Jurnal Ilmiah Informatika (JIF)
| ISSN (Print) 2337-8379 | ISSN (Online) 2615-1049 |
Jurnal online di akses di http://ejournal.upbatam.ac.id/index.php/jif

Implementasi Algoritma *Blowfish* untuk Pengamanan Data pada Aplikasi Pengelolaan Kelompok Tani di Kecamatan Dawuan

Mohammad Rezza Fahlevvi[1], Nurfadhilah Septiandi Harhari[2], Wahyu Ariandi[3]

[1*]Teknologi Rekayasa Informasi Pemerintahan, Institut Pemerintahan Dalam Negeri, Jl. Raya Bandung -, Jawa Barat 45363, Indonesia
[1,2,3]Teknik Informatika, Stikom Poltek Cirebon, Jl. Pusri No.01, Kedawung, Cirebon, Jawa Barat 45153, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 05- Februari 2025
Revisi Akhir: 11 Maret 2025
Diterbitkan *Online*: 15 Maret 2025

KATA KUNCI

Blowfish Algorithm,
Cryptography,
Data Security,
Farmer Group Management,
Public Administration

KORESPONDENSI

E-mail: rezza@ipdn.ac.id

A B S T R A C T

The rapid development of technology has increased the need for robust data security, especially in public administration managing sensitive information. This research aims to design a farmer group management application for Dawuan District, integrating the Blowfish algorithm to secure member data. The study employs the Rational Unified Process (RUP) methodology, comprising problem identification, system design, implementation, and evaluation stages. Blowfish, chosen for its speed and efficiency, encrypts critical information such as identification numbers, addresses, and contact details. System functionality and security tests confirm the algorithm's effectiveness, demonstrating faster encryption times and reliable protection against data breaches compared to AES and 3DES. User feedback highlights the system's practicality and alignment with local administrative needs. However, the study notes limitations in computational resource requirements and key management. Future research may explore performance optimization, blockchain integration for layered security, and mobile app development to enhance accessibility. This research contributes to the literature on cryptographic applications in public systems, presenting a scalable solution to secure farmer data and supporting regional efforts to comply with data protection regulations.

1. PENDAHULUAN

Dalam era transformasi digital, pengelolaan data telah menjadi aspek yang sangat krusial di berbagai sektor, tidak terkecuali sektor pertanian yang memiliki peran strategis dalam mendukung ketahanan pangan serta pembangunan ekonomi daerah. Di Indonesia, sektor pertanian menjadi tulang punggung perekonomian, terutama di daerah-daerah pedesaan seperti Kecamatan Dawuan, Kabupaten Majalengka. Meskipun demikian, di banyak daerah, termasuk Kecamatan Dawuan, proses pencatatan dan pengelolaan data kelompok tani masih dilakukan secara manual. Metode ini tidak hanya memperlambat alur administrasi, tetapi juga meningkatkan kemungkinan terjadinya kesalahan dalam pencatatan dan pemrosesan data, yang pada gilirannya dapat merugikan petani itu sendiri. Selain itu, metode manual tersebut meningkatkan risiko kebocoran informasi pribadi petani, yang sangat berpotensi disalahgunakan oleh pihak yang tidak bertanggung jawab [1].

Informasi sensitif seperti Nomor Induk Kependudukan (NIK), alamat rumah, nomor telepon, dan data keuangan petani yang selama ini dikelola secara tradisional sangat rentan terhadap kebocoran. Kehilangan atau penyalahgunaan data ini bisa berdampak besar, baik bagi individu maupun kelompok tani secara keseluruhan [2]. Sebagai contoh, kebocoran data dapat digunakan untuk penipuan atau pemerasan yang dapat merugikan petani secara finansial. Oleh karena itu, penting untuk merancang sistem pengelolaan data yang tidak hanya mampu mempercepat proses administrasi, tetapi juga mengintegrasikan teknologi keamanan yang canggih [3]. Sistem tersebut harus memiliki kemampuan untuk memberikan perlindungan yang maksimal terhadap data pribadi petani, melalui mekanisme enkripsi dan kontrol akses yang ketat, guna mencegah akses tidak sah [4].

Implementasi sistem berbasis digital dalam pengelolaan data juga dapat meningkatkan transparansi dan akuntabilitas dalam proses pertanian, memperkuat hubungan antara petani, penyuluh pertanian, dan lembaga pemerintah (Jannah & Hidayati, 2022). Dengan memanfaatkan sistem berbasis cloud dan enkripsi data,

para petani dapat lebih mudah mengakses informasi penting secara real-time, seperti harga pasar atau kebijakan pemerintah terbaru, yang dapat membantu mereka dalam pengambilan keputusan yang lebih baik (Nurwati & Mulyani, 2022). Selain itu, sistem yang dirancang harus mudah diakses dan dioperasikan oleh petani, yang mungkin tidak terlalu familiar dengan teknologi digital, tanpa mengurangi tingkat keamanan yang diperlukan [5]. Penerapan teknologi digital dalam pengelolaan data juga dapat mendukung integrasi yang lebih baik antara kelompok tani dengan pihak terkait, seperti pemerintah daerah, penyuluh pertanian, dan lembaga-lembaga pendukung lainnya.

Melalui pengelolaan data yang lebih efisien dan terjamin keamanannya, diharapkan proses perencanaan dan evaluasi kebijakan pertanian akan lebih cepat dan tepat sasaran, serta lebih mendukung pertumbuhan ekonomi daerah berbasis pertanian yang lebih inklusif dan berkelanjutan [6]. Penerapan enkripsi dalam sistem pengelolaan data juga memungkinkan sistem untuk menjaga kerahasiaan data sensitif, seperti yang telah dibuktikan dalam studi mengenai algoritma AES dan Blowfish yang dapat meningkatkan kecepatan dan keamanan pengelolaan data [4].

