JUPITER : Jurnal Penelitian Mahasiswa Teknik Dan Ilmu Komputer
Volume 1 - Nomor 1, Mei 2021

ISSN: (print)
ISSN: (online)

PURWARUPA SISTEM E-VOTING MENGGUNAKAN ENKRIPSI HOMOMORPHIC DI KOMISI PEMILIHAN UMUM KOTA BANDUNG

Aditya Maulana Rajak [1*], Richi Dwi Agustia [2]

[1,2)]Program Studi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Komputer Indonesia
Jl. Dipati Ukur No. 112 – 116, Bandung, Indonesia 40132

email: aditya.maulana.rojak@gmail.com[1], richi@email.unikom.ac.id[2]

(Naskah masuk: *03/05/2021*; diterima untuk diterbitkan: *31/05/2021*)

ABSTRAK *– Komisi Pemilihan Umum (KPU) Kota Bandung ingin meningkatkan waktu kecepatan proses pemungutan suara dan rekapitulasi suara dengan memanfaatkan perkembangan teknologi E-voting. Selain permasalahan waktu Komisi Pemilihan Umum Kota Bandung juga ingin mengurangi tingkat pelanggarana terkait validasi hak pemilih seperti yang terdata dalam laporan Evaluasi pelaksanaan pemilihan 2018. serta pelanggaran terkait manipulasi suara yang masuk dalam kategori pelanggaran kode etik penyelenggara pemilu berjumlah 25 orang yang muncul pada Pemilihan Kepala daerah (pilkada) serentak 2018 berdasarkan Laporan Kinerja 2018 Dewan Kehormatan Penyelenggara pemilu. dengan teknologi e-voting yan dikombinasikan dengan face recognition dan enkripsi homomorfik diharapkan permasalahan yang ada dapat terselesaikan. Dari hasil penelitian didapatkan hasil bahwasanya dengan penggunaan e-voting waktu pemugnutan dan rekapitulasi suara menjadi lebih cepat, dengan face recognition permasalhan validasi pemilih dapat dikurangi dan dengan enkripsi homomorfik keamanan terkait data suara dapat ditingkatkan.*

Kata Kunci *– Komisi Pemilihan Umum (KPU) Kota Bandung, Aplikasi website, E-voting, face recognition, enkripsi homomorfik.*

PROTOTYPES E-VOTING SYSTEM USING HOMOMORPHIC ENCRYPTION IN THE GENERAL ELECTION COMMISSION BANDUNG

ABSTRACT *– The General Election Commission (KPU) of Bandung City wants to increase the speed of the voting process and vote recapitulation by utilizing the development of E-voting technology. In addition to the problem of timing, the General Election Commission of the City of Bandung also wants to reduce the level of violations related to the validation of voter rights as recorded in the 2018 election evaluation report. As well as violations related to voting manipulation that fall into the category of violations of the election management code of ethics totaling 25 people who appeared in the 2018 simultaneous regional head elections (pilkada) based on the Performance Report 2018 Honorary Council of Election Administrators. With e-voting technology combined with face recognition and homomorphic encryption, it is hoped that existing problems can be resolved. From the research results, it was found that by using e-voting, the voting time and recapitulation of votes became faster, with face recognition the problems of voter validation could be reduced, and with homomorphic encryption the security related to voice data could be improved.*

Keywords *– General Election Commission (KPU) of Bandung City, website application, E-voting,Face recognition, homomorphic encryption.*

1. PENDAHULUAN

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. Dalam penyelenggaraan pemilihan kepada daerah (pilkada) serentak 2018 terutama pemilihan umum wali kota Bandung 2018 oleh Komisi Pemilihan Umum (KPU) Kota Bandung proses pemungutan suara dilaksanakan secara konvensional dimana pemilih memilih

dan hasil suara direkapitulasi di Tempat Pemungutan Suara (TPS). Hasil rekapitulasi dari tiap Tempat Pemungutan Suara (TPS) dikumpulkan secara bertahap dari mulai tingkat Kelurahan menuju ke Kecamatan dan berakhir di tingkat Kota. Hasil rekapitulasi suara tersebut akan selesai dihitung setelah 2 minggu hari terhitung setelah berakhirnya proses pemungutan suara hingga pemunguman pemenang pasangan calon, waktu 2 minggu tersebut oleh Komisi Pemilihan Umum (KPU) Kota Bandung dirasa terlalu lama.

Komisi Pemilihan Umum (KPU) Kota Bandung ingin meningkatkan waktu kecepatan proses pemungutan suara dan rekapitulasi suara dengan memanfaatkan perkembangan teknologi informasi, salah satu teknologi informasi yang dapat dimanfaatkan dan digunakan ialah pemungutan suara elektronik atau yang biasa disebut E-voting. Selain permasalahan waktu Komisi Pemilihan Umum Kota Bandung juga ingin mengurangi tingkat pelanggarana terkait validasi hak pemilih dimana terkadang pemilih diluar Daftar Pemilih Tetap (DPT) suatu Tempat Pemungutan Suara (TPS) dapat memilih di TPS tersebut, ataupun seperti pemilih dapat memilih lebih dari satu kali seperti yang terdata dalam laporan Evaluasi pelaksanaan pemilihan 2018[2], serta pelanggaran terkait manipulasi suara yang masuk dalam kategori pelanggaran kode etik penyelenggara pemilu berjumlah 25 orang yang muncul pada Pemilihan Kepala daerah (pilkada) serentak 2018 berdasarkan Laporan Kinerja 2018 Dewan Kehormatan Penyelenggara pemilu[3].

