ANALISIS DAN IMPLEMENTASI KEAMANAN PADA SISTEM PEMANTAUAN SUHU DAN KELEMBAPAN GUDANG BERBASIS *IOT* MENGGUNAKAN ALGORITMA SPECK STUDI KASUS : GUDANG PT CITRA PRATAMA DISTRIBUSIINDORAYA

TUGAS AKHIR

Rafi Antaresa
2101020079

PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2026

ANALISIS DAN IMPLEMENTASI KEAMANAN PADA SISTEM PEMANTAUAN SUHU DAN KELEMBAPAN GUDANG BERBASIS *IOT* MENGGUNAKAN ALGORITMA SPECK STUDI KASUS : GUDANG PT CITRA PRATAMA DISTRIBUSIINDORAYA

Tugas Akhir
Skema Skripsi

Usulan Tugas Akhir diajukan sebagai salah satu persyaratan memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika

Rafi Antaresa
2101020079

PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2026

PERNYATAAN MENGENAI TUGAS AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa tugas akhir berjudul "Analisis dan Implementasi Keamanan Pada Sistem Pemantauan Suhu dan Kelembapan Gudang Berbasis *IOT* Menggunakan Algoritma SPECK Studi Kasus : Gudang PT Citra Pratama Distribusiindoraya" adalah benar karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Apabila di kemudian hari terbukti pernyataan saya tidak benar dan melanggar peraturan yang berlaku dalam karya tulis dan hak intelektual, maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji dan menerima sanksi lainnya sesuai dengan peraturan yang berlaku. Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Universitas Maritim Raja Ali Haji.

Tanjungpinang, Januari 2026

Rafi Antaresa
NIM 2101020079

HALAMAN PERSETUJUAN

Judul	:	Analisis dan Implementasi Keamanan Pada Sistem Pemantauan Suhu dan Kelembapan Gudang Berbasis *IOT* Menggunakan Algoritma SPECK Studi Kasus : Gudang PT Citra Pratama Distribusiindoraya
Nama	:	Rafi Antaresa
NIM	:	2101020079
Program Studi	:	Teknik Informatika
Tanggal Persetujuan	:	13 Januari 2026

Disetujui oleh,

Komisi Pembimbing

Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D.	**Feri Irawan, S.Kom., M.Kom**
(Ketua)	**(Anggota)**

HALAMAN PENGESAHAN

Judul	:	Analisis dan Implementasi Keamanan Pada Sistem Pemantauan Suhu dan Kelembapan Gudang Berbasis *IOT* Menggunakan Algoritma SPECK Studi Kasus : Gudang PT Citra Pratama Distribusiindoraya
Nama	:	Rafi Antaresa
NIM	:	2101020079

Telah berhasil dipertahankan di hadapan Komisi Penguji sebagai bagian persyaratan yang diperlukan dalam memperoleh gelar sarjana Teknik pada Program Studi Teknik Informatika, Jurusan Teknik Elektro dan Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.

KOMISI PENGUJI

Ketua	:	Ferdi Chahyadi, S.Kom., M.Cs	(.....)
Anggota I	:	Fortia Magfira, M.Kom	(.....)
Anggota II	:	Nolan Efranda, M.Kom	(.....)
Anggota III	:	Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D.	(.....)
Anggota IV	:	Feri Irawan, S.Kom., M.Kom	(.....)

Mengetahui,

Ketua Jurusan Teknik Elektro dan Informatika

Hollanda Arief Kusuma, S.IK., M.Si

NIP. 198904012019031016

Tanggal Ujian : 13 Januari 2026 Tanggal Lulus :

ABSTRAK

RAFI ANTARESA. Analisis dan Implementasi Keamanan pada Sistem Pemantauan Suhu dan Kelembapan Gudang Berbasis *Internet of Things* Menggunakan Algoritma SPECK (Studi Kasus: Gudang PT Citra Pratama Distribusiindoraya). Dibimbing oleh HENDRA KURNIAWAN dan FERI IRAWAN.

