# BAB 2
# TINJAUAN PUSTAKA

## 2.1 Studi Literatur

Adapun review literatur yang menjadi referensi dan memiliki keterkaitan dengan penelitian dapat dilihat pada Tabel 2.1, sebagai berikut :

**Tabel 2.1 Studi Literatur**

| Review Literatur Pertama | |
|---|---|
| Judul Artikel | New Fully Homomorphic Encryption Scheme Based On Multistage Partial Homomorphic Encryption Applied In Cloud Computing[9] |
| Penulis | Zainab Hikmat Mahmood, Mahmood Khalel Ibrahem |
| Judul Jurnal / Proceeding | International Conference on Information and Sciences (AICIS) |
| Tahun Penerbit | 2018 |
| Masalah Utama yang diangkat | Permasalahan keamanan di datacenter yang tidak terenkripsi. |
| Kontribusi Penulis | Melakukan Analisis teori perhitungan Fully Homomorphic Encryption Scheme di Cloud Computing |
| Ikhtisar Artikel | Dalam penelitian ini dilengkapi dengan teknologi Homomorphic encryption, sehingga sistem yang dibuat dapat lebih aman lalu dilakukan pengujian berkaitan dengan tingkat kecepatan yang meningkat, pengurangan waktu komputasi, meningkatkan kerahasian terkait data yang disimpan di komputasi awan. |

| Review Literatur Pertama | |
|---|---|
| Hasil Penelitian, Kesimpulan dan Saran | a. Hasil Penelitian : sebuah sistem yang menggunakan fully homomorphic encryption scheme yang dibangun berdasarkan partial homomorphic dalam pengamanan data di komputasi awan.<br>b. Kesimpulan : dengan mengkombinasikan partial dan fully homomorphic didapati dapat mengurangi waktu komputasi dan meningkatkan level keamanan. |
| Persamaan dan Perbedaan dengan penelitian | a. Persamaan : pemanfaatan teknologi Homomorphic encryption dalam mengamankan data<br>b. Perbedaan : Dalam hal penerapan dan cakupan sistem. |
| Komentar | Literatur memberikan gambaran mengani penggunaan homomorphic encryption dalam pengamanan data. |
| Review Literatur Kedua | |
| Judul Artikel | Advanced E-Voting System Using Paillier Homomorphic Encryption Algorithm[10] |
| Penulis | Shifa Manaruliesya Anggriane, Surya Michrandi Nasution, Fairuz Azmi |
| Judul Jurnal / Proceeding | International Conference on Informatics and Computing (ICIC) |
| Tahun Penerbit | 2016 |
| Masalah Utama yang diangkat | Melakukan perhitungan efektifitas algoritma homomorphic encryption |
| Kontribusi Penulis | Melakukan analisis terkait homomorphic encryption di e-voting. |
| Ikhtisar Artikel | Melakukan analisis penggunaan homomorphic encryption dalam e-voting dimana difokuskan ke analisis perhitungan ciphertextnya. |

| | |
|---|---|
| Review Literatur Kedua | |
| Hasil Penelitian, Kesimpulan dan Saran | a. Hasil Penelitian : hasil analisis homomorphic encryption dapat memberikan kerahasian yag baik dalam melakukan pengamanan/perhitungan data voting di sistem.<br>b. Kesimpulan : hasil nilai ciphertext berbeda satu sama lain walupun nilai yang diencryption sama.<br>Saran : - |
| Persamaan dan Perbedaan dengan penelitian | a. Persamaan : menggunakan homomorphic encryption<br>b. Perbedaan : Dalam penerapan dan cakupan sistem. |
| Komentar | - |
| Review Literatur Ketiga | |
| Judul Artikel | Fully Homomorphic Encryption Schemes: the State of The Art [15] |
| Penulis | Konstantin G. Kogos, Kseniia S. Filippova, Anna V. Epishkina |
| Judul Jurnal / Proceeding | IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) |
| Tahun Penerbit | 2017 |
| Masalah Utama yang diangkat | Performisasi di homomorphic encryption |
| Kontribusi Penulis | Melakukan analisis homomorphic encryption dan melakukan perbandingan berdasarkan sistem yang digunakan. |
| Ikhtisar Artikel | Dalam penelitian ini penulis melakukan perbandingan performa dari skema yang digunakan, mulai dari perbedaan skema hingga pemanfaatan Cryptograf di database untuk meningkatkan level keamanan denganCryptDB. |
| | |

| | |
|---|---|
| Review Literatur Ketiga | |
| Hasil Penelitian, Kesimpulan dan Saran | a. Hasil Penelitian : enkripsi homomorphic menyebabkan tingkat keamanan meningkat dalam menyimpan dana.<br>b. Kesimpulan : kebanyakan skema yang digunakan masih memiliki komplesitas komputasi terlalu tinggi yang membuat penggunannya bermasalah.<br>Saran : survey singkat mengenai skema FHE serta menganalisis fungsionalitasnya dalam konteks operasi khusu basis data. |
| Persamaan dan Perbedaan dengan penelitian | a. Persamaan : menggunakan homomorphic envryption dalam aspek keamanan<br>b. Perbedaan : dilakukan implementasi, diterapkan cakupan sistem. Database yang digunakan berbeda. |
| Komentar | Literatur melihat homomorphic dari segi matemati dan gerbang logikanya. |
| Review Literatur Keempat | |
| Judul Artikel | BrocoVote: Secure System using Ethereum's Blockchain[12] |
| Penulis | Gaby G.Dagher, Franeeth Babu Marella, Matca Milojkovic, dan Jordan Mohler |
| Judul Jurnal/Proceeding | Science and Technology Publication |
| Tahun Penerbit | 2018 |
| Masalah Utama yang diangkat | e-voting yang belum efektif dari segi efisiensi dan keamanan. |
| Kontribusi Penulis | Membuat konsep suatu sistem yang menggunakan ethereum dan pailer encription lalu mengimplementasikannnya sistem tersebut bernama BrovoVote. |
| | |

| Review Literatur Keempat | |
|---|---|
| Ikhtisar Artikel | Penulis membuat konsep e-voting yang menggunakan blockchain dan homomorphic dengan studi kasus yang universal dimulai dengan menjeaskan siapa saja penggunanya lalu dilanjutkan dengan fungsionalitas apa saja yang akan dibangun. |
| Hasil Penelitian, Kesimpulan dan saran | a. Hasil Penelitian : suatu konsep yang terkait pemanfaatan blockchain dan homomorphic encryption di sistem e-voting<br>b. Kesimpulan :sistem ini sangat mudah untuk diimplementasikan dan diatur sesuai dengan kasus kasus serupa.<br>c. Saran : - |
| Persamaan dan Perbedaan dengan penelitian | a. Persamaan : membangun konsep dan mengimplementasikan homomorphic encryption<br>b. Perbedaan : berbeda cakupan sistem dan studi kasus dimana ini dibangun untuk lingkungan KPU kota bandung, penulis lebih fokus terhadap enkripsi dan proses perifikasi pemilihnya. |
| Komentar | - |
| Review Literatur Kelima | |
| Judul Artikel | Pengembangan Aplikasi E-Voting Menggunakan Enkripsi Homomorphik[8] |
| Penulis | Muhtar Hartopo, Dr. Ir. Rinaldi Munir, S.T., M.T. |
| Judul Jurnal/Proceeding | STEI - Teknik Informatika |
| Tahun Penerbit | 2017 |
| Masalah Utama yang diangkat | Resiko Keamanan di E-Voting |
| Kontribusi Penulis | Memberikan gambaran pengujian keamanan e-voting untuk pengujian akhir. |
| | |

