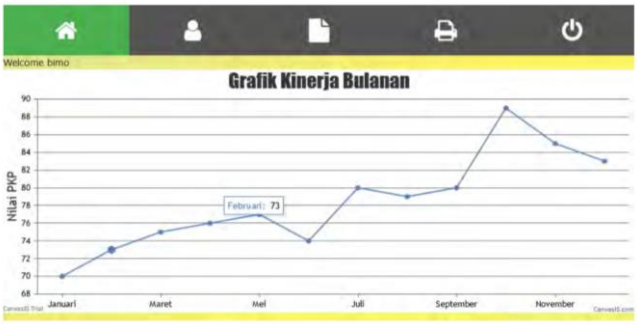
Aplikasi yang dibuat adalah duplikasi salah satu modul yang telah terdapat dalam integrasi sistem di perusahaan tempat penulis bekerja yaitu Penilaian Kinerja Pegawai, dimana modul tersebut menjadi percobaan untuk penerapan algoritma AES 256. Tampilan antar muka dari aplikasi seperti dapat dilihat di gambar 10 sampai 13.



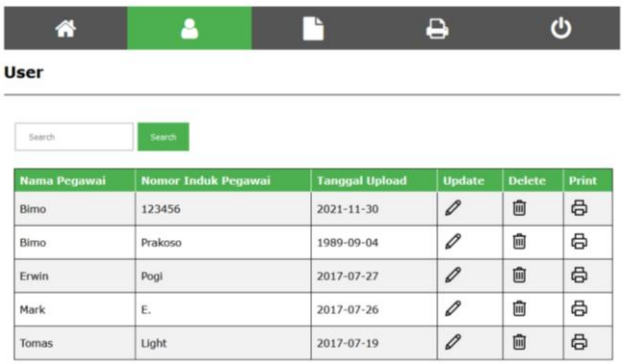
Gambar 9. *Class Diagram*



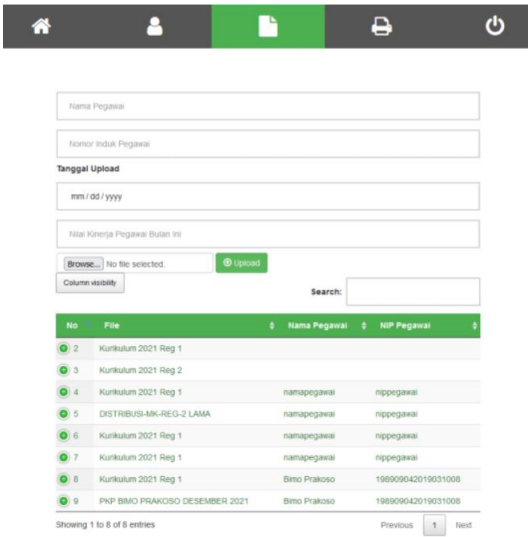
Gambar 10. Halaman Login



Gambar 11. Halaman Dashboard



Gambar 12. Halaman User



Gambar 13. Halaman Upload PKP

F. Analisis Hasil

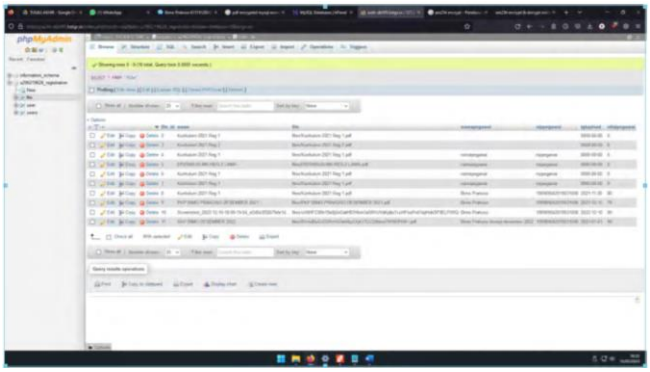
Ujicoba penerapan algoritma AES 256 yang dilakukan pada database aplikasi Penilaian Kinerja Pegawai melalui 2 tahap yaitu uji aplikasi dan uji algoritma.

