

Perancangan Aplikasi Chatting Berbasis Android Dengan Penerapan Kriptografi Menggunakan Algoritma Caesar Cipher

Julyanto^a, Deny Jollyta^b

^a Institut Bisnis dan Teknologi Pelita Indonesia, Jl. Ahmad Yani No, 78-88, Pekanbaru, Riau, julyanto@student.pelitaindonesia.ac.id

^b Institut Bisnis dan Teknologi Pelita Indonesia, Jl. Ahmad Yani No, 78-88, Pekanbaru, Riau, deny.jollyta@lecturer.pelitaindonesia.ac.id

INFORMASI ARTIKEL

Sejarah Artikel:

Diterima Redaksi: 19 Oktober 2022

Revisi Akhir: 15 Desember 2022

Diterbitkan Online: 31 Desember 2022

KATA KUNCI

Chat application, Software Development Life Cycle (SDLC), Object Oriented, Black Box.

KORESPONDENSI

julyanto@student.pelitaindonesia.ac.id

ABSTRACT

CV. Motor Harapan merupakan perusahaan penjualan sparepart kendaraan yang dalam berkomunikasi antara karyawan dan atasan dalam mengirimkan pesan ataupun mengirimkan gambar masih menggunakan aplikasi Chatting yang berupa Whatsapp. Namun, terkadang karyawan maupun atasan bisa saja terjadi human error yang dimana adanya kemungkinan adanya laporan yang salah kirim. Sehingga solusi yang dapat diberikan adalah membuat aplikasi Chatting tersendiri dan membuat database tersendiri yang dimana aplikasi ini bisa dijalankan menggunakan android sehingga dapat digunakan semua karyawan. Untuk metode penelitiannya akan menggunakan metode *Software Development Life Cycle (SDLC)* yang dimana tahapan penelitiannya sendiri dimulai dari survey lapangan untuk mendapatkan informasi yang diperlukan, selanjutnya akan dilakukan proses mendesign aplikasi chatting yang akan dirancang, setelah itu akan dilakukan perancangan perangkat lunak yang dimana dalam perancangannya akan menggunakan aplikasi *Android Studio*, dan dalam pembuatan database akan menggunakan *MySQL*. Setelah selesai dirancang proses selanjutnya adalah uji coba untuk memastikan bahwa aplikasi yang dibuat bekerja sesuai dengan tujuan dalam. Dalam proses uji coba akan digunakan teknik black box untuk menguji fungsionalitas dari program yang sudah dirancang, sehingga program dapat dinyatakan valid untuk digunakan.

1. PENDAHULUAN

Pada masa sekarang, komunikasi merupakan salah satu kegiatan yang penting di kehidupan sehari-hari. Cara yang paling mudah salah satunya adalah melalui aplikasi chatting. Salah satu perusahaan yang menggunakan aplikasi chatting untuk kegiatan sehari-hari adalah CV. Motor Harapan. CV. Motor Harapan merupakan perusahaan yang menjual sparepart kendaraan yang beralamat di Jalan Harapan Raya No.18 di kota Pekanbaru.

CV. Motor Harapan menggunakan aplikasi chatting seperti WhatsApp sebagai sarana komunikasi antara karyawan dan atasan yang biasa digunakan ketika ingin memberikan laporan ataupun meminta izin. Tetapi aktivitas ini beresiko tersebarnya rahasia yang ada didalam perusahaan. Yang dimana bisa saja dengan tidak sengaja mengirimkan laporan perusahaan ke orang yang tidak ada kaitannya dengan perusahaan dan meskipun pesan dapat dihapus masih ada aplikasi ilegal yang bisa membaca pesan WhatsApp yang telah dihapus oleh pengirim sehingga rahasia perusahaan bisa saja terancam tersebar keluar lingkungan perusahaan.

Dari Masalah tersebut, dilakukan penelitian untuk merancang aplikasi chatting yang menggunakan kriptografi *Caesar Cipher* di dalam ruangan chatnya yang hanya akan digunakan dalam ruang lingkup perusahaan. Sehingga dapat mengurangi kemungkinan data perusahaan untuk bocor.