Pemungutan suara elektronik atau yang biasa disebut e-voting sendiri adalah metode pemungutan suara dengan menggunakan media elektronik atau perangkat elektronik[4]. Pada penelitian ashtarout Nu'man tahun 2012 menyebutkan bahwa e-voting memiliki tujuan untuk meningkatkan tingkat partisipasi masyarakat, meningkatkan kecepatan pemungutan suara juga meningkatkan kenyamanan masyarakat[5]. E-voting pun dapat menghilangkan malpraktik pemilihan umum yang terkait dengan sistem pemilihan konvensional atau manual, mengurangi durasi pemilihan yang secara langsung akan mengarah pada pengurangan biaya keseluruhan[6].

Sebuah penelitian dilakukan oleh Cut fachrul dkk mengenai e-voting di tahun 2020[7], pada penelitian tersebut dilakukan penelitian terkait e-voting dengan mengimplementasikannya kepada kecamatan kluet utara, e-voting yang dibangun diberi mekanisme keamanan pada bagian bagaimana pengguna masuk ke dalam sistem voting untuk menjaga hanya orang terpilih saja atau yang berhak yang dapat melakukan voting, dari penelitian itu didapatkan beberapa kesimpulan salah satunya ialah dengan e-voting maka mempermudah pengguna dalam memberikan voting dan mendapatkan hasil voting. Penelitian yang dilakukan Muhtar hartopo di 2017[8], pada penelitian ini lebih berfokus kepada pemanfaatan enkripsi homomorfik dalam menjaga keamanan dan kerahasian data suara dalam e-voting, dipenelitian ini didapatkan kesimpulan bahwa enkripsi homomorfic itu sangatlah cocok digunakan untuk perhitungan suara e-voting karena memiliki kemampuan melakukan operasi penjumlahan pada data suara tanpa dekripsi data terlebuh dahulu selain itu e-voting yang dibangun telah memenuhi asas-asas pemilihan akan tetapi memiliki kekurangan karena belum menyediakan fitur reliability data. Enkripsi Homomorfic adalah enkripsi yang memungkinkan data yang terenkripsi olehnya dapat dilakukan perhitungan matematis tanpa perlu di dekripsi terlebih dahulu[9] sehingga cocok digunakan untuk menjaga kerahasian perhitungan suara.

Penelitian lainnya terkait enkripsi homomorfik dan e-voting dilakukan oleh shifa dkk di tahun 2016[10], pada penelitian ini juga berfokus pada penggunaan enkripsi homomorfic dalam meningkatkan keamanan e-voting, dalam penelitian ini didapatkan kesimpulan bahwa dengan memanfaatkan enkripsi homomorfic dengan benar akan menjamin terjaganya kerahasian data juga perhitungan yang dilakukan untuk pengolahan suara memiliki kemungkinan sukses 100%. Pada penelitian dari Konstantun G dkk mereka membahas pemanfaatan Enkripsi homomorfik dalam pengamanan suatu data dimana disimpulakn bahwasanya dengan enkripsi tersebut keamanan menyimpan data meningkat tetapi menyebabkan beban terhadap sistem penyimpanan data meningkat sehingga waktu yang dibutuhkan dalam menyimpan data bertambah[11]. Sebuah penelitian yang dilakukan Gaby dkk menghasilkan sebuah sistem E-voting yang disebut BrocoVote dengan memanfaatkan Enkripsi hoomomorfik dengan Blockchain sebagai media penyimpanan datanya, dan dengan memanfaatkan enkripsi tersebut meningkatkan tingkat keamanan sistem tersebut[12].

Dari keenam penelitian terdahulu tersebut didapatkan kesimpulan bahwasanya enkripsi homomorfik sangatlah bermanfaat dalam menjaga kerahasian suara dan dapat membantu mengurangi kemungkinan terjadinya percobaan manipulasi suara terutama dalam e-voting, jika melihat penelitian yang dilakukan di kecamatan kluet utama pengamanan suaranya tidak dilakukkan sehingga data suara rentan terhadap manipulasi karena tidak adanya mekanisme pengamanan suara tetapi hal itu bisa saja diatasi dengan pemanfaatan enkrpisi homomorfik. Selain enkrisi homomorfik potensi keamanan e-voting masih dapat ditingkatkan lagi. salah satu cara meningkatkan tingkat keamanan yang belum dilakukan dipenelitian sebelumnya ialah mengkombinasikannya dengan teknologi lain dalam penerapan e-voting, seperti face recognition yang dapat meningkatkan tingkat keamanan validasi pengguna yang melakukan voting dalam proses pemungutan suara.

2. LANDASAN TEORI

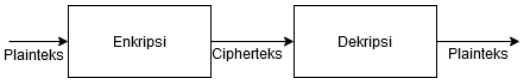
2.1. Pengertian *E-Voting*

E-voting atau electronic voting adalah pemanfaatan media komputer atau dapat disebut teknologi informasi sebagai media, alat, atau perantara proses pemungutan suara[14].

2.2. Kriptografi

Kriptografi modern merupakan sekumpulan metode atau teknik yang menyediakan keamanan informasi[15]. Dalam kriptografi proses penyandian suatu plainteks untuk menjadi cipherteks disebut enkripsi sedangkan proses pengembalian kebentuk semula disebut dekripsi[16].

Secara sederhana proses enkripsi dan dekripsi dapat dilihat pada gambar 1[17]:



Gambar 1 Alur Sederhana Proses Enkripsi dan Dekripsi

2.3. Enkripsi Homomorphic

Enkripsi Homomorphic adalah enkripsi yang memungkinkan dilakukannya proses komputasi matematika pada ciphertext tanpa harus melakukan dekripsi terhadap ciphertext itu sendiri[8]. Secara matematika Enkripsi ini adalah sebuah cryptosystem yang menggunakan fungsi enkripsi yang bersifat homomorphic dan memungkinkan dilakukannya operasi matematika ciphertext[18].

