

**DROIDVOTE, APLIKASI E-VOTING MENGGUNAKAN ALGORITMA
KRIPTOGRAFI BERBASIS SISTEM OPERASI ANDROID**

SKRIPSI



Disusun Oleh :
WAHYU EKOPRADONO
08.18.050

PROGRAM STUDI TEKNIK INFORMATIKA S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2013

LEMBAR PERSETUJUAN

**DROIDVOTE, APLIKASI E-VOTING MENGGUNAKAN ALGORITMA
KRIPTOGRAFI BERBASIS SISTEM OPERASI ANDROID**

SKRIPSI

Disusun dan diajukan untuk melengkapi dan memenuhi persyaratan
guna mencapai gelar Sarjana Komputer

Disusun Oleh :

WAHYU EKOPRADONO

08.18.050

Diperiksa dan disetujui,

Dosen Pembimbing I



Dr. Ir. Daval Gustopo S. MT

NIP. 103940264

Dosen Pembimbing II



Mira Orisa, ST

NIP. P. 1031000435

Mengetahui

Ketua Program Studi Teknik Informatika S-1



Joseph Dedy Irawan, ST, MT

NIP. 197404162005011022

**PROGRAM STUDI TEKNIK INFORMATIKA S1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG**

2013

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini, Saya :

Nama : Wahyu Ekopradono

NIM : 08.18.050

Program Studi : Teknik Informatika S-1, Institut Teknologi Nasional Malang

Menyatakan dengan sebenar – benarnya bahwa skripsi Saya yang berjudul :

**“ DROIDVOTE, APLIKASI E-VOTING MENGGUNAKAN ALGORITMA
KRIPTOGRAFI BERBASIS SISTEM OPERASI ANDROID “**

ini seluruhnya benar – benar merupakan hasil karya sendiri, bukan merupakan pengambilalihan tulisan atau pemikiran orang lain kecuali sumber landasan teori sebagai penunjang penulisan yang telah dituliskan sebagaimana mestinya di akhir penulisan skripsi ini. Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan skripsi ini merupakan hasil karya orang lain, Saya bersedia menerima sanksi yang seberat – beratnya atas perbuatan yang tidak terpuji tersebut.

Malang, 8 Maret 2013

Yang membuat pernyataan



Wahyu Ekopradono

(08.180.50)

**DROIDVOTE, APLIKASI E-VOTING MENGGUNAKAN ALGORITMA
KRIPTOGRAFI BERBASIS SISTEM OPERASI ANDROID**

Wahyu Ekopradono (08.18.050)

Teknik Informatika ITN Malang, donz88green@gmail.com

Abstrak

Electronic voting atau yang lebih sering disebut dengan e-voting merupakan hasil pengembangan dari model voting (pemungutan suara) konvensional. Aplikasi e-voting ini dikembangkan di lingkup Pemilukada Provinsi dan dalam versi aplikasi Android. Untuk dapat menggunakan aplikasi e-voting ini pengguna harus memasukkan NIK, username dan password sebagai kunci untuk mendapatkan hak akses kedalam aplikasi. Password merupakan salah satu kunci penting yang harus dijaga kerahasiaannya oleh sebab itu maka pada aplikasi ini password yang dihasilkan harus melalui proses enkripsi data dan dekripsi data. Proses enkripsi dan dekripsi tersebut dirancang menggunakan algoritma kriptografi yang merupakan algoritma umum dalam proses penyandian.

Kesimpulan dari pengembangan aplikasi ini adalah masyarakat dimudahkan dalam proses pemungutan suara dan pemerintah memiliki alternatif lain dalam proses pemungutan suara yang digunakan untuk skala besar. Begitu juga dalam segi efektifitas, aplikasi ini sangat efektif karena output yang dihasilkan cepat, akurat dan tepat serta hasil voting yang keluar merupakan data real yang terjamin keasliannya karena semua pengolahan data dilakukan oleh sistem yang terstruktur.

Kata kunci : e-voting, android, kriptografi, enkripsi, dekripsi

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT atas rahmat dan nikmat-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi ini yang berjudul “Droidvote, Aplikasi E-Voting Menggunakan Algoritma Kriptografi Berbasis Sistem Operasi Android”. Dalam penyusunan skripsi ini, penulis banyak mendapatkan bimbingan dan bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini tidak lupa penulis menyampaikan terimakasih yang sebesar – besarnya kepada :

1. Ir. Soeparno Djiwo, MT, Rektor Institut Teknologi Nasional Malang.
2. Ir. Anang Subardi, MT, Dekan Fakultas Teknologi Industri Institut Teknologi Nasional Malang
3. Joseph Dedy Irawan, ST, MT, Ketua Program Studi Teknik Informatika Institut Teknologi Nasional Malang.
4. Dr. Ir. Dayal Gustopo S, MT, Dosen Pembimbing I yang telah memberikan motivasi, pengarahan, saran dan koreksi dalam penyusunan skripsi ini.
5. Mira Orisa, ST, Dosen Pembimbing II yang telah memberikan motivasi, pengarahan, saran dan koreksi dalam penyusunan skripsi ini.
6. Semua pihak yang tidak dapat penulis sebutkan satu persatu di sini, yang telah membantu dalam penyelesaian skripsi ini.

Semoga semua bantuan yang telah diberikan bermanfaat bagi penulis serta menjadi amal di sisi Allah SWT. Akhirnya penulis berharap semoga skripsi ini bermanfaat dalam menunjang perkembangan IPTEK dan bermanfaat bagi yang membacanya khususnya dalam lingkup teknologi informasi.

Malang, 16 Februari 2013

Penulis

Wahyu Ekopradono

DAFTAR ISI

LEMBAR PERSETUJUAN	i
LEMBAR PERNYATAAN	ii
ABSTRAK	iii
KATA PENGANTAR	iv
DAFTAR ISI	v
DAFTAR GAMBAR	viii
DAFTAR TABEL	x
DAFTAR LAMPIRAN	xi
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Tujuan Pembuatan Aplikasi	3
1.4. Manfaat Pembuatan Aplikasi	3
1.5. Batasan Masalah	3
1.6. Sistematika Penulisan	4
BAB II LANDASAN TEORI	5
2.1. Electronic Voting (e-voting)	5
2.1.1. Pengertian Elektronik Voting	5
2.1.2. Implementasi Sistem Electronic Voting	6
2.1.3. Arsitektur Sistem Electronic Voting	7
2.1.4. Teknik Pengiriman Electronic Voting	8
2.2. Kriptografi	11
2.2.1. Pengertian Algoritma Kriptografi	11

2.2.2. Algoritma Kriptografi	12
2.3. Java	14
2.3.1. Kelebihan Bahasa Pemrograman Java	15
2.3.2. Kekurangan Bahasa Pemrograman Java	15
2.3.3. Komponen Java	16
2.4. XML	17
2.5. PHP	19
2.6. Database MySQL	20
2.6.1. Integrasi MySQL Dengan PHP	21
2.7. Eclipse	22
2.7.1. Sejarah ECLIPSE	23
2.7.2. Arsitektur ECLIPSE	23
2.7.3. Versi ECLIPSE	24
2.8. Android	24
2.8.1. Pengertian Android	24
2.8.2. Fitur Sistem Operasi Android	25
2.8.3. Arsitektur Sistem Operasi Android	27
2.8.4. Activity Lifecycle	31
2.8.5. Versi Sistem Operasi Android	32
BAB III PERANCANGAN DAN ANALISA SISTEM	33
3.1 Analisa Sistem	33
3.2 Hak Akses	33
3.3 Perancangan Algoritma Kriptografi	34
3.4 Context Diagram (Diagram Konteks)	37
3.5 Data Flow Diagram (DFD) I level 1	38

3.6 Rancangan Database	39
3.7 Desain Layout	41
3.8 Block Diagram	49
3.9 Flowchart	50
BAB IV IMPLEMENTASI DAN PENGUJIAN	52
4.1 Implementasi	52
4.1.1 Lingkungan Pengembangan	52
4.1.2 Batasan Implementasi	52
4.1.3 Implementasi File	52
4.1.4 Implementasi User Interface	54
4.2 Pengujian	65
4.2.1 Tujuan Pengujian	65
4.2.2 Lingkungan Pengujian	65
4.2.2.1. Spesifikasi Perangkat Keras	65
4.2.2.2. Spesifikasi Perangkat Lunak	66
4.2.3 Hasil Pengujian	66
4.2.3.1. Pengujian Aplikasi Fungsional Sistem	66
4.2.3.2. Pengujian Algoritma Kriptografi Sistem	67
BAB V KESIMPULAN DAN SARAN	69
5.1 Kesimpulan	69
5.2 Saran	69
DAFTAR PUSTAKA	70
LAMPIRAN	72

DAFTAR GAMBAR

Gambar 2.1 Client – Server (Mobile App)	6
Gambar 2.2 Arsitektur Sistem Electronic Voting	7
Gambar 2.3 Teknik Pengiriman E-Voting	9
Gambar 2.4 Alur Algoritma Simetrik	13
Gambar 2.5 Alur Algoritma Asimetrik	13
Gambar 2.6 Hubungan JVM, JRE dan JDK	17
Gambar 2.7 Tampilan Antar Muka Eclipse	22
Gambar 2.8 Arsitektur Sistem Operasi Android	28
Gambar 2.9 Android Activity Lifecycle	31
Gambar 3.1 Flowchart Kriptografi (Enkripsi – Dekripsi).....	35
Gambar 3.2 Diagram Konteks	37
Gambar 3.3 DFD Level 1 Aplikasi Droidvote	38
Gambar 3.4 Layout Halaman Login	42
Gambar 3.5 Layout Halaman Administrator	42
Gambar 3.6 Layout Halaman Data Pemilih	43
Gambar 3.7 Layout Halaman Data Calon Kepala Daerah	43
Gambar 3.8 Layout Halaman Tambah Data Pemilih	44
Gambar 3.9 Layout Halaman Data Pemilih (KPUD)	45
Gambar 3.10 Layout Halaman Data Calon Kepala Daerah (KPUD)	45
Gambar 3.11 Layout Autentikasi	46
Gambar 3.12 Layout Menu	47
Gambar 3.13 Layout Daftar Kandidat	47
Gambar 3.14 Layout Informasi Kandidat	48

Gambar 3.15 Layout Last Vote	48
Gambar 3.16 Layout Informasi Akun Pemilih	49
Gambar 3.17 Block Diagram	49
Gambar 3.18 Flowchart Aplikasi DroidVote	50
Gambar 4.1 Form Authentication	55
Gambar 4.2 Notifikasi Data Valid	55
Gambar 4.3 Notifikasi Data Tidak Valid	55
Gambar 4.4 Tampilan List Menu	56
Gambar 4.5 Tampilan List Kandidat	57
Gambar 4.6 Tampilan Detail Kandidat	57
Gambar 4.7 Alert Dialog Vote	58
Gambar 4.8 Tampilan List Menu Setelah Voting	58
Gambar 4.9 Tampilan Menu Hasil Vote	59
Gambar 4.10 Tampilan Menu Informasi Pemilih	60
Gambar 4.11 Alert Dialog Menu Keluar	60
Gambar 4.12 Form Login	61
Gambar 4.13 Halaman Administrasi ADMIN.....	61
Gambar 4.14 Halaman Data Pemilih (Administrator)	62
Gambar 4.15 Halaman Data Kandidat (Administrator)	62
Gambar 4.16 Halaman Tambah Data	63
Gambar 4.17 Halaman Administrasi KPUD	63
Gambar 4.18 Halaman Data Pemilih (Pejabat KPUD).....	64
Gambar 4.19 Halaman Data Kandidat (Pejabat KPUD)	65

DAFTAR TABEL

Tabel 3.1 Tabel User	40
Tabel 3.2 Tabel Pemilih	40
Tabel 3.3 Tabel Kandidat	41
Tabel 4.1 File Pembangun Aplikasi Client	53
Tabel 4.2 File Pembangun Aplikasi Server	53
Tabel 4.3 Hasil Pengujian Fungsional Sistem	66
Tabel 4.4 Hasil Pengujian Algoritma Kriptografi Sistem	67

BAB I

PENDAHULUAN

1.1. Latar Belakang

Pemilihan umum merupakan bagian pada suatu proses demokrasi. Indonesia adalah salah satu negara demokrasi yang melaksanakan pemilihan umum setiap lima tahun sekali. Di Indonesia, salah satu contoh pelaksanaan pemilihan umum dilakukan pada tingkat propinsi, pada tingkat ini proses pemungutan suara digunakan untuk pemilihan gubernur dan calon gubernur. Pemilihan umum di Indonesia masih dilakukan secara manual. Warga yang mempunyai hak pilih datang ke tempat pemungutan suara pada saat hari pemilihan. Mereka kemudian mencontreng (v) kertas suara. Setelah proses pemungutan suara selesai, kemudian dilakukan penghitungan suara^[1].

Electronic voting adalah suatu metode pemungutan suara dan penghitungan suara menggunakan perangkat elektronik bisa berupa aplikasi desktop, aplikasi smartphone dan aplikasi website. Tujuan dibangunnya sistem pemungutan suara menggunakan *electronic voting* adalah menyelenggarakan pemungutan suara dengan biaya yang lebih hemat tanpa harus mengalokasikan dana untuk keperluan biaya percetakan surat suara, bisa dilihat contoh pada pemilu pada Jawa Timur pada Putaran I tahun 2008^[9], untuk pencetakan suara saja menghabiskan dana sebesar Rp 16.871.155.851 yang dipasrahkan ke PT Temprina Media Grafika sebagai pihak pemenang tender, Kemudian juga sistem pemungutan suara yang lebih sederhana, penghitungan suara yang lebih cepat, efisien dan akurat dengan menggunakan sistem yang aman dan mudah untuk dilakukan audit oleh admin serta peralatan (hardware dan software) yang dapat digunakan berulang kali merupakan tujuan inti dibangunnya sistem *e-voting* ini.

Dengan semakin berkembangnya teknologi informasi serta semakin tingginya efisiensi dan efektifitas penggunaan smartphone oleh masyarakat luas maka

penerapan sistem *e-voting* pada *smartphone* diharapkan bisa memberikan trobosan baru bagi sistem pemungutan suara di negara kita, Android merupakan sistem operasi *open source* untuk *smartphone* dan tablet yang berkembang sangat pesat saat ini. Secara tidak langsung penggunaannya merupakan suatu bentuk dukungan user bagi pengembangan berbagai macam aplikasi penunjang kebutuhan user sendiri, inilah salah satu alasan penerapan *e-voting* pada sistem operasi Android yang diharapkan semakin memudahkan penggunaannya untuk melakukan *voting* dalam lingkup PEMILUKADA sehingga bisa dikembangkan penggunaannya dalam lingkup yang lebih luas yaitu Pemilu.

Algoritma adalah urutan tahapan yang menentukan operasi – operasi tertentu yang diperlukan untuk menyelesaikan suatu masalah atau mengerjakan suatu perintah tertentu. Perintah – perintah ini dapat diterjemahkan secara bertahap dari awal hingga akhir. Algoritma kriptografi merupakan fungsi matematika yang digunakan untuk proses enkripsi dan dekripsi, yaitu langkah-langkah atau tahapan dalam melakukan proses perubahan teks terang menjadi teks sandi atau teks sandi menjadi teks terang, untuk melakukan kedua proses tersebut biasanya harus melakukan input kunci *public* dan kunci *private* agar data dapat terenkripsi dan terdekripsi dengan benar. Dalam aplikasi *e-voting* ini kunci untuk perubahan teks terang menjadi teks sandi (enkripsi) ataupun teks sandi menjadi teks terang (dekripsi) tidak perlu diinputkan karena sudah dideklarasikan dalam *source code* pembangun aplikasi, jadi enkripsi data dan dekripsi data bisa terjadi secara otomatis.

Dari uraian diatas selain sebagai judul pengerjaan skripsi dan mengikuti perkembangan dunia teknologi informasi khususnya dalam pengembangan aplikasi *e-voting* yang berbasis android sebagai metode lain sistem pemungutan suara, tetapi juga bertujuan untuk memajukan kinerja pemerintah dalam bidang teknologi informasi. Sehingga diperoleh output yang cepat, akurat dan tepat serta hasil *voting* yang keluar merupakan data real yang terjamin keasliannya karena semua pengolahan data dilakukan oleh sistem yang terstruktur.

1.2. Rumusan Masalah

Berdasarakan uraian pada latar belakang diatas, maka perumusan masalah pada skripsi ini dapat dirumuskan “ Bagaimana merancang serta membangun sebuah aplikasi *e-voting* berbasis pada sistem operasi Android untuk digunakan dalam proses pemungutan suara dalam lingkup Pemilukada yang didalamnya menggunakan algoritma kriptografi sebagai sistem pengamanan datanya ? ”

1.3. Tujuan Pembuatan Aplikasi

Tujuan dari skripsi ini adalah dapat merancang serta membangun sebuah aplikasi *e-voting* berbasis pada sistem operasi Android untuk digunakan dalam proses pemungutan suara dalam lingkup Pemilukada yang didalamnya menggunakan algoritma kriptografi sebagai sistem pengamanan datanya.

1.4. Manfaat Pembuatan Aplikasi

Manfaat yang dapat diperoleh dari pembuatan aplikasi *e-voting* ini adalah

- a. memberikan layanan dan fasilitas voting (pemungutan suara) secara lebih mudah dan efisien yang dapat dilakukan di TPS manapun tidak harus di TPS di wilayah dimana kita tinggal.
- b. Memperkenalkan sistem pemungutan suara berbasis teknologi informasi.
- c. Membuat sistem pengamanan data berbasis pada algoritma kriptografi.
- d. Mengangkat nama institusi pemerintahan dan memajukan kinerja pemerintah dalam bidang teknologi informasi.

1.5. Batasan Masalah

Batasan – batasan masalah yang digunakan dalam skripsi ini adalah :

- a. Data – data warga berupa identitas KTP aktif.
- b. Interaksi antara program dan user dengan meinputkan *NIK (Nomor Induk Kependudukan)* KTP aktif, username dan password sebagai hak akses untuk proses pencocokan atau autentifikasi.
- c. Pemungutan suara dilakukan dalam lingkup PEMILUKADA.
- d. Pembangunan aplikasi berbasis Android menggunakan software Eclipse.

- e. Output berupa hasil voting yang bisa diakses secara live report via web based ataupun mobile based dan laporan audit hasil perolehan suara yang dilakukan oleh admin.
- f. Penyimpanan data – data penunjang aplikasi menggunakan database MySQL (client-server).
- g. Bahasa pemrograman yang digunakan JAVA, XML, HTML dan PHP.

1.6. Sistematika Penulisan

Untuk mempermudah dan memahami pembahasan penulisan skripsi ini, maka sistematika penulisan disusun sebagai berikut :

Bab I : Pendahuluan

Berisi Latar Belakang, Rumusan Masalah, Tujuan dan manfaat Penelitian, Pembatasan Permasalahan dan Sistematika Penulisan.

Bab II : Landasan Teori

Berisi teori-teori yang didapat dari studi literatur dan konsep-konsep yang terkait dengan skripsi ini, beserta dengan penyelesaian masalah yang diambil dalam penyusunan skripsi.

Bab III : Perancangan dan Analisa Sistem

Dalam bab ini berisi mengenai analisa dan perancangan dari sistem yang akan dibangun meliputi analisis sistem, komponen e-voting berbasis android, rancangan basis data dan perancangan antarmuka

Bab IV : Implementasi dan Pengujian

Berisi tentang cara menjalankan aplikasi serta uji coba dari program yang telah dibuat tersebut.

Bab V : Penutup

Merupakan bab terakhir yang memuat intisari dari hasil pembahasan yang berisikan kesimpulan dan saran yang dapat digunakan sebagai pertimbangan untuk pengembangan penulisan selanjutnya.

BAB II

LANDASAN TEORI

Pada bab ini akan dijelaskan mengenai teori-teori yang berhubungan dengan studi kasus ini, sehingga dapat dijadikan sebagai landasan berpikir dan akan mempermudah dalam hal pembahasan hasil utama pada bab berikutnya. Adapun teori-teori tersebut mencakup pengertian *E-voting*, *Algoritma Kriptografi*, *Java*, *XML*, *HTML PHP*, *DatabaseMySQL*, *Eclipse*, dan *Android*.