2. TINJAUAN PUSTAKA

2.1. Android

Menurut [1] Android merupakan sistem operasi yang dikembangkan untuk perangkat mobile berbasis Linux. Pada awalnya sistem operasi ini dikembangkan oleh Android Inc. yang kemudian dibeli oleh Google pada tahun 2005. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam peranti bergerak. Secara umum Android merupakan salah satu sistem operasi atau operating system berbasis mobile yang sangat banyak digunakan sekarang ini.

2.2. Caesar Cipher

Caesar Cipher merupakan salah satu algoritma cipher tertua dan paling diketahui dalam perkembangan ilmu kriptografi. Caesar cipher merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plaintext menjadi tepat satu karakter pada cipher teks.

Rumus algoritmanya adalah Enkripsi : $E(x) = (x + n) \bmod 26$ dan Dekripsi: $D(x) = (x - n) \bmod 26$. Dimana x merupakan huruf yang ingin di enkripsi atau dekripsi dan n merupakan nilai kunci yang telah ditetapkan sedangkan mod 26 itu didapat dari jumlah huruf abjad yang totalnya 26.

2.3. Aplikasi

Menurut [2], aplikasi merupakan program yang secara langsung dapat melakukan proses-proses yang digunakan dalam komputer oleh pengguna. Aplikasi merupakan kumpulan dari file-file tertentu yang berisi kode program yang menghubungkan antara pengguna dan perangkat keras komputer.

2.4. MySQL

Menurut [3] MySQL adalah sistem manajemen database SQL yang bersifat open source dan paling populer saat ini. Sistem database MySQL mendukung fitur seperti multithreaded, multi-user dan SQL Database Manajemen Sistem (DBMS). Database ini dibuat untuk keperluan sistem database yang cepat, handal dan mudah digunakan. MySQL adalah multiuser database yang menggunakan bahasa Structured Query Language (SQL).

2.5. Phpmyadmin

Menurut [4] Phpmyadmin adalah sebuah aplikasi open source yang berfungsi untuk memudahkan manajemen MySQL. Dengan menggunakan phpmyadmin, anda dapat membuat database, membuat tabel, menginsert, menghapus dan mengupdate data dengan GUI dan terasa lebih mudah, tanpa perlu mengetikkan perintah SQL secara manual

2.6. Database

Menurut [3] Database merupakan komponen terpenting dalam pembangunan SI, karena menjadi tempat untuk menampung dan mengorganisasikan seluruh data yang ada dalam sistem, sehingga dapat dieksplorasi untuk menyusun informasi-informasi dalam berbagai bentuk. Basis data merupakan himpunan kelompok data yang saling berkaitan. Basis data (database) adalah suatu susunan/kumpulan data operasional lengkap dari suatu organisasi atau perusahaan yang diorganisir atau dikelola dan disimpan secara terintegrasi dengan menggunakan metode tertentu menggunakan komputer sehingga mampu menyediakan informasi yang optimal yang diperlukan pemakainya

2.7. XAMPP

Menurut [5] Xampp merupakan singkatan dari X (empat sistem operasi apapun), XAMPP merupakan perangkat lunak bebas, yang mendukung banyak sistem operasi, dan merupakan kompilasi dari beberapa program. Seperti Apache, MYSQL, PHPP, dan Perl.

2.8. Bahasa Pemrograman Java

Menurut [1], Java adalah sebuah teknologi dimana pada teknologi tersebut mencakup java sebagai bahasa pemrograman yang memiliki sintaks dan aturan pemrograman tersendiri, juga mencakup java sebagai platform dimana teknologi ini memiliki virtual machine dan library yang diperlukan untuk menulis dan menjalankan program yang ditulis dengan bahasa pemrograman java, alasan terbesar dalam pembuatan bahasa pemrograman java adalah keinginan akan terbentuknya suatu bahasa pemrograman yang bisa berjalan di berbagai perangkat tanpa harus terikat oleh platform, sehingga java ini bersifat portable dan platform independent (tidak tergantung mesin atau sistem operasi).

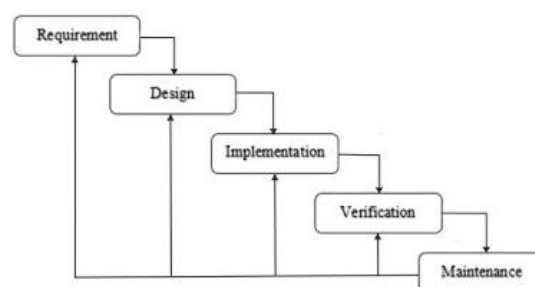
2.9. Firebase

Menurut [6], Firebase adalah API (Application Programming Interface) yang disediakan google untuk penyimpanan dan penyelarasan data kedalam aplikasi Android, iOS, atau web. Realtime database adalah salah

satu fasilitas yang menyimpan data ke database dan mengambil data darinya dengan sangat cepat tetapi firebase bukan hanya realtime database, jauh lebih dari itu Firebase memiliki banyak fitur seperti authentication, database, storage, hosting, pemberitahuan dan lain-lain.