2.4. Paillier Cryptosystem

GPS Paillier cryptosystem adalah enkripsi yang memiliki sifat homomorphic aditif, ditemukan tahun 1999 oleh pascal paillier[19]. Paillier cyptosystem memiliki dua kunci yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Langkah-langkah pembuatan kunci adalah sebagai berikut:

1. Pilih 2 bilangan prima p dan q secara acak dan independen satu sama lain sehingga
   $$\boldsymbol{gcd\left(pq,(p-1),(q-1)\right)=1} \quad \textbf{(1)}$$
2. Hitung RSA modulus n = pq dan fungsi Carmichael $\boldsymbol{\lambda = lcm\,(p-1),(q-1)}$ juga bisa dihitung dengan cara lain seperti
   $$\boldsymbol{\lambda = \frac{(p-1)(q-1)}{gcd\,(p-1),(q-1)}} \quad \textbf{(2)}$$
3. Dapatkan nilai generator g dimana $g \in \mathbb{Z}^*_{n^2}$ ada 2 cara untuk mendapatkan nilai g tersebut.
   a. Secara acak pilih nilai g dari set $\mathbb{Z}^*_{n^2}$, dimana
      $$\textbf{gcd}\left(\frac{g^{\lambda}\ mod\ n^2-1}{n}, n\right) = 1 \quad \textbf{(3)}$$
      Ada $\phi\,(n) * \phi\,(n)$, nilai generator yang valid, oleh karena itu probabilitas untuk memilih mereka dari $n\phi\,(n)$ elemen $\mathbb{Z}^*_{n^2}$ set relatif tinggi untuk n besar.
   b. Pilih α dan β secara acak dari set $\mathbb{Z}^*_{n^2}$, lalu hitung
      $$\boldsymbol{g = (an+1)\beta^n mod\ n^2} \quad \textbf{(4)}$$
4. Hitung modular multiplicative inverse dengan persamaan
   $$\boldsymbol{\mu = (L(g^{\lambda}\ mod\ n^2))^{-1}\ mod\ n} \quad \textbf{(5)}$$
   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(λ, μ).

Untuk melakukan proses enkripsi maka dijelaskan sebagai berikut :

1. Jadikan m sebagai pesan yang akan di enkripsi, dimana $m \in \mathbb{Z}_n$
2. Pilih nilai acak r, dimana $r \in \mathbb{Z}^*_n$
3. Hitung ciphertext dengan persamaan :
   $$\boldsymbol{c = g^m . r^n\ mod\ n^2} \quad \textbf{(6)}$$

Untuk melakukan proses dekripsi maka dijelaskan sebagai berikut :

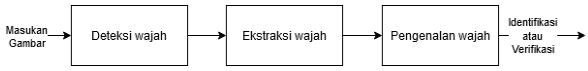
1. Ciphertext $c \in \mathbb{Z}^*_{n^2}$
2. Hitung pesan dengan
   $$\boldsymbol{m = L\left(c^{\lambda}\ mod\ n^2\right).\mu\ mod\ n} \quad \textbf{(7)}$$

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.
   $$\boldsymbol{D(E(m_1,r_1) * E(m_2,r_2) mod\ n^2) = m_1 + m_2\ mod\ n} \quad \textbf{(8)}$$
2. Satu buah ciphertext dengan plaintext dengan penggunaan g akan didekripsi untuk menghitung hasil penjumlahan plaintext yang sesuai.
   $$\boldsymbol{D(E(m_1,r_1) * g^{m_2}\ mod\ n^2) = m_1 + m_2\ mod\ n} \quad \textbf{(9)}$$

2.5. *Face Recognition*

Face recognition adalah teknik yang dipakai untuk melakukan identifikasi terhadap wajah, biasanya digunakan untuk tujuan keamanan sistem selain pengenalan sidik jari ataupun retina mata. Di penelitian yang dilakukan Jigar dkk, Teknik pengenalan wajah secara sederhana digambarkan dalam diagram alir yang digambarkan pada gambar 2 sebagai berikut[20]:



Gambar 2 Diagram Alir Pengenalan Wajah

3. METODOLOGI PENELITAN

Metodologi peneltiian yang digunakan adalah Deskriptif yaitu Metode yang memiliki sebuah tujuan untuk bisa mengumpulkan data secara detail, mendalam dan juga actual. Adapun metode pengumpulan data yang digunakan dalam penulisan penelitian ini adalah sebagai berikut :

1. Studi Literatur
   Studi literatur merupakan pengumpulan data dengan cara mempelajari sumber kepustakaan

diantaranya hasil penelitian, jurnal, paper, buku referensi, dan bacaan-bacaan yang ada.

2. Wawancara
   Tahap pengumpulan data dengan cara tanya jawab langsung dengan pihak terkait permasalahan yang diambil.
3. Kuesioner
   Tahap pengumpulan data dengan cara memberikan pertanyaan ke sejumlah responden terkait permasalahan yang diambil.

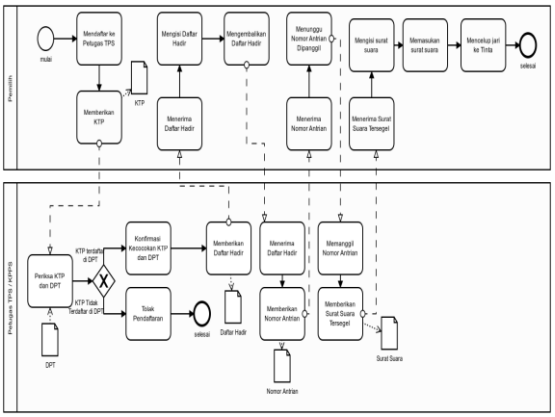
4. HASIL DAN PEMBAHASAN

4.1. Analisis Sistem Yang Sedang Berjalan

Analisis sistem yang sedang berjalan adalah proses pemecahan suatu sistem yang utuh ke dalam bagian-bagian kecil dimaksudkan untuk mengevaluasi dan mengidentifikasi suatu masalah hingga didapat suatu solusi. Dilakukan analisis sistem pada proses pemungutan suara terutama pada proses pemberian suara dan rekapitulasi suara di Komisi Pemilihan Umum Kota Bandung.