| Review Literatur Kelima | |
|---|---|
| Ikhtisar Artikel | Penulis mengembangkan aplikasi E-voting mengunakan enkripsi homomorphic sebagai pengaman datanya. |
| Hasil Penelitian, Kesimpulan dan saran | a. Hasil Penelitian : suatu sistem e-voting yang menggunakan enkripsi homomorphic.<br>b. Kesimpulan :Enkripsi homomorfik parsaal yang bersifat additive dapat diterapkan pada sistem e-voting.<br>c. Saran : - |
| Persamaan dan Perbedaan dengan penelitian | a. Persamaan : membangun e-voting dengan enkripsi homomorphic.<br>b. Perbedaan : implementasi secara real diterakpakn untuk KPU, dan verifikasi wajah. |
| Komentar | - |
| Review Literatur Keenam | |
| Judul Artikel | RANCANG BANGUN APLIKASI E-VOTING PEMILIHAN GEUCHIK PADAKECAMATAN KLUET UTARA ( SK: DI DESA KRUENG BATEE )BERBASIS WEB[7] |
| Penulis | Cut Fachrul Rozi, Sarini Vita Dewi |
| Judul Jurnal/Proceeding | Journal of Informatics and Computer Science Vol. 6 |
| Tahun Penerbit | 2020 |
| Masalah Utama yang diangkat | Meningkatkan efisiensi dari proses pemiliahan konsensional menjadi online. |
| Kontribusi Penulis | Memberikan Gambaran sederhana penerapan E-voting. |
| Ikhtisar Artikel | Penulis mengembangkan E-voting yang nyaman mudah dimengerti untuk pengguna dan penyelenggara proses pemungutan suara. |
| | |

| Review Literatur Keenam | |
|---|---|
| Hasil Penelitian, Kesimpulan dan saran | a. Hasil Penelitian :suatu sistem e-voting.<br>b. Kesimpulan :e-voting akan berjalan lancar jika digunakan dengan semestinya, juga dengan e-voting mempermudah dan meningkatkan efisinesi proses pemungutan suara.<br>Saran : - |
| Persamaan dan Perbedaan dengan penelitian | a. Persamaan :membangun suatu sistem e-voting.<br>b. Perbedaan : penggunaan enkripsi homomorfik. |
| Komentar | - |

## 2.2 Profil Komisi Pemilihan Umum (KPU)Kota Bandung

Komisi Pemilihan Umum (KPU) adalah lembaga penyelenggara pemilu yang bersifat nasional, tetap, dan mandiri yang bertugas melaksanakan pemilu[1]. Komisi Pemilihan Umum (KPU) Kota Bandung adalah lembaga yang bertanggung jawab dalam Pemilihan Umum di Kota Bandung. Komisi Pemilihan Umum (KPU) Kota Bandung beralamat di Dln. Soekarno Hatta No. 260 Bandung dengan kode POS 40286.

### 2.2.1 Sejarah Komisi Pemilihan Umum

KPU yang ada sekarang merupakan KPU kelima yang dibentuk sejak era Reformasi 1998. KPU pertama (1999-2001) dibentuk dengan Keppres No 16 Tahun 1999, beranggotakan 53 orang anggota, dari unsur pemerintah dan Partai Politik. KPU pertama dilantik Presiden BJ Habibie. KPU kedua (2001-2007) dibentuk dengan Keppres No 10 Tahun 2001, beranggotakan 11 orang, dari unsur akademis dan LSM. KPU kedua dilantik oleh Presiden Abdurrahman Wahid (Gus Dur) pada tanggal 11 April 2001.

KPU ketiga (2007-2012) dibentuk berdasarkan Keppres No 101/P/2007 yang berisikan tujuh orang anggota yang berasal dari anggota KPU Provinsi, akademisi, peneliti dan birokrat dilantik tanggal 23 Oktober 2007 minus

Syamsulbahri yang urung dilantik Presiden karena masalah hukum. KPU keempat (2012-2017) dilantik oleh Presiden Susilo Bambang Yudhoyono yang diketuai oleh Husni Kami Malik. Selanjutnya KPU yang kelima (2017-2022) dilantik oleh Presiden Joko Widodo, yang saat ini diketuai oleh Arief Budiman. Untuk menghadapi pelaksanaan Pemilihan Umum, image KPU harus diubah sehingga KPU dapat berfungsi secara efektif dan mampu memfasilitasi pelaksanaan Pemilu yang jujur dan adil. Terlaksananya Pemilu yang jujur dan adil tersebut merupakan faktor penting bagi terpilihnya wakil rakyat yang lebih berkualitas, dan mampu menyuarakan aspirasi rakyat. Sebagai anggota KPU, integritas moral sebagai pelaksana pemilu sangat penting, selain menjadi motor penggerak KPU juga membuat KPU lebih kredibel di mata masyarakat karena didukung oleh personal yang jujur dan adil. Tepat tiga tahun setelah berakhirnya penyelenggaraan Pemilu 2004, muncul pemikiran di kalangan pemerintah dan DPR untuk meningkatkan kualitas pemilihan umum, salah satunya kualitas penyelenggara Pemilu. Sebagai penyelenggara pemilu, KPU dituntut independen dan non-partisan. Untuk itu atas usul insiatif DPR-RI menyusun dan bersama pemerintah mensyahkan Undang-undang Nomor 22 Tahun 2007 Tentang Penyelenggara Pemilu. Sebelumnya keberadaan penyelenggara Pemilu terdapat dalam Pasal 22-E Undang-undang Dasar Tahun 1945 dan Undang-undang Nomor 12 Tahun 2003 Tentang Pemilu DPR, DPD dan DPRD, Undang-undang Nomor 23 Tahun 2003 Tentang Pemilu Presiden dan Wakil Presiden.

Dalam Undang-undang Nomor 22 Tahun 2007 Tentang Penyelenggara Pemilu diatur mengenai penyelenggara Pemilihan Umum yang dilaksanakan oleh suatu Komisi Pemilihan Umum (KPU) yang bersifat nasional, tetap, dan mandiri. Sifat nasional mencerminkan bahwa wilayah kerja dan tanggung jawab KPU sebagai penyelenggara Pemilihan Umum mencakup seluruh wilayah Negara Kesatuan Republik Indonesia. Sifat tetap menunjukkan KPU sebagai lembaga yang menjalankan tugas secara berkesinambungan meskipun dibatasi oleh masa jabatan tertentu. Sifat mandiri menegaskan KPU dalam menyelenggarakan Pemilihan Umum bebas dari pengaruh pihak mana pun. Perubahan penting dalam undang-undang Nomor 22 Tahun 2007 Tentang Penyelenggara Pemilu, meliputi pengaturan mengenai lembaga penyelenggara Pemilihan Umum Anggota Dewan

Perwakilan Rakyat, Dewan Perwakilan Daerah, dan Dewan Perwakilan Rakyat Daerah, Pemilihan Umum Presiden dan Wakil Presiden; serta Pemilihan Umum Kepala Daerah dan Wakil Kepala Daerah yang sebelumnya diatur dalam beberapa peraturan perundang-undangan kemudian disempurnakan dalam 1 (satu) undang-undang secara lebih komprehensif.

Dalam undang-undang Nomor 22 Tahun 2007 Tentang Penyelenggara Pemilu diatur mengenai KPU, KPU Provinsi, dan KPU Kabupaten/Kota sebagai lembaga penyelenggara pemilihan umum yang permanen dan Bawaslu sebagai lembaga pengawas Pemilu. KPU dalam menjalankan tugasnya bertanggung jawab sesuai dengan peraturan perundang-undangan serta dalam hal penyelenggaraan seluruh tahapan pemilihan umum dan tugas lainnya. KPU memberikan laporan Presiden kepada Dewan Perwakilan Rakyat.

Undang-undang Nomor 22 Tahun 2007 Tentang Penyelenggara Pemilu juga mengatur kedudukan panitia pemilihan yang meliputi PPK, PPS, KPPS dan PPLN serta KPPSLN yang merupakan penyelenggara Pemilihan Umum yang bersifat ad hoc. Panitia tersebut mempunyai peranan penting dalam pelaksanaan semua tahapan penyelenggaraan Pemilihan Umum dalam rangka mengawal terwujudnya Pemilihan Umum secara langsung, umum, bebas, rahasia, jujur, dan adil.

