

BAB II

LANDASAN TEORI

2.1 Data

Arti dari data menurut KBBI (Kamus Besar Bahasa Indonesia) yaitu keterangan atau bahan nyata yang dapat dijadikan dasar kajian (analisis atau kesimpulan). Data merupakan bentuk dari dasar atas peristiwa, benda, aktivitas atau transaksi yang dicatat, dikumpulkan dan disimpan yang belum terolah dalam volume yang besar (Widodo, 2016). Berdasarkan penjabaran diatas dapat ditarik kesimpulan bahwa data merupakan suatu kejadian atau peristiwa yang dicatat dan dikumpulkan untuk menjadi landasan dari suatu analisis, hipotesis, dan kesimpulan.

2.2 Pemilu

Pemilu yang merupakan kependekan dari Pemilihan Umum adalah cara untuk menyampaikan suara untuk melakukan pemilihan anggota eksekutif dan legislatif yang dilakukan di Indonesia dengan rentang lima tahun sekali (Retno, 2018). Peserta yang menjadi kandidat Pemilihan Umum menurut Undang-Undang No. 7 Tahun 2017 adalah partai politik untuk lembaga DPR, DPRD Provinsi, anggota DPRD kota atau kabupaten, perseorangan untuk Pemilu anggota DPD, dan pasangan calon presiden dan wakil presiden dari gabungan partai atau partai politik.

2.2.1 Voting

Voting atau pemungutan suara merupakan suatu cara untuk mengumpulkan sebuah pendapat atau kumpulan pendapat dari individu ataupun kelompok (Yi, 2019). Cara ini digunakan dalam pengambilan keputusan yang penting atau krusial, seperti contohnya wakil rakyat, dan calon pemimpin negara seperti presiden dan wakil presiden (Risnanto, 2017) . Dengan demikian, Indonesia melakukan proses *voting* yang merupakan tahapan dari dari Pemilu untuk mengumpulkan suara atau pendapat-pendapat yang diajukan dari individu terhadap calon pemimpin negara dan wakil rakyat.

2.2.2 E-Voting

Electronic Voting merupakan cara yang digunakan dalam pengumpulan suara serta perhitungan suara dalam sebuah pemilihan dengan menggunakan alat elektronik (Risnanto, 2017). Sebuah sistem *E-voting* diperlukan untuk memiliki asas yang diterapkan di Indonesia sesuai undang-undang yang berlaku yaitu langsung, umum, bebas, rahasia yang dikenal dengan singkatan LUBER serta jujur dan adil yang dikenal dengan singkatan JURDIL.

2.3 Integritas

Menurut Kamus Besar Bahasa Indonesia (KBBI) Integritas adalah mutu, sifat, atau keadaan yang menunjukkan kesatuan yang utuh sehingga memiliki potensi dan kemampuan yang memancarkan kejujuran (Arti kata integritas -

Kamus Besar Bahasa Indonesia (KBBI) Online, 2019). Integritas berhubungan terhadap kesatuan yang utuh dari sebuah data dari terbuat awal yang dapat menunjukkan adanya perubahan (Tika Ramadhan, 2014). Berdasarkan pengertian tersebut, integritas data merupakan hal yang penting dalam menjaga keaslian dan adanya perubahan dari suatu data dimana yang nantinya akan mempengaruhi hasil akhir.

2.4 Sistem

Sistem merupakan sebuah entitas yang terdiri dari beberapa elemen yang terhubung atau saling bekerjasama agar mencapai suatu tujuan yang telah ditentukan sebelumnya (Husain, 2017). Dalam perancangan sistem, diperlukan prosedur-prosedur yang tepat untuk melakukan instruksi yang diberikan atau persoalan yang telah diberikan untuk diproses sehingga hasil yang diinginkan itu tercapai dengan efektif dan efisien.

2.4.1 *Waterfall*

Waterfall merupakan pengembangan perangkat lunak dengan prinsip linear atau sekuensial yang dimulai dari kebutuhan dasar dan spesifikasi pengguna melalui *planning*, *modeling*, *construction*, dan *deployment*, dan melakukan pemeliharaan terhadap sistem yang telah selesai dibangun (Suryan, 2014).