2.1. Electronic Voting (*e-voting*).

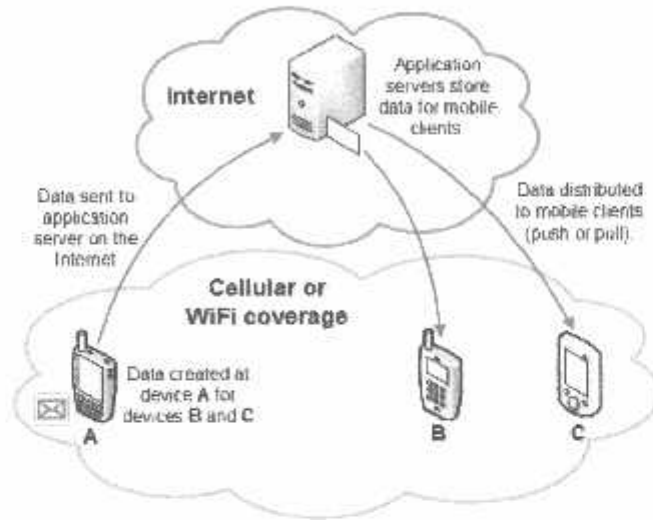
2.1.1. Pengertian Electronic Voting

Seiring dengan perkembangan jaman, sudah banyak penelitian pemanfaatan elektronik pada proses pemungutan suara menggantikan proses pemungutan suara secara manual. *E-voting* adalah proses pemungutan suara yang memanfaatkan elektronik. Penelitian mengenai *e-voting* telah berlangsung cukup lama. Sebagai contoh, pada 1 Juni 1869 Thomas A. Edison menerima paten dari pemerintah Amerika untuk sebuah "*electronic vote recorder*" yang akan digunakan pada Kongres, tetapi teknologi tersebut tidak pernah digunakan karena anggota Kongres belum siap untuk menggunakannya^[15].

Pada tahun 1970 dikenalkan kembali dengan sebutan teknologi pencatatan langsung secara elektronik atau lebih dikenal dengan istilah DRE (*direct recording electronic*). Cara memilih dengan sistem ini adalah dengan memilih kandidat yang sudah tercetak pada layar komputer atau gadget. Untuk berinteraksi, pemilih hanya perlu menekan tombol yang ada di layar komputer atau gadget. Cara kerja dari sistem *e-voting* adalah dengan menekan tombol vote, suara pemilih langsung disimpan pada suatu piranti memori atau pada sirkuit memori *non volatile*^[5].

E-voting ini merupakan aplikasi *client-server* yang melakukan tugasnya di dua sisi yaitu *client* dan *server*, sehingga komunikasi data harus tetap terjaga dengan baik agar tidak ada aktifitas yang terhenti dan akhirnya mengakibatkan sistem tidak

berjalan dengan baik. Seperti yang diilustrasikan dengan aplikasi *mobile* pada Gambar 2.2 dibawah ini.



Gambar 2.1 Client Server (Mobile App)

2.1.2. Implementasi Sistem Electronic Voting ^[15]

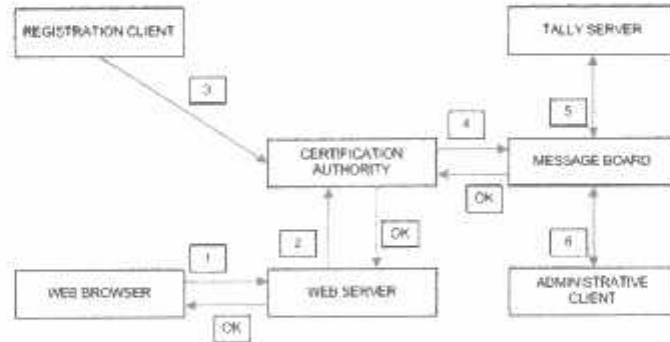
Untuk mengimplementasikan sebuah sistem *e-voting* ada beberapa syarat yang harus dipenuhi. Berikut ini beberapa persyaratan yang harus dipenuhi dalam suatu sistem *e-voting*.

1. **Accuracy (akurasi)** yaitu ketepatan hasil perhitungan suara. Ketepatan ini meliputi tidak ada satupun pihak yang diperbolehkan mengubah suara yang telah masuk, semua suara yang valid dihitung dengan tepat, dan suara yang tidak valid tidak boleh dihitung.
2. **Democracy (demokrasi)** yaitu hanya calon pemilih yang memenuhi syarat yang berhak untuk memilih dan setiap pemilih hanya berhak untuk memasukkan suaranya satu kali.
3. **Privacy (privasi)** yaitu tidak seorang pun yang dapat menghubungkan seseorang dengan hasil pilihannya.
4. **Robustness** yaitu tidak ada gangguan yang menghalangi pelaksanaan pemungutan suara. Jadi aspek ini berkaitan erat dengan aspek *security* (keamanan).

5. *Verifiability* yaitu setiap orang dapat membuktikan bahwa tidak ada manipulasi terhadap hasil perhitungan.
6. *Uncoercibility* yaitu tidak adanya paksaan kepada pemilih dalam menentukan pilihannya. Agar tidak terjadi maka pemilih harus tidak dapat membuktikan hasil pilihannya kepada orang lain (*receipt freeness*).
7. *Fairness* yaitu setiap orang tidak dapat mengetahui hasil pemilihan sebelum proses pemilihan selesai dan dilakukan perhitungan suara.
8. *Verifiable participation* yaitu mampu membuktikan apakah seseorang telah melakukan pemungutan suara atau belum.

2.1.3. Arsitektur Sistem Electronic Voting

Sistem *e-voting* mempunyai kelebihan mengenai banyaknya pilihan arsitektur sistem yang bisa digunakan. Misalnya, proses penanganan otentikasi calon pemilih ada banyak alternatif yang bisa digunakan, alternatif tersebut antara lain otentikasi dengan satu *password*, otentikasi dengan dua *password*, otentikasi menggunakan kartu *chip*, dan lain-lain. Model aplikasi yang digunakan dalam pembuatan skripsi ini adalah sebuah aplikasi *mobile* dengan bentuk umum arsitektur sistem *e-voting*. Gambar 2.2 adalah contoh model arsitektur umum sistem *e-voting*.



Gambar 2.2 Arsitektur Sistem Electronic Voting

Berikut ini adalah penjelasan setiap komponen dari Gambar 2.1 :

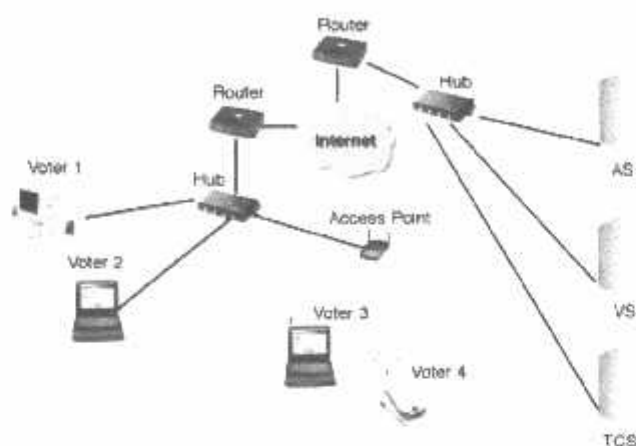
1. *Web browser* adalah aplikasi untuk mengakses *web server* yang berisi aplikasi *evoting*. Jadi *web browser* menjadi suatu *e-voting front end* yang berinteraksi langsung dengan pemilih.
2. *Web server* adalah aplikasi di sisi *server* yang mengelola aplikasi *e-voting* yang akan diakses oleh pemilih menggunakan *web browser*.
3. *Certification Authority (CA)* adalah modul yang berfungsi untuk memeriksa apakah calon pemilih mempunyai hak akses memilih atau tidak.
4. *Registration client* berisi daftar calon pemilih. Daftar calon pemilih tersebut akan dimasukkan ke modul *CA* dan modul *Message board* untuk membuktikan apakah calon pemilih yang masuk tersebut telah terdaftar atau belum.
5. *Message board* adalah bagian *server* yang berfungsi untuk mengumpulkan dan menghitung suara yang telah masuk.
6. *Tally server* adalah bagian *server* untuk melakukan dekripsi terhadap hasil pemungutan suara setelah proses pemungutan suara selesai dilakukan.
7. *Administrative client* adalah komputer *client* untuk kegiatan administratif yang hanya digunakan apabila kegiatan administratif tersebut tidak dilakukan otomatis pada *Message board*. Kegiatan administratif tersebut antara lain perhitungan suara manual, pemeriksaan daftar pemilih, dan pemeriksaan daftar suara yang masuk.

Dengan bentuk arsitektur umum tersebut, diharapkan akan mudah untuk mengembangkan aplikasi serupa yang tidak selalu berbasis pada *web browser* sebagai *front end* nya, yaitu dengan mengembangkan aplikasi *e-voting* yang berbasis pada *mobile application*.

2.1.4. Teknik Pengiriman Electronic Voting

Saat ini penggunaan *mobile Smartphone* sebagai sarana pengiriman data cukup meningkat drastis, semakin banyaknya minat dari para penggunanya maka semakin berkembang pesat pula aplikasi – aplikasi penunjang kebutuhan para penggunanya. Dalam penyusunan skripsi ini *E-voting* mencoba dikembangkan dengan platform *mobile application* karena pada dasarnya pengiriman data *E-voting*

dapat dilakukan dengan berbagai perangkat elektronik yang sudah ada. Seperti contoh dibawah ini. Dalam Gambar 2.2 adalah ilustrasi pengiriman data dari sistem *e-voting* dengan sarana *multiplatform* (berbagai *device*).



Gambar 2.3 Teknik Pengiriman E-Voting

Seperti yang diilustrasikan dalam Gambar 2.3, aplikasi e-voting memerlukan berbagai komponen pendukung antara lain:

1. Multiplatform Devices

Perangkat yang digunakan oleh pengguna untuk melakukan proses voting. Pengguna juga bisa melihat informasi tentang dirinya dan data para calon kandidat. Informasi diberikan dalam bentuk Gambar dan text. *Devices* bisa berupa Mobile Smartphone, Notebook dan PC.

2. Communication Network

Komponen ini membutuhkan jaringan *internet* sebagai media pendukung pengiriman data yang nantinya digunakan untuk proses autentikasi data pengguna dan media penyimpanan suara pengguna dari perangkat elektronik ke database yang ada di web server. Kemudian informasi akan dikirimkan ke pengguna apakah data yang diautentikasi tadi benar atau tidak dan apakah suara yang telah digunakan tadi telah tersimpan di server atau belum. *Communication network* dapat berupa jaringan seluler (GSM, CDMA), Wireless Local Area Network (WLAN), atau Wireless Wide Area Network (WWAN).

3. *Web Server*

Disinilah semua data pembangun dan penunjang aplikasi ditempatkan. Web server disini dibagi menjadi dua, database server dan aplikasi server. Di dalam database server semua data pengguna dan kandidat calon kepala daerah disimpan sedangkan di dalam aplikasi server semua *resource* pembangun aplikasi ditanam, melalui *resource* tersebut proses penyimpanan suara pengguna dan proses autentikasi data pengguna terjadi secara otomatis.

Agar pengguna bisa menggunakan aplikasi dan menggunakan hak aksesnya terhadap aplikasi ini, maka terlebih dahulu diperlukan informasi mengenai data diri pengguna. Untuk mengetahui informasi tersebut dilakukan proses autentikasi data pengguna oleh sistem, pengguna memasukkan data berupa NIK aktif, username dan password yang kemudian akan dicocokkan ke server melalui jaringan komunikasi. Melalui jaringan komunikasi, informasi tersebut diteruskan ke jaringan internet untuk selanjutnya dihubungkan dengan *data server* untuk mendapatkan hak akses bagi pengguna. Selanjutnya informasi yang telah dioalah dan diambil dari data server tadi dikirim kembali ke pengguna melalui jaringan internet dan jaringan komunikasi. Pada akhirnya pengguna dapat menerima informasi seperti apa yang diinginkan.

Ada empat informasi yang dibutuhkan oleh pengguna dalam aplikasi *e-voting* ini, yaitu:

1. Mengetahui apakah data yang diinputkan yang berupa NIK, username dan *password* tadi *valid* atau tidak.
2. Mendapatkan informasi kandidat berupa no.urut kandidat, nama pasangan kandidat, visi misi kandidat, sehingga pengguna dapat memilih kandidat yang sesuai dengan pilihan hatinya.
3. Mendapatkan info update terbaru jumlah perolehan suara tiap kandidat yang mendaftar.
4. Mendapatkan informasi bahwa pengguna telah melakukan *vote*.

2.2. Kriptografi

2.2.1. Pengertian Kriptografi ^[8].

Kriptografi (*cryptography*) berasal dari Bahasa Yunani yaitu cryptos yang berarti secret yaitu rahasia dan graphein artinya writing yaitu tulisan. Sehingga kriptografi berarti secret writing yaitu tulisan rahasia. Menurut Schneier, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Sedangkan menurut Menezes, kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1. Kerahasiaan (*confidentiality*)

Merupakan layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak - pihak yang tidak berhak.

2. Integritas Data (*integrity*)

Merupakan layanan yang menjamin bahwa pesan masih utuh/asli atau belum pernah dimanipulasi selama pengiriman.

3. Otentikasi (*authentication*)

Merupakan layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak – pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*).

4. Nir Penyangkalan (*non repudiation*)

Merupakan layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.2.2. Algoritma Kriptografi

Dalam matematika dan komputasi, algoritma merupakan kumpulan perintah untuk menyelesaikan suatu masalah. Perintah-perintah ini dapat diterjemahkan secara bertahap dari awal hingga akhir. Algoritma kriptografi diartikan sebagai langkah-langkah untuk mengubah teks terang menjadi teks sandi ataupun sebaliknya. Secara umum algoritma kriptografi terbagi menjadi dua yaitu :

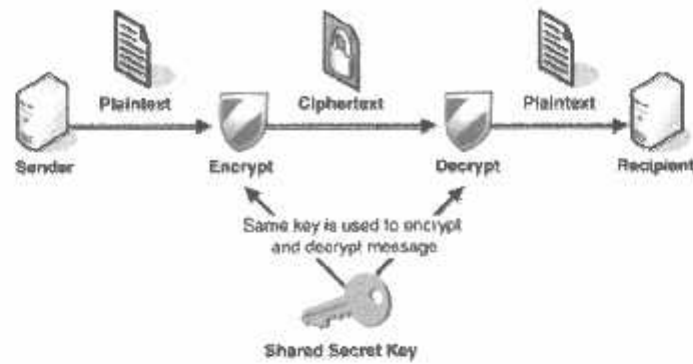
1. Algoritma Enkripsi / Dekripsi

Algoritma enkripsi /dekripsi adalah langkah – langkah atau tahapan untuk melakukan proses perubahan teks terang menjadi teks sandi (enkripsi) atau sebaliknya (dekripsi). Dalam proses ini kunci merupakan input yang harus diberikan selain teks terang (*plaintext*) dan sandi (*chipertext*). Sehingga kunci ini harus dijaga agar tidak jatuh kepihak yang tidak berkepentingan. Berdasarkan kunci, algoritma enkripsi dibagi menjadi dua,yaitu :

a. Algoritma Kunci Simetrik (*Symmetric Key Algorithm*)

Merupakan algoritma enkripsi dimana input kunci untuk enkripsi dan dekripsi sama, seperti yang diilustrasikan pada Gambar 2.4. Skema ini berdasarkan jumlah data per proses dan alur pengolahan data didalamnya dibedakan menjadi dua kelas, yaitu *block-cipher* dan *stream-cipher*.

- *Block-Chiper* adalah skema algoritma sandi yang akan membagi - bagi teks terang yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t , dan setiap blok dienkripsi dengan menggunakan kunci yang sama. Pada umumnya, block-cipher memproses teks terang dengan blok yang relatif panjang lebih dari 64 bit, untuk mempersulit penggunaan pola – pola serangan yang ada untuk membongkar kunci.
- *Stream-Chiper* adalah algoritma sandi yang mengenkripsi data persatuan data, seperti bit, byte, nibble atau per lima bit (saat data yang di enkripsi berupa data Boudout). Setiap mengenkripsi satu satuan data digunakan kunci yang merupakan hasil pembangkitan dari kunci sebelumnya.

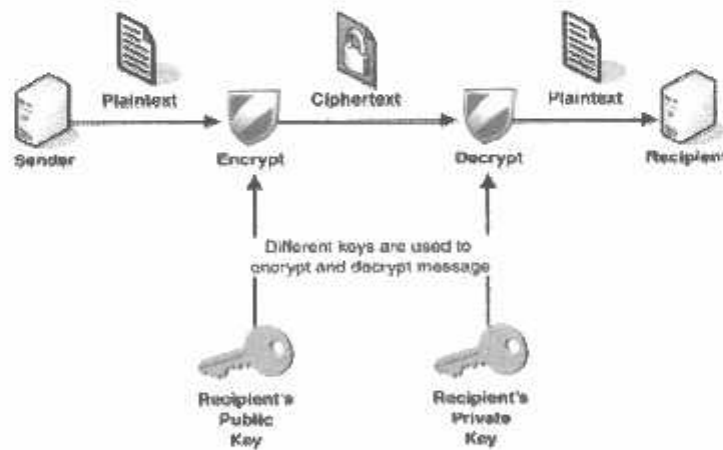


Gambar 2.4 Alur Algoritma Simetrik

Beberapa contoh Algoritma Kunci Simetrik yang umum digunakan sebagai berikut : *DES (Data Encryption Standard)*, *Blowfish* dan *AES*.

b. Algoritma Kunci Asimetrik (*Asymmetric Key Algorithm*)

Dapat dilihat pada gambar 2.5 yang merupakan alur dari algoritma kunci asimetrik, dimana input kunci untuk enkripsi dan dekripsi berbeda. Algoritma ini memiliki karakteristik yang unik dimana kunci untuk enkripsi boleh diketahui oleh pihak-pihak yang tidak memiliki otoritas karena dekripsi menggunakan kunci yang berbeda. Dapat dianalogikan seperti kotak pos yang hanya dapat dibuka oleh tukang pos yang memiliki kunci tapi setiap orang dapat memasukkan surat ke dalam kotak tersebut.



Gambar 2.5 Alur Algoritma Kunci Asimetrik

Pada algoritma ini, kunci untuk mengenkripsi sering disebut sebagai kunci publik (*public key*) dan kunci untuk mendekripsi disebut sebagai kunci privat (*private key*). Algoritma yang umum digunakan dalam model ini adalah *RSA* (*Rivert-Shamir-Adelman*).

2. Algoritma Hash

Merupakan langkah-langkah dalam melakukan fungsi yang mengubah input yang panjangnya sembarang dan mengkonversinya menjadi output dengan panjang yang tetap (umumnya berukuran jauh lebih kecil daripada ukuran semula). Algoritma ini bersifat satu arah, sehingga input tidak dapat diperoleh dengan memasukkan kembali output kedalam algoritma hashnya. Contoh Algoritma yang umum digunakan saat ini yaitu *MD5* (*Message-Digest Algoritim 5*).

2.3. Java ^[10]

Java adalah bahasa pemrograman yang dapat dijalankan di berbagai komputer termasuk *mobile phone*. Bahasa ini awalnya dibuat oleh James Gosling saat masih bergabung di "Sun Microsystems" saat ini merupakan bagian dari "Oracle" dan dirilis tahun 1995. Bahasa ini banyak mengadopsi sintaksis yang terdapat pada C dan C++ namun dengan sintaksis model objek yang lebih sederhana.

Aplikasi-aplikasi berbasis Java umumnya dikompilasi ke dalam p-code (*bytecode*) dan dapat dijalankan pada berbagai *Java Virtual Machine* (JVM). Java merupakan bahasa pemrograman yang bersifat umum/non-spesifik (*general purpose*), dan secara khusus didesain untuk memanfaatkan dependensi implementasi seminimal mungkin. Karena fungsionalitasnya yang memungkinkan aplikasi Java mampu berjalan di beberapa *platform* sistem operasi yang berbeda, Java dikenal pula dengan slogannya, "Tulis sekali, jalankan di mana pun". Saat ini Java merupakan bahasa pemrograman yang paling populer digunakan, dan secara luas dimanfaatkan dalam pengembangan berbagai jenis aplikasi berbasis *desktop* ataupun berbasis web.

2.3.1. Kelebihan Bahasa Pemrograman Java

1. **Multiplatform.** Kelebihan utama dari Java ialah dapat dijalankan di beberapa *platform*/sistem operasi komputer, sesuai dengan prinsip tulis sekali, jalankan di mana saja. Dengan kelebihan ini *programmer* cukup menulis sebuah program Java dan di-*compile* sekali lalu hasilnya dapat dijalankan di atas beberapa *platform* tanpa perubahan. *Platform* yang didukung sampai saat ini adalah Microsoft Windows, Linux, Mac OS dan Sun Solaris.
2. **Pemrograman Berorientasi Objek (*Object Oriented Programming*)**
3. **Perpustakaan Kelas (*Class Libraries*) Yang Lengkap.** Java terkenal dengan kelengkapan *library*/perpustakaan (kumpulan program-program yang disertakan dalam pemrograman Java) yang sangat memudahkan dalam penggunaan oleh para *programmer* untuk membangun aplikasinya.
4. **Bergaya C++.** *Source code* seperti bahasa pemrograman C++ sehingga menarik banyak pemrogram C++ untuk pindah ke Java.
5. **Pengumpulan sampah otomatis (*automatic garbage collector*).** Memiliki fasilitas pengaturan penggunaan memori sehingga para *programmer* tidak perlu melakukan pengaturan memori secara langsung (seperti halnya C++ yang dipakai secara luas).

