Aplikasi Keamanan *Smartphone* Berbasis Android Menggunakan *Short Message Service*

Fathur Rahman[1], Lidya Wati [2], Devit Satria[3]
Jurusan Teknik Informatika, Politeknik Negeri Bengkalis, Bengkalis[1,2]
Jurusan Teknik Informatika, Sekolah Tinggi Teknologi Dumai, Dumai[3]
Fathurra261@gmail.com[1], Lidiyawati@polbeng.ac.id[2], devitsatria24@gmail.com [3]

Abstrack

Data security is very important in maintaining the confidentiality of information, especially confidential information that can only be known by the eligible only. For that we need a useful Android security system to protect our phones from abuse by others such as hijacked mobile phones, mobile phones carried away friends or lost by locking the screen Smartphone. Therefore made an Android Smartphone security application using Short Message Service (SMS). Which is capable of locking smartphone through short message service. This application is built using Android Studio with java programming. This application is able to lock the screen from a remote point, anywhere and anytime as long as the keywords set in the application in accordance with the type in SMS messages.

Keywords - Android, Security, Short Message Service (SMS), Smartphone

Abstrack

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama informasi rahasia yang hanya boleh diketahui oleh pihak yang berhak saja. Untuk itu diperlukan sistem keamanan Android yang berguna melindungi ponsel kita dari penyalahgunaan oleh orang lain misalnya ponsel dibajak, ponsel terbawa teman atau hilang dengan cara mengunci layar *Smartphone*. Maka dari itu dibuat sebuah aplikasi keamanan *Smartphone* berbasis Android menggunakan *Short Message Service* (SMS). yang mampu melakukan penguncian *smartphone* melalui *short message service*. Aplikasi ini dibangun memggunakan Android Studio dengan pemograman *java*. Aplikasi ini mampu mengunci layar dari jarah yang jauh, dimana saja dan kapan saja asalkan kata kunci yang *set* di aplikasi sesuai dengan yang di ketik pada pesan SMS.

Kata Kunci - Android, Keamanan, *Short Message Service* (SMS), *Smartphone*.

I. PENDAHULUAN

Belakangan ini perkembangan teknologi informasi sangat pesat, salah satunya adalah telepon selular ponsel. Mulai dari ponsel yang hanya bisa digunakan untuk bicara dan SMS hingga ponsel cerdas atau *Smartphone* yang memiliki berbagai fungsi seperti multimedia, transfer data, video streaming dan lain - lain. Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pengiriman data berupa pesan singkat melalui *Short Message Service* atau SMS.

Salah satu sistem operasi pada ponsel yang sangat popular pada saat ini adalah Android. Android adalah sebuah sistem operasi untuk perangkat telepon yang berbasis linux yang mencakup sistem operasi, *middleware,* aplikasi dan menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka [1].

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama informasi sensitif yang hanya boleh diketahui oleh pihak yang berhak saja. Informasi yang merupakan hasil pengolahan dari data, mempunyai nilai yang berbeda bagi setiap orang. Seringkali sebuah informasi menjadi sangat berharga dan tidak semua orang diperkenankan untuk mengetahuinya, namun selalu saja ada pihak yang berusaha untuk mengetahui informasi dengan cara - cara yang tidak semestinya bahkan bermaksud untuk merusaknya [2].

II. TINJAUAN PUSTAKA

2.1 Kajian Terdahulu

Penitian yang dilakukan [2], yang berjudul "Keamanan Komunikasi Data Sms Pada Android Dengan Menggunakan Aplikasi *Cryptography Advance Encryption Standard (Aes)*" bertujuan untuk mengamankan komunikasi data dari ancaman - ancaman dari luar seperti menyadap SMS. Kerahasiaan data SMS rentan bocor akibat pihak ketiga yang berhasil mendapatkan akses informasi dari dalam sistem komunikasi, penanggulangan masalah ancaman tersebut harus di pecahkan dengan penguncian data enkripsi yang akan di deskripsi oleh penerima.