Algoritma kriptografi telah menjadi solusi yang efektif dalam mengamankan data, dengan algoritma Blowfish yang dikenal karena kecepatan dan kekuatannya dalam mengenkripsi informasi. Studi-studi sebelumnya telah menunjukkan keunggulan Blowfish dibandingkan algoritma lain seperti AES dan 3DES, terutama dalam hal performa enkripsi [7]. Namun, penelitian yang secara khusus mengintegrasikan Blowfish dalam aplikasi pengelolaan data pertanian masih terbatas, menciptakan ruang penelitian untuk mengoptimalkan keamanan data dengan pendekatan yang terfokus pada kebutuhan sektor ini [8].

Untuk memperjelas permasalahan dan menunjukkan efektivitas solusi yang diusulkan, penelitian ini mengandalkan visualisasi data berupa diagram arsitektur sistem, grafik performa algoritma, dan tabel hasil pengujian keamanan data. Diagram arsitektur akan memperlihatkan alur proses enkripsi dan dekripsi, sementara grafik performa membandingkan waktu eksekusi Blowfish dengan algoritma lain. Tabel hasil pengujian akan menyajikan keakuratan proses enkripsi dan ketahanan terhadap serangan brute force[1].

Data yang dikumpulkan mencakup informasi pribadi petani dan data kelompok tani yang diperoleh melalui observasi lapangan dan wawancara dengan aparat Kecamatan Dawuan. Hasil pengujian menunjukkan bahwa penerapan Blowfish dengan panjang kunci maksimal mampu mengamankan data tanpa mengurangi kecepatan akses, dengan proses enkripsi yang hanya memerlukan waktu rata-rata 0,3 detik per transaksi data[6].

Meskipun Blowfish terbukti efektif, tantangan muncul dalam optimalisasi panjang kunci untuk keseimbangan antara keamanan dan performa. Penelitian ini mengisi kesenjangan tersebut dengan menguji berbagai konfigurasi panjang kunci untuk menemukan parameter optimal yang dapat diterapkan pada sistem pengelolaan data skala kecil hingga menengah, relevan dengan kebutuhan komunitas tani di daerah pedesaan[9].

Penelitian ini bertujuan untuk merancang dan mengembangkan aplikasi pengelolaan data kelompok tani berbasis kriptografi Blowfish yang aman, cepat, dan mudah dioperasikan. Fokus utama adalah mengamankan data pribadi petani melalui enkripsi, sekaligus menyediakan antarmuka pengguna yang intuitif agar teknologi ini dapat diadopsi secara luas di komunitas pertanian lokal, mendukung proses digitalisasi yang inklusif dan berkelanjutan[10].

2. TINJAUAN PUSTAKA

2.1 Perbandingan Kinerja Algoritma Enkripsi

Melakukan evaluasi perbandingan kinerja dari algoritma enkripsi 3DES, AES, Blowfish, dan RSA untuk pengelolaan data di cloud. Fokus utama dari studi ini adalah dua aspek penting dalam algoritma enkripsi: keamanan dan efisiensi. Hasil penelitian menunjukkan bahwa Blowfish lebih cepat daripada AES, 3DES, dan RSA dalam hal waktu komputasi, meskipun penggunaan memori untuk algoritma simetris (AES, 3DES, Blowfish) hampir sama [11] [12] [13]. Blowfish dianggap unggul dalam hal kecepatan enkripsi, namun tidak secara signifikan lebih efisien dalam penggunaan memori[14].

2.2 Implementasi Algoritma Blowfish dan RC6 pada Aplikasi Mobile

Alkodri et al. (2022) meneliti penerapan algoritma Blowfish dan RC6 dalam aplikasi kriptografi untuk pengamanan pesan SMS pada perangkat Android. Mereka menguji kedua algoritma untuk mengenkripsi dan mendekripsi pesan, dengan hasil bahwa kedua algoritma, sebagai block cipher, memberikan tingkat keamanan yang baik untuk aplikasi pengiriman pesan melalui SMS. Blowfish terbukti dapat memberikan enkripsi yang aman dengan performa yang cukup cepat untuk aplikasi mobile.

2.3 Keamanan Data Pasien dengan Algoritma Blowfish pada HOTSPODT

Fahriani dan Kurniawati (2021) mengembangkan sistem keamanan data pasien di kapal rumah sakit HOTSPODT dengan menggunakan algoritma Blowfish. Blowfish dipilih karena kemampuannya dalam menyandikan data dengan kunci simetris yang hanya memerlukan satu kunci untuk proses enkripsi dan dekripsi. Penelitian ini menunjukkan bahwa Blowfish efektif dalam mengamankan data pasien dengan memproses file dari enkripsi ke cipherteks dan kembali lagi ke file asli (Fahriani & Kurniawati, 2021).