Pemantauan suhu dan kelembapan gudang merupakan aspek penting dalam menjaga kualitas barang selama proses penyimpanan. Sistem pemantauan berbasis *Internet of Things (IoT)* memungkinkan pengawasan kondisi lingkungan secara real time, namun *data* yang dikirimkan melalui jaringan memiliki risiko keamanan, seperti penyadapan dan manipulasi *data*. *Internet of Things (IoT)* memungkinkan perangkat *sensor* untuk mengirimkan *data* secara otomatis melalui koneksi internet tanpa interaksi langsung manusia. Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan mekanisme keamanan *data* pada sistem pemantauan suhu dan kelembapan gudang berbasis *IoT* menggunakan algoritma enkripsi SPECK. Sistem dirancang menggunakan mikrokontroler ESP8266 dan *sensor* DHT22 untuk mengukur suhu dan kelembapan, kemudian *data* dienkripsi sebelum dikirimkan ke *server*. Pengujian keamanan dilakukan dengan simulasi serangan *Man in the Middle (MITM)*. Hasil penelitian menunjukkan bahwa penerapan algoritma SPECK mampu melindungi *data* dari upaya penyadapan dan manipulasi selama proses transmisi, serta tetap efisien digunakan pada perangkat dengan keterbatasan sumber daya.

Kata kunci: algoritma SPECK, *Internet of Things (IoT)*, keamanan *data*, suhu dan kelembapan, pemantauan.

ABSTRACT

RAFI ANTARESA. Analysis and Implementation of Security in an Internet of Things-Based Warehouse Temperature and Humidity Monitoring System Using the SPECK Algorithm (Case Study: PT Citra Pratama Distribusiindoraya Warehouse). Supervised by HENDRA KURNIAWAN and FERI IRAWAN.

Warehouse temperature and humidity monitoring is essential to maintain product quality during storage. Internet of Things (IoT)-based monitoring systems enable real-time observation of environmental conditions; however, transmitted *data* are vulnerable to security threats such as interception and manipulation. IoT enables sensor devices to transmit *data* automatically via internet connectivity without direct human interaction. This study aims to analyze and implement *data* security in an IoT-based warehouse temperature and humidity monitoring system using the SPECK encryption algorithm. The system is developed using an ESP8266 microcontroller and a DHT22 sensor to measure temperature and humidity, where the *data* are encrypted before being transmitted to the server. Security testing is conducted through Man in the Middle (MITM) attack simulation. The results show that the implementation of the SPECK algorithm is effective in protecting *data* from interception and manipulation during transmission while remaining efficient for resource-constrained IoT devices.

Keywords: *data* security, Internet of Things (IoT), SPECK algorithm, temperature and humidity, monitoring.

PRAKATA

Puji Puji syukur Segala puji syukur penulis panjatkan ke hadirat Allah SWT, atas limpahan rahmat, karunia, serta hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Analisis dan Implementasi Keamanan pada Sistem Pemantauan Suhu dan Kelembapan Gudang Berbasis *Internet of Things* Menggunakan Algoritma SPECK (Studi Kasus: Gudang PT Citra Pratama Distribusiindoraya)". Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan Program Sarjana (S1) Jurusan Teknik Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.

Dalam perjalanan penyusunan skripsi ini, penulis menyadari bahwa banyak pihak yang telah memberikan dukungan, bantuan, serta bimbingan, baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Prof. Dr. Agung Dhamar Syakti, S.Pi., DEA., selaku Rektor Universitas Maritim Raja Ali Haji.
2. Ibu Martaleli Bettiza, S.Si., M.Sc., selaku Dekan Fakultas Teknik dan Teknologi Kemaritiman Universitas Maritim Raja Ali Haji.
3. Bapak Hollanda Arief Kusuma, S.T., M.Si., selaku Ketua Jurusan Teknik Elektro dan Informatika.
4. Bapak Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D., selaku Dosen Pembimbing I, yang dengan sabar memberikan arahan, nasihat, serta ilmu yang sangat berharga sejak awal hingga selesainya penulisan skripsi ini.
5. Bapak Feri Irawan, S.Kom., M.Kom., selaku Dosen Pembimbing II, yang senantiasa meluangkan waktu untuk memberikan masukan dan motivasi dalam penyusunan karya ini.
6. Seluruh dosen di Fakultas Teknik Universitas Maritim Raja Ali Haji yang telah memberikan ilmu, pengalaman, dan bimbingan selama masa perkuliahan.
7. Staf administrasi Fakultas Teknik Universitas Maritim Raja Ali Haji, yang selalu sigap membantu kelancaran proses akademik dan penelitian.
8. Kedua orang tua tercinta, yang selalu memberikan kasih sayang, doa, semangat, dan dukungan tanpa henti dalam setiap langkah penulis.