2.4.2 Aplikasi

Aplikasi merupakan sebuah perangkat lunak yang terdiri dari perintah atau instruksi yang berguna untuk pekerjaan atau proses tertentu seperti manipulasi data, pembuatan data, menampilkan data (Astari, 2018). Dalam sebuah sistem, terdapat beberapa aplikasi yang terhubung atau terintegrasi satu dengan yang lainnya. Aplikasi yang dirancang sudah selayaknya melakukan fungsi-fungsi yang telah ditetapkan dengan baik dan memiliki kesalahan seminimal mungkin agar memberikan hasil yang tepat.

2.4.3 Platform

Platform merupakan sebuah komputer atau perangkat keras atau sistem operasi terkait atau sebuah rekayasa lingkungan dimana sebuah perangkat lunak atau *software* dapat dilakukan instalasi dan dijalankan (Platform - Glossary, 2020). Beberapa contoh *platform* menurut *National Institute of Standards and Technology* salah satunya adalah *Linux*, *Microsoft Windows Vista* dan *Java*.

2.4.4 Autentikasi

Autentikasi merupakan sebuah proses untuk menentukan dan memastikan terhadap pengguna yang mengajukan sebuah sumber daya atau sesuatu yang diklaim oleh dirinya dengan melakukan komparasi terhadap kredensial yang sebelumnya disimpan didalam sistem (Fahmy & Elkhateeb, 2018). Proses autentikasi sudah selayaknya diterapkan pada sebuah sistem

yang membutuhkan validasi atau kepastian pengguna yang mengakses sistem.

2.4.5 Biometrik

Biometrik merupakan penggunaan dari keunikan dari psikologis, karakteristik perilaku untuk menentukan identitas dari seseorang (Ogbanufe et al., 2018). Biometrik dapat digunakan dalam tahap autentikasi dalam sebuah sistem karena penggunaan keunikan dari masing-masing individu.

2.4.6 Sidik Jari

Sidik jari atau *fingerprint* merupakan pola yang terdiri serpeti lembah dan pegunungan yang terdapat pada lapisan *epidermis* kulit yang terletak pada setiap jari kita (Almajmaie et al., 2019). Pola dari sidik jari tersebut sudah selayaknya berbeda satu individu dengan individu lainnya sehingga memungkinkan kita untuk menentukan sebuah individu tersebut.

2.4.7 .NET Framework

.NET Framework merupakan kerangka kerja yang digunakan dalam ruang lingkup pengembangan yang dapat menjalankan beberapa bahasa pemrograman seperti *C#* dan *VB.NET* yang memiliki kompilasi dalam program secara lebih baik, performa yang cepat dan dapat menjaga dari segi keamanan dalam aplikasi yang telah di kompilasi oleh kerangka kerja tersebut (Katkar et al., 2020). Menggunakan kerangka kerja atau *framework* *.NET* terdiri dari berbagai komponen objek yang dapat digunakan dalam

sebuah pengembangan sistem yang menyesuaikan dengan *platform* yang dibuat.

2.4.8 *ExpressJS Framework*

ExpressJS Framework merupakan kerangka kerja berbasis *web* yang berjalan pada *Node.JS* dengan bahasa pemrograman berbasis *JavaScript* modul HTTP dan modul *connect* (Mardan, 2014). Menggunakan *ExpressJS* membantu dalam pembuatan kode secara rapih dan terstruktur sehingga kode yang telah dibangun dapat dipakai kembali dalam pengembangan sistem yang berkelanjutan.

2.4.9. *End to End Verifiable*

E2E Verifiable (e2e) yang merupakan proses pemberian informasi terhadap pemilih yang telah menandakan dia telah melakukan *voting* tanpa menampilkan identitas pemilih didalam sistem (Wang et al., 2017).

2.4.10 *Advanced Encryption Standard*

Advanced Encryption Standard (AES) merupakan enkripsi dengan kunci *symmetric* yang telah ditetapkan standar oleh *National Institute of Standards and Technology* (James & Kumar, 2016). Enkripsi *AES* memiliki cara kerja dengan membagi data yang ingin di enkripsi menjadi sebuah blok kemudian di konversi kedalam satuan byte yang terdiri dari 4 baris dan 4

kolom matriks kemudian dilakukan perubahan dari byte tersebut dengan mencocokkan dengan tabel *Rijindael S-Box* dengan merubah nilai byte atau substitusi byte dalam kolom menjadi bilangan basis 16 atau heksadesimal sesuai posisi kolom *S-box* tersebut, kemudian menggeser byte dalam setiap baris secara *incremental* dan mencampurkan data tersebut dengan mengali setiap kolom dengan matriks *Rijindael Galois*. Hasil tersebut dilakukan operasi *exclusive or* (XOR) dengan hasil karakter kunci dalam heksadesimal ataupun byte setiap kolom dari blok tersebut.

