ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.5 No.1 Tahun 2026
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-5 2026
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2026

Penerapan Metode Waterfall dalam Perancangan Sistem Informasi Deteksi Kebocoran Data Berbasis Mobile

Implementation of the Waterfall Method in Designing a Mobile-Based Data Leakage Detection Information System

Silfa Salsa Bila Putri1, Eka Juliyana Rahayu[2], Hannifa Indah Rahayu[3]
[1,2,3]Teknik Informatika, Teknik, Universitas Pelita Bangsa
[1]silfasalsabilaputri@gmail.com, [2]eka610407@gmail.com *, [3]hannifaindah11311@gmail.com *

Abstract

The rapid growth of digital technology has increased the risk of personal data leakage among internet users in Indonesia. This research aims to design AMARTA, a mobile-based information system for detecting potential data leakage using email or phone number analysis. The system is developed to support digital trust and personal data protection by providing early detection and real-time notification to users. The Waterfall method is implemented to guide system development through structured stages such as requirement analysis, system design, implementation, testing, and maintenance. System requirements consist of functional aspects, such as user authentication, data scanning, notification features, and scan history, as well as non-functional aspects including security, performance, and usability. The system design phase utilizes UML modelling—use case, activity, sequence, class diagrams—along with ERD and UI prototypes to describe data flow, interaction logic, and interface structure. Results indicate that AMARTA provides an efficient workflow for data scanning using external API verification and delivers accurate results back to the users. The proposed model demonstrates that a structured development method can support secure information processing and ensure accuracy in data validation. This research contributes to the development of mobile security applications and public awareness toward data protection. Future work may focus on implementation, API expansion, and penetration testing to enhance accuracy and system reliability.

Keywords: *data leakage, information system, mobile security, Waterfall model, cybersecurity*

Abstrak

Perkembangan teknologi digital telah meningkatkan risiko kebocoran data pribadi pada pengguna internet di Indonesia. Penelitian ini bertujuan untuk merancang AMARTA, sebuah sistem informasi berbasis mobile yang berfungsi mendeteksi potensi kebocoran data melalui pemindaian email atau nomor handphone. Sistem ini dikembangkan untuk mendukung perlindungan data pribadi dengan memberikan deteksi dini serta notifikasi hasil pemindaian kepada pengguna. Metode Waterfall diterapkan sebagai dasar pengembangan sistem melalui tahapan analisis kebutuhan, perancangan, dan dokumentasi sistem. Kebutuhan sistem terdiri dari aspek fungsional seperti autentikasi pengguna, proses pemindaian, riwayat pemeriksaan, serta pengiriman notifikasi, serta aspek non-fungsional seperti keamanan, performa, dan kemudahan penggunaan. Tahap perancangan menggunakan pemodelan UML—use case, activity, sequence, class diagram—beserta ERD dan desain antarmuka untuk menggambarkan alur proses dan struktur sistem. Hasil penelitian menunjukkan bahwa desain AMARTA mampu menyediakan alur pemindaian data yang terstruktur melalui integrasi API eksternal sebagai sumber pemeriksaan kebocoran, dan hasilnya dapat disampaikan kembali kepada pengguna secara efektif. Penelitian ini berkontribusi pada pengembangan sistem keamanan data berbasis mobile serta peningkatan kesadaran masyarakat mengenai perlindungan data pribadi.

Kata kunci: kebocoran data, sistem informasi, mobile, Waterfall, keamanan data

Pendahuluan

Perkembangan teknologi digital telah membawa perubahan signifikan dalam cara masyarakat menyimpan, mengelola, dan bertukar informasi. Namun, kemajuan ini juga diikuti dengan meningkatnya ancaman terhadap keamanan data pribadi. Indonesia dalam beberapa tahun terakhir mencatat berbagai kasus kebocoran data besar, termasuk insiden yang melibatkan data pemilih nasional yang terekspos di ruang digital dan dijual secara ilegal, menunjukkan lemahnya mekanisme perlindungan data di berbagai sektor (Data Leakage of the Indonesian Elections Commission…, 2024). Kondisi ini semakin menegaskan bahwa keamanan data merupakan elemen fundamental dalam membangun kepercayaan digital atau digital trust.