Penelitian yang dilakukan [3], yang berjudul "Aplikasi Screen Lock Pada *Smartphone* Menggunakan Identifikasi Wajah Dengan Menerapkan Pointwise" bertujuan untuk membangun aplikasi identifikasi wajah pada *Smartphone* Android sebagai proteksi supaya hanya pemiliknya saja yang dapat menggunakannya. Aplikasi identifikasi wajah (*face recognition*) digunakan sebagai pengganti PIN atau *code phone* pada *Smartphone* Android supaya hanya wajah pemilik saja yang dapat digunakan untuk membuka kunci (lock) *Smartphone* yang terkunci oleh pemiliknya.

Penelitian yang dilakukan [4], yang berjudul "*Review on Android and Smartphone Security*" membahas tentang kemaanan Android yang tidak aman seperti yang terlihat,

meski begitu kuat, Android memiliki kelemahan juga. Keamanan adalah salah satu perhatian utama bagi pengguna ponsel cerdas saat ini karena Android rentan sekali terhadap serangan Virus dan lain lain.

2.2 Landasan Teori

Smartphone adalah sebuah media baru dalam proses komunikasi. *Smartphone* tidak lagi digunakan hanya untuk media komunikasi tetapi mulai dilirik oleh beberapa perusahaan pembuat *Smartphone* untuk dijadikan media hiburan dan edukasi. Smartphone merupakan sebuah telepon yang menyajikan fitur canggih seperti surel (surat elektronik), internet dan kemampuan membaca buku elektronik (*e-book*) atau terdapat papan ketik (baik sebagaimana jadi maupun dihubung keluar) dan penyambung VGA. Dengan kata lain, telepon cerdas merupakan komputer kecil yang mempunyai kemampuan sebuah telepon yang mempunyai daya guna bagi manusia [5].

Keamanan adalah satu kebutuhan bagi sebuah sistem untuk mengamankan kerahasiaan informasi terutama informasi sensitif yang hanya boleh diketahui oleh pihak yang berhak saja. Sebuah sistem harus mempunyai faktor keamanan yang cukup baik agar pemakai merasakan kenyamanan dan rasa aman dari gangguan ataupun serangan dari luar baik itu berupa spam atau virus sekalipun [2].

Short Message Service (SMS) adalah salah satu komunikasi teks melalui telepon seluler. SMS memuat konten teks berupa *keyword* (kata atau kumpulan beberapa kata yang akan menjadi kata kunci) ataupun kumpulan kalimat yang ditujukan pada target atau lawan komunikasi. SMS merupakan salah satu media yang paling banyak digunakan saat ini. Selain murah, prosesnya juga berjalan cepat dan langsung sampai pada tujuan, tetapi selama ini SMS baru digunakan sebatas untuk mengirim dan menerima pesan antara sesama pemilik telelepon seluler [6].

III. PERANCANGAN

3.1 Analisa Sistem

Pada tahap ini analisis sistem dan persiapan data dilakukan dengan menerapkan rancangan sistem yang telah ada (*Existing*) dan sistem yang akan diusulkan yaitu dengan melakukan Observasi dan Studi Literatur ditempat yang akan dijadikan penelitian.

3.1.1 Analisa sistem keamanan *smartphone* yang sedang berjalan

User bisa membuat *Password* sendiri dari sistem untuk mengunci *Smartphone* sehingga keamanan datanya terjamin. Tetapi ketika ada orang yang bisa membobol *Password,* keamanan datanya tidak terjamin. Dapat dilihat pada Gambar 3.1.

Gambar 3.1 Sistem yang berjalan
(Sumber : data olahan)

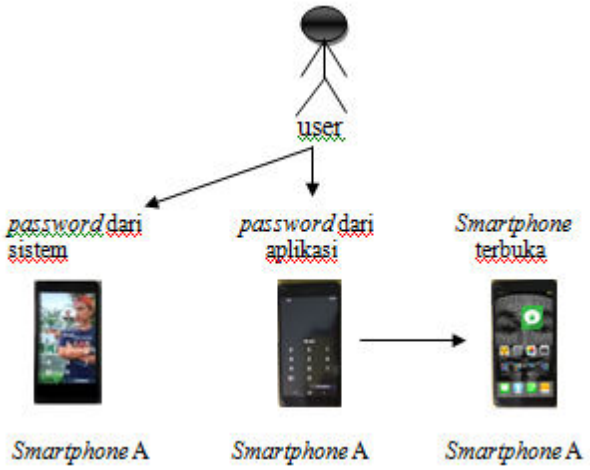
3.1.2 Analisa sistem keamanan *smartphone* yang diusulkan