3. METODOLOGI

Pada penelitian ini peneliti menggunakan metode waterfall System Development Life Cycle (SDLC) yang merupakan metode yang paling banyak digunakan untuk tahap pengembangan. Model waterfall ini juga memiliki beberapa tahapan, yaitu:



Gambar 1. Metode Waterfall

1. Requirements

Tahap ini pengembang sistem diperlukan komunikasi yang bertujuan untuk memahami perangkat lunak yang diharapkan oleh pengguna dan batasan perangkat lunak tersebut. Informasi dapat diperoleh melalui wawancara, diskusi atau survei langsung. Informasi dianalisis untuk mendapatkan data yang dibutuhkan oleh pengguna.

2. Design

Pada tahap ini, pengembang membuat desain sistem yang dapat membantu menentukan perangkat keras (hardware) dan sistem persyaratan dan juga membantu dalam mendefinisikan arsitektur sistem secara keseluruhan.

3. Implementation

Pada tahap ini, sistem pertama kali dikembangkan di program kecil yang disebut unit, yang terintegrasi dalam tahap selanjutnya. Setiap unit dikembangkan dan diuji untuk fungsionalitas yang disebut sebagai unit testing.

4. Verification

Pada tahap ini, sistem dilakukan verifikasi dan pengujian apakah sistem sepenuhnya atau sebagian memenuhi persyaratan sistem, pengujian dapat dikategorikan ke dalam unit testing (dilakukan pada modul tertentu kode), sistem pengujian (untuk melihat bagaimana sistem bereaksi ketika semua modul yang terintegrasi) dan penerimaan pengujian (dilakukan dengan atau nama pelanggan untuk melihat apakah semua kebutuhan pelanggan puas).

5. Maintenance

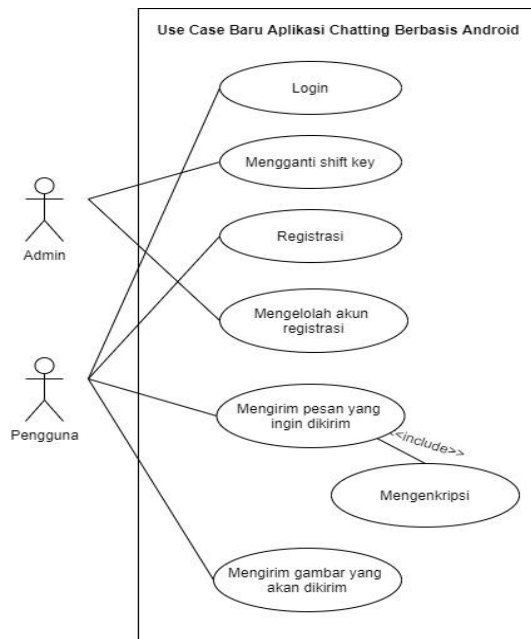
Ini adalah tahap akhir dari metode waterfall. Perangkat lunak yang sudah jadi dijalankan serta dilakukan pemeliharaan. Pemeliharaan termasuk dalam memperbaiki kesalahan yang tidak ditemukan pada langkah sebelumnya.

4. HASIL DAN PEMBAHASAN

4.1. Rancangan Sistem Informasi Baru

4.1.1. Use Case Diagram

Usecase diagram merupakan permodelan untuk menggambarkan kelakuan sistem yang akan dibangun. Diagram usecase mendeskripsikan sebuah interaksi antara satu atau lebih actor dengan sistem yang akan dibuat. Berikut use case diagram yang di gunakan pada sistem.

