Penerapan Algoritma AES dalam Perancangan Aplikasi Media Sosial Berbasis Android

Rony Chandra Halim*1, Slamet Sugiarto[2]
[1,2]Jurusan Teknik Informatika; STMIK Pontianak. Jl. Merdeka No.372 Pontianak, 0561-735555
e-mail: [*1]ronychan95@gmail.com, [2]Slamet.sugiarto@stmikpontianak.ac.id

Abstrak

Komunikasi merupakan suatu proses penyampaian informasi atau pesan dari suatu pihak kepada pihak yang lain. Pada umumnya, komunikasi dilakukan secara lisan atau verbal yang dapat dimengerti oleh kedua belah pihak. Seiring dengan kemajuan teknologi, komunikasi tidak hanya terbatas dengan tatap muka atau dengan telepon tetapi juga berbagai media seperti media sosial. Akan tetapi muncul dan berkembangnya media sosial menjadi sebuah ancaman terjadi nya pencurian data pengguna. Oleh karena itu, penulis merancang aplikasi media sosial sebagai media untuk berkomunikasi dengan penerapan algoritma kriptografi Advanced Encryption Standard (AES). Perancangan aplikasi media sosial ini diharapkan dapat menjadi media untuk berkomunikasi dan dengan penerapan algoritma AES diharapkan dapat mengamankan data pengguna. Database yang digunakan pada aplikasi ini menggunakan Firebase. Metode perancangan perangkat lunak yang digunakan adalah Rapid Application Development (RAD). Pengumpulan data yang dilakukan dengan studi dokumentasi. Perancangan aplikasi yang digunakan menggunakan bahasa pemrograman Java dengan Aplikasi Android Studio. Pengujian aplikasi menggunakan User Acceptance Test. Penelitian dari perancangan aplikasi media sosial dan penerapan algoritma AES dapat berjalan sesuai dengan yang diharapkan. Demi perkembangan aplikasi diharapkan penelitian selanjutnya dapat menambahkan fitur-fitur pada aplikasi ini.

Kata kunci : Media Sosial, Algoritma AES, Android

Abstract

Communication is the process of delivering information or message from one party to another party. In general, communication is carried out verbally or verbally which can be accessed by both parties. Along with the improvement of technology, communication is not only limited to various media but various media such as social media. However, the emergence and development of social media becomes data that is carried out by data users. Therefore, the authors use social media as a medium to communicate using the Advanced Encryption Standard (AES) cryptographic algorithm. This judicial application media is expected to be a medium for communication and by using AES algorithms that can be accessed by user data. The database on this application uses Firebase. The software design method used is Rapid Application Development (RAD). Data collection is done by documentation study. Application design that uses the Java programming language with the Android Studio Application. Application testing uses User Acceptance Test. Research from the design of social media applications and the application of the AES algorithm can proceed as expected. For the sake of application development, it is hoped that further research can add features to this application.

Keywords : Social Media, AES Algorithm, Android

1. PENDAHULUAN

Media sosial adalah satu set baru komunikasi dan alat kolaborasi yang memungkinkan banyak jenis interaksi yang sebelumnya tidak tersedia untuk orang biasa [1]. Karakteristik media sosial adalah : 1) Jangkauan yang bisa meliputi skala khalayak kecil dan khalayak global; 2) Lebih mudah diakses publik dengan biaya yang lebih terjangkau; 3) Media sosial relatif lebih mudah digunakan karena tidka memerlukan ketrampilan dan pelatihan khusus; 4) Media sosial dapat memancing respon khalayak lebih cepat; 5) Media sosial dapat menggantikan komentar secara instan atau mudah melakukan proses pengeditan [2]. Pemanfaatan aplikasi media sosial dapat memberikan banyak manfaat seperti mempermudah komunikasi, penyampaian informasi, memperluas jaringan pertemanan, sarana untuk berbagi dan mengekspersikan diri.

Saat ini berbagai aplikasi seperti salah satu nya media sosial menjadi sasaran tindakan hacker dan kejahatan cyber yang semakin meningkat, karena menyimpan berbagai data dan informasi pengguna. Hal ini tentunya akan merugikan para pengguna media sosial jika data pengguna disalah gunakan. Oleh karena itu media sosial membutuhkan keamanan didalam penyimpanan data. Usaha perlindungan data atau pesan dapat dilakukan dengan berbagai macam cara, salah satunya dengan mengimplementasikan kriptografi. Kriptografi atau yang dikenal sebagai ilmu penyadian merupakan suatu bidang ilmu untuk menjaga pesan, informasi, dan data yang hanya boleh diakses oleh orang tertentu supaya tidak terjadi kebocoran dan penyalahgunaan oleh pihak yang tidak berwewenang. Dengan kriptografi, data yang dianggap rahasia dapat disembunyikan dengan melakukan teknik penyandian, sehingga data menjadi tidak dapat dibaca atau tidak dimengerti oleh orang lain, selain oleh pembuat dan penerimanya saja. Salah satu algoritma yang menjadi standar dari kriptografi adalah Algoritma *Advanced Encryption Standard*.

