IMPLEMENTASI ENKRIPSI *PAYLOAD* PADA PROTOKOL LoRaWAN MENGGUNAKAN ALGORITME SPECK 64/128 BIT

PROPOSAL SKRIPSI

Disusun oleh:
Nama : Dian Astika Rini
NIM : 155150200111136

PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
TAHUN

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1 PENDAHULUAN

1.1 Latar Belakang

IoT (Internet of Things) mendapatkan popularitas tinggi di dunia saat ini. Sistem tertanam ini telah menjadi bagian utama dari kehidupan kita. Setiap orang kini dapat mengontrol, memantau, dan melakukan lebih banyak hal dari jarak yang jauh. Hal ini dilakukan dengan cara menghubungkan berbagai benda mengurangi jarak fisik. IoT (Internet of Things) adalah konektivitas dari berbagai objek dengan menggunakan konektivitas jaringan. Sistem ini dioperasikan dengan menggunakan baterai dan memerlukan cadangan baterai yang tinggi. Sistem ini membutuhkan teknologi yang mengkonsumsi daya lebih sedikit dan juga mencakup jarak yang jauh. Tetapi banyak teknologi seperti Zig-Bee, Wi-Fi, Bluetooth yang populer digunakan saat ini mengkonsumsi daya tinggi dan tidak cocok untuk sistem yang dioperasikan dengan baterai. Teknologi yang menjawab kebutuhan perangkat tertanam yang dioperasikan dengan baterai ini adalah Teknologi LoRa yang merupakan teknologi rendah dengan daya yang panjang (Devalal and Karthikeyan, 2018).

LoRa (Long Range) adalah termasuk pada konektivitas IoT (Internet of Things) nirkabel terbaru yang yang sedang bevolusi dan mendapatkan popularitas dalam sistem tertanam yang dioperasikan dengan daya rendah yang perlu mentransfer sejumlah kecil data pada interval pendek dalam jarak jauh. Sementara keamanan koneksi yang telah disadari oleh banyak orang namun hanya berfokus pada keamanan gateway dan IP device ke Internet dan keamanan antara gateway dan end device cenderung diabaikan. (Semiconductors, 2018). LoRa memiliki jaringan yaitu jaringan LoRaWAN (Long Range Network Protokol). Jaringan LoRaWAN (Long Range Network Protocol) bertipe Low Power Wide Area Network (LPWAN) dan mencakup perangkat bertenaga baterai yang memastikan komunikasi dua arah (Lavric and Popa, 2017) . Sehingga, diperlukan upaya untuk mengamankan koneksi yang digunakan oleh klien dan server dalam melakukan komunikasinya. Upaya yang dilakukan mencangkup confidentiality, integrity, dan availability yang merupakan konsep keamanan. Dalam hal ini akan ditekankan pada confidentiality. Pada konsep confidentiality ini akan dilakukan enkripsi pada data atau pesan yang akan dikirimkan baik dari server maupun dari klien. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. atau bisa didefinisikan juga enkripsi, merupakan proses untuk mengubah plainteks menjadi chiperteks. Plainteks sendiri adalah data atau pesan asli yang ingin dikirim, sedangkan chiperteks adalah data hasil enkripsi. Definisi lain tentang enkripsi adalah proses mengacak data sehingga tidak dapat dibaca oleh pihak lain. (Purba, 2017)

Algoritme yang digunakan adalah algoritme SPECK 64/128 bit. SPECK 64/128 bit adalah keluarga blokcipher ringan yang di rilis oleh Badan Keamanan Nasional A.S. pada tahun 2013. Keluarga SPECK 64/128 bit terdiri dari 10 versi, mendukung berbagai ukuran blok dan kunci. Metode keamanan tersebut dapat diterapkan

pada pesan yang dibawa Payload. Pada penelitian ini, akan digunakan algoritma SPECK 64/128 bit untuk enkripsi pesan yang ditransmisikan (Mohanty and Mohanty, 2014). Berdasarkan penelitian yang telah dilakukan, SPECK 64/128 bit akan berjalan dengan optimal pada processor 64 bit. Selain itu juga waktu pencarian pada SPECK 64 membutuhkan waktu yang cukup sedikit dibandingkan dengan versi SPECK yang lainnya (Song, Huang and Yang, 2016).

