

## BAB III METODOLOGI PENELITIAN

### 3.1 Alat dan Bahan

#### 3.1.1 Alat

Sebelum mengimplementasikan perangkat IoT yaitu sensor pendeteksi suhu dan kelembaban, ada beberapa peralatan yang harus disiapkan. Daftar peralatan yang digunakan ada pada tabel 3.1 sebagai berikut:

**Tabel 3.1 Tabel Alat**

No	Nama Alat	Jenis/Spesifikasi	Fungsi	Jumlah
1	Komputer / Laptop	Windows 10 / Ubuntu 20.04	Untuk memprogram NodeMcu dan membuat aplikasi web	1 unit
2	Multitester	Analog / Digital	Untuk mengukur tegangan dan arus	1 unit
3	Pemotong Kabel	Cutter / Gunting	Untuk memotong kabel atau kaki komponen	1 buah

#### 3.1.2 Bahan

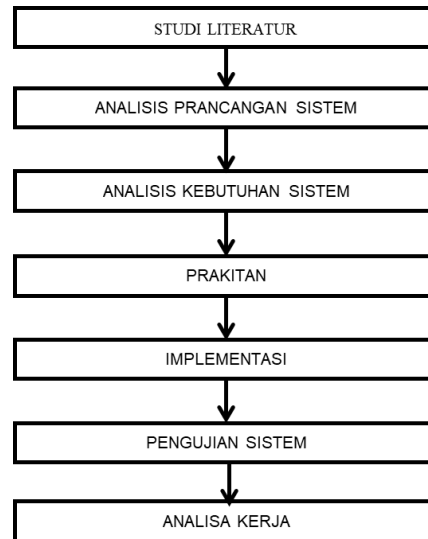
Sebelum mengimplementasikan perangkat IoT yaitu sensor pendeteksi suhu dan kelembaban, ada beberapa komponen yang harus disiapkan. Daftar komponen yang digunakan dalam penelitian dapat dilihat pada tabel 3.2:

**Tabel 3.2 Tabel Bahan**

No	Nama	Fungsi	Jumlah
1	NodeMCU	Memproses data yang dibaca oleh sensor dan mengirimkannya ke web server	1 unit
2	DHT11	Mengukur suhu dan kelembaban yang dibutuhkan oleh mikrokontroler untuk diproses	1 unit
3	Power Bank	Sebagai sumber tegangan yang digunakan node sensor	1 unit
4	Kabel	Untuk menghubungkan sensor dan mikrokontroler	8 buah

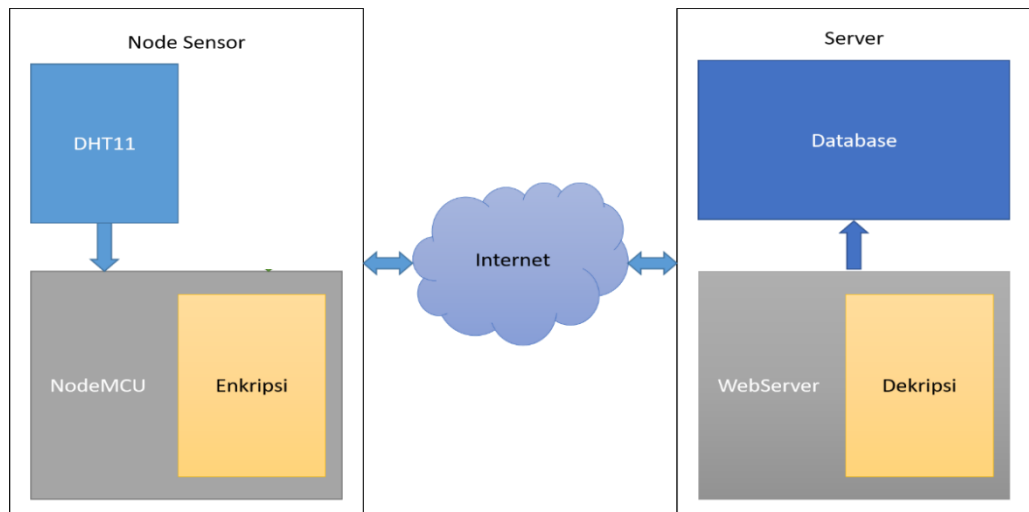
### 3.2 Tahapan Penelitian

Metode penelitian ini akan menjelaskan langkah – langkah penelitian yang akan dilakukan dalam membangun Keamanan Data Internet of Things (IoT) dalam lingkup *Smart Home* menggunakan algoritma Rivest Code 4. Berikut alur penelitian yang digunakan :



