Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika
Volume 3 Nomor 5, September 2025
e-ISSN : 3031-8912; p-ISSN : 3031-8904; Hal 41-60
DOI: https://doi.org/10.61132/merkurius.v3i5.1036
Tersedia: https://journal.arteii.or.id/index.php/Merkurius

Implementasi Algoritma Kriptografi Hybrid AES dan RSA dalam Rancang Bangun Aplikasi Bank Sampah Pancadaya Berbasis Web untuk Keamanan Data Transaksi Nasabah

Mardhyah Fathania 'Izzati, Widya Darwin
Program Studi Informatika, Universitas Negeri Padang

Alamat: Jl. Prof. Dr. Hamka, Air Tawar Bar., Kec. Padang Utara, Kota Padang, Sumatera Barat, Indonesia 25171
**Penulis korespondensi: mardhyah01@gmail.com*

Abstract. *This research aims to develop a transaction data security system on the web-based Pancadaya Waste Bank application by applying a hybrid cryptographic algorithm that combines Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA). The problem faced in the previous system is the weak recording and security of customer transaction data, because the process is still carried out manually so that it is prone to recording errors, loss of important information, and potential misuse of data by unauthorized parties. To answer these problems, this study uses the Rapid Application Development (RAD) method which allows the application development process to be carried out quickly, flexibly, structured, and according to user needs. The research method used was a qualitative approach with interview techniques with the management of the Pancadaya Waste Bank and the Environment Office, as well as an in-depth literature study on the application of hybrid cryptographic algorithms in modern information systems. The system is built using the PHP programming language, MySQL database, and OpenSSL library as the main support for the data encryption and decryption process. The implementation of the algorithm is carried out by encrypting transaction data using AES for efficiency and speed, then the AES key is secured through RSA to ensure a higher level of security while preventing illegal access. The test results showed that the system was able to encrypt and decrypt transaction data in real-time, as well as display transaction results in the form of digital notes on deposit and balance withdrawal activities. In addition, performance tests using GTmetrix showed that the application has excellent speed, stability, and processing efficiency, making it feasible to be widely implemented in Pancadaya Waste Bank operations.*

Keywords: *AES; Web Applications; Waste Bank; Hybrid Cryptography; RSA*

Abstrak. Penelitian ini bertujuan untuk mengembangkan sistem keamanan data transaksi pada aplikasi Bank Sampah Pancadaya berbasis web dengan menerapkan algoritma kriptografi hybrid yang menggabungkan Advanced Encryption Standard (AES) dan Rivest Shamir Adleman (RSA). Permasalahan yang dihadapi pada sistem sebelumnya adalah lemahnya pencatatan serta keamanan data transaksi nasabah, karena proses masih dilakukan secara manual sehingga rawan terjadi kesalahan pencatatan, kehilangan informasi penting, maupun potensi penyalahgunaan data oleh pihak yang tidak berwenang. Untuk menjawab permasalahan tersebut, penelitian ini menggunakan metode Rapid Application Development (RAD) yang memungkinkan proses pengembangan aplikasi dilakukan secara cepat, fleksibel, terstruktur, serta menyesuaikan kebutuhan pengguna. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan teknik wawancara bersama pengelola Bank Sampah Pancadaya dan Dinas Lingkungan Hidup, serta studi literatur mendalam mengenai penerapan algoritma kriptografi hybrid pada sistem informasi modern. Sistem dibangun menggunakan bahasa pemrograman PHP, basis data MySQL, dan pustaka OpenSSL sebagai pendukung utama proses enkripsi dan dekripsi data. Implementasi algoritma dilakukan dengan cara mengenkripsi data transaksi menggunakan AES untuk efisiensi dan kecepatan, kemudian kunci AES diamankan melalui RSA untuk memastikan tingkat keamanan yang lebih tinggi sekaligus mencegah akses ilegal. Hasil pengujian menunjukkan bahwa sistem mampu mengenkripsi sekaligus mendekripsi data transaksi secara real-time, serta menampilkan hasil transaksi dalam bentuk nota digital pada kegiatan setor maupun tarik saldo. Selain itu, uji performa menggunakan GTmetrix menunjukkan bahwa aplikasi memiliki kecepatan, stabilitas, serta efisiensi pemrosesan yang sangat baik, sehingga layak diimplementasikan secara luas pada operasional Bank Sampah Pancadaya. Dengan demikian, aplikasi ini memberikan solusi inovatif dan berkelanjutan dalam meningkatkan keamanan, akurasi, transparansi, serta efisiensi pengelolaan data transaksi pada sistem bank sampah berbasis digital.

Kata kunci: AES; Aplikasi Web; Bank Sampah; Kriptografi Hybrid; RSA

Naskah masuk: 30 Juli, 2025; Revisi: 10 Agustus, 2025; Diterima: 25 Agustus, 2025; Tersedia: 28 Agustus, 2025

1. LATAR BELAKANG

Pengelolaan sampah menjadi isu strategis dalam kebijakan lingkungan hidup di Indonesia, sebagaimana ditegaskan dalam Undang-Undang Republik Indonesia Nomor 18 Tahun 2008 tentang Pengelolaan Sampah. Undang-undang tersebut menekankan pentingnya penanganan sampah secara sistematis, menyeluruh, dan berkesinambungan, khususnya melalui penerapan prinsip 3R (reduce, reuse, recycle). Hal ini mengindikasikan adanya pergeseran paradigma dari sekadar membuang sampah menjadi upaya pengelolaan sumber daya yang lebih ramah lingkungan. Kota Padang sebagai salah satu daerah metropolitan di Sumatera Barat menghadapi tantangan serius dalam pengelolaan sampah, mengingat volume timbulan harian yang mencapai 660,06 ton (KLHK, 2024). Angka ini menuntut kebijakan yang tidak hanya reaktif tetapi juga partisipatif dan inovatif, termasuk melalui inisiasi pendirian Bank Sampah yang tidak hanya berorientasi pada pengurangan volume sampah, tetapi juga pada peningkatan nilai ekonomis dari sampah tersebut.

Untuk menanggapi tantangan tersebut, Pemerintah Kota Padang melalui Badan Pengendalian Dampak Lingkungan Daerah (Bapedalda) telah menginisiasi pembentukan Bank Sampah berbasis masyarakat di berbagai kelurahan. Program ini sejalan dengan semangat desentralisasi pengelolaan lingkungan yang mengutamakan peran serta masyarakat dalam menjaga kebersihan dan kelestarian lingkungan. Bank Sampah tidak hanya berperan sebagai pusat pengumpulan sampah terpilah, tetapi juga menjadi sarana edukasi dan pemberdayaan ekonomi. Sampah yang sebelumnya dipandang sebagai limbah kini dikonversi menjadi aset yang memiliki nilai tukar, sebagaimana diungkapkan oleh Rahma Fitri et al. (2024), bahwa Bank Sampah telah mengubah pola pikir masyarakat dari membuang menjadi menabung sampah. Transformasi ini tentunya membutuhkan sistem pengelolaan data yang akuntabel dan efisien, mengingat setiap transaksi yang dilakukan akan berkontribusi pada saldo nasabah yang pada akhirnya dapat ditukar dengan berbagai bentuk insentif.

Salah satu Bank Sampah yang menjadi pusat perhatian adalah Bank Sampah Pancadaya yang terletak di Kecamatan Kuranji. Bank ini memiliki status sebagai Bank Sampah Induk (BSI) di Kota Padang dan telah aktif sejak tahun 2017. Dengan lebih dari 1000 nasabah dari berbagai unit bank sampah di kota tersebut, BSI Pancadaya menjalankan berbagai program, mulai dari edukasi pengelolaan sampah, pelatihan kerajinan, hingga sistem insentif yang inovatif. Namun demikian, implementasi sistem pencatatan transaksi masih mengalami berbagai kendala teknis, seperti tidak konsistennya nasabah dalam membawa buku tabungan, hingga kurangnya integrasi data antara pencatatan manual dan pembukuan sistem. Realitas ini menunjukkan pentingnya pengembangan sistem informasi yang mampu menjawab kebutuhan

akan efisiensi, akurasi, dan keamanan data transaksi. Oleh karena itu, diperlukan sebuah aplikasi berbasis web yang tidak hanya mampu mencatat data secara digital, tetapi juga memiliki fitur keamanan yang andal.