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas dapat dirumuskan permasalahan yang akan diselesaikan dalam penelitian ini :

1. Bagaimana hasil implementasi enkripsi *payload* pada protokol LoRaWAN menggunakan algoritme Speck 64/128 bit?
2. Bagaimana mekanisme algoritme Speck 64/128 bit pada proses enkripsi *payload* pada protokol LoRaWAN?

1.3 Tujuan

Tujuan dari penelitian ini adalah :

1. Mengetahui hasil implementasi enkripsi *payload* pada protocol LoRaWAN menggunakan algoritme Speck 64/128 bit
2. Mengetahui mekanisme algoritme Speck 64/128 bit pada proses enkripsi *payload* pada protocol LoRaWAN.

1.4 Manfaat

Manfaat dari penelitian ini adalah :

1. Meningkatkan keamanan dalam komunikasi antara gateway (server) dan end device
2. Memberikan mekanisme untuk mengamankan komunikasi pada protokol LoRaWAN menggunakan algoritme Speck 64/128bit
3. Membantu penulis dalam memahami mengenai teknologi LoRa pada IoT *(Internet of Things)*

1.5 Batasan Masalah

Berdasarkan pada latar belakang diatas didapatkan batasan masalah sebagai berikut :

1. Hanya melakukan proses enkripsi pada *payload*
2. Penggunaan algortime Speck hanya pada versi 64/128 bit
3. Pengimplementasian enkripsi pada protokol LoRaWAN
4. Pengimplementasian algoritme Speck 64/128bit menggunakan Bahasa C++

1.6 Sistematika Pembahasan

Sistematika susunan laporan penelitian ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini menjelaskan tentang pendahuluan yang meliputi latas belakang permasalahan, rumusan masalah, batasan masalah, tujuan, manfaat dan sistematika penulisan pada tugas akhir ini.

BAB II LANDASAN KEPUSTAKAAN

Bab ini menjelaskan teori-teori pemecah masalah yang digunakan sebagai pendukung segala sesuatu yang berhubungan dengan topik penelitian ini.

BAB III METODOLOGI

Bab ini menjelaskan mengenai rancang sistem dan juga alur yang akan menunjang keberhasilan peneilitan ini dan agar dapat diimplementasikan di dalam sistem yang sesuai harapan mengacu pada teori-teori penunjang dan metode yang sudah dijelaskan pada bab sebelumnya.

BAB IV PERANCANGAN

Bab ini berisi tentang perancangan algoritme, Perancangan sistem, perancangan algoritme Speck 64/128bit pada protokol LoRaWAN.

BAB V IMPLEMENTASI

Bab ini berisi tentang pengujian pada sistem yang telah dirancang untuk mengetahui bahwa sistem dapat dijalankan sesuai dengan spesifikasi, perancangan, dan tujuan.

BAB VI PENGUJIAN

Bab ini berisi tentang pengujian algoritme Speck 64/128bit untuk proses enkripsi yang dilakukan pada protokol LoRaWAN.

BAB VII PENUTUP

Bab ini menjelaskan tentang kesimpulan yang diambil berdasarkan tahapan-tahapan yang sudah dilakukan mulai dari perancangan, implementasi, pengujian. Pada kesimpulan juga menjawab pertanyaan-pertanyaan pada rumusan masalah dan menyebutkan saran untuk penelitian selanjutnya.

