PROPOSAL PROYEK AKHIR
TAHUN AJARAN 2023/2024

IMPLEMENTASI KEAMANAN KOMUNIKASI V2I PADA SKEMA PEMBANGKITAN KUNCI BERBASIS LORA

Oleh :
Habib Hammam Kurniawan
2221600006

DEPARTEMEN TEKNIK ELEKTRO
PROGRAM STUDI TEKNIK TELEKOMUNIKASI
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2024

ABSTRAK

Penelitian ini mengkaji implementasi keamanan komunikasi Vehicle-to-Infrastructure (V2I) dengan skema pembangkitan kunci berbasis teknologi LoRa. Dalam konteks meningkatnya jumlah kendaraan bermotor dan infrastruktur transportasi di Indonesia, komunikasi V2I menjadi krusial untuk meningkatkan efisiensi dan keselamatan transportasi. Namun, peningkatan keterhubungan ini menimbulkan kekhawatiran akan keamanan data yang ditransmisikan. Penelitian ini bertujuan untuk mengembangkan sistem aplikasi pelacakan posisi yang aman dengan menggunakan Raspberry Pi4 dan LoRa, serta mengimplementasikan skema pembangkitan kunci rahasia untuk komunikasi V2I. Metode yang digunakan melibatkan pembangkitan kunci rahasia berdasarkan kuat sinyal (RSSI), penerapan filter Kalman untuk meningkatkan korelasi data RSS, dan kuantisasi multibit dengan enkripsi AES-128 untuk pengamanan data.Eksperimen dilakukan dengan memanfaatkan tiga Raspberry Pi4 dan satu laptop untuk mensimulasikan serangan insider. Penelitian ini berfokus pada komunikasi mobile outdoor menggunakan standar CEN-DSRC pada frekuensi 5.8 GHz. Hasil penelitian diharapkan dapat meningkatkan keamanan dan privasi dalam sistem transportasi Indonesia, serta mendorong adopsi teknologi V2I yang lebih luas.

1. **Judul Proyek Akhir**
   Implementasi keamanan Komunikasi V2I pada Skema Pembangkitan Kunci berbasis LoRa
2. **Ruang Lingkup**
   Ruang lingkup dari penelitian proyek akhir ini berkisar pada bidang ilmu antara lain:
   - Kemanan Jaringan
   - Enkripsi dan Dekripsi
   - Pembangkita kunci rahasia
   - Pemrograman
   - Jaringan komputer

3. **Tujuan**

   Tujuan penelitian tugas akhir ini adalah membuat sistem aplikasi tracking posisi yang aman dengan skema pembangkitan kunci rahasia pada komunikasi V2I (Vehicle to Infrastructure) dengan memanfaatkan Raspberry Pi4 dan LoRa.

4. **Latar Belakang**

   Dalam beberapa tahun terakhir, Indonesia telah menyaksikan pertumbuhan pesat dalam jumlah kendaraan bermotor dan infrastruktur transportasi. Pertumbuhan ekonomi yang stabil dan urbanisasi yang terus berlanjut telah menjadi pendorong utama di balik lonjakan jumlah kendaraan di jalan raya. Menurut data terbaru yang diterbitkan oleh Kementerian Perhubungan, pada tahun 2023, jumlah kendaraan bermotor di Indonesia telah mencapai lebih dari 141 juta unit, dan angka ini diperkirakan terus meningkat setiap tahunnya. Seiring dengan itu, perkembangan infrastruktur jalan raya juga terjadi di seluruh negeri, dengan proyek-proyek pembangunan jalan baru dan peningkatan yang terus berlangsung.

   Dalam konteks pertumbuhan ini, komunikasi Vehicle-to-Infrastructure (V2I) menjadi semakin penting untuk meningkatkan efisiensi dan keselamatan transportasi di Indonesia. Konsep V2I melibatkan penggunaan teknologi untuk memfasilitasi komunikasi antara kendaraan bermotor dengan infrastruktur jalan raya, seperti lampu lalu lintas, rambu-rambu digital, dan sensor-sensor jalan. Dengan V2I, kendaraan dapat menerima informasi tentang kondisi lalu lintas, peringatan bahaya, dan rute alternatif secara real-time, sehingga membantu mengurangi kemacetan dan meningkatkan keselamatan pengguna jalan.

   Namun, seiring dengan meningkatnya keterhubungan antara kendaraan dan infrastruktur, timbul pula kekhawatiran akan keamanan data yang ditransmisikan melalui komunikasi V2I. Data sensitif seperti lokasi kendaraan, kecepatan, dan rencana perjalanan dapat menjadi target serangan cyber atau penyadapan yang dapat membahayakan privasi individu dan keselamatan lalu lintas secara keseluruhan. Dalam konteks ini, keamanan data menjadi aspek yang sangat penting untuk diperhatikan dalam pengembangan sistem transportasi yang cerdas dan terkoneksi.

   Data dari Badan Pusat Statistik (BPS) menunjukkan bahwa pada tahun 2022, lebih dari 135.000 kecelakaan lalu lintas terjadi di Indonesia, dengan lebih dari 31.000 korban meninggal dunia. Fakta ini menyoroti urgensi perlunya upaya untuk meningkatkan keamanan transportasi di Indonesia. Untuk mencapai tujuan ini, penerapan teknologi keamanan yang efektif dalam komunikasi V2I menjadi suatu keharusan. Teknologi kriptografi, yang mengenkripsi pesan-pesan yang ditransmisikan antara kendaraan dan

infrastruktur, dapat menjadi solusi yang efektif untuk melindungi integritas dan kerahasiaan data dalam komunikasi V2I.

Sementara itu, adopsi teknologi Internet of Things (IoT) terus berkembang pesat di Indonesia. Menurut laporan dari Asosiasi IoT Indonesia, diperkirakan jumlah perangkat IoT terkoneksi di Indonesia akan mencapai lebih dari 1,5 miliar pada tahun 2025. IoT telah membuka pintu untuk berbagai inovasi dalam berbagai sektor, termasuk transportasi. Dalam konteks infrastruktur transportasi, teknologi LoRa (Long Range) menawarkan solusi komunikasi nirkabel jarak jauh yang efisien dan hemat energi. Dengan kemampuannya untuk memberikan jangkauan komunikasi yang luas, LoRa memiliki potensi besar untuk mendukung implementasi komunikasi V2I di Indonesia.

Oleh karena itu, penelitian ini bertujuan untuk menginvestigasi dan mengimplementasikan keamanan komunikasi V2I dengan memanfaatkan teknologi LoRa dan skema pembangkitan kunci yang sesuai. Dengan mengintegrasikan keamanan komunikasi yang efektif dalam infrastruktur jalan raya berbasis LoRa, diharapkan dapat meningkatkan keamanan dan privasi dalam sistem transportasi di Indonesia serta mempromosikan adopsi teknologi V2I yang lebih luas dalam masyarakat.

5. Perumusan Masalah dan Batasan Masalah

1. Rumusan Masalah

Masalah yang dibahas dalam penelitian tugas akhir ini adalah sebagai berikut:

1. Bagaimana proses membangkitkan kunci rahasia dengan memanfaatkan kuat sinyal (RSSI) pada jaringan V2I?
2. Bagaimana mengimplementasikan metode kalman filter untuk meningkatkan korelasi data kuat sinyal (RSSI)?
3. Bagaimana proses kuantisasi data dengan kuantisasi multibit dan pengamanan data berbasis AES pada jaringan V2I?
4. Bagaimana tingkat keamanan sistem terhadap insider attack?
5. Bagaimana membuat aplikasi pelacakan (*tracking*) untuk mengetahui posisi kendaaran?

