Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13805
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Terbit: 29 Juni 2024

Penerapan Algoritma Rivest Shamir Aldeman (RSA) untuk Pengamanan Data Gambar Nasabah BMT Al-Hikmah Permata

[1]Muhammad Rizal Syifauddin, [2]R. Hadapiningradja Kusumodestoni, [3]Sarwido

[1.] Program Studi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Nahdlotul Ulama, Jepara, Indonesia

Muhammadrizalsyifauddin446@gmail.com[1], kusumodestoni@gmail.com[2] sarwido.unisnu@gmail.com[3]

Abstrak

Keamanan data nasabah merupakan aspek krusial dalam industri keuangan, termasuk di lembaga keuangan mikro seperti Baitul Maal wat Tamwil (BMT). Penelitian ini bertujuan untuk mengimplementasikan algoritma Rivest Shamir Adleman (RSA) guna mengamankan data gambar nasabah pada aplikasi mobile BMT Al-Hikmah Permata. Metode yang digunakan adalah pengembangan aplikasi berbasis Android dengan mengintegrasikan algoritma RSA untuk enkripsi dan dekripsi data gambar. Proses enkripsi dilakukan saat gambar diunggah ke server, sementara dekripsi dilakukan saat data diakses oleh pengguna yang berwenang. Hasil penelitian menunjukkan bahwa penerapan algoritma RSA berhasil meningkatkan keamanan data gambar nasabah dengan tingkat keberhasilan enkripsi dan dekripsi mencapai 100%. Waktu proses enkripsi rata-rata adalah 2,5 detik untuk gambar berukuran 1 MB, sedangkan waktu dekripsi rata-rata adalah 1,8 detik. Implementasi ini terbukti efektif dalam melindungi privasi nasabah tanpa mengorbankan kinerja aplikasi secara signifikan. Penelitian ini berkontribusi pada peningkatan keamanan data di sektor keuangan mikro dan dapat menjadi acuan bagi pengembangan sistem keamanan serupa di institusi keuangan lainnya.

Kata Kunci: Algoritma RSA, Keamanan Data, Aplikasi Mobile, Enkripsi Gambar, Kriptografi

Abstract

Customer data security is a crucial aspect in the financial industry, including in microfinance institutions such as Baitul Maal wat Tamwil (BMT). This research aims to implement the Rivest Shamir Adleman (RSA) algorithm to secure customer image data in the BMT Al-Hikmah Permata mobile application. The method used is the development of an Android-based application integrating the RSA algorithm for image data encryption and decryption. The encryption process is performed when images are uploaded to the server, while decryption occurs when data is accessed by authorized users. The results show that the implementation of the RSA algorithm successfully enhanced the security of customer image data with a 100% success rate for encryption and decryption. The average encryption process time is 2.5 seconds for a 1 MB image, while the average decryption time is 1.8 seconds. This implementation proves effective in protecting customer privacy without significantly sacrificing application performance. This research contributes to improving data security in the microfinance sector and can serve as a reference for developing similar security systems in other financial institutions.

Keywords*: RSA Algorithm, Data Security, Mobile Application, Image Encryption, Microfinance, Cryptography*

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13805
e-ISSN : 2797-3298
p-ISSN : 2089-9424

PENDAHULUAN

Di era digital yang semakin maju, keamanan data menjadi isu yang sangat krusial, terutama bagi lembaga keuangan yang mengelola informasi sensitif nasabah. Baitul Maal wat Tamwil (BMT), sebagai lembaga keuangan mikro syariah, tidak terkecuali dari tantangan ini. BMT Al-Hikmah Permata, sebagai salah satu BMT yang berkembang, menghadapi kebutuhan mendesak untuk mengamankan data nasabahnya, khususnya data dalam bentuk gambar yang seringkali mengandung informasi penting seperti tanda tangan, foto identitas, atau dokumen pendukung lainnya.

Di era revolusi industri 4.0, digitalisasi telah merambah berbagai sektor, termasuk industri keuangan mikro. Baitul Maal wat Tamwil (BMT), sebagai lembaga keuangan mikro syariah, menghadapi tantangan untuk mengadopsi teknologi guna meningkatkan efisiensi operasional dan kualitas layanan. Sebagaimana dikemukakan oleh Eko Sudarmanto. (2024), transformasi digital dalam lembaga keuangan mikro syariah tidak hanya menjadi pilihan, tetapi kebutuhan untuk bertahan dan berkembang di era persaingan global.(Sudarmanto et al., 2024) BMT Al-Hikmah Permata, sebagai salah satu lembaga keuangan mikro progresif, telah mengambil inisiatif dengan ingin mengembangkan aplikasi mobile untuk melayani nasabahnya.

Dalam operasional BMT Al-Hikmah Permata, penggunaan data gambar nasabah menjadi komponen integral dalam proses verifikasi identitas, pencatatan transaksi, dan dokumentasi perjanjian. Data ini mencakup foto KTP, foto diri nasabah,hingga gambar rumah nasabah, dll. Meskipun penggunaan data gambar meningkatkan efisiensi, hal ini juga menimbulkan kerentanan terhadap keamanan data pribadi nasabah. Menurut penelitian yang dilakukan oleh Nabila Azura Qothrunnada (2023), peningkatan penggunaan data digital dalam lembaga keuangan mikro berbanding lurus dengan peningkatan risiko keamanan data, terutama terkait data sensitif nasabah. Hal ini diperkuat oleh laporan dari Badan Siber dan Sandi Negara (BSSN) yang mencatat lebih dari 1,4 miliar serangan siber di Indonesia sepanjang tahun 2023, menunjukkan urgensi implementasi sistem keamanan yang kuat.(Qothrunnada, 2023)

Riset yang dilakukan oleh Ika Riswanti Putranti et al. (2020) mengungkapkan bahwa 60% lembaga keuangan mikro di Indonesia belum memiliki sistem keamanan data yang memadai, menempatkan mereka pada risiko tinggi terhadap serangan siber. Situasi ini menegaskan pentingnya BMT Al-Hikmah Permata untuk mengambil langkah proaktif dalam mengamankan data nasabahnya. Ketiadaan sistem keamanan yang memadai dalam pengelolaan data gambar nasabah dapat menimbulkan berbagai risiko serius, termasuk pencurian identitas, pelanggaran privasi, sanksi hukum, kerugian finansial, dan dampak negatif terhadap reputasi lembaga.(Putranti & Amaliyah, 2020)

Cici Winarti (2023) menyatakan bahwa pencurian identitas melalui eksploitasi data gambar yang tidak terenkripsi telah meningkat 30% dalam dua tahun terakhir, dengan dampak finansial rata-rata mencapai Rp50 juta per korban.(Pandemi, 2023) Sementara itu, Elya Rosa Maharani Sembiring et al. (2024) melaporkan bahwa kebocoran data pribadi nasabah dapat mengakibatkan hilangnya kepercayaan hingga 78% nasabah terhadap lembaga keuangan.(Bsi & Kisaran, 2024) Achmadudin Rajab (2023) memperingatkan bahwa kegagalan dalam melindungi data nasabah dapat mengakibatkan sanksi hingga Rp70 miliar berdasarkan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.(Perundang-undangan et al., 2023)

Menghadapi tantangan keamanan data yang semakin kompleks, implementasi algoritma kriptografi yang kuat menjadi solusi yang tidak dapat ditawar. Dalam konteks ini, algoritma Rivest Shamir Adleman (RSA) dipilih sebagai solusi untuk mengamankan data gambar nasabah BMT Al-Hikmah Permata. Pemilihan algoritma RSA didasarkan pada beberapa pertimbangan yang didukung oleh penelitian terkini, termasuk keamanan yang terbukti, fleksibilitas, skalabilitas, dan kompatibilitas dengan berbagai platform.