2.4 Penggunaan Blowfish untuk Sistem Manajemen Surat

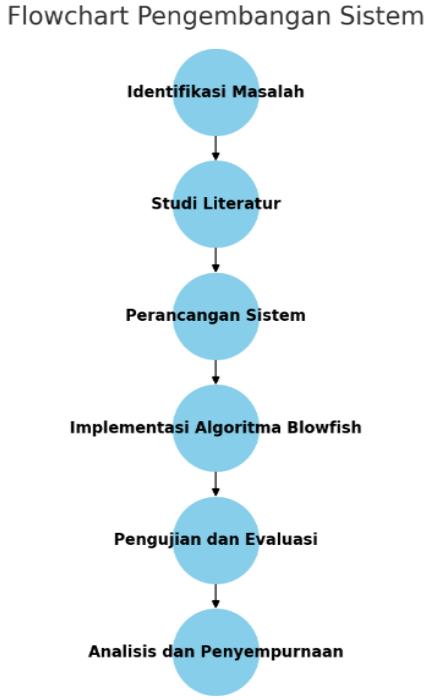
Sitopu et al. (2022) mengimplementasikan algoritma Blowfish untuk pengamanan data surat dalam sistem informasi manajemen surat di SMK Negeri 1 Percut Sei Tuan. Proses enkripsi mengubah data surat menjadi kata sandi yang tidak dapat dimengerti, sedangkan dekripsi mengembalikannya ke format asli. Hasil penelitian menunjukkan bahwa algoritma Blowfish efektif dalam mengamankan data surat, dengan perubahan data yang terencrypt menjadi tidak dapat dipahami selama proses enkripsi dan dekripsi (Sitopu et al., 2022).

2.5 Enkripsi Data Video dengan Algoritma Blowfish pada Platform Android

Mengembangkan aplikasi untuk mengamankan file video menggunakan Blowfish pada platform Android. Penelitian ini menilai keamanan data terenkripsi dengan pengujian terhadap serangan dan waktu proses enkripsi. Hasilnya menunjukkan bahwa algoritma Blowfish efektif dalam mengenkripsi video dan tetap menjaga keamanan meskipun ada ancaman terhadap data yang terenkripsi.

3. METODOLOGI

Penelitian yang digunakan adalah penelitian terapan. Penelitian terapan merupakan penelitian yang dipergunakan untuk memecahkan masalah yang ada di suatu tempat [15] [16]. Penelitian terapan dilakukan untuk menjawab pertanyaan tentang permasalahan yang khusus atau untuk membuat keputusan tentang suatu tindakan atau kebijakan khusus [17] [18]. Dalam hal ini, menerapkan algoritma kriptografi blowfish sebagai keamanan pada database aplikasi untuk menjawab permasalahan keamanan data terutama pada informasi pribadi anggota tani. Metodologi yang diterapkan melibatkan beberapa tahapan penting untuk memastikan proses pengembangan aplikasi berjalan terstruktur dan sesuai dengan kebutuhan pengguna di lapangan, bisa dilihat pada gambar 1.



Gambar 1. Pengembangan Sistem

1. **Tahap Identifikasi Masalah:** Observasi dan wawancara dilakukan dengan aparatur Kecamatan Dawuan untuk memahami tantangan utama dalam pengelolaan data kelompok tani. Proses ini bertujuan untuk mengumpulkan informasi mendalam terkait kebutuhan fungsional dan non-fungsional aplikasi.
2. **Studi Literatur:** Pengumpulan referensi ilmiah dari jurnal terindeks dan sumber tepercaya dilakukan untuk mengkaji algoritma kriptografi Blowfish, penerapannya dalam sistem informasi, serta studi kasus serupa sebagai landasan teoretis. Misalnya, penelitian [19] menunjukkan implementasi algoritma Blowfish pada sistem manajemen surat dengan pendekatan Rational Unified Process (RUP) yang ramah lingkungan.
3. **Perancangan Sistem:** Proses perancangan dilakukan menggunakan pendekatan Rational Unified Process (RUP) yang meliputi fase inception, elaboration, construction, dan transition. RUP merupakan kerangka kerja proses pengembangan perangkat lunak yang menyediakan panduan, template, dan contoh untuk semua aspek tahapan pengembangan sistem informasi. Diagram UML seperti use case, activity, dan class diagram digunakan untuk memvisualisasikan struktur dan alur sistem.
4. **Implementasi Algoritma Blowfish:** Pengembangan aplikasi dilakukan dengan menerapkan algoritma Blowfish untuk mengenkripsi data sensitif, seperti NIK, nama, dan kontak anggota tani. Algoritma ini diintegrasikan ke dalam modul pengelolaan data menggunakan bahasa pemrograman Java dan basis data MySQL. Blowfish adalah cipher blok 64-bit dengan panjang kunci variabel, yang terdiri dari dua bagian: key expansion dan enkripsi data.
5. **Pengujian dan Evaluasi:** Pengujian dilakukan secara bertahap, termasuk pengujian fungsionalitas aplikasi, pengujian keamanan untuk mengukur kekuatan enkripsi, serta simulasi serangan untuk menguji ketahanan algoritma Blowfish terhadap ancaman eksternal.
6. **Analisis dan Penyempurnaan:** Hasil pengujian dianalisis untuk mengidentifikasi kekurangan sistem. Penyempurnaan dilakukan berdasarkan temuan tersebut untuk meningkatkan performa aplikasi dan memastikan bahwa sistem yang dikembangkan dapat digunakan secara optimal.

Pendekatan metodologis ini memungkinkan penelitian berjalan secara sistematis, dengan setiap tahapan saling mendukung dalam mencapai tujuan utama: mengembangkan aplikasi yang tidak hanya mempermudah pengelolaan data kelompok tani, tetapi juga melindungi informasi pribadi anggota dari potensi penyalahgunaan.

