BAB 2

TINJAUAN PUSTAKA

2.1 Landasan Teori

Berikut adalah landasan teori yang digunakan terkait dengan penelitian yang akan dilakukan.

2.1.1 Stasiun Pengisian Kendaraan Listrik Umum (SPKLU)

Stasiun Pengisian Kendaraan Listrik Umum (SPKLU) merupakan sebuah pelayanan umum yang berfungsi untuk melakukan aktivitas pengisian daya pada kendaraan listrik milik konsumen. SPKLU baru - baru ini menjadi tren bagi masyarakat yang mulai menggunakan kendaraan dengan bahan bakar listrik dengan keunggulan dapat mengurangi tingkat pemanasan global yang diakibatkan dari pembakaran bahan bakar fosil.

2.1.2 Kriptografi

Kriptografi adalah ilmu yang mempelajari ilmu untuk memelihara suatu pesan atau data informasi sehingga data tersebut dalam keadaan aman. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat dipahami oleh pihak yang tidak sah. Kriptografi merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi sehingga dapat dikatakan kriptografi adalah ilmu yang mempelajari tentang teknik-teknik yang berkaitan dengan keamanan informasi seperti kerahasiaan, integritas data, autentikasi, dan ketiadaan penyangkalan. Ada dua istilah utama yang digunakan dalam kriptografi yaitu enkripsi dan dekripsi. Enkripsi adalah proses untuk mengubah teks biasa menjadi teks yang berbentuk sandi dan dekripsi adalah proses untuk mengubah teks yang berbentuk sandi menjadi teks biasa. Kriptografi digunakan untuk menyimpan dan mentransmisikan data agar hanya pihak pengirim dan penerima yang dapat memahami atau

memprosesnya sehingga seorang penyusup tidak dapat mengakses atau memahami data tersebut [7], [8], [9].

2.1.3 Kriptografi Simetris

Kriptografi simetris adalah kriptografi dengan penggunaan kunci yang sama untuk digunakan pada proses enkripsi dan dekripsi. Pengirim melakukan proses enkripsi data dengan menggunakan kunci yang aman dan sama digunakan oleh penerima untuk mendekripsi data. Ada banyak algoritma yang didasarkan pada kriptografi kunci simetris, seperti caesar cipher, block cipher contohnya adalah DES dan AES, stream cipher contohnya adalah RC4 dan A5 [7], [8].

2.1.4 Algoritma *Advanced Encryption Standard* (AES)

AES merupakan algoritma kriptografi jenis simetri yang dimana menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, kemudian dapat diimplementasikan dalam teknik tunggal atau gabungan seperti dengan steganografi atau kompresi data [5].

AES menggunakan sistem *cipherblock* dengan spesifikasi panjang blok yang digunakan adalah 128-bit, operasi AES dilakukan dengan satuan penyimpanan data yaitu *byte*/bita [1].

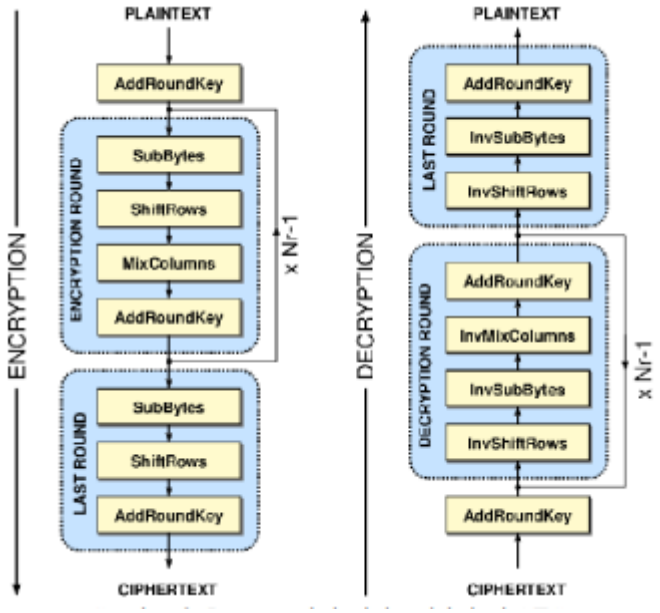
AES juga dikenal sebagai pengganti dari algoritma DES sehingga AES memiliki tingkat keamanan yang lebih baik, akurat dan mudah diimplementasikan, selain itu dikatakan juga bahwa AES dianggap lebih efektif untuk mengamankan transmisi pesan dibandingkan algoritma yang lainnya seperti *Rivest-Shamir-Adleman* (RSA), DES, *Triple Data Encryption Standard* (3DES) [10].