Sistem yang akan diusulkan dalam pembuatan aplikasi ini yaitu *user* dapat mengunci *Smartphone* dengan menggunakan SMS dari jarak jauh. Dengan cara memasukkan *Keyword* atau kata kunci dan *Password* yang baru pada aplikasi yang akan digunakan untuk mengunci *Smartphone*. Dapat dilihat pada Gambar 3.2.

a. Mengunci layar smartphone

Gambar 3.2 Mengunci layar *smartphone*

Dari Gambar 3.2 dapat diketahui bahwa *user* mengetik SMS untuk mematikan *Smartphone* dan mengirimkan pesan tersebut ke nomor yang sedang di gunakan oleh *smartphone* di aplikasi pengunci layar. Ketika pesan dari ponsel masuk maka aplikasi pengunci layar tersebut akan menterjemahkan dan mengunci layar *Smartphone.* Dan membuka layar smartphone.

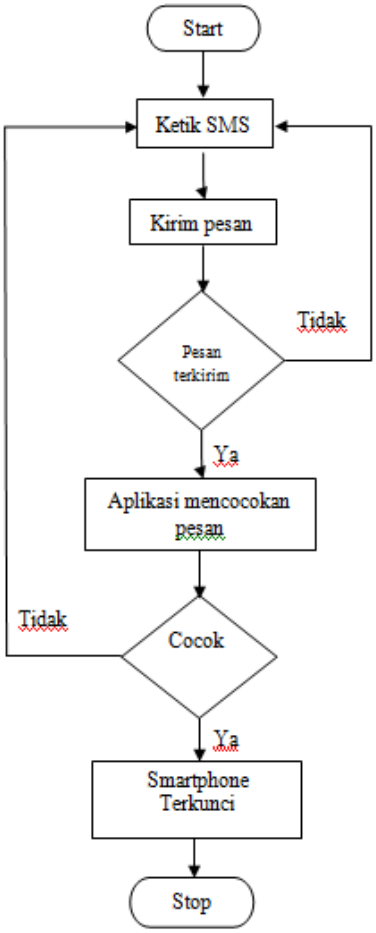


Gambar 3.3 Membuka layar *smartphone*

Dari Gambar 3.3 dapat diketahui bahwa *password* yang dibuat pada aplikasi ini akan menimpa *password* dari sistem Android. Untuk membuka kunci layar *smartphone, user* akan membuka *password* dari sistem Android terlebih dahulu. Selanjutnya *user*harus memasukkan *password* kedua yaitu *password* dari aplikasi yang dibuat ini. Kemudian kunci layar *smartphone* secara otomatis akan terbuka ke halaman utama layar.

3.1.3 Perancangan *flowchart* Mengunci *Smartphone.*

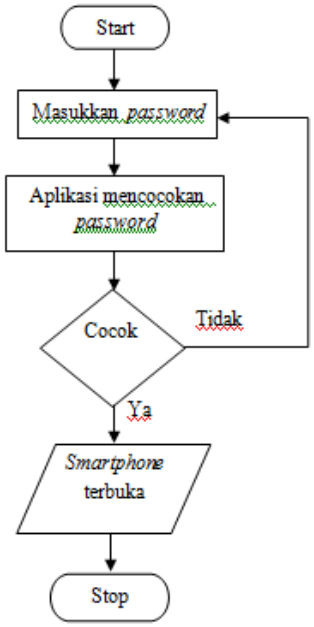
Perancangan *flowchart* untuk mengunci s*martphone* merupakan alur dari sistem yang dibuat dalam penelitian ini. Dapat dilhat pada Gambar 3.4.