2. Batasan Masalah

Masalah yang dibahas dalam penelitian tugas akhir ini adalah sebagai berikut:

1. Penelitian ini hanya memanfaatkan nilai kuat sinyal RSS sebagai parameter penentu kecocokan kanal komunikasi.
2. Penelitain dilakukan dengan menggunakan 3 buah Raspberry Pi 3 dan sebuah laptop untuk melakukan attack(eve).
3. Kuantisasi yang digunakan Kuantisasi Multibit
4. Enkripsi dan dekripsi di implementasikan menggunakan kunci simetris dengan metode AES-128.
5. Penelitian dilakukan pada aplikasi V2I (Vehicle-to-Infrastructure) secara mobile outdoor dengan standar komunikasi CEN-DSRC menggunakan frekuensi 5.8 GHz.

6. Tinjauan Pustaka

1. Penelitian Yang Pernah Dilakukan

Penelitian ini merupakan pengembangan dari proyek penelitian sebelumnya dengan menganalisa proyek-proyek tersebut. Berikut ini beberapa penelitian yang telah dilakukan sebelumnya dan dijadikan sebagai referensi untuk menunjang penyelesaian penelitian:

Pada tahun 2020 terdapat jurnal oleh Biao Han, Sirui Peng, Celimuge Wu, Xiaoyan Wang dan Baosheng Wang yang dilatar belakangi oleh perkembangan teknologi komunikasi Vehicle-to-Vehicle (V2V) dan Vehicle-to-Infrastructure (V2I) Dengan perkembangan ini, muncul kekhawatiran serius terkait keamanan, terutama karena komunikasi dilakukan melalui saluran nirkabel yang tidak aman. Masalah utama yang dihadapi adalah autentikasi dan keamanan komunikasi, karena teknologi yang ada saat ini seperti kunci yang dibagi sebelumnya (PSK) dianggap tidak cukup aman dan fleksibel. Untuk mengatasi tantangan ini, diperlukan skema pembangkitan kunci pada lapisan fisik yang lebih ringan dan tidak memerlukan infrastruktur pihak ketiga, serta mampu memperbarui kunci secara fleksibel berdasarkan karakteristik saluran waktu nyata. Jurnal tersebut ditulis untuk mempelajari dan mengembangkan skema pembangkitan kunci pada lapisan fisik dalam lingkungan V2V/V2I, menggunakan jaringan Long Range (LoRa) untuk mengumpulkan indikator kekuatan sinyal yang diterima (RSSI) sebagai informasi konsensus.

Pada tahun 2019 dilakukan pengerjaan proyek akhir oleh Adib Muhammad Visoka yang dilatarbelakangi oleh masalah keamanan pada kendaraan tahanan dan mobil polisi di Indonesia, terutama setelah insiden pembajakan kendaraan tahanan milik Kejaksaan Negeri pada tahun 2017. Ketidakhadiran sistem komunikasi yang aman membuat monitoring sulit dan meningkatkan risiko keamanan. Oleh karena itu, dikembangkan sistem komunikasi berbasis IP dengan enkripsi AES 128 bit, pelacakan GPS, dan koneksi server untuk monitoring. Keamanan diperoleh melalui skema pembangkitan kunci rahasia (SKG) menggunakan kuat sinyal RSS antara Road Side Unit (RSU) dan Raspberry Pi di kendaraan tahanan, yang diolah dengan Kalman filter, dikuantisasi menjadi bit-bit biner, dan dikonversi menjadi kode heksa dengan standar SHA-1 sebelum dienkripsi sebagai secret key. Keamanan komunikasi diuji dengan simulasi eavesdropping atau insider attack untuk mengukur efektivitas SKG dalam melindungi data antara RSU dan kendaraan.

Pada tahun 2020 dilakukan penelitian yang dilatarbelakangi oleh kebutuhan akan protokol keamanan yang lebih baik untuk komunikasi V2X (vehicle-to-everything) pada kendaraan. Komunikasi yang aman sangat penting untuk memastikan integritas dan keaslian pesan yang ditransmisikan antar kendaraan serta antara kendaraan dengan infrastruktur jalan. Oleh karena itu, dikembangkan protokol keamanan baru yang menggunakan metode kriptografi berbasis rantai hash untuk mengurangi overhead komputasi dan meningkatkan efisiensi komunikasi. Protokol ini diuji menggunakan perangkat DSRC komersial seperti Cohda Wireless MK5 dan dibandingkan dengan protokol standar seperti IEEE 1609 dan ETSI 103-097. Hasil pengujian menunjukkan bahwa protokol yang diusulkan lebih efisien dalam hal waktu tanda tangan dan verifikasi, serta mampu mengurangi overhead komunikasi secara signifikan.

Berdasarkan penelitian sebelumnya, maka pada proyek akhir ini akan dikembangkan sistem aplikasi pelacakan posisi yang aman menggunakan Raspberry Pi4 dan LoRa, serta mengimplementasikan skema pembangkitan kunci rahasia untuk komunikasi V2I. Metode yang digunakan melibatkan pembangkitan kunci rahasia berdasarkan kuat sinyal (RSSI), penerapan filter Kalman untuk meningkatkan korelasi data RSS, dan kuantisasi multibit dengan enkripsi AES-128 untuk pengamanan data. Eksperimen dilakukan dengan memanfaatkan tiga Raspberry Pi4 dan satu laptop untuk

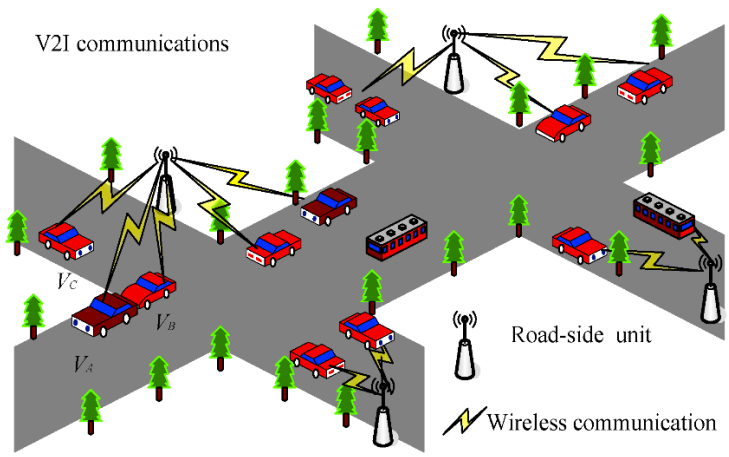
mensimulasikan serangan insider. Penelitian ini berfokus pada komunikasi mobile outdoor menggunakan standar CEN-DSRC pada frekuensi 5.8 GHz. Hasil penelitian diharapkan dapat meningkatkan keamanan dan privasi dalam sistem transportasi Indonesia, serta mendorong adopsi teknologi V2I yang lebih luas.

No	Judul Penelitian	Pra Proses	Kuantisasi	Rekonsiliasi	Privacy Amplification	Connection
1	LoRa-Based Physical Layer Key Generation for Secure V2V/V2I Communications	Tidak ada	Multibit	Cascade	Ada	LoRa
2	Analisa Keamanan Skema Secret Key Generation (Skg) Di Aplikasi Tracking Posisi Pemindahan Narapidana Dari Insider Attack	Kalman Filter	Jana Multibit	BCH error correction	Universal Hash	Wifi
3	Comparative Experiments of V2X Security Protocol Based on Hash Chain Cryptography	Tidak ada	Tidak ada	Tidak ada	Tidak ada	

2. Teori Penunjang

6.2.1 V2I

V2I (Vehicle-to-Infrastructure) adalah bagian dari ekosistem komunikasi yang lebih luas dalam Intelligent Transportation Systems (ITS), di mana kendaraan dapat berkomunikasi dengan infrastruktur di sekitarnya seperti lampu lalu lintas, rambu jalan, dan stasiun pengisian bahan bakar. V2I memungkinkan pertukaran data dua arah antara kendaraan dan infrastruktur jalan untuk meningkatkan keselamatan, efisiensi, dan kenyamanan dalam berkendara.