Ukuran kunci yang digunakan pada AES mulai dari 128-bit, 192-bit, dan 256-bit dengan jumlah putaran pada proses AES dipengaruhi dengan panjang kunci yang dipilih, yaitu mulai dari 10, 12, dan 14 [5].

AES Version	Key Length (Nk Words)	Block Size (Nb Words)	Number of Rounds (Nb)
AES – 128	4	4	10
AES – 192	6	4	12
AES – 256	8	4	14

Gambar 2. 1. Panjang kunci dan jumlah putaran yang dilakukan pada AES [5].

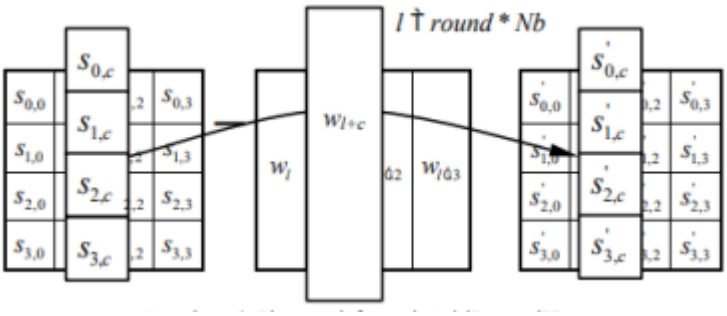
Pada proses algoritma AES ini terdapat 4 fungsi utama yaitu: SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Pada awal proses enkripsi, *plaintext* akan dilakukan perubahan nilai kedalam *Byte* pada fungsi *AddRoundKey*. Kemudian, *state* dilakukan proses subtitusi nilai pada fungsi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulangkali (proses Nr). Pada algoritma AES terdapat *round* function atau fungsi putaran inilah yang akan melakukan perulangan fungsi utama dari algortima AES sesuai dengan ketentuan dari awal jika panjang kunci yang digunakan adalah 128 bit maka perulangan akan dilakukan sebanyak 10 kali namun dikurangi 1 atau secara matematis menjadi N-1, kemudian pada bagian terakhir fungsi MixColumns tidak digunakan [4].



Gambar 2. 2. Gambaran umum proses enkripsi dan dekripsi AES [4].

AddRoundKey

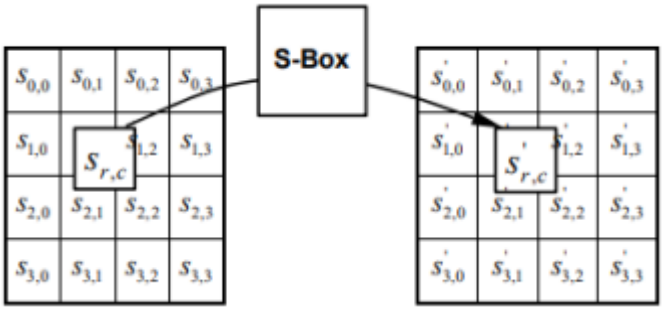
Pada setiap putaran pada proses AES, 16 *Byte round key* berasal dari kunci master yang diinterpretasikan menjadi *array Byte* 4 × 4. Kemudian, *array* kunci di XOR-kan dengan *array state*. Dinotasikan sebagai $a\ (i, j)$, sehingga menjadi baris i dan kolom j pada array state, sama halnya dengan array kunci yang dinotasikan sebagai $k\ (i, j)$. *AddRoundKey* dapat dinyatakan sebagai transformasi dari $a\ (i, j) = a\ (i, j) \oplus k\ (i, j)$ untuk setiap $1 \leq i \leq 4$ dan $1 \leq j \leq 4$ pada proses komputasi. Proses tersebut diilustrasikan pada gambar 2.3 [4].



Gambar 2. 3. Ilustrasi proses AddRoundKey pada AES [4].