1. Analisis Prosedur Pemungutan Suara

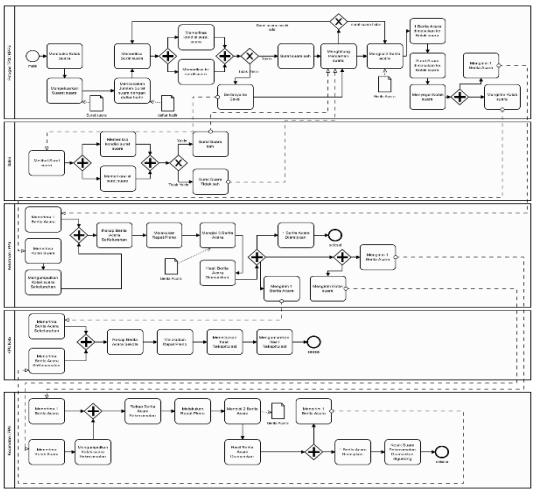
Analisis ini bertujuan untuk memberikan gambaran detail terhadap prosedur pemungutan suara. Proses pemungutan suara digambarkan pada gambar 3 BPMN pemungutan suara:



Gambar 3 Analisis Pemungutan Suara

2. Analisis Prosedur Rekapitulasi Suara

Analisis ini bertujuan untuk memberikan gambaran detail terhadap prosedur rekapitulasi suara. Proses pemungutan suara digambarkan pada gambar 4 BPMN rekapitulasi suara:



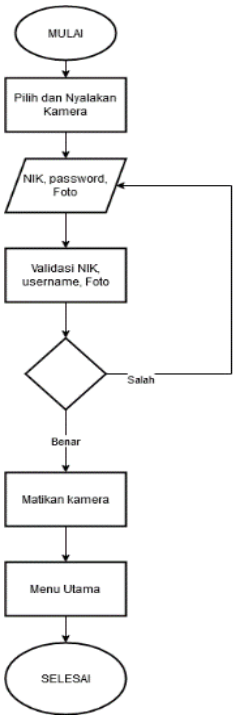
Gambar 4 Proses Rekapitulasi Suara

4.2. Analisis *E-Voting*

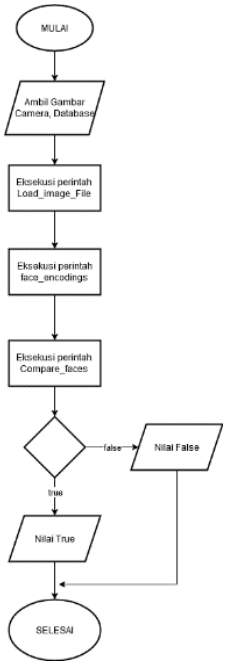
Analisis E-voting merupakan tahapan dimana kebutuhan apa saja yang dibutuhkan pemilih dan petugas . Analisis dilakukan berdasarkan hasil analisis proses yang berjalan dengan mengikuti asas Pemilihan Umum di Indonesia yang menganut asas Langsung, Umum, Bebas, dan Rahasia. Adapun E-voting pada sistem yang diusulkan dibagi kedalam dua tahapan yaitu analisis Face Recognition dan Analisis Enkripsi Homomophorphic

1. Analisis *Face Recognition*

Analisis *face recognition* merupakan tahapan analisis yang menjelaskan bagaimana proses validasi terhadap pemilih dilakukan untuk menjaga hanya pengguna yang memiliki hak pilih saja yang dapat memberikan suara..



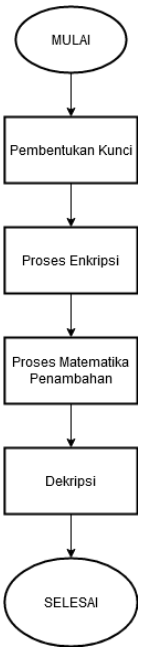
Gambar 5 Flowchart Validasi Pemilih



Gambar 6 Flowchart Validasi Pemilih

2. Analisis Enkripsi Homomorphic

Analisis Enkripsi Homomorphic merupakan tahapan analisis yang menjelaskan bagaimana proses Enkripsi terhadap suara yang diberikah oleh pemilih saat melakukan pemungutan suara.Berikut adalah contoh ilustrasi dari penerapan QR Code Scanner untuk membaca data dari suatu QR Code :



Gambar 7 Flowchart Enkripsi Homomorphic

3. Analisis Teknologi Geotagging

GPS Pada proses rekapitulasi suara pemilihan walikota kota bandung 2018 terdapat tiga kandidat calon, jumlah kandidat tersebut akan digunakan sebagai contoh proses enkripsi homomorfik dengan nilai suara awal masing-masing berjumlah nol, digambarkan pada Tabel 1 Jumlah suara awal.

Tabel 1 Jumlah Suara Awal

Kandidat No.	Suara
1	0
2	0
3	0

Enkripsi homomorfik menggunakan algoritma asimetrik dalam proses pembentukan kuncinya yang berarti ia akan memiliki kunci yang berbeda untuk proses enkripsi dan dekripsinya. Pembuatan Kunci dilakukan pertama kali untuk menghasilkan dua buah kunci. Untuk membuat kunci library python paillier menyediakan perintah paillier.generate_paillier_keypair(). Dengan perintah tersebut kunci publik dan privat pun terbentuk.