Gambar 3.4 *Flowchat* mengunci *smartphone*

Dari Gambar 3.4 dapat diketahui bahwa untuk mengunci *smartphone*, *user* harus melakukan pengetikan pesan yang berupa kata kunci yang sudah di set pada aplikasi. Selanjutnya user mengirim pesan ke *smartphone* yang ingin dikunci, jika pengiriman pesan gagal maka *user* harus mengetik ulang pesan. Jika pesan sudah terkirim maka aplikasi akan mencocok pesan. Selanjutnya, jika pesan yang terkirim tidak cocok maka *user* harus mengetik ulang pesan, jika pesan yang terkirim sudah cocok maka *smartphone* akan terkunci.

3.1.4 Perancangan *flowchart* Mengunci *Smartphone.*

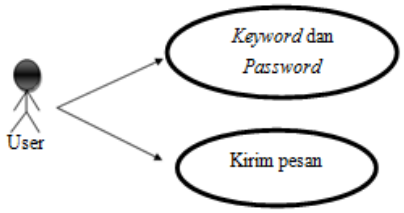


Gambar 3.5 *Flowchat* membuka *smartphone*

Dari Gambar 3.5 dapat diketahui bahwa untuk membuka *password, user* harus memasukkan *password* yang telah di buat sebelumnya pada aplikasi. Jika *password* yang di masukkan tidak cocok maka *user* harus memasukkan ulang *password.* Jika *password* yang di masukkan cocok maka *smartphone* akan terbuka.

3.2 *Use case Diagram*

Use case diagram merupakan umum tentang aliran sistem. *User* memasukkan *keyword* (kata kunci) sebagai kata kunci untuk pengiriman SMS. Sedangkan untuk *password* di *set* sebagai pin untuk mengunci layar *smartphone*. Dapat dilihat pada Gambar 3.6.



Gambar 3.6 *Usecase Diagram*

Deskripsi *Use case Keyword* dan *password*

Nama	: *Keyword* dan *password*
Aktor	: User
Tujuan	: User memasukkan *keyword* untuk

pesan sms dan *password* untuk mengunci layar *smartphone.*

Tabel 3.1 Deskripsi *Keyword* dan *password*

Actor Action	System Respond
1. User memasukkan *keyword* dan *password*	Melakukan proses penyimpanan data

Sumber: (Data Olahan)

Deskripsi *Use case* Kirim pesan
Nama : Kirim pesan
Aktor : User
Tujuan : User mengetik *keyword* di pesan sms dan mengirimkan pesan tersebut ke nomor *smartphone* yang terinstall Aplikasi ini

Tabel 3.2 Deskripsi Kirim pesan

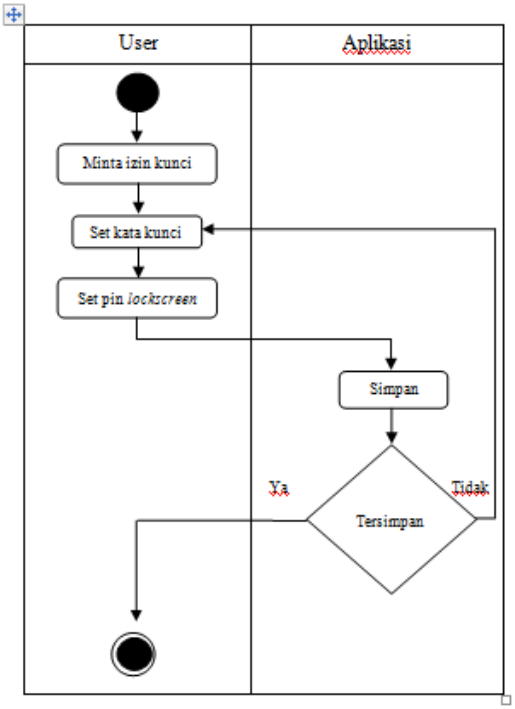
Actor Action	System Respond
1. User mengetik pesan sms dan mengirimkan pesan	Aplikasi akan langsung mengunci *smartphone* ketika sms sudah masuk

Sumber: (Data Olahan)