Gambar 1. Ilustrasi V2I

6.2.2 Lora AcSIP EK-S76SXB

LoRa merupakan sebuah teknologi komunikasi pada frekuensi radio VHF/UHF dengan modulasi unik yang dikembangkan oleh semtech pada tahun 2012, sedangkan LoRaWAN adalah suatu sistem standar komunikasi LoRa untuk memudahkan komunikasi antara node, gateway dan network server walaupun berbeda fabrikasinya. Beberapa fabrikasi chip elektronik berlomba lomba dalam membuat module LoRa, macam - macam module juga berbeda spesifikasinya, salah satunya adalah modul Acsip EK S76SXB. Modul Lora AcSIP EK-S76SXB ini sangat mudah digunakan karena di dalam ICnya terdapat sebuah MCU dari ST Microelectronics dengan part number STM32L073 dengan konsumsi daya yang sangat rendah sehingga tidak membutuhkan mcu eksternal untuk menghubungkan sensor yang akan dikirim menggunakan LoRa, serta Lora AcSIP EK S76SXB ini menyediakan firmware yang juga dapat di kontrol menggunakan interface UART untuk memudahkan penggunaanya. Spesifikasi dan fitur dari LoraAcSIP EK-S76SXB ini mendukung protokol Class A, B, dan C LoRaWan. GPIO yang dapat dikonfigurasi penggunannya. Lora AcSIP EK-S76SXB ini memiliki jangkauan sampai dengan 16 km, mempunyai frekuensi EU68 / US915 dengan badwidth 62.5~500KHz, serta pada Tx power dapat dikonfigurasi sampai 20 dBm dengan sensitivitas penerimanya sampai -137 dBm [2].

Gambar 2. Lora AcSIP EK S76SXB

6.2.3 Raspberry Pi

Raspberry Pi adalah sebuah komputer papan tunggal (single-board computer) atau SBC seukuran kartu kredit yang dapat digunakan untuk menjalankan program perkantoran, permainan komputer, dan sebagai pemutar media hingga video beresolusi tinggi. Raspberry Pi dikembangkan oleh yayasan nirlaba, Rasberry Pi Foundation dengan tujuan untuk belajar pemrograman. Raspberry Pi memiliki komponen yang hampir serupa dengan komputer pada umumnya. Seperti CPU, GPU, RAM, Port USB, Audio Jack, HDMI, Ethernet, dan GPIO. Untuk tempat penyimpanan data dan sistem operasi Raspberry Pi tidak menggunakan harddisk drive (HDD) melainkan menggunakan Micro SD dengan kapasitas paling tidak 4 GB, sedangkan untuk sumber tenaga berasal dari micro USB power dengan sumber daya yang direkomendasikan yaitu sebesar 5V dan minimal arus 700 mA. Raspberry Pi memiliki system Broadcom BCM2835 chip(SoC),yang mencakup ARM1176JZF-S 700 MHz processor (firmware termasuk sejumlah mode "Turbo" sehingga pengguna dapat mencoba overclocking, hingga 1 GHz, tanpa mempengaruhi garansi), VideoCore IV GPU, dan awalnya dikirim dengan 256 megabyte RAM, kemudian upgrade ke 512MB [3].

Gambar 3. Raspberry Pi

6.2.4 RAK2245 LoRaWAN Gateway

RAK2245 Pi HAT adalah modul compatible dengan Raspberry Pi. Seperti halnya pada Raspberry Pi 3 model B+. Pada modul ini Board adalah konsentrator Gateway LoRawan terkecil yang mengintegrasikan Modul GPS Ublox MAX-7Q dan heat sink dan juga modul ini mendukung delapan saluran dan tersedia untuk frekuensi band global LoRaWAN, yaitu : EU433, CN470, EU868, US915, AS923, AU915, KR920, IN865 dan AS920. Board dapat menyediakan link radio Lora dengan 20 data rate rendah dalam kecepatan yang sangat cepat. Hal tersebut didukung oleh konsentrator transceiver semtech SX1301 yang mampu mengelola paket dari banyak titik yang tersebar jauh. RAK2245 menggunakan chip Semtech SX1301 sebagai Transceiver Concentrator dengan dua chip Semtech SX125X sebagai Frontend I/Q Transceiver. RAK2245 dapat mentransmisikan daya (TX) sampai 27 dBm dengan sensitivitas terima (RX) sampai dengan -139 dBm.

Gambar 4. RAK2245 LoRaWAN Gateway

6.2.5 Channel Probing

Channel Probing adalah proses pertukaran RSSI antara Node dan Gateway. Pada tahap ini Node sensor melakukan pengiriman data secara confirmed dengan data payload berupa sekuen Ping ke Gateway. Pada proses Channel Probing Node melakukan join ke Gateway dengan mengirimkan pesan. Pengiriman pesan bertujuan agar Gateway dapat mengetahui bahwa Node telah bergabung. Kemudian Gateway akan mengirimkan Metadata. Di mana Metadata yang dikirimkan berupa Interval Ping, Setting Spreading Factor, dan waktu dari Gateway yang tersinkronisasi. Setelah Node menerima Meta End maka Node akan memulai proses Ping dengan mengirimkan data yang berisi Header dan Payload. Apabila pada proses Ping terjadi error maka proses Ping tersebut akan diulang kembali. Apabila proses Ping berhasil dan dapat menerima balasan dari Gateway maka dilanjutkan dengan pengiriman Ping selanjutnya. Ketika paket Ping sudah sesuai sukuens yang di setting atau pada penelitian ini sebanyak 100 kali maka data RSSI disimpan dalam file

CSV baik disisi Node maupun Gateway. Dari nilai RSSI yang sudah disimpan di file CSV disisi Node maupun Gateway dapat digunakan untuk menghitung nilai koefisien korelasi dengan menggunakan persamaan 3 [1].

6.2.6 Metode Privacy Amplification BCH

BCH error correction merupakan salah satu metode yang sering digunakan untuk melakukan error correction. Bose, Chaudhuri, dan Hocquenghern (BCH) code juga merupakan metode yang sangat baik untuk melakukan multiple-error correction berbasis kode siklik. Dengan memanfaatkan kode BCH diharapkan kesahalan pada bit- bit informasi dapat dikoreksi. Dalam teorinya, Kode BCH memiliki karakteristik yang memungkinkan pendisain untuk menentukan kapasitas koreksi yang diinginkan. Keunggulan lainnya kode BCH memiliki kemudahan pada proses decoding yang sangat efisien dan sederhana sehingga cocok untuk diimplementasikan pada hardware elektronik dengan kemampuan kalkulasi rendah [5].

6.2.7 Kuantisasi Multibit

Multibit quantization adalah proses mengubah nilai analog atau sinyal kontinyu menjadi nilai digital dengan representasi multibit. Dalam konteks komunikasi dan pengolahan sinyal, multibit quantization digunakan untuk meningkatkan resolusi dan akurasi sinyal digital. Proses ini melibatkan pemetaan amplitudo sinyal yang beragam menjadi nilai diskret dalam bentuk bit-bit biner. Dengan meningkatkan jumlah bit yang digunakan dalam kuantisasi, lebih banyak tingkat diskret dapat diwakili, yang pada gilirannya meningkatkan ketepatan dan kualitas rekonstruksi sinyal. Multibit quantization sangat penting dalam aplikasi yang memerlukan pengolahan sinyal presisi tinggi, seperti enkripsi data dan transmisi informasi dalam jaringan yang aman, karena memungkinkan sinyal untuk direpresentasikan dengan lebih rinci dan akurat.

6.2.8 Kalman Filter

Kalman filter adalah algoritma rekursif yang digunakan untuk memperkirakan status dari suatu sistem dinamis yang dipengaruhi oleh kebisingan acak. Algoritma ini menggabungkan serangkaian pengukuran yang diambil dari waktu ke waktu, yang mungkin mengandung kebisingan dan ketidakakuratan, dan menghasilkan estimasi nilai yang lebih akurat dari variabel yang diukur. Kalman filter bekerja dengan dua tahap utama: prediksi dan koreksi. Pada tahap prediksi, estimasi status saat ini dan kesalahan prediksi dihitung berdasarkan model sistem. Pada tahap koreksi, estimasi ini diperbarui dengan menggunakan pengukuran terbaru, dengan mempertimbangkan ketidakpastian dalam pengukuran dan prediksi. Kalman filter banyak digunakan dalam berbagai aplikasi, termasuk navigasi, pelacakan objek, dan pengolahan sinyal, karena kemampuannya untuk memberikan estimasi yang optimal dan real-time dalam lingkungan yang tidak pasti dan berisik.