Keamanan data menjadi isu utama dalam pengembangan aplikasi sistem transaksi bank sampah, mengingat data transaksi memiliki sensitivitas tinggi terutama ketika dikaitkan dengan konversi saldo menjadi aset bernilai seperti emas. Salah satu pendekatan yang diadopsi dalam penelitian ini adalah implementasi sistem keamanan berbasis kriptografi. Kriptografi merupakan ilmu dan seni menyembunyikan informasi agar hanya dapat diakses oleh pihak yang berwenang. Dalam konteks aplikasi bank sampah, kriptografi berperan melindungi data transaksi dari manipulasi dan akses tidak sah. Algoritma yang digunakan dalam penelitian ini adalah kombinasi antara algoritma simetris AES (Advanced Encryption Standard) dan algoritma asimetris RSA (Rivest–Shamir–Adleman). AES digunakan untuk mengenkripsi data transaksi karena kecepatannya dalam memproses data berukuran besar, sedangkan RSA digunakan untuk mengenkripsi kunci AES itu sendiri agar tidak mudah diakses oleh pihak luar.

Konsep penggabungan algoritma simetris dan asimetris ini dikenal dengan istilah hybrid cryptosystem. Pendekatan ini menawarkan solusi yang seimbang antara kecepatan pemrosesan dan keamanan distribusi kunci. Dalam sistem hybrid, AES bertugas untuk mengenkripsi isi pesan atau data transaksi, sedangkan RSA mengenkripsi kunci AES menggunakan kunci publik penerima. Proses ini memastikan bahwa hanya pihak yang memiliki kunci privat RSA yang dapat mendekripsi dan membaca isi pesan. Implementasi teknis dari pendekatan ini dilakukan dengan memanfaatkan library OpenSSL yang menyediakan fungsi-fungsi kriptografi yang diperlukan. Pendekatan hybrid cryptosystem dinilai mampu meminimalisasi risiko kebocoran data dan manipulasi transaksi, serta meningkatkan kepercayaan nasabah terhadap sistem aplikasi bank sampah. Ini menjadi penting terutama ketika sistem mulai terintegrasi dengan institusi keuangan seperti Pegadaian.

Kemitraan antara Bank Sampah Pancadaya dengan PT Pegadaian membuka peluang baru dalam memberikan nilai tambah kepada nasabah melalui konversi saldo sampah menjadi tabungan emas. Program “Memilah Sampah, Menabung Emas” yang diusung menjadi daya tarik tersendiri dan mendorong peningkatan partisipasi masyarakat. Dalam skema ini, setiap saldo hasil penyetoran sampah dapat ditukarkan dengan emas melalui proses transaksi resmi yang dikelola Bank Sampah bekerja sama dengan Pegadaian. Hal ini tidak hanya memberikan insentif ekonomi kepada masyarakat, tetapi juga mendorong budaya menabung dan investasi jangka panjang. Namun, karena bentuk transaksinya melibatkan nilai tukar emas, maka akurasi dan keamanan data menjadi sangat penting. Kesalahan dalam pencatatan atau kebocoran data

dapat menimbulkan kerugian nyata, baik bagi nasabah maupun lembaga pengelola. Oleh karena itu, sistem pengamanan berbasis hybrid cryptosystem menjadi kebutuhan mutlak untuk memastikan integritas sistem informasi dan perlindungan hak nasabah.

Berdasarkan hasil penelitian Lu & Mohamed (2021), hybrid cryptosystem terbukti lebih unggul dalam hal keamanan dan efisiensi dibandingkan penggunaan tunggal algoritma AES atau RSA. Dalam uji kecepatan pemrosesan data, AES menunjukkan performa paling cepat, namun dari sisi entropi atau tingkat keacakan data hasil enkripsi, hybrid encryption menghasilkan entropi tertinggi. Hal ini menandakan bahwa data yang dienkripsi menggunakan metode hybrid lebih sulit diprediksi dan diuraikan oleh pihak yang tidak berwenang. RSA, meskipun unggul dalam aspek keamanan pertukaran kunci, memiliki kelemahan dari segi kecepatan, terutama ketika digunakan untuk mengenkripsi data berukuran besar. Oleh karena itu, kombinasi AES dan RSA menjadi pilihan ideal karena menggabungkan kekuatan dari kedua pendekatan kriptografi ini.

Dengan mempertimbangkan keunggulan dari pendekatan hybrid cryptosystem, penelitian ini mengambil langkah untuk merancang aplikasi berbasis web yang mengintegrasikan algoritma AES dan RSA guna mengamankan transaksi nasabah Bank Sampah Pancadaya. Aplikasi ini dibangun menggunakan bahasa pemrograman PHP, basis data MySQL, dan server lokal XAMPP. Proses enkripsi dan dekripsi serta pengelolaan kunci dilakukan dengan bantuan OpenSSL, yang memfasilitasi penerapan algoritma secara optimal. Aplikasi ini diharapkan mampu menyelesaikan berbagai permasalahan yang telah diidentifikasi, seperti hilangnya buku tabungan, kesalahan pencatatan manual, dan lemahnya sistem keamanan. Selain itu, aplikasi ini juga dirancang agar dapat memberikan akses mudah bagi petugas dan nasabah dalam melihat saldo dan riwayat transaksi secara real-time, sekaligus menjaga kerahasiaan data melalui mekanisme pengamanan yang kuat.

Secara keseluruhan, pengembangan aplikasi bank sampah berbasis kriptografi hybrid ini tidak hanya menjadi jawaban terhadap persoalan teknis dan administratif dalam pengelolaan sampah, tetapi juga menjadi model inovatif dalam pemberdayaan masyarakat berbasis teknologi. Implementasi sistem keamanan yang canggih menjadi faktor kunci untuk menjaga keberlangsungan dan kepercayaan masyarakat terhadap sistem, terlebih ketika transaksi mulai bersifat ekonomi dan investasi, seperti konversi saldo menjadi emas. Penelitian ini menjadi langkah awal dalam integrasi teknologi informasi dengan kebijakan lingkungan dan pemberdayaan ekonomi lokal. Ke depan, sistem ini dapat dikembangkan lebih lanjut dengan menambahkan fitur analitik data, integrasi dengan sistem keuangan digital, hingga kolaborasi

lintas sektor untuk mewujudkan ekosistem pengelolaan sampah yang berkelanjutan, transparan, dan berdaya saing tinggi di era digital.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan dua metode utama, yaitu wawancara dan tinjauan literatur. Metode wawancara dilakukan dengan narasumber dari Dinas Lingkungan Hidup Kota Padang, guna memperoleh data empiris mengenai proses transaksi di Bank Sampah Pancadaya. Proses wawancara dikemas dalam bentuk diskusi terarah untuk memahami alur kerja mulai dari penimbangan, pencatatan dalam buku tabungan, hingga tantangan yang dihadapi pengelola dalam operasional sehari-hari. Untuk memastikan relevansi informasi yang dikumpulkan, peneliti menyusun rubrik wawancara dengan beberapa aspek penting, seperti sistem pencatatan, kendala operasional, dan kesiapan terhadap penerapan aplikasi digital. Di sisi lain, metode tinjauan literatur digunakan untuk memperoleh landasan teori yang kuat, khususnya mengenai kriptografi hybrid. Literatur yang ditelaah mencakup jurnal ilmiah, artikel akademik, dan buku referensi terkait algoritma kriptografi seperti AES (Advanced Encryption Standard) dan RSA (Rivest–Shamir–Adleman).

3. METODE PENGEMBANGAN SISTEM

Pengembangan aplikasi bank sampah dalam penelitian ini menggunakan pendekatan Rapid Application Development (RAD).

A. Requirements Planning

Bank Sampah Pancadaya merupakan salah satu bank sampah yang ada di Kota Padang dan berperan sebagai Bank Sampah Induk (BSI) di wilayah tersebut. Namun, seluruh proses tersebut masih dilakukan secara manual, yang pada akhirnya menyebabkan sejumlah kendala dalam pengelolaan data dan kegiatan operasional. Adapun permasalahan yang berhasil diidentifikasi dalam kegiatan operasional Bank Sampah Pancadaya dapat dirangkum sebagai berikut:

Tabel 1. Identifikasi Analisis Masalah.