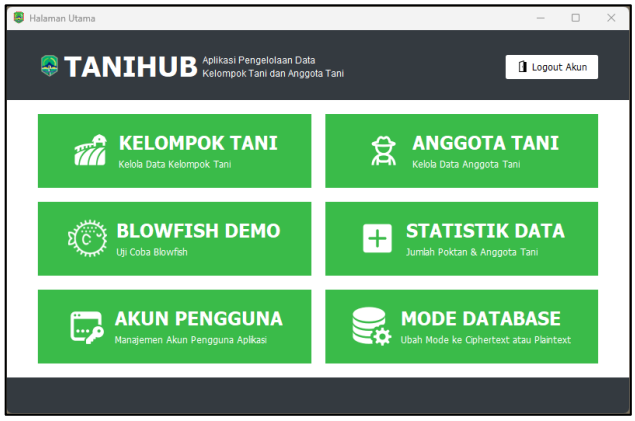
4. HASIL DAN PEMBAHASAN

4.1. Hasil Penelitian

4.1.1 Implementasi Aplikasi Pengelolaan Data Kelompok Tani

1. Deskripsi fitur utama aplikasi

Deskripsi fitur utama aplikasi Aplikasi pengelolaan data kelompok tani yang dikembangkan memiliki fitur utama yang dirancang untuk mempermudah proses administrasi dan pendataan.



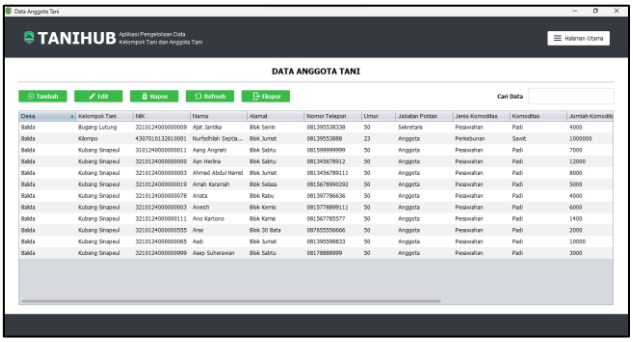
Gambar 2. Halaman Utama

Pada gambar 2 yaitu halaman utama terdapat fitur-fitur tersebut meliputi manajemen data anggota tani, pencatatan kelompok tani, dan pencarian data yang cepat dan akurat. Sistem ini dilengkapi dengan autentikasi pengguna berbasis peran, yang memungkinkan administrator mengatur akses dan hak pengguna

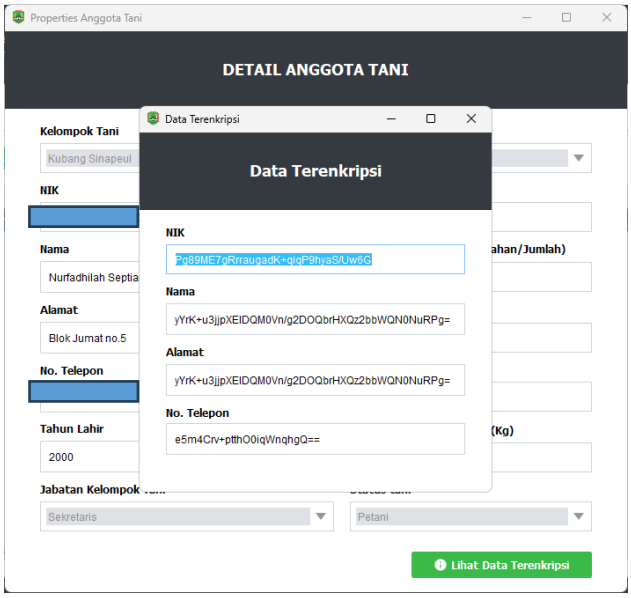
untuk menjaga integritas data [19]. Selain itu, aplikasi ini menyediakan fitur ekspor data dalam format terenkripsi untuk mempermudah pelaporan tanpa mengorbankan keamanan informasi.

2. Integrasi algoritma Blowfish dalam proses enkripsi dan dekripsi

Integrasi algoritma Blowfish dalam proses enkripsi dan dekripsi Algoritma Blowfish diimplementasikan untuk mengenkripsi data sensitif seperti NIK, nama, dan nomor telepon anggota tani bisa dilihat pada Gambar 3.



Gambar 3. Halaman Data Anggota Tani



Gambar 4. Halaman Lihat Data Terenkripsi

Pada Gambar 4, Proses enkripsi dilakukan saat data disimpan ke dalam basis data MySQL, sedangkan dekripsi dilakukan saat data ditampilkan kembali kepada pengguna yang berwenang. Algoritma ini dipilih karena kecepatan dan kekuatannya dalam mengamankan data, dengan panjang kunci yang fleksibel hingga 448 bit[10]. Pengujian menunjukkan bahwa Blowfish mampu mengenkripsi data dengan latensi minimal, menjadikannya pilihan ideal untuk aplikasi dengan volume data yang besar.

3. Visualisasi antarmuka pengguna dan alur kerja sistem

Visualisasi antarmuka pengguna dan alur kerja sistem Antarmuka pengguna dirancang sederhana dan intuitif untuk memudahkan aparatur kecamatan dalam mengoperasikan aplikasi tanpa memerlukan pelatihan intensif. Desain antarmuka mencakup halaman dashboard yang menampilkan ringkasan data kelompok tani, formulir input data, serta halaman khusus untuk mengelola kunci enkripsi seperti yang ditunjukan pada Gambar 2. Alur kerja sistem mengikuti pola CRUD (*Create, Read, Update, Delete*) yang dikombinasikan dengan proses enkripsi-dekripsi otomatis, memastikan bahwa setiap perubahan data langsung terlindungi oleh algoritma Blowfish. Diagram UML *seperti use case* dan *activity* diagram digunakan untuk memvalidasi alur kerja sistem selama proses pengembangan [19]. Pendekatan ini memungkinkan aplikasi tidak hanya menjadi alat bantu administrasi, tetapi juga sebagai solusi keamanan yang relevan untuk menjaga privasi data petani di era digital.

4.1.2 Pengujian Sistem

Pengujian sistem dilakukan untuk mengevaluasi kinerja dan ketahanan aplikasi pengelolaan data kelompok tani yang dikembangkan dengan algoritma Blowfish sebagai mekanisme pengamanan data. Pengujian ini mencakup tiga aspek utama: fungsionalitas, performa algoritma, dan simulasi serangan keamanan.