Pengujian Aplikasi

Aplikasi yang dibuat adalah merupakan duplikasi dari modul sistem integrasi di tempat kerja dimana modul tersebut menjadi percobaan untuk penerapan algoritma AES 256 sebelum diterapkan secara menyeluruh ke setiap modul yang berada dalam naungan sistem integrasi. Pengujian aplikasi dilakukan pada semester 2 2021 bertepatan dengan momentum banyaknya aplikasi buatan pemerintah banyak yang terkena musibah kebocoran data pengguna yang tidak terenkripsi di dalam databasenya, melainkan hanya enkripsi pada login dan antarmukanya saja.

Pengujian Algoritma

Algoritma yang diterapkan ke dalam database membuat isi database yang tidak dapat diketahui maknanya karena berupa cipher text yang telah terenkripsi dengan metode AES 256. Tidak seorangpun dapat mengetahui apa arti dari text yang terdapat di database bahkan oleh administrator sekalipun. Jika ingin mengetahui isi database maka harus membuka aplikasi dan melakukan autorisasi sebelum bisa melihat data yang tersimpan di database. Contoh tampilan data yang terdapat di database sebagai berikut.



Gambar 14. Data terenkripsi di database

V. KESIMPULAN

Berdasarkan rumusan masalah, implementasi, dan analisa sistem, maka data yang telah di enkripsi dapat ditampilkan kembali sesuai dengan bentuk awal dengan proses dekripsi tanpa mengubah apapun, dapat dilihat dari ukuran file yang tidak mengalami perubahan saat sebelum dienkripsi dan setelah didekripsi. Waktu proses yang dibutuhkan untuk akses aplikasi pada saat diimplementasikan algoritma AES 256 ini meningkat namun tidak signifikan, hanya sekitar 3-5% dari sebelum diimpementasikan algoritma tersebut. Data yang telah dienkripsi dan masuk ke database adalah data yang telah berubah dalam bentuk cypher sehingga tidak akan diketahui maknanya jika dilihat oleh pihak yang tidak bertanggung jawab. Pihak yang dapat melihat data tersebut adalah hanya pengguna karena merupakan data pribadi pengguna, bahkan admin database, admin website, admin jaringan pun tidak akan bisa mengetahui isi dari database tersebut kecuali mengetahui kode key dari proses enkripsi dekripsi, dimana key ini hanya diketahui oleh programmer. Sehingga sangat meminimalisir peluang celah dan memudahkan penyelidikan ketika terjadi kebocoran data karena yang bisa mengakses hanya beberapa orang saja.

Karena enkripsi hanyalah sebuah metode yang meminimalisir kemungkinan terjadinya kebocoran data, perlu adanya monitoring dan evaluasi khusus untuk perubahan key yang dinamis dan tidak memerlukan campur tangan admin, karena ketika ada maintenance yang membutuhkan perubahan di dalam file website, rentan sekali file enkripsi dan dekripsi dapat dilihat umum. Terlihat dari saat melakukan penerapan algoritma ini di tempat bekerja, penentuan key ciphernya masih dalam bentuk manual yaitu mengetik di notepad dan copy paste ke dalam file enkripsi dekripsi yang ditempatkan di dalam folder server.

DAFTAR PUSTAKA

[1] R. Andriyanto, K. Khairijal, and D. Satria, “Penerapan Kriptografi AES Class Untuk Pengamanan URL WEBSITE Dari Serangan SQL Injection,” *Jurnal Unitek*, vol. 13, no. 1, pp. 34–48, Jun. 2020, doi: https://doi.org/10.52072/unitek.v13i1.153.

[2] M. Fathur, “Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen,” *National Conference on Law Studies (NCOLS)*, vol. 2, no. 1, pp. 43–60, 2020.