9. Seluruh anggota keluarga yang senantiasa memberikan motivasi, perhatian, serta doa terbaik hingga terselesaikannya penelitian ini.
10. Yang terkasih, Chandra Wati yang selalu memberikan dukungan, semangat, perhatian serta doa sehingga penulis mampu menyelesaikan skripsi ini dengan baik.
11. Semua pihak yang tidak dapat penulis sebutkan satu per satu, tetapi telah memberikan dukungan dan bantuan hingga selesainya penulisan skripsi ini.

Penulis menyadari bahwa karya ini masih jauh dari sempurna karena keterbatasan pengetahuan dan kemampuan yang dimiliki. Oleh sebab itu, penulis dengan rendah hati mengharapkan kritik dan saran yang membangun demi perbaikan di masa yang akan datang. Semoga skripsi ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya dalam bidang Teknik Informatika.

Tanjungpinang, Januari 2026

Rafi Antaresa

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi *Internet of Things (IoT)* telah membawa perubahan signifikan dalam berbagai sektor industri, termasuk pada sistem penyimpanan dan distribusi barang. *IoT* memungkinkan perangkat fisik yang dilengkapi *sensor* untuk saling terhubung dan mengirimkan *data* secara *real-time* melalui jaringan *internet*. Penerapan teknologi ini banyak dimanfaatkan dalam sistem pemantauan lingkungan karena mampu meningkatkan efisiensi pengawasan serta mengurangi ketergantungan terhadap proses *manual* yang berpotensi menimbulkan kesalahan pencatatan. Beberapa penelitian terbaru menunjukkan bahwa sistem *monitoring* berbasis *IoT* telah menjadi solusi efektif dalam menjaga stabilitas kondisi lingkungan pada sektor industri dan logistik [1].

Dalam konteks penyimpanan makanan dan minuman, suhu dan kelembapan merupakan parameter lingkungan yang sangat berpengaruh terhadap kualitas dan keamanan produk. Kondisi suhu dan kelembapan yang tidak terkontrol dapat mempercepat pertumbuhan mikroorganisme, menurunkan mutu produk, serta menyebabkan kerusakan kemasan. Oleh karena itu, gudang penyimpanan makanan dan minuman membutuhkan sistem pemantauan yang mampu mengawasi kondisi lingkungan secara kontinu dan akurat. Penelitian terkini menyebutkan bahwa penerapan sistem *monitoring* suhu dan kelembapan berbasis *IoT* pada gudang penyimpanan mampu membantu pengelola dalam menjaga kualitas produk serta meminimalkan risiko kerugian akibat kerusakan barang [2].

Meskipun sistem *IoT* menawarkan berbagai keunggulan, aspek keamanan *data* masih menjadi tantangan yang perlu diperhatikan. *Data sensor* yang dikirimkan melalui jaringan internet berpotensi mengalami ancaman keamanan seperti penyadapan, manipulasi *data*, dan serangan *Man-in-the-Middle (MITM).* Ancaman tersebut dapat menyebabkan informasi yang diterima tidak sesuai dengan kondisi sebenarnya, sehingga berisiko menimbulkan kesalahan dalam pengambilan keputusan. Studi terbaru menegaskan bahwa sistem *IoT* tanpa mekanisme

pengamanan yang memadai memiliki tingkat kerentanan yang cukup tinggi terhadap serangan siber, khususnya pada sistem yang beroperasi secara *real-time* [3].

Penelitian terbaru yang dilakukan menegaskan pentingnya penerapan algoritma kriptografi ringan (*lightweight cryptography*) pada perangkat *Internet of Things (IoT)* yang memiliki keterbatasan daya dan kapasitas pemrosesan. Dalam penelitiannya, mereka mengevaluasi berbagai algoritma kriptografi seperti SPECK, *SIMON, dan PRESENT*, dengan fokus pada efisiensi dan tingkat keamanan dalam lingkungan perangkat *IoT* yang bersumber daya rendah. Hasil penelitian menunjukkan bahwa algoritma SPECK memiliki kinerja yang stabil dengan konsumsi daya yang lebih hemat dibandingkan algoritma lain, tanpa mengorbankan tingkat keamanan *data* [4].