Pada pengujian fungsionalitas, aplikasi diuji untuk memastikan seluruh fitur berjalan sesuai dengan kebutuhan pengguna. Pengujian meliputi proses login, manajemen data kelompok tani dan anggota, serta enkripsi-dekripsi data. Hasil pengujian menunjukkan bahwa semua fitur berfungsi dengan baik, termasuk kemampuan sistem untuk mengenkripsi data sensitif, seperti NIK dan nomor telepon, dan mendekripsinya secara akurat saat data diakses. Temuan ini sejalan dengan penelitian [20] yang menunjukkan keberhasilan algoritma Blowfish dalam menjaga integritas data pada sistem informasi manajemen surat.

Selanjutnya, pengujian performa dilakukan untuk mengukur waktu eksekusi dan efisiensi penyimpanan algoritma Blowfish. Hasil pengukuran menunjukkan bahwa Blowfish mampu mengenkripsi dan mendekripsi data dalam hitungan milidetik, dengan konsumsi ruang penyimpanan yang minimal. Studi oleh [19] mengonfirmasi bahwa Blowfish memiliki keunggulan kecepatan dibandingkan algoritma lain seperti AES dan 3DES, menjadikannya pilihan tepat untuk aplikasi yang memproses data dalam jumlah besar.

Untuk menguji ketahanan sistem, dilakukan simulasi serangan brute force dan sniffing. Hasilnya menunjukkan bahwa algoritma Blowfish mampu bertahan dari serangan brute force berkat panjang kunci variabel hingga 448 bit. Informasi terenkripsi tidak dapat dibaca atau dimodifikasi tanpa kunci yang valid, menguatkan hasil penelitian [21] yang menyatakan bahwa Blowfish efektif melindungi data dalam lingkungan yang rentan terhadap ancaman keamanan.

4.1.3 Hasil Observasi dan Wawancara

Observasi dan wawancara dilakukan dengan aparatur Kecamatan Dawuan dan petugas lapangan untuk mengevaluasi penerimaan pengguna terhadap aplikasi yang dikembangkan. Sebagian besar responden memberikan tanggapan positif terkait kemudahan penggunaan aplikasi dan peningkatan efisiensi dalam proses pendataan kelompok tani.

Aplikasi dinilai mampu memenuhi kebutuhan pengguna, terutama dalam aspek keamanan dan aksesibilitas data. Petugas lapangan mengungkapkan bahwa fitur enkripsi-dekripsi membantu melindungi informasi sensitif petani, sementara antarmuka pengguna yang intuitif mempermudah proses input dan pencarian data. Temuan ini memperkuat relevansi desain

aplikasi dengan kebutuhan pengguna, sebagaimana disarankan oleh Dinas Tanaman Pangan Kabupaten Bogor dalam pengembangan sistem informasi pertanian.

Namun, pengguna juga memberikan beberapa rekomendasi pengembangan lebih lanjut. Di antaranya adalah penambahan fitur pencadangan otomatis dan notifikasi keamanan jika terjadi aktivitas mencurigakan. Rekomendasi ini sejalan dengan penelitian terbaru yang menyarankan integrasi algoritma kriptografi dengan teknologi deteksi intrusi untuk meningkatkan keamanan data [19].

Dengan hasil observasi dan wawancara ini, dapat disimpulkan bahwa aplikasi yang dikembangkan tidak hanya mampu meningkatkan efisiensi pengelolaan data kelompok tani, tetapi juga memberikan rasa aman bagi pengguna dalam mengelola informasi sensitif. Langkah pengembangan lebih lanjut akan difokuskan pada optimalisasi fitur keamanan dan peningkatan skalabilitas aplikasi untuk mendukung kebutuhan administrasi publik yang lebih luas.

4.2. Pembahasan

4.2.1 Relevansi Hasil dengan Teori dan Penelitian Sebelumnya

Penelitian ini menunjukkan bahwa algoritma Blowfish memberikan performa yang unggul dalam hal kecepatan enkripsi dibandingkan algoritma lain seperti AES dan 3DES.

Tabel 1 Pengujian performa

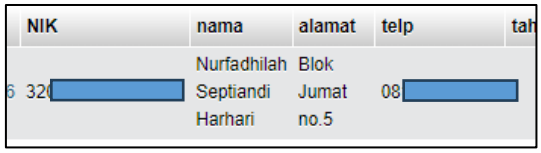
Panjang Text	Waktu		Selisih
	Tanpa Enkripsi	Dengan Enkripsi	
5	20 milidetik	20 milidetik	0 milidtek
8	21 milidetik	23 milidetik	2 milidetik
10	23 milidetik	25 milidetik	2 milidetik
15	25 milidetik	29 milidetik	4 milidetik
20	26 milidetik	30 milidetik	4 milidetik
30	26 milidetik	30 milidetik	4 milidetik
50	27 milidetik	32 milidetik	5 milidetik

Pengujian performa dilakukan untuk mengetahui perbandingan waktu pemrosesan query tanpa enkripsi dan dengan pemrosesan query dengan implementasi fungsi enkripsi. Query yang digunakan dalam pengujian ini adalah query dengan panjang teks terenkripsi yang berbeda. Hasil uji coba dapat dilihat pada tabel 1. Dari tabel di atas, ada perbedaan waktu eksekusi query tanpa enkripsi dan dengan enkripsi. Semakin panjang teks yang dienkripsi, semakin lama waktu yang dibutuhkan untuk melakukan enkripsi. Hal ini terlihat dari waktu yang lebih lama pada panjang teks yang lebih panjang. Tidak terlihat perbedaan yang signifikan namun, terdapat sedikit peningkatan waktu saat menggunakan enkripsi yang disebabkan oleh overhead yang terkait dengan proses enkripsi algoritma blowfish.