Konsep *digital trust* merujuk pada persepsi pengguna mengenai keamanan, reliabilitas, dan transparansi sebuah sistem digital dalam mengelola informasi mereka[1]. Kepercayaan digital tidak hanya terbentuk melalui regulasi, tetapi juga melalui kesiapan teknologi dan kemampuan sistem dalam memberikan perlindungan data secara proaktif. Keamanan data adalah salah satu pilar utama pembentukan kepercayaan digital pada layanan berbasis teknologi. Dalam konteks ini, keberadaan sistem yang mampu mendeteksi potensi kebocoran data pribadi seperti email dan nomor telepon menjadi sangat penting untuk meningkatkan rasa aman masyarakat ketika berinteraksi secara digital[2].

Indonesia telah memiliki kerangka hukum melalui UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP), namun implementasinya masih menghadapi berbagai tantangan, terutama dari sisi kesiapan sistem dan rendahnya kesadaran masyarakat terhadap risiko kebocoran data pribadi [3][4]. Hal ini memperkuat urgensi pengembangan solusi teknologi yang dapat membantu individu untuk memantau dan memastikan keamanan informasi pribadinya secara mandiri. Perlindungan data pribadi merupakan prasyarat penting bagi pertumbuhan ekonomi digital Indonesia, karena tanpa adanya kepercayaan digital, partisipasi masyarakat dalam ekosistem digital akan melemah[5].

Salah satu pendekatan yang dapat digunakan untuk membangun sistem keamanan data adalah pengembangan perangkat lunak dengan metodologi *Waterfall*. Metode ini memberikan struktur yang jelas dan sistematis melalui tahapan analisis, perancangan, implementasi, hingga pengujian, sehingga cocok digunakan dalam proyek pengembangan sistem informasi yang membutuhkan dokumentasi kuat dan alur pengembangan terprediksi [6]. Pada sistem yang berhubungan dengan keamanan dan pemantauan data, metode Waterfall terbukti efektif dalam menghasilkan rancangan yang matang dan minim kesalahan implementasi [7].

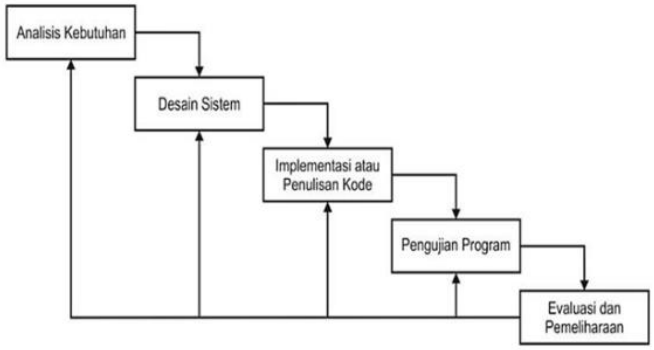
Berdasarkan permasalahan tersebut, penelitian ini mengembangkan **AMARTA**, sebuah sistem informasi berbasis web yang dirancang untuk mendeteksi indikasi kebocoran data pribadi pengguna seperti email dan nomor telepon. Sistem ini bertujuan untuk meningkatkan perlindungan data pengguna sekaligus memperkuat *digital trust* melalui notifikasi dini apabila ditemukan jejak kebocoran data di internet. Dengan mengombinasikan aspek teknologi deteksi kebocoran data dan metodologi pengembangan sistem yang terstruktur, AMARTA diharapkan mampu menjadi solusi inovatif dalam meningkatkan keamanan informasi pribadi masyarakat di era digital.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dan deskriptif yang dipadukan dengan metode penelitian dan pengembangan (R&D) berbasiskan model *Software Development Life Cycle* (SDLC) dengan model Waterfall dalam merancang dan membangun sistem informasi AMARTA. Metode ini dipilih karena sifatnya yang *linear* dan *terstruktur*, sehingga setiap tahapan pengembangan sistem dapat dijalankan secara sistematis dari awal hingga akhir tanpa melompati fase yang lain sangat cocok untuk proyek yang membutuhkan perencanaan dan dokumentasi yang matang seperti sistem keamanan dan deteksi kebocoran data.

Prosedur dan Tahapan Penelitian

Model waterfall adalah model yang paling banyak digunakan untuk tahap pengembangan. Model air terjun (waterfall) sering juga disebut model sekuensial linier (*sequential linear*) atau alur hidup klasik (*Classic cycle*). Model air terjun ini menyediakan pendekatan alur hidup perangkat lunak secara sequential terurut di mulai dari analisis, desain, implementasi, pengujian dan pemeliharaan[8].



