Implementasi dan Analisis Performa Algoritma Enkripsi ChaCha20 Berbasis Protokol Komunikasi ESP-NOW Pada Wireless Sensor Network

Disusun oleh:
Naufal Farras Trikusuma
NIM: 215150301111047

PROGRAM STUDI TEKNIK KOMPUTER
DEPARTEMEN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2024

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1 PENDAHULUAN

Pada bab pendahuluan ini berisi penelitian yang berisikan uraian mengenai latar belakang penelitian, rumusan masalah yang diangkat penulis, tujuan dan manfaat penelitian, serta batasan masalah dari lingkup penelitian ini. Pada bab ini terdapat sistematika penulisan mengenai isi secara umum dari setiap bab yang terdapat dalam penelitian ini.

1.1 Latar Belakang

Perkembangan teknologi pada bidang wireless sensor network dalam beberapa tahun terakhir memiliki fungsionalitas yang beragam untuk membantu proses automasi pekerjaan manusia seperti proses untuk pengumpulan data dari sensor, pengendalian sistem secara nirkabel, dan monitoring/pengawasan. Menurut Astuti dan Wibisono (2017), Jaringan Sensor Nirkabel (Wireless sensor network/WSN) merupakan kumpulan jaringan node sensor yang saling berkomunikasi untuk melakukan pemindaian dan pengiriman/penerimaan data secara nirkabel yang memiliki keterbatasan pada sumber daya dan kemampuan komunikasi.

Pada aplikasi WSN, keamanan data merupakan aspek penting yang perlu diperhatikan khususnya pada komunikasi yang dilakukan pada jaringan lokal ataupun internet. Data atau informasi yang ditransmisikan pada beberapa kasus merupakan data privat dan sensitif yang perlu diamankan karena dapat mengakibatkan data breach dan unauthorized access oleh orang yang tidak bertanggung jawab (Sarker et al, 2020). Oleh karena itu, diperlukan penggunaan metode kriptografi seperti menggunakan algoritma enkripsi pada data yang akan ditransmisikan untuk meningkatkan keamanan pada aspek konfidensialitas dan integritas.

Menurut Gunathilake et al (2019) perangkat pada sistem tertanam dan/atau WSN memiliki kapasitas komputasi dan sumber daya yang rendah seperti terbatasnya random access memory (RAM), penyimpanan internal, daya komputasi pada prosesor, dan energi/sumber daya seperti baterai. Perangkat seperti ini tidak dapat mengalokasikan secara besar penggunaan sumber daya komputasi hanya untuk aspek keamanan. Oleh karena itu, diperlukan lightweight cryptography (LWC) yang diharapkan dapat mengeksekusi algoritma kriptografi yang lebih ringan atau dengan penggunaan sumber daya komputasi yang lebih rendah dibandingkan teknik kriptografi konvensional dan masih dapat menyediakan fungsi keamanan yang kuat untuk menanggulangi *security attacks.*

Algoritma enkripsi ChaCha20 adalah stream cipher berkecepatan tinggi yang dirancang oleh D. J. Bernstein pada tahun 2008 sebagai penyempurnaan dari stream cipher Salsa20. ChaCha20 merupakan alternatif algoritma pada Transport Layer Security (TLS) protokol yang bertujuan untuk meningkatkan batas keamanan tanpa mengorbankan kinerja pada platform perangkat lunak namun menghasilkan performa high-throughput stream cipher. (Santis et al, 2017).