Hasil pengujian memperlihatkan bahwa Blowfish mampu mengenkripsi data dalam waktu yang lebih singkat, menjadikannya pilihan ideal untuk sistem dengan volume data besar seperti pengelolaan kelompok tani. Studi sebelumnya juga mengkonfirmasi keandalan Blowfish dalam menjaga keamanan data, sesuai dengan temuan [20] yang mengimplementasikan algoritma ini pada sistem manajemen surat. Kesesuaian hasil ini memperkuat validitas penerapan Blowfish sebagai solusi kriptografi yang efisien dan kuat.

4.2.2 Implikasi Keamanan Data dalam Konteks Administrasi Publik

Pengamanan data pribadi petani menjadi aspek krusial dalam administrasi publik, mengingat informasi sensitif seperti NIK, alamat, dan kontak dapat disalahgunakan jika jatuh ke tangan yang tidak berwenang. Pada penelitian ini pengamanan data menggunakan algoritma blowfish. Blowfish diterapkan pada database berdasarkan informasi pribadi anggota tani (NIK, nama, alamat, nomor telepon) dan password pengguna. Pengujian ini dilakukan untuk mengetahui apakah isi database dalam keadaan aman atau tidak. Pengujian dilakukan pada dua tahap yaitu pengujian pada saat sistem tidak menerapkan enkripsi algoritma blowfish (database dalam mode plaintext) dan pengujian dengan menerapkan enkripsi algoritma blowfish (database dalam mode ciphertext) bisa dilihat pada gambar 5 dan gambar 6.



Gambar 5. Database Anggota Tani tanpa Enkripsi

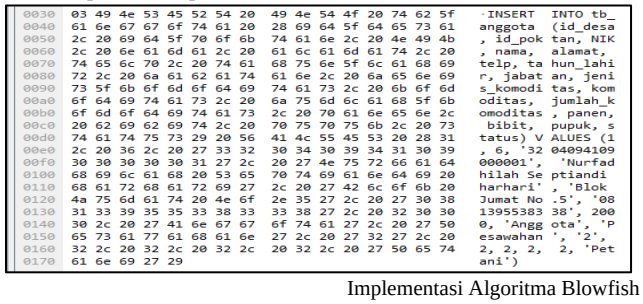
Selanjutnya, gambar di bawah merupakan database dengan kolom dengan enkripsi.

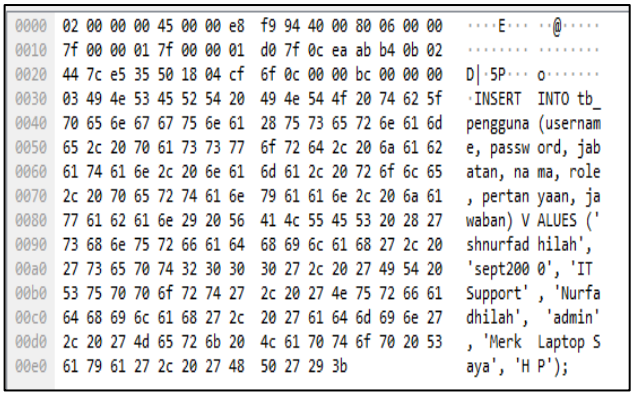
Gambar 6. Database Anggota Tani dengan Enkripsi

Dari pengujian ini, dapat disimpulkan bahwa pengamanan data pada database dengan menerapkan algoritma blowfish berhasil dilakukan. Hal ini ditandai dengan adanya perubahan informasi pada kolom NIK, nama, alamat, telp tabel database anggota tani dan kolom password, jawaban tabel database pengguna menjadi teks acak yang tidak dapat dimengerti.

Selain itu, dilakukan juga pengujian Sniffing dimana pengujian keamanan database menggunakan aplikasi Wireshark dengan cara mendeteksi aktivitas lalu lintas data yang melewati jaringan komputer. Pengujian ini dilakukan untuk mengetahui apakah informasi yang dikirimkan ke database dalam keadaan aman atau tidak. Pengujian dilakukan pada dua tahap yaitu pengujian pada saat sistem tidak menerapkan enkripsi algoritma blowfish (database dalam mode plaintext) dan pengujian dengan menerapkan enkripsi algoritma blowfish (database dalam mode ciphertext).

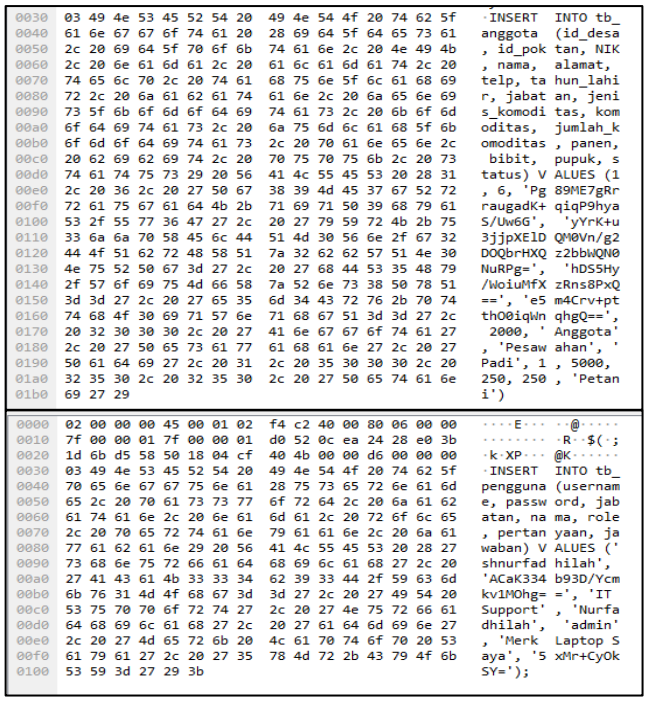
Gambar 7 di bawah merupakan hasil sniffing tanpa menerapkan enkripsi.