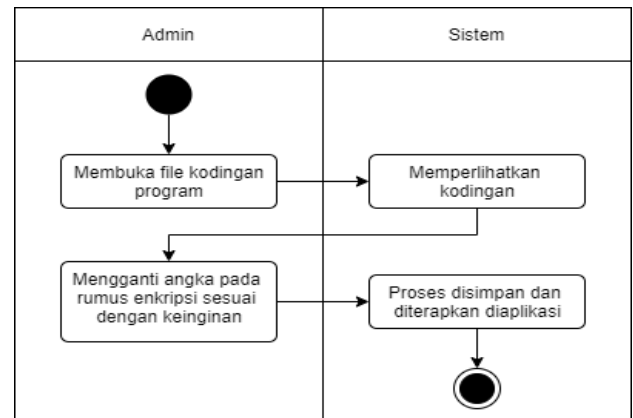


Gambar 2. Use Case Diagram Baru

Gambar 2 menjelaskan dalam system baru ini terdapat 2 aktor yang dimana terdiri dari admin yang berperan untuk mengganti kunci enkripsi disaat diinginkan oleh atasan. Admin juga berperan dalam mengelola akun pengguna dimana jika ada akun baru yang registrasi harus menerima konfirmasi dari admin terlebih dahulu dan jika ada akun yang akan dimatikan maka hanya admin yang bisa melakukannya. Selain itu didalam sistem terdapat juga aktor yang berperan sebagai user atau pengguna yang dimana dia bisa login kedalam aplikasi setelah memiliki akun jika belum memiliki akun maka user atau pengguna dapat mendaftarkan terlebih dahulu jika sudah memiliki akun maka user atau pengguna akan dapat mengirim pesan ataupun gambar yang dimana pesan yang akan dikirim akan dienkripsi oleh sistem secara otomatis sebelum dimunculkan kedalam ruang chat. Selain itu user atau pengguna juga bisa menerima pesan dari pengguna lain yang mengirim pesan ke kita dalam bentuk enkripsi jika ingin dibaca maka pesan bisa didekripsi melalui sistem setelah mengisi password login.

4.1.2. Activity Diagram

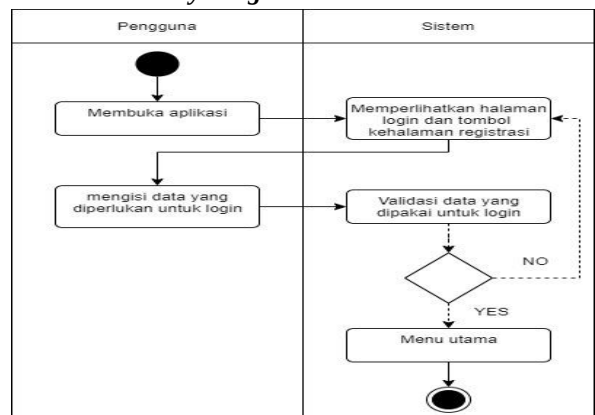
4.1.2.1 Activity Diagram Admin



Gambar 3. Activity Diagram Mengganti Key

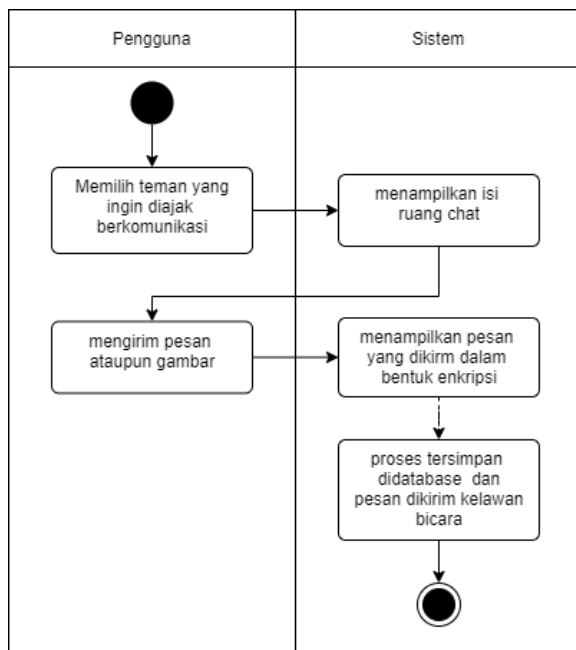
Gambar 3 menjelaskan ketika admin ingin mengubah pergeseran huruf yang akan dienkripsi. Admin harus melakukan Tindakan seperti membuka file kodingan dimana algoritma berada dan mengubah angka pergeseran enkripsi secara manual setelah itu file akan disimpan. Setelah itu sistem akan melakukan update yang dimana update akan menerapkan enkripsi baru dari perubahan kunci enkripsi yang barusan dilakukan oleh admin