SubBytes

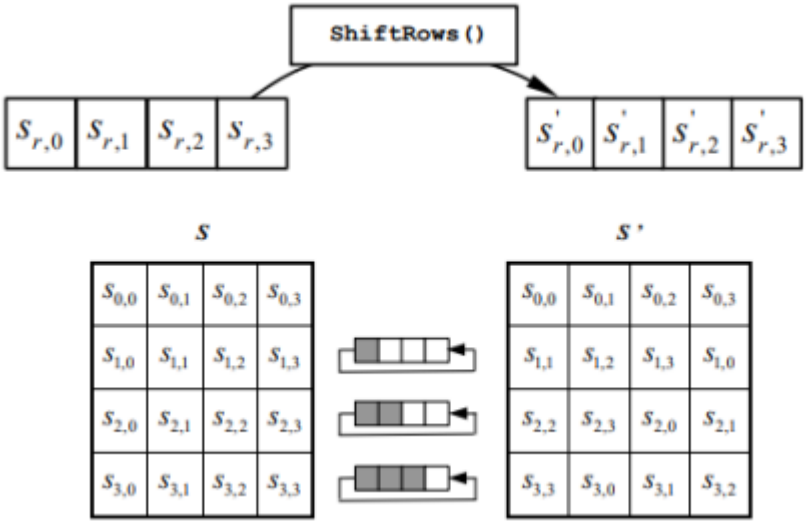
Setiap *Byte* pada *array state* diubah dengan setiap *Byte* dengan melakukan mapping pada *S-Box*. Seperti ditunjukkan pada Gambar 5, Tahap *SubBytes* dikomputasikan sebagai $ai, j = S\ (ai, j)$ untuk setiap $t1 \leq i \leq 4$ dan $1 \leq j \leq 4$ [13]. Proses ini hanya menggunakan satu *S-box* untuk mensubstitusi semua *Byte* dari *array state* [4].



Gambar 2. 4. Ilustrasi proses SubBytes pada AES [4].

ShiftRows

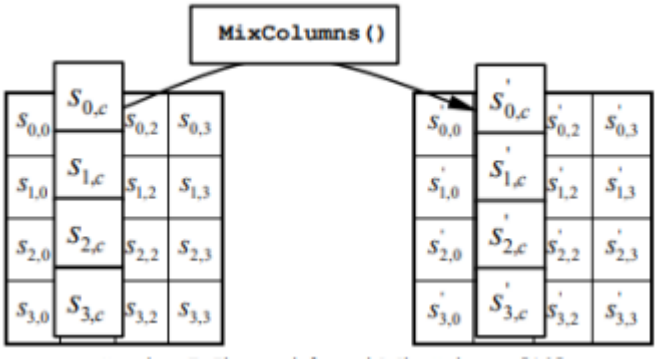
Pada gambar 2.5, proses *ShiftRows* merupakan proses tranformasi untuk mengeser baris dari suatu *state* matriks berdasarkan suatu pola (ke kiri atau ke kanan) dan nilai *offset*. *Byte* dari setiap baris dari *array state* digeser secara siklis ke kiri. Baris pertama dari *array* tidak digeser, baris ke-dua digeser satu tempat ke kiri, baris ke-tiga digeser dua tempat ke kiri, dan baris keempat digeser tiga tempat ke kiri. Sehingga *ShiftRows* dapat dinotasikan sebagai *Byte* a (2, 1) menjadi a (2, 4), *Byte* a (2, 2) menjadi a (2, 1) dan seterusnya [4].



Gambar 2. 5. Ilustrasi proses ShiftRows pada AES [4].