2.3.2. Kekurangan Bahasa Pemrograman JAVA

Disamping memiliki kelebihan, JAVA juga memiliki kekurangan. Kekurangan yang dimiliki oleh Java adalah pada satu slogannya, yakni "Tulis sekali dan jalankan dimana saja" ternyata tidak sepenuhnya benar. Beberapa hal harus disesuaikan jika dijalankan pada platform yang berbeda. Misalnya untuk J2SE dengan platform SWT-AWT bridge tidak dapat berfungsi di Mac OS X. Kekurangan lainnya yaitu :

1. **Easy to Decompile** atau mudah didekompilasi. Dekompilasi adalah suatu proses membalikkan sebuah aplikasi menjadi kode sumbernya. Hal ini memungkinkan terjadi pada Java karena berupa bytecode yang menyimpan bahasa tingkat tinggi.

Hal ini terjadi pula pada platform .NET dari Microsoft sehingga program yang dihasilkan mudah dibajak kodenya karena sulit untuk disembunyikan.

- 2. Memory Usage.** Penggunaan memori yang cukup banyak, lebih besar daripada bahasa tingkat tinggi sebelum generasi Java seperti C/C++ dan Pascal. Namun hal ini memang sesuai dengan fitur beragam yang dimiliki oleh Java. Masalah memori ini juga tidak dialami oleh semua pengguna aplikasi Java. Mereka yang sudah menggunakan perangkat keras dengan teknologi terbaru tidak merasakan kelambatan dan konsumsi memori Java yang tinggi. Lain halnya dengan mereka yang menggunakan teknologi lama atau komputer yang sudah berumur tua lebih dari empat tahun akan merasakan adanya kelambatan.

Namun apapun kelemahan yang dimiliki Java, faktanya Java merupakan bahasa pemrograman yang populer dan digunakan di seluruh dunia saat ini.

2.3.3. Komponen JAVA ^[12]

1. Java Virtual Machine (JVM)

JVM merupakan jantung dari JAVA platform. JVM ini adalah pihak yang bertanggung jawab untuk mengeksekusi program JAVA menjadi bahasa mesin untuk diproses oleh prosessor. JVM mampu menerjemahkan kode - kode JAVA dari hampir semua platform. JVM inilah yang membuat JAVA "*write once, run everywhere*" atau dapat dijalankan di segala *platform*.

2. Java Runtime Environment (JRE)

JRE inilah yang memungkinkan sebuah program JAVA dapat berjalan di dalam mesin. JRE mengeksekusi binary – binary dari class-class dan mengirimnya ke JVM untuk diproses lagi ke prosessor. Setiap JRE pasti memiliki sebuah JVM di dalamnya untuk melakukan pemrosesan selanjutnya. JRE juga dapat di-*install* tanpa JDK, karena bersifat modular/terpisah.

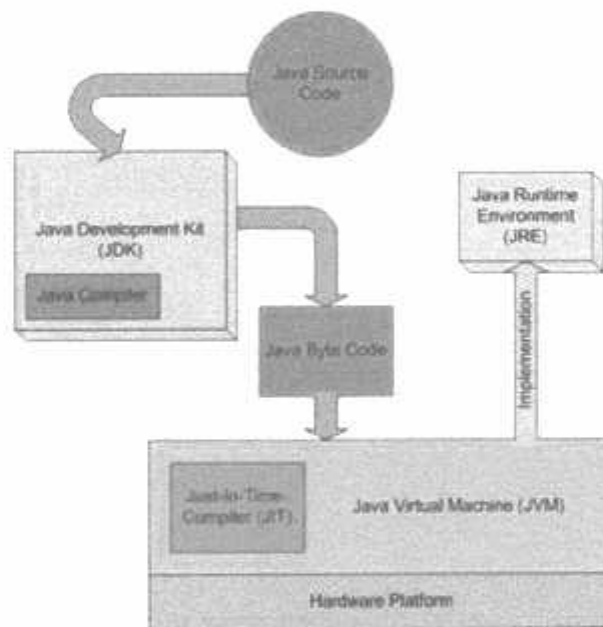
3. Java Development Kit (JDK)

Seperti namanya, JDK adalah semacam kotak peralatan (kit) yang digunakan sebagai *compiler source code* dari Java sehingga menjadi *byte*

code, yaitu *bit code* (biner) yang dapat dimengerti oleh mesin. JDK juga akan membentuk sebuah *object code* dari *source code*. Seperti halnya JRE, JDK juga memiliki JVM di dalamnya.

Dari ketiga komponen JAVA diatas, mempunyai keterkaitan atau hubungan satu dengan yang lainnya yang dapat dilihat ilustrasinya pada Gambar 2.6, sehingga dapat diambil kesimpulan singkat mengenai hubungan dari ketiganya, yaitu :

- JVM terdapat di dalam JRE
- JVM terdapat di dalam JDK juga
- JRE berfungsi untuk “membaca” program JAVA
- JDK berfungsi untuk “menulis” program JAVA



Gambar 2.6 Hubungan JVM, JRE dan JDK

2.4. XML (*Extensible Markup Language*)

XML (Extensible Markup Language) adalah sebuah bahasa markup. Markup yaitu bahasa yang berisikan kode – kode yang berupa tanda – tanda tertentu dengan aturan tertentu untuk memformat dokumen teks dengan tag sendiri ataupun mengikuti

format standar dari sebuah dokumen agar dapat dimengerti. Umumnya XML digunakan untuk deskripsi data dan penyimpanan data, serta tidak tergantung dengan tools tertentu (seperti editor, dbms, compiler, dsb). XML merupakan turunan (subset) atau versi ringkas dari SGML (*Standard Generalized Markup Language*). SGML sendiri merupakan sebuah standar ISO untuk format dokumen. SGML tidak berisi *tag-tag* siap pakai seperti halnya HTML, melainkan berupa aturan-aturan standar dalam pembuatan *tag-tag* format dokumen. SGML banyak dipakai untuk mengelola dokumen dalam jumlah besar, frekuensi revisi tinggi dan dibutuhkan dalam beragam format tampilan. SGML jarang dipakai karena sangat rumit dan kompleks. XML dibuat dengan konsep yang lebih sederhana dan ringkas, tujuannya agar bisa dipakai sebagai aplikasi di desktop dan jaringan Internet.

Meskipun XML hanya sekedar berisi data (tidak ada program didalamnya) banyak tools developer dan DBMS menggunakan XML, seperti: Java, Delphi, DotNET, Oracle, SQL Server, dan pemrograman web.

a. Tipe File XML

- XML, merupakan standar format dari struktur berkas (file).
- XSL, merupakan standar untuk memodifikasi data yang diimpor atau diekspor.
- XSD, merupakan standar yang mendefinisikan struktur database dalam XML.

b. Keunggulan XML

- *Pintar (Intelligence)*. XML dapat menangani berbagai tingkat kompleksitas.
- *Self-description*. Dokumen XML dapat disimpan tanpa perlu definisi tertentu karena mengandung *meta data* dalam bentuk *tag* dan atribut. Setiap *tag* XML dapat memiliki atribut dalam jumlah yang tidak terbatas.
- *Dapat beradaptasi*. Dapat mengadaptasi untuk membuat bahasa sendiri. Seperti Microsoft membuat bahasa MSXML atau Macromedia mengembangkan MXML.
- Mudah pemeliharaannya.

- *Sederhana*. Informasi atau *code* pada XML mudah dibaca dan dimengerti serta dapat diproses dengan mudah oleh komputer.
- *Mudah dipindah-pindahkan (Portability)*. XML mempunyai kemudahan perpindahan (portabilitas) yang lebih bagus.
- Pencarian data cepat, karena XML merupakan data dalam format yang terstruktur.

c. Tujuan Penggunaan XML

Dokumen XML dapat digunakan untuk berbagai macam tujuan dan kebutuhan, seperti :

- Sebagai file konfigurasi, di Java dokumen-dokumen XML sering kita jumpai seperti file *server.xml* dan *web.xml* yang digunakan Tomcat, atau perintah - perintah *query* yang disimpan dalam file XML yang dipakai pada framework *iBatis* atau *Hibernate*.
- Sebagai file layout, dalam pemrograman mobile application khususnya android, XML digunakan untuk membuat tampilan layout standard user interface nya.

2.5. PHP

PHP merupakan singkatan dari *Personal Home Page*, sebelum akhirnya dipaksakan menjadi singkatan rekursif dari *PHP : Hypertext Preprocessor*. Pertengahan tahun 1995 dirilis PHP/FI (FI adalah singkatan dari *Form Interpreter*) yang memiliki kemampuan dasar membangun aplikasi web, memproses form dan mendukung database MySQL. PHP juga merupakan salah satu bahasa *server side scripting* yang disisipkan di antara bahasa HTML untuk membuat halaman web yang dinamis. Dan karena bahasa berbasis *server side*, maka PHP akan dieksekusi di server, sehingga yang akan dikirimkan ke web browser adalah hasil dalam bentuk HTML dan kode PHP tidak akan terlihat.

Salah satu fungsi PHP adalah untuk menerima, mengolah, dan menampilkan data dari dan ke sebuah website. Data yang diterima akan diolah di sebuah program

database server dan kemudian hasilnya ditampilkan kembali ke layar web browser sebuah website. Seorang pengguna internet tidak dapat melihat kode program yang ditulis dalam PHP sehingga keamanan dari halaman web menjadi lebih terjamin. Bahasa pemrograman PHP memiliki beberapa kelebihan antara lain :

1. Bahasa pemrograman PHP adalah sebuah bahasa script yang tidak melakukan sebuah kompilasi dalam penggunaannya.
2. Web Server yang mendukung PHP dapat ditemukan di mana-mana dari mulai IIS sampai dengan Apache, dengan konfigurasi yang relatif mudah.
3. Dalam sisi pengembangan lebih mudah, karena banyaknya milis-milis dan developer yang siap membantu dalam pengembangan.
4. Dalam sisi pemahaman, PHP adalah bahasa scripting yang paling mudah karena referensi yang banyak.
5. PHP adalah bahasa open source yang dapat digunakan di berbagai mesin (linux, unix, windows) dan dapat dijalankan secara *runtime* melalui *console* serta juga dapat menjalankan perintah-perintah sistem.
6. PHP diterbitkan secara gratis dan dapat diambil oleh siapa saja.

2.6. Database MySQL

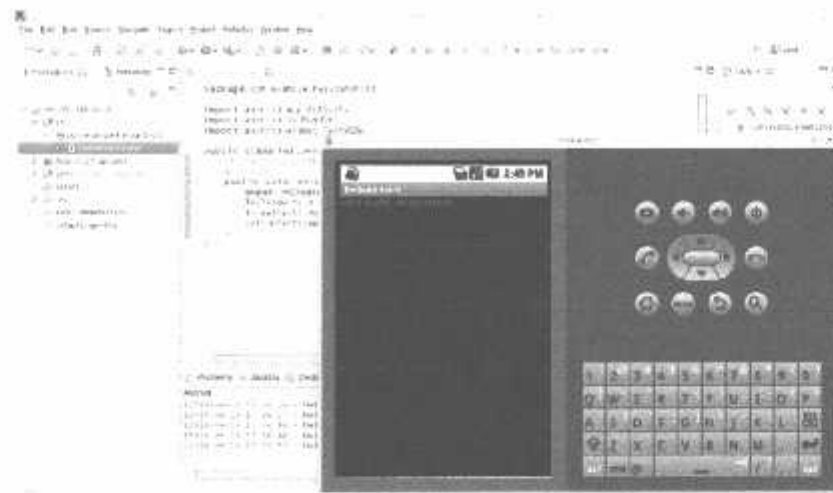
MySQL adalah sebuah perangkat lunak sistem manajemen basis data SQL (bahasa Inggris: *database management system*) atau DBMS yang *multithread*, *multi-user*, dengan sekitar 6 juta instalasi di seluruh dunia. MySQL AB membuat MySQL tersedia sebagai perangkat lunak gratis di bawah lisensi GNU General Public License (GPL), tetapi mereka juga menjual di bawah lisensi komersial untuk kasus-kasus di mana penggunaannya tidak cocok dengan penggunaan GPL. Tidak sama dengan proyek-proyek seperti Apache, di mana perangkat lunak dikembangkan oleh komunitas umum dan hak cipta untuk kode sumber dimiliki oleh penulisnya masing-masing, MySQL dimiliki dan disponsori oleh sebuah perusahaan komersial Swedia MySQL AB, di mana memegang hak cipta hampir atas semua kodenya.

2.6.1. Integrasi MySQL Dengan PHP

Umumnya dalam pembuatan sebuah *web application* dibutuhkan *source* yang digunakan untuk menghapus, menambah, mengedit dan menyimpan data ke *database* dan kemudian menampilkannya kembali. Itulah mengapa *database* harus diintegrasikan dengan PHP karena PHP mempunyai fungsi khusus untuk mengakses MySQL. Ada sekitar 48 fungsi yang didukung PHP dalam mengakses MySQL dalam membuat aplikasi. Adapun yang biasa digunakan di antaranya adalah :

- a) *mysql_connect()*. Fungsi *mysql_connect* digunakan untuk menghubungkan PHP dengan database MySQL. Format fungsinya adalah: *mysql_connect (string hostname, string username, string password)*.
- b) *mysql_select_db*. Setelah terhubung ke *database* MySQL, dengan menggunakan *mysql_connect*, langkah selanjutnya adalah memilih database yang akan digunakan. Fungsi *mysql_select_db* digunakan untuk memilih *database*. Format penulisan fungsinya adalah : *mysql_select_db (string database, koneksi)*.
- c) *mysql_query* Dalam database MySQL, perintah untuk melakukan transaksi ialah perintah SQL. Sebutan untuk mengirim perintah SQL dinamakan *query*. *Query* memberi perintah kepada *database* untuk melakukan apa yang dikehendaki. Format fungsinya adalah: *int mysql_query(string query, int [link_idenfifier])*.
- d) *mysql_num_rows* Kegunaan dari fungsi ini adalah untuk menghitung jumlah baris yang dikenai oleh proses SQL. Format fungsinya adalah: *int mysql_num_rows(int result)*.
- e) *mysql_fetch_array* Fungsi ini berkaitan dengan menampilkan data. Untuk menampilkan data, digunakan fungsi *mysql_fetch_array*. Dengan fungsi ini, hasil *query* ditampung dalam bentuk *array*. Format fungsinya adalah: *array mysql_fetch_array(int result, int [result_type])*:

2.7. Eclipse [6]



Gambar 2.7 Tampilan Antar Muka Eclipse

Gambar 2.7 merupakan jendela antarmuka Eclipse yang memiliki kemiripan pada semua versinya. Eclipse adalah sebuah IDE (*Integrated Development Environment*) untuk mengembangkan perangkat lunak dan dapat dijalankan di semua platform (*platformindependent*). Berikut ini adalah sifat dari Eclipse:

1. *Multi-platform*: Target sistem operasi Eclipse adalah Microsoft Windows, Linux, Solaris, AIX, HP-UX dan Mac OS X.
2. *Mult-language*: Eclipse dikembangkan dengan bahasa pemrograman Java, akan tetapi Eclipse mendukung pengembangan aplikasi berbasis bahasa pemrograman lain seperti C/C++, Cobol, Python, Perl, PHP, dan lain sebagainya.
3. *Multi-role*: Selain sebagai IDE untuk pengembangan aplikasi. Eclipse pun bisa digunakan untuk aktifitas dalam siklus pengembangan perangkat lunak seperti dokumentasi, pengujian perangkat lunak, pengembangan web, dan lain sebagainya.

Pada saat ini, Eclipse merupakan salah satu IDE favorit karena gratis dan *open source*. *Open source* berarti setiap orang boleh melihat kode pemrograman perangkat lunak ini. Selain itu, kelebihan dari Eclipse yang membuatnya populer adalah

kemampuannya untuk dapat dikembangkan oleh pengguna dengan membuat komponen yang disebut *plugin*.

2.7.1. Sejarah ECLIPSE

Eclipse awalnya dikembangkan oleh IBM untuk menggantikan perangkat lunak pengembangan IBM Visual Age for Java 4.0. Produk Eclipse ini diluncurkan oleh IBM pada tanggal 5 November 2001. IBM menginvestasikan US\$ 40 juta untuk pengembangannya. Sejak 5 November 2001, konsorsium Eclipse Foundation mengambil alih pengembangan Eclipse lebih lanjut.

2.7.2. Arsitektur ECLIPSE

Sejak versi 3.0, Eclipse pada dasarnya merupakan sebuah *kernel*. Apa yang dapat digunakan di dalam Eclipse sebenarnya adalah fungsi dari *plug-in* yang sudah dipasang (diinstal). Ini merupakan basis dari Eclipse yang dinamakan *Rich Client Platform* (RCP). Berikut ini adalah komponen yang membentuk RCP:

- *Core platform*
- OSGi
- SWT (*Standard Widget Toolkit*)
- Jface
- *Eclipse Workbench*

Secara standar Eclipse selalu dilengkapi dengan JDT (*Java Development Tools*), *plug-in* yang membuat Eclipse *compatible* untuk mengembangkan program Java, dan PDE (*Plug-in Development Environment*) untuk mengembangkan *plug-in* baru. Eclipse beserta *plug-in*-nya diimplementasikan dalam bahasa pemrograman Java. Eclipse memiliki konsep dalam pembuatannya, yaitu :

- terbuka (*open*),
- mudah diperluas (*extensible*) untuk apa saja, dan
- tidak untuk sesuatu yang spesifik.
- Eclipse tidak saja untuk mengembangkan program Java, tetapi juga untuk berbagai macam keperluan. Apabila ingin mengembangkan program C/C++ maka telah

terdapat *plug-in CDT (C/C++ Development Tools)* yang dapat dipasang di Eclipse untuk Eclipse menjadi perangkat untuk pengembangan C/C++.

2.7.3. Versi Eclipse

Eclipse Foundation mengkoordinasikan peluncuran Eclipse secara rutin dan simultan yang dikenal dengan nama *Simultaneous Release*. Setiap versi peluncuran terdiri dari Eclipse Platform dan juga sejumlah proyek yang terlibat dalam proyek Eclipse. Tujuan sistem ini adalah untuk menyediakan distribusi Eclipse dengan fitur – fitur dan versi yang terstandarisasi. Hal ini juga dimaksudkan untuk mempermudah *deployment* dan *maintenance* untuk sistem enterprise, serta untuk kenyamanan. Peluncuran simultan dijadwalkan pada bulan Juni setiap tahunnya. Hingga saat ini sudah ada 8 versi eclipse yang diluncurkan yaitu *Eclipse 3.0, Eclipse 3.1, Callisto, Europa, Ganymede, Galileo, Helios* dan *Juno*.

2.8. Android

2.8.1. Pengertian Android

Android adalah sebuah sistem operasi untuk perangkat *mobile* dan *tablet PC* yang menyertakan *middleware (virtual machine)* dan sejumlah aplikasi utama. Android merupakan modifikasi dari kernel Linux. Tujuan awal pembuatan sistem operasi ini adalah untuk menyediakan *platform* yang terbuka, yang memudahkan orang mengakses Internet menggunakan telepon seluler. Android juga dirancang untuk memudahkan *developer* untuk membuat dan mengembangkan aplikasi dengan batasan yang minim sehingga kreatifitas seorang *developer* menjadi lebih berkembang. Android memiliki empat karakteristik sebagai berikut :

1. Terbuka

Android dibangun untuk benar-benar terbuka sehingga sebuah aplikasi dapat memanggil salah satu fungsi inti ponsel seperti membuat panggilan, mengirim pesan teks, menggunakan kamera, dan lain-lain. Android menggunakan mesin virtual yang dirancang khusus untuk mengoptimalkan *memory resource* dan perangkat keras yang terdapat di dalam perangkat. Android merupakan *open*

source, dapat secara bebas diperluas untuk memasukkan teknologi baru yang lebih maju pada saat teknologi tersebut muncul. *Platform* ini akan terus berkembang untuk membangun aplikasi *mobile* yang inovatif.

2. Semua aplikasi dibuat sama

Android tidak memberikan perbedaan terhadap aplikasi utama dari telepon dan aplikasi pihak ketiga (*third-party application*). Semua aplikasi dapat dibangun untuk memiliki akses yang sama terhadap kemampuan sebuah telepon dalam menyediakan layanan dan aplikasi yang luas terhadap para pengguna.

3. Memecahkan hambatan pada aplikasi

Android memecah hambatan untuk membuat aplikasi yang baru dan inovatif. Misalnya, seorang *developer* dapat menggabungkan informasi yang diperoleh dari web dengan data pada ponsel seseorang seperti kontak pengguna, kalender atau letak geografis.

