BAB 2
LANDASAN TEORI

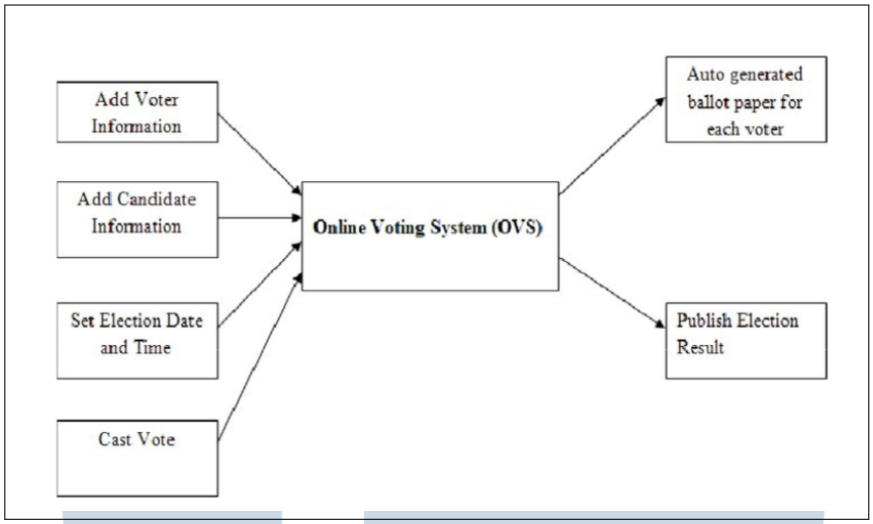
2.1 Rancang Bangun Sistem E-Voting

Electronic voting(e-voting) atau voting elektronik adalah sebuah hal yang relatif baru muncul di masyarakat. Mudanya usia voting elektronik dapat membuat banyak orang bingung akan perbedaannya dengan sistem voting tradisional yang sudah dilakukan secara internasional selama beberapa generasi. Oleh karena itu, bagian ini akan berfungsi untuk mendefinisikan pengertian voting elektronik yang akan digunakan pada penelitian ini, dan bagaimana rancang bangun sistem yang akan dibuat dalam penelitian ini.

Chauhan (2020) mendefinisikan *Online Voting System*, atau *Electronic Voting* sebagai sebuah sistem voting berbasis web yang dapat membantu kita mengontrol atau mengatur pemilu apapun secara mudah dan aman [17]. Suryavanshi (2020) menjelaskan bahwa *Online Voting System*, atau *Electronic Voting* adalah sebuah teknik voting secara online. Dalam sistem ini, orang-orang yang telah terdaftar dalam sistem dapat memberikan suara mereka secara online tanpa perlu datang secara langsung ke tempat pemungutan suara [18]. Sedangkan menurut Anand dan Divya (2012), *Online Voting System* adalah sebuah sistem pemberian suara dimana setiap pemberi suara dapat menggunakan hak pilihnya dari manapun tanpa perlu datang ke tempat pemungutan suara [19].

Dari ketiga definisi di atas, dapat kita simpulkan bahwa voting elektronik adalah sebuah cara dimana setiap pemberi suara dapat memberikan suara mereka dari manapun dan kapanpun melalui sebuah sistem voting yang umumnya berbasis web.

Chauhan (2020) juga memberikan sebuah proposal sistem voting elektronik yang dapat dibangun dalam bentuk diagram seperti dibawah ini [17].



Gambar 2.1. Proposal model sistem voting elektronik oleh Chauhan

Sumber: [17]

Chauhan (2020) juga menyertakan fitur-fitur yang akan diperlukan dalam model sistem voting elektronik yang disarankan di atas. Fitur-fitur tersebut adalah [17]:

1. User/Pengguna
2. Administrator
3. Pemberi suara
4. Fitur administrasi
5. Login
6. Manajemen kandidat
7. Manajemen posisi kandidat
8. Pemberian suara
9. Menampilkan hasil voting
10. Logout

Kadam (2016) menjabarkan beberapa hal yang harus dapat dilakukan oleh sistem voting elektronik, yaitu [20]:

1. Komisi Pemilihan Umum harus dapat menambahkan, menghapus, dan mengubah data pemberi suara.
2. Komisi Pemilihan Umum harus dapat menambahkan, menghapus, dan mengubah data kandidat.
3. Pemberi suara harus dapat memberikan suaranya untuk kandidat yang mereka inginkan.
4. Sistem harus dapat menghasilkan user ID unik untuk setiap pemberi suara yang terdaftar.
5. Hanya pengguna yang terdaftar yang boleh login dengan menggunakan user ID mereka.
6. Komisi Pemilihan Umum harus dapat mengevaluasi dan menerbitkan hasil pemilihan umum.