BAB 2 LANDASAN KEPUSTAKAAN

2.1 Kajian Pustaka

Terdapat beberapa penelitian yang berkaitan dengan penelitian yang akan dilakukan oleh penulis. Pada beberapa penelitian yang ada, dengan judul "*Implementasi Algoritme Speck untuk Enkripsi dan Dekripsi pada QR Code"* menjelaskan algoritme Speck dapat digunakan untuk melakukan enkripsi pada sebuah *plaintext* dan menghasilkan sebuah *chipertext* sebagai metode untuk pengamanan dalam hal ini adalah pesan yang dihasilkan tersebut. Kemudian LoRaWan merupakan suatu protokol yang berasal dari teknologi terbaru bernama LoRa yang cocok untuk diterapkan pada *IoT (Internet of Things),* seperti pada penelitian yang dilakukan oleh perusahaan bernama NXP Semiconductor yang berjudul *"IoT Device Secure Connection with LoRa"* menjelaskan bahwa LoRa memiliki protokol yaitu LoRaWAN. Pada penelitian tersebut dijelaskan LoRa terdiri dari beberapa layer. Layer yang dapat diimplementasikan untuk proses enkripsi pada layer aplikasi (*Aplication Layer Data Encryption).*

2.2 Dasar Teori

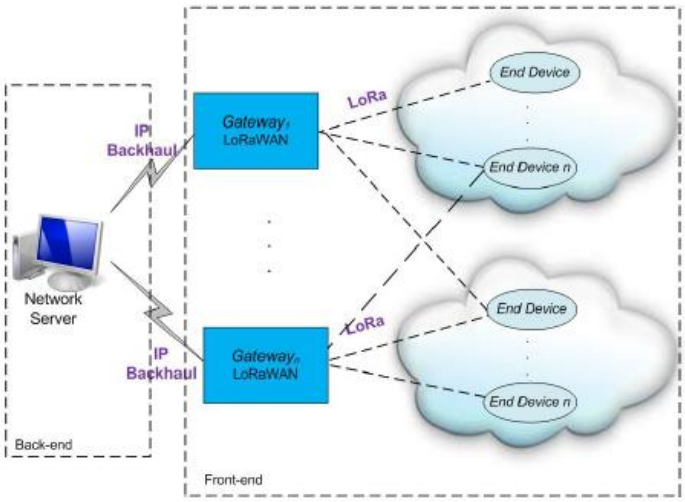
2.2.1 *Internet of Things*

IoT (Internet of Things) adalah konektivitas dari berbagai objek dengan menggunakan konektivitas jaringan (Devalal and Karthikeyan, 2018). IoT melibatkan beberapa miliar perangkat beragam yang saling terhubung pada sejumlah besar data yang cepat muncul atau serbaguna (yaitu, "*Big Data*"), dan berbagai layanan. Perangkat yang terhubung dapat berupa sensor, aktuator, ponsel pintar, komputer, bangunan dan peralatan rumah, mobil, elemen infrastruktur jalan, dan perangkat atau objek lain apa pun yang dapat dihubungkan, dipantau, atau digerakkan. Perangkat terhubung ke Internet, dpat berkomunikasi satu sama lain, melalui jaringan akses heterogen. Layanan bertujuan mengarah pada masyarakat dan ekonomi yang cerdas, berkelanjutan, dan inklusif. Dalam terang masalah yang dibahas, keberhasilan layanan IoT hanya dapat dicapai jika dikaitkan dengan aksesibilitas di mana-mana (yaitu, lebih banyak peluang bisnis), keandalan (misalnya, untuk menangani perubahan konteks atau kebijakan dan mencapai kepercayaan dari bagian-bagian dari pengguna), kinerja tinggi (misalnya, karena "data besar" yang terkait), efisiensi (untuk meningkatkan posisi semua pemangku kepentingan, misalnya penyedia dan pengguna), dan skalabilitas (misalnya, karena berbagai volume pengguna, sumber daya, dan data dapat terlibat dalam penyediaan layanan) (Biswas and Giaffreda, 2014).

2.2.2 LoRaWAN

Protokol LoRaWAN relatif baru dan menjadi fokus beberapa pusat penelitian di seluruh dunia. LoRa (Long Range) adalah teknik modulasi yang memungkinkan transfer informasi jarak jauh dengan kecepatan transfer rendah. Modulasi LoRa telah dipatenkan oleh Semtech Corporation.