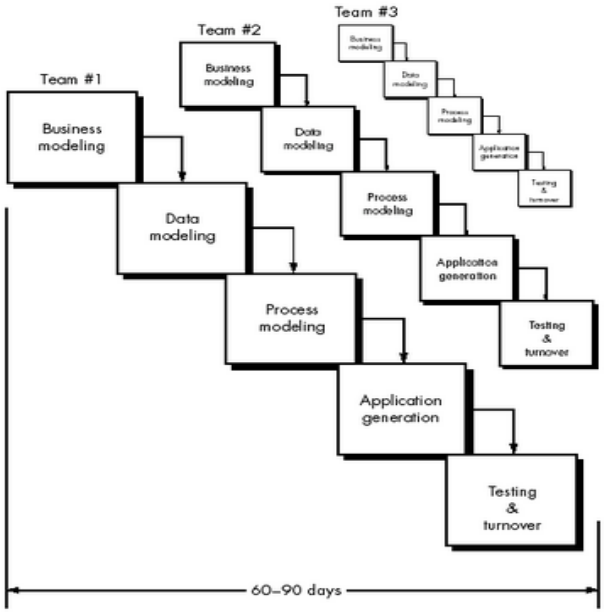
Algoritma *Advanced Encryption Standard* (AES) merupakan algoritma kriptografi yang ditetapkan oleh *National Institute of Standards and Technology* (NIST) melalui publikasi FIPS 197 pada tahun 2001 sebagai pemenang dari kontes AES, dan juga menggantikan algoritma *Data Encryption Standard* (DES) yang mulai rentan terhadap serangan *brute force*. Algoritma AES merupakan algoritma simetri dimana kunci yang digunakan untuk proses enkripsi dan dekripsi adalah sama. Algoritma AES ini cocok untuk digunakan sebagai pengamanan pesan karena sudah melalui berbagai pengujian dan ditetapkan sebagai standar kriptografi yang saat ini digunakan juga oleh beberapa aplikasi pengirim pesan seperti Whatsapp, Facebook, dan Telegram.

Sebelumnya telah dilakukan sebuah penelitian dengan topik penerapan enkripsi dan dekripsi file menggunakan algoritma AES. Penerapan algoritma AES pada aplikasi menjadikan suatu teks dan file dapat di-enkripsi dan di-dekripsi untuk menjaga kerahasiaan data yang dapat juga diterapkan pada berbagai aplikasi untuk keamanan[3]. Penelitian lainnya melakukan perancangan layanan pesan singkat atau SMS dengan menerapkan algoritma AES. Hasil dari penelitian tersebut menghasilkan suatu aplikasi pada telepon seluler berbasis android yang dapat mengenrkipsi pesan SMS dengan menggunakan metode AES supaya pesan tersebut tidak dapat diketahui oleh orang lain[4]. Dari hasil kedua penelitian tersebut peneliti merasa algoritma *Advanced Encryption Standard* cocok untuk diterapkan ke dalam media sosial. Tujuan penelitian ini adalah untuk menghasilkan aplikasi media sosial yang dapat melakukan sharing foto dan chatting dengan algoritma Advanced Encryption Standard.

2. METODE PENELITIAN

Penelitian ini menggunakan bentuk penelitian yang beracuan pada studi literatur, yaitu dengan cara mempelajari prinsip enkripsi dan dekripsi yang di dapat dari buku dan referensi dari berbagai sumber yang relevan tentang algoritma kriptografi AES. Metode penlitian yang digunakan adalah metode eksperimental, yaitu dilakukan dengan cara membuat suatu *software* atau perangkat lunak terlebih dahulu kemudian membandingkan kebenaran dari proses yang dibuat dengan hasil yang diharapkan setelah menggunakan perangkat ini. Metode pengumpulan

data yang digunakan adalah data primer dan data sekunder sedangkan teknik pengumpulan data meliputi observasi dan studi dokumentasi. Metode perancangan perangkat lunak yang digunakan adalah *Rapid Application Development (RAD).* Metode RAD terdapat 5 tahapan dimulai dari tahap *bussiness modelling*, pada tahap ini untuk mencari dan mendefinisikan fungsi-fungsi yang akan dipakai dalam pembuatan aplikasi. Tahap *data modelling* untuk menentukan banyaknya modul dan *form* yang akan digunakan dalam perancangan aplikasi. Tahap *process modelling* untuk merancang *form* dan modul yang sudah didefinisikan sebelumnya sehingga mementuk aplikasi yang utuh. Tahap *application generation* yaitu tahap membangun aplikasi dengan instrumen penelitian berupa algoritma. Terakhir adalah tahap *testing and turnover* yaitu melakukan testing aplikasi yang telah dibuat dan diuji apakah proses yang diharapkan dapat berjalan dengan baik atau tidak [5] (Gambar 1).