4. Pengembangan aplikasi yang cepat dan mudah

Android menyediakan akses yang sangat luas kepada pengguna untuk menggunakan *library* yang diperlukan dan *tools* yang dapat digunakan untuk membangun aplikasi yang semakin baik. Android memiliki sekumpulan *tools* yang dapat digunakan sehingga membantu para *developer* dalam meningkatkan produktivitas pada saat membangun aplikasi yang dibuat.

2.8.2. Fitur Sistem Operasi Android ^[9]

Menurut Tomas Katysovas (2008) sistem operasi Android memiliki fitur - fitur sebagai berikut:

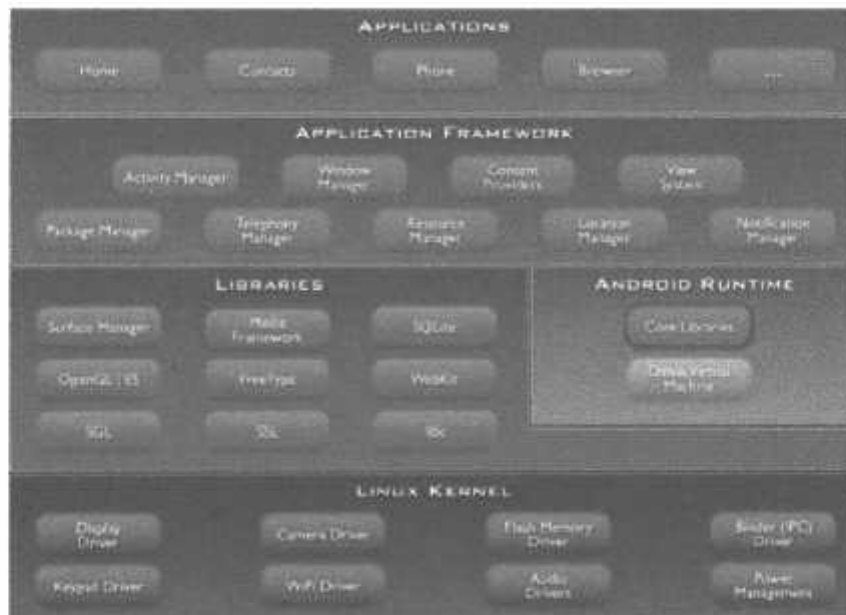
- a. **Application Framework** (Kerangka Kerja Aplikasi). Digunakan untuk menuliskan aplikasi di Android sehingga memungkinkan penggunaan kembali dan penggantian komponen. Kerangka kerja ini didukung oleh berbagai *open source libraries* seperti *openssl*, *sqlite*, dan *libc* serta didukung oleh *libraries* utama Android. Kerangka kerja sistem operasi Android didasarkan pada UNIX *file system permission* yang menjamin bahwa aplikasiaplikasi tersebut hanya memiliki kemampuan yang diberikan oleh pemilik ponsel pada waktu penginstalan.

- b. **Dalvik Virtual Machine (DVM).** DVM adalah sebuah mesin virtual yang menggunakan memori yang sangat rendah dan secara khusus dirancang untuk Android untuk dijalankan pada *embedded system*. DVM bekerja dengan baik pada situasi dengan tenaga yang rendah dan mengoptimalkan perangkat *mobile*. DVM juga mengatur atribut dari *Central Processing Unit (CPU)* serta membuat sebuah format *file* yang spesial (.dex) yang dibuat selama *build time post processing*. DVM dapat menggunakan kembali salinan informasi dari beberapa *class file* dan secara efektif mengurangi kebutuhan penyimpanan oleh setengah dari *Java Archive (.jar) file* tradisional. Konversi antara *class* Java dan format (.dex) dilakukan dengan memasukkan " dx-tool ". DVM menggunakan *assembly-code* yang berbeda dimana DVM menggunakan *register* sebagai unit utama dari penyimpanan data daripada menggunakan *stack*. Hasil akhir dari *executable-code* pada Android merupakan hasil dari DVM yang didasarkan bukan pada *Java byte-code* melainkan pada *file (.dex)*. Hal ini berarti bahwa *Java byte-code* tidak dieksekusi secara langsung melainkan dimulai dari *Java class file* terlebih dahulu dan kemudian mengkonversikannya ke dalam *file (.dex)* yang berhubungan.
- c. **Integrated Browser.** Didasarkan pada *open source WebKit engine* yang memiliki dua *layout* dan pengelompokan *frame*. *Layout* menampilkan halaman tanpa menunggu untuk melakukan pembalikan elemen eksternal seperti *Cascade Style Sheet (CSS)* atau eksternal *JavaScript*. Fitur – fitur inilah yang meningkatkan kecepatan dan penggunaan *browsing internet* melalui ponsel.
- d. **Optimated Grafik.** Didukung oleh library grafis 2D dan grafis 3D yang berdasarkan spesifikasi *OpenGL ES 1.0* (akselerasi perangkat keras bersifat opsional).
- e. **SQLite.** SQLite merupakan *relational database management system* yang kecil (sekitar 500 kb) yang diintegrasikan pada sistem operasi Android. SQLite didasarkan pada *function calls* dan *single file*, dimana semua definisi, tabel, dan data disimpan.
- f. **Media Support.** Dukungan media untuk suara, video dan format Gambar seperti *Moving Picture Experts Group 4 (MPEG4)*, *MPEG-1 or MPEG-2 Audio Layer 3*

- (MP3), *Advanced Audio Coding (AAC)*, *Adaptive Multi-Rate (AMR) audio codec*, *Joint Photographic experts Group (JPG)*, *Portable Network Graphics (PNG)*, *Graphics Interchange Format (GIF)*.
- g. **GSM Telephon.**, Untuk fitur ini tergantung dari perangkat keras yang digunakan oleh pengguna.
 - h. **Bluetooth, Enhanced Data Rates for GSM Evolution (EDGE), 3G dan WIFI.** Fitur ini juga tergantung dari perangkat keras yang digunakan.
 - i. **Multi – Touch.** Kemampuan layaknya *handset modern* yang dapat menggunakan dua jari atau lebih untuk berinteraksi dengan perangkat kerasnya.
 - j. **Kamera, Global Positioning System (GPS), kompas dan Accelerometer.** Fitur ini juga tergantung dari perangkat keras yang digunakan.
 - k. **Total Developing Environment Tools.** Seperti emulator, peralatan untuk *debugging*, memori dan *performance profiling*, serta *plug-in* untuk Eclipse IDE.
 - l. **Market.** Seperti kebanyakan *handphone* yang memiliki tempat penjualan aplikasi, Market pada android merupakan katalog aplikasi yang dapat di-*download* dan di-*install* pada *handphone* melalui internet.

2.8.3. Arsitektur Sistem Operasi Android ^[3]

Semua bentuk sistem operasi yang berkembang saat ini terbangun dari sebuah arsitektur pembangun sistem operasi. Begitu juga Android, pada Gambar 2.7 dibawah ini menunjukkan arsitektur sistem operasi Android. Terdapat lima blok besar pembangun sistem operasi Android dengan fungsi dan peranannya dari masing - masing bagian tersebut.



Gambar 2.8 *Arsitektur Sistem Operasi Android*

Dari Gambar 2.8 diatas, *software stack* dibagi dalam empat *layer* yang berbeda, yang meliputi lima kelompok yang berbeda, penjelasannya adalah sebagai berikut :

1. Linux Kernel

Pada layer bagian paling bawah dari Android adalah *Linux Kernel*. Android menggunakan modifikasi dari *Linux Kernel* versi 2.6. bagian ini bertanggung jawab untuk mengelola dan berkomunikasi dengan *hardware* dimana Android berjalan. Pemilihan *Linux Kernel* sebagai inti dari Android adalah karena dukungan dan kestabilannya terhadap berbagai macam komponen perangkat keras. Pada bagian ini disediakan driver (program pengendali) *hardware*, pengelola memori, pengelola proses, pengelola jaringan dan keamanan.

2. Libraries

Libraries merupakan layer kedua yang berisi kumpulan kode yang dapat digunakan oleh komponen atau program lain. Pada bagian ini kodenya ditulis menggunakan bahasa pemrograman C/C++. Fungsi masing – masing komponen di *libraries* ini adalah sebagai berikut,

- *Surface Manager*, berfungsi mengelola penggambaran dan komposisi komponen di layar (*window*, tombol, teks input, objek tiga dimensi (*3D Object*) dan sebagainya).
- *Open GL|ES*, merupakan engine grafis tiga dimensi.
- *SGL*, adalah engine grafis untuk dua dimensi.
- *Media Framework*, merupakan *codecs* untuk memutar dan merekam berbagai format video dan audio.
- *Free Type*, berfungsi untuk rendering font.
- *SSL*, berfungsi sebagai keamanan komunikasi jaringan.
- *SQLite*, merupakan layanan yang disediakan untuk pengelolaan database sebagai media penyimpanan data.
- *WebKit*, adalah *web browser engine* Android.
- *libc*, adalah library C standar.

3. Android Runtime

Di bagian inilah aplikasi Android berjalan. Inilah bagian *middleware* yang disebutkan pada definisi Android di awal. Aplikasi android ditulis menggunakan bahasa pemrograman *JAVA* dan untuk menjalankannya diperlukan sebuah *virtual machine* yang akan menerjemahkan instruksi – instruksi program *JAVA* tersebut ke instruksi yang dimengerti oleh sistem operasi. Namun berbeda dengan *platform* lainnya, Android tidak menggunakan *JAVA Virtual Machine (JVM)*, melainkan menggunakan *Dalvik Virtual Machine (DVM)* karena karakteristiknya yang memang dioptimasi untuk perangkat yang memiliki memori kecil dengan sumber tenaga yang terbatas dan kemampuan prosesor yang kecil.

4. Application Framework

Pada layer ini merupakan *framework* atau perangkat yang dapat digunakan oleh *developer* dalam membuat aplikasi Android. Pada dasarnya, bagian ini memiliki beberapa komponen dasar yang sangat penting perannya seperti,

- *Activity Manager*, mengatur siklus dari aplikasi dan menyediakan navigasi *backstack* untuk aplikasi yang berjalan pada proses yang berbeda.

- **Package Manager**, untuk melacak aplikasi apa saja yang terinstal di dalam perangkat Android
- **Windows Manager**, merupakan abstraksi dari bahasa pemrograman JAVA pada bagian atas dari level *services* (level yang paling rendah), yang disediakan oleh *Surface Manager*.
- **Telephony Manager**, berisi sekumpulan API untuk memanggil aplikasi.
- **Content Providers**, digunakan untuk memungkinkan aplikasi mengakses data dari aplikasi lain (seperti *contacts*) atau untuk membagikan data mereka sendiri.
- **Resource Manager**, digunakan untuk mengakses *resource* yang bersifat bukan *code* seperti *string* lokal, *bitmap*, deskripsi dari *layout file* dan bagian eksternal lain dari aplikasi.
- **View System**, digunakan untuk mengambil sekumpulan *button*, *list*, *grid* dan *text box* yang digunakan sebagai *user interface* oleh pengguna.
- **Notification Manager**, digunakan untuk mengatur tampilan peringatan dan fungsi – fungsi lain.

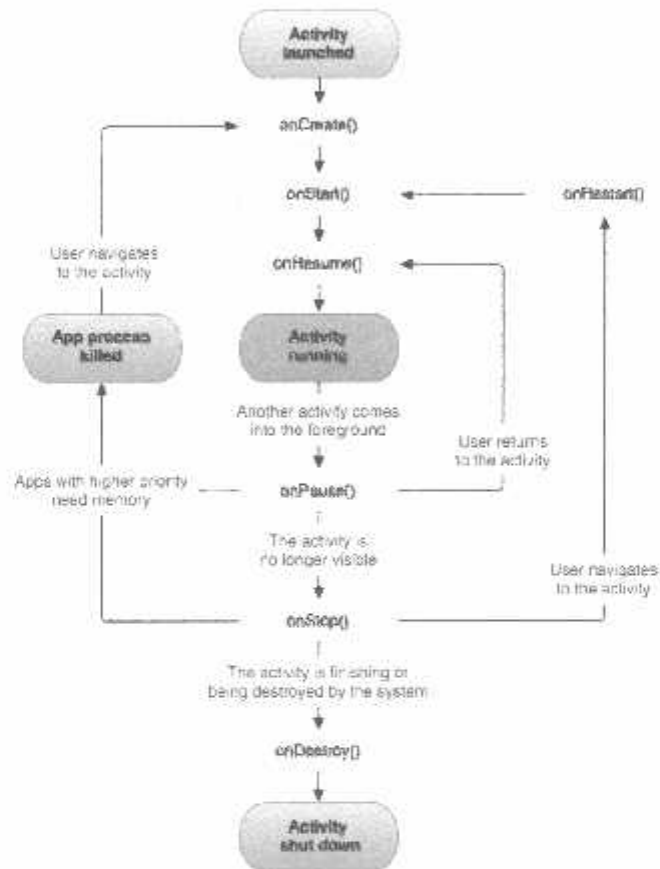
Seorang *developer* dapat memiliki akses *framework* yang sama dengan yang dapat diakses oleh aplikasi – aplikasi utama dari Android (*phone dialer*, buku telepon, SMS, *e-mail*, kalender dan sebagainya). Di sini terlihat keinginan dari Android untuk menjadi *platform* yang terbuka, sehingga memungkinkan *developer* untuk lebih kreatif dan inovatif.

5. Applications

Pada *layer* terakhir ini terdapat aplikasi – aplikasi yang dapat digunakan oleh pengguna Android. Aplikasi – aplikasi tambahan yang dipasang sendiri oleh pengguna, akan menempati bagian ini dan memiliki hak akses yang sama terhadap *Application Framework*. Apabila diperlukan, pengguna ataupun vendor dapat menggantikan aplikasi inti yang ada dengan aplikasi buatan sendiri yang memiliki fungsionalitas yang sama. Hal ini membuat kustomisasi sistem operasi Android jauh lebih bebas dibandingkan sistem operasi perangkat mobile lainnya.

2.8.4. Activity Lifecycle

Activity dalam sistem dikelola sebagai *activity stack*. Ketika *activity* baru dimulai, *activity* akan ditempatkan di bagian atas *stack* dan menjadi *running activity*. Apabila *activity* dihentikan, maka *activity* lainnya atau *activity* baru dipindahkan ke posisi atas *stack* dan menjadi aktif. Pada Gambar 2.9 menunjukkan fase dari setiap *state* pada *activity*.



Gambar 2.9 Android Activity Lifecycle

Berikut penjelasan pada masing - masing fase dalam Gambar 2.9,

1. **OnCreate**, fase ini terjadi pada saat suatu *activity* dibuat. Pada bagian ini, tampilan yang berhubungan langsung dengan pengguna dipanggil.

2. **OnStart**, fase ini dipanggil tepat sebelum suatu *activity* terlihat di layar. Fase ini berakhir ketika *activity* yang dipanggil menjadi *foreground activity* di layar sehingga fase berpindah ke fase *onResume*.
3. **OnResume**, fase ini, *activity* berjalan dan berinteraksi langsung dengan pengguna. Pada fase ini, aplikasi menerima *input* dari pengguna yang berasal dari *keyboard* dan *touch*.
4. **OnPause**, fase ini dipanggil ketika aplikasi lain dalam satu sistem akan menuju ke fase *resume*. Pada fase ini, *activity* yang berjalan tidak memiliki akses ke layar, jadi sebaiknya, semua proses yang mengkonsumsi sumber daya proses dan baterai sebaiknya dihindari. Fase ini sebaiknya digunakan untuk menyimpan *state* jika aplikasi akan ditampilkan ke layar kembali.
5. **OnStop**, fase ini dipanggil ketika *activity* tidak lagi terlihat karena *activity* lain sudah mengambil alih *foreground* atau karena *activity* kita sudah berakhir daur hidupnya.
6. **OnRestart**, fase ini dipanggil ketika *activity* yang masih berjalan namun tidak terlihat pada layar kembali dijalankan, yang kemudian akan berpindah ke fase *onStart*.
7. **OnDestroy**, fase ini merupakan fase berakhirnya suatu *activity*. Fase ini terjadi biasanya ketika aplikasi memanggil fungsi *finish()*.

2.8.5. Versi Sistem Operasi Android

1. Android 1.0 dan Android 1.1
2. Android 1.5 (Cupcake)
3. Android 1.6 (Donut)
4. Android 2.0 dan Android 2.1 (Eclair)
5. Android 2.2 (Frozen Yoghurt)
6. Android 2.3 (Gingerbread)
7. Android 3.0 dan Android 3.1 (Honeycomb)
8. Android 4.0 (Ice Cream Sandwich)
9. Android 4.1 dan Android 4.2 (Jelly Bean)

BAB III

PERANCANGAN DAN ANALISA SISTEM

3.1 Analisa Sistem

Secara garis besar sistem yang berjalan pada aplikasi *e-voting* ini berjalan seperti layaknya sistem Pemilu secara konvensional. Adanya undangan resmi dari pihak KPU Daerah yang ditujukan kepada para Pemilih sebagai informasi mengenai kapan dan dimana Pemilu akan dilaksanakan. Undangan resmi tersebut nantinya dibawa ke tempat (TPS) dimana Pemilih melakukan proses pencoblosan atau pencontrengan. Namun ada beberapa perbedaan yang sangat mencolok selain proses pemungutan suaranya dilakukan secara digital yaitu pada aplikasi ini undangan resmi yang diberikan KPU Daerah kepada Pemilih tidak sekedar berisi pemberitahuan waktu dan tempat pemungutan suaranya saja tetapi juga berisi data – data pendukung yang nantinya digunakan sebagai hak akses pemilih dan juga proses autentikasi data pemilih. Cara kerja aplikasi ini pemilih memasukkan data – data yang berupa NIK, *username* dan *password* sebagai hak akses yang kemudian dilanjutkan pada proses pemilihan suara. Proses pemilihan suara dilakukan dengan mengklik tombol *vote* yang ada pada halaman profile setiap kandidat. Kemudian selain mendapatkan hak memilih, pemilih juga mendapatkan hak untuk melihat total perolehan suara sementara pada menu hasil suara secara langsung saat itu juga sebelum ataupun setelah pemilih melakukan *voting*.

Dalam aplikasi *mobile* ini nantinya akan ada halaman administrasi dalam bentuk *web service* yang berfungsi untuk monitoring data, penambahan data serta proses audit laporan. Di dalam halaman administrasi ini monitoring data dilakukan terhadap halaman yang menampilkan data keseluruhan pemilih aktif yang masuk kedalam database dan juga data kandidat secara detail. Masih dalam halaman ini, proses pembuatan laporan hasil pemilihan suara dan proses pencetakan undangan pemungutan suara dilakukan disini. Untuk halaman tambah data pemilih, admin tidak melakukan input data *password* karena *password* untuk masing – masing pemilih akan ter-*generate* secara otomatis. Proses tersebut yang nantinya menggunakan algoritma kriptografi sebagai metode pengamanan datanya.

