BAB 2

LANDASAN TEORI

2.1 Pemilihan Umum

Pemilihan umum merupakan salah satu sarana penyaluran hak asasi warga negara yang sangat prinsipil, oleh karena itu dalam rangka pelaksanaan hak-hak asasi warga negara merupakan keharusan bagi pemerintah untuk menjamin terlaksananya penyelenggaraan pemilihan umum sesuai dengan Undang-Undang Dasar 1945 (selanjutnya disebut UUD 1945) yang merupakan Konstitusi Negara Republik Indonesia mengatur masalah pemilihan umum terdapat dalam Bab VIIB tentang Pemilihan Umum Pasal 22E sebagai hasil Amandemen ketiga UUD 1945 tahun 2000.

2.2 *Near Field Communication*

Near Field Communication (NFC) adalah teknologi komunikasi wireless yang beroperasi pada frekuensi 13.56MHz yang dapat melakukan perpindahan data antara dua perangkat NFC pada jarak beberapa centimeters dengan kecepatan 424 Kbps.

Protokol NFC mempunyai dua mode komunikasi yaitu mode komunikasi aktif dan mode komunikasi pasif. Pada mode aktif, inisiator dan target saling berkomunikasi dengan menghasilkan radio frekuensi tertentu untuk transmisi. Dua perangkat NFC pada mode aktif dapat menghasilkan medan radio frekuensi untuk membentuk link komunikasi dua arah untuk mentransfer data. Pada mode pasif, perangkat NFC yang beroperasi bertindak sebagai target dan tidak menghasilkan frekuensi sendiri. Sementara yang menjadi perangkat inisiator menghasilkan medan

radio frekuensi untuk komunikasi dan perangkat target menggunakan kopling induktif untuk menangkap atau mengambil radio frekuensi yang telah dihasilkan inisiator. Transfer data terjadi setelah kedua perangkat saling bermodulasi.

Pertukaran data antara perangkat NFC dengan *tag*, diformat menggunakan NFC Data Exchange Format (NDEF). Setiap pesan NDEF (NDEF-Messages) berisi satu atau lebih catatan NDEF (NDEF-Records).

2.3 Flutter

Flutter adalah sebuah SDK (*Software Development Kit*) yang bersifat *open-source* yang dikembangkan oleh Google. Flutter pertama kali diperkenalkan pada tahun 2017, dimana Flutter menggunakan bahasa pemrograman dart. Dengan menggunakan Flutter, maka aplikasi *mobile* yang akan dibangun secara *native* atau *native cross-platform* sehingga aplikasi tersebut dapat dijalankan pada sistem operasi Android dan IOS serta aplikasi tersebut dapat tersedia pada Google Play dan App Store.

2.4 REST API

REST adalah *web service* yang menerapkan konsep perpindahan antar *state* dimana dalam bernavigasi REST melalui link HTTP untuk melakukan aktivitas tertentu. REST menggunakan protokol HTTP yang bersifat *stateless*. Perintah HTTP yang bisa digunakan adalah fungsi GET, POST, PUT, PATCH dan DELETE.

Dalam penerapannya, REST lebih banyak digunakan untuk *web service* yang berorientasi pada *resource*. Maksud orientasi pada sumber daya adalah orientasi yang menyediakan sumber daya sebagai layanannya dan bukan kumpulan-

kumpulan dari aktifitas yang mengolah sumber daya itu. Bentuk *web service* menggunakan REST style sangat cocok digunakan sebagai backend dari aplikasi berbasis mobile karena cara aksesnya yang mudah dan hasil data yang dikirimkan berformat JSON sehingga ukuran *file* menjadi lebih kecil.

2.5 AES (*Advanced Encryption Standard*)

AES (Advanced Encryption Standard) merupakah sebuah teknik kriptografi untuk mengamankan data, AES merupakah lanjutan dari teknik kriptografi DES (Data Encryption Standard). Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128-bit tersebut disebut juga sebagai blok data atau *plaintext* yang nantinya akan dienkripsi menjadi *cipher text*. *Cipher key* dari AES terdiri dari key dengan panjang 128-bit, 192-bit, atau 256-bit. Perbedaan panjang kunci akan mempengaruhi jumlah *round* yang akan diimplementasikan pada algoritma AES ini.

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi *bytes*, yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah disalin ke dalam *state* akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak jumlah putaran. Proses ini dalam algoritma AES disebut sebagai *round function*. *Round* yang terakhir sedikit berbeda dengan *round-round* sebelumnya, dimana pada *round* terakhir, *state* tidak mengalami transformasi *MixColumns*.

2.6 SHA-1

Fungsi hash merupakan sebuah algoritma yang mengubah teks atau pesan menjadi sederetan karakter acak yang memiliki jumlah karakter yang sama. Hash juga termasuk salah satu bentuk teknik kriptografi dan dikategorikan sebagai kriptografi tanpa kunci (*unkeyed cryptosystem*). Hal yang mendasar yang menjadi perbedaan dari fungsi *hash* adalah pesan yang telah acak tidak dapat diubah kembali menjadi pesan yang sebenarnya (*one way function*). Sehingga apabila ada *attacker* yang ingin merubah pesan ditengah jalan, maka nilai hash akan ikut berubah pula dibandingkan dengan nilai *hash* sebelumnya.

SHA dikembangkan oleh National Institute of Standards and Technology (NIST) dan dipublikasikan sebagai Federal Information Processing Standards (FIPS 180) pada tahun 1993. Secure Hash Standard (SHS) menspesifikasikan SHA-1 untuk menghitung nilai *hash* dari sebuah pesan atau *file*. SHA-1 memiliki panjang pesan maksimal 264 bits dan memiliki keluaran sebesar 160 bits yang dinamakan *message digest* atau *hash code*. *Message digest* tersebut dapat digunakan sebagai masukan untuk Digital Signature Algorithm (DSA), yang digunakan untuk menghasilkan *signature* untuk memverifikasi pesan tersebut.