4.1.1.1 Activity Diagram User



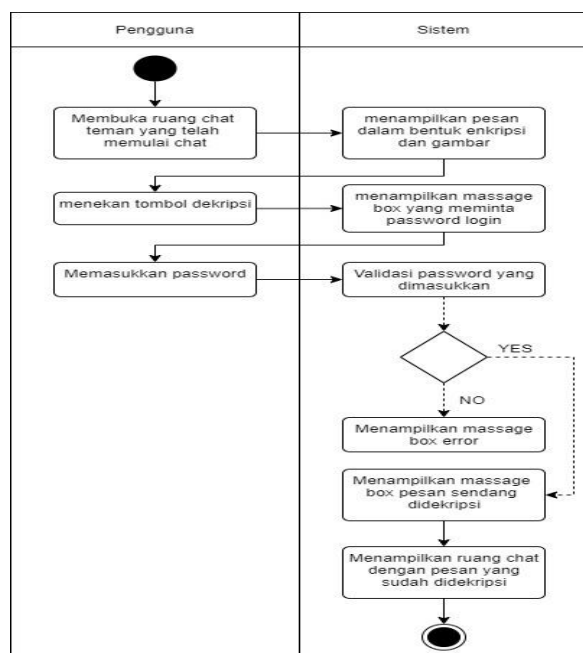
Gambar 4. Activity Diagram Login

Gambar 4 menjelaskan ketika pengguna sudah memiliki akun dan ingin login kedalam aplikasi maka pengguna harus membuka aplikasi dan sistem akan memperlihatkan halaman login yang dimana pengguna akan mengisi data yang diperlukan untuk login masuk kedalam aplikasi setelah itu data yang dimasukkan pengguna akan divalidasi sistem untuk dicek apakah data tersebut ada dan statusnya aktif jika datanya ada dan statusnya aktif pengguna akan sistem akan membawanya kemenu utama sedangkan jika data tersebut tidak ada atau statusnya belum aktif maka pengguna akan dibalikkan kembali kehalaman login.



Gambar 5. Activity Diagram Chatting

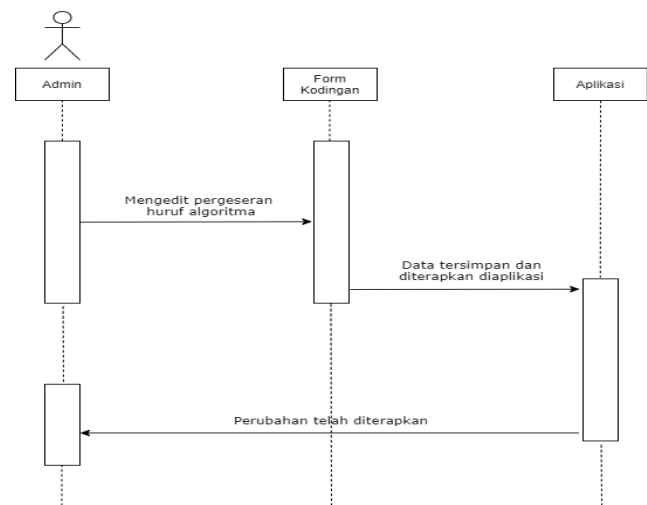
Gambar 5 menjelaskan ketika pengguna ingin mengirimkan pesan ke pengguna yang lainnya, pengguna bisa memilih ruang chat dari pengguna lain yang pernah diajak bicara atau memulai ruang chat baru dengan orang yang belum pernah diajak berbicara. Setelah memilih maka sistem akan membawa pengguna ke dalam ruang chat dan di dalam ruang chat pengguna bisa mengirim pesan yang nantinya akan ditampilkan dalam bentuk enkripsi ataupun mengirimkan gambar ke pengguna lainnya.