No.	Permasalahan
1	Proses pencatatan transaksi dan data nasabah masih dilakukan secara manual
2	Belum adanya sistem yang mengintegrasikan data bank sampah dengan data nasabah
3	Pendataan sampah yang masuk tidak selalu valid terhadap jumlah sampah yang disetor
4	Tidak adanya sistem monitoring dan pencatatan kegiatan secara real-time
5	Belum diterapkan sistem keamanan data digital

a. Identifikasi Sistem Berjalan

Pengelolaan data di Bank Sampah Pancadaya, meliputi data nasabah, transaksi, saldo, dan jenis sampah, masih dilakukan secara manual dengan pencatatan tertulis.

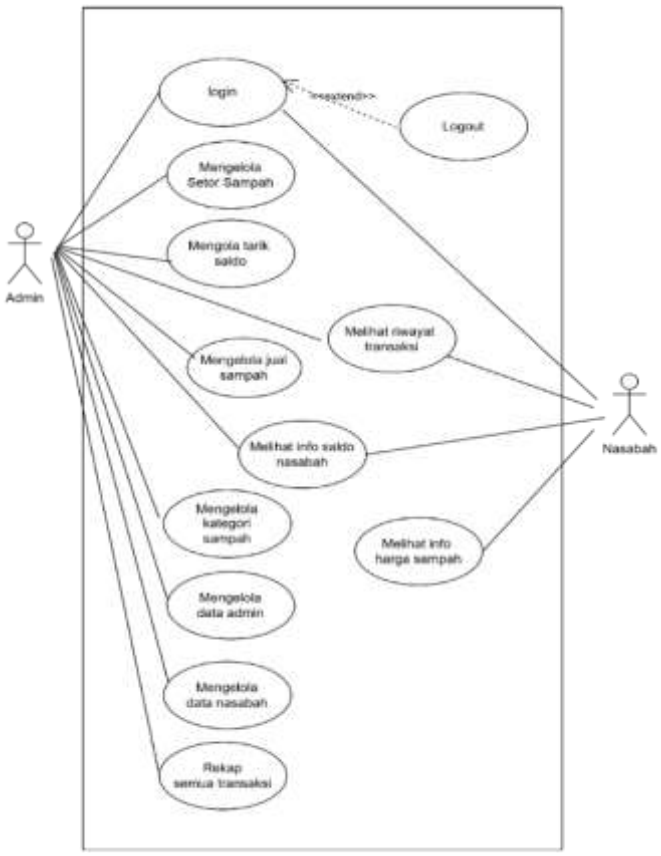
b. Identifikasi Sistem Usulan

Solusi yang diusulkan adalah membangun aplikasi Bank Sampah berbasis komputerisasi dengan fitur keamanan. Aplikasi ini memungkinkan nasabah mengecek saldo uang maupun emas secara real-time.

B. Desain Pengguna (User Design)

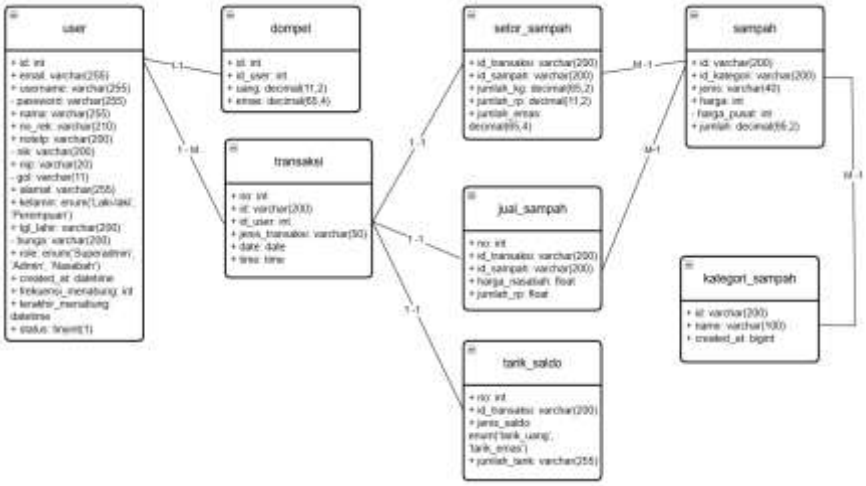
Pada tahap desain, dilakukan pembuatan model menggunakan UML yang berfungsi sebagai sarana untuk merancang sistem yang berorientasi objek. yang terdiri dari use case diagram, class diagram untuk menggambarkan alur proses dan struktur sistem. . Terdapat perancangan algoritma kriptografi *hybrid* yang akan digunakan untuk mengamankan data dalam sistem. Berikut adalah rancangan yang disusun pada tahap desain sistem:

a. Use case Diagram



Gambar 1. *Use case Diagram Bank Sampah.*

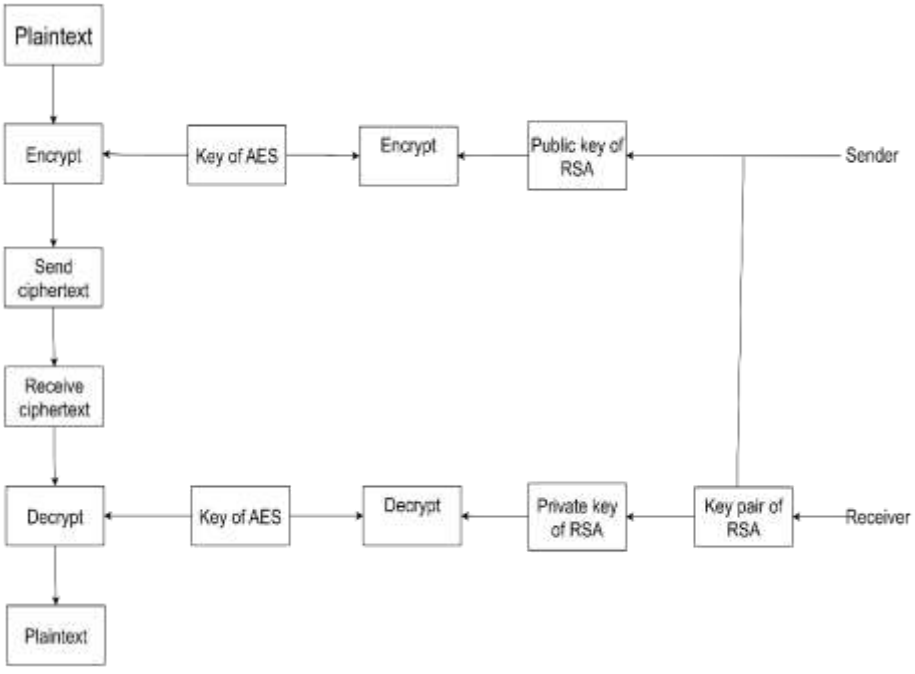
b. Class Diagram



Gambar 2. Class Diagram.

C. Desain Algortima Hybid Encrytion

Data transaksi dalam bentuk plaintext dienkripsi menggunakan AES sehingga menjadi ciphertext. Kunci AES tersebut kemudian dienkripsi lagi dengan RSA menggunakan public key pihak penerima. Ciphertext beserta kunci AES terenkripsi dikirim ke penerima. Penerima mendekripsi kunci AES menggunakan private key RSA, lalu menggunakan kunci tersebut untuk mendekripsi ciphertext kembali menjadi plaintext.



Gambar 3. Desain Algortima Hybid Encrytion.

D. Construction

Contruction merupakan tahap pada RAD dimana pengembang bekerja secara langsung dengan user, membuat rancangan akhir, membangun dan menguji prototype. Pada tahap ini penulis mulai membuat sistem yang sudah direncakanan dengan menyusun kode program atau coding, untuk merubah desain sistem yang telah dibuat menjadi sebuah aplikasi yang telah direncanakan agar dapat digunakan.