### 3.3 Perancangan Sistem

Perancangan sistem merupakan suatu hal yang dilakukan untuk mempermudah proses pembuatan alat. Konsep tersebut digambarkan pada diagram blok yang menjelaskan gambaran umum mengenai cara kerja dari sistem. Secara umum sistem digambarkan sebagai berikut :

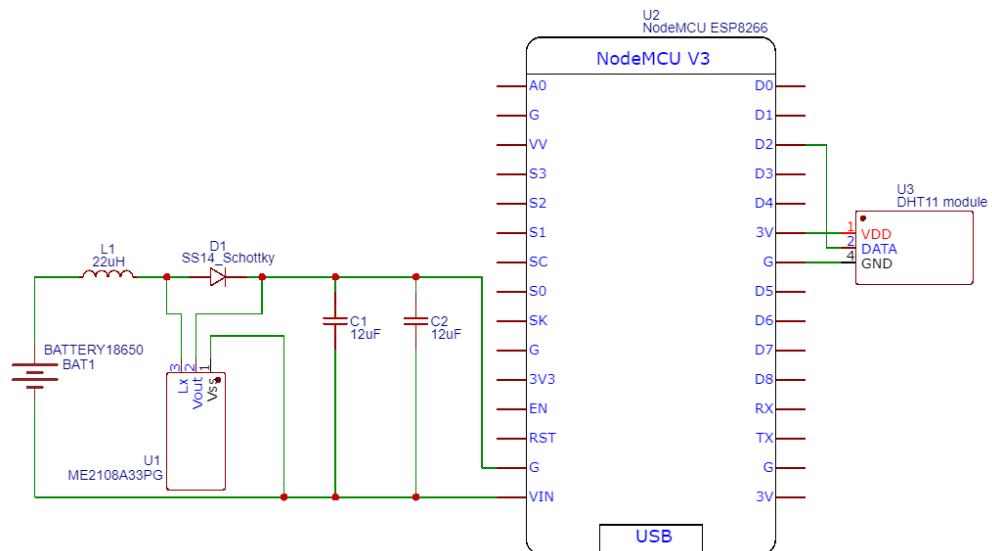


**Gambar 3.1 Blok Diagram Sistem**

Dari gambar diatas dapat diketahui data sensor didapatkan menggunakan sensor DHT11 untuk mengukur suhu dan kelembaban. Kemudian data tersebut diproses berupa plaintext dan dienkripsi menggunakan NodeMCU menjadi chipertext dengan metode Rivest Code 4 lalu dikirim ke web server melalui internet. Data yang diperoleh web server kemudian di dekripsi menjadi plaintext kembali dan disimpan pada database web server.