6.2.9 *Advance Encryption Standart* (AES)

Advanced Encryption Standard (AES) adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris. *Advanced Encryption Standard* (AES) dipublikasikan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001. AES merupakan blok kode simetris untuk menggantikan DES (*Data Encryption Standard*). Saat ini, AES merupakan algoritma kriptografi

yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia.

Algoritma AES merupakan algoritma simetris yaitu mengunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192 dan AES-256 [7]. Dalam algoritma kriptografi AES 128, 1 blok plainteks berukuran 128 bit terlebih dahulu dikonversi menjadi matriks heksadesimal berukuran 4x4 yang disebut state. AES dipublikasikan oleh NIST pada tahun 2001 yang digunakan untuk menggantikan algoritma DES yang sudah dianggap kuno dan mudah dibobol. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Urutan data dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi chipertext. Panjang kunci dari AES terdiri dari panjang kunci 128 bit, 192 bit, dan 256 bit. Perbedaan panjang kunci ini yang nantinya mempengaruhi jumlah putaran pada algoritma AES ini. Jumlah putaran yang digunakan algoritma ini ada tiga macam seperti pada Tabel I.

Tabel 1. Pengelompokan Jenis AES

Jenis AES	**Panjang Kunci (Nk words)**	**Ukuran Blok (Nb words)**	**Jumlah Putaran (Nr)**
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Catatan: 1 word = 32 bit

Secara umum, proses enkripsi algoritma AES mempunyai beberapa tahapan, yaitu [8]:

1) *AddRoundKey*: yaitu, proses melakukan X-OR(*Exclusive Or*) antara state awal (*plaintext*) dan *cipherkey*. Tahap ini disebut juga dengan *initial round*.
2) *Round*: yaitu, putaran sebanyak NR –1 kali. Pada setiap putaran atau ronde memiliki beberapa proses, diantaranya adalah:
   a. *SubBytes*: yaitu, mensubstitusikan byte dengan menggunakan tabel S-Box (tabel substitusi).
   b. *Shiftrows*: yaitu, melakukan pergeseran tiap baris *array state* secara *wrapping*.
   c. *MixColumns*: yaitu, mengacak data pada tiap kolom *array state*.
   d. *AddRoundKey*: yaitu, melakukan X-OR antara hasil state sekarang dengan kunci hasil proses *expand key*.
3) *Final Round*: yaitu, proses untuk putaran atau ronde terakhir:
   a. *SubBytes*
   b. *Shiftrows*
   c. *AddRoundKey*

6.2.10 Performansi

Setelah sistem pembangkitan kunci berhasil dibuat, dapat dilakukan evaluasi kinerja dengan menggunakan tiga parameter yaitu *Key Generation Rate* (KGR), *Key Disagreement Rate* (KDR), dan *randomness* (keacakan) [8].

a. *Key Disagreement Rate* (KDR)

KDR adalah persentase dari bit yang berbeda di antara kunci yang dihasilkan oleh Alice dan Bob, yang didefinisikan sebagai

$$\text{KDR} = \frac{\sum_{i=1}^{N} |K^A(i) - K^B(i)|}{N} \quad (11)$$

dimana N adalah panjang kunci. KDR harus lebih kecil dari kemampun koreksi rekonsiliasi informasi, jika tidak, maka pembangkitan kunci akan gagal. Untuk mencari nilai KDR dapat dilihat pada persamaan 11.

b. *Key Generation Rate* (KGR)

KGR menjelaskan jumlah bit rahasia yang dihasilkan dalam satu detik/pengukuran. Hal ini terutama bergantung pada kondisi lingkungan, yang menentukan jumlah keacakan yang tersedia untuk ekstraksi. KGR yang tinggi sangat penting untuk proses pembuatan kunci karena skema kriptografi membutuhkan panjang kunci tertentu. Sebagai contoh, enkripsi tingkat lanjut standar (AES) membutuhkan urutan kunci dengan panjang minimum dari 128 bit.

Persamaan umum untuk mendapatkan nilai KGR dapat dilihat pada persamaan 12.

$$KGR = \frac{K}{T} \quad (12)$$

dimana K merupakan rata-rata jumlah bit yang dihasilkan Alice dan Bob dan T merupakan waktu pengukuran dan komputasi program.

c. *Randomness* (keacakan)

Randmomness adalah fitur yang paling penting dari sistem pembangkitan kunci. Aplikasi kriptografi memiliki persyaratan yang ketat pada keacakan kunci. Terdapat sebuah uji keacakan yang disediakan oleh National Institute of Standards and Technology (NIST) yang banyak digunakan untuk menguji keacakan dari bilangan acak random number generator (RNG) dan pseudo random number generator (PRNG). Pada dasarnya, sebuah sistem pembangkitan kunci adalah sebuah jenis RNG, sehingga rangkaian uji statistik NIST juga bisa diterapkan [9]. Uji keacakan digunakan untuk menghitung tingkat kepercayaan nilai *P* terhadap H0. Jika nilai *P* sama dengan 1, maka urutan kunci yang dihasilkan sangat acak, tetapi, jika nilai *P* sama dengan 0, maka urutan kunci yang dihasilkan secara sempurna adalah tidak acak. Kita dapat memilih nilai α sebagai nilai tingkat signifikansi. Jika nilai $P \geq \alpha$, maka H0 akan diterima dan menerima urutan kunci sebagai rangkaian acak, sebaliknya jika nilai $P < \alpha$ maka H0 akan ditolak dan menerima urutan kunci sebagai rangkaian yang nonrandom. Biasanya, α telah dipilih dalam kisaran [0,001, 0,01], nilai α yang biasanya digunakan pada kriptografi adalah 0,01.

6.2.11 Secure Hash Algorithm (SHA)

Security Hash Algorithm (SHA) dikembangkan pada tahun 1993 oleh *National Institute of Standards and Technology* (NIST) dan *National Security Agency* (NSA). Algoritma ini dirancang sebagai algoritma yang akan digunakan untuk hashing yang aman dalam Standar Tanda Tangan Digital AS. Fungsi hash adalah salah satu metode enkripsi yang paling umum digunakan. Hash adalah fungsi matematika khusus yang melakukan enkripsi satu arah. SHA-l adalah versi revisi dari SHA yang dirancang oleh NIST dan diterbitkan sebagai *Federal Information Processing Standard* (FIPS). Seperti MD5, SHA-l memproses data input dalam blok 512 bit. SHA-l menghasilkan pesan 160 bit. Sedangkan MD5 menghasilkan *message digest* sebesar 128 bit [6].

6.2.12 Octave

GNU *Octave* adalah suatu perangkat lunak gratis (freeware) dan bahasa tingkat tinggi untuk komputasi numerik dan visualisasi data. *Octave* dirancang sebagai tiruan dari Matlab. *Octave* biasa digunakan untuk melakukan komputasi numerik dengan matriks dan vektor. Program tersebut juga dapat digunakan untuk perhitungan umum dan untuk menggambar grafik fungsi. *Octave* dikembangkan oleh John W. Eaton (Universitas Texas). Kelebihan utama dari *Octave* yaitu gratis (*freeware*) dan tersedia untuk berbagai sistem operasi seperti Windows 98/2000/XP, Mac OS/X, Debian, Suse, Fedora, RedHat Linux. Pada kebanyakan sistem operasi program GNU *Octave* dapat dijalankan dengan memberikan perintah *Octave* pada shell command. Setelah perintah tersebut kita berikan maka akan muncul suatu jendela GNU *Octave*. Pada jendela tersebut akan ditampilkan beberapa pesan singkat mengenai *Octave* dan kemudian di bawah pesan singkat tersebut ditampilkan sebuah prompt, yang menandakan bahwa *Octave* siap untuk menerima perintah yang akan kita berikan.