Gambar 1 Tahapan Metode *Rapid Application Development* [6]

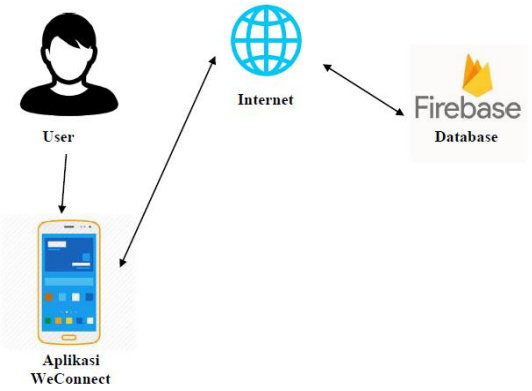
Dalam penelitian ini, pemodelan perangkat lunak yang digunakan yaitu UML. UML merupakan bahasa visual yang menjadi standar untuk menspesifikasikan, menggambarkan, membangun, dan dokumentasi dari sistem perangkat lunak [7]. UML menyediakan 9 jenis diagram yang dapat dikelompokkan berdasarkan sifatnya statis atau dinamis, seperti diagram kelas, diagram objek, use-case diagram, sequence diagram, collaboration diagram, statechart diagram, activity diagram, component diagram, dan deployment diagram [8].

3. HASIL DAN PEMBAHASAN

Perancangan aplikasi media sosial dengan penerapan algoritma AES yang diberi nama WeConnect menggunakan metode perancangan *Rapid Application Development* dimana tahapannya dimulai dengan tahap *bussiness modelling* yaitu analisis algortima *Advanced Encryption Standard.* Algoritma AES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis chiper blok yang beroperasi pada ukuran blok 128 bit, 192 bit, dan 256 bit. Tahap – tahapan pada enkripsi algoritma AES adalah pada awal proses enkripsi, input yang telah dicopykan ke dalam *state* akan mengalami transformasi *byte AddRoundKey.* Setelah itu, *state* akan mengalami transformasi *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey* secara berulang – ulang sebanyak Nr. Proses ini dalam algoritma AES disebut juga sebagai *round function. Round* yang

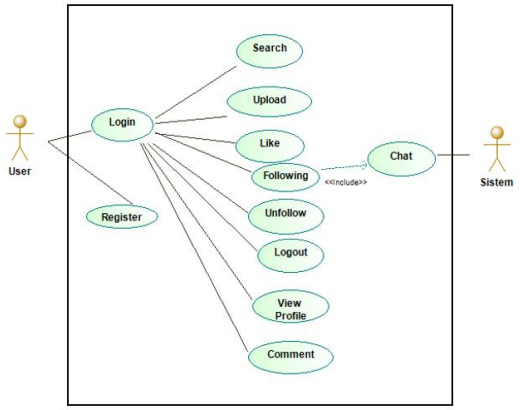
terakhir agak berbeda dengan *round – round* sebelumnya, dimana pada *round* terakhir *state* tidak mengalami transformasi *MixColumns.*

Setelah menentukan *bussinness modelling* dengan analisis algoritma AES, tahap berikutnya adalah tahap *data modelling* untuk menentukan banyaknya form yang akan digunakan dalam aplikasi yang akan diracang. Perancangan aplikasi media sosial menggunakan beberapa form, yaitu form login, form register, form utama, form profile, form edit profile, form pencarian, form chat, dan form logout. Adapun setelah menentukan form dilakukan gambaran arsitektur perangkat lunak untuk menggambarkan komponen perangkat lunak (Gambar 2).