Dalam rangka mewujudkan KPU dan Bawaslu yang memiliki integritas dan kredibilitas sebagai Penyelenggara Pemilu, disusun dan ditetapkan Kode Etik Penyelenggara Pemilu. Agar Kode Etik Penyelenggara Pemilu dapat diterapkan dalam penyelenggaraan Pemilihan Umum, dibentuk Dewan Kehormatan KPU, KPU Provinsi, dan Bawaslu.

Di dalam Undang-undang Nomor 12 Tahun 2003 Tentang Pemilu DPR, DPD dan DPRD, jumlah anggota KPU adalah 11 orang. Dengan diundangkannya Undang-Undang Nomor 22 Tahun 2007 Tentang Penyelenggara Pemilu, jumlah anggota KPU berkurang menjadi 7 orang. Pengurangan jumlah anggota KPU dari 11 orang menjadi 7 orang tidak mengubah secara mendasar pembagian tugas, fungsi, wewenang dan kewajiban KPU dalam merencanakan dan melaksanakan tahap-tahap, jadwal dan mekanisme Pemilu DPR, DPD, DPRD, Pemilu Presiden/Wakil Presiden dan Pemilu Kepala Daerah Dan Wakil Kepala Daerah.

Menurut Undang-undang Nomor 22 Tahun 2007 Tentang Penyelenggara Pemilu, komposisi keanggotaan KPU harus memperhatikan keterwakilan perempuan sekurang-kurangnya 30% (tiga puluh persen). Masa keanggotaan KPU 5 (lima) tahun terhitung sejak pengucapan sumpah/janji. Penyelenggara Pemilu berpedoman kepada asas: mandiri; jujur; adil; kepastian hukum; tertib penyelenggara Pemilu; kepentingan umum; keterbukaan; proporsionalitas; profesionalitas; akuntabilitas; efisiensi dan efektivitas.

Cara pemilihan calon anggota KPU-menurut Undang-Undang Nomor 22 Tahun 2007 Tentang Penyelenggara Pemilu-adalah Presiden membentuk Panitia Tim Seleksi calon anggota KPU tanggal 25 Mei 2007 yang terdiri dari lima orang yang membantu Presiden menetapkan calon anggota KPU yang kemudian diajukan kepada Dewan Perwakilan Rakyat untuk mengikuti fit and proper test. Sesuai dengan bunyi Pasal 13 ayat (3) Undang-undang N0 22 Tahun 2007 Tentang Penyelenggara Pemilu, Tim Seleksi Calon Anggota KPU pada tanggal 9 Juli 2007 telah menerima 545 orang pendaftar yang berminat menjadi calon anggota KPU. Dari 545 orang pendaftar, 270 orang lolos seleksi administratif untuk mengikuti tes tertulis. Dari 270 orang calon yang lolos tes administratif, 45 orang bakal calon anggota KPU lolos tes tertulis dan rekam jejak yang diumumkan tanggal 31 Juli 2007.

Dengan berlakunya Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum, maka seleksi calon anggota KPU Provinsi dan KPU Kabupaten/Kota menjadi kewenangan KPU. Sedangkan untuk seleksi calon anggota KPU panitia seleksi dibentuk oleh Presiden, kemudian panitia seleksi setelah melalui proses seleksi mengusulkan 14 nama calon anggota KPU kepada Presiden untuk dilakukan uji kepatutan dan kelayakan (fit and proper test) kepada DPR. Kemudian DPR menentukan 7 Nama untuk ditetapkan sebagai calon anggota KPU dalam rapat paripurna DPR. Proses selanjutnya adalah Presiden menerbitkan Keppres tentang penetapan anggota KPU untuk kemudian dilantik oleh Presiden selama masa periode 5 tahun. Berdasarkan Undang-Undang Nomor 7 Tahun 2017 ini juga ditetapkan masa periodesasi untuk anggota KPU, KPU Provinsi dan KPU Kabupaten/Kota dibatasi hanya 2 periode saja. Hingga sekarang KPU telah mengawal pelaksanaan demokrasi di Indonesia selama kurun

waktu 1999-2019. Selama itu pula KPU terus bertekat untuk menjadi penyelenggara Pemilu yang independen dan nonpartisan.[16]

### 2.2.2 Visi dan Misi

Komisi Pemilihan Umum (KPU) Kota Bandung memiliki Visi dan Misi[17]. Visi Komisi Pemilihan Umum (KPU) Kota Bandung adalah Menjadi Penyelenggara Pemilihan Umum yang Mandiri, Professional, dan Berintegritas untuk Terwujudnya Pemilihan Umum dan Pemilihan Kepala Daerah yang LUBER (Langsung., Umum, Bebas, Rahasia) dan JURDIL (Jujur, Adil ).

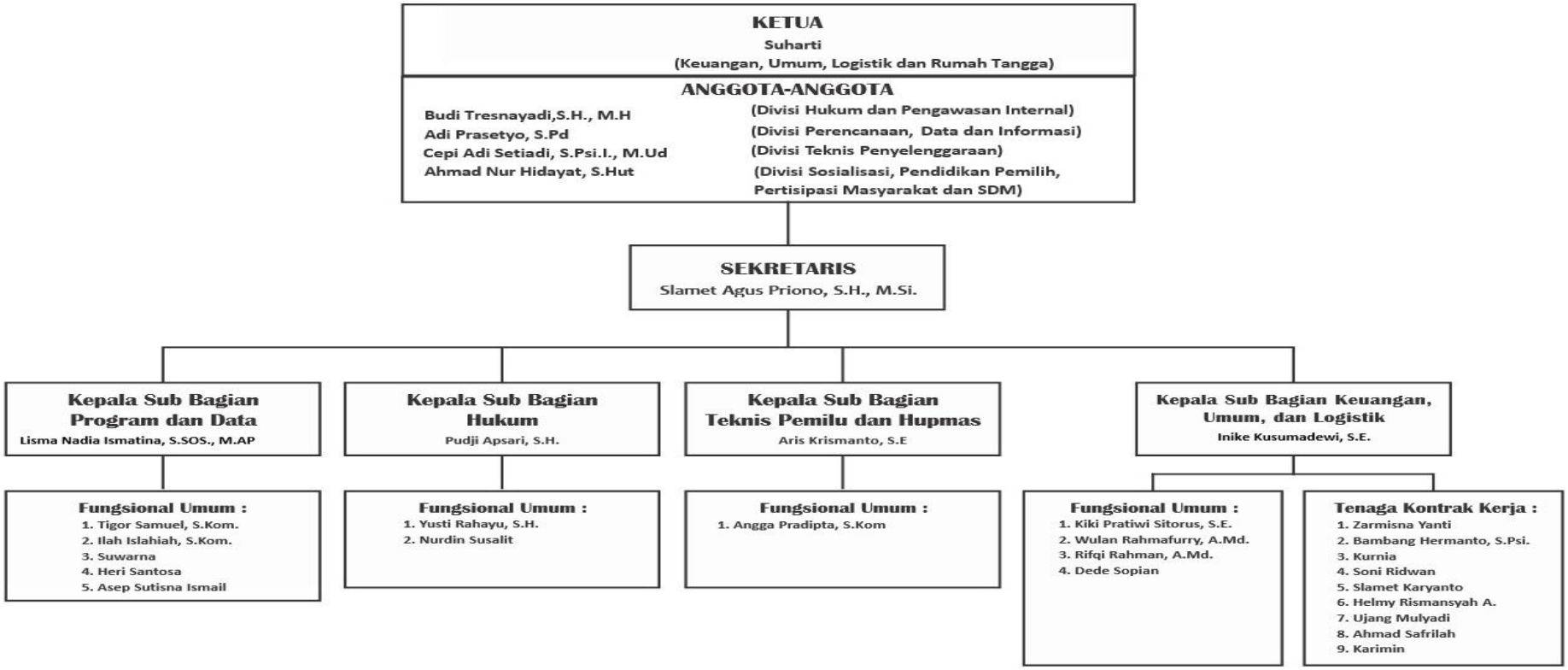
Berikut merupakan Misi Komisi Pemilihan Umum (KPU) Kota Bandung :

1. Membangun SDM yang memiliki kompetensi, kredibilitas, dan kapabilitas sebagai upaya menciptakan lembaga Penyelenggara Pemilu dan Pemilihan Kepala Daerah yang Profesional.
2. Meningkatkan kualitas pelayanan Pemilu, khususnya untuk para pemangku kepentingan dan umumnya untuk seluruh masyarakat.
3. Meningkatkan partisipasi dan kualitas pemilih melalui sosialisasi dan pendidikan pemilih yang berkelanjutan.
4. Memperkuat Kedudukan Organisasi dalam Ketatanegaraan.
5. Meningkatkan integritas penyelenggara Pemilu dengan memberikan pemahaman secara intensif dan komprehensif khususnya mengenai kode etik penyelenggara Pemilu.
6. Mewujudkan penyelenggara Pemilu yang efektif dan efisien, transparan, akuntabel, serta aksesable.
7. Mewujudkan KPU sebagai pusat informasi, edukasi dan dokumentasi Pemilu dan Demokrasi di Kota Bandung.