6.2.13 Wireshark

Wireshark adalah salah satu analisis paket bebas serta sumber terbuka. Perangkat ini untuk digunakan sebagai pemecah suatu permasalahan jaringan, analisis, perangkat lunak dan serta mengembangkan protokol komunikasi, dan juga pendidikan, dari sekian banyak aplikasi *Network Analyzer* yang banyak digunakan oleh *Network Administrator* untuk menganalisa kinerja jaringannya dan mengontrol lalu lintas data di jaringan yang dikelola *Wireshark*. *Wireshark* mampu menangkap paket-paket data yang ada pada jaringan tersebut. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa.

6.2.14 Python

Python adalah bahasa pemrograman interpretatif multiguna dengan filosofi perancangan yang berfokus pada tingkat keterbacaan kode. Python diklaim sebagai bahasa yang menggabungkan kapabilitas, kemampuan, dengan sintaksis kode yang sangat jelas, dan dilengkapi dengan fungsionalitas pustaka standar yang besar serta komprehensif. Python mendukung multi paradigma pemrograman, utamanya; namun tidak dibatasi; pada pemrograman berorientasi objek, pemrograman imperatif, dan pemrograman fungsional. Salah satu fitur yang tersedia pada python adalah sebagai bahasa pemrograman dinamis yang dilengkapi dengan

manajemen memori otomatis. Seperti halnya pada bahasa pemrograman dinamis lainnya, python umumnya digunakan sebagai bahasa script meski pada praktiknya penggunaan bahasa ini lebih luas mencakup konteks pemanfaatan yang umumnya tidak dilakukan dengan menggunakan bahasa script. Python dapat digunakan untuk berbagai keperluan pengembangan perangkat lunak dan dapat berjalan di berbagai platform sistem operasi.

7. Metodologi

Metodologi adalah rangkaian kegiatan dalam melaksanakan penelitian berdasarkan rumusan, batasan dan tujuan pada penelitian. Adapun metodologi dalam penelitian ini adalah sebagai berikut.

7.1 Studi Literatur

Studi literatur ini meliputi beberapa hal yang harus dipelajari, antara lain:

1. Mempelajari metode pra proses menggunakaan metode *Kalman Filter*
2. Mempelajari proses Kuantisasi *Multibit*
3. Proses rekonsiliasi menggunakan metode BCH *error correction code*
4. Proses *Privacy Amplification* menggunakan metode *Universal Hash*
5. Proses Enskripsi dan Deskripsi menggunakan AES (*Advance Enscypsi Standart)*

7.2 Perancangan dan Pembuatan Sistem

7.2.1 Perangkat yang Digunakan

Dalam proses pengerjaan Proyek ini, dibutuhkan perangkat untuk menunjang pengerjaan sistem secara keseluruhan, baik perangkat keras (hardware) maupun perangkat lunak (software). Perangkat yang digunakan pada pengerjaan Proyek Akhir ini adalah sebagai berikut.

1. **Perangkat Keras (Hardware)**

   Pada proyek akhir ini digunakan prosesor utama sebagai pengolahan data untuk membuat kunci yaitu Raspberry Pi 3 dengan Sistem Operasi Raspbian, LoRa AcSIP EK-S76SXB, dan RAK2245 LoRaWAN Gateway.

2. **Perangkat Lunak (Software)**

   Dalam proses pengerjaan Proyek Akhir ini juga dibutuhkan perangkat lunak (software) diantaranya adalah sebagai berikut.

   1. **Wireshark**

      Wireshark merupakan sebuah software yang digunakan untuk melakukan capture paket-paket data pada jaringan. Software ini digunakan untuk menangkap kuat sinyal/RSSI pada saat pengkuran.

   2. **Python**

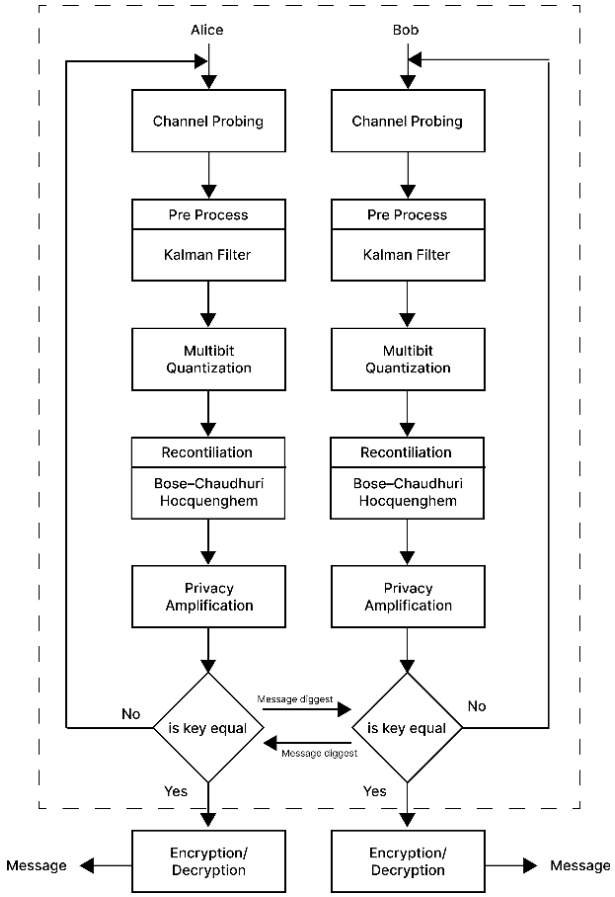
      Pemrograman pada Proyek Akhir ini menggunakan software IDLE Python 3.6 dalam proses pembangkitan kunci rahasia dengan menggunakan bahasa pemrograman Python. Terdapat integrasi antara file Python dengan file C pada proses uji NIST.

3. **Octave**

Octave digunakan untuk melakukan komputasi numerik dengan matriks dan vector. Program tersebut juga dapat digunakan untuk perhitungan umum dan untuk menggambar grafik fungsi.

7.2.2 Rancangan Sistem

Cara kerja sistem proyek akhir ini adalah melakukan proses pengambilan data RSSI dengan cara komunikasi antara node dan gateaway, pra proses menggunakan Kalman Filter, proses kuantisasi multibit, proses koreksi error menggunakan BCH error correction code, proses privasi amplifikasi menggunakan universal hash, proses enskripsi deskripsi dengan menggunakan AES-128, kemudian dilanjutkan dengan melakukan pengujian, dan melakukan analisa serta menyimpulkan hasil yang telah didapatkan dari sistem yang telah dibuat. Secara ringkas, cara kerja sistem dapat diilustrasikan sebagai berikut:



Gambar 5. Rancangan Sistem

Pada diagram blok rancangan sistem merupakan sebuah cara untuk mendapatkan data serta memproses data tersebut sehingga bisa didapatkan sebuah sistem pembangkitan kunci rahasia dengan metode Deep Learning sesuai tujuan awal penelitian yaitu pembangkitan kunci rahasia yang lebih optimal untuk menjaga keharasiaan pertukaran informasi dan komunikasi yang dilakukan.