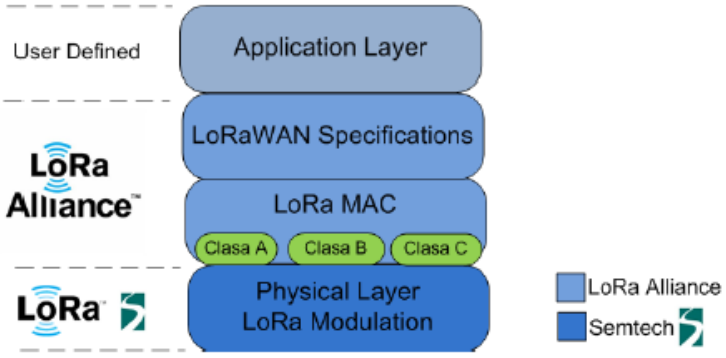
LoRa adalah jenis modulasi Spektrum SS-Spread, dan teknik ini terdiri dari penggunaan sinyal yang bervariasi secara konstan dengan frekuensi. Keuntungan menggunakan metode ini adalah bahwa waktu dan frekuensi *offset* ke pengirim dan penerima adalah sama, sehingga sangat mengurangi kompleksitas penerima. Gambar 2.1 merupakan gambar asitektur LoRa.



Gambar 2.1 Arsitektur LoRa

Jaringan LoRaWAN (Long Range Network Protocol) bertipe Low Power Wide Area Network (LPWAN) dan mencakup perangkat bertenaga baterai yang memastikan komunikasi dua arah. Spesifikasi LoRaWAN memastikan interoperabilitas yang sempurna antara objek IoT, tanpa perlu implementasi lokal yang kompleks.

Jaringan LoRa diimplementasikan dengan menggunakan topologi jaringan bintang. Struktur arsitektur LoRa dapat dipisahkan menjadi bagian back-end dan front-end. Bagian back-end terdiri dari server jaringan yang menyimpan informasi yang diterima dari sensor. Front-end terdiri dari modul Gateway dan node perangkat akhir. Modul Gateway bertindak sebagai jembatan antara node perangkat akhir dan server jaringan. Informasi antara server jaringan dan modul Gateway dikirim melalui koneksi IP (Lavric and Popa, 2017). Gambar 2.2 menggambarkan ilustrasi komunikasi protokol LoRaWAN.



Gambar 2.2 Arsitektur Komunikasi Protokol LoRaWAN

2.2.3 Kriptografi

Kriptografi merupakan ilmu yang mempelajari mengenai bagaimana keamanan dan kerahasiaan suatu pesan terjaga saat dikirimkan dari tempat asal atau tempat pengirim ke tempat tujuan atau tempat penerima. Kriptografi juga dapat dikatakan sebagai sebuah cara untuk mengamankan data dengan menggunakan metode matematika (Candra, 2016). Kriptografi memiliki 3 konsep utama untuk keamanan informasi, yaitu :

1. Confidentiality, menjaga suatu informasi dari orang-orang yang tidak berhak atas informasi tersebut,
2. Integrity, informasi tidak boleh dirubah tanpa ijin,
3. Authentication, merupakan suatu kemampuan untuk mengonfirmasi bahwa data tersebut adalah asli, tidak palsu.

Teknik enkripsi adalah teknik yang dapat mencapai salah satu konsep yaitu confidentiality. Enkripsi merupakan teknik menujaga kerahasiaan pesan dengan mengubah pesan asli (*Plaintext)* menjadi pesan yang telah menjadi pesan rahasia (*Chipertext).* Teknik enkripsi memiliki 2 kunci yaitu asimetrik dan simetrik. Perbedaan dari asimetrik dan simetrik terletak pada kuncinya. Pada asimetrik, menggunakan kunci yang berbeda pada proses enkripsi dan dekripsi. Sementara pada simetrik menggunakan kunci yang sama baik untuk enkripsi dan dekripsi.