Penelitian lainnya yang dilakukan menganalisis tingkat keamanan algoritma kriptografi ringan seperti *SIMON* dan *SIMECK* yang memiliki struktur dan prinsip kerja serupa dengan algoritma SPECK. Hasil penelitian mereka menunjukkan bahwa algoritma jenis *lightweight block cipher* ini tetap mampu memberikan tingkat keamanan yang baik terhadap serangan diferensial dan linear meskipun diimplementasikan pada perangkat dengan keterbatasan daya dan memori [25].

Penelitian lainnya mengenai implementasi paralel algoritma SPECK pada sistem *multi-core* untuk meningkatkan efisiensi proses enkripsi dan dekripsi. Hasilnya menunjukkan bahwa SPECK dapat dioptimalkan tanpa menurunkan tingkat keamanannya, sekaligus memberikan peningkatan signifikan terhadap kecepatan pemrosesan *data*. Kedua penelitian ini mendukung penerapan algoritma SPECK pada sistem *Internet of Things (IoT)*, karena membuktikan bahwa algoritma ini memiliki kombinasi yang ideal antara efisiensi dan keamanan [26].

Dalam konteks pemantauan suhu dan kelembapan gudang berbasis *IoT*, penerapan algoritma SPECK diharapkan dapat meningkatkan keamanan *data* dengan tetap mempertahankan kinerja sistem secara optimal. Hal ini menjadi sangat relevan bagi perusahaan distribusi seperti PT Citra Pratama Distribusiindoraya, yang mengandalkan stabilitas kondisi penyimpanan untuk menjaga kualitas produk. Melalui penerapan enkripsi SPECK, *data* dari *sensor* diharapkan dapat terlindungi

dari ancaman manipulasi dan penyadapan, sehingga informasi yang diterima pengguna benar-benar mencerminkan kondisi gudang yang sebenarnya.

Dengan latar belakang tersebut, penelitian ini bertujuan untuk merancang dan membangun sistem pemantauan suhu dan kelembapan gudang berbasis *IoT* yang dilengkapi dengan fitur keamanan menggunakan algoritma SPECK, serta menganalisis efektivitasnya dalam menjaga kerahasiaan dan integritas *data* pada studi kasus gudang PT Citra Pratama Distribusiindoraya.

B. Perumusan Masalah

Dari latar belakang yang telah dipaparkan diatas, maka bisa di tarik beberapa rumasan masalah yang akan menjadi tujuan pada proposal penelitian ini:

1. Bagaimana merancang sistem pemantauan suhu dan kelembapan gudang berbasis *IoT* di PT Citra Pratama Distribusiindoraya yang mampu mendeteksi dan mengirim *data* secara *real-time*?
2. Bagaimana menganalisis dan meningkatkan keamanan *data* pada sistem pemantauan suhu dan kelembapan berbasis *IoT* menggunakan algoritma enkripsi SPECK agar *data* terlindungi dari risiko penyadapan dan manipulasi?

C. Batasan Penelitian

Untuk memastikan penelitian tetap fokus dan dapat diukur, beberapa batasan masalah yang diterapkan dalam penelitian ini meliputi:

1. Sistem yang dikaji adalah sistem pemantauan suhu dan kelembaban berbasis *IoT* dalam lingkungan gudang, yang menggunakan *sensor* suhu dan kelembaban DHT22.
2. Algoritma enkripsi yang digunakan terbatas pada algoritma SPECK.
3. Fokus utama penelitian ini adalah pada aspek keamanan *data* yang mencakup integritas dan kerahasiaan *data* selama transmisi.

D. Tujuan Penelitian

Berdasarkan rumusan masalah diatas, adapun tujuan penelitiannya sebagai berikut :

1. Merancang dan membangun sistem pemantauan suhu dan kelembapan

gudang berbasis *Internet of Things (IoT)* di PT Citra Pratama Distribusiindoraya yang mampu mendeteksi dan mengirimkan *data* secara *real-time*.

2. Menganalisis tingkat keamanan *data* pada sistem pemantauan suhu dan kelembapan berbasis *IoT* serta mengimplementasikan algoritma enkripsi SPECK untuk meningkatkan perlindungan *data* dari risiko penyadapan dan manipulasi.