3.2 Hak Akses

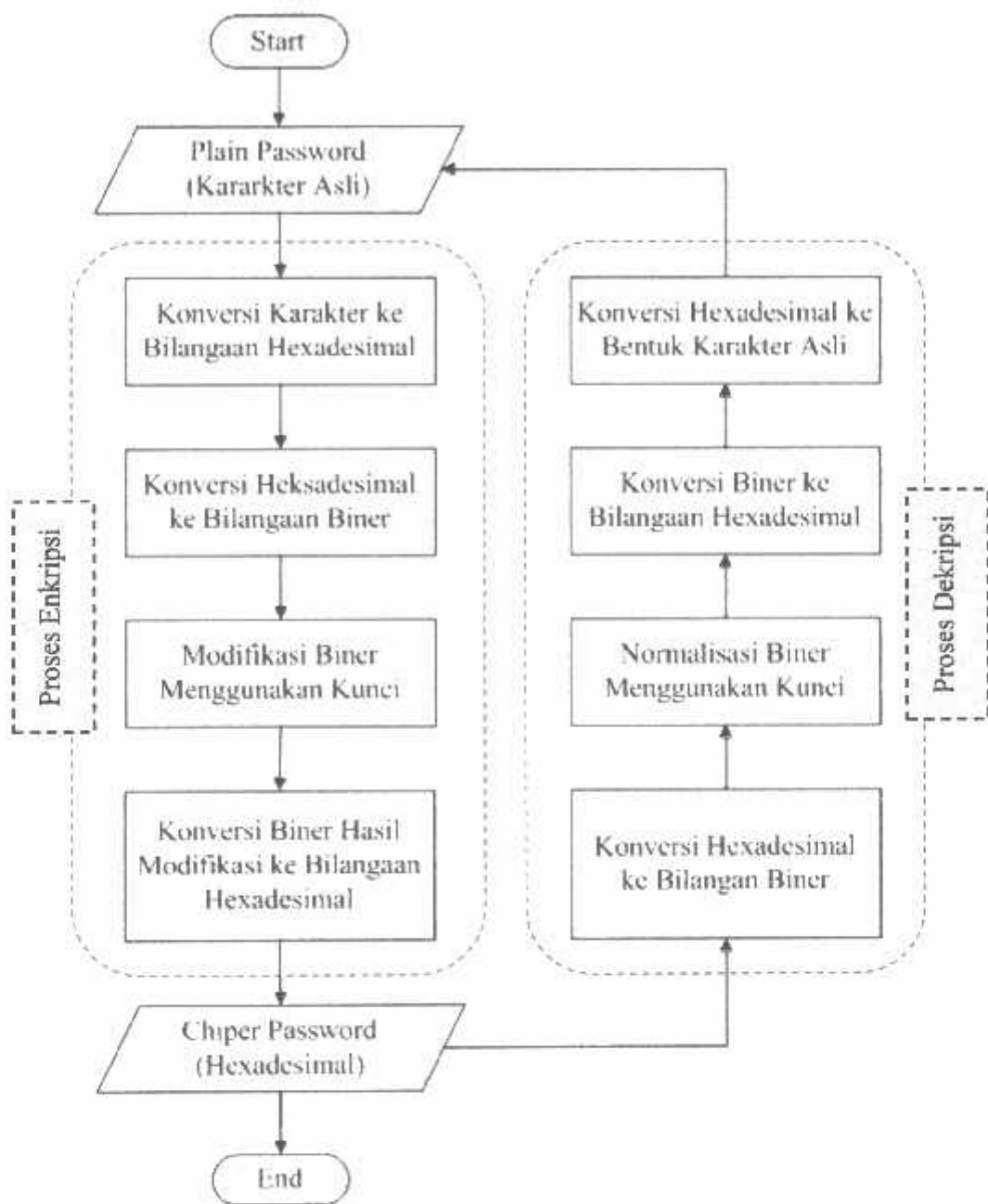
Ada tiga hak akses yang dimiliki aplikasi ini. Hak akses yang pertama dipegang oleh pemilih yang menggunakan *mobile* sebagai *user interface*-nya sebagai media pemungutan suara. Sedangkan hak akses yang kedua dan ketiga dipegang oleh panitia pemilu yang

menggunakan *web service* sebagai *user interface*-nya. Hak akses kedua adalah milik *administrator* yang hanya bertugas melakukan proses menambah, mengedit dan menghapus data pemilih saja, sedangkan hak akses ketiga dipegang oleh KPU Daerah (provinsi) yang memiliki tugas sebagai berikut:

- a. Mencetak surat undangan resmi untuk pemilih yang berisi :
 - Waktu pemungutan suara
 - NIK
 - *Username*
 - *Password*
- b. Melakukan *print out* laporan hasil voting sebagai hasil dari proses pemungutan suara dan juga sebagai penentu kandidat mana yang menang dalam Pemiluakada.

3.3 Perancangan Algoritma Kriptografi

Untuk sebuah tingkat keamanan suatu data yang baik dibutuhkan algoritma yang baik pula contohnya perubahan data dari teks asli menjadi teks sandi menggunakan algoritma kriptografi. Dalam aplikasi *e-voting* ini ada beberapa tahap dalam proses kriptografinya dari pembuatan teks asli hingga penyandiannya sampai kemudian dikembalikan lagi dari hasil penyandian ke teks asli. Berikut beberapa tahapan tersebut yang telah digambarkan pada flowchart gambar 3.1 :



Gambar 3.1 Flowchart Kriptografi (Enkripsi – Dekripsi)

Penjelasan singkat mengenai flowchart pada gambar 3.1 sebagai berikut :

1. Tahap pengacakan *password*. Pada proses penambahan data pemilih, *password* untuk pemilih akan ter-*generate* secara otomatis secara acak dengan kombinasi huruf dan angka. Pada tahap ini kondisi *password* masih dalam bentuk *plain text* (teks asli) yang masih harus dilakukan *penyandian* (enkripsi).

2. Tahap enkripsi *password*. Pada tahap ini *password* akan dimodifikasi sehingga menghasilkan bentuk enkripsi data yang sesuai dengan kebutuhan. Ada beberapa tahap yang dilakukan untuk proses pengenkripsian.

a. **Pertama**, perubahan teks asli menjadi bilangan *hexadecimal*. Contohnya pada angka 0,0 memiliki nilai *hexadecimal* 30. Nilai bilangan *hexadecimal* pada sebuah karakter (huruf atau angka) umumnya berjumlah dua *digit* angka atau kombinasi antara huruf dan angka. Misalnya jika *password* berjumlah lima karakter, maka akan terdapat sepuluh *digit* karakter *hexadecimal* yang artinya setiap dua *digit* bilangan *hexadecimal* mewakili satu karakter teks asli. Untuk mengetahui nilai bilangan *hexadecimal* dari sebuah karakter dapat dilihat pada tabel ASCII.

b. **Kedua**, tahap perubahan dari bentuk *hexadecimal* menjadi bentuk biner.

c. **Ketiga**, tahap modifikasi biner. Biner yang terbentuk pada tahap kedua masih sangat standard oleh karena itu pada tahap ini biner standard tersebut dimodifikasi menggunakan beberapa kunci agar biner tidak mudah diterjemahkan ke bentuk *hexadecimal* oleh pihak – pihak yang tidak bertanggungjawab yang berusaha untuk membongkar data asli.

d. **Keempat**, tahap konversi nilai biner yang telah dimodifikasi ke bentuk *hexadecimal*. Misalkan hasil dari tahap modifikasi biner angka 0 (nol) menghasilkan empat nilai biner yaitu 00100010, 00110001, 00101001 dan 10100001 maka nilai – nilai biner tersebut dikonversi menjadi bilangan *hexadecimal* sebagai berikut :

- 00100010 dikonversi menjadi 22.
- 00110001 dikonversi menjadi 31.
- 00101001 dikonversi menjadi 29.
- 10100001 dikonversi menjadi A1.

Jadi nilai hasil modifikasi biner ke bentuk *hexadecimal* dari angka 0 (nol) adalah **223129A1**.

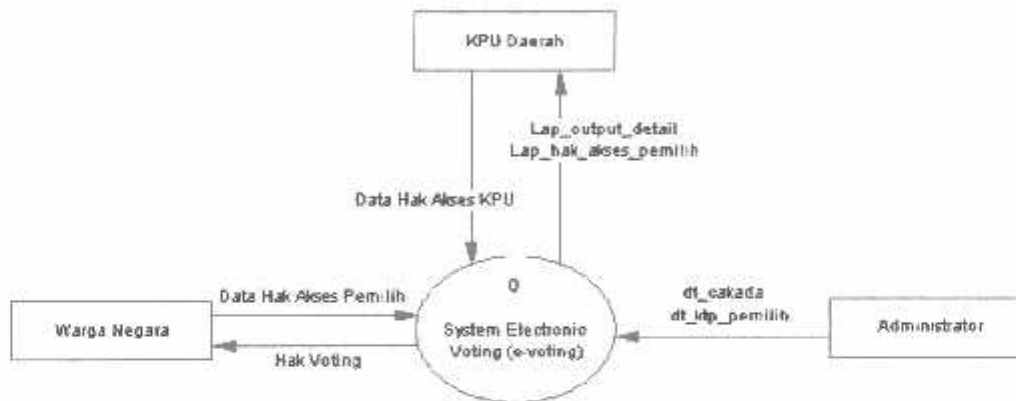
3. Tahap dekripsi *password*. *Password* yang pada tahap sebelumnya telah melalui proses enkripsi menjadi bilangan *hexadecimal* maka pada tahap ini, hasil enkripsi tersebut dikonversi menjadi bentuk karakter asli *password*. Proses dekripsi *password* dilakukan sesuai dengan proses mundur dari tahap enkripsi.

Dari ketiga tahap proses kriptografi *password* pada aplikasi *e-voting* ini, maka dapat dirumuskan dan diaplikasikan perintah – perintah dari tiap tahapnya ke dalam bentuk *source code* bahasa pemrograman PHP. Fungsi – fungsi tersebut antara lain fungsi *set_random_pass*,

fungsi *hex2teks*, fungsi *f_xor*, fungsi *biner2hex*, fungsi *encrypt* dan fungsi *decrypt*. Untuk alur proses enkripsi – dekripsi serta pembuktiannya pada sebuah kasus dapat dilihat pada Lampiran 1 di halaman akhir laporan skripsi ini.

3.4 Context Diagram (Diagram Konteks)

Context diagram atau diagram konteks merupakan rancangan diagram alur data paling awal dalam pembuatan suatu aplikasi maupun sistem informasi. Ciri-ciri dari diagram ini adalah terdapat satu proses utama yang menggambarkan satu aplikasi yang dikembangkan dan memiliki nomor proses 0. Diagram konteks aplikasi ini dapat dilihat pada gambar 3.2.



Gambar 3.2 Diagram Konteks

Dari diagram konteks dalam gambar 3.2, dapat dijabarkan penjelasan lebih detail mengenai entitas, proses dan data yang digunakan sebagai berikut :

a. Entitas

Merupakan pelaku-pelaku yang berperan dalam kegiatan/aktifitas yang dilakukan oleh sistem/aplikasi. Dalam aplikasi ini terdapat 2 entitas, yaitu :

- Administrator.
- Warga Negara (Pemilih).
- KPU Daerah.

b. Proses

Merupakan kegiatan – kegiatan yang dilakukan dalam sebuah sistem. Namun pada diagram konteks biasanya satu proses utama dinamakan dengan nama aplikasi atau sistem tersebut. Proses utama dalam aplikasi ini adalah *System Electronic Voting (e-voting)*.

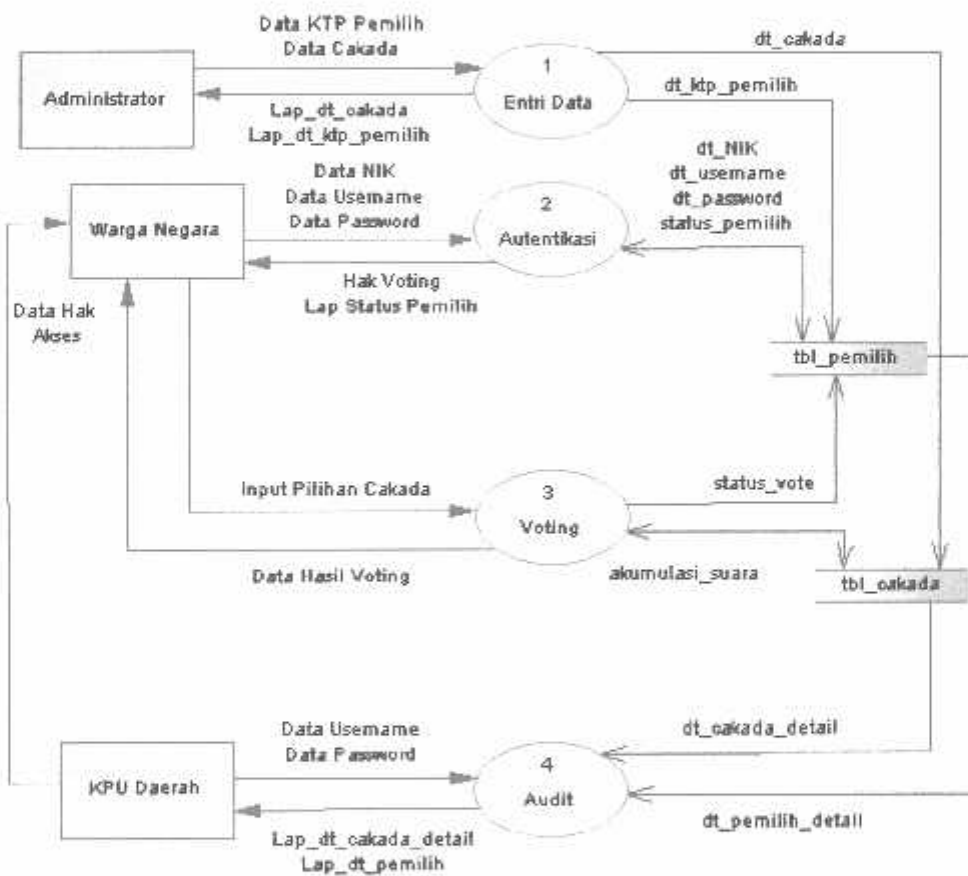
c. Data

Merupakan sebuah informasi yang belum diolah / informasi mentah. Dalam aplikasi ini terdapat beberapa data yang digunakan, yaitu :

- Data hak akses pemilih.
- Data hak akses KPU Daerah.
- Data calon kepala daerah.
- Data pemilih.

3.5 Data Flow Diagram (DFD) Level 1

DFD level 1 merupakan penjabaran yang lebih detail dari digram konteks. Untuk DFD level 1 dalam aplikasi ini dapat dilihat dalam gambar 3.3.



Gambar 3.3 DFD Level 1 Aplikasi DroidVote

Dalam gambar 3.3, dapat dijabarkan *input* dan *output* data dari masing-masing entitas dan proses sebagai berikut:

- Administrator

- Input : Data Pemilih (sesuai KTP), Data Cakada.
- Output : Laporan Data Pemilih, Laporan Data Cakada.
- Warga Negara
 - Input : Data NIK, Data Username, Data Password.
 - Output : Hak voting, Hak akses update akumulasi suara.
- KPU Daerah
 - Input : Data Username, Data Password
 - Output : Laporan Data Hak Akses Pemilih, Laporan Data Cakada Detail
- Proses Entri Data
 - Input : Data Pemilih (sesuai KTP), Data Cakada
 - Output : Laporan Data Pemilih, Laporan Data Cakada
- Proses Autentikasi
 - Input : Data NIK, Data Username, Data Password
 - Output : Hak Voting, Laporan Status Pemilih
- Proses *Voting*
 - Input : Pilihan cakada
 - Output : Data Hasil voting
- Proses *Audit*
 - Input : Data Username, Data Password
 - Output : Laporan Data Pemilih Detail, Laporan Data Cakada Detail

3.6 Rancangan Database

Pemilihan umum di Indonesia memiliki asas LUBER yang artinya “ *Langsung, Bebas dan Rahasia* ” dan JURDIL yang artinya “ *Jujur dan Adil* ” yang berlaku di semua tingkat pemerintahan, berdasarkan atas asas yang berlaku tersebut maka dalam perancangan dan pembangunan database pada aplikasi *e-voting* ini hubungan antar tabel tidak diperlukan sama sekali. Satu kata dari asas pemilukada yang sangat berpengaruh terhadap perancangan database untuk aplikasi *e-voting* ini yaitu *RAHASIA*, kerahasiaan merupakan faktor mengapa tidak ada hubungan antar tabel. Tidak adanya hubungan antar tabel membuat pemilik suara tidak memiliki bukti untuk menunjukkan siapa yang dia pilih dan kandidat juga tidak memiliki bukti apapun untuk mengetahui siapa yang memilihnya. Sehingga fungsi tabel yang terdapat dalam database ini nantinya hanya sebagai tempat penyimpanan data saja yang berdiri sendiri – sendiri.

Struktur tabel yang digunakan dalam aplikasi *e-voting* ini ada 3 tabel, yaitu tabel user, tabel pemilih dan table cakada. Tabel – tabel ini nantinya menyimpan berbagai macam informasi penting dari masing – masing entitas pada proses pemungutan suara elektronik ini seperti total suara yang masuk pada masing – masing kandidat pada tabel cakada dan status pemilih apakah sudah menggunakan hak pilihnya atau belum pada tabel pemilih. Berikut penjelesan dan gambaran dari masing – masing tabel tersebut :

a. Tabel User

Tabel ini menyimpan hak akses *administrator* dan panitia dari KPU daerah. Dapat ditunjukkan dalam Tabel 3.1.

Tabel 3.1 Tabel User

Kolom	Tipe Data(Panjang Data)	Deskripsi
<u>id_admin</u> (PK)	int(2)	Not Null, Autoincrement
Username	Varchar(20)	Not Null
Password	Varchar(50)	Not Null
hak_akses	Varchar(13)	Not Null

b. Tabel Pemilih

Tabel ini menyimpan seluruh data dari pemilih berdasarkan data dari KTP nya. Struktur tabel pemilih dapat ditunjukkan pada Tabel 3.2.

Tabel 3.2 Tabel Pemilih

Kolom	Tipe Data(Panjang Data)	Deskripsi
<u>NIK</u> (PK)	Int(18)	Not Null
Username	Varchar(10)	Not Null
Password	Varchar(40)	Not Null
Nama	Varchar(50)	Not Null
Domisili	Varchar(50)	Not Null
Isvoted	Varchar(3)	Not Null
Status	Varchar(16)	Not Null

c. Tabel Kandidat

Tabel kandidat merupakan tabel yang memiliki peran paling penting, karena aplikasi ini dibangun dengan dasar pemilihan kandidat. Tabel ini berfungsi untuk menyimpan seluruh

data dari pasangan kandidat sekaligus total hasil pemungutan suara perkandidatnya. Struktur tabel kandidat dapat dilihat pada Tabel 3.3.

Tabel 3.3 Tabel Kandidat

Kolom	Tipe Data(Panjang Data)	Deskripsi
<u>Id_cand</u> (PK)	Int(1)	Not Null
Name_cand	Varchar(20)	Not Null
Picture	Varchar(100)	Not Null
Hits	int(20)	Not Null
Last_voted	Timestamp	Not Null
Profile	Varchar(500)	Not Null

3.7 Desain Layout

Karena aplikasi ini dibuat berdasarkan sistem *client – server*, maka *layout* dalam aplikasi ini terdiri dari 2 bagian, yaitu *layout* untuk *web service* sebagai tampilan *server* dan *layout* untuk *mobile android* sebagai tampilan *client*.

a. Layout Halaman Web Service

Halaman *web service* merupakan halaman administrasi yang diperuntukkan bagi *administrator* dan pejabat berwenang (KPU Daerah). Untuk penjelasan dari masing – masing desain halaman *web service* tiap *entity* adalah sebagai berikut :

1. Administrator

Ada lima desain layout halaman yang nantinya dapat diakses oleh *administrator*, yaitu *layout* halaman login, *layout* halaman navigasi *administrator*, *layout* tampil data pemilih, *layout* halaman tampil data cakada dan *layout* tambah data pemilih. Berikut penjelasan tiap – tiap layoutnya.

a. Layout Halaman Login

Merupakan halaman yang digunakan oleh administrator dan pejabat KPU daerah untuk dapat masuk ke dalam sistem agar dapat melakukan aktifitas seperti menambahkan data user dan memantau update terakhir hasil pemilihan suara. *Input* yang dibutuhkan adalah *username* dan *password*. Desain halaman login dapat dilihat dalam gambar 3.4.

Username :

Password :

Login

Gambar 3.4 Layout Halaman Login

Sistem login ini menggunakan *session* yang berguna untuk menyimpan data user yang login kedalam sistem dan menentukan sekaligus memberikan batas hak akses dari masing – masing *entity*.

b. Layout Halaman Administrator

Merupakan halaman dimana berisi *list* menu yang berisi halaman – halaman yang dapat diakses oleh administrator saja. Desain halaman login dapat dilihat dalam Gambar 3.5.

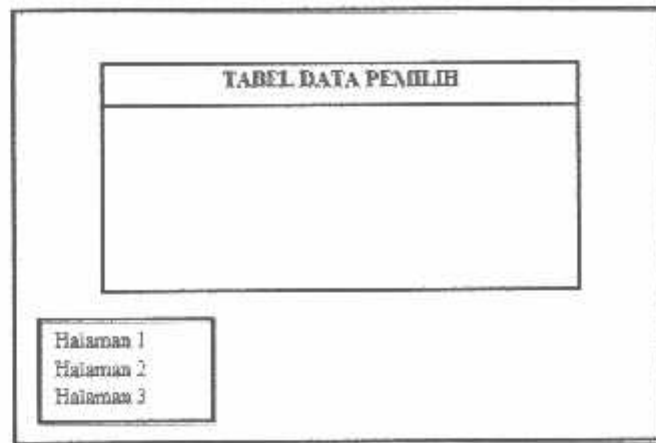
Administrator

- Halaman 1
- Halaman 2
- Halaman 3
- Halaman 4

Gambar 3.5 Layout Halaman Administrator

c. Layout Halaman Data Pemilih

Pada halaman ini data para pemilih yang sudah terdaftar dapat dilihat secara detail. Seperti dilihat pada Gambar 3.6, halaman ini berisi sebuah tabel yang nantinya diisi dengan data para pemilih.