Algoritme simetrik terbagi menjadi 2 macam berdasarkan prosesnya, yaitu *stream chiper* dan *block chiper. Stream chiper* mengenkripsi tiap bot pesan dengan *keystream* yang dihasilkan oleh *stream chiper.* Sementara *block chiper,* proses enkripsi dibagi menjadi blok-blok dengan ukuran yang sama dan setiap block dienkripsi dengan *keystream* yang dihasilkan oleh *block chiper.*

2.2.3.1 Algoritme Speck

SPECK adalah keluarga blokcipher ringan yang di rilis oleh Badan Keamanan Nasional A.S. pada tahun 2013. Keluarga SPECK terdiri dari 10 versi, mendukung berbagai ukuran blok dan kunci (Mohanty and Mohanty, 2014). Salah satu contohnya adalah Speck 64/128bit yang berarti versi *block chiper* Speck dengan

ukuran blok 64 bit dan ukuran *key* 128bit. Tabel 2.1 Menujukkan daftar parameter dari algoritme Speck.

Tabel 2.1 Daftar Parameter Algoritme Speck

Block Size 2*n*	Key Size *mn*	Word Size *N*	Key Words *m*	Round *T*	α	β
32	64	16	4	22	7	2
48	72	24	3	22	8	3
	96		4	23	8	3
64	96	32	3	26	8	3
	128		4	27	8	3
96	96	48	2	28	8	3
	144		3	29	8	3
128	128	64	2	32	8	3
	192		3	33	8	3
	256		4	34	8	3

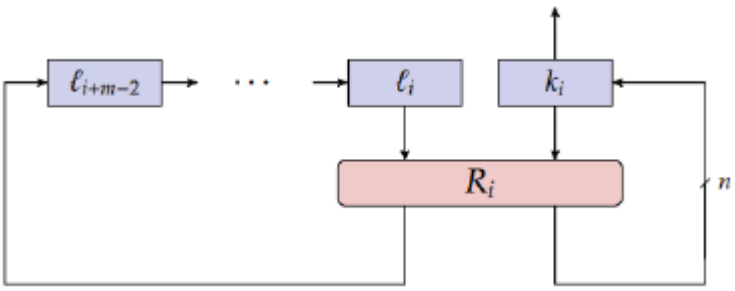
Enkripsi SPECK2n memetakan plaintext dari dua kata n-bit (x0, y0) ke dalam ciphertext (xT, yT), menggunakan urutan putaran T. Fungsi putaran *key-dependent* didefinisikan sebagai :

$$R^k(x,y) = (((x \ggg \alpha) \boxplus y) \oplus k, (y \lll \beta) \oplus ((x \ggg \alpha) \boxplus y) \oplus k),$$

Dimana *k* adalah *round key,* dan rotasi konstan α dan β seperti pada Tabel 2.1. *Key Schedule* dari algortima Speck menggunakan kembali fungsi putaran untuk menghasilkan *round key* $k_0, \ldots, k_T$ (Song, Huang and Yang, 2016). Kunci master *m-word* K = $(l_{m-2}, \ldots, l_0, k_0)$ digunakan seperti persamaan dibawah:

$$l_{i+m-1} = (k_i \boxplus (l_i \ggg \alpha)) \oplus i$$
$$k_{i+1} = (k_i \lll \beta) \oplus l_{i+m-1}.$$

Gambar 2.3 merupakan alur skematis pada fungsi *round* dan *key scheduling* algoritme SPECK.



Gambar 2.3 Alur Sekematis Fungsi *Round* Dan *Key Scheduling* Pada Algoritme Speck

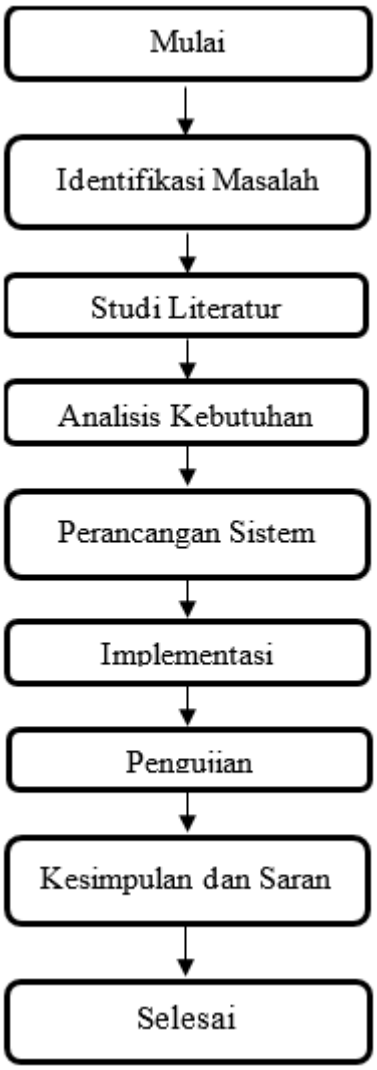
Sumber : (Fatmala, Kusyanti and Data, 2018)