Penelitian ini mengangkat masalah keamanan data dan keterbatasan sumber daya pada perangkat dalam aplikasi Wireless Sensor Network (WSN). Solusi yang ditawarkan adalah menganalisis performa algoritma enkripsi ChaCha20 dengan algoritma lainnya pada

protokol komunikasi ESP-NOW berbasis ESP8266. Pengujian meliputi kecepatan enkripsi, dekripsi, serta uji penetrasi seperti sniffing dan *known-plaintext attack* (KPA). Selain itu, penelitian ini juga menilai penggunaan sumber daya pada mikrokontroler, untuk menentukan apakah algoritma ChaCha20 efektif dalam memberikan keamanan pada WSN yang memiliki keterbatasan sumber daya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan diatas, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana performa algoritma ChaCha20 dalam hal waktu komputasi pada perangkat ESP8266?
2. Bagaimana pengaruh penggunaan algoritma enkripsi ChaCha20 terhadap penggunaan sumber daya komputasi pada ESP8266?
3. Bagaimana implementasi algoritma enkripsi ChaCha20 pada protokol komunikasi ESP-NOW dan hasil pengujian algoritma dalam aspek keamanan?

1.3 Tujuan

Adapun beberapa tujuan yang ingin dicapai oleh penulis dari penelitian ini adalah sebagai berikut:

1. Menganalisis dan evaluasi performa algoritma ChaCha20 dalam hal waktu komputasi pada perangkat ESP8266.
2. Menganalisis pengaruh penggunaan algoritma enkripsi ChaCha20 terhadap penggunaan sumber daya komputasi pada ESP8266.
3. Mengetahui implementasi dan evaluasi aspek keamanan algoritma enkripsi ChaCha20 pada protokol komunikasi ESP-NOW.

1.4 Manfaat

Penelitian ini diharapkan dapat bermanfaat bagi para peneliti atau masyarakat terkhusus dalam mengimplementasikan dan menggunakan algoritma keamanan pada sistem WSN. Sehingga pembaca dapat memilih lebih tepat algoritma enkripsi yang lebih hemat sumber daya, cepat, dan aman pada sistem atau penelitian selanjutnya. Selain itu, penulis berharap agar masyarakat yang membaca skripsi ini dapat meningkatkan pemahaman mengenai aspek keamanan yang efisien pada *wireless sensor network*.

1.5 Batasan Masalah

Agar lingkup penelitian ini lebih spesifik dan keterbatasan pengujian maka perlu adanya beberapa batasan masalah, yaitu:

1. Implementasi sistem berupa prototipe menggunakan 3 perangkat ESP8266.
2. Subjek pengujian dalam perbandingan performa algoritma sebanyak 3.

1.6 Sistematika Pembahasan

Pada sistematika pembahasan terdapat penjelasan umum tiap bagian bab yang terdapat dalam penelitian ini. Penelitian ini dibagi pada beberapa bagian bab yang sesuai dengan alur penelitian. Sistematika penulisan skripsi dibagi menjadi beberapa bab, yaitu:

BAB I PENDAHULUAN

Bab ini memiliki beberapa subbab berisikan latar belakang dari penelitian, rumusan masalah dari latar belakang penelitian, tujuan, manfaat, batasan masalah, dan sistematika pembahasan skripsi.

BAB II LANDASAN KEPUSTAKAAN

Bab ini memuat kajian atau tinjauan kepustakaan dan landasan teori dari penelitian sebelumnya. Tinjauan dan landasan teori yang digunakan akan memiliki keterkaitan dengan teori dan implementasi dari penelitian ini sebagai landasan metode dan referensi.

BAB III METODOLOGI PENELITIAN

Bab ini berisikan alur proses dan metode yang akan digunakan dalam penelitian ini. Pada bab III secara lebih spesifik akan dimuat mengenai metode yang akan digunakan oleh penulis seperti diagram alir dan penjelasan prosesnya.

BAB IV REKAYASA KEBUTUHAN

Bab ini memuat pengkajian masalah secara umum, kebutuhan fungsional yang dimiliki sistem meliputi perangkat lunak, perangkat keras, dan alat yang digunakan dalam pengujian.