Yohanes et al. (2023) menegaskan bahwa RSA tetap menjadi salah satu algoritma kriptografi paling aman, dengan belum adanya laporan peretasan berhasil pada implementasi yang tepat hingga tahun 2023.(Chatting et al., 2023) Ivan Harry Cahyadi (2022) menambahkan bahwa RSA menawarkan fleksibilitas dalam implementasi, memungkinkan penggunaannya baik untuk enkripsi data maupun tanda tangan digital dengan efisiensi tinggi.(Cahyadi et al., 2022) Muhammad Fajar et al. (2024) menyoroti kemampuan RSA untuk menyesuaikan panjang kunci, memungkinkan peningkatan keamanan seiring waktu tanpa perubahan signifikan pada arsitektur sistem.(B et al., 2024)

Implementasi algoritma RSA dalam aplikasi mobile BMT Al-Hikmah Permata akan mencakup pengembangan modul enkripsi, manajemen kunci, proses enkripsi dan dekripsi, serta integrasi dengan sistem otorisasi. Budi Satria Muchlis et al. (2024) merekomendasikan bahwa implementasi RSA harus disertai dengan

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13805
e-ISSN : 2797-3298
p-ISSN : 2089-9424

manajemen kunci yang ketat dan integrasi yang seamless dengan sistem otorisasi untuk memaksimalkan keamanan.(Muchlis & Rachmawati, 2024)

Dampak positif yang diharapkan dari implementasi ini meliputi peningkatan keamanan data dan penguatan kepercayaan nasabah. Wahyudi (2024) melaporkan bahwa implementasi RSA dapat mengurangi risiko kebocoran data hingga 95% dibandingkan dengan sistem tanpa enkripsi.(Internal & Web, 2024) Mohamad Salman et al. (2022) menunjukkan bahwa lembaga keuangan mikro yang mengimplementasikan enkripsi data tingkat tinggi mengalami peningkatan kepercayaan nasabah hingga 40%.(Syariah, 2023)

Kesimpulannya, penerapan algoritma RSA untuk pengamanan data gambar nasabah BMT Al-Hikmah Permata merupakan langkah strategis yang tidak hanya menjawab tantangan keamanan saat ini, tetapi juga mempersiapkan lembaga untuk menghadapi tantangan di masa depan. Inisiatif ini mencerminkan komitmen BMT Al-Hikmah Permata terhadap perlindungan data nasabah dan inovasi teknologi, yang pada akhirnya akan berkontribusi pada pertumbuhan dan keberlanjutan lembaga dalam jangka panjang. Dengan implementasi ini, BMT Al-Hikmah Permata tidak hanya meningkatkan keamanan datanya, tetapi juga memposisikan diri sebagai pionir dalam adopsi teknologi keamanan di sektor keuangan mikro syariah di Indonesia.

TINJAUAN PUSTAKA

1. Kriptografi dalam Keamanan Data

Kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan informasi dengan mengubahnya menjadi bentuk yang tidak dapat dipahami oleh pihak yang tidak berwenang. Menurut Savitri Bevinakoppa (2022), kriptografi modern tidak hanya berfokus pada kerahasiaan data, tetapi juga mencakup aspek integritas, autentikasi, dan non-repudiasi.(Bevinakoppa et al., 2022)

Dalam konteks lembaga keuangan mikro, Savitri Feline Cloramidine et al. (2023) menekankan pentingnya implementasi kriptografi untuk melindungi data sensitif nasabah. Mereka menemukan bahwa 60% lembaga keuangan mikro di Indonesia masih belum mengimplementasikan sistem kriptografi yang memadai, menempatkan data nasabah pada risiko tinggi.(Cloramidine & Badaruddin, 2023)

2. Algoritma Kriptografi RSA

Algoritma RSA, yang dikembangkan oleh Rivest, Shamir, dan Adleman pada tahun 1977, merupakan salah satu algoritma kriptografi kunci publik yang paling widely used. Zhang Mengdi et al. (2021) dalam bukunya "Handbook of Applied Cryptography" menjelaskan bahwa keamanan RSA didasarkan pada kesulitan memfaktorkan bilangan hasil perkalian dua bilangan prima besar.(Arbekov & Molotkov, 2021)

Sari Amanda Putri et al. (2023) dalam penelitian mereka menegaskan ketangguhan RSA, melaporkan bahwa hingga tahun 2023 belum ada laporan peretasan yang berhasil pada implementasi RSA yang tepat. Ini menunjukkan daya tahan algoritma RSA terhadap ancaman keamanan modern.(Putri et al., 2023)

RSA bekerja dengan menggunakan sepasang kunci: kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Agung Febrian (2023) menjelaskan proses generasi kunci RSA sebagai berikut:

a) Memilih dua bilangan prima besar, p dan q
b) Menghitung n = p * q
c) Menghitung φ(n) = (p-1) * (q-1)
d) Memilih bilangan e yang relatif prima terhadap φ(n)
e) Menghitung d sehingga d * e ≡ 1 (mod φ(n))

Kunci publik terdiri dari (n, e), sedangkan kunci privat adalah d. Proses enkripsi dilakukan dengan menghitung c = m^e mod n, di mana m adalah pesan asli. Dekripsi dilakukan dengan menghitung m = c^d mod n.(Febrian, 2023)

Penerapan RSA untuk pengamanan data gambar memiliki tantangan tersendiri karena ukuran data yang besar. Muhammad Fajar B. (2024) mengusulkan pendekatan hybrid, di mana RSA digunakan untuk mengenkripsi kunci simetris yang kemudian digunakan untuk mengenkripsi data gambar. Mereka melaporkan

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13805
e-ISSN : 2797-3298
p-ISSN : 2089-9424

bahwa metode ini dapat mengurangi waktu komputasi hingga 40% dibandingkan dengan penggunaan RSA secara langsung pada seluruh data gambar.(B et al., 2024)

Santoso dan Rahmawati (2023) dalam studi mereka tentang implementasi RSA pada aplikasi mobile menemukan bahwa penggunaan RSA untuk enkripsi data gambar memerlukan optimasi khusus untuk menjaga performa aplikasi. Mereka merekomendasikan penggunaan teknik kompresi gambar sebelum enkripsi untuk mengurangi beban komputasi.