3.3 *Activity Diagram*

3.3.1 *Activity Diagram Keyword* dan *password*

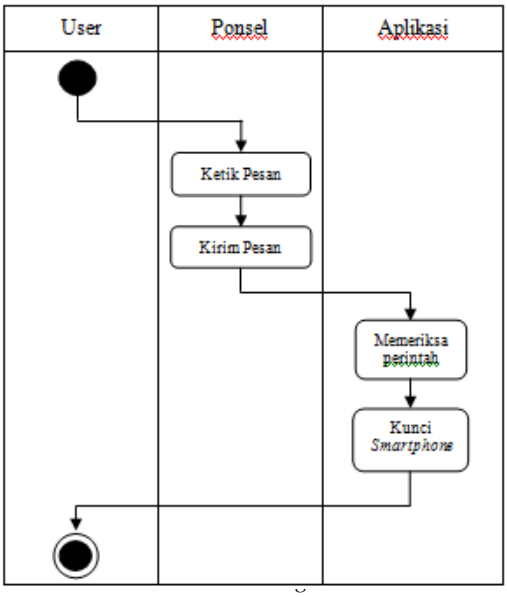
Activity diagram adalah gambaran berbagai alir aktivitas dalam sistem yang sedang dirancang. Dapat dilhat pada Gambar 3.7.



Gambar 3.7 *Usecase Diagram Keyword* dan *password*

3.3.2 *Actuvity Diagram* Kirim Pesan

Activity diagram kirim pesan adalah gamba aliran aktivitas dalam sistem yang sedang dirancang. Dapat dilhat pada Gambar 3.8.



IV. HASIL DAN PENGUJIAN

4.1 Hasil Tampilan Antarmuka

4.1.1 Antar Muka *Icon*

Icon merupakan tahap awal yang digunakan pengguna untuk membuka aplikasi KunciHpSms sehingga aplikasi dapat dibuka dengan *tapping icon* aplikasi KunciHpSms yang telah terinstal pada *device* seperti pada Gambar 4.1.

Gambar 4.1 Antar muka icon

4.1.2 Antar Muka Halaman Utama

Antar muka digunakan untuk menyimpan *keyword* dan kata kunci seperti Gambar 4.2.

Gambar 4.2 Antar Muka Halaman Utama

4.1.3 Antar Muka Halaman Lockscreen

Tampilan *lockscreen* yang telah dibuat terlihat pada Gambar 4.3 merupakan tampilan saat *smartphone* akan terkunci setelah SMS masuk. Disini *user* wajib mengisi *password* yang telah di buat di pada Aplikasi sebelumnya untuk membuka *smartphone*.

Gambar 4.3 Antar muka *lockscreen*

4.2 Hasil Input dan Output

4.2.1 Tampilan Halaman Utama

Antar muka digunakan untuk menyimpan *keyword* dan kata kunci ke dalam memory seperti Gambar 4.4.