BAB V PERANCANGAN DAN IMPLEMENTASI

Bab ini berisikan proses perancangan dan implementasi sistem, yaitu bagaimana merancang sistem dari perangkat lunak dan perangkat keras berdasarkan rekayasa kebutuhan seperti membuat blok diagram, skematik, konfigurasi sistem, dan diagram alir hingga proses implementasi sistem.

BAB VI PENGUJIAN DAN ANALISIS

Bab ini berisikan hasil pengujian untuk menganalisis dan mengevaluasi kinerja sistem secara keseluruhan. Pada bab ini juga akan terdapat jawaban daripada rumusan masalah yang ada.

BAB VII PENUTUP

Bab ini memuat kesimpulan dan saran yang didapat setelah penelitian dilakukan berdasarkan hasil pengujian dan analisis. Saran dan kesimpulan penelitian diharapkan dapat meningkatkan penelitian selanjutnya dari hasil penelitian penulis.

Performance Evaluation of IoT Encryption Algorithms: Memory, Timing, and Energy

BAB 2 LANDASAN KEPUSTAKAAN

Landasan kepustakaan berisi uraian dan pembahasan tentang teori, konsep, model, metode, atau sistem dari pustaka ilmiah, yang berkaitan dengan tema, masalah, atau pertanyaan penelitian. Dalam landasan kepustakaan terdapat landasan teori dari berbagai sumber pustaka yang terkait dengan teori dan metode yang digunakan dalam penelitian. Jika dibutuhkan sesuai dengan karakteristik penelitiannya dan syarat kecukupan khusus keminatan tertentu, bisa juga terdapat kajian pustaka yang menjelaskan secara umum penelitian-penelitian terdahulu yang berhubungan dengan topik skripsi dan menunjukkan persamaan dan perbedaan skripsi tersebut terhadap penelitian terdahulu yang dituliskan.

2.1 Tinjauan Kepustakaan

Pada saat dimulai penelitian, penulis meninjau beberapa literatur dan jurnal yang berhubungan/berkaitan dengan penelitian untuk mendapatkan informasi dan referensi dalam penelitian ini. Berikut adalah isi dari kajian pustaka yang berisikan penelitian-penelitian sebelumnya, dapat dilihat pada Tabel.2.1.

Tabel 2.1 Daftar Tinjauan Pustaka

No.	Nama Penulis (Tahun), Judul Penelitian	Persamaan Penelitian	Perbedaan	
			Penelitian Sebelumnya	Penelitian Sekarang
1	Maitra et al (2019) "Performance Evaluation of IoT Encryption Algorithms: Memory, Timing, and Energy."	Menggunakan algoritma enkripsi pada WSN dalam pengujian performa sebagai subjek penelitian.	Menggunakan PIC18F27K40 8-bit, pengujian performa algoritma AES pada kecepatan komputasi, penggunaan memori, dan energi.	Menggunakan ESP8266, pengujian performa algoritma chacha20 pada penggunaan kecepatan dan sumber daya komputasi.

2	Iman et al (2022) "Implementasi Algoritme Clefia 128-Bit untuk Pengamanan Modul Komunikasi Lora. "	Menggunakan algoritma enkripsi pada WSN dan pengujian keamanan algoritma sebagai subjek penelitian.	Menggunakan arduino uno, modul LoRa, pengujian algoritma clefia 128-bit.	Menggunakan ESP8266 dan protokol ESP-NOW, pengujian performa algoritma chacha20.
3	Pratama et al (2021), "Implementasi Algoritma Enkripsi Snow-V pada Wireless Sensor Network (WSN)"	Menggunakan algoritma enkripsi pada WSN, pengujian performa dan keamanan algoritma sebagai subjek penelitian.	Menggunakan arduino uno, modul nRF24L01, pengujian performa algoritma snow-v.	Menggunakan ESP8266 dan protokol ESP-NOW, pengujian performa algoritma chacha20