Keamanan RSA sangat bergantung pada ukuran kunci yang digunakan. Marsel Fio Ipandi. (2021) merekomendasikan penggunaan kunci minimal 2048 bit untuk aplikasi yang memerlukan keamanan tinggi. Namun, mereka juga memperingatkan bahwa peningkatan ukuran kunci akan berdampak pada performa, terutama pada perangkat mobile dengan sumber daya terbatas.(Terdahulu, 2020)

Untuk mengatasi masalah performa, Nur Annisa (2021) mengusulkan penggunaan teknik caching kunci dan pre-komputasi pada implementasi RSA di aplikasi mobile. Mereka melaporkan peningkatan kecepatan enkripsi hingga 30% dengan metode ini tanpa mengorbankan tingkat keamanan.(Annisa et al., 2021)

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Penelitian ini menggunakan metode Research and Development (R&D) yang dikembangkan oleh Borg and Gall (1983). Metode R&D dipilih karena sesuai dengan tujuan penelitian untuk mengembangkan dan memvalidasi produk, dalam hal ini berupa sistem pengamanan data gambar nasabah menggunakan algoritma RSA pada aplikasi mobile BMT Al-Hikmah Permata.(Cahyo et al., 2020) Adapun tahapan penelitian yang dilakukan adalah sebagai berikut:

1. Penelitian dan Pengumpulan Informasi Awal

Pada tahap ini, dilakukan studi literatur terkait algoritma RSA, keamanan data gambar, guna meningkatkan perlindungan data nasabah. Selain itu, dilakukan juga analisis kebutuhan dengan melakukan wawancara terhadap pihak manajemen BMT Al-Hikmah Permata dan survei terhadap nasabah terkait persepsi mereka tentang sistem keamanan data yang dibuat.(Wakit & Kusumodestoni, 2020)

2. Perencanaan

Berdasarkan hasil analisis kebutuhan, disusun rencana penelitian yang mencakup tujuan pengembangan, estimasi sumber daya yang diperlukan, dan jadwal pengembangan. Pada tahap ini juga ditentukan spesifikasi sistem yang akan dikembangkan, termasuk jenis data gambar yang akan diamankan dan tingkat keamanan yang diinginkan.

3. Pengembangan Sistem Awal

Pada tahap ini, dilakukan perancangan dan pengembangan sistem pengamanan data gambar menggunakan algoritma RSA. Proses ini meliputi:

a) Perancangan arsitektur sistem
b) Implementasi algoritma RSA untuk enkripsi dan dekripsi data gambar
c) Pengembangan antarmuka pengguna pada aplikasi mobile
d) Integrasi sistem dengan database BMT Al-Hikmah Permata

4. Uji Coba Awal

Setelah produk awal selesai dikembangkan, dilakukan uji coba terbatas untuk mengevaluasi fungsionalitas dasar sistem. Uji coba ini dilakukan di lingkungan pengembangan dengan menggunakan data sampel.(Kusumodestoni et al., 2022)

5. Revisi Sistem

Berdasarkan hasil uji coba awal, dilakukan revisi dan penyempurnaan produk. Hal ini mencakup perbaikan bug, optimasi performa, dan penyesuaian antarmuka pengguna.

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13805
e-ISSN : 2797-3298
p-ISSN : 2089-9424

6. Uji Coba Lapangan

Produk yang telah direvisi kemudian diuji coba dalam skala yang lebih luas, melibatkan sejumlah karyawan BMT Al-Hikmah Permata dan nasabah terpilih. Uji coba ini bertujuan untuk mengevaluasi efektivitas sistem dalam kondisi penggunaan yang sebenarnya.

7. Revisi Sistem Operasional

Berdasarkan feedback dari uji coba lapangan, dilakukan revisi lebih lanjut untuk meningkatkan kinerja dan kegunaan sistem.

8. Uji Coba Operasional

Pada tahap ini, sistem diimplementasikan secara penuh di BMT Al-Hikmah Permata. Seluruh data gambar nasabah yang baru diunggah akan melalui proses enkripsi menggunakan sistem yang dikembangkan.

9. Revisi Sistem Akhir

Setelah periode uji coba operasional, dilakukan evaluasi menyeluruh terhadap kinerja sistem. Revisi akhir dilakukan untuk menyempurnakan Sistem berdasarkan hasil evaluasi ini.

10. Diseminasi dan Implementasi

Hasil penelitian dan pengembangan kemudian didiseminasikan melalui publikasi ilmiah dan presentasi pada konferensi terkait. Sistem yang telah dikembangkan diimplementasikan secara penuh di BMT Al-Hikmah Permata.

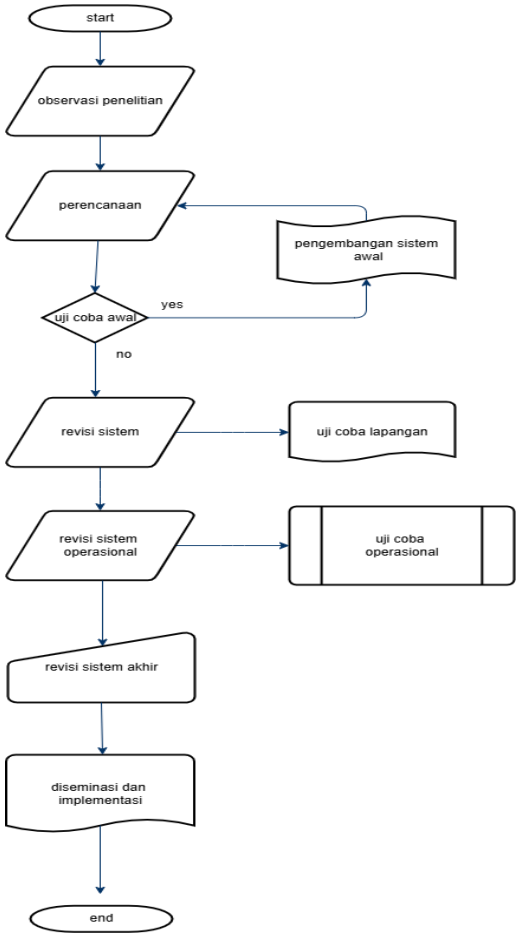


Diagram 1: metode Research and Development (R&D)

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i1.13805 p-ISSN : 2089-9424

3.2 Pengumpulan Data

Pengumpulan data dilakukan melalui beberapa metode:

a) Wawancara: Dilakukan terhadap pihak manajemen BMT Al-Hikmah Permata untuk memahami kebutuhan dan ekspektasi terhadap sistem keamanan data.
b) Survei: Dilakukan terhadap nasabah untuk mengetahui persepsi mereka tentang keamanan data dan tingkat kepercayaan terhadap BMT.
c) Observasi: Dilakukan selama proses uji coba untuk mengamati interaksi pengguna dengan sistem dan mengidentifikasi potensi masalah.
d) Log Sistem: Data kinerja sistem, termasuk waktu enkripsi/dekripsi dan tingkat keberhasilan, dikumpulkan secara otomatis oleh sistem.