Gambar 4.4 Antar Muka Halaman Utama

Tabel 4.1 *Source Code* Halaman Utama

Source Code Halaman Utama

```
    mDevicePolicyManager =
(DevicePolicyManager)getSystemService(Context.DEVICE_POLI
CY_SERVICE);
    mComponentName = new ComponentName(this,
MyAdminReceiver.class);

    keyword = (EditText) findViewById(R.id.editKataKunci);
    pin = (EditText) findViewById(R.id.editPIN);
    tombolAdmin = (Button) findViewById(R.id.btnAdmin);
    tombolAdmin.setOnClickListener(new
View.OnClickListener() {
        @Override
        public void onClick(View view) {
          //cek izin admin
          boolean isAdmin =
mDevicePolicyManager.isAdminActive(mComponentName);
          //kalau sudah aktif
          if (isAdmin) {
            //munculkan notifikasi
            Toast.makeText(getApplicationContext(), "Izin admin
telah aktif", Toast.LENGTH_SHORT).show();
          //kalau belum
          }else{
            //registrasi dulu
            Intent intent = new
Intent(DevicePolicyManager.ACTION_ADD_DEVICE_ADMIN);

intent.putExtra(DevicePolicyManager.EXTRA_DEVICE_ADMIN,
mComponentName);

intent.putExtra(DevicePolicyManager.EXTRA_ADD_EXPLANAT
ION,description);
            startActivityForResult(intent, ADMIN_INTENT);
          }
        }
    });

    tombolBtlAdmin = (Button)
findViewById(R.id.btnBtlAdmin);
    tombolBtlAdmin.setOnClickListener(new
View.OnClickListener() {
        @Override
        public void onClick(View view) {
          //cek izin admin
          boolean isAdmin =
mDevicePolicyManager.isAdminActive(mComponentName);
          //kalau sudah aktif
          if (isAdmin) {
            //cabut izin admin
                        Toast.makeText(getApplicationContext(),
"Izin admin telah dicabut", Toast.LENGTH_SHORT).show();
          //kalau belum
          }else{
            Toast.makeText(getApplicationContext(), "Izin admin
belum aktif", Toast.LENGTH_SHORT).show();
          }
        }
    });

    tombolSimpan = (Button) findViewById(R.id.btnSimpan);
    tombolSimpan.setOnClickListener(new
View.OnClickListener() {
        @Override
        public void onClick(View view) {
          //ambil katakunci yang di input
          String perintah = keyword.getText().toString();
          if(keyword.getText().length() > 0){
            //ambil pin yang di input
            String kunci_pin = pin.getText().toString();
            if(pin.getText().length() > 0){
              //simpan isi katakunci & pin ke memori
              SharedPreferences prefs =
getSharedPreferences("my_prefs", MODE_PRIVATE);
              SharedPreferences.Editor edit = prefs.edit();
              edit.putString("KATAKUNCI", perintah);
              edit.putString("KUNCIPIN", kunci_pin);
```

```
                edit.apply();
                //munculkan nonitifikasi sudah tersimpan ke memori
                Toast.makeText(getApplicationContext(),
"Tersimpan", Toast.LENGTH_SHORT).show();
              }
              else{
                Toast.makeText(getApplicationContext(), "PIN
tidak boleh kosong", Toast.LENGTH_SHORT).show();
              }
            }
            else{
              Toast.makeText(getApplicationContext(), "Keyword
tidak boleh kosong", Toast.LENGTH_SHORT).show();
            }
          }
        });
    }
}
```

4.2.2 Tampilan Halaman *Lockscreen*

Tampilan *lockscreen* merupakan tampilan saat *smartphone* akan terkunci setelah SMS masuk. Seperti Gambar 4.5. dibawah ini

Gambar 4.5 Antar muka *lockscreen*

Tabel 4.2 *Source Code* LockscreenActivity

Source code LockscreenActivity

```
  View.OnClickListener pinButtonHandler = new
View.OnClickListener() {
        public void onClick(View v) {

          if (keyPadLockedFlag == true)
          {
            return;
          }

          Button pressedButton = (Button)v;


          if (userEntered.length()<PIN_LENGTH)
          {
            userEntered = userEntered +
pressedButton.getText();
            Log.v("PinView", "User entered="+userEntered);

            //Update pin boxes

passwordInput.setText(passwordInput.getText().toString()+"*"
);

passwordInput.setSelection(passwordInput.getText().toString().
length());
    if (userEntered.length()==PIN_LENGTH)
      {
    //Check if entered PIN is correct
    //ambil isi katakunci dari memori untuk kunci layar hp
     SharedPreferences bb = getSharedPreferences("my_prefs",
0);
          String userPin = bb.getString("KUNCIPIN", "");


if (userEntered.equals(userPin))
  {
  statusView.setTextColor(Color.GREEN);
  statusView.setText("Correct");
  Log.v("PinView", "Correct PIN");
  finish();
  }
     else
     {
      statusView.setTextColor(Color.RED);
      statusView.setText("Wrong PIN. Keypad Locked");
      keyPadLockedFlag = true;
      Log.v("PinView", "Wrong PIN");

      new LockKeyPadOperation().execute("");
          }
        }
    }
    else
    {
    //Roll over
    passwordInput.setText("");

    userEntered = "";
    statusView.setText("");

    userEntered = userEntered + pressedButton.getText();
    Log.v("PinView", "User entered="+userEntered);

    //Update pin boxes
    passwordInput.setText("8");

          }
        }
    };
    // Lock home button
    public void lockHomeButton() {
      mLockscreenUtils.lock(LockscreenActivity.this);
    }

    private class LockKeyPadOperation extends
  AsyncTask<String, Void, String> {

        @Override
        protected String doInBackground(String... params) {
          for(int i=0;i<2;i++) {
            try {
              Thread.sleep(1000);
            } catch (InterruptedException e) {
              // TODO Auto-generated catch block
              e.printStackTrace();
            }
          }

          return "Executed";
        }

  }
```