2.1.1 Implementation and Performance Analysis of AES-128 CBC algorithm in WSNs

Penelitian ini dilakukan oleh Maitra et al (2019,) yang berjudul ”Performance Evaluation of IoT Encryption Algorithms: Memory, Timing, and Energy” merupakan penelitian mengenai evaluasi performa algoritma enkripsi pada IoT khususnya pada aspek kecepatan, penggunaan memori, dan energi. Hasil pengujian pada riset ini menghasilkan kesimpulan bahwa penggunaan algoritma AES pada perangkat mikrokontroler yang memiliki keterbatasan sumber daya tidak *feasible* atau kurang cocok jika dibandingkan dengan algoritma yang lebih ringan seperti XTEA yang dari sisi pengujian yang lebih efisien pada aspek daya. Namun algoritma XTEA tidak dapat dibandingkan secara level keamanan dengan AES yang merupakan algoritma modern.

2.1.2 Implementasi Algoritme Clefia 128-Bit untuk Pengamanan Modul Komunikasi Lora.

Penelitian yang dilakukan Muhammad Fadhil Iman et al (2022), dengan judul ”Implementasi Algoritme Clefia 128-Bit Untuk Pengamanan Modul Komunikasi LoRa” adalah implementasi algoritma enkripsi clefia 128-bit pada modul LoRa yang tidak memiliki sistem keamanan untuk melindungi aspek konfidesialitas pada suatu data yang di transmisikan. Pada implementasi ini sistem diuji dengan berbagai pengujian seperti tes vektor, uji serangan aktif seperti *known-plaintext-attack (*KPA), dan uji serangan pasif seperti *sniffing.* Secara umum implementasi sistem dari algoritma ini mampu melewati pengujian yang dilakukan dengan baik. Pengujian pada riset ini hanya terkhusus pada aspek keamanan data, aspek lain seperti kecepatan komputasi dan penggunaan sumber daya tidak di uji. Oleh karena itu, diperlukan pengujian lebih lanjut mengenai performa algoritma ini karena salah satu tantangan utama dari sistem WSN adalah terbatasnya sumber daya yang memengaruhi *lifetime* dari sistem.

2.1.3 Implementasi Algoritma Enkripsi Snow-V pada Wireless Sensor Network (WSN)

Penelitian selanjutnya yang dilakukan Yulius Adi Pratama et al (2021), dengan judul ”Implementasi Algoritma Enkripsi Snow-V pada Wireless Sensor Network (WSN)”. Penelitian ini dilakukan untuk mengimplementasikan salah satu algoritma enkripsi snow-v yang berbasis Arduino Uno dan modul komunikasi nRF24L01. Pada penelitian disebutkan bahwa selain implementasi dilakukan juga proses pengujian seperti tes vektor untuk memastikan aspek *availability* data, uji *sniffing* saat data berjalan di jalur komunikasi, dan menghitung waktu komputasi enkripsi dan dekripsi yang berturut-turut rata-rata waktunya 241ms dan 185ms. Dalam konteks kecepatan komputasi, waktu yang didapatkan algoritma ini dalam keseluruhan proses enkripsi dapat mencapai ±426ms yang dapat memberikan delay yang cukup signifikan yang dimana delay lain seperti proses komunikasi, proses akuisisi data sensor belum termasuk. Selanjutnya, pada penelitian ini peneliti belum menguji penggunaan sumber daya komputasi yang digunakan saat proses

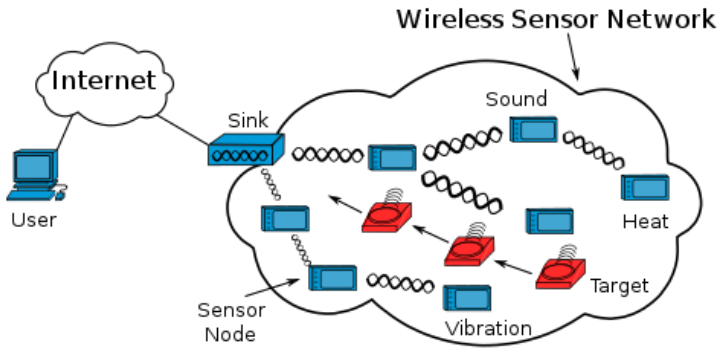
enkripsi, yang dimana aspek efisiensi daya menjadi hal utama dalam konsep wireless sensor network.