Gambar 6. Activity Diagram Dekripsi Chat

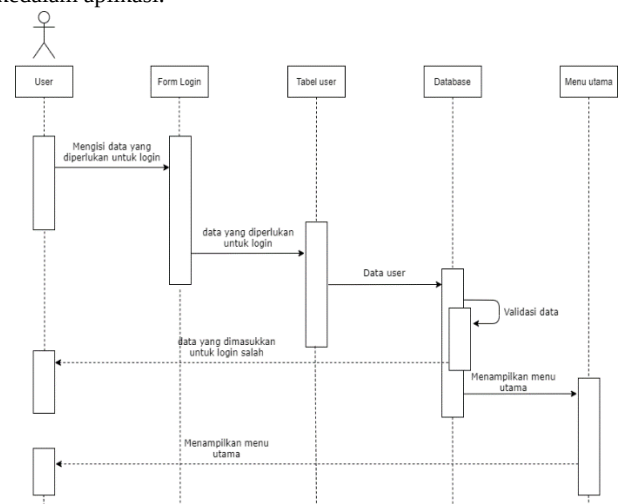
Gambar 6 menjelaskan ketika pengguna membuka ruang chat yang telah memiliki riwayat chat dengan kita maka sistem akan menampilkan isi ruang chat yang terdiri dari pesan yang sudah dienkripsi dan juga gambar jika ada. Untuk membaca pesan yang dienkripsi pengguna harus menekan tombol dekripsi yang tersedia di halaman ruang chat yang kemudian sistem akan menampilkan message box yang meminta password login. Ketika pengguna sudah memasukkan passwordnya maka sistem akan memvalidasi password. Jika password yang dimasukkan sesuai dengan yang ada di database maka sistem akan mendekripsi pesan yang ada di ruang chat secara otomatis oleh sistem.

4.1.2. Sequence Diagram



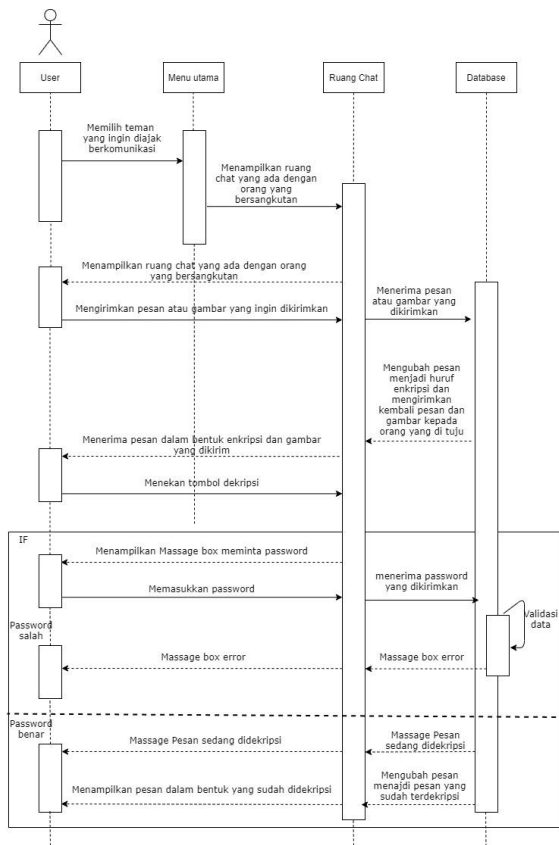
Gambar 7. Sequence Diagram Mengubah Key

Gambar 7 menjelaskan ketika admin ingin mengubah key atau kunci yang digunakan untuk pergeseran huruf pada enkripsi maka admin harus membuka kodingan aplikasi dan mengubah kunci sesuai dengan keinginan setelah itu maka file form kodingan akan disimpan dan secara otomatis akan langsung diterapkan ke dalam aplikasi sehingga aplikasi akan melakukan update perubahannya diterapkan akan diterapkan ke dalam aplikasi.



Gambar 8. Sequence Diagram Login

Gambar 8 menjelaskan ketika ada user yang ingin login ke dalam aplikasi maka user harus mengisi data yang diperlukan untuk login kemudian data yang telah dimasukkan akan dikirim ke tabel user dan kemudian akan dikirim ke database untuk di validasi jika data tersebut ditemukan maka aplikasi akan memunculkan menu utama. Sedangkan jika tidak ditemukan maka akan dimunculkan pesan data yang dimasukkan untuk login salah.