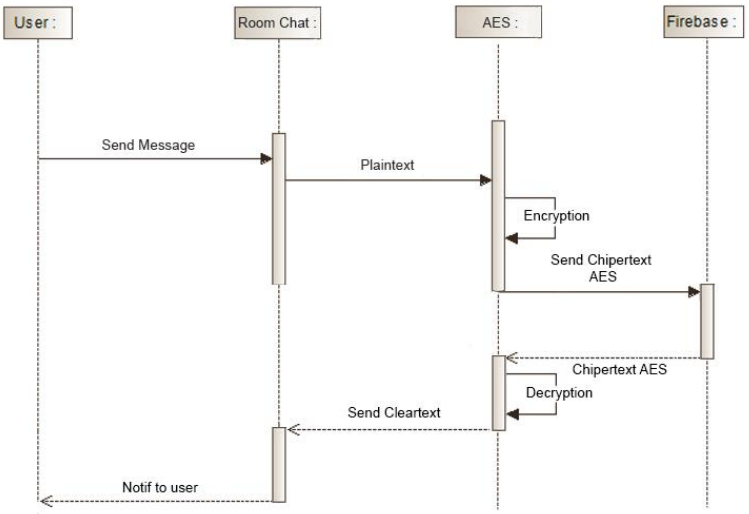
Gambar 2 Arsitektur Perangkat Lunak

Setelah melakukan *data modelling* dilakukan *process modelling* yaitu perancangan aplikasi WeConnect dengan menggunakan *Use Case Diagram, Sequence Diagram* dan *Activity Diagram. Use Case Diagram* berfungsi untuk menjelaskan manfaat sistem jika dilihat menurut pandangan orang yang berada diluar sistem atau *actor* atau *user*. *Use case diagram* WeConnect terdiri dari user. Aktor user memulai dengan melakukan register akun dengan menggunakan email supaya bisa melakukan login ke dalam aplikasi WeConnect. Jika user sudah pernah register maka user dapat langsung melakukan login ke dalam aplikasi WeConnect. Ketika user sudah melakukan Login ke dalam aplikasi, maka tampilan yang ditampilkan berupa 4 buah tabs yaitu Halaman Utama, Search, Profile, dan Upload. Untuk melakukan chatting pada aplikasi WeConnect user diharuskan melakukan follow terlebih dahulu dengan cara masuk ke menu search dan menginputkan username pengguna lain. Setelah melakukan follow maka user dapat melakukan chat dengan pengguna lain dengan cara masuk ke tab chat dan memilih pengguna yang akan di chat. Bagian Profile pengguna dapat melihat informasi akun seperti username, nama pengguna, jumlah post, jumlah following, jumlah followers, foto profile dan foto yang dishare. Pada bagian profile pengguna dapat melakukan penggantian foto profile dan berbagai informasi akun seperti username, website, desrkipsi, email dan nomor handphone. Pada bagian option di halaman profile pengguna dapat logout dari aplikasi WeConnect (Gambar 3).



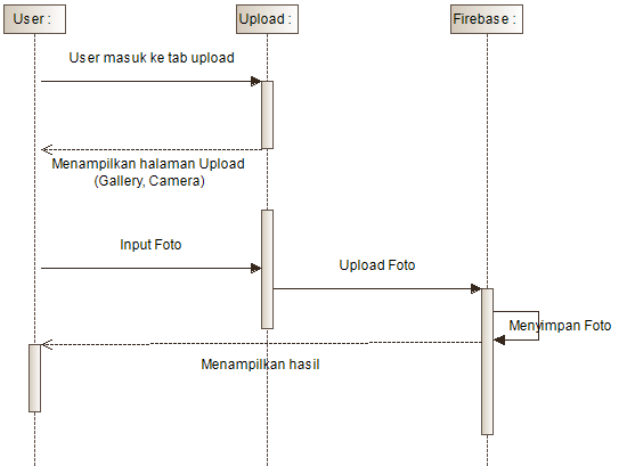
Gambar 3 Use Case Diagram Perancangan Aplikasi WeConnect

Sequence Diagram digunakan untuk menggambarkan skenario atau langkah – langkah yang dilakukan sebagai suatu respon untuk menghasilkan output tertentu. Berikut ini beberapa *sequence diagram* dalam perancangan aplikasi WeConnect. *Sequence diagram chat* yaitu untuk mengambarkan alur dari fitur chatting pada aplikasi WeConnect. Proses chat dimulai dari user melakukan pengiriman pesan berupa plaintext yang akan di enkripsi dengan metode AES kemudian hasil dari enkripsi yang berupa Chipertext disimpan di dalam Firebase dan di kirimkan ke penerima dengan berupa chipertext aes yang di dekripsi kemudian dihasilkan cleartext ke penerima pesan (Gambar 4).



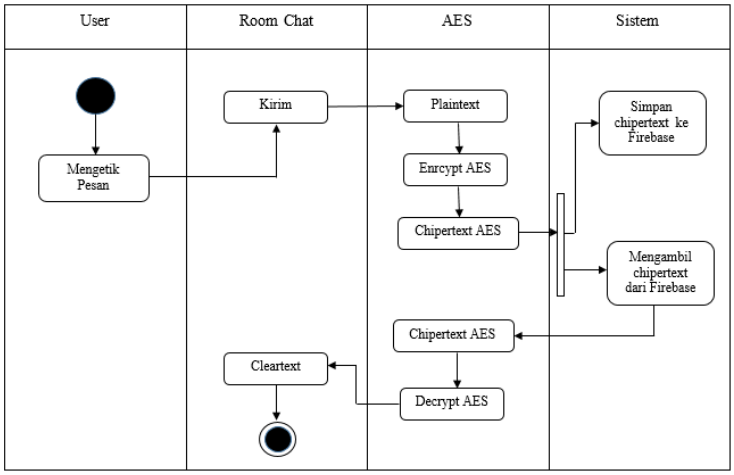
Gambar 4 *Sequence Diagram Chat* WeConnect