2.2 Dasar Teori

Pada dasar teori akan dijelaskan teori-teori yang digunakan dalam mengimplementasikan penelitian ini. Dengan adanya pengertian, persamaan, dan cara kerja yang diharapkan dapat sebagai penunjang pemahaman dalam penelitian.

2.2.1 Wireless Sensor Network

Jaringan Sensor Nirkabel (Wireless sensor network) merupakan kumpulan jaringan *node* sensor yang saling berkomunikasi untuk melakukan pemindaian dan pengiriman/penerimaan data secara nirkabel yang memiliki keterbatasan pada sumber daya dan kemampuan komunikasi (Astuti dan Wibisono, 2017).



Gambar 2.1 Wireless Sensor Network

(Sumber: commons.wikimedia.org)

2.2.2 Kriptografi

Kriptografi adalah konsep penyandian yang digunakan untuk menjaga kerahasiaan data, sehingga hanya pihak yang berwenang yang dapat mengetahui informasi dari data tersebut. Dalam kriptografi, data asli (plaintext) akan dienkripsi menjadi ciphertext dan kemudian didekripsi kembali menjadi plaintext ketika diterima oleh pihak yang berhak. Saat ini, algoritma modern banyak digunakan untuk mengamankan data, yang secara umum dibagi menjadi dua jenis, yaitu stream ciphers dan block ciphers. Stream ciphers bekerja dengan melakukan operasi XOR antara keystream dan plaintext untuk menghasilkan ciphertext. (Qadir dan Varol, 2019).

2.2.3 Algoritma ChaCha20

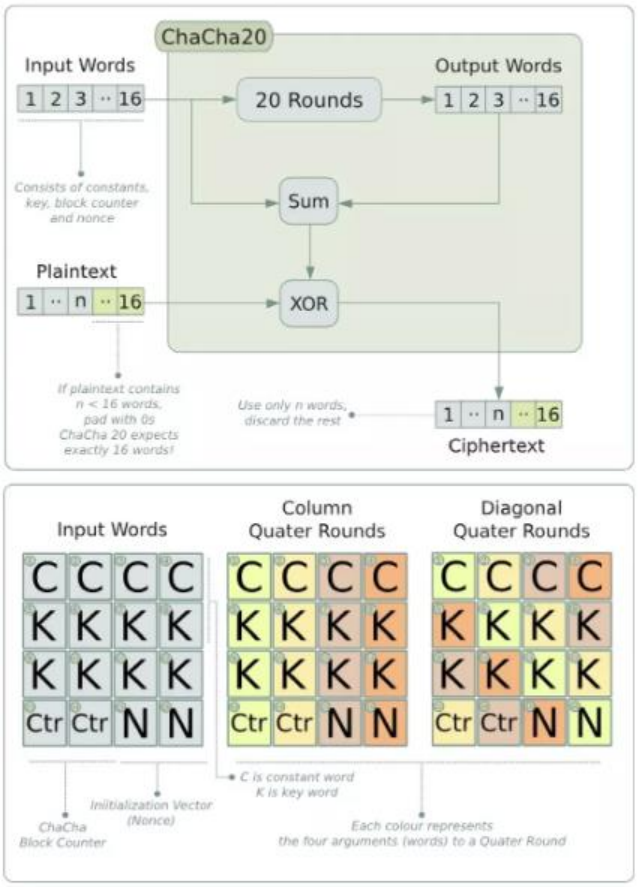
ChaCha20 adalah stream cipher berkecepatan tinggi yang dirancang oleh D. J. Bernstein pada tahun 2008 sebagai penyempurnaan dari stream cipher Salsa20. ChaCha20 merupakan alternatif algoritma pada *Transport Layer Security* (TLS) protokol yang bertujuan untuk meningkatkan batas keamanan tanpa

mengorbankan kinerja pada platform perangkat lunak namun menghasilkan performa *high-throughput stream cipher*. (Santis et al, 2017).