E. Cutover

Tahap ini merupakan proses pengujian menyeluruh terhadap sistem yang telah dikembangkan. Pengujian dilakukan untuk mengevaluasi kinerja aplikasi, khususnya dari sisi performa akses pengguna. Dalam penelitian ini, digunakan GTmetrix sebagai alat bantu untuk menguji kecepatan pemuatan halaman, serta memberikan analisis terhadap elemen-elemen yang mempengaruhi waktu muat aplikasi.

4. HASIL DAN PEMBAHASAN

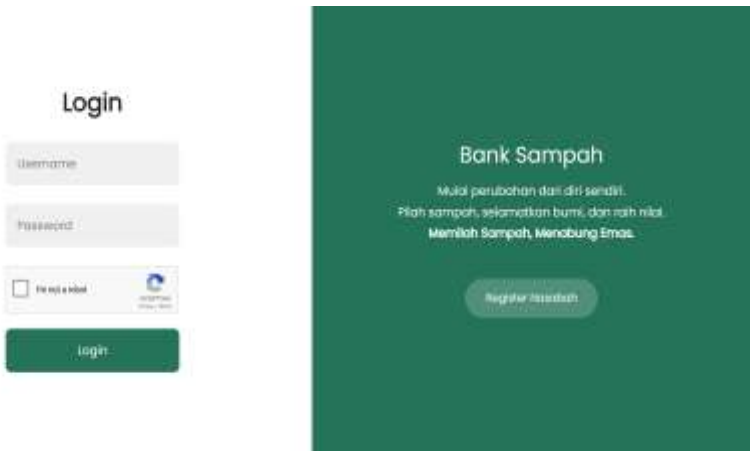
A. Hasil dan Pembahasan Rancangan Aplikasi Bank Sampah

Aplikasi bank sampah pancadaya berbasis web yang dirancang dalam penelitian ini diperuntukkan bagi dua jenis pengguna, yaitu admin dan nasabah.

Implementasi Fitur untuk Role Admin

a. *Login* Admin dan Nasabah

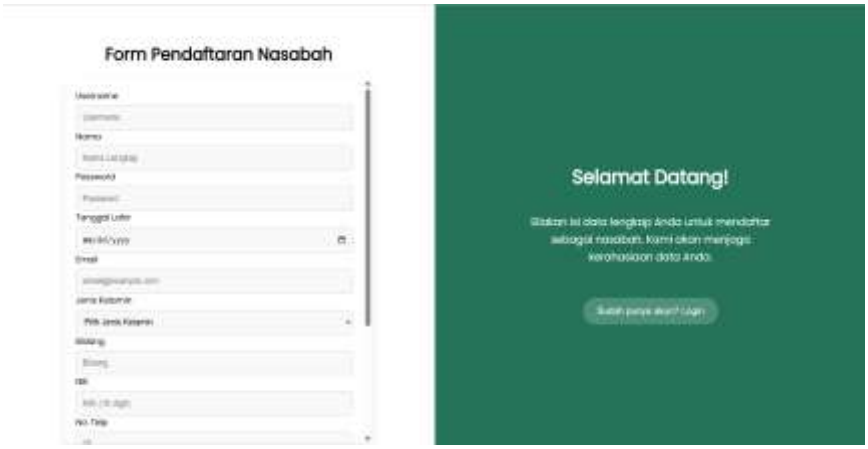
Halaman *login* ini untuk admin dan nasabah, dengan reCAPTCHA sebagai pengaman agar login hanya dilakukan oleh manusia dan terhindar dari bot atau spam.



Gambar 4. Tampilan Halaman *Login.*

b. Register nasabah

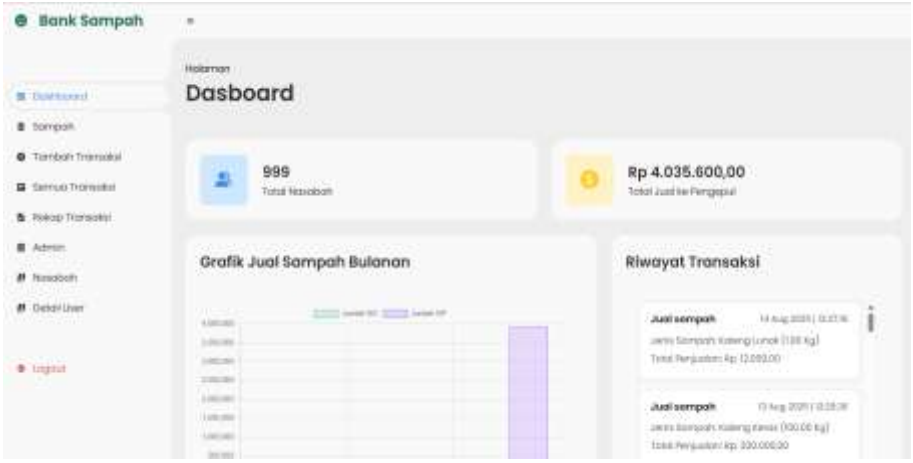
Pendaftaran nasabah dilakukan dengan mengisi *form* data diri secara lengkap. Setelah mendaftar, nasabah perlu menunggu verifikasi dari admin sebelum bisa *login*.



Gambar 5. Tampilan Halaman Register Nasabah.

c. *Dashboard* Admin

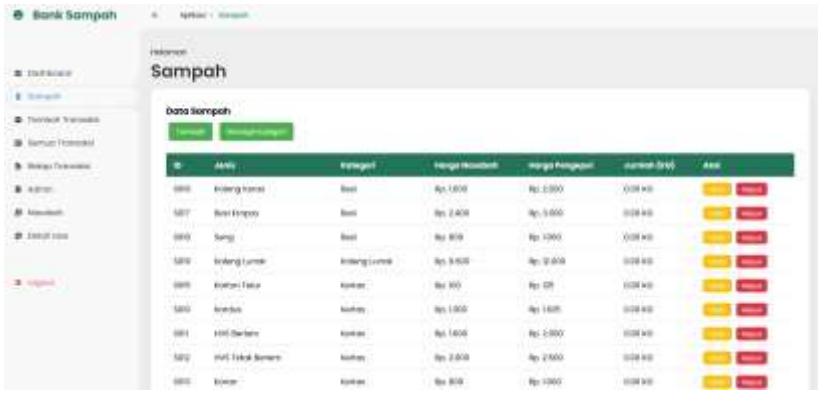
Setelah berhasil melakukan *login*, pengguna dengan *role* admin akan diarahkan ke halaman *dashboard* utama,



Gambar 6. Tampilan *Dashboard* Admin.

d. Data Sampah

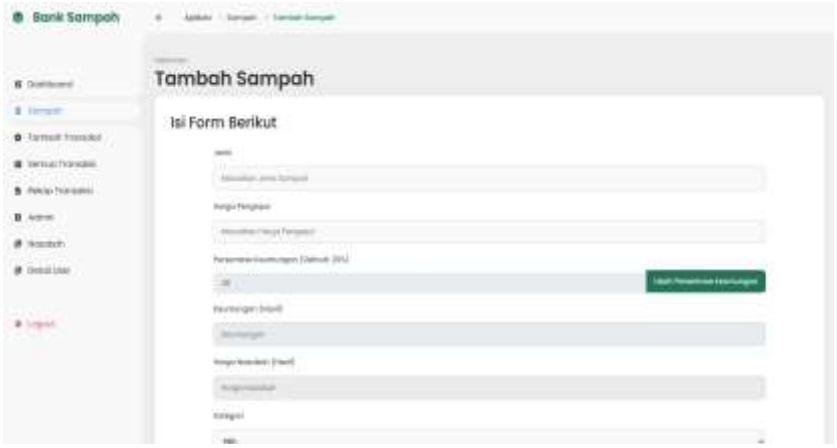
Halaman data sampah berisi informasi jenis sampah, kategori, harga untuk nasabah dan pengepul, serta jumlah dalam kilogram.