### 2.2.3 Struktur Organisasi

Struktur Organisasi Komisi Pemilihan Umum (KPU) Kota Bandung terbagi menjadi 2 yaitu struktur komisioner dan struktur sekretariat. Adapun struktur komisioner dapat dilihat pada gambar 2.1 sedangkan struktur sekretariat pada gambar 2.2.


**Gambar 2.1 Struktur Komisioner**




**Gambar 2.2 Struktur Sekretariat**

### 2.2.4 Logo dan Makna Logo


**Gambar 2.3 Logo Komisi Pemilihan Umum (KPU)**

Makna yang terkandung dalam logo Komisi Pemilihan Umum (KPU) yang ditunjukan di Gambar 2.3 adalah sebagai berikut[18] :

1. Bentuk segiempat lonjong menggambarkan bentuk perisai yang bermakna penjagaan diri.
2. Burung garuda dan lambang lima sila pancasila yang berada di tengah melambangkan dasar Negara Indonesia, yakni Pancasila.
3. Warna merah putih yang juga berada di tengah merupakan warna bendera resmi Indonesia.
4. Tulisan KOMISI PEMILIHAN UMUM menyatakan bahwa lambang ini dimiliki oleh KPU.
5. Warna hijau melambangkan kesuburan dan kemakmuran.
6. Warna kuning melambangkan keagungan, kemuliaan, dan kekayaan.
7. Warna hitam melambangkan keteguhan dan keabadian.
8. Warna merah melambangkan keberanian.
9. Warna putih melambangkan kemurnian, kesucian, dan kejujuran.

## 2.3 Landasan Teori

Landasan teori merupakan materi atau teori yang digunakan sebagai acuan dalam melakukan sebuah penelitian. Landasan teori yang akan diuraikan merupakan hasil dari literatur dan buku-buku.

### 2.3.1 Pengertian Purwarupa

Purwarupa dalam bahasa indonesia adalah bentuk awal atau standar ukuran dari sebuah model. Menurut kamus besar bahasa Indonesia pengertian purwarupa adalah rupa yang pertama atau rupa awal. Sehingga purwarupa dapat disebut sebagai rupa awal yang dibuat untuk mewakili skala sebenarnya sebelum dikembangkan atau justru dibuat khusus untuk pengembangan sebelum dibuat dalam skala sebenarnya[19].

### 2.3.2 Pengertian Sistem

Sistem merupakan kumpulan elemen yang saling berhubungan satu sama lain yang membentuk satu kesatuan dalam usaha mencapai suatu tujuan. Sebagai contoh dii dalam perusahaan, yang dimaksud elemen dari sistem adalah departemen-departemen internal, seperti persediaan barang mentah, produksi, persediaan barang jadi, promosi, penjualan, keuangan, personalia, serta pihak eksternal seperti supplier dan konsumen yang saling terkait satu sama lain dan membentuk satu kesatuan usaha[20].

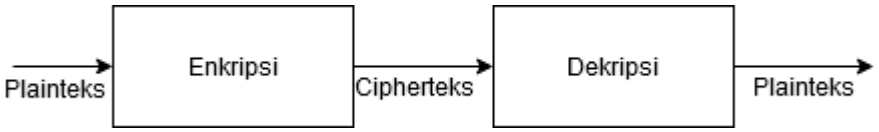
### 2.3.3 Pengertian Website

Website merupakan kumpulan dari halaman-halaman yang saling berhubungan dengan file-file lain yang saling berkaitan. Dalam sebuah website terdapat satu halaman yang dikenal dengan sebutan home-page. Homepage adalah sebuah halaman yang pertama kali dilihat ketika seseorang mengunjungi sebuah website[21].

### 2.3.4 Kriptografi

Kriptografi adalah ilmu yang berdasarkan pada teknik matematika yang erat kaitannya dengan keamanan informasi seperti kerahasian, keutuhan data dan

otentikasi entitas. Jadi pengertian kriptografi modern adalah bukan hanya pada penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi[22]. Proses penyandian suatu plainteks untuk menjadi cipherteks disebut enkripsi sedangkan proses mengembalikan cipherteks menjadi plainteks disebut dekripsi[23]. Alur sederhana dari proses enkripsi dan dekripsi diperlihatkan di gambar 2.4[24].




**Gambar 2.4 Alur sederhana enkripsi dan dekripsi**

### 2.3.4.1 Enkripsi Homomorphik

Enkripsi Homomorphik adalah enkripsi yang memungkinkan dilakukannya komputasi pada ciphertext tanpa harus mendekripsi terlebih dahulu ciphertext tersebut. Operasi matematika yang dapat dilakukan pada ciphertext yang menggunakan enkripsi homomorfik akan menghasilkan ciphertext yang jika didekripsi akan menghasilkan hasil yang sama dengan operasi serupa pada plaintext[8]. Secara matematis. Enkrpisi homomorfik adalah sebuah cryptosystem yang menggunakan fungsi enkripsi yang bersifat homomorfik dan memungkinkan dilakukannya operasi ciphertext. Ada dua jenis operasi pada enkripsi homomorfik yaitu penjumlahan dan pengurangan[25]. Suatu kriptosystem dikatakan memiliki sifat aditif jika dan hanya jika :

$$\exists \Delta : \varepsilon(\chi 1)\ \Delta\ \varepsilon(\chi 2) = \varepsilon(\chi 1 + \chi 2) \qquad \textbf{(1)}$$

Dengan x1 dan x2 adalah plaintext, $\varepsilon$ adalah fungsi enkripsi dan $\Delta$ adalah suatu operator yang bergantung pada sifat algoritma enkripsi yang digunakan. Kemudian suatu kriptosystem dikatakan multiplikatif jika dan hanya jika :

$$\exists \Delta : \varepsilon(\chi 1)\ \Delta\ \varepsilon(\chi 2) = \varepsilon(\chi 1.\ \chi 2) \qquad \textbf{(2)}$$

Terdapat dua jenis enkripsi homomorpik yaitu enkripsi homomorpik sebagian dan enkripsi homomorpic keseluruhan. Enkripsi homomorpik sebagian merupakan jenis enkripsi homomorfik yang memungkinkan dilakukannya satu jenis operasi tertentu pada ciphertext. Sedangkan enkripsi homomorfik keseluruhan merupakan jenis enkripsi homomorfik yang mampu untuk dua jenis operasi penjumlahan dan perkalian dilakukan pada ciphertext[25].

**2.3.4.1.1Paillier Cryptosystem**

Paillier cryptosystem adalah enkripsi yang memiliki sifat homomorfik aditif, ditemukan pada tahun 1999 oleh pascal paillier[26]. Paillier cryptosystem memiliki kunci publik n dan g, yang merupakan modulus RSI. Cryptosystem ini mengenkripsi pesan 'm' dengan $c = g^m r^n \bmod n^2$, di mana r adalah bilangan bulat acak. Untuk mendapatkan nilai n diperlukan bilangan prima p dan q. Bilangan prima harus berbeda satu sama lain. Selain ditentukan, hitung fungsi Carmichael dengan $\lambda = \mathrm{lcm}\,(p - 1),(q - 1)$.