Menurut Procter (2014), ChaCha akan membuat *keystream* menggunakan blok fungsi ChaCha20 pada kunci, *nonce,* dan *counter block.* Persamaan blok fungsi ChaCha20 adalah berikut:

$$\mathrm{CC} : \{0,1\}^{256} \times \{0,1\}^{32} \times \{0,1\}^{96} \rightarrow \{0,1\}^{512} \tag{2.1}$$

Diatas adalah blok fungsi ChaCha20 yang memiliki input 32-byte kunci, 4-byte blok angka, 12-byte *nonce,* dan 64 *pseudo-random* bytes output.



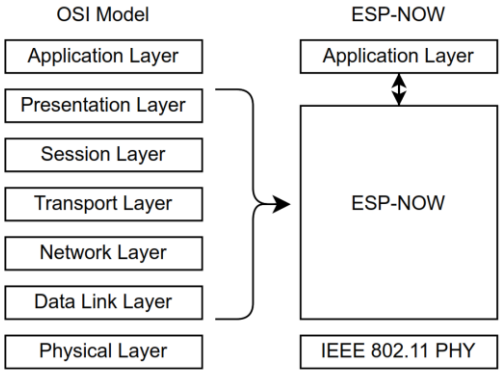
Gambar 2.2 Cara Kerja ChaCha20

(Sumber: datatracker.ietf.org)

2.2.4 Protokol ESP-NOW

ESP-NOW merupakan protokol komunikasi nirkabel sebagai solusi untuk *low cost* dan *low power* protokol untuk perangkat IoT yang berjalan pada frekuensi 2.4 GHz *Industrial, Scientific, and Medical* (ISM) spektrum. ESP-NOW memungkinkan banyak perangkat berkomunikasi secara 2 arah, yang secara teoritis jangkauan sinyal dapat lebih baik hingga 15 kali daripada *Bluetooth Low Energy* (BLE).

Pada *physical layer* protokol ini berjalan secara *native* pada standar IEEE802.11 ESP-NOW memerlukan alamat *Medium Access Protocol* (MAC) dari tiap perangkat untuk melakukan komunikasi, pada MAC layer digunakan metode *Carrier Sense Multiple Access/Collision Avoidance* (CSMA/CA) untuk mencegah terjadinya tabrakan ataupun data yang tidak terkirim karena adanya komunikasi lain pada jalur atau satu waktu yang sama. (Urazayev et al, 2023).



Gambar 2.3 ESP-NOW Layer

(Sumber: (Urazayev et al, 2023))

BAB 3 METODOLOGI

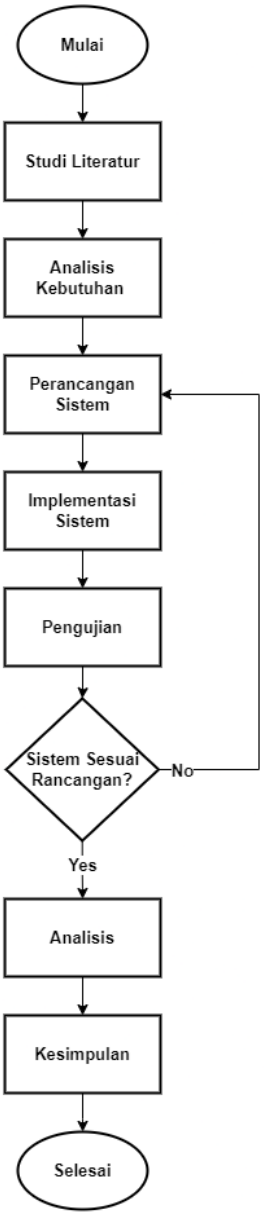
Pada bab ketiga atau bab metodologi dalam penelitian ini, penulis akan membahas beberapa sub-bab. Pertama, akan dijelaskan tentang tipe penelitian yang digunakan dalam penelitian ini. Selanjutnya, akan terdapat metode penelitian melalui sebuah diagram alir. Terakhir, penulis akan mencantumkan peralatan yang mendukung jalannya penelitian.