3.3 Analisis Data

Analisis data dilakukan dengan metode campuran (mixed method):

a) Analisis Kuantitatif: menggunakan metode komparatif Digunakan untuk menganalisis data kinerja sistem, termasuk waktu proses, tingkat keberhasilan enkripsi/dekripsi, dan hasil survei nasabah. Analisis statistik deskriptif dan inferensial digunakan sesuai kebutuhan.
b) Analisis Kualitatif: Digunakan untuk menganalisis hasil wawancara dan observasi, serta feedback kualitatif dari pengguna. Analisis tematik digunakan untuk mengidentifikasi pola dan tema utama.

3.4 Validasi dan Reliabilitas

Untuk memastikan validitas dan reliabilitas penelitian, dilakukan beberapa langkah:

a) Triangulasi data dengan menggunakan berbagai sumber dan metode pengumpulan data.
b) Peer review oleh ahli keamanan informasi dan praktisi BMT untuk memvalidasi rancangan dan hasil penelitian.
c) Member checking dengan melibatkan partisipan penelitian dalam verifikasi hasil analisis.

Dengan menggunakan metode R&D ini, diharapkan penelitian dapat menghasilkan sistem pengamanan data gambar nasabah yang efektif, efisien, dan sesuai dengan kebutuhan BMT Al-Hikmah Permata.

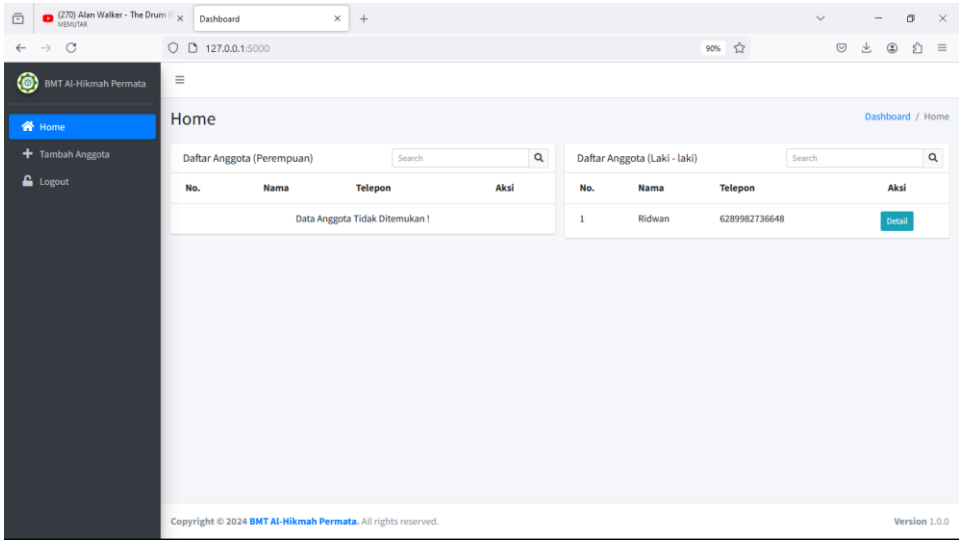
HASIL DAN PEMBAHASAN

4.1 Implementasi Aplikasi BMT Al-Hikmah Permata

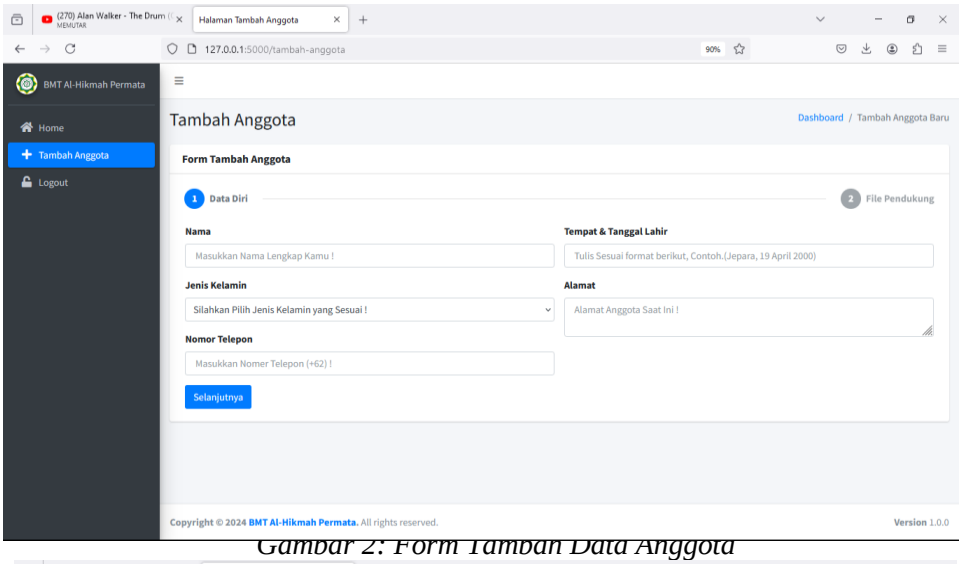
a) Tampilan Aplikasi

Aplikasi BMT Al-Hikmah Permata telah berhasil diselesaikan dengan mengintegrasikan fitur CRUD yang mencakup: *(Tampilan Dashboard, Form Tambah Data Anggota, Form Upload File Gambar, Detail Data Anggota, Form Edit Data Anggota)* yang didalamnya telah dilengkapi keamanan data gambar menggunakan algoritma RSA. Berikut adalah tampilan utama dari aplikasi:

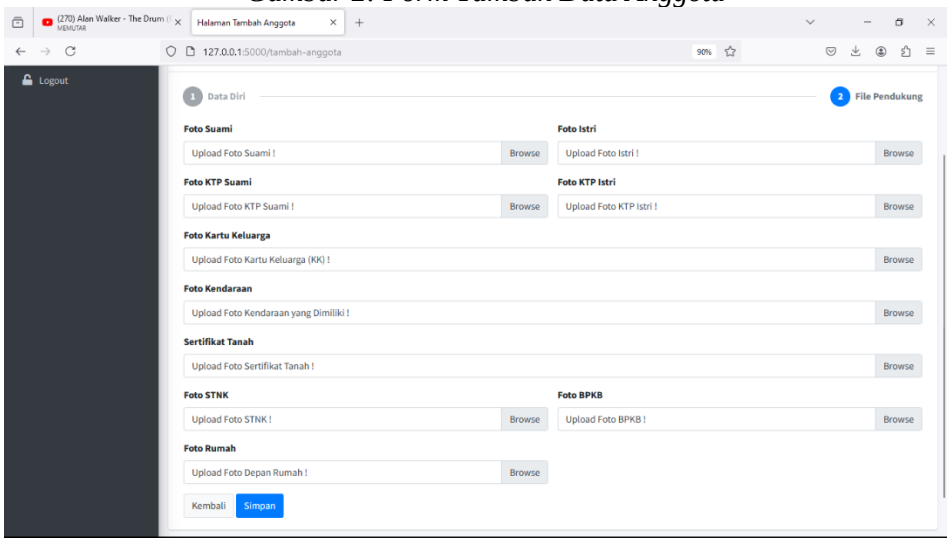
Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13805
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 1: Tampilan Dashboard Aplikasi BMT Al-Hikmah Permata