Paillier cryposystem memiliki dua kunci. Kunci publik untuk proses enkripsi dan kunci pribadi untuk proses dekripsi. Langkah-langkah pembuatan kunci adalah sebagai berikut [27]:

1. Pilih 2 bilangan prima p dan q secara acak dan independen satu sama lain sehingga

$$\gcd\,(pq,(p - 1),(q - 1)) = 1 \qquad \textbf{(3)}$$

2. Hitung RSA modulus n = pq dan fungsi Carmichael $\lambda = \mathrm{lcm}\,(p - 1),(q - 1)$ juga bisa dihitung dengan cara lain seperti

$$\lambda = \frac{(p - 1)(q - 1)}{\gcd\,(p - 1),(q - 1)} \qquad \textbf{(4)}$$

3. Dapatkan nilai generator g dimana $g \in Z^*_{n^2}$ ada 2 cara untuk mendapatkan nilai g tersebut.

   **a.** Secara acak pilih nilai g dari set $Z^*_{n^2}$ dimana

$$\gcd\left(\frac{g^\lambda \bmod n^2 - 1}{n}\ ,\ n\right) = 1$$

**(5)**

Ada $\phi(n) * \phi(n)$ , nilai generator yang valid, oleh karena itu probabilitas untuk memilih mereka dari $n\phi(n)$ elemen $Z_{n^2}^*$ set relatif tinggi untuk n besar.

b. Pilih $\alpha$ dan $\beta$ secara acak dari set $Z_{n^2}^*$ lalu hitung

$$g = (an + 1)\beta^n \bmod n^2 \quad \textbf{(6)}$$

4. Hitung modular multiplicative inverse

$$\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n. \quad \textbf{(7)}$$

Dimana fungsi L didefinisikan dengan $L(u) = \frac{u - 1}{n}$ . multiplicative inverse hanya ada jika dan hanya jika nilai generator valid telah didapat dari tahap sebelumnya.

5. Maka dari itu didapatkan kunci publik dan privat. Publik(enkripsi) kunci (n, g) dan private(dekripsi) kunci($\lambda$, $\mu$).

Cari lainnya untuk mendapatkan kuncinya ialah

$$g = n + 1, \quad \lambda = \phi(n) \quad \textbf{(8)}$$

dan

$$\mu = \phi(n)^{-1} \bmod n, \text{ dimana } \phi(n) = (p - 1)(q - 1) \quad \textbf{(9)}$$

Untuk melakukan proses enkripsi maka dijelaskan sebagai berikut :

1. Jadikan m sebagai pesan yang akan di enkripsi, dimana $m \in Z_n$
2. Pilih nilai acak r, dimana $r \in Z_n^*$
3. Hitung ciphertext dengan

$$c = g^m \cdot r^n \bmod n^2 \quad \textbf{(10)}$$

Untuk melakukan proses dekripsi maka dijelaskan sebagai berikut :

1. Ciphertext $c \in Z_{n^2}^*$
2. Hitung pesan dengan

$$m = L(c^\lambda \bmod n^2) \cdot \mu \bmod n \quad \textbf{(11)}$$

Fitur utama dari paillier cryptosystem adalah sifat sifat homomorfiknya. Karena fungsi enkripsi adalah homomorfik aditif maka akan dijelaskan sebagai berikut :

1. Penambahan plaintext homomorphic

Dua buah ciphertext akan didekripsi untunk menghitung hasil penjumlahan plaintext yang sesuai.

$$D(E(m_1,r_1) * E(m_2,r_2) \bmod n^2) = m_1 + m_2 \bmod n \quad \textbf{(12)}$$

Satu buah ciphertext dengan plaintext dengan penggunaan g akan didekripsi untuk menghitung hasil penjumlahan plaintext yang sesuai.

$$D(E(m_1,r_1) * g^{m_2} \bmod n^2) = m_1 + m_2 \bmod n \quad \textbf{(13)}$$

### 2.3.5 E-voting

Electronic voting atau e-voting adalah penggunaan komputer atau komputerisasi pada proses pemungutan suara pemilihan[28]. Council of Europe (CoE) mendefinisikan e-voting memiliki kemampuan untuk mempercepat tabulasi data, mengurangi biata pemilihan dan berkontribusi untuk mencegah pemilih yang tidak sah[29].

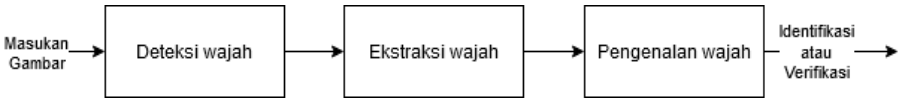
E-voting juga merupakan subjek multidisiplin ilmu yang dipelajari pada ahli dari berbagai bidang seperti sofeware engineering, cryptography, politik, hukung, ekonomi, dan ilmu sosial. E-voting adalah topik yang menantang bagi dunia kriptografi, tantanganya disini adalah perlunya mencapai anonimitas pemilih, dengan kata lain menghapus identitas pemilih dari suara-suara yang telah dipilih untuk menjaga privasi pemilih dan juga untuk memastikan bahwa proses e-voting telah terjalan dengan benar tanpa pelanggaran dan memastikan bahwa hanya pemilih sah yang dihitung[30].

Menurut Schneier ada tujuh aspek dasar yang harus dipenuhi dalam e-voting , yaitu [31]:

1) Hanya orang yang terdaftar yang bisa memilih
2) Tidak ada yang bisa memilih lebih dari satu kali
3) Tudak ada yang dapat tahu pilihan orang lain
4) Tidak ada yang bisa menduplikasi hasil pemilihan orang
5) Tidak ada yang bisa mengubah pilihan orang lain tanpa diketahui
6) Setiap pemilih harus yakin kalau pilihanya masuk dalam hitungan
7) Setiap orang bisa mengetahui hasil pemilihan

### 2.3.6 Face recognition

Face recognition adalah teknik citra yang dipakai di berbagai aplikasi untuk tujuan keamanan sistem selain pengenalan sidik jari ataupun retina mata. Dalam implementasinya pengenalan wajah menggunakan kamera untuk menangkap citra wajah seseorang kemudia dibandingkan dengan wajah yang sebelumnya telah dimiliki dan disimpan di dalam database[32]. Di penelitian Jigar dkk, Teknik pengenalan wajah secara sederhana digambarkan dalam diagram alir yang digambarkan oleh gambar 2.5 sebagai berikut[33].




**Gambar 2.5 diagram alir tahapan pengenalan wajah**

Face detection merupakan bagian yang mendeteksi keberadaan wajah pada citra atau gambar dengan berbagai variasi pose, pencahayaan, ekspresi wajah, penghalang(kaca mata, kumis, dan jenggot) serta ukuran.

Dalam face extraction ada dua cara yang digunakan yaitu feature selection dan feature extraction. Pemilihan fitur bertujuan untuk memilih sejumlah fitur yang banyak berpengaruh dari n fitur yang ada. Ekstraksi fitur memproyeksikan fitur kedalam dimensi yang lebih rendah. Fitur sendiri ialah semua jenis aspek pembeda, kualitas atau karakteristik. Bisa berupa simbolik(warna) atau numerik(intensitas). Fitur fitur itulah yang akan mencerminkan karakteristik tertentu dari suatu wajah.

Setelah melalui tahap face extraction maka wajah akan yang akan dibandingkan disandingkan dan dianalisis berdasarkan fitur yang dimiliki wajah, apakah sesuai atau tidak. Dari penyandingan tersebut didapatkanlah suatu hasil siapa pemilik wajah tersebut.