Sequence diagram upload yaitu alur yang menggambarkan proses pengguna dapat melakukan upload foto ke media sosial WeConnect. *User* membuka halaman share, kemudian sistem akan menampilkan 2 buah pilihan gallery / camera. User memilih gallery/camera. Jika user memilih gallery maka sistem akan menampilkan halaman gallery. Jika user memilih camera maka sistem akan menampilkan halaman camera. Sistem akan menyimpan foto yang diupload ke dalam database dan akan menampilkan hasilnya setelah selesai upload (Gambar 5).



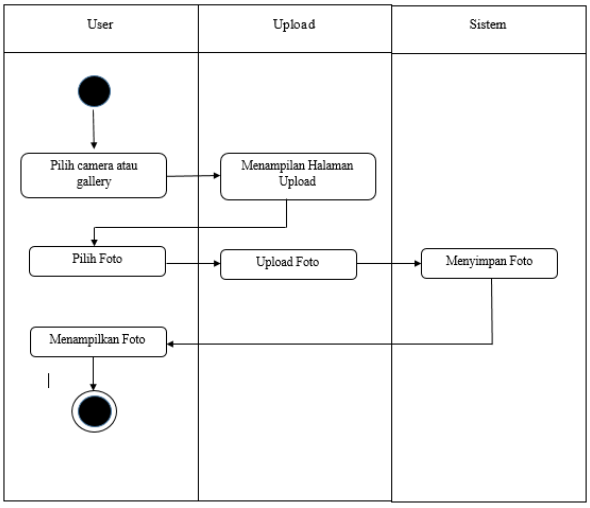
Gambar 5 *Sequence Diagram Upload* WeConnect

Activity Diagram yaitu diagram yang menggambarkan urutan aktifitas dalam sebuah proses. Kegunaan dari *activity diagram* adalah memperlihatkan urutan aktifitas sistem. Berikut ini beberapa *activity diagram* WeConnect. *Activity Diagram* proses *Chatting* WeConnect, ketika *user* mengirimkan pesan berupa plaintext, maka pesan akan di lakukan enkripsi menjadi chipertext aes, kemudian disimpan di dalam Firebase lalu hasil akan dikirimkan kembali ke penerima dengan didekripsi chipertext AES menjadi cleartext yang dapat dibaca oleh penerima (Gambar 6).



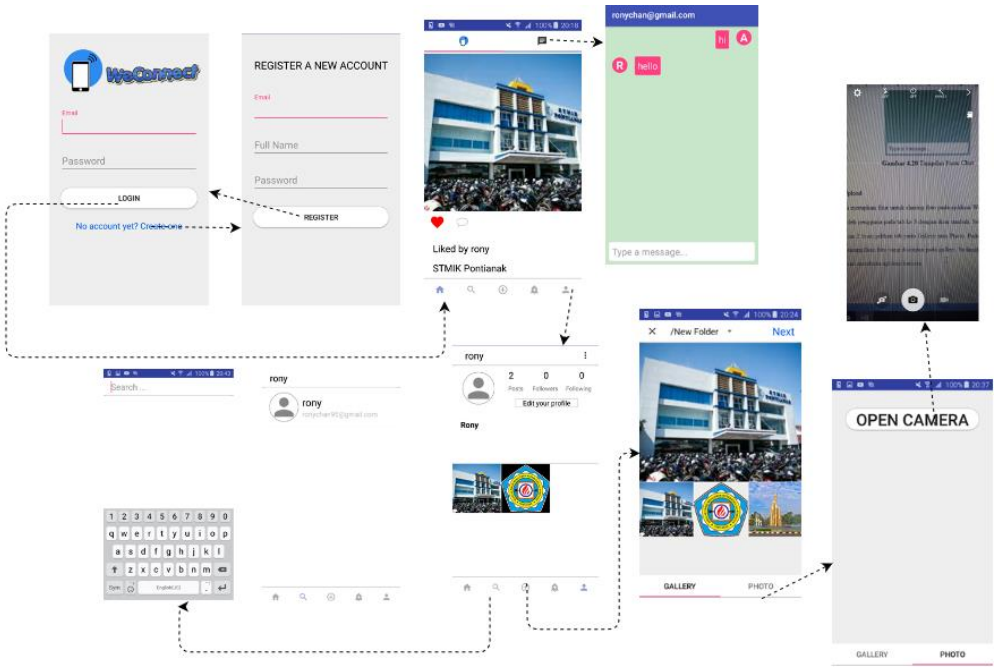
Gambar 6 *Activity Diagram* Proses *Chatting* WeConnect

Activity diagram upload, user memilih *camera* atau *gallery* kemudian akan menampilkan halaman upload, user memilih foto yang ingin diupload dan tekan upload. Maka sistem akan mengirimkan foto ke dalam database Firebase untuk disimpan dan ditampilkan kembali ke *user* (Gambar 7).