1. Kunci publik
2. Kunci private

Setelah tahapan pembuatan kunci maka dilakukanlah proses enkripsi terhadap seluruh suara yang dimiliki masing-masing kandidat. Proses enkripsi akan dilakukan dengan menggunakan kunci publik yang telah dibuat sebelumnya sehingga didapatkan ciphertext yang merepresentasikan suara yang telah ter enkripsi. Untuk melakukan enkripsi digunakan perintah public_key.encrypt(), hasil dilihat pada Tabel 2 Enkripsi.

Tabel 2 Hasil Enkripsi

Kandidat No	m / suara	c / ciphertetxt
1	0	985781 … 0190

Setiap dilakukan pemungutan suara / pemberian suara oleh pemilih nilai akan ditambahkan satu serta data id pemilih akan disimpan sehingga tidak dimungkinkan untuk memberikan suara lebih dari satu kali. Nilai suara yang terenkripsi akan ditambahkan nilai satu sehingga membuat ciphertext suara berubah, contoh dapat dilihat di Tabel 3 Enkripsi + satu.

Tabel 3 Hasil Enkripsi + satu

Kandidat No.	c / Ciphertext	c / Ciphertext + satu
1	985781 … 0190	410088 … 089675

Dilakukan dekripsi untuk melihat serta memastikan apakah perhitungan yang dilakukan sudah benar atau tidak. Proses dekripsi dilakukan dengan penggunaan paarameter kunci publik yaitu parameter λ, μ. Untuk melakukan dekripsi digunakan perintah private_key.decrypt(), dilihat pada Tabel 4 Dekripsi.

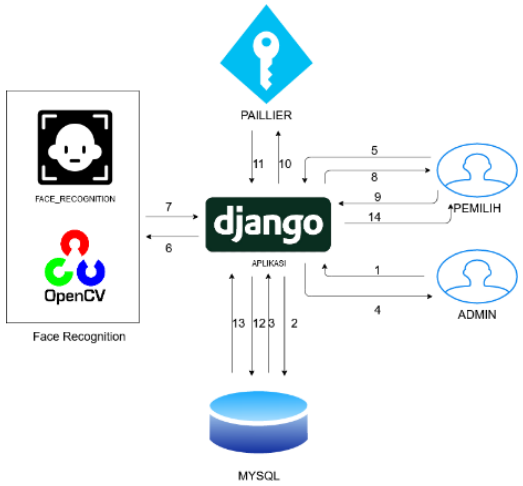
Tabel 4 Hasil Dekripsi

Kandidat No.	Ciphertext + satu	Hasil Dekripsi

1	410088 … 089675	1

4.3. Analisis Arsitektur Sistem

Analisis arsitektur bertujuan untuk mengidentifikasi kebutuhan yang dibangun berdasarkan sistem berbasis website. Arsitektur perangkat lunak pada platform website menggambarkan bagaimana perangkat lunak saling berinteraksi seperti diilustrasikan pada gambar 8 Arsitektur Sistem.



Gambar 8 Gambaran Arsitektur Sistem

1. Penjelasan arsitektur sistem:
2. Admin mengakses aplikasi agar dapat melihat dan mengelola data.
3. Sistem meminta database Mysql untuk menyimpan data yang diolah oleh admin.
4. Database Mysql memberikan data yang diolah kepada sistem.
5. Sistem akan menampilkan seluruh data dari database Mysql kepada admin.
6. Pemilih meminta mengakses aplikasi agar dapat melihat data.
7. Aplikasi meminta sistem face recognition untuk melakukan verifikasi terhadap pemilih.
8. Sistem face recognition memberikan data verifikasi face recognition pemilih kepada aplikasi.
9. Aplikasi memberikan akses aplikasi kepada pemilih.
10. Pemilih mengakses aplikasi agar melihat data dan melakukan pemungutan suara
11. Aplikasi meminta paillier untuk mengenkripsi suara yang diberikan pemilih.
12. Paillier memberikan respon berupa data suara telah dienkripsi.
13. Aplikasi meminta database mysql menyimpan data suara terenkripsi.
14. Databse mysql memberikan suara yang terenkripsi untuk ditampilkan di aplikasi.
15. Aplikasi memberikan pesan bahwa ia berhasil memberikan suara ke pemilih.

4.4. Analisis Kebutuhan Non-Fungsional

Perangkat keras dan lunak merupakan komponen sistem yang tidak dapat dipisahkan, dibutuhkan suatu spesifikasi untuk Perangkat keras dan lunak agar sistem yang dibangun berjalan sesuai dengan apa yang diharapkan seperti yang ditampilkan di Tabel 5 dan 6.

Tabel 5 Kebutuhan Perangkat Keras

Spesifikasi Perangkat Keras yang dibutuhkan		
No.	Perangkat Keras	Spesifikasi
1	Processor	AMD ryzen 5 setara atau keatas dan support SSE2 untuk windows
2	Layar / diplay	1366 x 768 pixel
3	VGA	3 GB
4	Harddisk	500 GB
5	Memori(Ram)	4/8 GB

Tabel 6 Kebutuhan Perangkat Lunak

Spesifikasi Perangkat Lunak yang dibutuhkan		
No.	Perangkat Lunak	Keterangan
1	Windows 10 Student / Ubuntu 18.04	Sebagai Sistem Operasi
2	Django 3.0	Sebagai framework Pthon
3	Pycharm	Sebagai text Editor
4	Python 3.8.2	Sebagai bahasa Pemprograman
5	Face_recognition 1.4.0	Sebagai library deteksi wajah
6	Python_paillier stable version	Sebagai library enkripsi homomorfik
7	nginx	Sebagai web service