Gambar 1 *Sytem Development Life Cycle* (SDLC) Waterfall

Analisis Kebutuhan

Pada tahap ini penulis melakukan pengumpulan data untuk memahami permasalahan yang ada dan merancang sistem yang dibutuhkan melalui wawancara terhadap seseorang yang ahli di bidang keamanan data, dan studi pustaka dari literatur terkait sistem informasi.

Desain Sistem

Setelah kebutuhan sistem teridentifikasi, maka dibutlah perancangan sistem informasi menggunakan Unified Modeling Language (UML). Dalam tahapan ini terdapat beberapa diagram yang digunakan meliputi: diagram use case, diagram activity, diagram class, sequence diagram, data model diagram, deployment diagram, dan user interface. Desain sistem ini memiliki tujuan yaitu memastikan alur kerja sistem, antarmuka, dan fungsionalitas sesuai dengan kebutuhan pengguna sebelus sistem dikembangkan.

Implementasi

Tahap ini, dilakukan dengan membangun sistem yang telah dirancang, semua fitur yang mendukung terhadap keamanan data, notifikasi *real time*, dan pemindaian kebocoran data dikembangkan agar dapat diakses dengan mudah melalui perangkat mobile.

Pengujian

Tahap pengujian dilakukan setelah sistem selesai, hal ini dilakukan agar diketahui sistem bisa berjalan dengan baik sesuai rancangan yang telah dibuat. Pengujian ini meliputi pengecekan fungsionalitas, validasi data, serta uji coba melalui berbagai perangkat. Tahapan ini sangan penting untuk menemukan potensi kesalahan dan memastikan bahwa sistem ini bisa digunakan secara efisien.

Pemeliharaan

Tahap terakhir yaitu pemeliharaan, tahap ini dilakukan untuk memastikan sistem tetap berfungsi secara optimal setelah digunakan. Dari tahap ini lah perbaikan dan penyempurnaan dapat dilakukan jika ditemukan masalah atau diperlukan penyesuaian tambahan. Pemeliharaan bertujuan menjaga sistem tetap relevan, akurat, dan dapat diandalkan dalam jangka Panjang[9].

Hasil dan Pembahasan

Analisis Kebutuhan Sistem

Analisis sistem AMARTA dilakukan untuk mengidentifikasi pengguna dan memetakan masalah kebocoran data, sehingga diperoleh kebutuhan fungsional dan non-fungsional yang menjadi dasar penyusunan spesifikasi sistem sesuai tahapan Waterfall.

Identifikasi Pengguna

Berdasarkan ide project, tujuan pengembangan, serta permasalahan kebocoran data yang telah diuraikan sebelumnya, identifikasi pengguna utama sistem Amarta dilakukan dengan mempertimbangkan potensi pengembangan aplikasi ke tahap lanjutan.

Masyarakat umum pengguna internet (end-user)

Mereka merupakan target utama yang membutuhkan perlindungan data pribadi dari kebocoran, terutama pengguna aktif media sosial, e-commerce, layanan publik digital, maupun platform online lainnya. Golongan ini membutuhkan solusi praktis dan real-time untuk mendeteksi kebocoran data secara langsung.

Kelompok non-teknis dan pengguna awam

Aplikasi Amarta dirancang dengan antarmuka yang sederhana dan edukatif, sehingga cocok untuk individu yang tidak memiliki latar belakang teknis namun ingin mengamankan data pribadinya secara mandiri. Ini mencakup ibu rumah tangga, pelajar, pegawai non-IT, dan lansia yang mulai aktif secara digital.

Pelaku UMKM dan Karyawan sector informal

Banyak pelaku UMKM menggunakan email dan nomor pribadi dalam operasional bisnis mereka. Mereka termasuk golongan yang sangat rentan terhadap penyalahgunaan data, namun belum memiliki sistem keamanan siber. Amarta dapat membantu mereka melakukan perlindungan awal secara mandiri.

Lembaga dan Komunitas digital (sebagai mitra edukasi dan distribusi)

Pihak seperti Komdigi dan komunitas literasi digital dapat menjadi pengguna sistem secara tidak langsung, yaitu melalui kerja sama kampanye kesadaran atau pelatihan penggunaan Amarta kepada masyarakat luas.