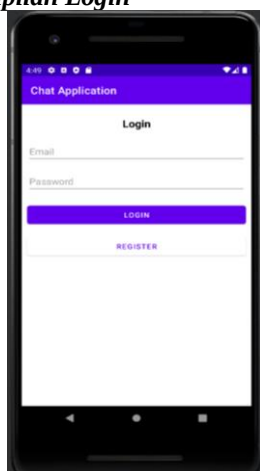


Gambar 9. Sequence Diagram Chatting

Gambar 9 menjelaskan ketika user ingin memulai chatting dengan user lain maka user harus memilih teman yang ingin diajak komunikasi di menu utama setelah dipilih maka aplikasi akan menampilkan ruang chat yang ada dengan user yang bersangkutan. Setelah itu user dapat mengirimkan pesan ataupun gambar yang ingin dikirim yang nantinya pesan dan gambar tersebut akan dikirim ke database sebelum nantinya dikirim dari database ke user yang ingin dikirimkan pesan dalam bentuk enkripsi. Sedangkan Ketika user ingin membaca pesan yang ada di ruang chat maka user harus menekan tombol dekripsi. Setelah itu akan muncul message box yang meminta untuk memasukkan password login jika password yang dimasukkan salah maka akan muncul message box yang mengatakan error dan pesan tidak akan didekripsi sedangkan jika password yang dimasukkan benar maka akan muncul message box yang mengatakan pesan sedang didekripsi setelah menunggu sebentar maka pesan yang ada di ruang chat akan didekripsi dan bisa dibaca dengan mudah.

4.2. Tampilan Program

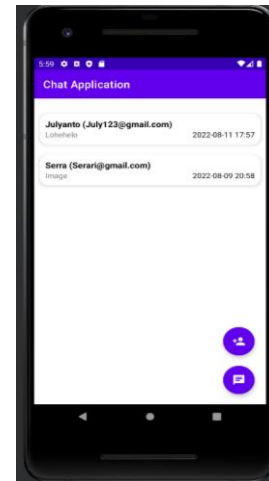
4.2.1. Tampilan Login



Gambar 10. Login

Pada gambar 10 merupakan tampilan *form login* merupakan tampilan yang muncul pertama kali ketika user membuka aplikasi.

4.1.1. Tampilan Menu Utama



Gambar 11. Menu Utama

Pada gambar 11 merupakan tampilan yang akan muncul ketika kita berhasil login masuk kedalam aplikasi di dalam menu utama ini terdapat ruang chat dari user yang sudah pernah memulai berbicara ataupun yang kita mulai pembicaraan. Selain itu di menu ini terdapat tombol list friend dan tombol untuk memulai pembicaraan baru.

4.1.1. Tampilan Ruang Chat



Gambar 12. Ruang Chat Terenkripsi

Pada Gambar 12 dapat dilihat tampilan ruang chat yang masih dalam bentuk enkripsi, sehingga pesan yang muncul merupakan huruf acak yang akan mempersulit orang lain yang ingin membacanya.



Gambar 13. Ruang Chat Terdekripsi

Pada gambar 13 merupakan tampilan dari ruang chat ketika pesan sudah selesai di dekripsi. Jika pesan sudah terdekripsi maka huruf acak yang sebelumnya muncul di ruang chat akan berubah menjadi kata kata yang bisa dengan mudah di pahami oleh user.

4.2. Pengujian

Ketika sistem sudah diimplementasikan dalam bentuk aplikasi maka akan dilakukan proses uji coba terhadap sistem. Dalam pengujian akan menggunakan Teknik Black Box. Dimana dalam sistem tersebut akan diuji fungsionalitas pada program tersebut.

Tabel 1: Pengujian Sistem

No	Variabel	Langkah Pengujian	Hasil Pengujian	Status Validasi
1	Login	Menginput Email dan password yang sudah pernah di registrasi	Masuk ke dalam main menu	Valid
2	Login	Menginput email dan password yang belum pernah di registrasi	Keluar pesan user not found	Valid
3	registrasi	Menginput nama yang kurang dari 5 huruf	Keluar pesan nama harus lebih dari 5 huruf	Valid
4	registrasi	Menginput email tanpa memasukan alamat email	Keluar pesan email address not found	Valid
5	registrasi	Memasukkan nomor telpon di bawah 10 angka	Keluar pesan phone must be 10 digit or more	Valid
6	registrasi	Memasukkan password di bawah 8 karakter	Keluar pesan password must be 8 character length or more	Valid
7	registrasi	Memasukkan password confirmaion yang berbeda dari password yang ingin di buat	Keluar pesan confirmation password not match	Valid
8	registrasi	Menginput nama email nomor telepon dan password sesuai dengan aturan	Keluar pesan register successful dan Kembali ke menu login	Valid
9	Main Menu	Menekan tombol menambah teman	Masuk ke menu friendlist	Valid
10	Main Menu	Menekan tombol pesan	Keluar menu untuk memasukkan alamat email yang ingin di masukkan agar bisa memulai percakapan	Valid
11	Main Menu	Menekan room chat yang ada ketika sudah pernah memulai percakapan	Masuk kedalam room chat	Valid