Pada proses Enkripsi dimulai dari membuat putaran sebanyak T-1 setelah itu, dilanjutkan dengan mengolah nilai X, selanjutnya geser nilai X ke kanan sebanyak alfa berikutnya mengolah nilai y dan geser nilai y ke kiri sebanyak beta

BAB 3 METODOLOGI

Pada bab ini akan dijelaskan langkah apa saja yang dilakukan untuk menyelesaikan masalah pada penelitian ini. Langkah yang akan disusun untuk menyelesaikan masalah pada penelitian ini meliputi : Identifikasi masalah, studi literatur, analisis kebutuhan, perancangan sistem, implementasi, pengujian, dan pengambilan kesimpulan dan saran.

Pada Gambar 3.1 adalah susunan Metodologi yang akan dilakukan dalam penelitian ini.



Gambar 3.4 Alur Metodologi Penelitian

3.1 Identifikasi Masalah

Penulis menemukan masalah pada keamanan protokol LoRaWAN. Pada beberapa kasus, jarang sekali pengguna melakukan pengamanan pada sisi

komunikasi antara gateway (server) dan end device (*client*) sehingga pada penelitian ini memberikan solusi berupa pengamanan komunikasi dengan menggunkana teknik enkripsi. Pada skripsi ini, penulis mencoba menggunakan metode *Application Layer Data Encryption*, dengan memberikan inputan berupa palin text yang nantinya akan dilakukan proses enkripsi sehingga menghasilkan sebuah chipertext dengan menggunakan algoritme Speck 64/128bit.

3.2 Studi Literatur

Studi literatur merupakan kegiatan yang dilakukan untuk menentukan objek penelitian yang sesuai dengan topik yang diambil. Dalam pembahasan studi literatur penelitian ini, penulis melakukan studi literatur agar dapat mempelajari teori–teori pendukung dalam penelitian ini. Referensi yang digunakan berasal dari beberapa jurnal yang berbicara tentang algoritme Speck yang merujuk pada paper yang dikarang oleh Ling Song dkk, lalu pengaplikasian algoritme Speck, salah satunya yaitu "Implementasi Algoritme Speck untuk Enkripsi dan Dekripsi pada QR Code" yang disusun oleh Yuniar Siska. Untuk mendukung penelitian lebih lanjut, penulis juga melakukan *review* terhadap jurnal-jurnal lain yang mengkaji tentang protokol LoRaWAN, *Internet of Things* (IoT), dan teknologi LoRa. Kemudian penulis juga mendapatkan referensi dari jurnal dan penelitian resmi yang berkaitan dengan topik penelitian ini.

3.3 Analisis Kebutuhan

Analisis kebutuhan memiliki tujuan untuk memahami kebutuhan yang diperlukan pada penelitian ini

3.3.1 Analisis Kebutuhan Perangkat Keras

Penulis membutuhkan 2 perangkat keras dalam penelitian ini:

1. LoRa Board
2. Laptop, dengan jumlah dan fungsi sebagai berikut :
   - Jumlah : 1
   - Fungsi : Untuk menjalankan kode C++ untuk penerapan algortime Speck 64/128 bit

3.3.2 Analisis Kebutuhan Perangkat Lunak

Penulis menggunakan kurang lebih 2 perangkat lunak pada penelitian ini. Beriku beberapa perangkat lunak yang digunakan :