Pemerintah dan Lembaga keamanan siber (pengguna institusional)

Lembaga seperti Badan Siber dan Sandi Negara (BSSN) dapat menggunakan amarta sebagai mitra edukasi dan validasi keamanan aplikasi. Dalam skenario pengembangan lebih lanjut, mereka juga dapat terlibat dalam pengawasan, kolaborasi data, atau integrasi sistem keamanan nasional.

Pengguna layanan premium atau korporat

Dalam pengembangan ke versi berbayar (Premium), target pengguna dapat diperluas ke perusahaan kecil dan menengah (UKM), organisasi, atau pengguna individu yang membutuhkan fitur keamanan tambahan dan pelaporan lanjutan secara berkala.

Kebutuhan Fungsional

Kebutuhan fungsional menggambarkan fitur atau layanan utama yang harus tersedia dalam system agar pengguna dapat menjalankan aktivitas yang diharapkan. Berikut rincian kebutuhan fungsional sebagai berikut:

Tabel 1 tabel fungsional

No	Fitur	Dekripsi
1	Login/Register	Pengguna membuat/masuk akun dengan validasi aman
2	Input Data	Masukkan email/nomor HP untuk scan kebocoran
3	Pemindaian	Proses otomatis cocokkan dengan database bocor
4	Riwayat Scan	Tampilan hasil pemindaian sebelumnya
5	Notifikasi	Kirim alert real-time jika bocor terdeteksi
6	Logout	Keluar akun untuk keamanan

Kebutuhan Non-Fungsional

Kebuthan non-fungsional merupakan spesifikasi teknis dan kualitas system yang memengaruhi performa dan kenyamanan pengguna dalam menggunakan aplikasi. Berikut rinciannya:

Tabel 2 tabel non-fungsional

No	Aspek	Deskripsi
1	Kompatibillitas	Android 6.0+, iOS 12+
2	Koneksi	Internet stabil, alert jika offline
3	Ukuran	<10 MB, ringan untuk low-end device
4	UI/UX	Sederhana, intuitif, aksesibel semua usia
5	Respons	Scan <3 detik
6	Notifikasi	Real-time tanpa delay

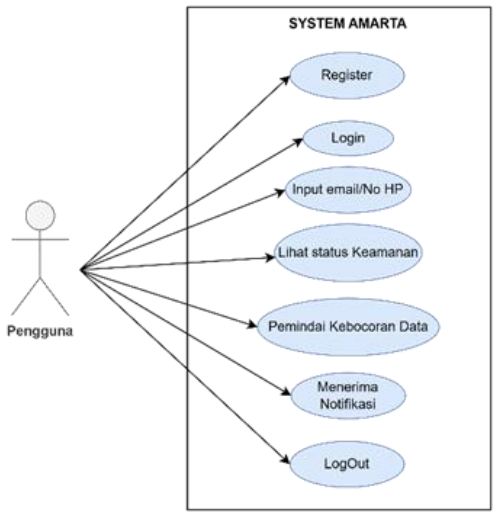
Perancangan Sistem

Tahap perancangan system bertujuan untuk menyusun gambaran menyeluruh mengenai bagaimana system informasi AMARTA akan bekerja dan memenuhi kebutuhan pengguna. Perancangan dilakukan untuk memastikan alur proses, struktur data, serta interaksi antar komponen system dapat dipahami dengan jelas sebelum memasuki tahap pengembangan. Pada penelitian ini digunakan beberapa jenis diagram Unified Modeling Language (UML), yaitu Use Case diagram, Activity Diagram, dan Sequence Diagram, Class Diagram. Selain UML, perancangan juga mencakup Entity Relationship Diagram (ERD) sebagai model basis data yang mendefinisikan struktur table, relasi antar data, serta penyimpanan hasil pemindaian pengguna. Dengan adanya keseluruhan model perancangan ini, system terbentuk melalui pendekatan terstruktur, konsisten, dan selaras dengan kebutuhan yang telah diidentifikasi pada tahap analisis[10].