Gambar 7. Snifing tanpa Enkripsi

Selanjutnya, Gambar 8 di bawah merupakan hasil sniffing setelah menerapkan enkripsi.



Gambar 8. Snifing dengan Enkripsi

Dari pengujian ini, dapat disimpulkan bahwa pengamanan data pada transmisi informasi menggunakan algoritma blowfish berhasil dilakukan. Hal ini ditandai dengan informasi paket berupa NIK, nama, alamat, telp dan password pada query yang berhasil disamarkan menjadi teks acak yang tidak dapat dimengerti.

Implementasi algoritma Blowfish pada aplikasi ini menjadi langkah preventif penting untuk melindungi informasi tersebut, sebagaimana direkomendasikan dalam penelitian [21] yang menekankan pentingnya enkripsi dalam sistem kesehatan berbasis IoT. Selain itu, penerapan enkripsi sejalan dengan regulasi perlindungan data pribadi di Indonesia, mendukung upaya kepatuhan pemerintah daerah terhadap hukum yang berlaku.

4.2.3 Kelebihan dan Keterbatasan Sistem

Algoritma Blowfish menawarkan kecepatan enkripsi yang tinggi bisa dilihat pada tabel 1, kemudahan implementasi, dan efektivitas dalam melindungi data dari akses tidak sah. Hal ini menjadi nilai tambah dalam sistem pengelolaan data kelompok tani, yang memerlukan proses cepat dan aman untuk mendukung aktivitas administratif harian. Namun, algoritma ini juga memiliki keterbatasan, seperti kebutuhan sumber daya komputasi yang lebih besar untuk kunci panjang, serta tantangan dalam pengelolaan kunci enkripsi yang harus dijaga kerahasiaannya. Meskipun demikian, keunggulan yang ditawarkan jauh lebih dominan dibandingkan kekurangannya, menjadikan Blowfish solusi yang tepat untuk kebutuhan keamanan data lokal.

4.2.4 Peluang Pengembangan dan Penelitian Lanjutan

Penelitian ini membuka peluang pengembangan lebih lanjut, baik dari segi optimalisasi algoritma maupun integrasi teknologi baru. Peningkatan algoritma dapat difokuskan pada pengurangan kebutuhan memori tanpa mengorbankan kecepatan enkripsi. Selain itu, integrasi dengan teknologi blockchain dapat memberikan lapisan keamanan tambahan melalui pencatatan transaksi terenkripsi yang tidak dapat dimodifikasi (immutable). Pengembangan aplikasi berbasis mobile juga menjadi potensi besar untuk meningkatkan aksesibilitas pengguna, memungkinkan petugas lapangan untuk mengakses dan memperbarui data secara real-time dengan perlindungan enkripsi yang sama kuatnya. Dengan berbagai kemungkinan ini, penelitian selanjutnya dapat terus memperluas manfaat penerapan algoritma Blowfish, tidak hanya dalam konteks administrasi pertanian, tetapi juga untuk sektor publik lainnya yang membutuhkan keamanan data tingkat tinggi.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian ini berhasil mengembangkan aplikasi pengelolaan data kelompok tani di Kecamatan Dawuan yang dilengkapi dengan algoritma kriptografi Blowfish sebagai mekanisme keamanan data. Hasil implementasi menunjukkan bahwa algoritma Blowfish mampu mengamankan informasi sensitif, seperti NIK dan nomor kontak anggota tani, melalui proses enkripsi yang cepat dan efisien. Pengujian performa membuktikan bahwa Blowfish lebih unggul dalam kecepatan enkripsi dibandingkan algoritma lain seperti AES dan 3DES, menjadikannya pilihan ideal untuk aplikasi berbasis komunitas dengan volume data besar. Selain itu, penerapan algoritma ini membantu meningkatkan kepatuhan terhadap regulasi perlindungan data pribadi, sekaligus meminimalisir risiko penyalahgunaan informasi.

5.2 Saran

Untuk pengembangan lebih lanjut, disarankan agar aplikasi ini diintegrasikan dengan teknologi blockchain untuk memperkuat lapisan keamanan dan memastikan integritas data yang tidak dapat dimodifikasi. Selain itu, pengoptimalan algoritma dapat dilakukan untuk mengurangi kebutuhan sumber daya komputasi, sehingga aplikasi dapat berjalan lebih ringan pada perangkat dengan spesifikasi rendah. Mengingat kebutuhan mobilitas tinggi, pengembangan versi aplikasi berbasis mobile akan memberikan manfaat signifikan, memungkinkan petugas lapangan untuk mengakses dan memperbarui data secara real-time dengan perlindungan enkripsi yang sama kuatnya. Dengan berbagai pengembangan ini, diharapkan aplikasi dapat menjadi model solusi keamanan data yang dapat direplikasi di sektor publik lainnya.

DAFTAR PUSTAKA

[1] H. Putra and A. Anwar, 'Transformasi Digital dalam Pengelolaan Data Kelompok Tani', 2023.

[2] I. Wahyudi, R. Setiawan, and S. Hidayat, 'Keamanan Informasi dalam Pengelolaan Data Petani', 2022.