MixColumns

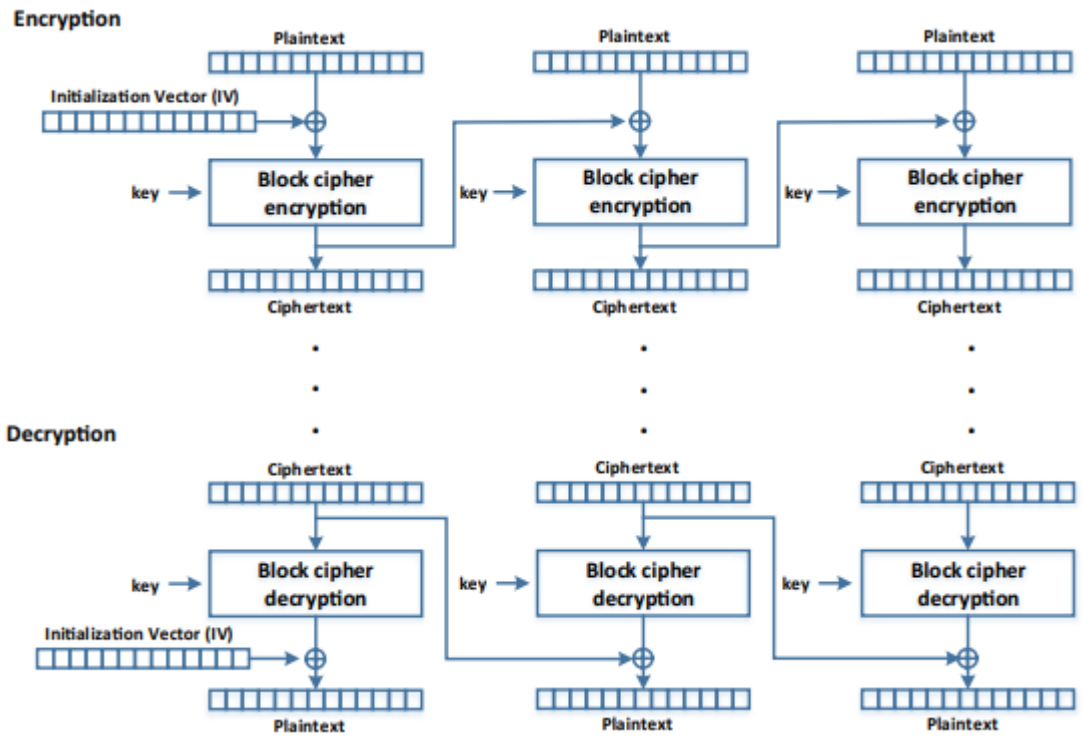
Pada gambar 2.6, diilustrasikan setiap kolom dicampur dari setiap transformasi linear yang telah terjadi pada *SubBytes* dan *ShiftRows*. Langkah ini bertujuan untuk menggantikan setiap Byte pada tiap kolom dengan fungsi dari semua *Byte* dalam kolom yang sama [4].



Gambar 2. 6. Ilustrasi proses MixColumns pada AES [4].

2.1.5 Mode CBC

CBC merupakan salah satu mode operasi block cipher yang menggunakan *initialitation vector* (IV) dengan ukuran yang sama dengan satu blok plain text. proses enkripsi dan dekripsi dilakukan berdasarkan operasi XOR antara blok plain dengan cipher sebelumnya [1]. Salah satu ciri utama dari CBC adalah setiap blokcipher selalu bergantung pada blok-blok sebelumnya. Proses enkripsi yang pertama memerlukan cipher awal yang diwakili oleh sebuah blok biner yang ditentukan sendiri dan disebut dengan istilah IV atau sering disebut cipher awal (C0) dimana Jumlah bit (C0) harus sama dengan jumlah bit kunci [11].



Gambar 2. 7. Ilustrasi Proses AES menggunakan mode CBC [12].

Seperti yang diilustrasikan pada Gambar 2.7, Vektor Inisialisasi IV digunakan di blok pertama, dari proses enkripsi, IV menggunakan fungsi logika OR eksklusif dengan blok plainteks pertama. Hasilnya dienkripsi dan blok ciphertext pertama dihasilkan. Kemudian, setiap blok plainteks adalah hasil XOR dengan output ciphertext dari tahap sebelumnya. Begitupun proses dekripsi, blok ciphertext menggunakan fungsi XOR dengan blok tahap sebelumnya, dan plainteks yang dihasilkan. Dalam hal ini, IV hanya digunakan sekali pada awal proses dekripsi, menggunakan operasi XOR, dengan blok dekripsi pertama yang dihasilkan dari blok ciphertext pertama, karena tidak ada tahap sebelumnya [12].

2.1.6 Internet of Things

Internet of things adalah sebuah teknologi yang memanfaatkan penggunaan internet yang bertujuan untuk menyediakan konektivitas antara benda mati agar dapat memberikan sebuah informasi dan memberikan keputusan berupa aksi yang difungsikan pada sebuah aktuator [13].

2.2 Literatur Review

Literatur review dilakukan untuk mengetahui penelitian-penelitian sebelumnya yang sudah dilakukan.