13	Friend list	Memasukkan user email yang belum pernah terdaftar didatabase dan menekan tombol add as friend	Keluar pesan email not valid	Valid
14	Friend List	Menghapus User yang sudah pernah menjadi teman	User yang ingin dihapus hilang dari friend list	Valid
15	Room Chat	Memasukkan pesan yang ingin dikirim tanpa ada Batasan huruf dan mengirimnya	Pesan terkirim dan terlihat dalam bentuk enkripsi di room chat	Valid
16	Room Chat	Mengirimkan gambar yang terdapat di dalam galeri	Gambar terkirim dan akan terlihat di dalam room chat	Valid
17	Room Chat	Menekan tombol menelepon	Akan terbuka aplikasi telepon	Valid
18	Room Chat	Menekan tombol decrypt	Memunculkan message box meminta password login	Valid
19	Room Chat	Memasukkan Password yang salah ketika message box decrypt muncul	Memunculkan message box password salah	Valid
20	Room Chat	Memasukkan Password yang benar ketika message box decrypt muncul	Memunculkan message box pesan sedang di dekripsi dan setelah menunggu sebentar pesan di ruang chat akan terdekripsi	valid

Dari tabel pengujian diatas dapat disimpulkan bahwa program telah bisa dipakai dengan layak karena memberikan respon yang sesuai.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan mengacu pada tujuan penelitian yang telah dirancang sebelumnya. Keberhasilan dalam mencapai tujuan penelitian dapat dibuktikan pada tahapan implementasi dan pengujian, maka dapat disimpulkan bahwa sistem komunikasi dengan menerapkan Metode SDLC menggunakan enkripsi Caesar cipher dan DBMS MySQL sebagai database yang digunakan. Sistem komunikasi ini juga sudah diuji menggunakan teknik black box, dimana dalam sistem yang dibuat telah diuji fungsionalitas programnya. Hasil pengujian sistem komunikasi pada Motor Harapan dinyatakan valid untuk digunakan.

5.2 Saran

Beberapa saran untuk mengembangkan sistem menjadi lebih baik ke peneliti selanjutnya. Perlunya dikembangkan aplikasi sehingga bisa memiliki fitur delete chat, mengenkripsi gambar, dan memiliki UI lebih bagus.

DAFTAR PUSTAKA

- [1] Maiyana, E. (2018) 'Pemanfaatan Android Dalam Perancangan Aplikasi Kumpulan Doa', Jurnal Sains Dan Informatika, 4(1), Pp. 54–65. Doi: 10.22216/Jsi.V4i1.3409.
- [2] Purwanti, H. (2013) 'Penerapan Pembelajaran Aplikasi Berbasis Android Pada Mata Pelajaran Pbm Dimasa Pandemi ovid-19', 42(2), Pp. 107–115.
- [3] Sudaria, Putra, A. S. And Novembrianto, Y. (2021) 'Sistem Manajemen Pelayanan Pelanggan Menggunakan Php Dan Mysql (Studi Kasus Pada Toko Surya)', Tekinfo, 22(1), Pp. 100–117.
- [4] Sofwan, A. (2011) 'Belajar Mysql Dengan Phpmyadmin Pendahuluan', Modul Kuliah Graphical User Interface I (Gui) Di Perguruan Tinggi Raharja, Pp. 1–29.
- [5] Novendri (2019) 'Aplikasi Inventaris Barang Pada Mts Nurul Islam Dumai Menggunakan Php Dan Mysql', Lentera Dumai, 0(2), Pp. 46–57.
- [6] Paraya, G. R. And Tanone, R. (2018) 'Penerapan Firebase Realtime Database Pada Prototype Aplikasi Pemesanan Makanan Berbasis Android', Jurnal Teknik Informatika Dan Sistem Informasi, 4(3), Pp. 397–406.