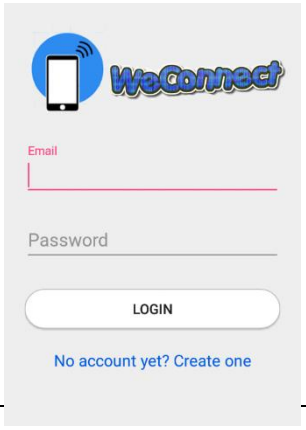
Gambar 7 *Activity Diagram Upload* WeConnect

Model View dimaksudkan untuk memberikan gambaran alur *feedback* kepada *user* jika suatu tombol ditekan. Gambaran alur tersebut dapat menjelaskan detail proses cara kerja aplikasi WeConnect. Berikut adalah *model view* dari aplikasi WeConnect (Gambar 8).



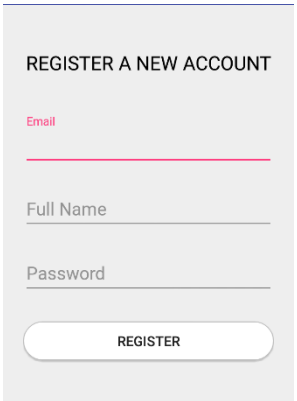
Gambar 8 *Model View* Aplikasi WeConnect

Perancangan *interface* aplikasi WeConnect yang dibuat dalam penelitian ini dirancang sedemikan rupa supaya tampilan antarmuka dari aplikasi ini menjadi lebih lebih interaktif dan mudah dalam pengoperasiannya (*user friendly*), sehingga pengguna tidak akan merasa kesulitan dalam menggunakan aplikasi ini. Pada aplikasi ini terdapat form login, form register, form utama, form profile, form chat, form search, form edit profile, logout. Form login merupakan tampilan awal yang muncul ketika pengguna menjalankan aplikasi WeConnect. Form ini bertujuan untuk memasukkan email dan password dari akun yang telah terdaftar pada database. Pada form ini terdapat juga pilihan untuk registrasi bagi pengguna baru (Gambar 9).



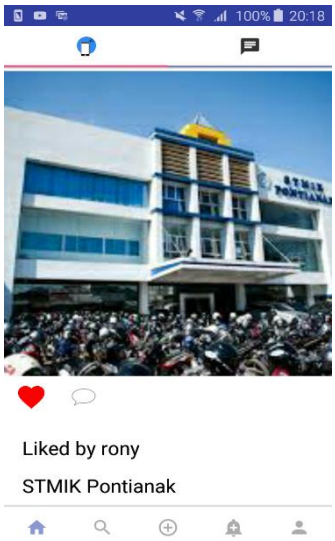
Gambar 9 Tampilan Form *Login* WeConnect

Form *register* bertujuan untuk membuat akun baru bagi pengguna. Terdapat 3 buah kolom yang harus diisi oleh pengguna yaitu email, nama lengkap dan password. Setelah menginputkan data dan tekan tombol *Register*, maka akun pengguna akan terdaftar. Setelah melakukan pendaftaran pengguna akan diarahkan kembali ke halaman *login* (Gambar 10).



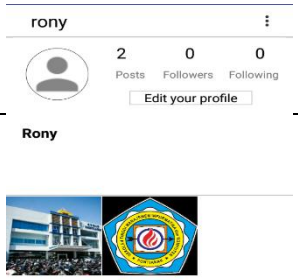
Gambar 10 Tampilan Form *Register* WeConnect

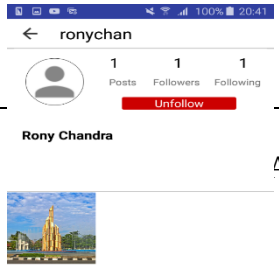
Form utama merupakan form awal setelah pengguna melakukan login. Pada form ini pengguna dapat mengakses ke berbagai form seperti search, upload, profile, dan chat (Gambar 11).