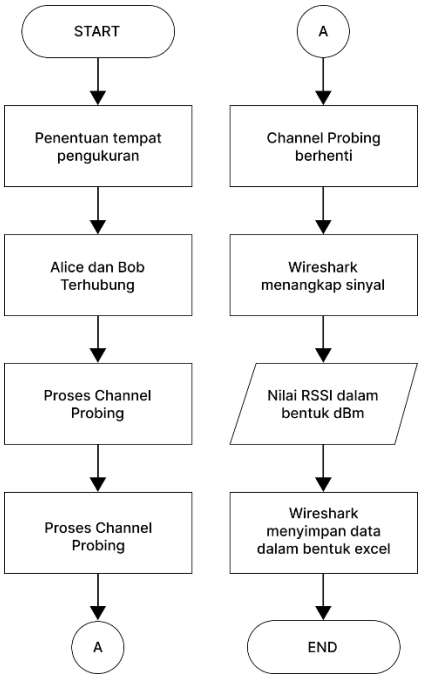
7.3 Implementasi Sistem

7.3.1 Channel Probing

Pada tahap ini terdapat 2 perangkat bernama Alice dan Bob yang bertukar request/reply probing sinyal satu sama lain dalam durasi waktu tertentu untuk mengumpulkan nilai RSSI. Salah satu segera membalas jika menerima request dari lainnya. Proses selanjutnya adalah menjumlahkan respon channel yang telah didapatkan dari Alice dan Bob seperti yang ditunjukkan oleh persamaan 4.

7.3.2 Pengukuran dan Pengolahan Data RSSI

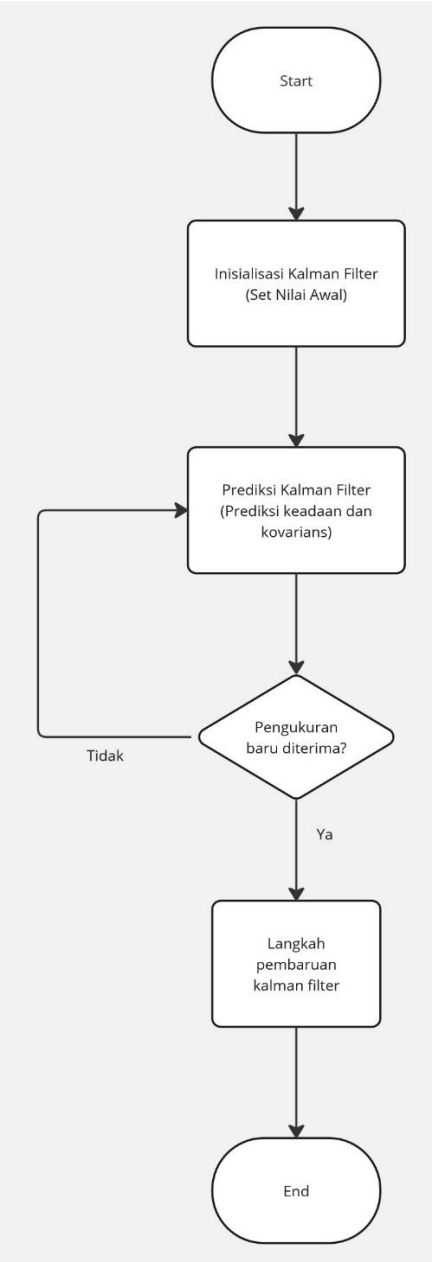
Pengukuran RSSI dilakukan di tempat yang direncanakan yaitu tempat yang sama saat melakukan channel probing atau komunikasi antara node dan gateway. Pada tempat pengukuran terdapat bahan-bahan yang dapat menyebabkan multipath, seperti halnya bahan bangunan tembok yang dapat menyebabkan difraksi atau refraksi. Software yang digunakan untuk melakukan pengukuran RSSI ini adalah Wireshark dengan interval 110 milidetik atau 0,11 detik. Flowchart dari pengukuran RSSI yang dilakukan pada Proyek Akhir ini pada Gambar 6.



Gambar 6. Flowchart Proses Pengukuran dan Pengolahan Data RSSI

7.3.3 Praproses Menggunakan Kalman Filter

Kalman filter adalah untuk menyatakan sebuah estimasi menggunakan struktur prediktor-korektor. Dalam update kali (prediksi) sistem state berikutnya diestimasi berdasarkan sistem state dan sifat transisi state yang diketahui sebelumnya. Flowchart praproses menggunakan Kalman Filter dapat dilihat pada Gambar 7.



Gambar 7. Flowchart Praproses Menggunakan Kalman Filter

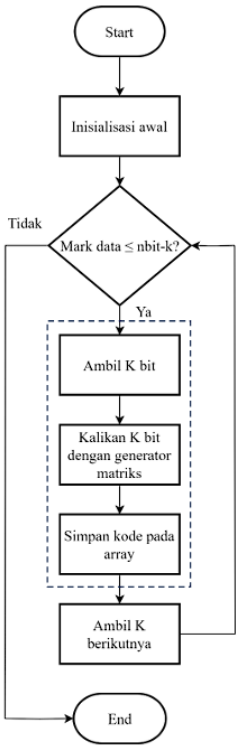
7.3.3 Proses Kuantisasi Multibit

Proses konversi data dari nilai dBm ke bentuk multibit dengan metode kuantisasi adaptive yaitu memastikan bahwa kunci yang dihasilkan aman dan memiliki entropi yang tinggi dengan memanfaatkan perubahan lingkungan atau data input untuk menghasilkan bit-bit kunci yang adaptif dan sulit diprediksi.. Flowchart dari proses kuantisasi dapat dilihat pada Gambar 8.

```
Range = Max(R)-Min(R)
Interval = Range 16
K1=blank_string
 For i = 1 to length (R) do
            For j = 0 to15 do
                        If (R[i]>Min(R)+j*interval)&(R[i]<=Min(R)+(j+1)*interval) then
                              temp Graycode(j)
                              K1+=temp
                  End if
            End for
endfor
```

7.3.3 Proses Rekonsiliasi

Setelah dilakukan proses kuantisasi akan dilakukan proses rekonsiliasi. Pada proses ini pada bit-bit yang tidak sesuai antar user akan diperbaiki. Teknik yang digunakan dalam proses ini menggunakan BCH error correction code yang mampu melakukan koreksi terhadap blok-blok kode yang tidak sama. Dalam proyek akhir ini menggunakan metode error correcting dengan kode BCH. Flowchart dari BCH error correcting code dapat dilihat pada Gambar 9.

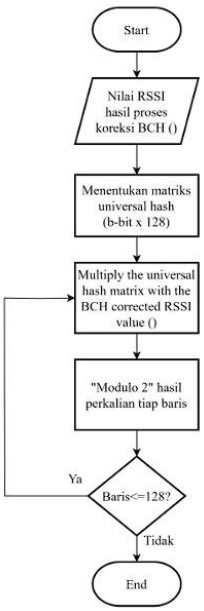


Gambar 8. Flowchart BCH Error Correcting Code

7.3.3 Proses Privacy Amplification

a. Universal Hash

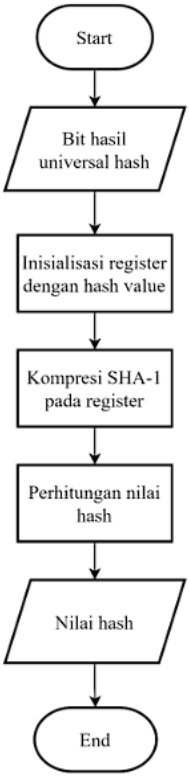
Setelah dilakukan proses correcting code menggunakan BCH selanjutnya terdapat proses untuk memenuhi syarat pembangkitan kunci rahasia, yaitu proses Universal Hash. Sehingga tingkat entropy dari bit yang akan digunakan sebagai kunci akan meningkat. Flowchart Universal Hash dapat dilihat pada Gambar 10.