Diagram UML & ERD

Use Case Diagram

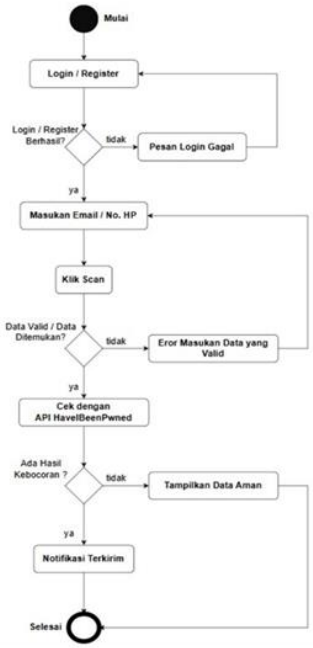
Use case diagram AMARTA menunjukkan interaksi utama antara pengguna dan sistem dalam proses pemindaian kebocoran data. Pengguna terlebih dahulu melakukan registrasi untuk membuat akun, kemudian masuk ke sistem melalui fitur login. Setelah berhasil login, pengguna dapat memasukkan email atau nomor handphone yang ingin diperiksa lalu menjalankan proses pemindaian. Sistem akan menampilkan status keamanan data berdasarkan hasil pemeriksaan dan mengirimkan notifikasi apabila ditemukan indikasi kebocoran. Selain itu, pengguna dapat melihat kembali status keamanan atau riwayat pemindaian sebelum keluar dari sistem melalui fitur logout.



Gambar 2 Use Case Diagram

Activity Diagram

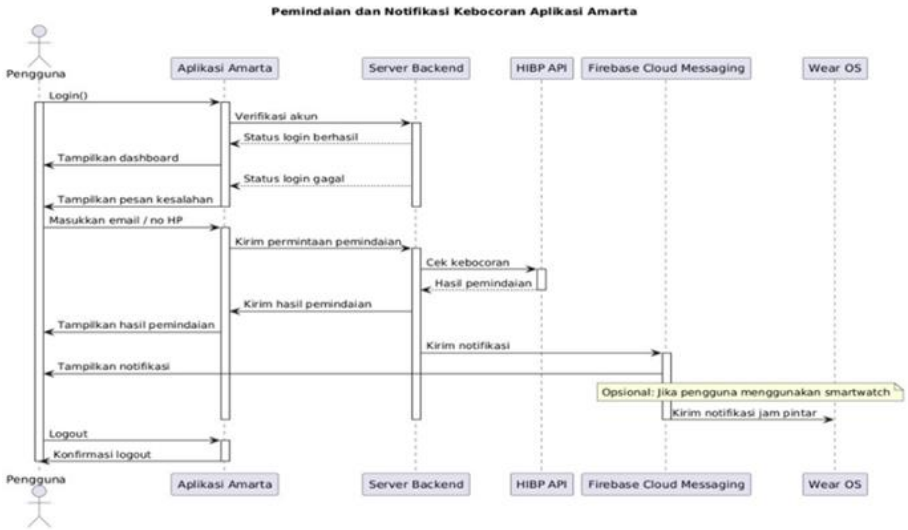
Activity Diagram pada sistem AMARTA menggambarkan alur proses utama yang dilakukan pengguna untuk memindai kebocoran data pribadi. Proses dimulai ketika pengguna membuat akun atau melakukan login ke dalam sistem. Jika proses login berhasil, pengguna dapat memasukkan email atau nomor handphone yang ingin dipindai, kemudian melanjutkan dengan menekan tombol scan. Sistem selanjutnya akan memeriksa kevalidan data yang dimasukkan. Jika data tidak valid, pengguna akan menerima pesan kesalahan dan diminta mengulang input. Namun apabila data valid, sistem akan melakukan pengecekan menggunakan API HaveIBeenPwned untuk mengetahui apakah terdapat indikasi kebocoran data. Jika hasil pemindaian menunjukkan bahwa tidak ada kebocoran, sistem menampilkan informasi bahwa data aman. Sebaliknya, jika terdapat kebocoran, pengguna akan menerima notifikasi hasil pemindaian. Rangkaian aktivitas ini dirancang agar proses deteksi dapat berjalan otomatis, cepat, dan memberikan hasil yang informatif kepada pengguna.