4.5. Analisis Kebutuhan Fungsional

Analisis kebutuhan fungsional menggunakan pendekatan berbasis objek dengan tools pemodelan yaitu UML. tahapan analisis akan menggunakan pemodelan dari UML meliputi diagram use case, skenario use case, diagram activity, dan diagram class. Hasil Analisis kebutuhan fungsional pada sistem e-voting adalah sebagai berikut :

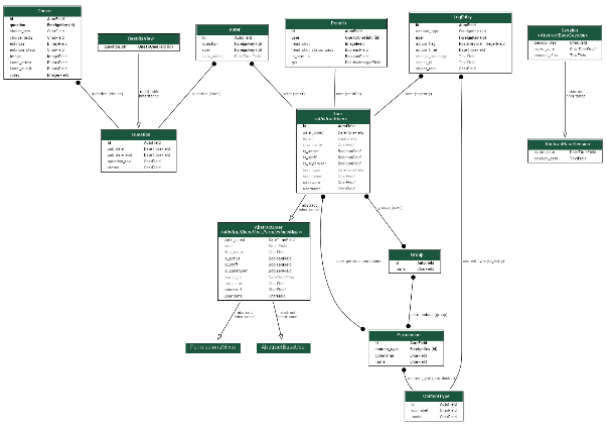
1. Use Case Diagram

Use Case diagram menggambarkan kasus atau situasi kebutuhan pengguna. Penggambaran diagram use case pada gambar 9 Diagram Use Case

Gambar 9 Diagram Use Case

2. Class Diagram

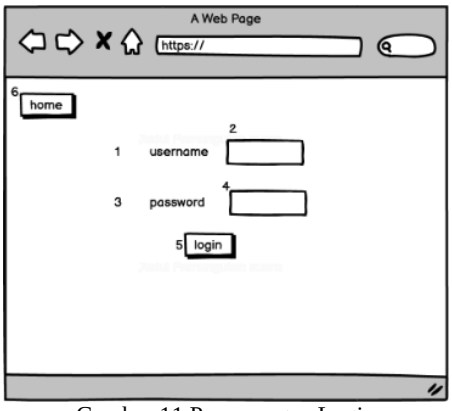
Class diagram menggambarkan berbagai objek yang dibutuhkan sistem untuk memenuhi kebutuhan masalah, Class Diagram digambarkan pada gambar 10 Class Diagram :



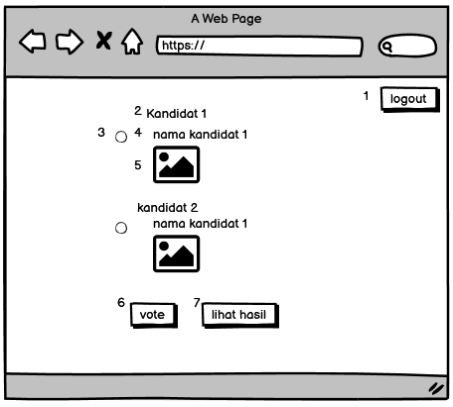
Gambar 10 Class Diagram

4.6. Perancangan Antarmuka *E-Voting*

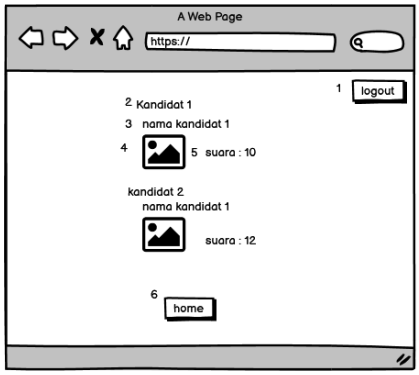
Berikut adalah hasil perancangan antarmuka pada sistem e-voting yang sedang dibangun :



Gambar 11 Perancangan Login



Gambar 12 Perancangan Antarmuka Memberi Suara



Gambar 13 Perancangan Antarmuka Hasil Pemilihan Suara

4.7. Implementasi Antarmuka

Implementasi Implementasi antar muka dilakukan pada setiap halaman tampilan yang dimiliki oleh siste, halaman antarmuka tersebut dibangun didalam bentuk *file python (dot)py dan html*.

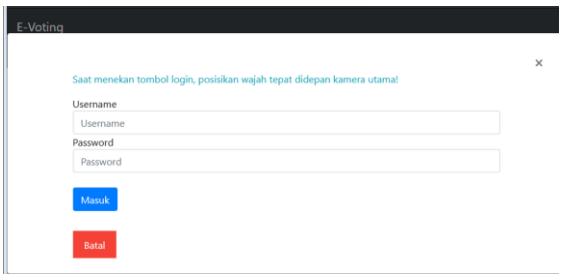
Tabel 7 Implementasi Antar Muka

No	Kode Antarmuka	Nama Antarmuka	Nama File
1	T01	Halaman menu utama pemilih	Common_home page.html, Homepage.html
2	T02	Halaman login pemilih	Common_home page.html, Login.html
3	T03	Halaman Index Pemilih	Common.html. index.html
4	T04	Halaman Voting Pemilih	Common.html, detail.html
5	T05	Halaman Hasil Voting Pemilih	Common.html, result.html
6	T06	Halaman Login Admin	Admin.py
7	T07	Halaman Menu Utama Admin	Admin.py
8	T08	Halaman pengguna Admin	Admin.py
9	T09	Halaman Pertanyaan Admin	Admin.py
10	T10	Halaman detail pengguna Admin	Admin.py
11	T11	Halaman detail pertanyaan Admin	Admin.py

No	Kode Antarmuka	Nama Antarmuka	Nama File
12	T12	Halaman dekripsi Admin	Common.html, dekripsi.html
13	T13	Halaman Tidak Tersedia	404.html

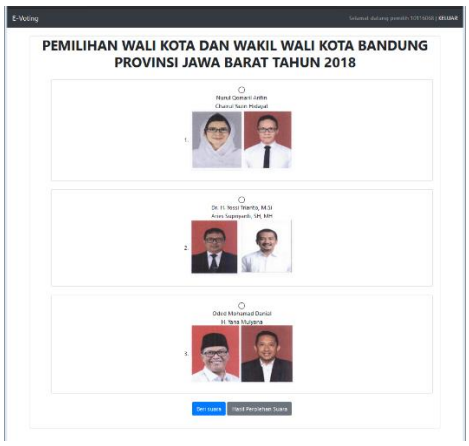
Berikut adalah beberapa hasil dari implementasi antarmuka pengguna pada sistem E-Voting.