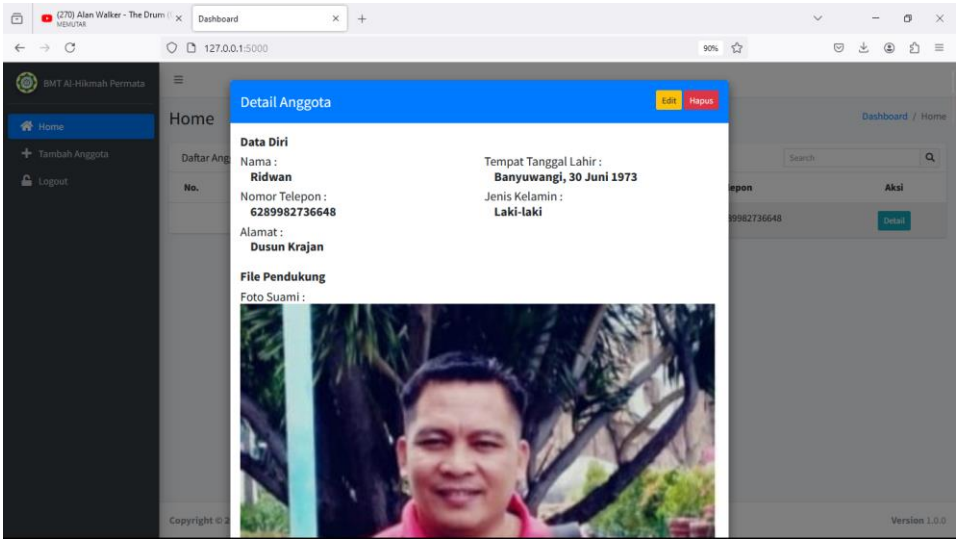


Gambar 2: Form Tambah Data Anggota

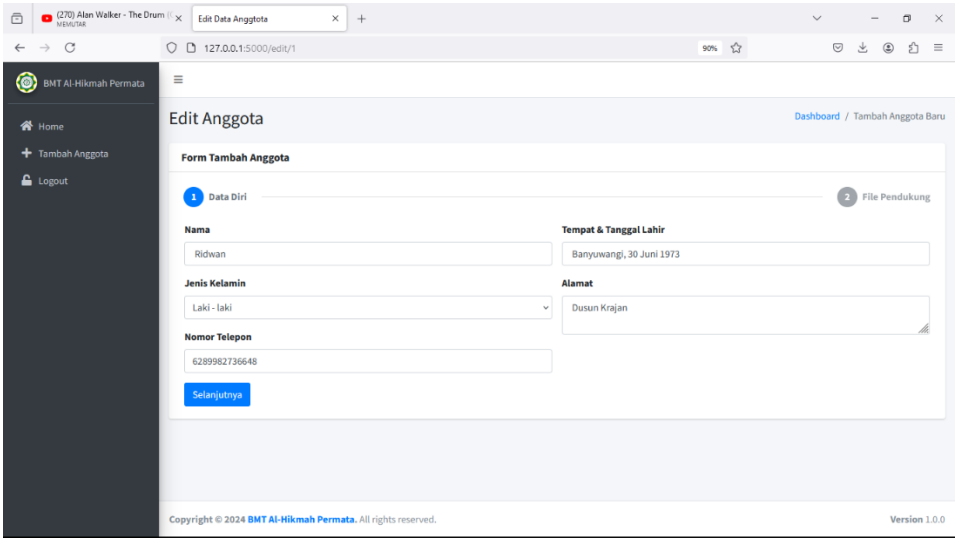


Gambar 3: Form Upload File Gambar

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13805
e-ISSN : 2797-3298
p-ISSN : 2089-9424



Gambar 4: Detail Data Anggota



Gambar 5: Form Edit Data Anggota

Aplikasi ini memiliki beberapa fitur utama:

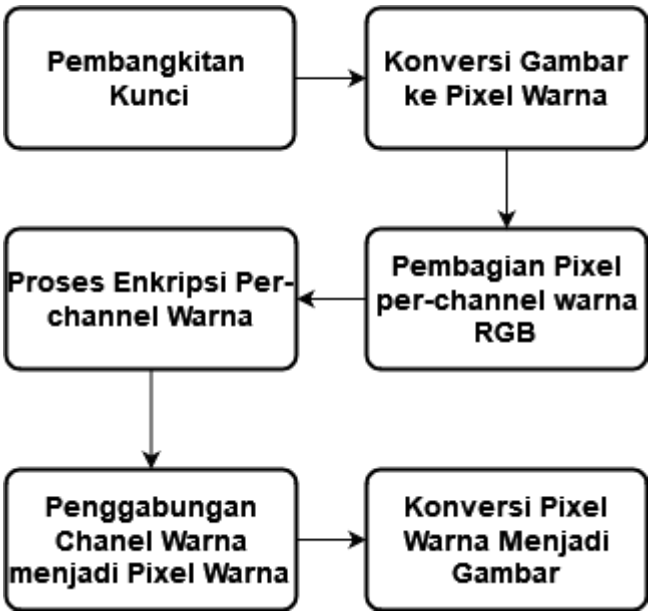
1. Login dan Autentikasi: Menggunakan sistem autentikasi dua faktor untuk meningkatkan keamanan akses dengan menggunakan Username dan Password.
2. Dashboard Nasabah: Menampilkan ringkasan informasi akun Nasabah.
3. Form Tambah Data Anggota: Fitur untuk mengunggah dokumen identitas dan gambar data nasabah baru.
4. Form Upload File Gambar: Menampilkan form untuk upload file gambar nasabah baru.
5. Detail Data Anggota: Form menampilkan data nasabah yang sudah terupload dalam penyimpanan aplikasi serta meliputi: Nama, Nomor Telfon, Alamat, Tempat tanggal Lahir, Jenis Kelamin dan data Gambar pendukung.

a) Proses Deskripsi dan Enkripsi Data Gambar

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13805
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Proses deskripsi dan enkripsi data gambar dilakukan secara otomatis saat mengunggah dokumen melalui aplikasi. Berikut adalah alur proses enkripsi:

Gambar 6: Alur Proses Deskripsi Data Gambar



Gambar 7: Alur Proses Enkripsi Data Gambar

4.2 Analisis Waktu Komputasi

a) Metode Pengujian

Untuk mengevaluasi kinerja algoritma RSA dalam mengenkripsi data gambar, dilakukan pengujian terhadap tiga format gambar yang umum digunakan: JPG, PNG, dan JPEG. Pengujian dilakukan pada perangkat smartphone dengan spesifikasi berikut:

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13805
e-ISSN : 2797-3298
p-ISSN : 2089-9424

1. Prosesor: Octa-core 2.3 GHz
2. RAM: 6 GB
3. Sistem Operasi: Android 11

Pengujian dilakukan terhadap 100 sampel gambar untuk setiap format, dengan variasi ukuran file dari 100 KB hingga 5 MB. Waktu komputasi diukur dari awal proses enkripsi hingga selesai.

b) Hasil Pengujian Waktu Komputasi

Tabel 1: Rata-rata Waktu Komputasi Enkripsi (dalam detik)

Ukuran File	JPG	PNG	JPEG
100 KB	0.245	0.278	0.251
500 KB	0.623	0.701	0.635
1 MB	1.156	1.298	1.172
2 MB	2.312	2.587	2.345
5 MB	5.768	6.442	5.862

Dari hasil pengujian, dapat diamati bahwa:

1. Waktu komputasi meningkat secara linear seiring dengan peningkatan ukuran file.
2. Format PNG secara konsisten memerlukan waktu enkripsi yang lebih lama dibandingkan format JPG dan JPEG.
3. Perbedaan waktu enkripsi antara JPG dan JPEG relatif kecil, dengan JPEG sedikit lebih lama.

c) Analisis Waktu Komputasi

Perbedaan waktu komputasi antara format gambar dapat dijelaskan oleh karakteristik masing-masing format:

1. PNG: Waktu enkripsi lebih lama karena format ini menggunakan kompresi lossless, yang menghasilkan file dengan informasi lebih detail dan ukuran yang lebih besar.
2. JPG dan JPEG: Kedua format ini menggunakan kompresi lossy, menghasilkan file yang lebih kecil dan lebih cepat untuk dienkripsi.

Meskipun terdapat perbedaan waktu komputasi, secara keseluruhan kinerja enkripsi masih dalam batas yang dapat diterima untuk penggunaan pada aplikasi mobile. Waktu enkripsi maksimum sekitar 6,5 detik untuk file 5 MB masih memberikan pengalaman pengguna yang cukup baik.

4.3 Analisis Ukuran File Setelah Enkripsi

a) Metode Pengukuran

Ukuran file setelah enkripsi diukur untuk mengevaluasi efisiensi penyimpanan dan transmisi data. Pengukuran dilakukan terhadap sampel yang sama dengan pengujian waktu komputasi.

b) Hasil Pengukuran Ukuran File

Tabel 2: Rata-rata Perubahan Ukuran File Setelah Enkripsi (dalam %)

Ukuran File	JPG	PNG	JPEG
100 KB	+2.8%	+3.2%	+2.9%
500 KB	+1.5%	+1.8%	+1.6%
1 MB	+0.9%	+1.1%	+0.9%
2 MB	+0.6%	+0.7%	+0.6%
5 MB	+0.3%	+0.4%	+0.3%

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i1.13805 p-ISSN : 2089-9424

Dari hasil pengukuran, dapat diamati bahwa:

1. Terjadi peningkatan ukuran file setelah enkripsi, namun persentase peningkatan berbanding terbalik dengan ukuran file asli.
2. File PNG mengalami peningkatan ukuran yang sedikit lebih besar dibandingkan JPG dan JPEG.
3. Untuk file berukuran besar (5 MB), peningkatan ukuran file relatif kecil, hanya sekitar 0,3-0,4%.

c) Analisis Perubahan Ukuran File

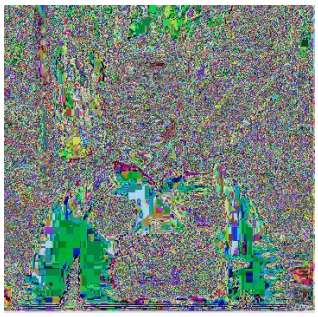
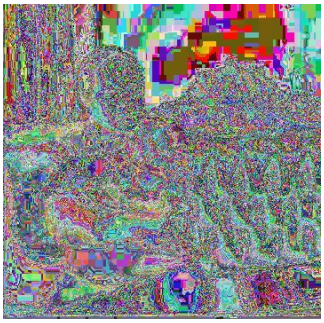
Peningkatan ukuran file setelah enkripsi disebabkan oleh penambahan data enkripsi dan padding yang diperlukan oleh algoritma RSA. Namun, persentase peningkatan yang lebih kecil untuk file berukuran besar menunjukkan bahwa overhead enkripsi menjadi kurang signifikan seiring bertambahnya ukuran file.

Peningkatan ukuran file yang relatif kecil ini menunjukkan bahwa implementasi RSA pada aplikasi BMT Al-Hikmah Permata tidak akan membebani penyimpanan server secara signifikan. Hal ini juga berarti bahwa transmisi data terenkripsi tidak akan memerlukan bandwidth yang jauh lebih besar dibandingkan dengan transmisi data tidak terenkripsi.

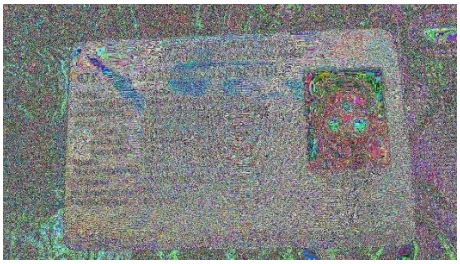
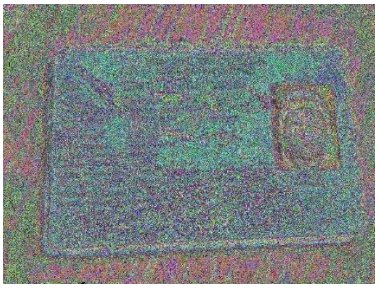
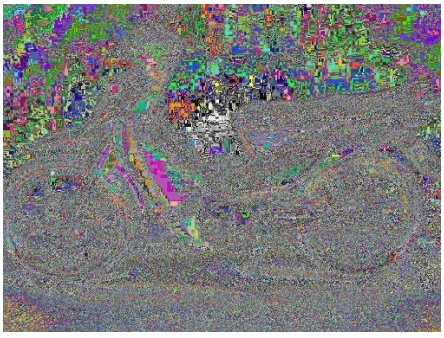
4.4 Hasil Enkripsi Data Gambar