### 2.3.7 Object Oriented Programming

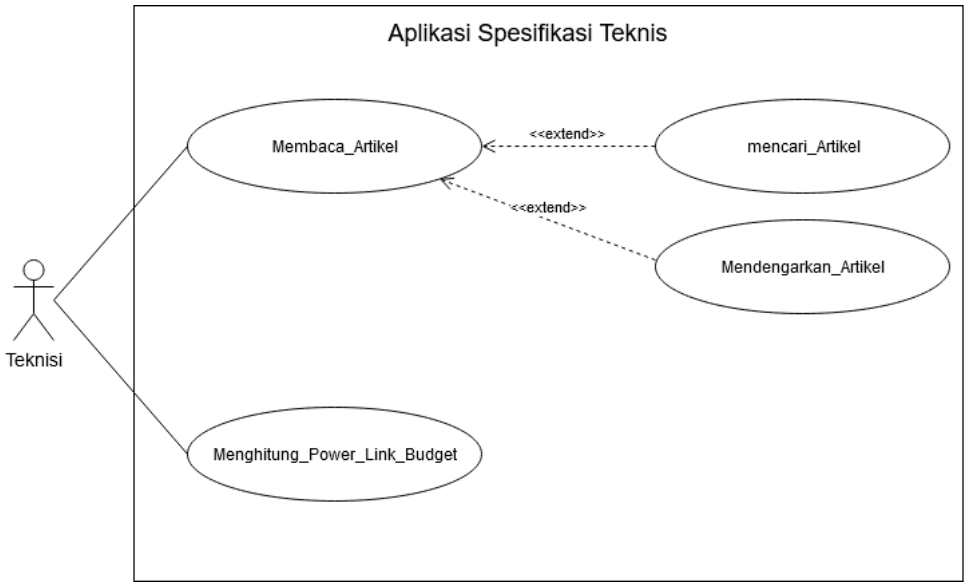
OOP (Object Oriented Programming) adalah sebuah istilah yang diberikan kepada bahasa pemprograman yang menggunakan teknik berorientasi atau berbasis pada sebuah objek dalam pembangunan program aplikasi, maksudnya bahwa orientasi pembuatan program tidak lagi menggunakan orientasi linear melainkan berorientasi pada objek-objek yang terpisah-pisah[34].

### 2.3.8 Unified Modeling Language

Unified modeling language adalah notafi grafik untuk menggambarkan diagram konsep suatu perangkat lunak. Unified modeling language dapat digunakan untuk menggambar diagram dari suatu domain masalah, desain perangkat lunak, atau suatu implementasi perangkat lunak yang sudah rampung[35].

#### 2.3.8.1 Use Case Diagram

Use case diagram adalah deskripsi perilaku sistem yang digambarkan. Use case diagram ditulis dari sudut pandang pengguna yang memberi tahu apa yang harus dilakukan leh sistem. Use case diagram menangkap urutan peristiwa yang terlihat oleh sistem dan dilalui oleh sistem sebagai respon terrhadap stimulus pengguna. Peristiwa yang terlihat maksudnya adalah setiap peristiwa yang dilihat pengguna. Use case tidak menggambarkan suatu aksi yang tidak terlihat[35]. Contoh Use Case Diagram dapat dilihat pada gambar 2.6 Contoh Use Case Diagram.




**Gambar 2.6 Contoh Use Case Diagram**

Ada beberapa komponen inti dari sebuah use case diagram yaitu:

1) Aktor

Menspesifikasikan himpunan peran yang pengguna mainkan, digambarkan dengan gambar sisbol manusia.

2) Association

Menggambarkan hubungan antara objek satu dengan objek lainnya, digambarkan dengan suatu garis.

3) Use Case

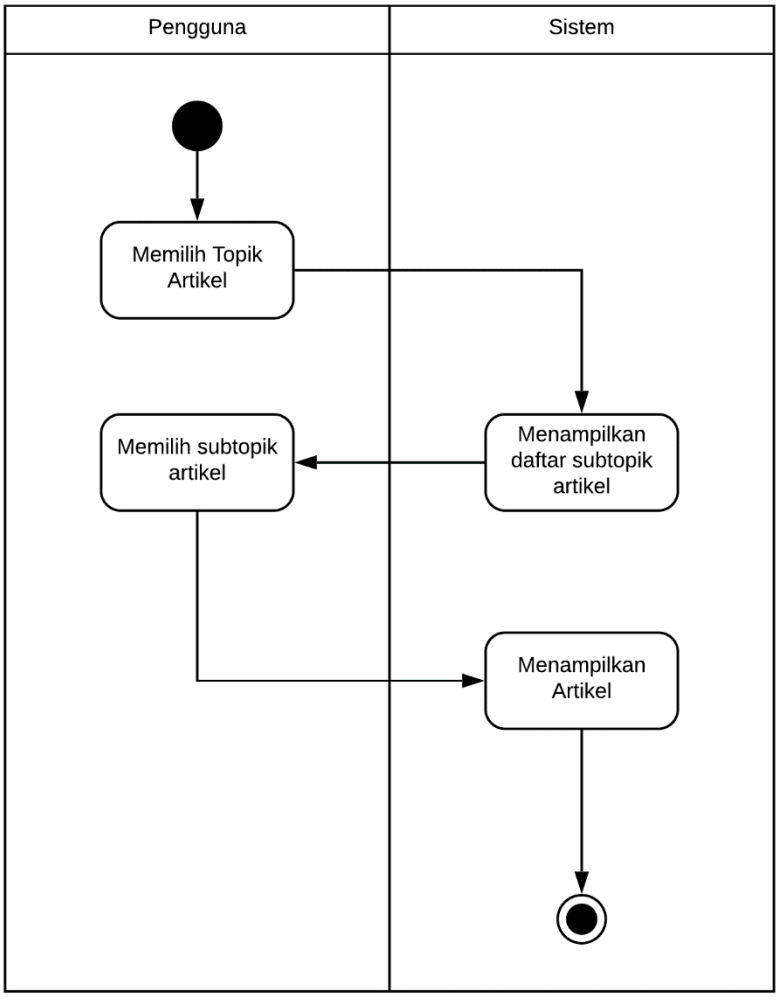
Deskripsi dari urutan aksi-aksi yang ditampilkan sistem, digambarkan dengan bentuk oval/ bulat.

4) System

Menspesifikasikan paket yang menampilkan sistem secara terbatas, digambarkan dengan bentuk persegi.

#### 2.3.8.2 Activity Diagram

Activity Diagram menggambarkan alur kerja atau aktivitas dari sebuah sistem atau proses bisnis atau menu yang ada pada perangkat lunak. Diagram ini memperlihatkan aliran dari suatu aktivitas lainnya dalam suatu sistem[36]. Contoh Activity Diagram dapat dilihat pada gambar 2.7 Contoh Activity Diagram.




**Gambar 2.7 Contoh Activity Diagram**

Ada beberapa komponen inti dari sebuah Activity Diagram yaitu:

1) Action

Kondisi dari sistem yang mencerminkan eksekusi dari suatu aksi yang dilakukan, digambarkan dengan bentuk persegi.

1) Trancition

Menggambarkan alur antar aksi-aksi yang ada disuatu sistem, digambarkan dengan arah panah.

2) Initial Node

Awal suatu objek, digambarkan dengan lingkaran hitam.