### 3.3.1 Rancangan Node Sensor

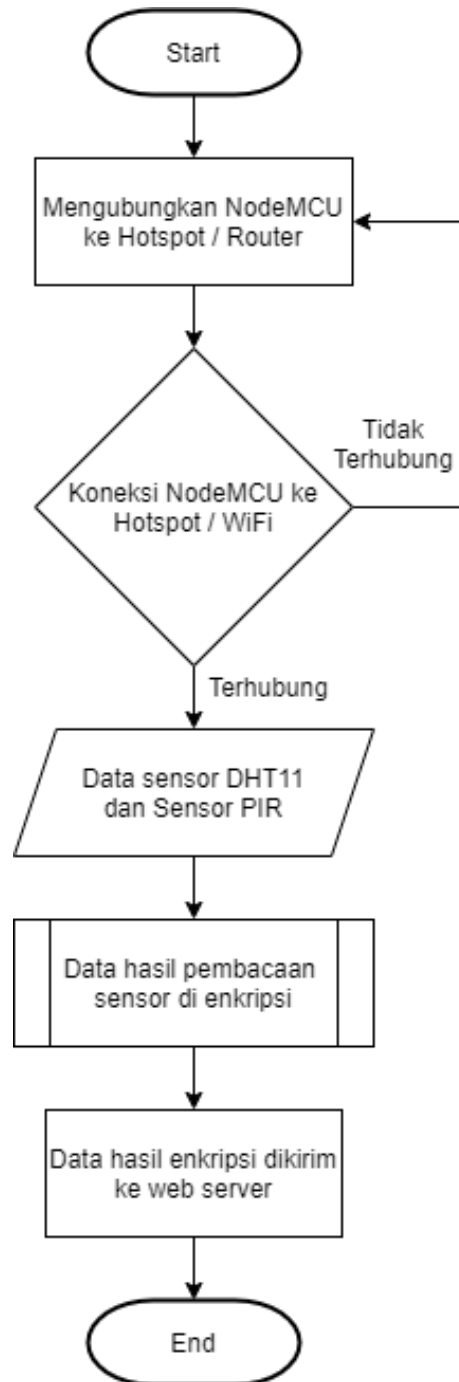
Rangkaian node sensor digunakan untuk mengambil data suhu, kelembaban, dan gerakan. Data sensor tersebut kemudian di enkripsi sebelum dikirim ke web server. Rancangan node sensor yang digunakan adalah sebagai berikut :



**Gambar 3.2 Skematik Diagram Node Sensor**

### 3.3.2 Diagram Alir Node Sensor

Node sensor bertugas sebagai unit pemroses data dari hasil pembacaan sensor dan mengirimkan data tersebut ke web server. Data yang akan dikirimkan ke web server akan di enkripsi terlebih dahulu untuk menjaga kerahasiaan data. Enkripsi digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Dengan demikian informasi hanya akan dapat diakses oleh pihak – pihak yang berhak saja. Proses tersebut di jelaskan pada diagram alir dibawah ini :

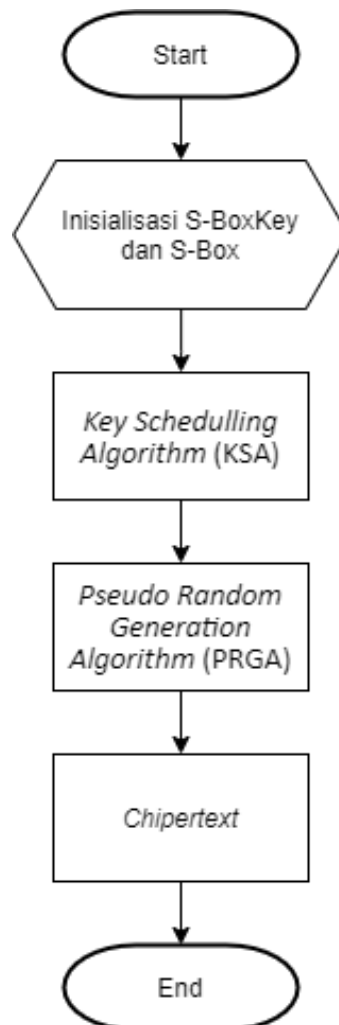


**Gambar 3.3 Diagram Alir Program Node Sensor**

### 3.3.3 Diagram Alir Enkripsi

Proses enkripsi dimulai dengan membuat variabel array S-BoxKey dan S-Box dengan panjang 256 sebagai kotak substitusi. Selanjutnya melakukan *Key Scheduling Algorithm* (KSA) dengan melakukan inisialisasi S-Box yang berisi permutasi dari bilangan 0 sampai 255. S-BoxKey berisi kunci untuk melakukan

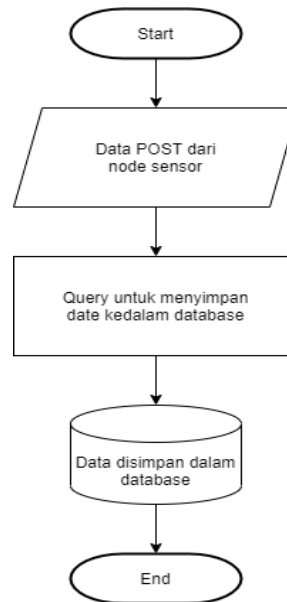
enkripsi. Isi array S-BoxKey dengan kunci yang diulangi sampai seluruh array terisi seluruhnya. Tahap selanjutnya adalah *Pseudo Random Generation Algorithm* (PRGA). Pada tahapan PRGA akan dihasilkan nilai pesuodorandom yang akan dikenakan operasi XOR dengan *plaintext* untuk menghasilkan *ciphertext*. Proses diatas dapat di lihat pada diagram alir dibawah ini :