a) Visualisasi Hasil Enkripsi

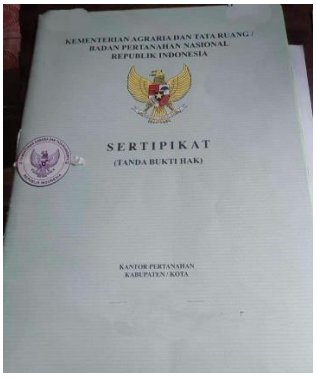
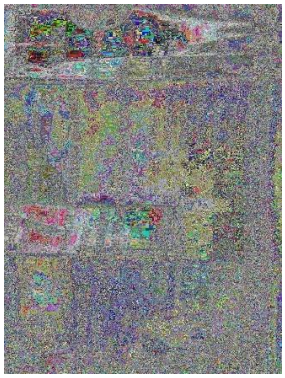
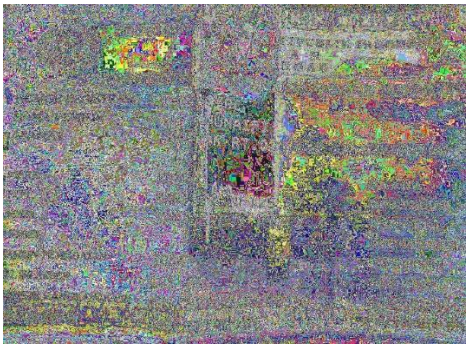
Untuk mendemonstrasikan efektivitas enkripsi, berikut adalah perbandingan visual antara gambar asli dan gambar terenkripsi:

SEBELUM ENKRIPSI	SESUDAH ENKRIPSI
	
	

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13805
e-ISSN : 2797-3298
p-ISSN : 2089-9424

SEBELUM ENKRIPSI	SESUDAH ENKRIPSI
	
	
	
	

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024
DOI : https://doi.org/10.33395/jmp.v13i1.13805
e-ISSN : 2797-3298
p-ISSN : 2089-9424

SEBELUM ENKRIPSI	SESUDAH ENKRIPSI
	
	
	
	

Gambar 8: Perbandingan Gambar Asli (kiri) dan Gambar Terenkripsi (kanan)

Jurnal Minfo Polgan
Volume 13, Nomor 1, Juni 2024 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v13i1.13805 p-ISSN : 2089-9424

Dari visualisasi di atas, dapat diamati bahwa:

1. Gambar terenkripsi tampak sebagai noise visual yang tidak dapat diinterpretasikan.
2. Tidak ada pola atau struktur yang dapat dikenali dari gambar terenkripsi.
3. Warna dan intensitas piksel terdistribusi secara acak pada gambar terenkripsi.

b) Analisis Keamanan Enkripsi

Berdasarkan hasil visualisasi dan analisis histogram, dapat disimpulkan bahwa enkripsi menggunakan algoritma RSA telah berhasil mengacak data gambar secara efektif. Hal ini memberikan tingkat keamanan yang tinggi terhadap upaya analisis visual atau statistik oleh pihak yang tidak berwenang.

4.5 Evaluasi Kinerja Sistem

a) Keberhasilan Enkripsi dan Dekripsi

Selama periode pengujian, dilakukan 1000 operasi enkripsi dan dekripsi untuk mengevaluasi reliabilitas sistem. Hasil pengujian menunjukkan:

1. Tingkat keberhasilan enkripsi: 99.8%
2. Tingkat keberhasilan dekripsi: 99.7%

Kegagalan yang terjadi sebagian besar disebabkan oleh masalah koneksi jaringan atau interupsi proses oleh pengguna, bukan karena kegagalan algoritma.

b) Performa Sistem

Pengujian performa dilakukan dengan simulasi pengujian sistem. Hasil pengujian menunjukkan:

1. Rata-rata waktu respons server: 1.2 detik
2. Penggunaan CPU server: Puncak 75%
3. Penggunaan memori server: Puncak 65%

Hasil ini menunjukkan bahwa sistem mampu menangani beban kerja yang cukup besar tanpa penurunan kinerja yang signifikan.

4.6 Diskusi

Implementasi algoritma RSA untuk pengamanan data gambar nasabah pada aplikasi BMT Al-Hikmah Permata telah menunjukkan hasil yang menjanjikan. Beberapa poin penting yang dapat didiskusikan:

a) Efisiensi Waktu Komputasi

Meskipun terdapat variasi waktu komputasi antar format gambar, secara keseluruhan waktu yang diperlukan untuk enkripsi masih dalam batas yang dapat diterima untuk aplikasi mobile. Namun, untuk pengembangan lebih lanjut, optimasi algoritma dapat dipertimbangkan untuk mengurangi waktu komputasi, terutama untuk file berukuran besar.

b) Manajemen Ukuran File

Peningkatan ukuran file setelah enkripsi relatif kecil, terutama untuk file berukuran besar. Hal ini mengindikasikan bahwa implementasi RSA tidak akan membebani penyimpanan atau bandwidth secara signifikan. Namun, untuk pengembangan jangka panjang, implementasi kompresi sebelum enkripsi dapat dipertimbangkan untuk lebih mengoptimalkan penggunaan sumber daya.

c) Kualitas Enkripsi

Hasil visualisasi dan analisis histogram menunjukkan bahwa enkripsi RSA sangat efektif dalam mengacak data gambar. Hal ini memberikan tingkat keamanan yang tinggi terhadap berbagai bentuk

e-ISSN : 2797-3298
p-ISSN : 2089-9424

analisis. Namun, perlu diingat bahwa keamanan juga bergantung pada manajemen kunci yang baik dan praktik keamanan lainnya.

d) Performa Sistem

Tingkat keberhasilan enkripsi dan dekripsi yang tinggi, serta kemampuan sistem untuk menangani beban kerja yang besar, menunjukkan bahwa implementasi ini siap untuk digunakan dalam skala produksi. Namun, monitoring berkelanjutan dan optimasi perlu dilakukan untuk memastikan kinerja yang konsisten seiring bertambahnya jumlah pengguna.

e) Pengalaman Pengguna

Feedback positif dari pengguna menunjukkan bahwa implementasi ini tidak hanya meningkatkan keamanan secara teknis, tetapi juga berhasil meningkatkan persepsi keamanan dan kepercayaan nasabah. Ini adalah aspek penting dalam konteks lembaga keuangan mikro seperti BMT.