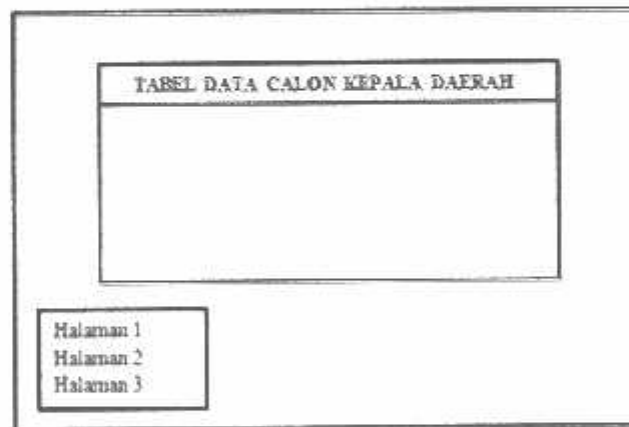


Gambar 3.6 *Layout Halaman Data Pemilih*

Pada Gambar 3.6 dapat dilihat ada satu area kecil berisi beberapa halaman, ini adalah area navigasi pengganti halaman navigasi administrator agar administrator dapat melakukan hak aksesnya langsung dari halaman dimana dia berada tanpa harus kembali dulu ke halaman navigasi.

d. Layout Halaman Data Calon Kepala Daerah

Pada halaman ini, bentuk layout halaman, fungsi dan komponen pembangunnya kurang lebih memiliki kesamaan dengan layout pada halaman data pemilih. Desain layoutnya dapat dilihat pada gambar 3.7.



Gambar 3.7 *Layout Halaman Data Calon Kepala Daerah*

e. Halaman Tambah Data Pemilih

Halaman ini berbentuk form yang berfungsi sebagai formulir untuk penambahan data. Banyak form yang digunakan tergantung pada banyak data yang ingin ditambahkan. Layout untuk halaman ini seperti yang diilustrasikan pada gambar 3.8.

Gambar 3.8 Layout Halaman Tambah Data Pemilih

Dalam form tambah data ini password tidak diinputkan secara manual oleh administrator, tetapi password akan ter-*generate* secara otomatis berbentuk *chiper text (sandi)* yang langsung akan tersimpan ke dalam database. Pada gambar 3.8, tepat dibawah form tambah data terdapat sebuah *text input* yang nantinya diisi dengan berapa banyak data pemilih yang akan ditambahkan ke dalam *database*.

2. Pejabat KPU Daerah

Hanya ada empat desain layout halaman yang nantinya dapat diakses oleh pejabat KPUD, yaitu layout halaman login, layout halaman navigasi KPUD, layout halaman tampil data pemilih dan layout halaman tampil data cakada. Penjelasan layout halaman login dan navigasi yang dimiliki oleh pejabat KPUD kurang lebih sama seperti yang dimiliki oleh administrator sehingga untuk penjelasan tiap layoutnya hanya berkisar pada dua layout saja yaitu layout halaman tampil data pemilih dan layout tampil data cakada yang memang berbeda dari segi fungsi dan komponen pembangunnya.

a. Layout Halaman Data Pemilih

Halaman ini memiliki desain layout yang kurang lebih sama dengan desain layout yang dimiliki oleh administrator, bedanya terdapat pada sebuah tombol yang terletak di dalam tabel data pemilih seperti yang terlihat pada gambar 3.9.

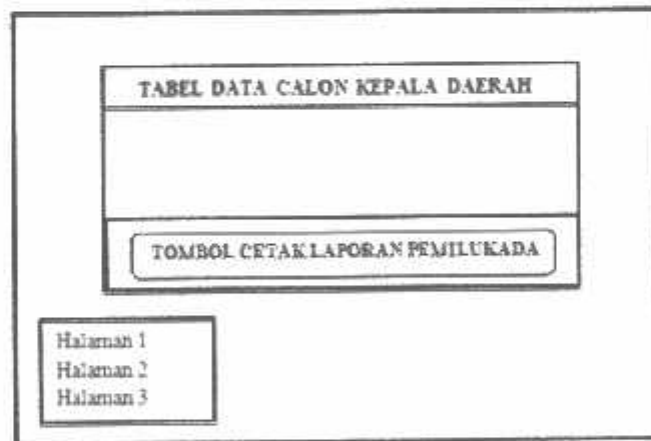


Gambar 3.9 *Layout Halaman Data Pemilih (KPUD)*

Tombol yang terdapat pada gambar 3.9 nantinya berfungsi untuk mencetak surat undangan resmi bagi pemilih untuk menggunakan suaranya atau hak pilihnya seperti yang umum dilakukan pada pemungutan suara secara konvensional, bedanya surat undangan ini nantinya tidak hanya berisi waktu pelaksanaan pemungutan suara tetapi juga berisi data yang digunakan untuk proses autentikasi pada saat pemilih menggunakan hak suaranya.

b. Layout Halaman Data Calon Kepala Daerah

Tidak terlalu berbeda juga dengan halaman data cakada administrator. Perbedaannya bisa dilihat pada gambar 3.10, terletak pada sebuah komponen tombol yang ada didalam tabel data cakada.



Gambar 3.10 *Layout Halaman Data Calon Kepala Daerah (KPUD)*

Bisa dilihat pada Gambar 3.10 terdapat sebuah tombol yang nantinya berfungsi untuk mencetak data detail hasil pemilukada dalam bentuk laporan resmi sebagai tembusan dari KPUD ke KPU Pusat.

b. Layout Halaman *Mobile (Android)*

Layout halaman pada mobile ini nantinya akan digunakan oleh pemilih untuk menggunakan hak pilihnya, berikut layout – layout yang nantinya dibutuhkan dalam pengaksesan aplikasi droidvote.

1. *Layout Autentikasi*

Layout ini merupakan halaman utama aplikasi DroidVote. Seperti yang dapat dilihat pada gambar 3.11, halaman ini nantinya akan berisi form yang berfungsi memeriksa valid atau tidaknya data pemilih yang terdiri dari NIK, *username* dan *password*.

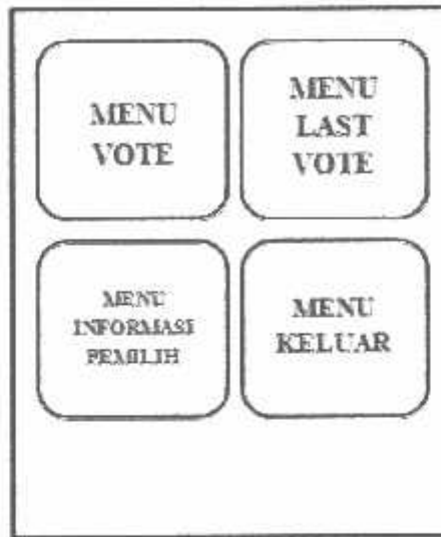
The diagram shows a rectangular frame representing a mobile application screen. At the top, centered, is the text 'FORM AUTENTIKASI'. Below this, there are three vertically stacked input fields. The first is labeled 'NIK', the second 'Username', and the third 'Password'. Each label is to the left of its corresponding input box. At the bottom center of the frame is a rounded rectangular button with the text 'TOMBOL AUTENTIKASI' inside it.

Gambar 3.11 Layout Autentikasi

Pada gambar 3.11, terdapat sebuah tombol autentikasi pada bagian bawah layout, tombol ini yang nantinya berfungsi menjalankan perintah otentikasi data pemilih sehingga apabila pemilih memiliki data yang *valid* maka secara otomatis diijinkan menggunakan hak pilihnya, sedangkan bila data yang di inputkan tidak *valid* maka pemilih tidak diijinkan untuk menggunakan hak pilihnya.

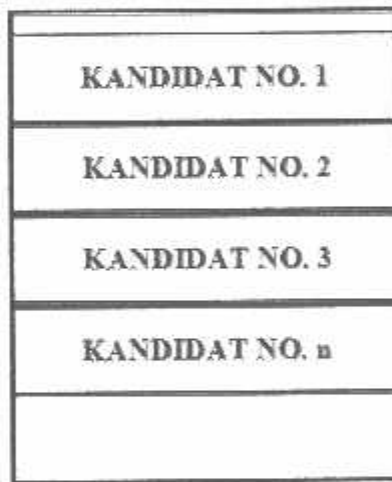
2. *Layout Menu*

Pada layout menu ini terdapat empat buah menu yang berbentuk tombol seperti yang terlihat pada gambar 3.12 yang berfungsi untuk menuju ke proses dan halaman lainnya, berikut penjelasan tiap menunya



Gambar 3.12 Layout Menu

a. *Menu Vote*, didalam menu inilah nantinya proses voting dilakukan. Sebelum menuju pada layout yang berisi proses voting, nantinya pemilih akan menjumpai layout yang berisi *list* para kandidat dimana pemilih diharuskan memilih satu kandidat yang dianggap sesuai dengan hati nurani, seperti yang terdapat pada gambar 3.13.



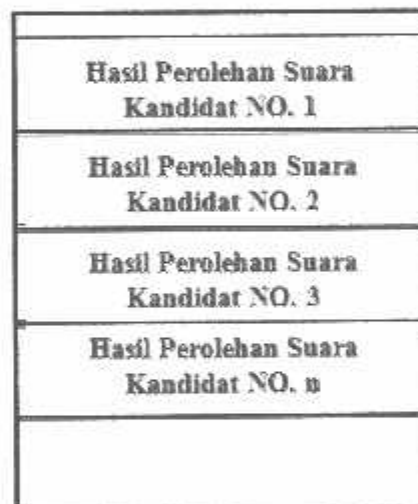
Gambar 3.13 Layout Daftar Kandidat

Kemudian setelah memilih satu kandidat maka pemilih akan dibawa menuju layout yang berisi data detail dari pasangan kandidat tersebut, pada layout seperti gambar 3.14 inilah proses voting dilakukan.



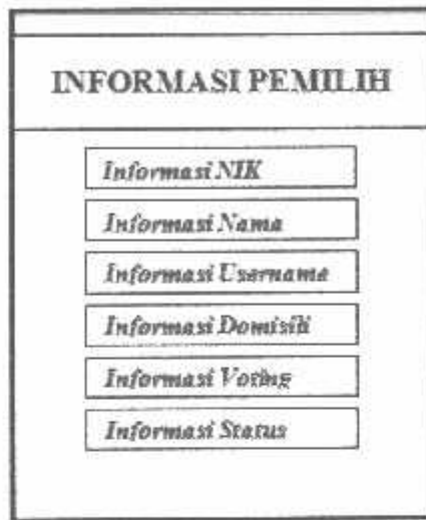
Gambar 3.14 Layout Informasi Kandidat

b. *Menu Last Vote*, pada menu ini hasil dari perolehan suara ditampilkan. Seperti pada gambar 3.15, hasil perolehan suara tiap kandidat akan ditampilkan dalam bentuk *list*. Karena salah satu asas dari sebuah proses pemungutan suara adalah rahasia, maka tidak ada bekas apapun yang ditinggalkan tentang pemilik suara dari masing – masing kandidat, hanya pemilih yang tahu kepada siapakah suaranya diberikan.



Gambar 3.15 Layout Last Vote

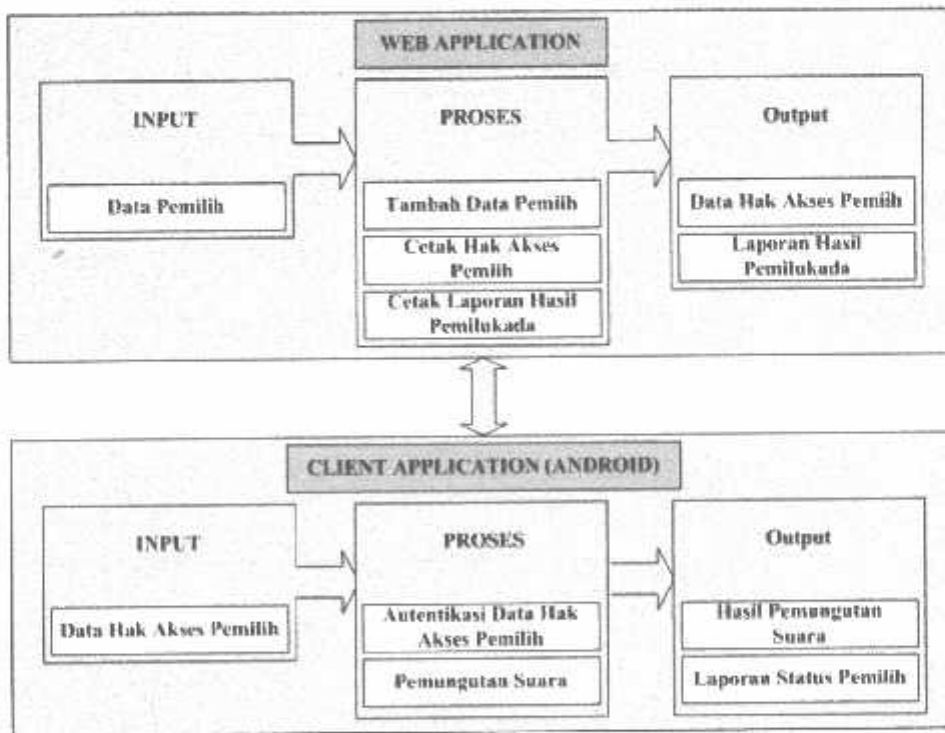
c. *Menu Informasi Akun Pemilih*, menampilkan data lengkap dari pemilih yang melakukan *login* pada aplikasi ini. Seperti yang dapat dilihat pada gambar 3.16, halaman ini nantinya berisi informasi akun dari pemilih. Semua informasi pada layout ini akan ditampilkan sesuai dengan data yang tersimpan di database server.



Gambar 3.16 Informasi Akun Pemilih

d. *Menu Keluar*, menu ini digunakan apabila pemilih dirasa sudah cukup menggunakan hak aksesnya dan ingin keluar dari aplikasi. Dengan menekan tombol menu keluar ini maka pemilih akan keluar dari sistem dan dibawa kembali menuju ke halaman utama aplikasi DroidVote.

3.8 Block Diagram

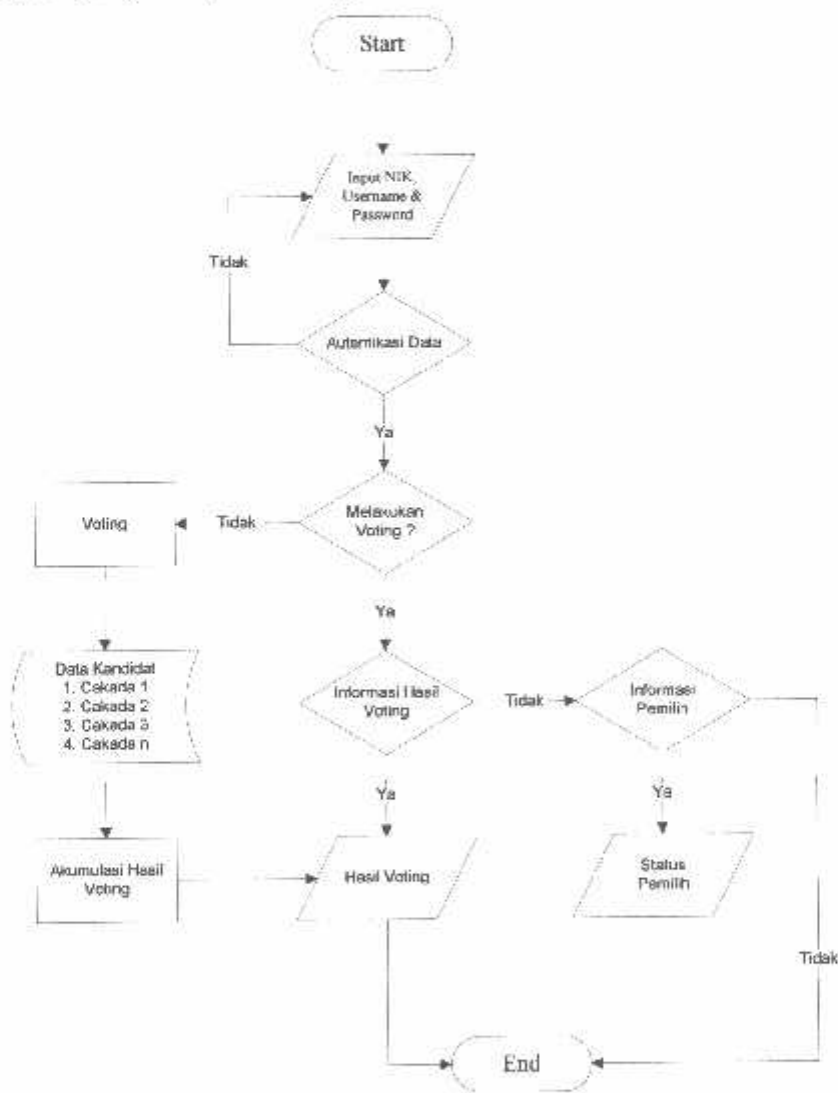


Gambar 3.17 Block Diagram Sistem

Block Diagram merupakan gambaran secara umum proses berjalannya sebuah sistem terstruktur. Pada gambar 3.17 dijelaskan ada dua buah sistem *platform* yang saling berhubungan dalam aplikasi *e-voting* ini. Pada setiap *platform* yang berjalan memiliki sistem input, sistem proses dan sistem output. Agar aplikasi *e-voting* ini berjalan dengan baik maka pada bagian *web service* ditempatkan semua informasi penunjang yang nantinya akan diakses melalui media aplikasi android oleh *user* atau pemilih.

3.9 Flowchart

Pada setiap pembangunan sebuah aplikasi diperlukan sebuah gambaran desain sistem yang memiliki alur sistem kerja yang jelas mulai dari start hingga finish yang digambarkan dalam bentuk *flowchart* (diagram alur). Flowchart dari aplikasi DroidVote ini dapat dijabarkan seperti yang terdapat dalam gambar 3.18



Gambar 3.18 Flowchart Aplikasi DroidVote

Dalam gambar 3.18, dapat dijelaskan alur dari cara kerja aplikasi DroidVote ini, yaitu dimulai dengan memasukkan data – data pada *form* autentikasi data. Kemudian system akan melakukan proses autentikasi data yang kemudian dapat diketahui apakah data yang dimasukkan pemilih *valid* atau tidak, jika *valid* maka pemilih dapat melakukan proses selanjutnya dan jika tidak *valid* maka pemilih akan tetap berada di halaman menu utama serta tidak dapat melanjutkan ke proses selanjutnya. Proses autentikasi ini juga sekaligus memeriksa status pemilih sudah menggunakan hak pilihnya atau belum. Jika sudah, sekalipun pemilih memiliki data *valid* maka tetap saja dia tidak dapat melakukan *voting* untuk kedua kalinya dan jika belum maka menu *voting* masih bisa digunakan.

Proses selanjutnya yaitu pemilih dihadapkan pada halaman menu, yang berisi menu *voting*, menu informasi pemilih, menu *last vote* dan menu keluar. Menu yang bisa digunakan tergantung dari status *voting* pemilih yang *login* kedalam aplikasi, apabila statusnya sudah pernah memilih maka hanya bisa mengakses menu informasi pemilih, menu *last vote* dan menu keluar dan jika sebaliknya, maka pemilih dapat menggunakan seluruh menu yang tersedia.

Bagi pemilih yang belum menggunakan hak pilihnya maka menu *voting* bisa diakses, di dalam menu ini terdapat daftar kandidat yang harus dipilih salah satu sesuai hati nurani. Setelah memilih maka pemilih akan dibawa kedalam halaman profil kandidat yang berisi informasi detail kandidat dari nomor urut hingga visi misi yang dilengkapi dengan sebuah tombol “VOTE” untuk memberikan hak suara. Setelah melakukan *voting* kemudian pemilih dibawa menuju halaman *last vote* yang berisi perolehan suara sementara secara *live report*. Kemudian pemilih dapat menggunakan tombol *back* yang terdapat pada *device* android untuk menuju ke halaman menu lagi dan menggunakan menu lain seperti informasi pemilih atau jika dirasa sudah cukup dapat menggunakan menu keluar untuk keluar dari aplikasi.

BAB IV

IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi

Pada subbab ini berisi penjelasan tentang lingkungan pengembangan yang digunakan dalam tahap pembangunan aplikasi, batasan implementasi dan proses hasil implementasi.

4.1.1. Lingkungan Pengembangan

Aplikasi ini dikembangkan menggunakan perangkat keras dan perangkat lunak dengan spesifikasi sebagai berikut :

a. Spesifikasi Perangkat Keras

1. Prosesor AMD Athlon II P320 Dual-Core Processor 2.1 GHz.
2. RAM 4GB.
3. VGA ATI Mobility RADEON HD 4200.

b. Spesifikasi Perangkat Lunak

1. Sistem Operasi Windows 7 Ultimate 32bit.
2. IDE Eclipse JUNO SDK 4.2.0.
3. JAVA Development Kit (JDK) versi 6.
4. JAVA Runtime Environment (JRE) versi 6.
5. Notepad ++ versi 5.9.6.2.
6. Photoshop CS3.
7. CorelDraw X4.
8. FileZilla 3.5.2.

4.1.2. Batasan Implementasi

Batasan implementasi dalam pembangunan aplikasi DroidVote pada skripsi ini adalah dapat dijalankan minimal pada sistem operasi android versi 2.2 atau lebih sering dikenal dengan versi Froyo (Frozen Yoghurt).