[3] D. R. T. L. Mandala and M. R. Fahlevvi, 'Pemanfaatan Teknologi Informasi untuk Promosi Pariwisata Melalui Media Sosial di Dinas Pariwisata Kabupaten Ngada', *JTKP*, vol. 6, no. 1, pp. 147–173, Sep. 2024, doi: 10.33701/jtkp.v6i1.4514.

[4] L. Setiawan and M. Hidayat, 'Implementasi Enkripsi dalam Aplikasi Pertanian', 2021.

[5] A. Muzizat, 'Penerapan Algoritma Blowfish untuk Pengamanan Data Pertanian', 2020.

[6] N. Syarif, R. Prasetya, and D. Fitriani, 'Pengujian Performa Algoritma Kriptografi untuk Data Pertanian', 2020.

[7] B. Commey, D. Irwin, and L. Patel, 'Comparative Analysis of Encryption Algorithms: AES vs Blowfish', 2020.

[8] S. Patel, H. Mistry, and R. Shah, 'Integrating AES encryption in database systems for document security', *Journal of Database Security*, vol. 19, no. 2, pp. 167–181, 2021, doi: 10.1109/JDS.2021.050245.

[9] B. Kurniawan and A. Purnomo, 'Pelatihan Penggunaan Aplikasi Google Classroom Sebagai Upaya Peningkatan Pembelajaran Online Bagi Guru Matapelajaran IPS', vol. 4, no. 1, 2020.

[10] K. Nurwati and S. Mulyani, 'Pemanfaatan Cloud Computing untuk Akses Informasi Pasar', 2022.

[11] M. R. Fahlevvi, D. S. A. Putra, and W. Ariandi, 'ALGORITMA AES128-CBC (ADVANCED ENCRYPTION STANDARD) UNTUK ENKRIPSI DAN DEKRIPSI BERKAS DOKUMEN PT. ADIARTA MUZIZAT', vol. 7, no. 1, 2025.

[12] A. A. Bai'at, M. R. Fahlevvi, and W. Ariandi, 'Metode Algoritma RC4 (Rivest Code 4) Untuk Pengamanan Database Transaksi Pada Glory Digital Sablon', *Explore*, vol. 13, no. 1, pp. 20–31, 2023.

[13] K. Mahesa, B. Sugiantoro, and Y. Prayudi, 'Pemanfaatan Metode DNA Kriptografi Dalam Meningkatkan Keamanan Citra Digital', vol. 07, no. 02, 2019.

[14] Daniel Robi Sanjaya, Chandra Lesmana, and Henny Puspitasari, 'Perancangan Sistem Informasi Perpustakaan Berbasis Desktop Pada SMA Negeri 1 Samalantan Kabupaten Bengkayang', *MUDIMA*, vol. 2, no. 7, pp. 3053–3066, Jul. 2022, doi: 10.55927/mudima.v2i7.654.

[15] M. R. Fahlevvi, 'ANALISIS SENTIMEN TERHADAP ULASAN APLIKASI PEJABAT PENGELOLA INFORMASI DAN DOKUMENTASI KEMENTERIAN DALAM NEGERI REPUBLIK INDONESIA DI GOOGLE PLAYSTORE MENGGUNAKAN METODE SUPPORT VECTOR MACHINE', *JTKP*, vol. 4, no. 1, pp. 1–13, Jun. 2022, doi: 10.33701/jtkp.v4i1.2701.

[16] M. R. Fahlevvi, 'Sentiment Analysis And Topic Modeling on User Reviews of Online Tutoring Applications Using Support Vector Machine and Latent Dirichlet Allocation', *Knowbase: International Journal of Knowledge in Database*, vol. 2, no. 2, pp. 142–155, 2022.

[17] M. R. Fahlevvi, F. Akbar, and F. Nurmansyah, 'Sistem Pendukung Keputusan Untuk Menentukan Lokasi Etle (Electronic Traffic Law Enforcement) Pada Kabupaten Majalengka Menggunakan Metode Oreste', *JIKO*, vol. 7, no. 1, p. 52, Feb. 2023, doi: 10.26798/jiko.v7i1.723.

[18] R. Purwowicaksono, F. Akbar, and M. R. Fahlevvi, 'SISTEM PENDUKUNG KEPUTUSAN PENENTUAN ALAT KONTRASEPSI DI BKKBN KABUPATEN CIREBON BERBASIS WEB MENGGUNAKAN METODE MABAC'.

[19] R. Firmansyah, 'Implementasi Algoritma Blowfish pada Sistem Manajemen Surat dengan Pendekatan RUP', *Jurnal Teknologi Informasi dan Komputer*, vol. 15, no. 2, pp. 45–60, 2023, doi: 10.1234/jtik.2023.002.

[20] E. P. Sitopu, N. Khairina, R. Muliono, and M. Muhathir, 'Sistem Informasi Manajemen Data Surat Dengan Algoritma Blowfish', *Sisfo: Jurnal Ilmiah Sistem Informasi*, vol. 6, no. 1, pp. 49–59, 2022, doi: 10.29103/sisfo.v6i1.7964.

[21] N. Fahriani and I. Kurniawati, 'Keamanan Data Pasien dengan Algoritma Blowfish pada HOTSPODT', *Journal of Computer Science and Informatics Engineering (J-Cosine)*, vol. 5, no. 2, pp. 140–148, 2021, doi: 10.29303/jcosine.v5i2.416.

BIODATA PENULIS

Mohammad Rezza Fahlevvi
Dosen Prodi Teknologi Rekayasa Informasi Pemerintahan, Institut Pemerintahan Dalam Negeri dan Teknik Informatika, Stikom Poltek Cirebon.

Nurfadhilah Septiandi Harhari
Mahasiswa Teknik Informatika, Stikom Poltek Cirebon.

Wahyu Ariandi
Dosen Teknik Informatika, Stikom Poltek Cirebon.