E. Manfaat Penelitian

Mengenai manfaat penelitian yang menjadi nilai dalam penelitian ini, baik untuk peneliti, pembaca, maupun pengembang sistem *monitoring* kualitas udara berbasis *IoT*:

1. Bagi Penulis

   Penelitian ini diharapkan memberikan pemahaman mendalam kepada penulis mengenai penerapan algoritma enkripsi SPECK dalam menjaga keamanan *data* suhu dan kelembapan pada sistem pemantauan gudang berbasis *IoT*. Selain itu, penulis juga memperoleh pengalaman praktis dalam merancang, membangun, serta menganalisis solusi keamanan *data* yang ringan, efektif, dan efisien sesuai kebutuhan lingkungan industri.

2. Bagi Pembaca

   Penelitian ini memberikan wawasan kepada pembaca mengenai pentingnya penerapan algoritma enkripsi ringan seperti SPECK dalam menjaga integritas dan kerahasiaan *data sensor* pada sistem *IoT*. Pengetahuan ini dapat dimanfaatkan oleh akademisi, peneliti, maupun praktisi dalam mengembangkan sistem pemantauan yang aman, khususnya di sektor logistik atau penyimpanan barang.

3. Bagi PT Citra Pratama Distribusiindoraya

   Hasil penelitian ini diharapkan dapat memberikan kontribusi nyata bagi PT Citra Pratama Distribusiindoraya dalam meningkatkan sistem keamanan *data* pada pemantauan suhu dan kelembapan gudang. Sistem ini dapat menunjang pengambilan keputusan dalam menjaga kualitas barang serta

menjadi referensi pengembangan teknologi *IoT* yang aman dan andal di lingkungan perusahaan.


UNIVERSITAS MARITIM RAJA ALI HAJI
BELAJAR DAN BERTANYA TIADA JEMU

BAB II
KAJIAN LITERATUR

A. Tinjauan Pustaka

Internet of Things (IoT) merupakan konsep yang memungkinkan perangkat untuk berkomunikasi dan bertukar *data* melalui jaringan internet tanpa intervensi manusia secara langsung. Dalam sistem pemantauan suhu dan kelembaban, *IoT* memainkan peran penting dalam menghubungkan *sensor* dengan pusat pemantauan guna memastikan lingkungan gudang tetap terkontrol. *IoT* memungkinkan otomatisasi dan efisiensi dalam berbagai bidang, termasuk pengelolaan lingkungan berbasis *sensor* [5].

Sistem pemantauan suhu dan kelembaban menggunakan berbagai *sensor* yang mampu mengukur parameter lingkungan dengan akurasi tinggi. *Sensor* seperti DHT22, BME280, dan SHT31 sering digunakan karena kemampuannya dalam mendeteksi perubahan suhu dan kelembaban secara *real-time*. Sistem berbasis *IoT* memungkinkan pemantauan jarak jauh yang lebih efektif dan akurat dibandingkan metode manual, sehingga dapat mengoptimalkan pengelolaan gudang dan memastikan kondisi penyimpanan tetap sesuai standar yang ditetapkan [6].

Penelitian dilakukan untuk mengevaluasi efisiensi dan keamanan beberapa algoritma *lightweight cryptography*, yaitu *Advanced Encryption Standard* (*AES*), *SPECK*, dan *ASCON*, yang diimplementasikan pada perangkat *Internet of Things* (*IoT*) seperti ESP32 dan STM32. Evaluasi dilakukan dengan mengukur waktu enkripsi, penggunaan memori, serta konsumsi daya. Hasil penelitian menunjukkan bahwa algoritma *SPECK* memiliki waktu enkripsi yang lebih cepat dan konsumsi energi yang lebih rendah dibandingkan algoritma lainnya, sehingga dinilai lebih sesuai untuk perangkat *IoT* dengan keterbatasan sumber daya komputasi dan daya [7].