[3] A. Prihantini, Master Bahasa Indonesia, Yogyakarta: PT Bentang Pustaka, 2015.

[4] N. I. Wibowo, T. A. Maulana and N. Aini, "Perbandingan Algoritma Klasifikasi Sentimen Twitter Terhadap Insiden Kebocoran Data Tokopedia," *in JISKa*, Vol. 6, No. 2, Mei, pp. 120-129, 2021.

[5] H. S. Tambunan, I. Gunawan, R. S. Novica Aswita, Z. M. Nasution, and S. Sumarno, “Implementasi Algoritma AES & RC4 Terhadap Keamanan Data Produk Benih Sayuran di PT. Ewindo,” *Jurnal Sosial Sains*, vol. 1, no. 6, pp. 461–468, Jun. 2021, doi: https://doi.org/10.36418/sosains.v1i6.126.

[6] D. M. O. Wibowo, E. D. Astuti and H. Sibyan, "Implementasi Algoritma Advanced Encryption Standard (AES) Untuk Keamanan QR-Code Sebagai Digital Signature Pada Aplikasi E-Surat," in *Journal of Economic, Business and Engineering (JEBE)*, Vol. 3, No. 1, 2021.

[7] A. Ignasius and D. V. Shaka Yudha Sakti, “Penerapan Algoritma AES (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di PT. Gunung Geulis Elok Abadi,” *SKANIKA*, vol. 5, no. 1, pp. 1–10, Jan. 2022, doi: https://doi.org/10.36080/skanika.v5i1.2118.

[8] A. Nugrahantoro, A. Fadlil and I. Riadi, "Optimasi Keamanan Informasi Menggunakan Algoritma Advanced Encryption Standard (AES) Mode Chiper Block Chaining (CBC)," in *Jurnal Ilmiah FIFO*, vol. 12, no. 1, 2020.

[9] J. A. Saputra, J. Andjarwirawan, and L. P. Dewi, "Implementasi Algoritma AES, ElGamal, dan SHA3 untuk Keamanan File Digital," *Jurnal Infra*, vol. 9, no. 2, pp. 96–102, 2021, Accessed: Mar. 21, 2023. [Online]. Available: https://publication.petra.ac.id/index.php/teknik-informatika/article/view/11431

[10] R. Priambudi, "Penerapan Algoritma Kriptografi AES (Advanced Encryption Standard) Dan Algoritma Kompresi RLE (Run Length Encoding) Untuk Pengamanan File Dokumen - Repository UPN Veteran Jakarta," *Upnvj.ac.id*, Jul. 2021, doi: http://repository.upnvj.ac.id/11126/1/ABSTRAK.pdf.

[11] I. K. Nurhareza and S. Siswanto, "Penerapan Algoritme Kriptografi AES 256 Untuk Mengamankan Dokumen Berbasis Web Pada Kelurahan Belendung," *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, vol. 1, no. 1, pp. 302–309, 2022.

[12] K. I. Santoso and W. Priyoatmoko, "Pengamanan Data Mysql Pada E-Commerce Dengan Algoritma AES 256," *SESINDO 2016*, vol. 2016.

[13] Khoiruddin and Ubaidi, "Analisa Traffic Jaringan Menggunakan Squid Proxy Server Untuk Peningkatan Performa Akses Internet Di Universitas Madura," in *Jurnal Insand Comtech, Vol. 6, No. 2,*, 2020.

[14] B. Komala, A. Kodar, "Model Reservasi Massage Berbasis Website Menggunakan Algoritma FIFO Dengan Metode Scrum", Universitas Mercu Buana, *repository*, 2018.

[15] U. Salamah and A. Purnomo, "Aplikasi Simpan Pinjam Koperasi Pada PT. Primantara Berbasis Mobile Menggunakan Algoritma FIFO," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 9, no. 1, pp. 51–58, Mar. 2020, doi: https://doi.org/10.32736/sisfokom.v9i1.711.