1. Implementasi Login Pemilih



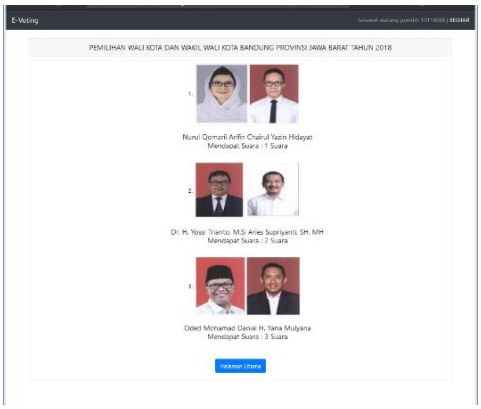
Gambar 14 Tampilan Halaman Login Pemilih

2. Implementasi Halaman Voting Pemilih



Gambar 15 Tampilan Halaman Voting Pemilih

3. Implementasi Halaman Hasil Voting Pemilih



Gambar 16 Tampilan Halaman Hasil Voting

4.8. Pengujian Sistem

Pengujian Sistem E Voting dilakukan kedalam beberapa tahapan pengujian antara lain penguujian blackbox, pengujian waktu penggunaan, pengujian face recognition, dan pengujian enkripsi. Berikut adalah hasil dari setiap pengujian yang telah dilakukan

1. Hasil Pengujian Blackbox

Hasil Pengujian black box menampilkan hasil pengujian secara fungsionalitas dimana didapatkan hasil bahwasanya keseluruhan fungsionalitas sistem berjalan sesuai dengan apa yang diharapkan kecuali proses validasi face-recognition yang hanya berjalan normal di lingkungan development sedangkan di lingkungan production tidak berjalan sesuai dengan apa yang diharapkan.

2. Hasil Pengujian Waktu Penggunaan

Pengujian waktu penggunaan diuji oleh 3 orang penguji dengan prosedur penguji melakukan login hingga memberikan suara pada sistem, waktu yang dibutuhkan penguji direkam dan disimpan untuk dilakukan evaluasi waktu. Tabel 8 memperlihatkan perbandingan waktu pemungutan suara sedangkan Tabel 9 memperlihatkan perbandingan waktu rekapitulasi suara.

Tabel 8 Waktu Penggunaan pemungutan suara

No	Pengguna	Waktu konvensional	Waktu e-voting	Kesimpulan
1	Penguji 1	229 detik	55 detik	Waktu e-voting lebih cepat
2	Penguji 2	163 detik	30 detik	Waktu e-voting lebih cepat
3	Penguji 3	201 detik	67 detik	Waktu e-voting lebih cepat
Rata rata waktu		197 detik	50 detik	Waktu e-voting lebih cepat 147 detik

Tabel 9 Waktu Penggunaan rekapitulasi suara

No	Waktu konvensional	Waktu e-voting	Kesimpulan
1	2 minggu	37 detik	Waktu rekapitulasi suara dengan e-voting lebih cepat dari waktu konvensional

3. Hasil Pengujian Face Recognition

Pengujian enkripsi homomorphic diuji dengan memberikan tiga calon masing-masing satu, dua, dan tiga suara. Dilihat apakah enkripsi homomorphic dapat menjaga kerahasian suara serta apakah suara yang dienkripsi dapat melakukan proses matematika sesuai dengan jumlah suara yang diberikan, dipelihatkan pada tabel 10 Pengujian Dekripsi.

Tabel 10 Pengujian Dekripsi

Sebelum didekripsi	Setelah didekripsi	Keterangan
		Sukses
		Sukses
		Sukses

4. Hasil Pengujian Enkripsi

Pengujian validasi pemilih dengan face recognition dengan tiga penguji didapatkan hasil yang ditampilakn pada Tabel 11 Pengujian *face recognition*.

Tabel 11 Pengujian face recognition

No	Wajah di database	Wajah saat login	hasil
1			Berhasil masuk
2			Berhasil masuk
3			Berhasil masuk
4			Tidak berhasil masuk
5			Tidak berhasil masuk
6			Tidak berhasil masuk

5. PENUTUP

5.1. Kesimpulan

Berdasarkan hasil pengujian perangkat lunak purwarupa sistem e-voting berbasis website maka diperoleh kesimpulan sebagai berikut:

1. Penerapan electronic voting dapat mempercepat dan menyederhanakan proses validasi dan perhitungan suara pada pemungutan suara.
2. Penerapan validasi pemilih meningkatkan tingkat keamanan validasi pemilih yang ingin memberikan suara.
3. Penerapan enkripsi homomorfik meningkatkan tingkat keamanan serta kerahasian dalam penyimpanan serta perhitungan proses perhitungan pemungutan suara karena hasil hanya dapat dilihat dan diperoleh setelah proses pemungutan suara selesai