Gambar 3 Activity Diagram

Sequence Diagram

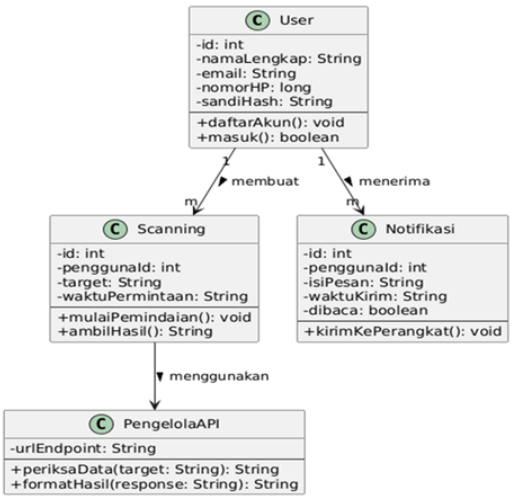
Sequence diagram menggambarkan proses Ketika pengguna melakukan pemindaian data. Alur dimulai dari pengguna yang login ke aplikasi lalu memasukkan email atau nomor HP untuk dipindai. Permintaan pemindaian dikirim ke server backend dan selanjutnya server melakukan pengecekan kebocoran melalui API HaveIBeenPwned. Hasil yang diterima dari API kemudian dikirim Kembali ke aplikasi untuk ditampilkan kepada pengguna, baik status aman maupun adanya kebocoran. Selain itu, server juga mengirimkan notifikasi hasil pemindaian melalui Firebase Cloud Messaging, dan secara opsional hasil notifikasi dapat diteruskan ke perangkat Wear OS apabila pengguna menggunakan smartwatch.



Gambar 4 Sequence Diagram

Class Diagram

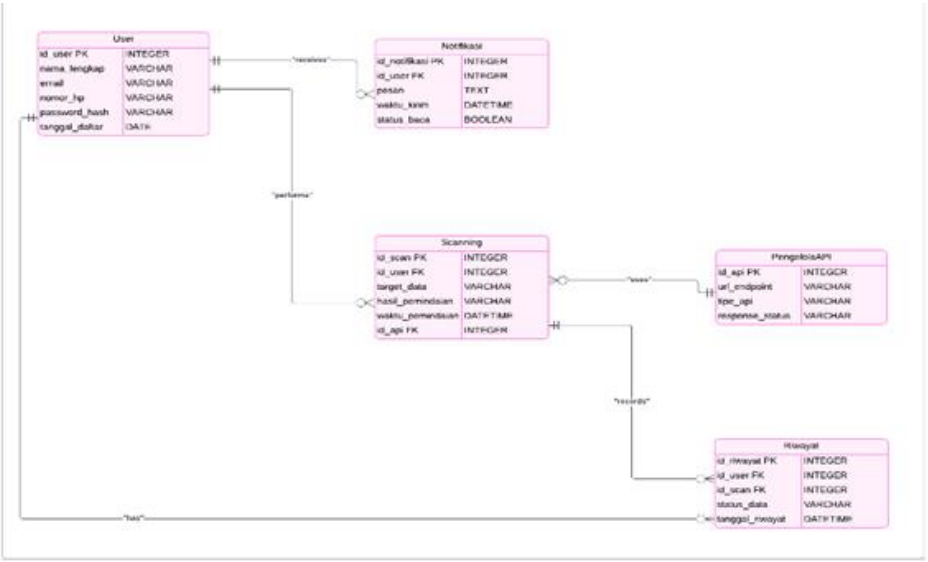
Class diagram menunjukkan empat kelas utama, yaitu User, Scanning, Notifikasi, dan Pengelolaan API. User melakukan proses pemindaian melalui kelas scanning, yang menyimpan data target pemindaian pengguna. Scanning kemudian menggunaka kelas PengelolaAPI untuk memeriksa data melalui endpoint API eksternal. Hasil pemidaian selanjutnya diteruskan ke kelas Notifikasi untuk dikirimkan Kembali kepada pengguna. Diagram ini menggambarkan alur objek yang saling terhubung dalam proses login, pemindain data, hingga pengiriman notifikasi kepada user.