3.1 Tipe Penelitian

Penelitian ini dilakukan dengan tipe penelitian implementatif - pengembangan pada bidang rekayasa sistem komputer (RSK). Tipe penelitian ini berfokus pada implementasi analisis performa algoritma enkripsi ChaCha20 pada WSN dengan pengembangan jenis pengujian dan perbandingan dengan algoritma lain yang menghasilkan prototipe dan hasil analisis sistem secara komperehensif.

3.2 Metode Penelitian

Metode penelitian yang digunakan penulis akan dijelaskan dalam bentuk diagram alir yaitu pada gambar 3.1 dan penjelasan tiap langkahnya secara spesifik untuk mencapai tujuan penelitian.



Gambar 3.1 Diagram Alir Penelitian

3.2.1 Studi Literatur

Tahap studi literatur oleh penulis dilakukan dengan *literature review* dan meninjau terhadap kepustakaan yang memiliki keterkaitan dengan topik untuk menyusun dasar teori dalam memenuhi kebutuhan penelitian, lalu untuk mengimplementasikan beberapa metode berdasarkan jurnal-jurnal yang dicatut. Terdapat beberapa literatur berupa jurnal, buku, ataupun sumber lainnya mengenai aspek-aspek seperti *wireless sensor network,* kriptografi, algoritma ChaCha20, dan protokol komunikasi ESP-NOW yang akan digunakan sebagai dasar dalam penelitian ini.

3.2.2 Rekayasa Kebutuhan

Tahap selanjutnya adalah melakukan analisis terhadap kebutuhan sistem yang akan diimplementasikan agar penelitian ini dapat dilakukan. Penulis melakukan perencanaan kebutuhan perangkat keras dan perangkat lunak yang akan digunakan selama proses implementasi, pengujian, hingga analisis sistem. Berikut merupakan kebutuhan yang akan digunakan dalam penelitian.

Kebutuhan perangkat keras:

1. ESP8266
2. Sensor arus dan daya INA219
3. Sensor suhu dan kelembapan DHT22
4. Baterai 9V
5. Kabel USB dan Jumper
6. Power Supply DC

Kebutuhan perangkat lunak:

1. Arduino IDE
2. Library algoritma enkripsi ChaCha20
3. Library sensor INA219 dan DHT

3.2.3 Perancangan dan Implementasi Sistem

Pada tahap ini dilakukan perancangan perangkat keras maupun lunak sistem berdasarkan rekayasa kebutuhan. Pada perancangan perangkat keras pembuatan diagram skematik yang tersusun dari ESP8266, sensor DHT22 dan komponen pengujian sumber daya komputasi seperti seperti sensor INA219 dan power supply dc. Selanjutnya, perancangan perangkat lunak adalah dengan menyusun kode program untuk menjalankan dan pengujian sistem. Setelah dilakukan perancangan, dilakukan implementasi dengan mengintegrasikan perangkat lunak dan perangkat keras yang telah disusun seperti pengunggahan kode program dan *wiring* pada komponen perangkat keras.