Gambar 7. Tampilan Halaman Data Sampah.

e. Tambah Sampah

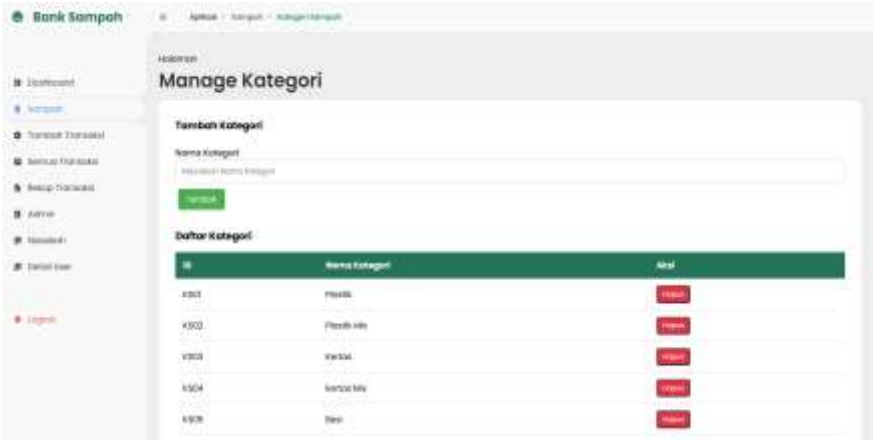
Selain menambah data sampah, admin juga bisa mengatur persentase keuntungan agar harga jual ke nasabah sesuai kebijakan.



Gambar 8. Tampilan Halaman Tambah Sampah.

f. Manage Kategori

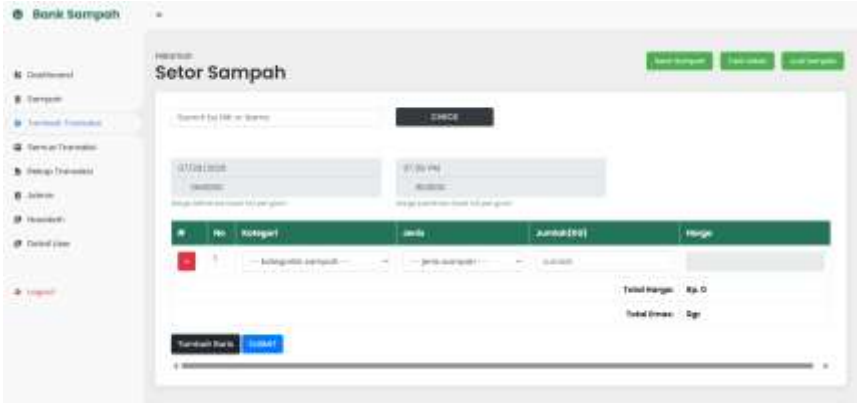
Admin dapat menambah, melihat, dan menghapus kategori sampah



Gambar 9. Tampilan Halaman Manage Kategori.

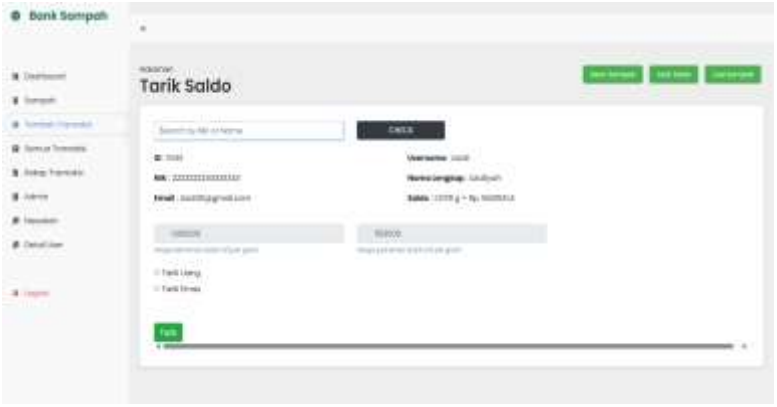
g. Tambah Transaksi

1) Setor Sampah, Halaman setor sampah digunakan untuk mencatat transaksi penyetoran sampah oleh nasabah.



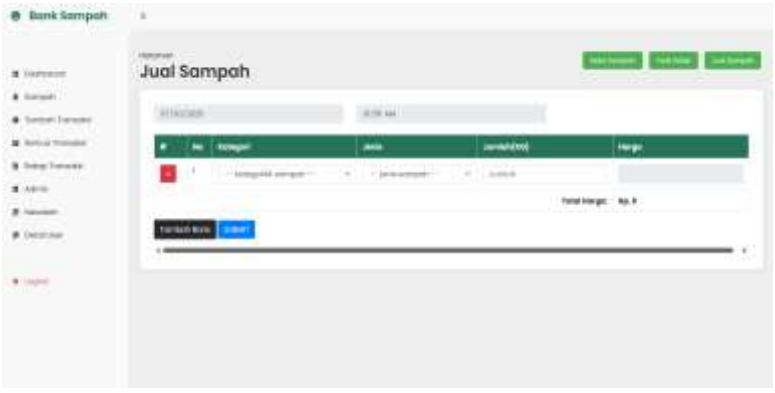
Gambar 10. Tampilan Halaman Setor Sampah.

2) Tarik Saldo, Nasabah yang ingin mencairkan saldo dibantu oleh admin.



Gambar 11. Tampilan Halaman Tarik Saldo.

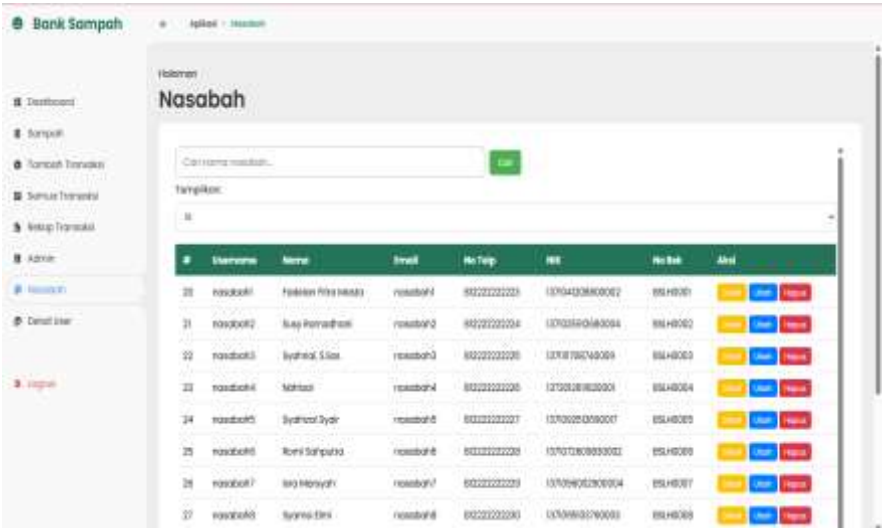
3) Jual Sampah, Pencatatan transaksi penjualan sampah ke pengepul dilakukan melalui halaman jual sampah,



Gambar 12. Tampilan Halaman Jual Sampah.

h. Kelola Nasabah

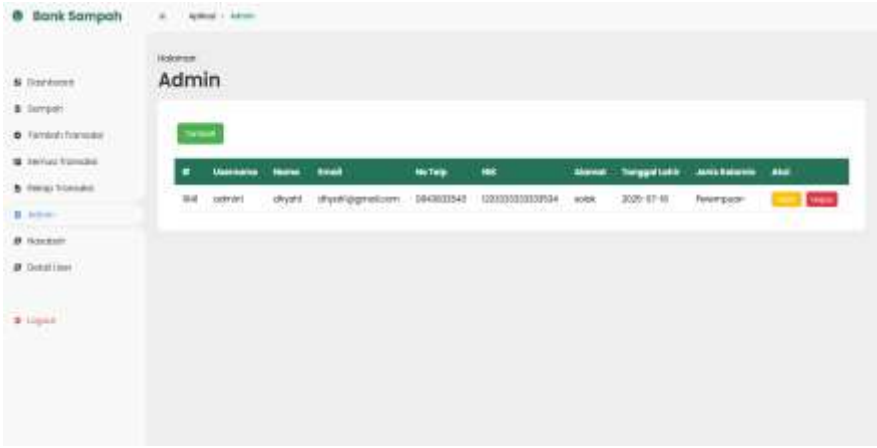
Seluruh data nasabah yang terdaftar akan ditampilkan pada halaman nasabah, dan admin memiliki akses untuk melakukan pencarian, pembaruan, maupun penghapusan data sesuai kebutuhan.