4.3 Pengujian

Pengujian aplikasi juga diimplementasikan dengan menggunakan beberapa perangkat *smartphone* dengan sistem operasi Android, dengan hasil implemtasi sebagai berikut :

4.3.1 Pengujian Fungsionalititas Aplikasi

Tabel 4.3 Pengujian Fungsionalititas Aplikasi

No	Item Pengujian	Hasil	Keterangan
1	Minta izin kunci layar	Berhasil	-
2	Simpan	Berhasil	-
3	*Lockscreen*	Berhasil	-
4	Set kata kunci	Berhasil	-
5	Set PIN *lockscreen*	Berhasil	-
6	Masukkan kata kunci	Berhasil	-

4.3.2 Pengujian Sistem

Berikut adalah pengujian menggunakan *smartphone* Samsung J1 ACE :

1. Gunakan dua *smartphone* untuk melakukan pengiriman SMS dan penguncian. Pastikan *smartphone* yang di kunci sudah diroot.
2. Buka aplikasi KunciHpSMS pada *smartphone* yang ingin di kunci.

Gambar 4.6 Aplikasi KunciHpSMS

3. Muncul tampilan seperti gambar dibawah. Masukan kata kunci pada set kata kunci untuk digunakan pada pengiriman SMS dan masukkan pin untuk mengunci layar.

Gambar 4.7 Halaman utama KunciHpSMS

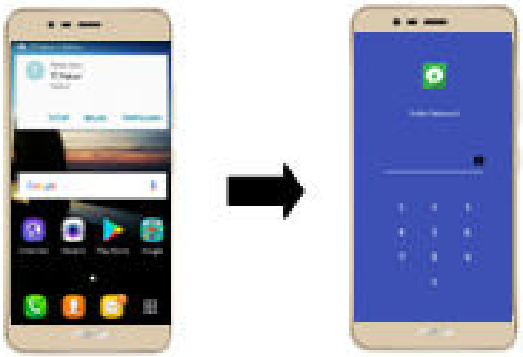
4. Aktikan Minta izin kunci layar untuk pengiriman SMS. Selanjutnya klik tombol simpan untuk melakukan pengiriman SMS

Gambar 4.8 Minta izin KunciHpSMS

5. Siapkan *smartphone* untuk melakukan pengeiriman SMS. Ketik pesan dengan isi kata kunci yang telah di set pada aplikasi KunciHpSMS. Selanjutnya kirim pesan tersebut ke *smartphone* yang di kunci

Gambar 4.9 Kirim pesan

6. Jika pesan sudah masuk, maka *smartphone* akan terkunci.



Gambar 4.10 Pesan masuk

7. Masukkan *password* yang telah di set sebelumnya pada aplikasi. *Password* ini berfungsi untuk membuka *lockscreen.*

Gambar 4.11 Membuka *password*

4.3.3 Pengujian dengan menggunakan *Mobile Android Devices*

Tabel 4.7 Pengujian dengan menggunakan *Mobile Android Devices*

No	Spesifikasi	Versi Android	Ukuran Layar	Root	Hasil
1	CPU 1.25 Ghz RAM 2 GB	Android Versi 5.1 (lolipop)	5.0" Inch	Ya	Aplikasi berjalan dengan baik, tidak ada kendala apapun yang di hadapi
5	CPU 1.8 Ghz RAM 2 GB	Android v7.1 (Marshmello)	5.0 inci		Aplikasi berjalan. Tetapi aplikasi meminta konfirmasi untuk mengunci layar

4.4 Pembahasan

4.4.1 Hasil Uji Coba

Hasil yang didapat setelah melakukan pengujian dengan menggunakan *smartphone* Samsung J1 ACE yaitu aplikasi berjalan jalan dengan baik, penguncian *smartphone* bisa dilakukan menggunakan *short message service* (SMS), untuk tombol *home* dan *recent* sudah bisa terkunci secara otomatis. Sebelum menggunakan aplikasi ini, *smartphone* yang di gunakan sudah dalam keadaan diroot. Jika *smartphone* dalam keadaan belum diroot maka aplikasi ini akan meminta konfirmasi secara terus menerus untuk mengunci layar, konfirmasi ini berupa text dan sudah ada di sistem Android Lollipop, jika menekan tombol Ok maka tombol home dan recent akan terkunci, jika menekan tombol No maka tombol *home* dan *recent* tidak akan terkunci.