3.2.4 Pengujian

Tahap pengujian akan implementasi sistem berfungsi untuk mengetahui fungsionalitas kesuluruhan sistem dan mengumpulkan data guna menyelesaikan rumusan masalah yang telah disusun. Pengujian yang akan dilakukan adalah uji tes vektor pada algoritma enkripsi untuk memvalidasi kerja algoritma, uji performa algoritma khususnya pada kecepatan komputasi dan penggunaan sumber daya komputasi seperti penggunaan memori, daya/energi yang digunakan saat melakukan proses enkripsi dan dekripsi. Lalu dilakukan pengujian pada aspek keamanan dengan melakukan uji serangan pasif (sniffing) dan uji serangan aktif (known-plaintext attack) untuk melihat kerentanan pada algoritma enkripsi. Pengujian akan dilakukan pada beberapa algoritma sekaligus sebagai komparasi,

yaitu algoritma ChaCha20, Clefia, AES, dan Snow-V yang dimana semua menggunakan 256-bit key.

3.2.5 Analisis Hasil Pengujian

Selanjutnya pada tahap analisis akan dilakukan pengolahan data hasil uji dan menampilkan hasil pengujian sistem yang telah dikerjakan sebelumnya dengan analisis dan perbandingan terhadap pengujian dengan algoritma lain untuk melihat keseluruhan performa pada masing-masing algoritma.

3.2.6 Kesimpulan dan Saran

Pada akhir penelitian ini, penulis akan menyimpulkan temuan yang menjawab pertanyaan pada rumusan masalah. Kesimpulan ini didasarkan pada hasil pengujian yang telah diperoleh. Selain itu, penulis juga memberikan beberapa saran agar penelitian dengan topik serupa dapat dikembangkan lebih lanjut di masa depan.

DAFTAR REFERENSI

Astuti, L.D. and Wibisono, W., 2017. Peningkatan Networklifetimepada Wireless Sensor Network Menggunakan Clustered Shortest Geopath Routing (C-SGP) Protocol. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 4(3), pp.148-15.

De Santis, F., Schauer, A. and Sigl, G., 2017, March. ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications. In Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017 (pp. 692-697). IEEE.

Gunathilake, N.A., Buchanan, W.J. and Asif, R., 2019, April. Next generation lightweight cryptography for smart IoT devices:: implementation, challenges and applications. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (pp. 707-710). IEEE.

Iman, M.F., Kusyanti, A. and Primananda, R., 2022. Implementasi Algoritme Clefia 128-Bit untuk Pengamanan Modul Komunikasi Lora. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 9(7).

Kane, L. E., Chen, J. J., Thomas, R., Liu, V., & Mckague, M. (2020). Security and performance in IoT: A balancing act. *IEEE access*, *8*, 121969-121986.

Lee, Hyeopgeon, Kyounghwa Lee, and Yongtae Shin. "Implementation and Performance Analysis of AES-128 CBC algorithm in WSNs." In 2010 The 12th International Conference on Advanced Communication Technology (ICACT), vol. 1, pp. 243-248. IEEE, 2010.

Maitra, S., Richards, D., Abdelgawad, A., & Yelamarthi, K. (2019, March). Performance evaluation of IoT encryption algorithms: memory, timing, and energy. In *2019 IEEE sensors applications symposium (SAS)* (pp. 1-6). IEEE.

Pratama, Y. A., Budi, A. S., & Kusyanti, A. (2021). Implementasi Algoritma Enkripsi Snow-V pada Wireless Sensor Network (WSN). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 5(10), 4689-4697.

Qadir, A.M. and Varol, N., 2019, June. A review paper on cryptography. In 2019 7th international symposium on digital forensics and security (ISDFS) (pp. 1-6). IEEE.

Sarker, V.K., Gia, T.N., Tenhunen, H. and Westerlund, T., 2020, June. Lightweight security algorithms for resource-constrained IoT-based sensor nodes. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-7). IEEE.

Urazayev, D., Eduard, A., Ahsan, M., & Zorbas, D. (2023, May). Indoor performance evaluation of ESP-NOW. In 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST) (pp. 1-6). IEEE