2.2.1 Pentingnya sebuah keamanan pada perangkat IoT

Berdasarkan hasil penelitian yang dilakukan [14] disebutkan bahwa pentingnya sebuah keamanan data yang kini menjadi pondasi dalam sistem infomasi terutama untuk melakukan analisis data yang dikumpulkan menggunakan teknologi *internet of things*, dan ancaman-ancaman yang terjadi pada internet of things menjadi sebuah penghambat keberlangsungan data yang akan digunakan untuk analisis. Kemudian penelitian yang dilakukan [3] disebutkan bahwa banyak sekali celah keamanan yang bisa diserang oleh penyerang untuk mendapatkan data yang dihasilkan dari *internet of things* dengan motivasi apapun, sehingga pentingnya menjaga sebuah keamanan dari segi layer-layer yang digunakan pada *internet of things* guna penyalahgunaan data yang diambil dengan tidak bertanggungjawab. Sehingga dengan melakukan sebuah pengamanan data perangkat IoT baik itu ketika sedang melakukan transmisi data ke server menjadi sebuah pilihan agar data yang dikirimkan perangkat dalam keadaan aman dan tidak mengganggu proses analisis yang dilakukan sebuah sistem yang mendapatkan data tersebut.

Pada penelitian [3] juga menjelaskan dengan terlihatnya data yang ditransmisikan oleh perangkat IoT menimbulkan tindak penyalahgunaan informasi, salah satunya seperti yang diceritakan pada penelitian tersebut adalah menghasilkan informasi banyaknya penghuni rumah hasil dari data aktivitas konsumsi daya listrik yang ditransmisikan perangkat IoT. Hal ini bisa menimbulkan motivasi untuk melakukan tindak kejahatan hanya berdasar dari banyaknya penghuni rumah tersebut.

Menurut penelitian Zeadally, dkk [15] menjelaskan bahwa pada perangkat IoT masih banyak beberapa aspek yang harus diperhatikan, salah satunya adalah mengenai segi keamanan yang dimana perangkat IoT ini banyak sekali

dijumpai menggunakan jaringan internet publik, sehingga memungkinkan terjadinya penyerangan yang mengakibatkan terganggunya sistem yang sudah berjalan. Kriptografi menjadi salah satu solusi yang dapat diterapkan pada perangkat IoT, mengingat dengan menggunakan teknik ini bisa memberikan beberapa keunggulan, yaitu kerahasiaan data, integritas data, otentikasi pesan, manajemen kunci, dan tanda tangan digital.

2.2.2 Penerapan algoritma AES pada perangkat IoT

Pemilihan pengamanan data yang tepat menjadi sebuah pilihan yang yang digunakan untuk perangkat IoT karena pada penelitian [1], [2], [4]–[6], [10] menjelaskan bahwa pentingnya melihat sumber daya pada perangkat menjadi pertimbangan untuk menerapkan sebuah kriptografi dikarenakan prosesnya memakan sumber daya perangkat sehingga dengan digunakannya, algoritma AES sebagai kriptografi yang digunakan karena terbukti cocok dan efisien dalam penggunaan sumber daya perangkat IoT.

Pada penelitian [5] menerapkan mekanisme enkripsi data hanya pada saat data tersebut ditransmisikan ke perangkat android untuk ditampilkan pada pengguna, sehingga proses dekripsi dilakukan pada perangkat android untuk menampilkan data sesungguhnya pada pengguna.

Pada penelitian [1], [10] mekanisme yang diterapkan adalah menggunakan algoritma AES dengan menambahkan mode CBC dan base64. Kemudian enkripsi diterapkan pada saat sebelum transmisi data dari perangkat IoT dilakukan. Sehingga pada saat ditransmisikan, data dalam keadaan terenkripsi. Data yang ditransmisikan terdapat dua data yaitu IV dan data. Namun key dari IV dan data masih terlihat pada saat ditransmisikan.

Berbeda dengan penelitian [4] menggunakan algoritma AES dengan mode ECB sehingga tidak menggunakan operasi tambahan seperti yang dilakukan pada mode CBC menggunakan IV. Sehingga data yang ditransmisikan tidak mengandung IV.

Pada penelitian [6] menerapkan mekanisme enkripsi serupa dengan penelitian [1], [10] hanya saja terlihat bahwa pada saat server menerima data yang ditransmisikan perangkat IoT, sebelum disimpan pada basis data dilakukan dekripsi terlebih dahulu sehingga data yang masuk pada basis data sudah dalam bentuk data yang sesungguhnya.