Dalam sistem yang akan dibangun dalam penelitian ini, User adalah pemberi suara yaitu seluruh mahasiswa UMN, dan administrator yaitu anggota KPU UMN yang bertugas pada tahun pemilu tersebut dilaksanakan. Fitur administrasi akan berisi manajemen kandidat, dan manajemen posisi kandidat yang dapat diakses oleh anggota KPU UMN yang bertugas pada tahun pemilu tersebut dilaksanakan. Fitur pemberian suara akan dapat dilakukan dengan menampilkan kandidat organisator himpunan mahasiswa dari prodi sang pemberi suara dan posisi mereka.

2.2 Algoritma Enkripsi Paillier

Algoritma Enkripsi Paillier dicetuskan oleh Pascal Paillier pada tahun 1999 [8]. Algoritma Paillier adalah sebuah algoritma asimetris yang berarti algoritma tersebut menggunakan pasangan *public key* dan *private key* dalam sistemnya. *Public key* akan digunakan untuk melakukan enkripsi data dan bersifat publik, berarti siapa saja dapat mengetahuinya. Sedangkan *private key* akan digunakan untuk melakukan dekripsi data dan bersifat rahasia. Hanya penerima pesan enkripsi yang telah dienkripsi dengan *public key* yang terkait yang dapat mengetahuinya.

Algoritma Paillier adalah sistem kriptografi yang bersifat homomorfis secara aditif. Hal ini berarti seseorang dapat menghitung jumlah dari pesan asli M_1 dan M_2 hanya dengan mengetahui *public key* dan hasil enkripsi M_1 dan M_2. Sifat tersebut memungkinkan sistem yang akan dibangun untuk dapat

menghitung hasil pemungutan suara tanpa perlu melakukan dekripsi terlebih dahulu, menjaga kerahasiaan suara yang telah diberikan. Terdapat 4 proses yang dilakukan oleh sistem dalam penerapan Algoritma Paillier yaitu menghasilkan *key* yang akan digunakan, melakukan enkripsi suara yang diberikan sebelum disimpan di *database*, melakukan perhitungan suara dengan memanfaatkan sifat homomorfis Algoritma Paillier, dan melakukan dekripsi data jumlah akhir suara untuk ditampilkan.

A Menghasilkan Kunci

Proses menghasilkan kunci yang akan digunakan oleh sistem terdiri dari 4 tahap, yaitu :

1. Pilih 2 bilangan prima p dan q secara acak dan independen satu sama lain yang memenuhi syarat dimana faktor persekutuan terbesar dari $p*q$ dan $(p-1)*(q-1)$ adalah 1. Jika p dan q memiliki jumlah digit yang sama, maka syarat tersebut terpenuhi secara otomatis [21].

2. Hitung n dan λ dimana n adalah hasil dari $p*q$ dan λ adalah $\varphi(n)$, yaitu hasil perkalian dari $p-1$ dan $q-1$.

3. Pilih bilangan asli g dimana $g = n+1$.

4. Pastikan n membagi *order* dari g dengan mengecek keberadaan dari *modular multiplicative inverse* $\mu = \varphi(n)^{-1} \, mod \, n$.

   Keterangan :
   p : bilangan prima yang berbeda dari q.
   q : bilangan prima yang berbeda dari p.
   n : $p*q$.
   λ : $\varphi(n)$.
   $\varphi(n)$: Hasil perkalian dari $p-1$ dan $q-1$.
   g : $n+1$.
   μ : $\mu = \varphi(n)^{-1} \, mod \, n$.

B Enkripsi Suara

Proses enkripsi suara m yang dimana $0 \leq m < n$ terdiri dari 2 tahap, yaitu :

1. Pilih bilangan asli r secara acak dimana $0 < r < n$.

2. Hitung *ciphertext* c dengan $c = g^m * r^n \, mod \, n^2$.

   Keterangan :
   m : data suara yang akan dienkripsi.
   r : bilangan asli lebih kecil dari n.
   c : ciphertext hasil proses enkripsi.

C Penjumlahan Homomorfis

Proses penghitungan suara akan dilakukan dengan memanfaatkan sifat homomorfis aditif dari Algoritma Paillier dengan mengalikan seluruh *ciphertext* untuk mendapatkan *ciphertext* dari jumlah akhir suara.

D Dekripsi Jumlah Suara

Proses dekripsi *ciphertext* c dimana $c \in \mathbb{Z}_n^*$ dilakukan dengan menghitung $m = (L(c^\lambda \, mod \, n^2)) * \mu \, mod \, n$.

Keterangan :
$L(x)$: $\frac{x-1}{n}$.