Gambar 11 Tampilan Form Utama WeConnect

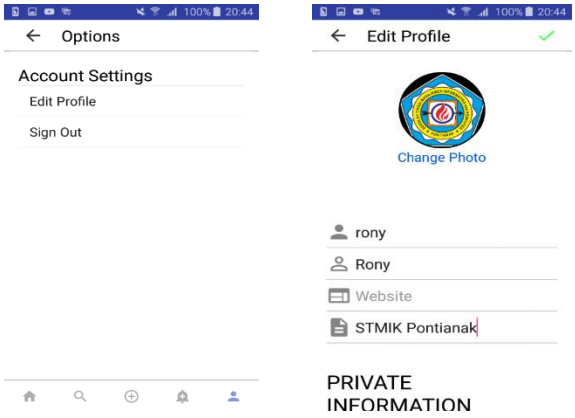
Form *Profile* menampilkan *profile* pengguna seperti total postingan foto, followers, following, foto *profile*, nama pengguna, foto – foto yang di upload pengguna dan fitur mengedit profile pengguna (Gambar 12).





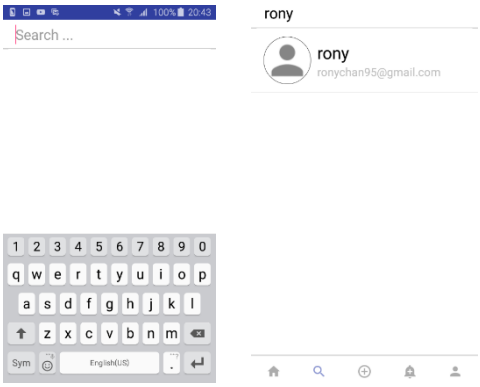
Gambar 12 Tampilan Form Profile Pengguna WeConnect

Form *Edit Profile* untuk mengubah data pengguna seperti username, nama, website, deskripsi, email, dan nomor handphone (Gambar 13).



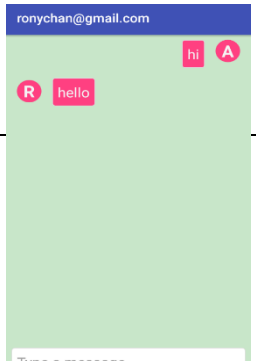
Gambar 13 Tampilan *Edit Profile* WeConnect

Form *Search* bertujuan untuk mencari *profile* pengguna lain dengan menginputkan username pengguna yang akan di cari pada kolom search (Gambar 14).



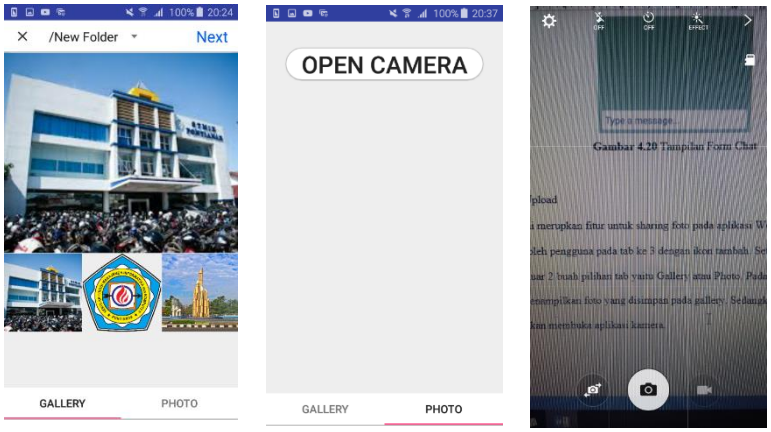
Gambar 14 Tampilan *Search* WeConnect

Form *Chat* bertujuan untuk melakukan chat antara pengguna dengan pengguna lain (Gambar 15).



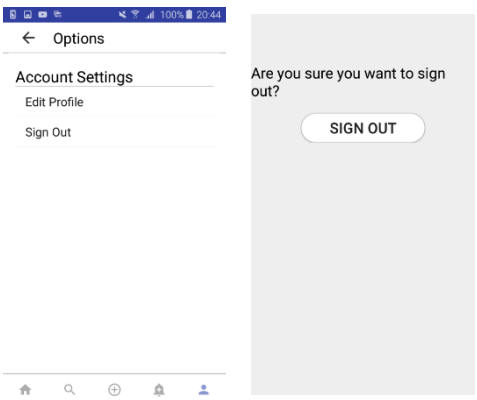
Gambar 15 Tampilan *Chat* WeConnect

Form *Upload* merupkan fitur untuk sharing foto pada aplikasi WeConnect. Fitur ini dapat diakses oleh pengguna pada tab ke 3 dengan ikon tambah. Setelah masuk ke tab maka akan keluar 2 buah pilihan tab yaitu Gallery atau Photo. Pada tab Gallery maka sistem akan menampilkan foto yang disimpan pada gallery. Sedangkan pada tab Photo maka sistem akan membuka aplikasi kamera (Gambar 16).



Gambar 16 Tampilan *Upload* WeConnect

Form *logout* merupakan fitur terakhir yang tentunya ada pada setiap aplikasi media sosial. Fitur ini terletak pada form profile pada ikon tiga titik vertikal pada kanan atas. Tujuan fitur ini adalah keluar dari akun pengguna dan mengarahkan pengguna kembali ke halaman login (Gambar 17).