Gambar 9. Flowchart *Universal Hash*

b. SHA-1

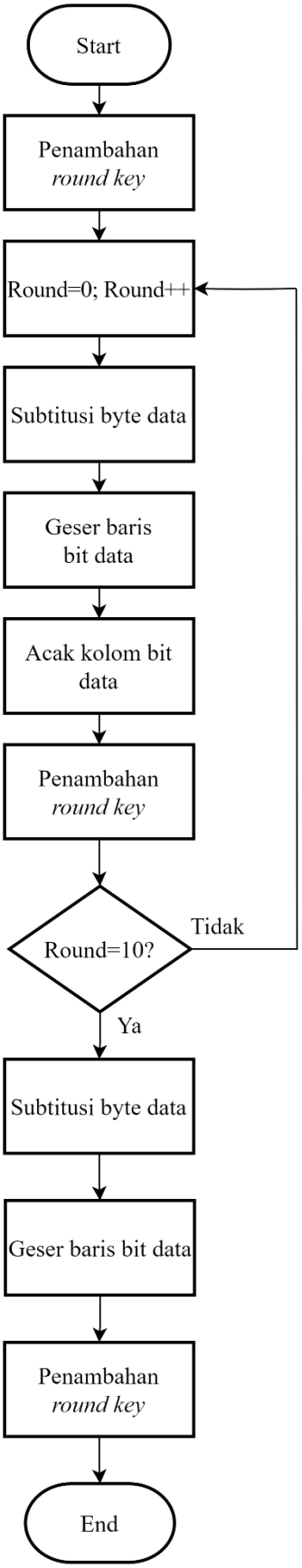
Setelah dilakukan proses universal hash selanjutnya kunci yang memiliki approximate entropy tertinggi digunakan dalam algoritma SHA-1 untuk meningkatkan keamanan sistem. SHA-1 digunakan karena kunci yang dibangkitkan sepanjang 128 bit. Setelah dilakukan proses SHA-1 akan dihasilkan sebuah nilai yang akan dikirim dari Node ke Gateway untuk dilakukan verifikasi kecocokan nilai hash yang terbentuk. Untuk flowchart proses SHA-1 seperti terlihat pada Gambar 11.



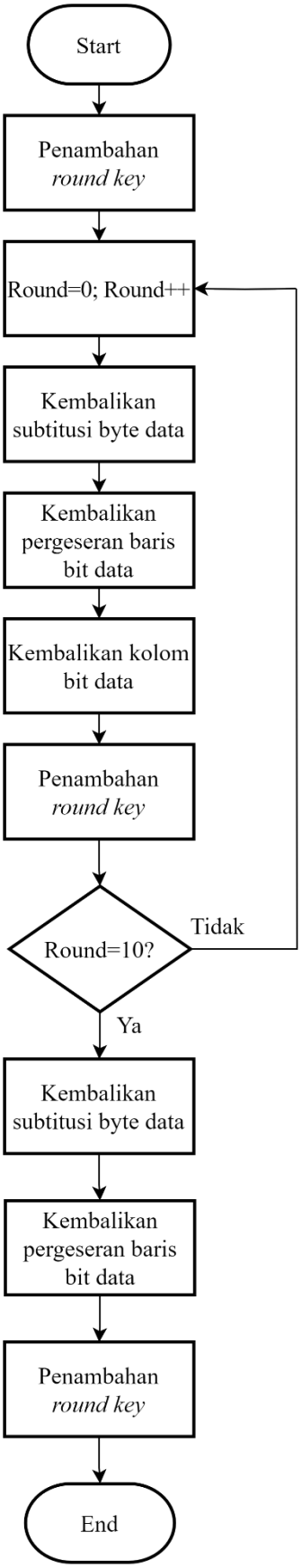
Gambar 10. Flowchart SHA-1

7.3.3 Proses Enskripsi dan Deskripsi

Setelah didapatkan hasil dari proses privacy amplification selanjutnya dilakukan proses enkripsi dan menggunakan skema AES-128. Proses enkripsi AES terdiri 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumn dan AddRoundKey. Enkripsi dilakukan menggunakan kunci yang telah lolos uji NIST dan terverikasi SHA-1. Hasil dari proses enkripsi yaitu berupa Chipertext yang dikirimkan pada Gateway. Flowchart dari enkripsi AES-18 dapat dilihat pada Gambar 12 dan deskripsi AES-128 pada Gambar 13.



Gambar 11. Flowchart Enkripsi AES-128



Gambar 12. Flowchart Deskripsi AES-128

7.4 Implementasi Sistem

Sistem yang telah dibuat perlu diuji untuk mengetahui tingkat kehandalan sistem dan tingkat kerahasiaan dari kunci yang telah dibangkitkan dari serangkaian proses yang telah dilakukan. Pengujian sistem pada Proyek Akhir ini adalah sebagai berikut:

7.4.1 Pengujian Performansi

Pengujian performansi dilakukan untuk menganalisa dan mengevaluasi dari metode yang digunakan pada sistem dalam pembuatan Proyek Akhir ini. Pengujian performansi meliputi beberapa bagian sebagai berikut.

a. Korelasi

Tujuan dari pengujian korelasi adalah untuk mengetahui tingkat kemiripan data RSSI antara Alice dan Bob. Pengujian ini dilakukan setelah melakukan pengukuran RSSI pada masing-masing user serta setelah dilakukan tahapan praproses sehingga akan diketahui karakteristik dari metode yang digunakan, apabila nilai korelasinya semakin tinggi maka tingkat kemiripan data RSSI antara Alice dan Bob juga semakin tinggi.

b. *Key Generation Rate* (KGR)

Tujuan dari pengujian *Key Generation Rate* (KGR) adalah untuk mengetahui jumlah bit yang dihasilkan dalam satu detik/pengukuran. Pengujian KGR akan dilakukan setelah proses kuantisasi, proses *error correcting* dan proses *privacy amplification*. Sehingga nantinya akan diketahui jumlah bit per detik yang dihasilkan pada setiap proses tersebut.

c. *Key Disagrement Rate* (KDR)

Tujuan dari pengujian *Key Disagrement Rate* (KDR) adalah untuk mengetahui presentase perbedaan bit Alice dan Bob. Proses pengujian ini dilakukan setelah metode kuantisasi.

d. *Randomness* (Keacakan)

Untuk menguji *randomness* (keacakan) dilakukan oleh NIST Statistical Test Suite dimana kunci tersebut akan digunakan sebagai key untuk proses enkripsi dan dekripsi dengan AES. Terdapat enam parameter penting dalam ini yaitu:

1) *Frequency (Monobit) Test*

Tujuan tes ini adalah untuk mengetahui apakah jumlah bit 0 dan 1 hampir sama. Jika jumlah bit 0 dan 1 sama persis, maka nilai P-value adalah 1, atau nilai sempurna.

2) *Frequency Test within a Block*

Tujuan dari tes ini adalah proporsi dari bit 1 dalam Mbit blok. Tujuan dari tes ini adalah untuk mengetahui frekuensi dari bit 1 dalam M-bit blok sekitar M/2. Untuk ukuran blok M=1, maka yang digunakan adalah tes pertama, tes frekuensi (monobit).

3) *Runs Test*

Tujuan dari tes ini adalah pada jumlah runs pada sekuen, dimana run adalah uninterrupted sequence dari bit-bit yang identik. Tujuan dari tes ini adalah untuk mengetahui apakah jumlah runs dari bit 0 dan 1 dengan panjang bit yang bervariasi memenuhi persyaratan untuk dianggap sebagai *random sequence*.

4) *Longest Runs of Ones in a Block*

Tujuan dari tes ini untuk mengetahui apakah sekuen yang diuji konsisten terhadap panjang dari run dari bit 1 yang diharapkan dalam *random sequence*.

5) *Approximate Entropy*

Tujuan dari tes ini adalah frekuensi dari semua kemungkinan *overlapping* dari m-bit patterns sepanjang sekuen. Tujuan dari tes ini adalah membandingkan frekuensi dari *overlapping block* dari 2 panjang sekuen yang berurutan (m dan m+1) dibandingkan hasil yang diharapkan dari *random sequence.*

6) *Cumulative Sums*

Tujuan dari tes ini adalah untuk mengetahui apakah cumulative sum dari sekuen parsial pada sekuen yang diuji terlalu besar atau kecil dibandingkan dari tren yang diharapkan.