2.5 Blockchain

Blockchain merupakan kumpulan dari data atau transaksi yang terekam yang digambarkan sebagai sebuah balok atau *block* yang memiliki *timestamp* dan pernyataan integritas dari blok sebelumnya dalam bentuk *hash* yang saling terhubung antar blok sehingga membentuk rantai dari blok tersebut (Damai et al., 2019). Blok yang terhubung dan telah dibuat dalam sebuah komputer akan digandakan ke dalam perangkat komputer yang telah terhubung dalam satu jaringan, sehingga bersifat secara desentralisasi (Yi, 2019). Data yang telah di tulis kedalam blockchain tidak bisa diubah karena data dari blok tersebut terhubung dengan blok sebelumnya, sehingga dibutuhkan proses perubahan seluruh data yang terhubung dengan blok yang ingin dirubah serta komputer yang terhubung dalam satu jaringan yang

memegang data *blockchain* yang terduplikasi tersebut sehingga menyulitkan penyerang untuk melakukan perubahan data yang sudah tertulis.

2.5.1 *Ethereum*

Ethereum merupakan sebuah *platform* perangkat lunak dengan sifat aplikasi desentralisasi dan memiliki *smart contracts* yang memiliki kegagalan proses atau kecurangan yang minim (Teles, 2019). *Ethereum* beroperasi dengan menggunakan *Ethereum Virtual Machine* (EVM) dalam lintas sistem operasi sehingga memungkinkan EVM jalan diberbagai sistem operasi.

2.5.2 *Smart Contracts*

Smart Contracts adalah sebuah perjanjian elektronik yang dibuat dalam bahasa pemrograman yang digunakan untuk menjalankan aturan atau klausula yang telah disepakati secara desentralisasi (Muhammad, 2019). Untuk melakukan operasi atau penulisan data kedalam *blockchain* diperlukan *smart contracts*. *Smart Contracts* sendiri disimpan didalam sebuah blok didalam *blockchain*, sehingga kontrak yang sudah dibuat dan disepakati tidak dapat diubah ataupun ditambahkan.

2.5.3 *Consortium Blockchain*

Consortium Blockchain merupakan blockchain yang memiliki proses konsensus yang dikontrol oleh komputer tertentu atau *node* pilihan (Mao et al., 2019). Komputer yang ingin bergabung ke dalam jaringan blockchain

ini perlu mendapat izin atau hak akses menjadi anggota konsensus dalam *blockchain*.

2.5.4 Geth

Geth merupakan *tools* untuk menerapkan dari infrastruktur *ethereum blockchain* yang dibuat dengan bahasa Golang (Go Ethereum, 2019). Dengan menggunakan *Geth*, maka dapat dilakukan pengaturan konsensus sesuai arsitektur pengembangan *blockchain* dalam melakukan proses sinkronisasi data dan *mining* dari setiap operasi data yang akan dituliskan kedalam *blockchain* tersebut serta digunakan untuk membuka *remote control procedure* yang memanggil fungsi yang dibutuhkan untuk melakukan operasi *blockchain* pada suatu *node*.

2.6 Business Process Diagram

Business Process Diagram (BPD) merupakan cara dengan melakukan penggambaran atau melakukan visualisasi terhadap aktivitas atau alur dalam proses bisnis (Romney & Steinbart, 2015). Menggunakan BPD dapat memudahkan memahami alur atau aktivitas yang digunakan dengan cara memilah tanggung jawab didalam proses bisnis.

2.7 Unified Modelling Language (UML)

Unified Modelling Language merupakan bahasa pemodelan umum yang merupakan standar dalam menentukan dan menggambarkan sistem perangkat lunak atau *software* berorientasi objek (Pratama & Hendini, 2019). Dalam pembuatan model sistem menggunakan UML, terdapat 4 jenis diagram yang digunakan, yaitu *Use Case Diagram*, *Activity Diagram*, *Class Diagram*, *Sequence Diagram*.

2.7.1 Use Case Diagram

Use Case Diagram adalah gambaran fungsional dari sebuah sistem yang dikembangkan (Pratama & Hendini, 2019). Dari setiap *use case* yang menyatakan perilaku atau fungsi dari sebuah sistem yang membutuhkan aktor atau pengguna untuk mencapai target atau memenuhi tujuan dari fungsi tersebut.