Gambar 17 Tampilan *Logout* WeConnect

Tahap t*esting & turnover* merupakan tahap pengujian terhadap sistem yang dibangun. Pengujian yang dilakukan mencakup integritas serta fungsional sistem dan terkait dengan hal-hal teknis sistem. Hal ini untuk menghindari sistem dari kesalahan maupun error dan menghasilkan sistem yang sesuai dengan yang diharapkan. Adapun pengujian yang dilakukan yaitu menggunakan metode *User Acceptance Test.*

Tabel pengujian *User Acceptance Test* oleh pengguna aplikasi. Responden terdiri dari 20 orang mahasiswa kelas C4 STMIK Pontianak yang diberikan kuisioner mengenai hasil dari aplikasi media sosial WeConnect yang telah dicoba (Tabel 1).

SB = Sangat Baik.
B = Baik
C = Cukup
K = Kurang
SK = Sangat Kurang

Tabel 1 Hasil Kuisioner Pengujian *User Acceptance Test*

No	**Pertanyaan**	**Skala**				
		SB	**B**	**C**	**K**	**SK**
1	Bagaimana pendapat anda tentang tampilan aplikasi WeConnect?	6	12	2	0	0
2	Apakah aplikasi WeConnect mudah digunakan?	12	7	1	0	0
3	Apakah fitur pada WeConnect sudah lengkap?	4	8	7	1	0
4	Apakah fitur-fitur yang tersedia dapat berjalan dengan benar?	10	9	1	0	0
5	Apakah aplikasi WeConnect sudah dapat digunakan sehari-hari?	1	9	7	3	0
6	Apakah proses pengiriman pesan sudah cepat?	5	10	4	1	0
7	Apakah proses upload foto sudah cepat?	5	10	4	1	0
8	Bagaimana pendapat anda tentang keselurahan aplikasi?	4	9	5	2	0

Berdasarkan hasil kuisioner responden diatas dapat disimpulkan bahwa tampilan aplikasi WeConnect yang dirancang sudah baik (84%). Selain itu, aplikasi WeConnect yang dirancang mudah digunakan (91%). Fitur aplikasi pada WeConnect yang dirancang cukup lengkap (75%). Fitur pada aplikasi WeConnect sudah dapat berjalan dengan baik (89%). Aplikasi WeConnect belum bisa dapat digunakan sehari hari karena masih terdapat beberapa kekurangan (68%). Proses pengiriman pesan cukup cepat (79%). Proses upload foto cukup cepat (79%). Keselurahan aplikasi sudah cukup baik (75%).

4. KESIMPULAN

Perancangan aplikasi media sosial dan penerapan algoritma AES dapat berjalan sesuai dengan yang diharapan pada sistem operasi Android dan dapat digunakan untuk melakukan sharing foto dan chatting. Selain itu, aplikasi yang dirancang memiliki tampilan yang sederhana dan mudah digunakan.

5. SARAN

Diharapkan untuk penelitian selanjutnya, pengembangan aplikasi media sosial dapat berjalan pada sistem operasi selain Android. Aplikasi diperlukan penambahan beberapa fitur untuk melengkapi kebutuhan pengguna.

DAFTAR PUSTAKA

[1] Brogran, Chris. 2010. *Social Media 101: Tactics and Tips to Develop Your Business Online.* John Wiley&Sons.

[2] Purnama, Hadi. 2011. *Media Sosial Di Era Pemasaran 3.0 Corporate and Marketing Communication.* Jakarta : Pusat Studi Komunikasi dan Bisnis Program Pasca Sarjana Universitas Mercu Buana.

[3] Rifkie Primartha. 2013. Penerapan Enrkipsi dan Dekripsi File Menggunakan Algoritma Advanced Encrpytion Standard (AES), *Journal of Research in Computer Science and Applications* , vol. 1, no. 2.

[4] Raisul Azhar, dkk. 2016. Aplikasi Keamanan SMS Menggunakan Algoritma Rijndael, *Jurnal Matrik*, vol.16, no.1.

[5] Roger, S.Pressman. 2012, *Rekayasa Perangkat Lunak (Pendekatan Praktisi) Edisi 7 : Buku 1*. Yogyakarta : Andi

[6] Roger, S.Pressman. 2002. *Rekayasa Perangkat Lunak Pendekatan Praktisi (Buku Satu).* Yogyakarta : Andi

[7] Yuni Sugiarti. 2013. *Analisis Dan Perancangan UML (Unified Modeling Language) Generated VB.6.* Yogyakarta: Graha Ilmu

[8] Adi Nugroho. 2005. *Rekayasa Perangkat Lunak Menggunakan UML dan JAVA.* Yogyakarta : Andi