3) Final Node

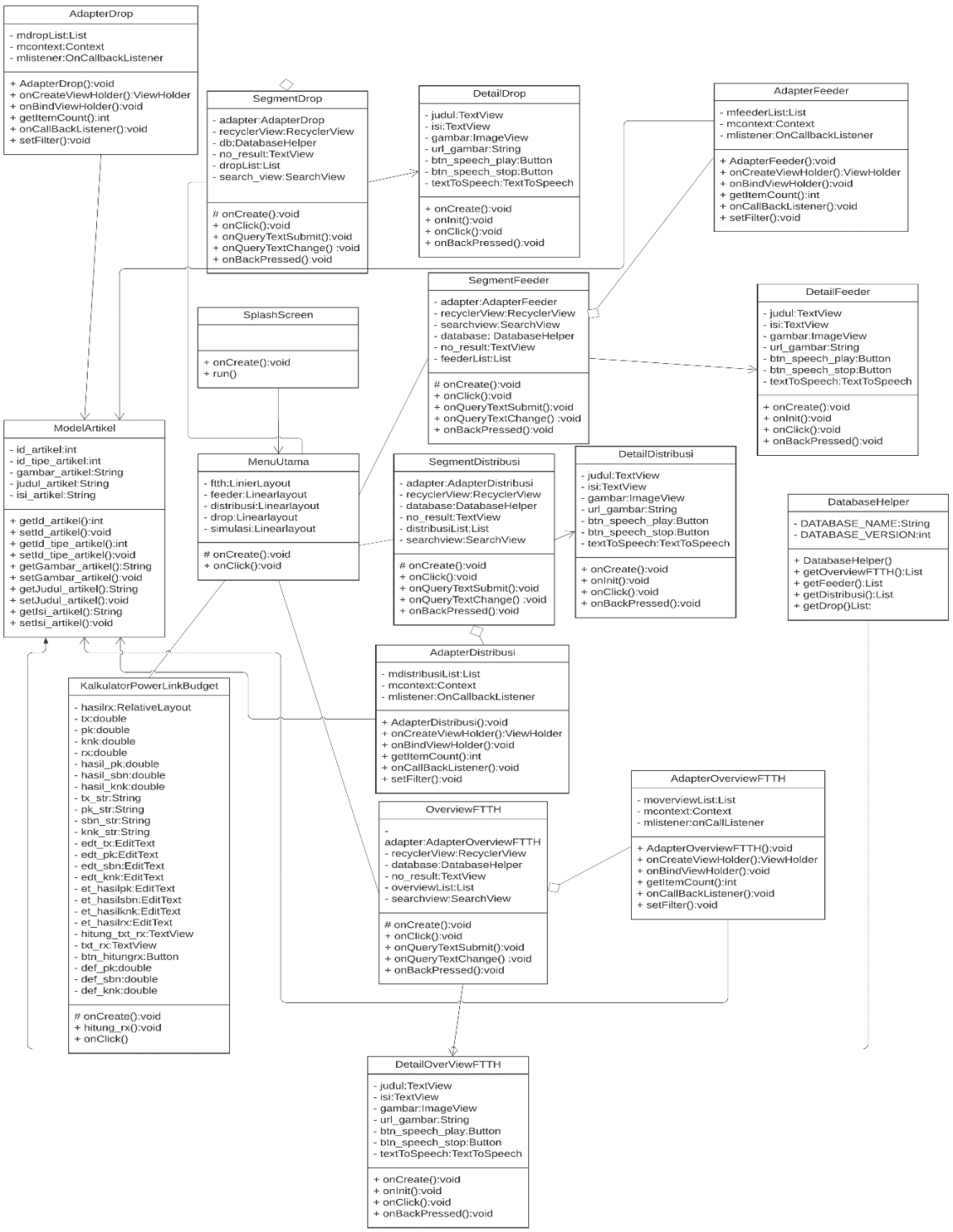
Akhir suatu objek, digambarkan dengan lingkaran hitam dengan lingkaran putih diluarkanya.

4) Decision

Percabangan dimana pilihan atau kondisi dilakukan, digambarkan dengan bentuk berlian.

#### 2.3.8.3 Class Diagram

Class diagram atau kelas diagram memungkinkan untuk menunjukan konten statis, dan hubungan antara kelas. Kelas diagram dapat menunjukan variabel anggota dan fungsi anggota suatu kelas. Kelas diagram juga dapat menunjukan apakah suatu kelas mewarisi dari lain, atau apakah ia memiliki referensi ke yang lainnya. Singkatnya kelas diagram dapat menggambarkan semua dependensi dari kode sumber diantara kelas[35]. Contoh Class Diagram dapat dilihat pada Gambar 2.8 Contoh Class Diagram.




**Gambar 2.8 Contoh Class Diagram**

Ada beberapa kommponen inti dari sebuah class diagram diagram yaitu:

1) Generalization

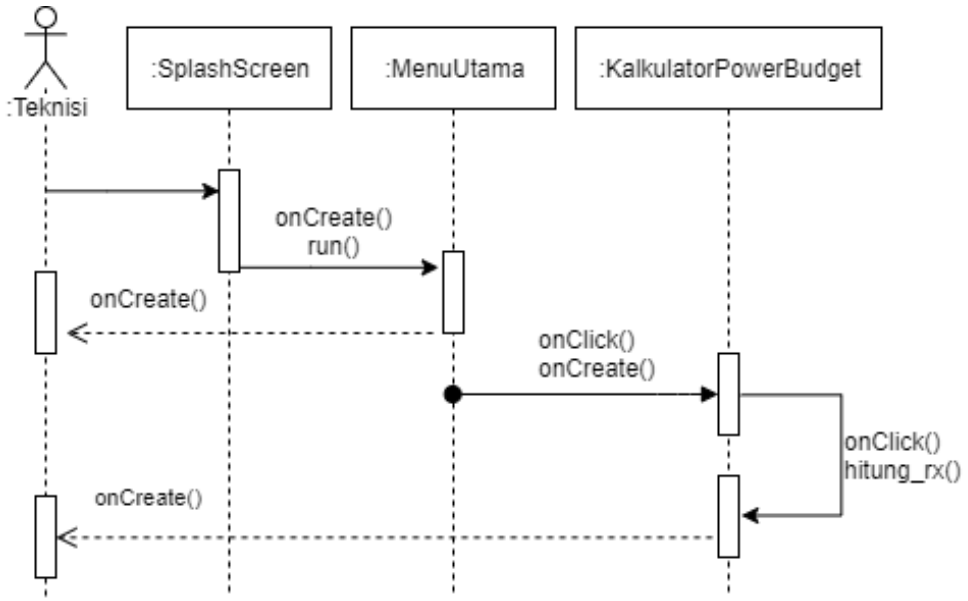
Hubungan dimana objek anak berbagi dengan dengan objek diatasnya, digambarkan dengan sebuah garis.

5) Class

Himpunan dari objek-objek yang berbagi atribut serta operasi yang sama, digambarkan dengan persegi.

**2.3.8.4 Sequence Diagram**

Sequence diagram adalah tool yang sangat populer dalam pengembangan sistem informasi secara object-oriented untuk menampilkan interaksi antar objek[37]. Ada dua hal yang dapat dilakukan dengan sequence diagram, pertama untuk menguraikan sebuah proses bisnis menjadi aktivitas-aktivitas yang lebih kecil untuk mengidentifikasi kebutuhan interaksi pemakai pada masing-masing aktivitas tersebut[38]. Penggunaan kedua, sequence diagram digunakan pada setiap interaksi untuk menganalisa perilaku sistem informasi dalam rangka untuk merancang tampilan pada interaksi tersebut[37]. Contoh Sequence Diagram dapat dilihat pada Gambar 2.9 Contoh Sequence Diagram.




**Gambar 2.9 Contoh Sequence Diagram**

Ada beberapa komponen inti dari sebuah sequence diagram yaitu:

6) Object

Representasi objek atau kelas, digambarkan dengan kotak.

7) Activition boxes

Representasi waktu yangdibutuhkan objek untuk mealksanakan suatu tugas, digambarkan dengan persegi panjang.

8) Actors

Komponen yang mewakili pengguna sistem.

9) Lifeline

Komponen garis putus-putus yang menghubungkan objek.

### 2.3.9 Business Process Model and Notation

Business Process Model and Notation (BPMN) merupakan representasi visual proses bisnis yang bertujuan untuk meningkatkan proses bisnis operasional. Misalnya, dengan memodelkan proses bisnis dan menganalisanya mengunakan simulasi, pihak manajemen dapat mendapatkan ide bagaimana cara mengurangi biaya sembari meningkatkan pelayanan yang diberikan. Selain itu BPMN sering dikaitkan dengan perangkat lunak untuk mengelola, mengendalikan, dan mendukung proses operasional[39].