5.2. Saran

Perangkat lunak yang dibangun merupakan produk yang hanya berfokus pada proses validasi pemilih dan perhitungan suara, oleh karena itu ada beberapa saran yang dapat digunakan sebagai panduan pengembangan perangkat lunak ini kearah yang lebih baik agar perangkat lunak ini dapat berkembang dan menjadi perangkat yang lebih baik dari sebelumnya, adapun saran-saran terhadap pengembangan perangkat lunak e-voting adalah sebagai berikut:

1. Persoalan terkait distribusi akun pemilih dibahas lebih dalam karena saat ini belum ada aturan terkait hal tersebut.
2. Mengembangkan perangkat lunak dari segi performasi dan tampilan agar pengalaman pengguna menjadi lebih baik.
3. Memperbaiki dan meningkatkan keamanan aplikasi yang telah dipaparkan pada pengujian keamanan.
4. Meningkatkan fitur sampai berita acara, diakrenkan sistem hanya mencangkup samapai rekapitulasi s.

DAFTAR PUSTAKA

[1] Komisi Pemilihan Umum, “Tentang KPU.” [Online]. Available: http://kpu-bimakab.go.id/pages/tentang-kpu.

[2] B. Pengawas, P. Umum, and R. Indonesia, “EVALUASI PELAKSANAAN PEMILIHAN 2018 UNTUK PERBAIKAN PROSEDUR PENYELENGGARAAN PEMILIHAN UMUM 2019,” 2019.

[3] “Laporan Kinerja 2018,” 2018.

[3] “Laporan Kinerja 2018,” 2018.

[4] I. M. Rodiana, B. Rahardjo, and A. I. W., “Design of a Public Key Infrastructure-based Single Ballot E-Voting System,” in 2018 International Conference on Information Technology Systems and Innovation (ICITSI), 2018, pp. 6–9, doi: 10.1109/ICITSI.2018.8696083.

[5] A. Nu'man, "A Framework for Adopting E-Voting in Jordan.," Electron. J. e-Government, vol. 10, no. 2, pp. 133–146, 2012.

[6] O. M. Olaniyi, D. O. Adewumi, E. a Oluwatosin, O. T. Arulogun, and M. a Bashorun, "Framework for multilingual mobile e-voting service infrastructure for democratic governance," African J. Comput. ICT, vol. 4, no. 3, pp. 23 – 32, 2011.

[7] C. F. Rozi and S. V. Dewi, "Journal of Informatics and Computer Science Vol . 6 No . 1 April 2020 Universitas Ubudiyah Indonesia RANCANG BANGUN APLIKASI E-VOTING PEMILIHAN GEUCHIK PADA KECAMATAN KLUET UTARA (SK : DI DESA KRUENG BATEE) BERBASIS WEB DESIGN AND DEVELOPMENT OF GEUCHIK," vol. 6, no. 1, pp. 1–10, 2020.

[8] M. Hartopo, "Pengembangan Aplikasi E-Voting Menggunakan Enkripsi Homomorfik."

[9] Z. H. Mahmood and M. K. Ibrahem, "New fully homomorphic encryption scheme based on multistage partial homomorphic encryption applied in cloud computing," in Proceedings - 2018 1st Annual International Conference on Information and Sciences, AiCIS 2018, 2019, pp. 182–186, doi: 10.1109/AiCIS.2018.00043.

[10] . M. Anggriane, S. M. Nasution, and F. Azmi, "Advanced e-voting system using Paillier homomorphic encryption algorithm," 2016 Int. Conf. Informatics Comput. ICIC 2016, no. Icic, pp. 338–342, 2017, doi: 10.1109/IAC.2016.7905741.

[11] A. V. E. Konstantin G. Kogos, Kseniia S. Filippova, "FULLY HOMOMORPHIC ENCRYPTION : CURRENT STATE OF THE ART Homomorphic Encryption," pp. 463–466, 2012.

[12] . M. Anggriane, S. M. Nasution, and F. Azmi, "Advanced e-voting system using Paillier homomorphic encryption algorithm," 2016 Int. Conf. Informatics Comput. ICIC 2016, no. Icic, pp. 338–342, 2017, doi: 10.1109/IAC.2016.7905741.

[13] rasko, B. Sutomo, and B. Santoso, "Penyuluhan Metode Audio Visual Dan Demonstrasi Terhadap Pengetahuan Menyikat Gigi Pada Anak Sekolah Dasar," J. Kesehat. Gigi, vol. 03, no. 2, pp. 53–57, 2016.

[14] M. Kahani, "Experiencing Small-Scale e-Democracy in Iran," Electron. J. Inf. Syst. Dev. Ctries., vol. 22, no. 1, pp. 1–9, 2005, doi: 10.1002/j.1681-4835.2005.tb00143.x.

[15] R. Sadikin, Kriptografi Untuk Keamanan Jaringan. Yogyakarta: Penerbit Andi, 2012.

[16] Wahana Komputer, Kriptografi Dalam Memahami Model Enkripsi Dan Security Data. Yogyakarta: Penerbit Andi, 2003.

[17] M. Kahani, "Experiencing Small-Scale e-Democracy in Iran," Electron. J. Inf. Syst. Dev. Ctries., vol. 22, no. 1, pp. 1–9, 2005, doi: 10.1002/j.1681-4835.2005.tb00143.x.

[18] P. Gerhard and B. Eng, "KV Web Security : Applications of Homomorphic Encryption," pp. 1–16, 2013.

[19] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 1999, doi: 10.1007/3-540-48910-X_16.

[20] J. Pandya, D. Rathod, and J. Jadav, "A survey of face recognition approach," Int. J. Eng. …, vol. 3, no. 1, pp. 632–635, 2013.

[21] B. Schneier, "Applied Cryptography," Electr. Eng., 1996, doi: 10.1.1.99.2838.