Gambar 5 Class Diagram

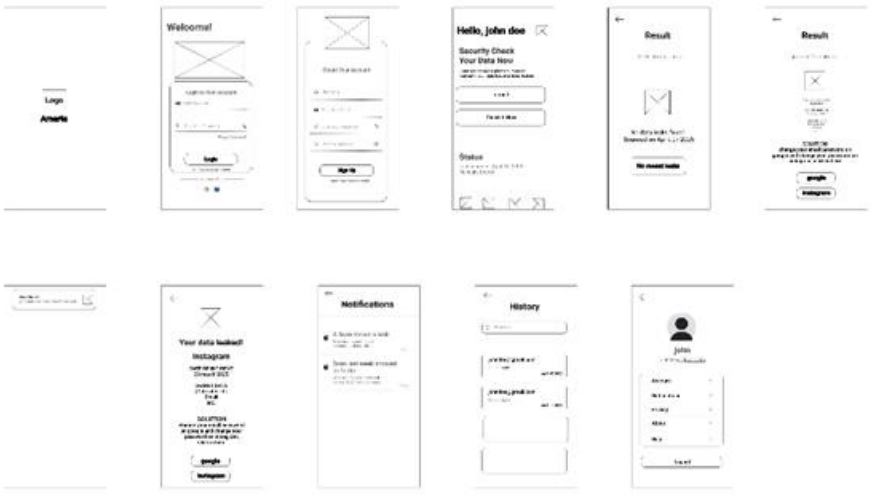
Entity Relationship Diagram (ERD)

ERD menggambarkan struktur basis data yang terdiri dari lima entitas utama, yaitu User, Scanning, Notifikasi, PengelolaAPI, dan Riwayat. Diagram ini menunjukkan alur penyimpanan dan hubungan data selama proses pemindain. Setiap pengguna disimpan dalam entitas User dan dapat melakukan banyak pemindaian yang tercatat pada entitas Scanning. Saat pemindaian dijalankan, sistem mengambil data target dan menghubungkannya dengan entitas PengelolaAPI untuk mengetahui sumber pemeriksaan yang digunakan. Hasil pemindaian kemudian dicatat sebagai riwayat pada entitas Riwayat agar pengguna dapat melihat histori pemeriksaannya. Di sisi lain, sistem juga menghasilkan pesan notifikasi kepada pengguna yang tersimpan pada entitas Notifikasi. Alur ini menunjukkan bahwa seluruh aktivitas pemindaian dan hasilnya dikelola secara terstruktur melalui relasi antar entitas database.



Gambar 6 ERD

Desain Antarmuka (UI/UX)



Gambar 7 Wireframe

Gambar 8 Desain UI AMARTA

Gambar 9 Desain UI AMARTA

Gambar 10 Desain UI AMARTA

Prinsip UX AMARTA

Aplikasi AMARTA dirancang dengan prinsip UX yang dengan memperhatikan navigasi intuitif dengan 2-3, ketukan untuk mengakses fitur utama, Hierarki visual yang jelas dengan elemen penting ditampilkan mencolok, Warna biru muda yang melambangkan keamanan dan kepercayaan, Aksesibilitas dengan tombol besar dan desain responsive.

Kesimpulan

Aplikasi Amarta hadir sebagai solusi inovatif terhadap meningkatnya kasus kebocoran data pribadi di era digital. Melalui fitur pemindaian email atau nomor HP dan notifikasi real-time, Amarta membantu pengguna mendeteksi potensi kebocoran data secara cepat dan mudah.

Proses pengembangan menggunakan metode Waterfall, dimulai dari tahap analisis, desain, implementasi, pengujian, hingga pemeliharaan. Setiap tahap dilakukan secara sistematis dan kolaboratif oleh anggota tim untuk mencapai hasil yang optimal.

Secara keseluruhan, Amarta berhasil menjadi langkah nyata dalam meningkatkan kesadaran masyarakat terhadap pentingnya perlindungan data pribadi, sekaligus memberikan alat praktis yang dapat digunakan untuk menjaga keamanan informasi digital secara *real-time*.

Ucapan Terima Kasih

Kami mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan dalam penyusunan penelitian ini. Selain itu, kami berterima kasih kepada rekan-rekan yang turut membantu dalam proses pengerjaan, diskusi, maupun penyempurnaan penelitian ini. Semoga penelitian ini dapat memberikan manfaat bagi berbagai pihak yang membutuhkan.

Daftar Rujukan

[1] J. Saveljeva and T. Volkova, "A Survey on Digital Trust: Towards a Validated Definition," Jun. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/digital5020014.

[2] S. Strazzullo, "Fostering digital trust in manufacturing companies: Exploring the impact of industry 4.0 technologies," *Journal of Innovation and Knowledge*, vol. 9, no. 4, Oct. 2024, doi: 10.1016/j.jik.2024.100621.