### 2.3.10 Pengujian

Pengujian suatu sofeware atau perangkat lunak diperlukan untuk memastikan apakah sofeware yang dibuat atau dibangun dapat berjalan sesuai dengan tujuan atau fungsionalitas yang diharapkan. Penguji sofeware harus menyiapkan sesi khusus untuk menguji sofeware yang sudah dibuat agar kesalahan ataupun kekurangan daapt diketahui sejak dini dan diperbaiki secepat mungkin. Pengujian atau testing sendiri merupakan tahapan yang sangat krusial dan penting untuk menjamin kualitas sofeware dan merupakan bagian dari siklus pengembangan sofeware[40].

#### 2.3.10.1 Pengujian Black Box

Penelitian M. sidi mustaqbal dkk[41] menjelaskan bahwasanya black box berfokus pada spesifikasi fungsional dari perangkat lunak. Penguji dapat mendefinisikan kumpulan kondisi input dan melakukan pengujian pada spesifikasi fungsionalitas ssofeware. Pengujian black box cenderung untuk menemukan hal-hal berikut :

1. Fungsi yang tidak benar atau tidak ada.
2. Kesalahan antarmuka.
3. Kesalahan pada struktur data dan akses basis data.
4. Kesalahan performasi.

5. Kesalahan inisialisasi dan terminasi.

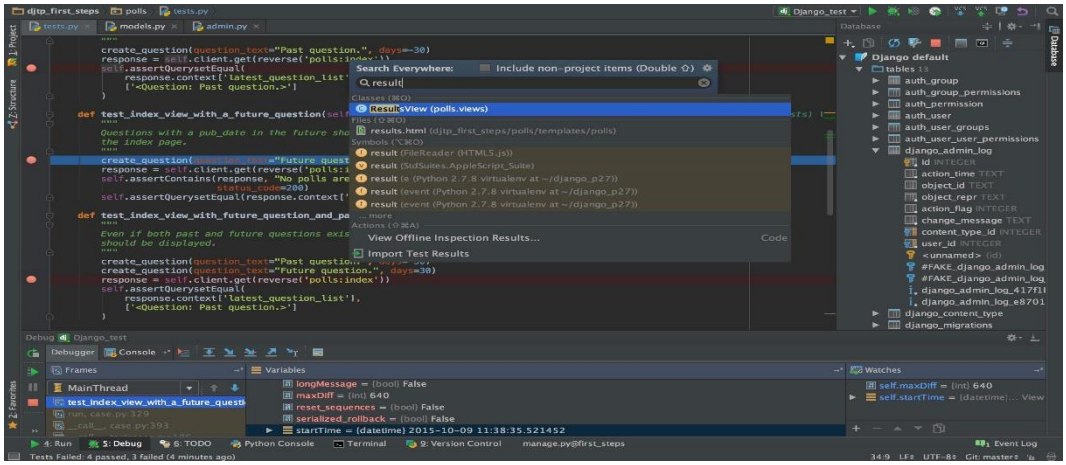
Pengujian Black Box juga diberikan kriteria uji tambahan yang berasal dari 7 aspek yang harus ada dalam e-voting dari Schneier[31].

### 2.3.11 Sofeware

Sofeware atau perangkat lunak adalah suatu alat yang dibangun sebagai jembatan penghubung antara pengguna dengan komputer selain itu juga untuk menyelesaikan tugas-tugas spesifik dalam kehidupan manusia.

#### 2.3.11.1 Pycharm

Pycharm merupakan editor kode yang berjalan di desktop dan tersedia untuk windows, mac, dan linux. Pycharm memberikan dukungan khusus untuk bahasa pemprograman python.



**Gambar 2.10 Pycharm User Interface**

#### 2.3.11.2 Python

Python adalah bahasa pemprograman tingkat tinggi yang berorientasi objek. Dibangun dengan tingkat tinggi dalam struktur data, dikombinasikan dengan dynamic typing dan dynamic binding, memuat python menarik dan cepat dalam penggunaanya. Python mendukung modul dan paket yang lengkap yang tersebar hampir di berbagai majam platform besan dan didistribukan secara gratis[42].

**2.3.11.2.1Django**

Django adalah framework yang menggunakan bahasa pemprograman python. Django memungkinkan pengembangan yang cepat dalam pembangunan situs web yang aman dan dikelola dengan bahasa pemprograman python. Django bersifat gratis dan open source juga memiliki komunitas dan dokumentasi yang aktif dan besar[43].

**2.3.11.3 Library Face recognition**

Library Face Recornition atau Face_Recognition merupakan API yang tersedia di github secara open source dan gratis. Library ini berfokus pada pendeteksian dan manipulasi wajah dalam bahasa pemprograman Python. Dibangun menggunakan library dlib dan deep learning. Memiliki keakurasian model 99.38% di benchmark yang diberikan oleh university of massachusetts dengan kategori labeled faces in the wild home[44].

**2.3.11.4 Python-paillier**

Python-paillier library adalah library yang dibangun untuk pelakukan pengimplementasian paillier enkripsi homomorfik sebagian. Library ini berdasarkan dari paillier cryptosystem dan dapat melakukan 3 hal yaitu, mengenkripsi angka dan melakukan perkalian didalamnya, mengenkripsi angka dan melakukan penambahan didalamnya, ddan mengenkripsi angka dan nemabahkan angka diluar angka yang dienkripsi.

**2.3.11.5 Telerik Fiddler**

Telerik Fiddler (atau Fiddler) adalah server proxy tujuan khusus untuk men-debug lalu lintas web dari aplikasi seperti browser. Ini digunakan untuk menangkap dan mencatat lalu lintas web dan kemudian meneruskannya ke server web. Respons server kemudian dikembalikan ke Fiddler dan kemudian dikembalikan ke klien. Fiddler dapat mendekripsi lalu lintas HTTPS dan menampilkan serta mengubah permintaan yang tidak dapat dipahami oleh pengamat di jaringan menggunakan teknik dekripsi man-in-the-middle. Untuk mengizinkan proses debug yang lancar tanpa peringatan keamanan, sertifikat akar

Fiddler dapat dipasang di penyimpanan Sertifikat Tepercaya dari sistem atau browser web[45].

**2.3.11.6 Zed Attack Proxy (ZAP)**

Zed Attack Proxy (ZAP) adalah alat pengujian penetrasi open-source gratis yang dikelola di bawah payung Proyek Keamanan Aplikasi Web Terbuka (OWASP). ZAP dirancang khusus untuk menguji aplikasi web. Pada intinya, ZAP dikenal sebagai "proxy man-in-the-middle." Ini berdiri di antara browser penguji dan aplikasi web sehingga dapat mencegat dan memeriksa pesan yang dikirim antara browser dan aplikasi web, memodifikasi konten jika diperlukan, dan kemudian meneruskan paket tersebut ke tujuan. Ini dapat digunakan sebagai aplikasi yang berdiri sendiri[46].

**2.3.11.7 Nikto**

Nikto adalah pemindai server web Open Source (GPL) yang melakukan tes komprehensif terhadap server web untuk beberapa item, termasuk lebih dari 6700 file / program yang berpotensi berbahaya, memeriksa versi suatu item lebih dari 1250 server. Ini juga memeriksa item konfigurasi server seperti keberadaan beberapa file indeks, opsi server HTTP, dan akan mencoba mengidentifikasi server web dan perangkat lunak yang diinstal[47].

**2.3.11.8 MySQL**

MySQL dikembangkan oleh sebuah perusahaan bernama MySQL AB yang pada saat itu bernama TcX DataKonsult AB tahun 1994-1995. MySQL adalah salah satu jenis database server yang sangat terkenal dan banyak digunakan untuk membangun aplikasi web yang databse sebagai sumber dan pengelolaan datanya. Kepopuleran MySQL antara lain karena MySQL menggunakan SQL sebagai bahasa dasar untuk mengakses databse-nya sehingga mudah untuk digunakan. MySQL juga bersifat open source dan free di berbagai platform[48].