4.1.3. Implementasi File

Karena aplikasi DroidVote ini berbasis pada pemrograman *client – server* maka implementasi *file* yang digunakan untuk membangun aplikasi ini terbagi dalam dua kategori *file* pembangun yaitu *file* pembangun dari sisi aplikasi client dan *file* pembangun dari sisi aplikasi *server*.

a. File Pembangun Dari Sisi Client

Tabel 4.1 File Pembangun Aplikasi Client

Nama File	Fungsi
About.java	Proses menampilkan lisensi aplikasi
Authentic.java	Proses autentikasi data pemilih
DetailCand.java	Proses menampilkan profil tiap kandidat
InfoUser.java	Proses menampilkan data pemilih
JSONParser.java	Proses parsing data dari database web server
LastVote.java	Proses menampilkan jumlah suara terkumpul berdasarkan nomor urut kandidat
ListCand.java	Proses menampilkan kandidat dalam bentuk list
Menu.java	Menampilkan menu yang dapat diakses oleh pemilih yang telah diautentikasi datanya
MenuOption.java	Memberikan menu alternatif tambahan seperti menu keluar meskipun pada <i>device</i> android sudah tersedia tombol keluar
BuildConfig.java	Bersifat <i>AUTO GENERATED</i> , tidak boleh diedit
R.java	Bersifat <i>AUTO GENERATED</i> , tidak boleh diedit
AndroidManifest.java	Memberi hak akses pada semua <i>activity</i> yang telah dibangun, sehingga aplikasi dapat berjalan baik

b. File Pembangun Dari Sisi Server

Tabel 4.2 File Pembangun Aplikasi Server

Nama File	Fungsi
authentication_andro.php	Autentikasi data pemilih yang diinputkan ke <i>database server</i>
usernote.php	Berisi beberapa fungsi untuk melakukan proses enkripsi dan dekripsi <i>password</i> .
detailcand_andro.php	Mengambil data tiap kandidat dari database untuk ditampilkan pada halaman profil tiap kandidat secara detail
informationshow_andro.php	Menampilkan detail data pemilih yang diambil dari <i>database server</i>

isvoted_andro.php	Memberikan status “Yes” pada pemilih yang telah memberikan suaranya, yang artinya sudah memilih
listcand_andro.php	Mengambil beberapa data dari tiap kandidat untuk ditampilkan dalam bentuk <i>list</i> ke dalam aplikasi DroidVote
updatestatus_andro.php	Menrubah status pemilih yang ada didalam database menjadi “Activated” karena data yang diinputkan ke dalam form autentikasi valid dan benar
vote_andro.php	Menambahkan jumlah perolehan suara kandidat yang sudah di- <i>vote</i>
connectdb.php	Menghubungkan database server dengan <i>file – file</i> yang berisi perintah agar berjalan dengan baik sehingga proses yang terjadi pada sisi <i>client</i> dapat tereksekusi di sisi <i>server</i> juga

4.1.4. Implementasi *User Interface*

User Interface atau tampilan antarmuka adalah hal penting yang harus diperhatikan yang nantinya akan mendapatkan hasil apakah aplikasi ini menyulitkan pengguna dalam pengoperasiannya atau tidak. Tampilan antarmuka juga ada dalam dua kategori, yaitu antarmuka yang diterapkan untuk aplikasi Android dan antarmuka yang diterapkan untuk aplikasi web. Penjelasan tiap kategorinya sebagai berikut :

a. *Tampilan Pada Aplikasi Android*

Dalam aplikasi DroidVote ini terdapat beberapa tampilan antarmuka yang akan berhubungan langsung dengan pemilih. 4.1 adalah tampilan form autentikasi yang digunakan pemilih untuk memasukkan data – data autentikasinya yaitu berupa NIK, *Username dan Password*.

FORM AUTHENTICATION

NIK :

Username :

Password :

Authentication

Gambar 4.1 Form Atuthentication

Jika data yang diinputkan benar maka ketika tombol *authentication* ditekan maka akan keluar notifikasi yang menyatakan bahwa data *valid* seperti pada gambar 4.2, dan apabila data yang diinputkan tidak *valid* maka notifikasi yang keluar akan terlihat seperti gambar 4.3.

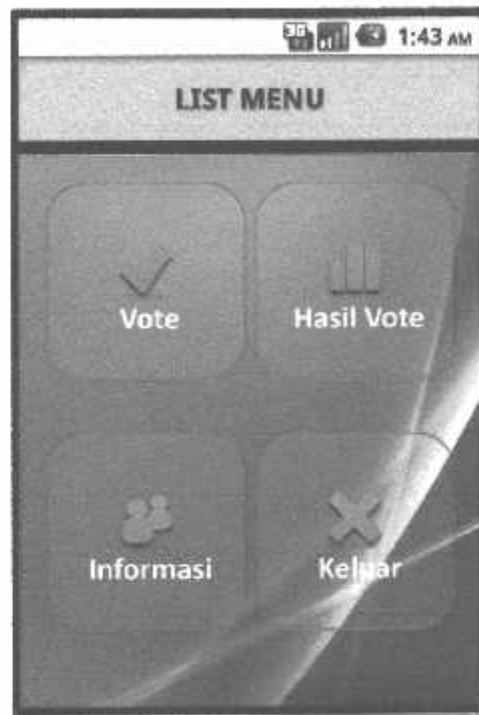


Gambar 4.2 Notifikasi Data Valid



Gambar 4.3 Notifikasi Data Tidak Valid

Setelah melewati proses autentikasi dan data dinyatakan valid, maka kemudian pemilih dibawa menuju ke halaman selanjutnya yaitu halaman *List Menu*. Gambar 4.4 adalah tampilan halaman *List Menu* dengan beberapa tombol untuk mengakses tiap – tiap menunya.



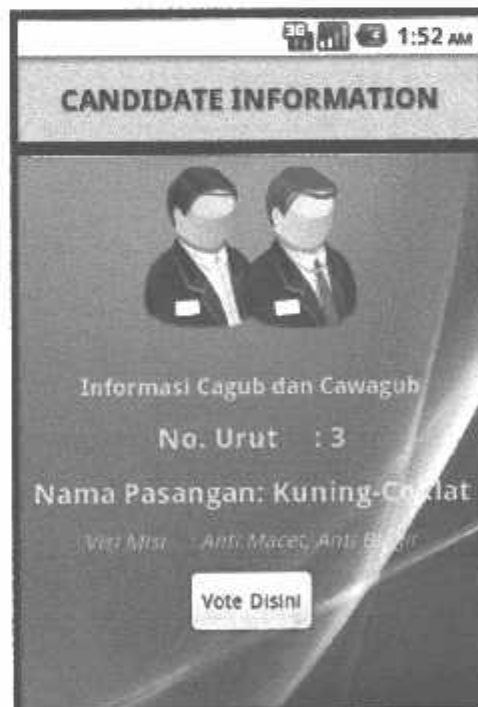
Gambar 4.4 Tampilan List Menu

Aplikasi ini dibangun dengan tujuan utama bisa digunakan untuk melakukan voting atau pemungutan suara sehingga bisa diasumsikan bahwa pemilih pertama kali mengakses menu vote ketika dibawa menuju halaman ini setelah melakukan proses autentikasi. Gambar 4.5 adalah halaman yang berbentuk *list* yang berisi nama para kandidat dengan visi dan misinya masing – masing, ini merupakan tampilan awal sebelum menuju tombol vote. Pada tampilan *list* ini pemilih bisa melihat – lihat profil detail setiap kandidat tanpa harus takut hak pilihnya akan hangus atau sudah dipergunakan, disamping itu dengan menggunakan aplikasi ini akan meminimalisir hingga 0% suara yang tidak sah atau bisa dikatakan semua suara yang digunakan untuk memilih berstatus suara sah.



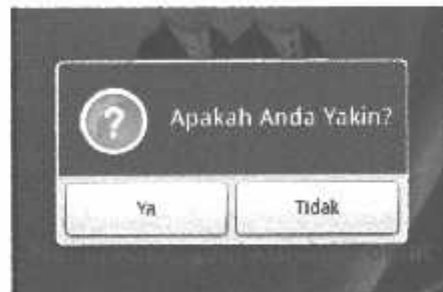
Gambar 4.5 Tampilan List Kandidat

Ketika pemilih sudah yakin dengan suara hatinya untuk memilih pasangan kandidat, maka keputusan ada pada tombol vote yang terdapat pada halaman profil setiap kandidat, bisa dilihat pada gambar 4.6.



Gambar 4.6 Tampilan Detail Kandidat

Apabila pemilih tiba - tiba mengalami ketidakyakinan dengan kandidat yang dia vote, sistem sudah dilengkapi dengan sebuah alert dialog seperti yang bisa dilihat pada gambar 4.7 yaitu menanyakan keyakinan pemilih terhadap kandidat yang akan divote, jika yakin maka tekan tombol ya dan suara akan ditambahkan serta secara otomatis pemilih akan dibawa ke halaman list menu dan jika tidak yakin maka tombol tidak adalah solusinya.



Gambar 4.7 Alert Dialog Vote

Setelah pemilih menggunakan hak pilihnya, halaman yang tadinya berada di halaman profil kandidat secara otomatis akan di *direct* menuju menu list kandidat. Dapat dilihat pada gambar 4.8, ini merupakan tampilan halaman menu list bagi pemilih yang telah menggunakan hak pilihnya, yaitu dengan dinonaktifkannya tombol menuju menu vote.



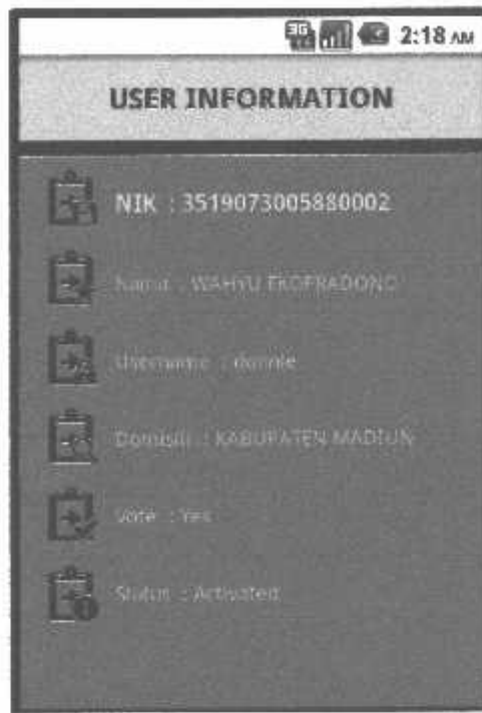
Gambar 4.8 Tampilan List Menu Setelah Voting

Menu lain yang bisa diakses adalah menu hasil vote. Gambar 4.9 adalah tampilan menu hasil vote. Pada halaman ini ditampilkan hasil perolehan suara dari tiap pasangan kandidat sekaligus dengan waktu vote terakhir suara yang masuk pada tiap kandidat.



Gambar 4.9 Tampilan Menu Hasil Vote

Menu terakhir yang dapat diakses oleh pemilih yaitu menu informasi pemilih. Disini pemilih dapat memastikan bahwa suaranya telah diperhitungkan dan dianggap sah. Gambar 4.10 adalah tampilan halaman yang didalamnya berisi tentang data diri dari pemilih seperti NIK, Nama, Username, Domisili, Status Voting dan Status Pemilih. Pada informasi pemilih ini akan terlihat perbedaannya apabila pemilih mengakses menu ini terlebih dahulu sebelum memilih menu voting karena informasi pada baris Status Voting bernilai "No" secara *default* yang artinya pemilih belum menggunakan hak pilihnya.



Gambar 4.10 Tampilan Menu Informasi Pemilih

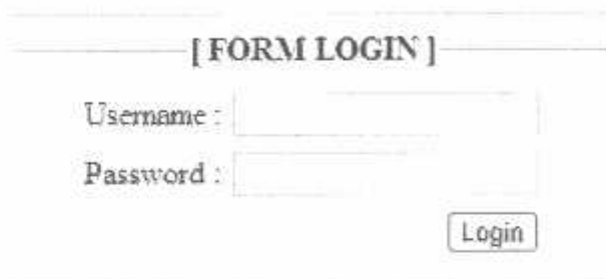
Jika dirasa cukup dan pemilih ingin keluar dari aplikasi maka pemilih bisa kembali menuju halaman list menu dengan menekan tombol kembali yang terdapat pada *device* android yang kemudian bisa dilanjutkan dengan menekan tombol keluar yang terdapat pada menu list. Gambar 4.11 adalah tampilan ketika pemilih menekan tombol keluar yaitu terdapat *alert dialog* untuk memastikan apakah pemilih benar – benar ingin keluar dari aplikasi.



Gambar 4.11 Alert Dialog Menu Keluar

b. Tampilan Pada Aplikasi Web

Dalam aplikasi web ini terdapat beberapa tampilan antarmuka yang akan berhubungan langsung dengan administrator dan pejabat KPUD yang berwenang. 4.12 adalah tampilan form login yang digunakan mereka untuk memasukkan username dan password sebagai inputan untuk mendapatkan hak akses terhadap sistem.



[FORM LOGIN]

Username :

Password :

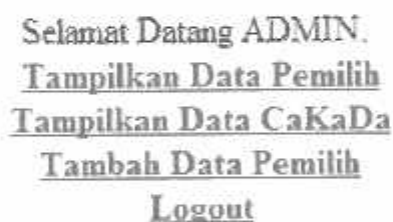
Login

Gambar 4.12 Form Login

Ada dua kondisi yang mempengaruhi tampilan tiap halamannya setelah *user* memasukkan *username* dan *password* yaitu kondisi bila *user* merupakan administrator dan kondisi bila *user* merupakan pejabat KPUD yang berwenang, berikut penjelasan tiap kondisinya :

1. Administrator.

Jika *user* dikategorikan sebagai administrator maka gambar 4.13 adalah tampilan halaman administrasinya yang berisi beberapa *link* halaman untuk melakukan *update data* dan *monitoring data*.



Selamat Datang ADMIN.
Tampilkan Data Pemilih
Tampilkan Data CaKaDa
Tambah Data Pemilih
Logout

Gambar 4.13 Halaman Administrasi ADMIN

Seperti yang terlihat pada gambar 4.13, Administrator memiliki akses ke beberapa halaman lain disamping halaman administrasinya sendiri, berikut penjelasan tiap halamannya :

a. Halaman Data Pemilih

[DATA PENDUDUK PROVINSI JAWA TIMUR]

NIK	Nama	Username	Password	Domisili	Voting	Status
3521134912090001	ASTRI NILAMKANI	astri	20132EA354475FD726952DA525462a6b75440C4	KABUPATEN NGAWI	No	
351807002020001	WAHYU EKOPRADONO	waHYU	427149C1225728A156455DD153409DE12032BA3	KABUPATEN MADURA	Yes	ACT-80-P
357801008020001	SASON ADI PUTRA	sason	45564bc457445CD4225128A115564EC927942CA4	KOTA MOJOKERTO	No	
3515150100870001	MULIAANGAD ANLITE	mulic	435049C166455BD224024A079624A475444Y4	KABUPATEN MADOARA	No	
357703050190001	ARI PRASTIAN DHANA	pr-a	225022AC4654DC55A4951D940546C425462a6b	KABUPATEN MALANG	Yes	ACT-80-P
357000500600001	ANA DWI WAHYUNI	ana	59425320425149C14A5841C944574FC73635DA5	KOTA MADURA	No	
3519070911550001	TINDANG MURNIATI	tindang	405249C34A5841C944574FC73635DA5	KABUPATEN MADURA	No	
352000670480001	RITA DIANA LANTH	rita	215022AC4654DC55A4951D940546C425462a6b	KABUPATEN MAGETAN	No	
350118070780001	SUYU LIANTI	suy	24072EA72632DA55F4C54DC485840C326832BA3	KABUPATEN TULUNGAGUNG	No	
3572030520190001	ANITA EARTH SYABINA	anita	20322EA357465CD4225128A115564EC927942CA4	KOTA MALANG	No	

Jumlah Record
11 Orang Pemilih Suara
Untuk Provinsi Jawa Timur

Halaman Administrasi
Tampilkan Data Cakada
Logout

Gambar 4.14 Halaman Data Pemilih (Administrator)

Gambar 4.14 merupakan halaman dimana data pemilih ditampilkan secara detail. Data yang ditampilkan meliputi NIK, nama, *username*, *password* yang terenkripsi, domisili, status *voting* dan status pemilih itu sendiri. Dengan tampilan *password* yang terenkripsi, telah menunjukkan bahwa hak akses Administrator terbatas.

b. Halaman Data Cakada

[DATA KANDIDAT CAGUB DAN CAWAGUB PROVINSI JAWA TIMUR]

No. Urut	Nama Pasangan	Jumlah Vote	Waktu Vote Terakhir	Visi Misi
1	Merah Hijau	12	2012-11-10 03:39:57	Sekolah Gratis, Makanan Gratis
2	Biru Orange	5	2012-11-10 03:54:56	Obat Gratis, Rumah Gratis
3	Kuning-Coklat	5	2012-11-12 14:02:51	Anti Macet, Anti Banjir
4	Hijau-Ungu	5	2012-11-10 04:02:58	Anti Korupsi, Anti Sogokan

Jumlah Record
4 Calon Pasangan Cagub dan Cawagub
Untuk Provinsi Jawa Timur

Halaman Administrasi
Tampilkan Data Pemilih
Logout

Gambar 4.15 Halaman Data Kandidat (Administrator)

Halaman ini berisi data detail dari pasangan kandidat. Gambar 4.15 menunjukkan bahwa jumlah suara yang diperoleh juga ditampilkan secara terbuka sekaligus dengan waktu terakhir suara masuk di tiap kandidatnya sehingga mencerminkan salah satu asas pemungutan suara yaitu *TERBUKA*

c. Halaman Tambah Data

[FORM TAMBAH DATA]

NIK : 1910

Nama : Nama

Username : 123456789

Domisili : Domisil

Submit

Tambah Data Orang Add

Gambar 4.16 Halaman Tambah Data

Administrator memiliki tugas untuk memasukkan semua data pemilih yang memiliki ktp aktif ke dalam sistem sebelum tanggal pemungutan suara. Gambar 4.16 merupakan *form* yang digunakan administrator untuk menambahkan pemilih baru kedalam sistem. Pada akhir *form* terdapat *form* kecil untuk menambahkan *form* sebanyak data baru yang akan disimpan sehingga administrator dapat lebih cepat bekerja daripada menggunakan satu *form* untuk menambahkan banyak data.

2. Pejabat KPUD

Selamat Datang KPUJATIM.
Tampilkan Data Pemilih
Tampilkan Data CaKaDa
Logout

Gambar 4.17 Halaman Administrasi KPUD

Seperti yang terlihat pada gambar 4.17, Administrator memiliki akses ke beberapa halaman lain disamping halaman administrasinya sendiri, berikut penjelasan tiap halamannya :

a. Halaman Data Pemilih

[DATA PENDUDUK PROVINSI JAWA TIMUR]

NIK	Nama	Username	Password	Domisili	Vote	Status
3521136812890001	ASTRI NILAMSANI	astri	2F47U	KABUPATEN NGAWI	No	
3519073005830002	WAHYU EKOPRADONO	donie	P0DA2	KABUPATEN MADIUN	Yes	Activated
3576013009830001	SASON ADI PUTRA	sason	WE0W5	KOTA MOJOKERTO	No	
3515150106970002	MUKHAMMAD ANCHE	anche	QB17U	KABUPATEN SIDOARJO	No	
3	de	de	1THY7	KABUPATEN MALANG	Yes	Activated
3577030504900002	ARYA PRATIWI DIANA	arya	JPNV4	KOTA MADIUN	No	
3519085506900001	ANA DWI WAHYUNI	ana	NK6XX	KABUPATEN MADIUN	No	
3519074912560002	ENDANG MURNIATI	endang	RXD13	KABUPATEN MADIUN	No	
3520036704830001	RITA DIANA SANTHI	rita	1DAHY	KABUPATEN MAGETAN	No	
3504193707920001	EVY YULIANTI	evi	64MY4	KABUPATEN TULUNGAGUNG	No	
3573035201900005	ANITA IZATHY CHAIRINA	anita	2EW86	KOTA MALANG	No	

Cetak Surat Undangan

Jumlah Record
11 Orang Pemilih Suara
Untuk Provinsi Jawa Timur

[Halaman Administrasi](#)
[Tampilkan Data Cakada](#)
[Logout](#)

Gambar 4.18 Halaman Data Pemilih (Pejabat KPUD)

Gambar 4.18 merupakan halaman dimana data pemilih ditampilkan secara detail. Halaman ini memiliki kesamaan dengan halaman data pemilih yang dimiliki oleh administrator, data yang ditampilkan meliputi NIK, nama, *username*, *password*, domisili, status *voting* dan status pemilih. Perbedaannya terletak pada tombol dan data *password* yang telah didekripsi. *Password* yang terdekripsi nantinya akan dicetak dalam bentuk surat undangan atau surat pemberitahuan pemungutan suara sehingga pemilih mendapatkan informasi yang akurat dan jelas sebelum melakukan proses pemungutan suara seperti yang ditampilkan pada Lampiran 2.

b. Halaman Data Cakada

Gambar 4.19 merupakan tampilan halaman data cakada dari sisi pejabat KPUD. Tombol yang ada didalam tabel berfungsi untuk mencetak hasil perolehan suara kedalam format laporan resmi yang nantinya digunakan untuk laporan kepada KPU tingkat pusat. Untuk hasil cetak laporan dapat dilihat pada Lampiran 3.