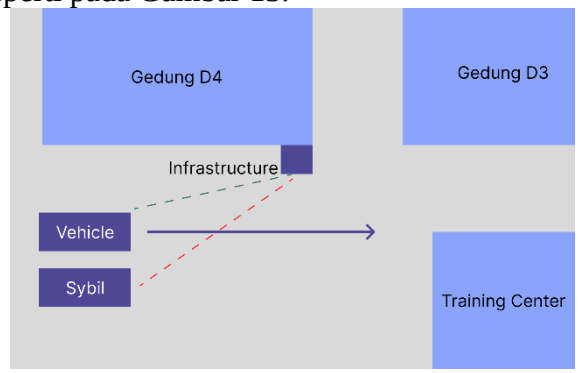
e. Akurasi

Tujuan dari pengujian akurasi adalah untuk mengetahui tingkat keberhasilan sistem dibandingkan dengan sistem yang telah dibuat pada proyek akhir sebelumnya.

7.4.1.1 Skenario Kecepatan Kendaraan

1. Kecepatan Kendaraan kencang

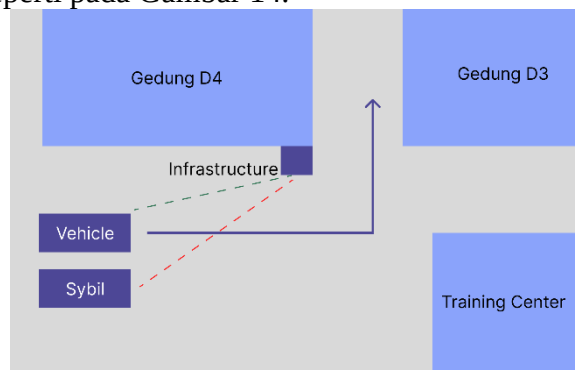
Pada pengujian pertama pada kondisi kendaraan berjalan dengan kecepatan 50Km/jam yang dilakukan di gedung area PENS dengan kondisi kendaraan berjalan lurus dengan ada *Insider Sybil Attacker* seperti pada Gambar 13.



Gambar 13. Skenario kecepatan kendaran 40Km/Jam

2. Kecepatan Kendaraan Pelan

Pada pengujian pertama pada kondisi kendaraan berjalan dengan kecepatan 30Km/jam yang dilakukan di gedung area PENS dengan kondisi kendaraan berbelok kiri dan ada *Insider Sybil Attacker* seperti pada Gambar 14.



Gambar 14. Skenario kecepatan kendaran 60Km/Jam

7.4.2 Waktu Komputasi

Waktu komputasi merupakan waktu yang dibutuhkan untuk memproses sistem mulai dari channel probing hingga proses enkripsi dan dekripsi pesan. Sehingga untuk pengujian komputasi akan dilakukan pada setiap pengukuran.

7.4.3 Insider Attack Sybil

Insider attack merupakan salah satu tipe serangan yang menargetkan suatu jaringan atau sistem computer oleh seseorang yang memahami akses sistem. Tipe serangan ini biasanya dilakukan oleh pelaku yang sudah familiar dan mengetahui arsitektur jaringan yang digunakan pada proses komunikasi data.

Tujuan dari insider adalah mencuri data sensitive. Teknik yang digunakan dalam proyek akhir ini adalah Sybil attack. Pelaku penyerangan dengan metode Sybil Attack akan menggunakan identitas tiruan untuk menyerang keseluruhan sistem[15]. Dimana pelaku akan menggunakan informasi yang melewati kanal udara yang dapat diakses menggunakan aplikasi seperti wireshark, tujuan khusus penyerangan ini adalah untuk mencuri informasi kunci rahasia.

7.5 Hasil dan Analisa

Pada tahap ini dilakukan analisa hasil kinerja sistem dengan parameter pengujian, karakteristik data, waktu dan tempat pengujian, hasil pengujian dan analisa pengujian.

7.6 Kesimpulan dan Saran

Dari analisa yang telah dilakukan pada tahap sebelumnya maka selanjutnya, dibuat kesimpulan dari hasil penelitian yang telah dilakukan dan memberikan saran untuk penelitian berikutnya.

8. Hasil Yang Diharapkan

Hasil yang diharapkan pada pengerjaan proyek akhir ini adalah sistem pembangkitan kunci rahasia yang optimal untuk keamaan proses pertukaran informasi dan komunikasi pada perangkat IoT.

9. Relevansi

Hasil dari proyek akhir ini merupakan sistem pembangkitan kunci rahasia yang dapat diimplementasikan pada perangkat IoT. Sehingga dapat meningkatkan keamaan proses pertukaran informasi dan komunikasi.

10. Jadwal Kegiatan

No	Kegiatan	Bulan ke-											
		1	2	3	4	5	6	7	8	9	10	11	12
1	Studi Literatur												
2	Perancangan Sistem												
3	Pembuatan Sistem												
4	Pengujian dan Analisa												
5	Penyusunan Laporan												
6	Evaluasi Bulanan												

11. Rencana Pembiayaan

Rincian rencana pembiayaan dapat dilihat pada Tabel 3.

Tabel 3. Rencana Pembiayaan

No.	Uraian	Jumlah	Harga Satuan	Total
1.	Lora AcSIP EK-S76SXB	1 Buah	Rp 1.500.000,-	Rp 1.500.000,-
2.	Raspberry Pi	1 Buah	Rp 2.250.000,-	Rp 2.250.000,-
3.	RAK2245 LoRaWAN *Gateway*	1 Buah	Rp 3.697.000,-	Rp 3.697.000,-
4.	Pembuatan Proposal	3 Buah	Rp 12.000,-	Rp 36.000,-
5.	Pembutan Buku PA	3 Buah	Rp 80.000,-	Rp 240.000,-
Total				Rp 7.723.000,-

12. Daftar Pustaka

[1] Istiqomah, N., Yuliana, M., dan Santoso, T. B. "*Mekanisme Peningkatan Reciprocity Channel Probing Pada LoRaWAN Menggunakan Savitzky Golay Filter*", Jurnal Komputer Terapan Vol. 8, No. 1, Mei 2022, 168 – 177.

[2] The Things Network User (2018, Februari 28). Diambil dari https://www.thethingsnetwork.org/community/jakarta/post/review-lora-dengan-acsip-ek-s76sxb.

[3] Riadi, M. (2020, Desember 17). Diambil dari https://www.kajianpustaka.com/2020/12/Raspberry-Pi.html.

[4] Purnamasari, D. P, Saputro, A. K. "*Sistem Penentuan Posisi Dalam Ruangan Berdasarkan Receive Signal Strength Indicator* (RSSI)", Jurnal Simantec Vol. 11, No. 1 Desember 2022.

[5] E. Supriyanto, "*Perancangan dan Implementasi Encoder Decoder Kode Bch (15,7) Berbasis Fpga (Field Programmable Gate Array)*", Universitas Telkom Bandung, 2011.

[6] Thakur, D. "*SHA-1 – What is Secure Hash Algorithm-l (SHA-1)?*" Networking Security

[7] Muharram, F., Azis, H., Manga, A. R. "*Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)*", Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi Vol. 3, No. 2, Desember 2018 e-ISSN 2540-7902 dan p-ISSN 2541-366X

[8] Zhang, J., Duong, T. Q., Marshall, A., dan Woods, R. "*Key Generation From Wireless Channels: A Review*" IEEE Digital Object Identifier

[9] Visoka, A. M. "*Analisa Keamanan Skema Secret Key Generation (Skg) Di Aplikasi Tracking Posisi Pemindahan Narapidana Dari Insider Attack*", Proyek Akhir. Departemen Elektro. D4 Teknik Telekomunikasi. Politeknik Elektonika Negeri Surabaya. 2019.

[10] Han, B., Peng, S., Wu, C., Wang, X., & Wang, B. (2020). LoRa-Based Physical Layer Key Generation for Secure V2V/V2I Communications.

[11] Yaqoob, I., Ahmed, E., Ahmed, A.I.A., Al-Habsi, N., Jayaraman, P.P., Imran, M., & Guizani, M. (2020). "Secure and reliable vehicular communication for 5G enabled transportation networks,"