[3] M. R. Syailendra, "PERSONAL DATA PROTECTION LAW IN INDONESIA: CHALLENGES AND OPPORTUNITIES," *Indonesia Law Review*, vol. 14, no. 2, Aug. 2024, doi: 10.15742/ilrev.v14n2.4.

[4] S. Supeno, R. Rosmidah, and S. M. U. Iqbal, "Personal Data Protection in Review of Legal Theories and Principles," *Journal of Law and Legal Reform*, vol. 6, no. 3, pp. 1349–1376, Jul. 2025, doi: 10.15294/jllr.v6i3.10252.

[5] A. Wibowo, W. Alawiyah, and Azriadi, "The importance of personal data protection in Indonesia's economic development," *Cogent Soc Sci*, vol. 10, no. 1, 2024, doi: 10.1080/23311886.2024.2306751.

[6] R. Farta Wijaya and R. Budi Utomo, "KLIK: Kajian Ilmiah Informatika dan Komputer Metode Waterfall Dalam Rancang Bangun Sistem Informasi Manajemen Kegiatan Masjid Berbasis Web," *Media Online*, vol. 3, no. 5, pp. 563–571, 2023, [Online]. Available: https://djournals.com/klik

[7] O. Keamanan Dan Monitoring Jaringan Infrastruktur Di Kantor DPRD Bekasi Faris Jawad, R. Amanda Amalia, T. Sutan Nadzarudien, P. Sistem Informasi, and S. Tinggi Ilmu Komputer Cipta Karya Informatika, "Optimizing Security And Monitoring Infrastructure Networks At The Bekasi DPRD Office," 2023.

[8] M. Nunes Asqueli, A. Suryadi, R. Pratama Adhi, and D. Rahmat Saputra, "Perancangan Sistem Informasi Pemesanan Tiket Online Wisata Berbasis Website Dengan Metode Waterfall," 2025. [Online]. Available: https://journal.universitasichsansatya.ac.id/index.php/JRIKOM

[9] Hilmiatus Soleha, Firman Santoso, and Salam Bikwanto, "PERANCANGAN SISTEM INFORMASI PENGECEKAN ASET BERGERAK DI DINAS PEMADAM KEBAKARAN DAN PENYELAMATAN KABUPATEN BANYUWANGI," *Jurnal Riset Sistem Informasi*, vol. 2, no. 4, pp. 84–89, Sep. 2025, doi: 10.69714/xyphqk72.

[10] N. Mei *et al.*, "PERANCANGAN SISTEM INFORMASI PENGADUAN MASYARAKAT KEPADA DINAS SOSIAL BERBASIS WEB DENGAN METODE WATERFALL," vol. 6, no. 2, pp. 315–325, 2025.

[11] Amoo, H. B., & Omideyi, D. A. (2024). A web based mobile archival system using waterfall model approach. UNIZIK Journal of Engineering and Applied Sciences, 3(4), 1081–1101.

[12] A. Hidayat, E. Haryanto, D. Hartono, and A. Prasetyo, "Rancang Bangun Sistem Computer Security Incident Response Team (CSIRT)," Jurnal Teknik Informatika UNISI, vol. 10, no. 2, pp. 145–152, 2024.

[13] D. Santika, M. R. Aprilyawan, and F. Mahardika, "Desain Sistem Internet Of Things untuk Monitoring Kebocoran Gas Berbasis Website dengan Notifikasi Real-Time," *Simpatik: Jurnal Sistem Informasi dan Informatika*, vol. 5, no. 1, pp. 37–43, Jun. 2025.

[14] F. Y. Putri and Zulfariansyah, "Penerapan Metode Waterfall pada Sistem Informasi Kehadiran PT. Borneo Mobil Indo Samarinda," *Journal of Social Computer and Religiosity (SCORE)*, vol. 2, no. 1, pp. 51–61, 2024.

[15] A. Dillah, G. F. Nama, D. Budiyanto, and M. A. Muhammad, "RANCANG BANGUN APLIKASI MONITORING OPERASI P2TL PENGUKURAN TIDAK LANSGUNG 2 PHASA DI PT . PLN (PERSERO) UNIT PELAKSANA PELAYANAN PELANGGAN (UP3) METRO," vol. 12, no. 3, 2024.