2.7.2 Activity Diagram

Activity Diagram menggambarkan sebuah proses dalam suatu sistem yang berdasarkan *use case diagram* yang telah dibuat yang memiliki notasi guna memvisualisasikan aktivitas yang sedang berjalan secara bersamaan dan proses pengambilan keputusan yang kompleks (Pratama & Hendini, 2019).

2.7.3 Class Diagram

Class Diagram merupakan sebuah diagram yang mendeskripsikan objek yang ada di dalam sebuah sistem secara statis (Gustriansyah et al., 2019). Dalam sebuah *class diagram* terdapat *system class*, atribut, operasi atau prosedur, serta relasi antar *class*.

2.7.4 Sequence Diagram

Sequence Diagram menggambarkan interaksi objek pada *Use Case* dengan mendeskripsikan waktu hidup objek serta prosedur atau peran yang dikirimkan kemudian diterima oleh antar objek (Pratama & Hendini, 2019). Interaksi antar objek yang digambarkan dapat berupa prosedur atau *method* dalam class yang berhubungan.

2.8 Penelitian Terdahulu

Tabel 2.1. Penelitian Terdahulu

Nama Peneliti	Nama Jurnal	Judul Penelitian	Hasil Penelitian	Kesimpulan
Hang, Lei Kim, Do Hyeun	Sensors (Switzerland), Vol. 19	Design and Implementati on of an Integrated iot <i>blockchain</i> platform for sensing data integrity	Data aktivitas sensor di dalam sistem berbasis <i>Internet of Things</i> (IOT) yang tercatat di dalam <i>blockchain</i> , sesuai dan tidak dapat diubah.	Sistem yang dibuat secara mayoritas menganut arsitektur sentral yang mempunyai risiko tinggi dalam kegagalan

		(Hang & Kim, 2019)	Arsitektur sistem secara <i>decentralized</i> dapat mengatasi permasalahan keamanan data, dan mengurangi kegagalan secara terpusat.	secara terpusat sehingga proses terganggu dan integritas data terancam. Dengan sifat jaringan yang dianut <i>blockchain</i> secara <i>peer to peer</i> , maka dapat mengurangi kegagalan secara terpusat, serta mencegah perubahan terhadap data yang tersimpan
Ade Oktarino	Scientia Journal No. 3, Vol. 4, Page 238-247	Perancangan Sistem Informasi Rekam Medis Pasien Pada Klinik Bersalin Kasih Ibu Menggunakan Metode Waterfall (Oktarino, 2015)	Metode ini berlandaskan sistematis, yang membutuhkan penyelesaian dari tahap tersebut sehingga mencegah terjadinya kegagalan pada proses selanjutnya sehingga menjadi adanya perulangan pada	Menggunakan Metode pengembangan sistem <i>Waterfall</i> membantu penyelesaian tahap demi tahap karena setiap tahapan mempunyai hubungan yang sangat terkait atau krusial guna mencegah

			proses sebelumnya.	kesalahan beruntun.
Obi Ogbanufe, Dam J. Kim	<i>Decision Support Systems</i> , Page 5-25	Comparing Fingerprint-based Biometrics Authentication versus Traditional Authentication Methods for E-payment	Penggunaan <i>Biometric Authentication</i> dalam sistem <i>e-payment</i> menambah tingkat keamanan dan meminimalisir penyalahgunaan kartu kredit dalam bertransaksi serta meningkatkan rasa kepercayaan pengguna terhadap sistem tersebut.	Sistem yang dibuat dengan menggunakan <i>Biometric Authentication</i> dapat meningkatkan keamanan dalam proses autentikasi terhadap pengguna sistem.
Aditiyo Pratikno Ramadhan, Anita Pebri Fitriani, Sugeng Suharto, Titiek Kartika Hendrastiti	Jurnal Sospol, Vol. 4, No. 2, Page 73-83	Electronic Voting in Indonesia: Head of Village Election (Ramadhan et al., 2018)	Dengan mengimplementasi sistem <i>E-Voting</i> , dapat menghemat waktu dan proses dalam pemungutan suara. Dengan penggunaan <i>E-Voting</i> dapat meningkatkan jumlah orang yang berpartisipasi menyuarakan kandidat.	Menggunakan <i>E-Voting</i> , maka proses manual yang memakan waktu dapat di hindari sehingga mempercepat proses, dan memaksimalkan hak suara.