2.3 Arsitektur Framework Model-View-Controller

Junindar (2019) menjelaskan bahwa Model-View-Controller atau MVC adalah sebuah metode untuk membuat sebuah aplikasi dengan memisahkan data (Model) dari tampilan (View) dan bagaimana cara memprosesnya (Controller) [22]. Perkins (2013) mendefinisikan MVC sebagai sebuah pola yang membantu desainer dan developer untuk memisahkan sistem menjadi logika input, logika bisnis, dan logika antarmuka pengguna. Model merupakan kelas yang digunakan untuk menyimpan, memanipulasi, dan mengambil informasi dari *database*, view merupakan tampilan antarmuka dari aplikasi yang menampilkan dan mendukung manipulasi data yang ditampilkan tersebut, dan controller mengatur interaksi antara model dan view [23]. Voorhees (2020) menjelaskan bahwa Model-View-Controller (MVC) adalah sebuah arsitektur perangkat lunak

yang membagi sebuah aplikasi menjadi tiga komponen desain : model, view, dan controller. Model bertanggungjawab dalam manajemen data, view bertanggungjawab dalam menyediakan antarmuka untuk interaksi pengguna ketika dibutuhkan, dan controller bertanggungjawab dalam berkomunikasi dengan komponen model dan view sehingga menjadi bagian yang menyatukan ketiga komponen tersebut [24].

Voorhees juga menjelaskan bahwa terdapat dua keuntungan dalam menggunakan MVC. Pertama, memisahkan antarmuka pengguna dengan manajemen data memungkinkan teknologi untuk salah satu komponen tersebut untuk diubah tanpa berdampak kepada teknologi yang digunakan pada komponen yang lain. Kedua, penggunaan MVC akan menghasilkan tiga komponen yang masing-masing lebih kohesif [24].

Dari ketiga definisi di atas, dapat kita simpulkan bahwa MVC adalah sebuah pola arsitektur yang digunakan untuk membantu pembangunan framework aplikasi web atau mobile. MVC dapat dibagi menjadi tiga bagian, yaitu Model, View dan Controller. Setiap bagian tersebut memiliki fungsi dan tugas yang berbeda. Model adalah bagian yang menyimpan, mengatur, dan merepresentasikan data, logika, dan aturan aplikasi. Model berhubungan dengan database untuk menyimpan dan mengambil data. Sedangkan view adalah bagian yang berinteraksi langsung dengan pengguna dalam bentuk antarmuka pengguna. View berfungsi untuk menampilkan data yang telah diambil oleh model sesuai dengan aturan dari controller. Lalu, controller adalah bagian yang menghubungkan view dan model. Controller berfungsi untuk meneruskan input dari view kepada model, dan meneruskan data dari model ke view untuk ditampilkan. Controller juga mengatur bagaimana view harus menampilkan data yang telah diambil dari model.

2.4 Pemilihan Umum Himpunan Mahasiswa di UMN

Pemilihan umum (Pemilu) di UMN dilaksanakan oleh KPU UMN di semester gasal setiap tahunnya.Pelaksanaan pemilu di UMN dimulai dengan dilakukannya pendaftaran terbuka oleh KPU UMN dimana seluruh mahasiswa aktif UMN dapat mendaftarkan diri sebagai calon organisator. Setelah proses seleksi awal selesai, calon organisator yang terpilih akan melewati sesi wawancara dan *focus group discussion* (FGD). Calon organisator yang melewati kedua tahap sebelumnya lalu akan diseleksi secara internal oleh panitia regenerasi setiap himpunan mahasiswa. Calon-calon organisator yang lolos tahap tersebut akan

membentuk pasangan calon yang akan maju dalam pemilihan umum.

Setelah seluruh proses seleksi selesai, KPU UMN dan setiap himpunan mahasiswa akan mempublikasikan daftar pasangan calon organisator untuk setiap himpunan mahasiswa dan memulai bulan demokrasi. Dalam bulan demokrasi, para calon organisator akan dapat melakukan kampanye, debat, dan talkshow dalam usaha mereka untuk mendapatkan dukungan dari mahasiswa UMN sebagai pemberi suara. Selesainya bulan demokrasi menandakan dimulainya masa tenang dimana segala bentuk kampanye dilarang. Setelah masa tenang selesai, *election week* akan dimulai. Dalam *election week*, pemberi suara yaitu seluruh mahasiswa aktif UMN akan dapat memberikan suaranya dan memilih satu pasangan calon dari daftar pasangan calon untuk himpunan mereka.

Setelah *election week* berakhir, KPU UMN akan memulai perhitungan suara dan mengumumkan pasangan calon yang terpilih sebagai ketua dan wakil ketua masing-masing himpunan untuk satu tahun kedepan dengan menggunakan sistem pemegang suara terbanyak satu putaran. Dalam penelitian ini, ditetapkan jumlah maksimal pemberi suara adalah 9999. Batas tersebut dipilih karena program studi UMN dengan jumlah mahasiswa terbanyak pada semester ganjil 2021 adalah Ilmu Komunikasi dengan 2086 mahasiswa [25]. Sehingga, jumlah 9999 dianggap masih dapat mencakup perkembangan jumlah mahasiswa UMN untuk waktu yang cukup lama.