**Gambar 3.4 Diagram Alir Enkripsi**

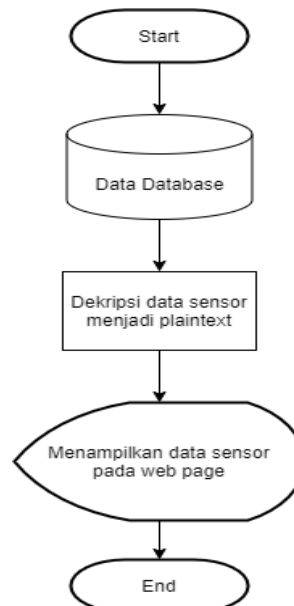
### 3.3.4 Diagram Alir Web Server

Terdapat dua skema diagram alir pada web server. Pertama data yang diterima dari node sensor disimpan dalam database. Proses tersebut dapat dilihat pada diagram alir dibawah ini :



**Gambar 3.5 Diagram Alir Menyimpan Data ke Database**

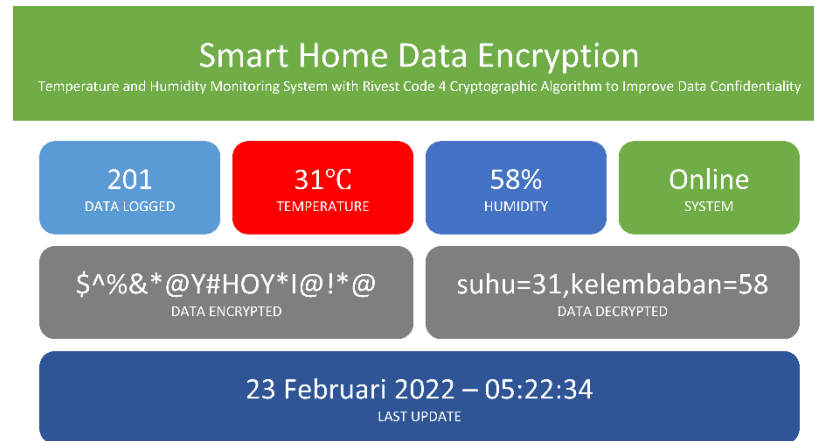
Proses selanjutnya adalah melakukan dekripsi data yang ada di database yang akan ditampilkan pada web page. Proses tersebut dapat dilihat pada diagram alir dibawah ini :



**Gambar 3.6 Diagram Alir Menampilkan Data ke Web Page**

### 3.3.5 Desain Antarmuka Web Server

Antarmuka web server menampilkan hasil dari pembacaan sensor yang dikirimkan oleh sensor node. Berikut desain antarmuka web server yang akan di buat :



**Gambar 3.7 Antarmuka Web Server**

### 3.4 Metode Pengujian sistem

Pengujian ditujukan untuk mengetahui kemampuan sistem dalam melakukan kriptografi. Data yang digunakan merupakan data sensor pada node sensor dan data yang disimpan dalam database pada sisi web server. Pada penelitian ini, pengujian dilakukan dengan menguji performa algoritma dan pengujian black box. Pengujian yang akan dilakukan adalah sebagai berikut :

1. Menghitung waktu yang dibutuhkan untuk melakukan enkripsi dan dekripsi. Uji coba dilakukan menggunakan 3 kunci yang berbeda untuk mengetahui apakah panjang kunci berpengaruh secara signifikan terhadap waktu enkripsi maupun dekripsi.
2. Melakukan *packet sniffing* untuk mengetahui bentuk data yang dikirim node sensor ke webserver.
3. Menyandingkan performa sistem dengan kriptografi dan sistem tanpa kriptografi.
4. *Black box testing* untuk memastikan sistem secara konsisten menghasilkan data yang valid dalam 15 percobaan.