Gambar 13. Tampilan Halaman Nasabah.

i. Kelola Admin

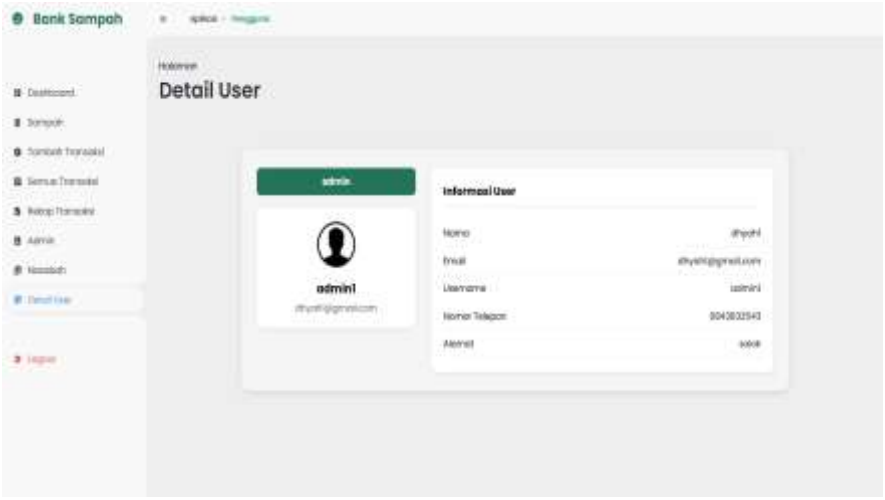
Pengelolaan akun administrator dilakukan pada halaman ini, termasuk fitur untuk menambah, mengedit, maupun menghapus data admin yang ada.



Gambar 14. Tampilan Halaman Admin.

j. Detail *User* Admin

Halaman detail *user* digunakan untuk mengetahui informasi lengkap mengenai *user* yang sedang *login* saat ini.



Gambar 15. Tampilan Halaman Detail *User* Admin.

k. Nota Transaksi

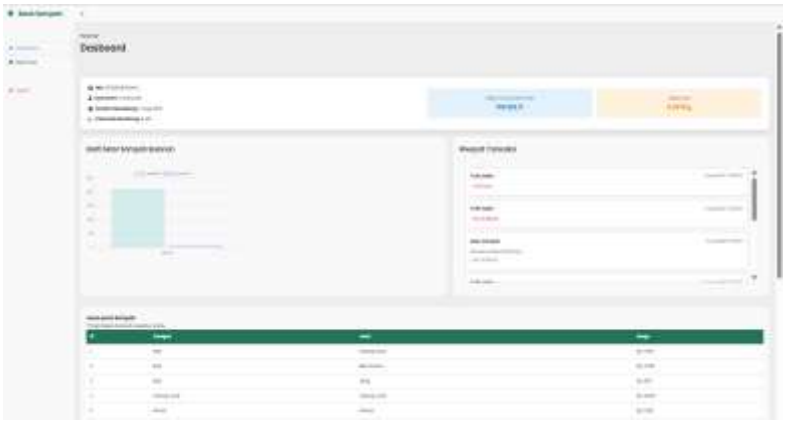
Pada aplikasi bank sampah, setiap transaksi setor sampah, tarik saldo, dan jual sa,pah akan menghasilkan nota yang memuat nomor transaksi, tanggal pelaksanaan, NIK penyetor, dan nama admin yang bertugas.

Gambar 16. Tampilan Halaman Nota Transaksi.

Implementasi Fitur untuk Role Nasabah

a. *Dashboard* Nasabah

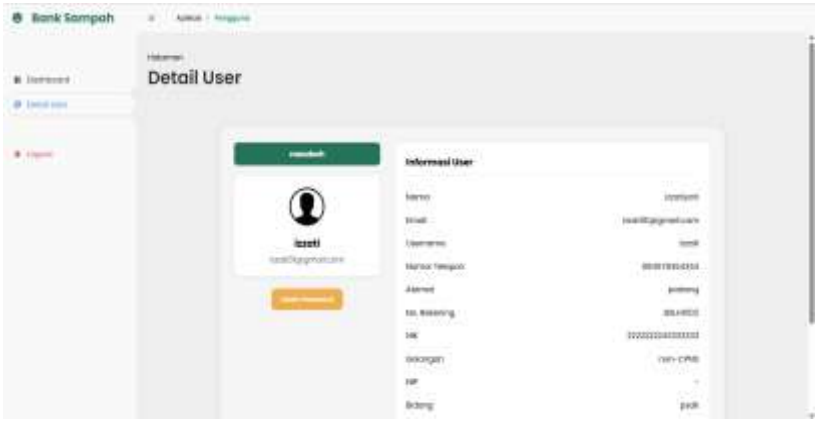
Setelah berhasil *login*, nasabah akan langsung diarahkan ke halaman *dashboard* utama yang menampilkan data profil, frekuensi menabung, grafik setor sampah



Gambar 17. Tampilan Halaman *Dashboard* Nasabah.

b. Detail *User* Nasabah

Melalui halaman detail *user*, nasabah dapat melihat informasi pribadi yang terdaftar di akun mereka secara ringkas.



Gambar 18. Tampilan Halaman Detail *User* Nasabah.

4. HASIL DAN PEMBAHASAN PROSES ALGORTIMA *HYBRID* AES DAN RSA

Pada tahap pembahasan ini, akan diuraikan proses implementasi sistem enkripsi dan dekripsi data menggunaka kriptografi hybrid RSA dan AES. Implementasi dilakukan menggunakan PHP dengan dukungan library OpenSSL,

A. Penggunaan Enkripsi pada Penyimpanan Data Transaksi Setor Sampah

Dalam proses penyimpanan data transaksi setor sampah, dilakukan enkripsi terhadap data sensitif seperti jumlah_rp dan jumlah_emas menggunakan algoritma AES.

Data harga dan emas_converted terlebih dahulu dikonversi ke bentuk *string*, kemudian dienkripsi dengan memanggil fungsi encryptWithAES() seperti pada potongan kode berikut

```
// Enkripsi data

$encrypted_harga = encryptWithAES((string)$harga);
$encrypted_emas  = encryptWithAES((string)$emas_converted);
```

Hasil enkripsi ini tidak lagi dalam bentuk asli, sehingga aman dari akses langsung di *database*. Data yang sudah terenkripsi kemudian disimpan ke dalam tabel setor_sampah melalui *query* SQL.

```
// Query insert ke tabel setor_sampah
$setor_sampah_query = "INSERT INTO setor_sampah (no, id_transaksi, id_sampah, jumlah_kg,
jumlah_rp, jumlah_emas)

VALUES(NULL,'$id_transaksi','$id_jenis','$jumlah',
'$encrypted_harga', '$encrypted_emas')";
```

Berikut adalah tampilan data terenkripsi yang tersimpan pada tabel setor_sampah.