1. Wireshark

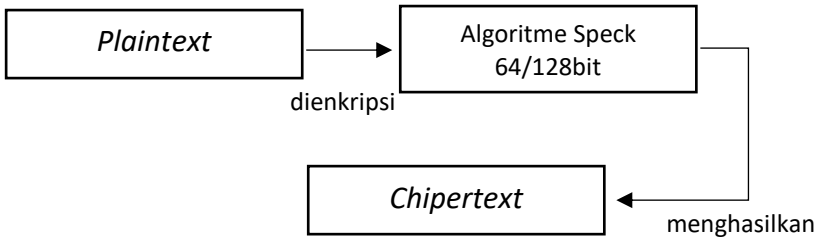
   Wireshark digunakan untuk meng-capture paket data maupun informasi yang tersedia di jaringan

2. Sublime Text

   Digunakan untuk menuliskan kode berupa Bahasa C++ dalam penerapan algoritme Speck 64/128bit

3.4 Perancangan Sistem

Dalam tahap perancangan , peneliti melakukan perancangan yang meliputi alur sistem yang dibuat, Bahasa pemrograman serta library yang digunakan. Penelitian bersifat implementatif, data yang digunakan menggunakan data *dummy,* bukan berasal dari sensor. Berikut merupakan alur perancangan yang dibuat:



Gambar 3.5 Alur Perancang Sistem

Gambar 3.2 merupakan gambaran model perancangan sistem. Sebuah inputan berupa *plaintext* akan dilakukan proses enkripsi menggunakan algoritme Speck 64/128bit yang akan menghasilkan *chipertext.*

3.5 Implementasi

Tahapan implementasi merupakan kegiatan pengimplementasian sistem yang telah dirancang dan disusun sebelumnya. Implementasi dilakukan dengan mengunakan Bahasa C++ dan perangkat lunak yang telah disebutkan sebelumnya pada analisis kebutuhan.

3.6 Pengujian

Pada tahap ini, sistem telah berhasil dirancang lalu penulis akan melakukan pengujian pada sistem yang dibangun. Pengujian dilakukan untuk mengetahui bahwa sistem telah dapat berjalan sesuai dengan spesifikasi, kebutuhan, dan tujuannya. Tahap implementasi dilakukan dengan menguji *inputan* berupa *plaintext* yang dienkripsi menggunakan algoritme Speck 64/128bit

3.7 Kesimpulan dan Saran

Kesimpulan merupakan hasil akhir dari setiap langkah-langkah yang dilewati pada penelitian ini yang akan menjawab rumusan masalah yang telah disebutkan terlebih dahulu pada awal penelitian.

DAFTAR REFERENSI

Devalal, S. and Karthikeyan, A., 2018. LoRa Technology - An Overview. *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, [online] (Iceca), pp.284–290. Available at: <https://ieeexplore.ieee.org/document/8474715/>.

Purba, Y., 2017. *Enkripsi*.

Semiconductors, N.X.P., 2018. IoT Device Secure Connection with LoRa.

Biswas, A.R. and Giaffreda, R., 2014. IoT and cloud convergence: Opportunities and challenges. *2014 IEEE World Forum on Internet of Things (WF-IoT)*, [online] pp.375–376. Available at: <http://ieeexplore.ieee.org/document/6803194/>.

Candra, 2016. Keamanan Data Dengan Metode Kriptografi Kunci Publik. *Jurnal TIMES*, 2(2), pp.11–15.

Fatmala, Y.S., Kusyanti, A. and Data, M., 2018. Implementasi Algoritme Speck untuk Enkripsi dan Dekripsi pada QR Code. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2(12), pp.6253–6260.

Lavric, A. and Popa, V., 2017. Internet of Things and LoRa™ Low-Power Wide-Area Networks: A survey. *ISSCS 2017 - International Symposium on Signals, Circuits and Systems*.

Mohanty, B. and Mohanty, M.N., 2014. A novel SPECK algorithm for faster image compression. *Proceedings - 2013 International Conference on Machine Intelligence Research and Advancement, ICMIRA 2013*, pp.479–482.

Song, L., Huang, Z. and Yang, Q., 2016. Automatic differential analysis of ARX block ciphers with application to SPECK and LEA. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9723, pp.379–394.