4.4.2 Kendala

Kendala yang dihadapi selama melakukan pengujian ini yaitu *smartphone* yang digunakan sudah harus dalam keadaan diroot. Jika *smartphone* tidak root maka aplikasi ini tidak akan berjalan. Aplikasi ini juga tidak bisa berjalan pada *smartphone* Xiaomi.

4.4.3 Kelebihan

Kelebihan yang didapat selama melakukan pengujian ini yaitu Aplikasi ini bisa mengunci *smartphone* dari jarak jauh. Dan Aplikasi juga dapat mengamankan data – data pribadi saat *smartphone* tertinggal atau dibajak.

4.4.4 Kekurangan

Kekurangan yang didapat selama melakukan pengujian ini yaitu Aplikasi ini membaca semua pesan yang masuk, jika pesan mengandung kata kunci dari Aplikasi maka smartphone akan terkunci. Dan Aplikasi tidak bisa berjalan pada *smartphone* Xiaomi.

V. KESIMPULAN

5.1 Kesimpulan

Adapun kesimpulan yang didapat setelah melakukan penelitian ini adalah menghasilkan sebuah aplikasi keamanan *Smartphone* berbasis Android menggunakan *Short Message Service*. Dilakukan pengujian untuk mengetahui sistem yang dibuat berjalan dengan baik, adapun hasil yang didapat setelah pengujian adalah penguncian *smartphone* bisa dilakukan menggunakan *short message service* (SMS) dimana saja dan kapan saja asalkan kata kunci yang *set* di aplikasi sesuai dengan yang di ketik pada pesan SMS.

5.2 Saran

Adapun saran yang dapat dikembangkan setelah melakukan pengujian aplikasi adalah sebagai berikut:

1. Untuk penelitian selanjutnya diharapkan untuk memakai Aplikasi ini *smartphone* yang digunakan tidak perlu diroot.
2. Untuk penelitian selanjutnya diharapkan Aplikasi ini sudah tidak membaca semua pesan yang masuk, jika pesan yang masuk mengandung kata kunci dari Aplikasi maka smartphone akan terkunci.
3. Untuk penelitian selanjutnya diharapkan Aplikasi ini sudah bisa digunakan pada *smartphone* Xiaomi.
4. Untuk penelitian selanjutnya diharapkan Aplikasi ini sudah bisa memakai *password* gabungan (abjad, angka, simbol).

VI. REFERENSI

[1] Arif, F, I, 2013, *Sistem Keamanan Pesan Pada Androidgingerbread (2.3.4) Dengan Algoritma Luc.* Skripsi. Fakultas Matematika dan Ilmu Pengetahuan Alam. Universitas Jember, Jember.

[2] Harry, A., dan Gunadhi, E., 2015, Keamanan Komunikasi Data Sms Pada Android Dengan Menggunakan Aplikasi Kriptograpi Advance Encryption Standard (AES), *Jurnal Algoritma, (12)* 1, 1 – 6.

[3] Andi, W., dan Bintang, M, D., 2013 – 2014, Aplikasi Screen Lock pada Smartphone Menggunakan

Identifikasi Wajah dengan Menerapkan Pointwise, *Jurnal Teknik Informatika, (1)* 1, 1 – 14.

[4] Mohini, T., dkk., 2013, Review on Android and Smartphone Security, *Journal of Computer and Information Technology Sciences,* 2320 – 6527.

[5] Sharen, G., dan Iis, N, K., 2015, Intensitas Penggunaan Smartphone Terhadap Perilaku Komunikasi, *Jurnal Sosioteknologi, (14*) 2, 170 -178.

[6] Ali, I., 2011, Pengembangan Sistem Informasi Monitoring Tugas Akhir Berbasis Short Message Service (SMS) Gateway di Fasilkom Unsri, *Jurnal Sistem Informasi, (1)* 1, 81 – 92.