	no	id_transaksi	id_sampah	jumlah_kg	jumlah_rp	jumlah_emas
Delete	82322	TRANS2025000442	S006	1000.00	EMFPTFOENMW+MqkwPAkwvOMxin2KDK5ShEwY/Tn8C6sm0tFB...	vYSE9jJ41UKGGa60IfVLOfWXp8ByEwiarBtr+y9xjHNyzNm49V...
Delete	82323	TRANS2025000445	S005	1000.00	uYCw4jhTSVPP8J0MIY9tKVozFqBK04pYeKAoNF2Egl4+jTvNRm...	IZNb7eqGlfdvmkuADZa7DqaLSOvK9dpwfNNnFAzoR64KwO2XK2T...
Delete	82324	TRANS2025000447	S005	54.00	6hvuNOQatnPOXgKDfKbewnrO3x7zq1P4X88C9U/kaqlj...	ZR5GgnzC/vtxrOXJW6eCqlv+E9gFoLJ6kzm+4BM9/ReTw==
Delete	82325	TRANS2025000450	S003	9000.00	XY79sJQYpp9B4uTiSFLKaoFF2541A6vf1Xbpzt222K3Fy+V8ovl...	03mqCO8RadOrBXOlHoZ24bFCVxFfcRpPWQkBWBK2Uvo86vgHAa...
Delete	82326	TRANS2025000460	S003	9000.00	oLQ3PWUgNFvlKwmZf880r9W1KpzdPa/N4olo8i6U71qobebygtl...	XlrZanke8D+FVTZjVjN1hfEpGsFCwRLs0nTzFsAX53a54YHvNPh...
Delete	82327	TRANS2025000470	S001	10.00	x53TTtgkn0LHJKu1cgbaaX1th1TurUaZCcd9kU9fMvO7rMlzr...	2fTgp57LnPVR6mdLwSAzyGKFNtE/szICFHXNumPq1TKM0z5...
Delete	82328	TRANS2025000470	S005	34.00	7r2qWZ6dpXwsaMknMqr1BjlXbZ9Ydav8osCy7U7ob6up1Zny...	TFHYpntoB3wCHpclcemZ2XOgiQpFwB/LaYIXjMOYsrSmU3M5...
Delete	82329	TRANS2025000472	S003	4.00	G1g4fVvMVEQKasTFzoHWV56g5C2ERGfdEwb6/emuYxZc0tGNn7...	jWOVer1zdlSm71XPQCVCGanzrEwfyNzN8vGcTNvZXAwXEC91C...
Delete	82330	TRANS2025000474	S019	100.00	eK14au8EmBHrQeQy4cRovOvjL3drv7OS+zxr4Oj2Dv2LEJEah...	uvQ9oXOgspEwspEDFnlAuBqbnP/gkJV3S6KAOgl11fv1/B19fy...
Delete	82331	TRANS2025000475	S019	200.00	owJXPyWjbAmaUQUaVNczG8FQmvN+4t5nVUmPOV+K0GdRlnxl7R...	YUTheV4VLLwQnjS2PKdc2GSBgEiTnMHRQrQpBmdUOmuDuw9CX...
Delete	82332	TRANS2025000477	S024	7.00	KQLzG7fXqKU+D8Z6mHJN+MoLc5aiAnXtw4WjFS3+HRHV+IAXT9...	SJmtEZOQJZMHQkKHq7uiGTB+jRpJMakfJ13pN3WOT7aw9YAfv...

Gambar 19. Data Terenkripsi yang Tersimpan pada Tabel Setor Sampah.

Terlihat bahwa nilai pada kolom jumlah_rp dan jumlah_emas tidak lagi dalam bentuk angka asli, melainkan dalam bentuk teks acak yang merupakan hasil enkripsi.

B. Penggunaan Enkripsi pada Penyimpanan Data Transaksi Tarik Saldo

Pada fitur transaksi tarik saldo, data jumlah penarikan juga dilindungi dengan enkripsi menggunakan algoritma AES. Nilai penarikan ($jumlah_tarik) ditentukan berdasarkan jenis penarikan yang dipilih oleh nasabah, apakah dalam bentuk uang tunai atau dalam bentuk emas. Setelah nilai diperoleh, data tersebut langsung dikonversi ke bentuk *string* dan dienkripsi dengan fungsi encryptWithAES() seperti berikut.

```
$jumlah_tarik=($withdraw_type==='money')? $_POST['jumlah_uang'] : $_POST['jumlah_emas'];

$jumlah_tarik_encrypted=encryptWithAES((string)$
jumlah_tarik);
```

Berikut adalah tampilan data terenkripsi yang tersimpan pada tabel tarik_sado.

	no	id_transaksi	jenis_saldo	jumlah_tarik
Edit Copy Delete	107	TRANS2025000438	tarik_uang	l7GBDK4zGY1G7ThWPqhFHZbhZbQP3pcEg9nULJaXSmDb1A/b+
Edit Copy Delete	108	TRANS2025000439	tarik_uang	uOAtl+X5yhEs0zU2F+ehVR2k1l67f3l3PUa4xPPyoQ2Eg5LavO
Edit Copy Delete	109	TRANS2025000440	tarik_uang	O7BbISxqRh0n0D1QEGF8Z4DOlMrHagQSAOP3VBNRx4hw5P0Y
Edit Copy Delete	110	TRANS2025000441	tarik_emas	DZB+KlKpcdS4zyK0wtZSqS32x1FIPeGsmn09PqDDLUK0kSyVU
Edit Copy Delete	111	TRANS2025000443	tarik_emas	ieg0h5My4H7x/e+rDUkPcINXW75+dBy5WHECOAj8w6hTfRvu
Edit Copy Delete	112	TRANS2025000444	tarik_emas	+NtlK9PwOVbL9DdARW8f21CdcrG5oulmWCQzLB3UZiTK00NJUq
Edit Copy Delete	113	TRANS2025000446	tarik_uang	94MT77KfdfJeNEUyuPz4CuxH6QtmgfZd6aKYlAsS2YfPRrH332f
Edit Copy Delete	114	TRANS2025000448	tarik_uang	0ATq/AnTqtuLXttagADwwxMyPpev0BiV6Q9hkhfmXjEIqLsZZo
Edit Copy Delete	115	TRANS2025000449	tarik_uang	Bb44GQ8/Y+lr6Bu9vZU3XkXTa/115sWw2zYioQrH0XggRZG/sE

Gambar 20. Data Terenkripsi yang Tersimpan pada Tabel Tarik Saldo.

Terlihat bahwa nilai bahwa data pada kolom jumlah_tarik tidak lagi tersimpan dalam bentuk angka asli, melainkan dalam format string acak hasil enkripsi AES.

C. Penggunaan Dekripsi pada Penyimpanan Nota Transakasi

Pada pembuatan nota transaksi, data yang sebelumnya terenkripsi dengan AES didekripsi kembali. Untuk transaksi setor sampah, data diambil dari tabel setor_sampah yang berelasi dengan tabel sampah dan kategori_sampah. Nilai pada kolom jumlah_rp dan jumlah_emas kemudian diproses dengan fungsi decryptWithAES() untuk mengembalikan data ke bentuk aslinya.

```
 if ($transaksi['jenis_transaksi'] == 'setor_sampah') {

    $items_query = "SELECT s.jenis as barang_name, ks.name
                as kategori_name,ss.jumlah_kg,
                ss.jumlah_rp, ss.jumlah_emas

FROM setor_sampah ss
JOIN sampah s ON ss.id_sampah = s.id
        JOIN kategori_sampah ks ON s.id_kategori = ks.id
        WHERE ss.id_transaksi = ?";

  if ($items_stmt = $koneksi->prepare($items_query)) {

   $items_stmt->bind_param("s", $id_transaksi);
   $items_stmt->execute();
   $items_result = $items_stmt->get_result();

   $items = [];
    while ($item = $items_result->fetch_assoc()) {
      try {
        $item['jumlah_rp']     decryptWithAES($item['jumlah_rp']);
              $item['jumlah_emas']= decryptWithAES($item['jumlah_emas']);
```

Sementara itu, untuk transaksi tarik saldo, data jumlah_tarik juga disimpan dalam bentuk terenkripsi dan didekripsi saat ingin ditampilkan.

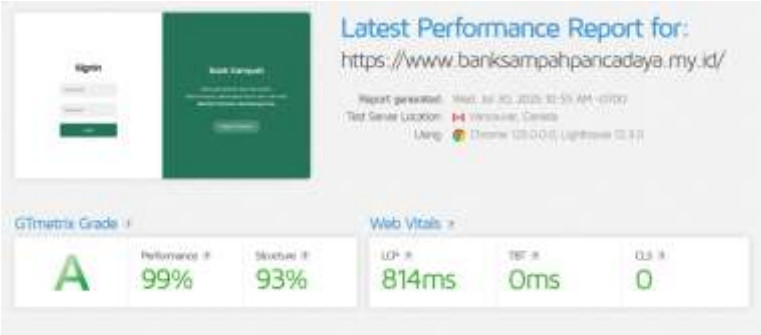
```
elseif ($transaksi['jenis_transaksi'] == 'tarik_saldo') {

$tarik_saldo_query= "SELECT ps.jenis_saldo, ps.jumlah_tarik

                FROM tarik_saldo ps
                WHERE ps.id_transaksi = ?";

 if ($tarik_stmt = $koneksi->prepare($tarik_saldo_query)) {

    $tarik_stmt->bind_param("s", $id_transaksi);
    $tarik_stmt->execute();

    $tarik_result = $tarik_stmt->get_result();
    $tarik_saldo = $tarik_result->fetch_assoc();

    if ($tarik_saldo) {
      try {
              $tarik_saldo['jumlah_tarik']=   decryptWithAES($tarik_saldo['jumlah_tarik']);

      } catch (Exception $e) {
        $tarik_saldo['jumlah_tarik'] = 'gagal dekripsi';
```