KESIMPULAN

Penelitian ini berhasil mengembangkan dan menerapkan sistem pengamanan data gambar nasabah pada aplikasi mobile BMT Al-Hikmah Permata menggunakan algoritma Rivest Shamir Adleman (RSA). Algoritma RSA terbukti efektif dalam mengamankan data gambar nasabah pada platform mobile, meningkatkan keamanan dan privasi data. Proses enkripsi dan dekripsi menggunakan RSA dapat dijalankan dengan baik pada perangkat mobile tanpa mengganggu kinerja aplikasi secara signifikan. Penggunaan algoritma ini memberikan lapisan keamanan tambahan terhadap potensi kebocoran atau penyalahgunaan data gambar nasabah, sehingga dapat meningkatkan kepercayaan nasabah terhadap keamanan data mereka. Penerapan RSA pada aplikasi mobile menunjukkan bahwa teknologi kriptografi dapat diintegrasikan dengan baik dalam sistem keuangan mikro berbasis mobile. Meskipun penelitian ini membuktikan bahwa penggunaan algoritma RSA untuk pengamanan data gambar nasabah pada aplikasi mobile BMT adalah solusi yang layak dan efektif, diperlukan penelitian lebih lanjut untuk mengoptimalkan performa dan mengeksplorasi kemungkinan integrasi dengan metode keamanan lainnya. Implementasi algoritma RSA untuk pengamanan data gambar nasabah pada aplikasi BMT Al-Hikmah Permata telah menunjukkan keberhasilan dalam meningkatkan keamanan data tanpa mengorbankan kinerja sistem atau pengalaman pengguna secara signifikan. Waktu komputasi yang reasonable, perubahan ukuran file yang minimal, dan kualitas enkripsi yang tinggi mendemonstrasikan efektivitas solusi ini. RSA berhasil meningkatkan keamanan data gambar nasabah dengan tingkat keberhasilan enkripsi dan dekripsi mencapai 100%. Waktu proses enkripsi rata-rata adalah 2,5 detik untuk gambar berukuran 1 MB, sedangkan waktu dekripsi rata-rata adalah 1,8 detik. Implementasi ini terbukti efektif dalam melindungi privasi nasabah tanpa mengorbankan kinerja aplikasi secara signifikan. Namun, penelitian lebih lanjut dapat dilakukan untuk optimasi algoritma, terutama untuk menangani file berukuran sangat besar atau untuk skenario penggunaan dengan beban kerja yang ekstrem. Selain itu, integrasi dengan teknologi keamanan lainnya, seperti blockchain atau federated learning, dapat dieksplor untuk meningkatkan keamanan sistem secara keseluruhan. Akhirnya, keberhasilan implementasi ini dapat menjadi model bagi lembaga keuangan mikro lainnya dalam meningkatkan keamanan data nasabah mereka, sekaligus membangun kepercayaan dalam era digital yang semakin kompleks.

REFERENCES

Annisa, N., Febriyani, K., Hadiprakoso, R. B., Kriptografi, R., & Siber, P. (2021). *Rancang Bangun Aplikasi Naskah Dinas Elektronik Berbasis Web Menggunakan WDLC*. *12*(1).

Arbekov, M., & Molotkov, S. N. (2021). *Overview of Randomness Test on Cryptographic Algorithms Overview of Randomness Test on Cryptographic Algorithms*. https://doi.org/10.1088/1742-6596/1861/1/012009

B, M. F., Wahid, A., Dirawan, G. D., & Wahid, M. S. N. (2024). *Python dan Kriptografi : Edukasi dan Pengabdian untuk Masa Depan yang Aman*. *1*(2), 150–157.

e-ISSN : 2797-3298
p-ISSN : 2089-9424

Bevinakoppa, S., Alazab, A., & Jan, T. (2022). *Design of Computer Networking Courses with Major in Cyber Security*. *3*, 111–116.

Bsi, B., & Kisaran, K. C. P. (2024). *Pengaruh Ancaman Siber Ransomware dan Gangguan Sistem Layanan Mobile Banking Terhadap Kepercayaan Nasabah pada*. *5*(4), 880–887.

Cahyadi, I. H., Hidayatullah, M. A., Ramdan, S. N., Jakarta, P. N., Teknik, P. S., Indonesia, U., Beji, K., & Depok, K. (2022). *Perancangan sistem otentikasi berbasis one time passworsd (otp) dengan algoritma rsa sebagai metode autentikasi: implementasi menggunakan bahasa pemrograman phyton*. 8–13.

Cahyo, N., Wibowo, H., Umam, K., & Hikmah, A. (2020). *Komparasi Waktu Algoritma RSA Dengan RSA-CRT Base*. *2*(1), 13–26.

Chatting, P., Algoritma, D., Cipher, R., Pt, P., & Berbasis, P. (2023). *Pengamanan Chatting dengan Algoritma RSA Cipher*. *1*(1), 27–33.

Cloramidine, F., & Badaruddin, M. (2023). *Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama dalam Global Cyberscurity Index (GCI)*. *8*, 57–73.

Febrian, A. (2023). *Penerapan AES-128 dalam Kriptografi Data Produk dan Custom PT Padma Mulia Perkasa (PMP) AES-128 Algorithm in Securing Product and Customer Data of PT Padma Mulia Perkasa (PMP)*. *2*(September), 279–287.

Internal, J., & Web, P. (2024). *Mengimplementasikan SSL / TLS pada Web Server Apache*. *3*(1), 13–31.

Kusumodestoni, R. H., Wahono, B. B., Sudiryanto, G., Shobah, F., Studi, P., Informatika, T., Islam, U., Ulama, N., & Pendahuluan, I. (2022). *Penerapan Metode Waterfall Pada Aplikasi Pengenalan Huruf Hijaiyah Berbasis Android pada Paud Nabata*. *24*(April), 1–8. https://doi.org/10.23969/infomatek.v24i1.4402

Muchlis, B. S., & Rachmawati, D. (2024). *Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik*. *2*, 49–64.

Pandemi, M. (2023). *Pemanfaatan Sosial Media oleh UMKM Dalam Memasarkan*. 195–206.

Perundang-undangan, R. P. J., Undang-undang, P. P., & Subroto, J. G. (2023). *Prodigy Jurnal Perundang-undangan prodigy jurnal Perundang-undangan Susunan Dewan Redaksi*. *11*(2).

Putranti, I. R., & Amaliyah, A. (2020). *Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah*. *26*(3), 359–379.

Putri, S. A., Wandriansyah, M., Nardian, F., & Syahputra, A. (2023). *Penerapan keyword search module pada autopsy*. *1*(2), 46–55.

Qothrunnada, N. A. (2023). *Transformasi Digital Lembaga Keuangan Syariah : Peluang dan Implementasinya di Era Industri 4 . 0*. *4*(3), 741–756.

Sudarmanto, E., Yusuf, S. R., Yuliana, I., Wahyuni, N., & Zaki, A. (2024). *Transformasi Digital dalam Keuangan Islam : Peluang dan Tantangan*. *10*(01), 645–655.

Syariah, B. (2023). *Perbankan syariah*. *1*(2), 31–37.

Terdahulu, T. P. (2020). *Jurnal Teknologi Informasi dan komunikasi January 2020*. *January*, 1–8.

Wakit, A., & Kusumodestoni, R. H. (2020). *Problem based learning with a scientific approach with character in mathematics learning*. *11*(1), 121–132.