[DATA KANDIDAT CAGUB DAN CAWAGUB PROVINSI JAWA TIMUR]

No. Urut	Nama Pasangan	Jumlah Vote	Waktu Vote Terakhir	Visi Misi
1	Merenh-Hjira	1,2	2012-11-10 03:39:57	Sekolah Gratis, Milikn Gratis
2	Risa-Orange	5	2012-11-10 03:54:36	Cibin Gratis, Rumah Gratis
3	Kisang-Coklat	5	2012-11-12 14:02:51	Anti Mabar, Anti Pinjol
4	Hizani-Ungu	3	2012-11-10 04:02:34	Anti Korupsi, Anti Sogokan

[Detail Hasil Perolehan]

Jumlah Record
1 Calon Pasangan Cagub dan Cawagub
Untuk Provinsi Jawa Timur

[Halaman Administrasi](#)
[Tampilkan Data Pemilih](#)
[Logout](#)

Gambar 4.19 Halaman Data Kandidat (Pejabat KPUD)

4.2 Pengujian

Bagian ini berisi penjelasan mengenai pengujian terhadap aplikasi yang telah diimplementasikan. Metode pengujian yang dipakai adalah metode *black – box* yaitu pengujian yang memperhatikan *input* dan *output* dari *use case* yang dijalankan.

4.2.1 Tujuan Pengujian

Setelah membuat rancangan sistem aplikasi dan mengimplementasikannya kedalam aplikasi maka kemudian dilakukan pengujian terhadap aplikasi tersebut. Tujuan dilakukannya pengujian adalah :

- Menguji apakah aplikasi telah berjalan sesuai dengan rancangan sistem yang telah dibuat dan sesuai dengan sasaran pembuatan aplikasi.
- Menguji apakah implementasi dari aplikasi *e-voting* ini telah berjalan dengan baik atau tidak sesuai dengan skenario yang telah dirancang.

4.2.2 Lingkungan Pengujian

Lingkungan pengujian Aplikasi *e-voting* ini akan dilakukan dengan spesifikasi perangkat keras dan perangkat lunak sebagai berikut

4.2.2.1. Spesifikasi Perangkat Keras

- a. Prosesor AMD Athlon II Dual-Core Processor 2.1 GHz dengan RAM 4GB dilengkapi VGA ATI Mobility RADEON HD 4200.
- b. Modem dengan koneksi internet.
- c. Device Android Samsung Galaxy Mini GT-S5570
- d. Device Android Sony Xperia P LT22i

4.2.2.2. Spesifikasi Perangkat Lunak

- a. Sistem Operasi Windows 7 Ultimate 32bit.
- b. Browser Mozilla Firefox 19.0
- c. Browser Google Chrome 25.0
- d. Sistem Operasi Android 2.3.7 CyanogenMod 7.2.0 RC4
- e. Sistem Operasi Android 4.0.4 (Ice Cream Sandwich)

4.2.3 Hasil Pengujian

Berikut ini adalah hasil pengujian yang dilakukan pada aplikasi DroidVote. Ada dua tabel pengujian yang akan di jelaskan disini yaitu tabel pengujian berdasarkan pada fungsional sistem dan tabel pengujian algoritma kriptografi terhadap delapan data *password* berdasarkan hitungan manual yang nantinya akan diketahui apakah menghasilkan hasil enkripsi *password* yang sama seperti yang dihasilkan oleh sistem.

4.2.3.1. Pengujian Fungsional Sistem

Tabel 4.3 Hasil Pengujian Fungsional Sistem

No	Uraian Fungsi	Berjalan Pada Sisi User		Platform Pengujian			
				Android		Browser	
		Pemilih	Admin	2.3.7	4.0.4	Mozilla Firefox	Google Chrome
1	Autentikasi	√	-	√	√	-	-
2	Voting	√	-	√	√	-	-
3	Akumulasi Suara	√	-	√	√	-	-
4	Memantau Hasil Voting	√	-	√	√	-	-
5	Melihat Data Diri	√	-	√	√	-	-
6	Keluar Aplikasi	√	-	√	√	-	-
7	Login Web Service	-	√	-	-	√	√
8	Tambah Data Pemilih	-	√	-	-	√	√
9	Melihat Data Pemilih	-	√	-	-	√	√
10	Melihat Data Kandidat	-	√	-	-	√	√

11	Cetak Undangan Pemilukada	-	√	-	-	√	√
12	Cetak Laporan Pemilukada	-	√	-	-	√	√
13	Logout Web Service	-	√	-	-	√	√

4.2.3.2. Pengujian Algoritma Kriptografi Sistem

Tabel 4.4 Hasil Pengujian Algoritma Kriptografi Sistem

No	Plain Password	Tahap Modifikasi Hexadesimal				Chiper Password		
		1	2	3	4	Hasil Manual	Hasil Sistem	
1	DS3Q3	D	56	45	5D	D5	56455DD5	56455DD5
		S	41	52	4A	C2	41524AC2	41524AC2
		3	21	32	2A	A2	21322AA2	21322AA2
		Q	43	50	48	C0	435048C0	435048C0
		S	21	32	2A	A2	21322AA2	21322AA2
2	9SG1U	9	2B	38	20	A8	2B3820A8	2B3820A8
		S	41	52	4A	C2	41524AC2	41524AC2
		G	55	46	5E	D6	55465ED6	55465ED6
		1	23	30	28	A0	233028A0	233028A0
		U	47	54	4C	C4	47544CC4	47544CC4
3	KF2IT	K	59	4A	52	DA	594A52DA	594A52DA
		F	54	47	5F	D7	54475FD7	54475FD7
		2	20	33	2B	A3	20332BA3	20332BA3
		I	5B	48	50	D8	5B4850D8	5B4850D8
		T	46	55	4D	C5	46554DC5	46554DC5
4	V4Y9X	V	44	57	4F	C7	44574FC7	44574FC7
		4	26	35	2D	A5	26352DA5	26352DA5
		Y	4B	58	40	C8	4B5840C8	4B5840C8
		9	2B	38	20	A8	2B3820A8	2B3820A8
		X	4A	59	41	C9	4A5941C9	4A5941C9

5	DTT5Z	D	56	45	5D	D5	56455DD5	56455DD5
		T	46	55	4D	C5	46554DC5	46554DC5
		T	46	55	4D	C5	46554DC5	46554DC5
		5	27	34	2C	A4	27342CA4	27342CA4
		Z	48	5B	43	CB	485B43CB	485B43CB
6	G52MH	G	55	46	5E	D6	55465ED6	55465ED6
		5	27	34	2C	A4	27342CA4	27342CA4
		2	20	33	2B	A3	20332BA3	20332BA3
		M	5F	4C	54	DC	5F4C54DC	5F4C54DC
		H	5A	49	51	D9	5A4951D9	5A4951D9
7	RR6DI	R	40	53	4B	C3	40534BC3	40534BC3
		R	40	53	4B	C3	40534BC3	40534BC3
		6	24	37	2F	A7	24372FA7	24372FA7
		D	56	45	5D	D5	56455DD5	56455DD5
		I	5B	48	50	DB	5B4850DB	5B4850DB
		M	5F	4C	54	DC	5F4C54DC	5F4C54DC
8	M08VS	0	22	31	29	A1	223129A1	223129A1
		8	2A	39	21	A9	2A3921A9	2A3921A9
		V	44	57	4F	C7	44574FC7	44574FC7
		S	41	52	4A	C2	41524AC2	41524AC2

BAB V

KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran – saran yang bersifat membangun sebagai sarana untuk menambah pengetahuan penulis dalam penyusunan skripsi serta sebagai bahan acuan kedepan dalam pengembangan aplikasi *e-voting* berbasis sistem operasi android.

5.1 Kesimpulan

Dari hasil pengembangan dan proses pengujian aplikasi *e-voting* DroidVote berbasis android yang menggunakan algoritma kriptografi sebagai sistem keamanan datanya dapat diambil kesimpulan sebagai berikut :

- a. Pengujian fungsi – fungsi sistem terhadap platform *web service* menggunakan media *web browser* berjalan sesuai dengan yang diharapkan.
- b. Pengujian fungsi – fungsi sistem terhadap platform sistem operasi android berjalan baik dan akurat.
- c. Perhitungan manual algoritma kriptografi yang diterapkan kedalam sistem memiliki *output* yang sama dengan perhitungan otomatis sistem.

5.2 Saran

Aplikasi *e-voting* DroidVote berbasis sistem operasi Android yang dibangun merupakan aplikasi *e-voting* generasi pertama yang dibangun oleh penulis sehingga masih membutuhkan pengembangan dalam segi fitur dan *user-interface*. Oleh sebab itu perlu dilakukan pengembangan ke arah yang lebih baik guna memenuhi kebutuhan setiap proses pemungutan suara di semua tingkat. Adapun saran – saran terhadap pengembangan aplikasi *e-voting* DroidVote ke depan adalah sebagai berikut :

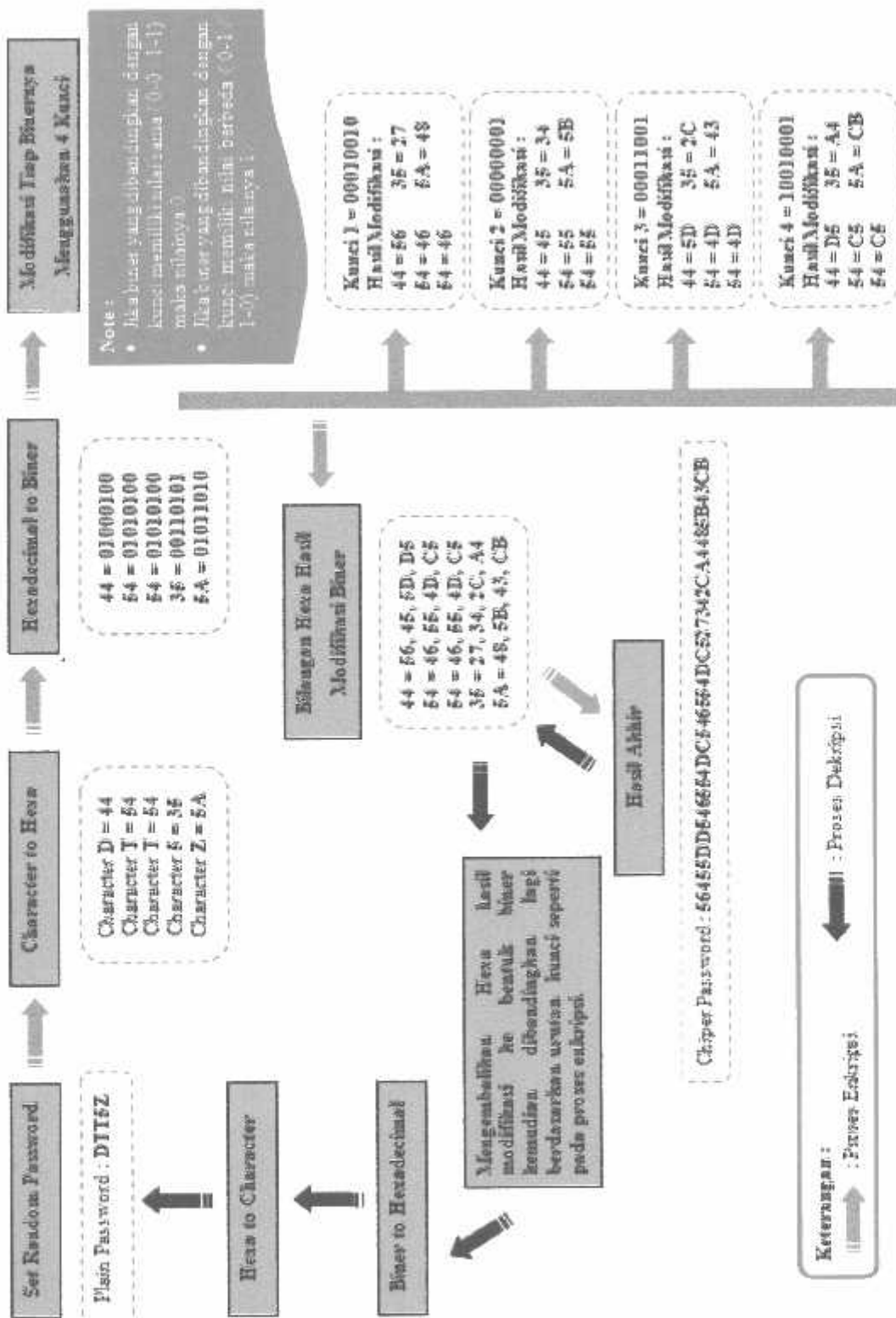
- a. Aplikasi yang sudah ada dapat dikembangkan dengan menambahkan data - data pendukung seperti menampilkan hasil perolehan suara tiap kota dan adanya *time counter* sebagai batas penutupan proses pemungutan suara.
- b. Untuk proses enkripsi dan dekripsi data yang lebih optimal dapat digunakan algoritma kriptografi lain seperti RSA dan AES.

DAFTAR PUSTAKA

1. Achmad Rouzni Noor, 2012, *E-Voting, Inovasi Teknologi untuk Pungutan Suara*, diakses 30 Oktober 2012 dari <http://inet.detik.com/read/2012/03/21/135658/1873345/398/e-voting-inovasi-teknologi-untuk-pungutan-suara.html>
2. Andry, 2011, *Android A sampai Z, Bandung*, PC Plus
3. Andry Chowanda, 2012, *Perancangan Aplikasi Pencarian Buku Berdasarkan Lokasi Dengan Menggunakan Sistem Operasi Android (e-thesis)*, Jakarta, Bina Nusantara, diunduh 2 November 2012.
4. Anjar Febri, 2009, *E-Voting Application Based on Client-Server (Examples case the Chairman of General Elections in Forums Warga Betawi Ciracas Jakarta) (e-thesis)*, Bandung, UNIKOM, diunduh 30 Oktober 2012.
5. Dave Springgay, Jin Li, Julian Jones, Greg Adams, 2002, *Eclipse User Interface Guidelines*, Object Technology International, Inc. and others, diakses 2 November 2012 dari <http://www.eclipse.org/articles/Article-UI-Guidelines/v200202/Contents.html>
6. Esti Rahmawati Agustina, Agus Kurniati, 2009, *Pemanfaatan Kriptografi Dalam Mewujudkan Keamanan Informasi Pada e-Voting Di Indonesia (e-thesis)*, Yogyakarta, UPN "Veteran" Yogyakarta, diunduh 04 November 2012.
7. Hadi, IT Training Center, 2011, *Android (e-book)*, diunduh 02 November 2012.
8. Hendriansyah, 2010, *Implementasi Polling Dengan SMS Gateway Berbasis Web (e-thesis)*, Medan, Universitas Sumatra Utara, diunduh 01 November 2012.
9. Jaringan Anti Korupsi, *Melawan Lupa: Cara Soekarwo - Saifulah memenangkan PII/UB Jatim pada tahun 2008*, 2009, diakses 17 November 2012.
10. JavaSoft White Paper, *The Java Language: An Overview*, Diakses 31 Oktober 2012, dari <http://java.sun.com/doc/Overviews/java>
11. M. Shalahuddin, 2009, *Pembuatan Model E-Voting Berbasis Web (Studi Kasus Pemilu Legislatif Dan Presiden Indonesia)(e-thesis)*, Bandung, Institut Teknologi Bandung, diunduh 30 Oktober 2012.
12. Prof. Dr. Rolf Dornberger, 2011, *JDK/SDK/JRE and Java Development-Tools (Programming with Java) (e-book)*, Advanced Technologies Supporting Business Areas, diunduh 31 Oktober 2012.
13. Rokhman, A., 2011, *Prospek dan Tantangan Penerapan e-Voting di Indonesia. (Seminar Nasional Peran Negara dan Masyarakat dalam Pembangunan Demokrasi dan*

Masyarakat Madani di Indonesia, 7 Juli 2011)(e-thesis), Jakarta, Universitas Terbuka, diunduh 30 Oktober 2012.

14. Witarjo, 2010, *SIG Kepadatan Lalu Lintas Dan Daerah Rawan Kecelakaan Kota Surabaya*, Surabaya, Institut Teknologi Sepuluh November (e-thesis), diunduh 1 November 2012.





INTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
PROGRAM STUDI TEKNIK INFORMATIKA S-1
Jl. Karanglo Km. 2 Malang


**BERITA ACARA UJIAN SKRIPSI
FAKULTAS TEKNOLOGI INDUSTRI**

Nama : Wahyu Ekopradono
NIM : 08.18.050
Jurusan : Teknik Informatika S-1
Judul : Droidvote, Apikasi E-Voting Menggunakan Algoritma Kriptografi Berbasis Sistem Operasi Android

Dipertahankan dihadapan Majelis Penguji Skripsi Jenjang Strata Satu (S-1) pada :
Hari : Selasa
Tanggal : 19 Februari 2013
Nilai : 81,65 (A)

Panitia Ujian Skripsi :

Ketua Majelis Penguji


Joseph Dedy Irawan, ST, MT
NIP. 197404162005011022

Anggota Penguji :

Penguji Pertama



Febriana Santi W., S.Kom, M.Kom
NIP.P. 1031000425

Penguji Kedua



Karina Aulisari, ST, M.Eng
NIP.P. 1031000426



FORMULIR PERBAIKAN SKRIPSI

Nama : Wahyu Ekopradono
NIM : 08.18.050
Jurusan : Teknik Informatika S-1
Judul : Droidvote, Aplikasi E-Voting Menggunakan Algoritma Kriptografi Berbasis Sistem Operasi Android

Tanggal	Penguji	Uraian	Paraf
19 - 02 - 2013	I	1. Flowchart Algoritma Kriptografi 2. Kesimpulan Bab V 3. Rapikan Format Penulisan	
19 - 02 - 2013	II	1. Daftar Pustaka 2. Kesimpulan Bab IV 3. Flowchart Algoritma Kriptografi 4. Blok Diagram Sistem 5. Teori Bab II terlalu banyak	

Anggota Penguji :

Penguji Pertama

Febriana Santi W., S.Kom, M.Kom
NIP.P. 1031000425

Penguji Kedua

Karina Anisari, ST, M.Eng
NIP.P. 1031000426

Mengetahui

Dosen Pembimbing I

Dr. Ir. Dayal Gustopo S, MT
NIP. 103940264

Dosen Pembimbing II

Mira Orisa, ST
NIP. P. 1031000435



FORMULIR BIMBINGAN SKRIPSI

Nama : Wahyu Ekopradono
NIM : 08.18.050
Judul : Droidvote, Apikasi E-Voting Menggunakan Algoritma Kriptografi Berbasis Sistem Operasi Android

No	Tanggal	Uraian	Paraf
1	19/ 11/ 2012	Perbaiki BAB I, Rumusan Masalah, Tujuan	
2	19/ 11/ 2012	Perbaiki BAB II, Penambahan data real	
3	23/ 11/ 2012	ACC BAB I ,II, III, IV	
4	03/ 12/ 2012	Perbaiki BAB V, Kesimpulan dan Saran	
5	04/ 12/ 2012	ACC BAB V	
6	7/ 12/ 2012	ACC Makalah Seminar Hasil	
7			
8			

Malang, 5 Maret 2013

Dosen Pembimbing I

Dr. Ir. Dayal Gustopo S, MT
NIP. 103940264

Form S-4b



FORMULIR BIMBINGAN SKRIPSI

Nama : Wahyu Ekopradono
NIM : 08.18.050
Judul : Droidvote, Apikasi E-Voting Menggunakan Algoritma Kriptografi Berbasis Sistem Operasi Android

No	Tanggal	Uraian	Paraf
1	10/ 11/ 2012	Revisi BAB III masalah ERD sistem	
2	13/ 11/ 2012	ACC BAB III	
3	24/ 11/ 2012	Preview BAB I, II, IV	
4	27/ 11/ 2012	Revisi Teknis BAB IV	
5	04/ 11/ 2012	ACC BAB I, II, IV	
6	08/ 12/ 2012	Preview dan ACC BAB V	
7	15/ 12/ 2012	ACC Makalah Seminar Hasil	
8			

Malang, 5 Maret 2013
Dosen Pembimbing II

Mira Orisa, ST
NIP. P. 1031000435

Form S-4b