Hasil dekripsi ini kemudian digunakan untuk menyusun tampilan nota transaksi, seperti pada bagian berikut yang menampilkan detail kategori, jenis sampah, dan nominal rupiah hasil dekripsi.

```
<?php if (!empty($items)): ?>

 <?php foreach ($items as $item): ?>

  <tr>
   <td><?php echo htmlspecialchars
   ($item['kategori_name']); ?></td>

   <td><?php echo htmlspecialchars
   ($item['barang_name']); ?></td>

   <td><?php echo htmlspecialchars
   ($item['jumlah_kg']); ?></td>
   <td>
      <?php
      $jumlahRp = $item['jumlah_rp'];

      if (isEncryptedAES($jumlahRp)) {
         $jumlahRp = decryptWithAES($jumlahRp);
      }
      echo 'Rp ' . number_format
      ((float)$jumlahRp, 0,   ',', '.');
      ?>
   </td>
  </tr>
  <?php endforeach; ?>

<?php else: ?>
```

Pengujian Sistem

Pengujian menggunakan GTmetrix pada Aplikasi Bank Sampah Pancadaya bertujuan untuk menganalisis dan mengoptimalkan kinerja situs web atau aplikasi berbasis web. GTmetrix mengevaluasi berbagai aspek, seperti kecepatan pemuatan halaman (Loading Speed), struktur halaman, dan metrik Web Vitals.



Gambar 21. Pengujian menggunakan GTmetrix.

Gambar di atas menampilkan hasil pengujian performa situs web https://www.banksampahpancadaya.my.id/. Berikut adalah tabel hasil pengujian menggunakan GTmetrix yang berisi nomor, aspek yang diuji, skor, dan penjelasan singkat.

Tabel 2. Hasil pengujian menggunakan GTmetrix.

No.	Aspek	Skor	Penjelasan
1	Performance	99%	Menunjukkan tingkat efisiensi pemuatan halaman secara keseluruhan.
2	Structure	93%	Menggambarkan seberapa baik struktur HTML, CSS, dan JavaScript disusun.
3	LCP (Largest Contentful Paint)	814 ms	Waktu yang dibutuhkan untuk menampilkan elemen terbesar di layar.
4	TBT (Total Blocking Time)	0 ms	Tidak ada jeda pemrosesan yang menghambat interaksi pengguna.
5	CLS (Cumulative Layout Shift)	0	Tidak ada pergeseran tata letak yang mengganggu pengalaman pengguna.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil dan pembahasan untuk menjawab rumusan masalah dalam penelitian ini, dapat disimpulkan bahwa implementasi kriptografi hybrid berhasil diterapkan dalam Aplikasi Bank Sampah Pancadaya dengan menggabungkan algoritma AES untuk mengenkripsi data transaksi nasabah dan RSA untuk mengenkripsi kunci AES, sehingga meningkatkan lapisan keamanan data. Selain itu, Aplikasi Bank Pancadaya berbasis web juga mampu memberikan alternatif yang efektif dalam pengelolaan data bank sampah, karena adanya integritas data yang terjaga antara bank sampah dengan nasabah.

DAFTAR PUSTAKA

Arywa, V. U. (2025). Sistem distribusi e-book berbasis kriptografi asimetris menggunakan algoritma RSA untuk perlindungan hak cipta.

Fadillah, S. N. (2021). Implementasi algoritma kriptografi Hill Cipher dengan kunci terenkripsi Rivest Shamir Adleman (RSA) untuk meningkatkan keamanan citra digital.

Hardiyantik, N. (2023). Implementasi algoritma Blum-Blum Shub pada algoritma One Time Pad (OTP) cipher dalam pengamanan pesan [Skripsi, Universitas Islam Negeri Maulana Malik Ibrahim Malang].

Hidayat, M., Tahir, M., Sukriyadi, A., & Sulton, A. (2023). Penerapan kriptografi Caesar Cipher dalam pengamanan data. Jurnal Ilmiah Multidisiplin, 2(03), 35–41. https://doi.org/10.56127/jukim.v2i03.619

Hidayat, N., & Hati, K. (2021). Penerapan metode Rapid Application Development (RAD) dalam rancang bangun sistem informasi rapor online (SIRALINE). Jurnal Sistem Informasi, 10(1), 8–17. https://doi.org/10.51998/jsi.v10i1.352

Kementerian Lingkungan Hidup dan Kehutanan. (2024). Timbulan sampah Kota Padang tahun 2024. https://sipsn.kemenlh.go.id/sipsn/public/data/timbulan

Lu, Z., & Mohamed, H. (2021). A complex encryption system design implemented by AES. Journal of Information Security, 12(2), 177–187. https://doi.org/10.4236/jis.2021.122009

Munir, R. (2023a). Advanced Encryption Standard (AES). https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/08%20-%20AES-2023.pdf

Munir, R. (2023b). Kriptografi klasik (Bagian 1). Program Studi Teknik Informatika, STEI ITB.

Ningsih, K. S., Aruan, N. J., & Ikhsan, M. (2022). Aplikasi buku tamu menggunakan fitur kamera dan Ajax berbasis website pada Kantor Dispora Kota Medan. SITek (Jurnal Sains, Informasi dan Teknologi), 1(3), 94–95.

Nurmasari, N., Komalasari, E., Mulianto, B., Nurman, N., & Amrillah, M. F. (2024). Pelatihan inovasi bank sampah plastik untuk peningkatan pendapatan ekonomi masyarakat di Bank Sampah Puan Sari Mandiri. Jurnal ADAM: Jurnal Pengabdian Masyarakat, 3(1), 35–40. https://doi.org/10.36378/bhakti_nagori.v3i2.3394

Rahma Fitri, N., Surya Himawan, A., Syiendi Fadillah, A., Putri Dahayu, H., & Marwenny, E. (2024). Mengulas regulasi terkait mekanisme pengelolaan sampah melalui bank sampah di Kota Padang. Jurnal Kajian Hukum dan Kebijakan Publik, 2(1), 38–42. https://jurnal.kopusindo.com/index.php/jkhkp

Ramadhani, H. (2024). Kajian kinerja pengelolaan Bank Sampah Induk Panca Daya Kota Padang berdasarkan PermenLHK No. 14 Tahun 2021.

Rudianto, B., Achyani, Y. E., & Ariyati, I. (2021). Rancang bangun sistem informasi persediaan obat berbasis web menggunakan model RAD. Jurnal Khatulistiwa Informatika, 7(2), 214–221. https://doi.org/10.31294/jtk.v7i2.10571

Safitri, S. I. (2023). Algoritma hybrid menggunakan Myszkowski Cipher dan RSA untuk mengamankan pesan teks.

Setyawati, N. Y., Khofid, A. N., Rundi, A. U. B., & Wati, V. (2021). Modifikasi kriptografi klasik kombinasi metode Vigenere Cipher dan Caesar Cipher. Journal of Smart System, 1(1), 1–8. https://doi.org/10.36728/jss.v1i1.1601

Siagian, R. R. A.-A. (2025). Persepsi masyarakat Indonesia terhadap kenaikan harga emas sebagai instrumen investasi jangka panjang: Sebuah tinjauan literatur. Future Academia: The Journal of Multidisciplinary Research on Scientific and Advanced, 3(1), 72–79. https://doi.org/10.61579/future.v3i1.298

Widyawan, D., & Imelda, I. (2021). Pengamanan file menggunakan kriptografi dengan metode AES-128 berbasis web di Komite Nasional Keselamatan Transportasi. SKANIKA: Sistem Komputer dan Teknik Informatika, 4(1), 15–22. https://doi.org/10.36080/skanika.v4i1.2216

Wijaya, M. E. B. A., & Megawati, S. (2024). Implementasi kebijakan pengelolaan sampah pada Bank Sampah Induk Dhuawar Sejahtera di Dinas Lingkungan Hidup Kabupaten Kulon Progo. Publika, 991–997.