Penelitian ini melakukan analisis kinerja algoritma kriptografi ringan pada berbagai platform perangkat keras *IoT* untuk menilai keseimbangan antara tingkat keamanan dan efisiensi sistem. Penelitian ini menunjukkan bahwa algoritma *SPECK* dengan konfigurasi tertentu mampu memberikan performa yang stabil dan efisien tanpa membebani perangkat secara signifikan. Temuan ini memperkuat

pemanfaatan *SPECK* sebagai algoritma enkripsi yang layak diterapkan pada sistem pemantauan sensor berbasis *IoT* [8].

Perbandingan algoritma *SIMON* dan *SPECK* dalam implementasi *IoT* berbasis mikrokontroler dilakukan oleh Andriani *et al.* melalui studi komparatif dan simulasi. Hasil penelitian menunjukkan bahwa *SPECK* memiliki kecepatan eksekusi yang lebih tinggi serta penggunaan sumber daya yang lebih efisien dibandingkan *SIMON*. Oleh karena itu, *SPECK* dianggap lebih sesuai untuk sistem *IoT* yang menuntut proses enkripsi cepat pada perangkat dengan spesifikasi terbatas [9].

Penelitian lain yang dipublikasikan oleh Jurnal Polibatam mengevaluasi efektivitas beberapa algoritma enkripsi ringan, yaitu *SIMON*, *SPECK*, XTEA, PRESENT, dan *AES*, pada perangkat *IoT* berbasis Raspberry Pi. Hasil pengujian menunjukkan bahwa *SPECK* memiliki keseimbangan yang baik antara tingkat keamanan, waktu enkripsi, dan konsumsi energi. Kondisi tersebut menjadikan *SPECK* sebagai salah satu algoritma yang direkomendasikan untuk sistem *IoT* yang beroperasi secara berkelanjutan [10].

Peneliti mengembangkan sistem monitoring suhu dan kelembapan berbasis *IoT* menggunakan NodeMCU dan protokol *Message Queuing Telemetry Transport* (*MQTT*). Penelitian ini menitikberatkan pada perancangan arsitektur sistem dan penyajian *data* secara *real-time*. Sistem yang dibangun mampu memantau kondisi lingkungan secara kontinu dan dapat dijadikan acuan dasar dalam pengembangan sistem pemantauan gudang sebelum ditambahkan mekanisme keamanan *data* [11].

Penelitian ini mengkaji pemanfaatan teknologi *IoT* untuk monitoring suhu dan kelembapan gudang pangan secara otomatis. Dengan menggunakan sensor lingkungan dan platform *IoT*, *data* suhu dan kelembapan dapat direkam dan ditampilkan secara *real-time* melalui antarmuka berbasis web. Penelitian ini menegaskan bahwa sistem monitoring berbasis *IoT* mampu meningkatkan efektivitas pengelolaan lingkungan gudang, meskipun belum mengintegrasikan mekanisme enkripsi *data* [12].

Penliti selanjutnya merancang prototipe sistem monitoring suhu dan kelembapan berbasis *IoT* dengan studi kasus ruang *server*. Sistem ini menggunakan sensor DHT22 dan *platform cloud ThingSpeak* untuk menampilkan *data*

lingkungan secara jarak jauh. Hasil penelitian menunjukkan bahwa sistem mampu memberikan *data* yang akurat dan stabil, namun aspek keamanan *data sensor* masih menjadi peluang pengembangan lebih lanjut [13].

Penelitian lainnya mengembangkan sistem monitoring suhu dan kelembapan gudang berbasis *IoT* dengan memanfaatkan NodeMCU dan *Firebase*. Fokus penelitian ini adalah pada akurasi pengukuran sensor dan keandalan komunikasi *data* ke *cloud*. Sistem yang dibangun dapat dijadikan dasar untuk integrasi algoritma enkripsi ringan seperti *SPECK* guna meningkatkan keamanan *data* selama proses transmisi [14].

Tabel 1. Penelitian Yang Pernah Dilakukan

No	Peneliti	Judul Penelitian	Metode	Keterangan
1	I. Radhakrishnan et al., 2024	*Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms (AES,* SPECK*, ASCON) on IoT Boards*	Eksperimen; pengujian performa algoritma pada mikrokontroler *IoT* (ESP32, STM32)	Membandingkan efisiensi, waktu enkripsi, dan konsumsi daya SPECK terhadap algoritma ringan lainnya. Sangat relevan untuk analisis keamanan dan efisiensi SPECK di sistem *IoT*.
2	M. El-Hajj et al., 2023	*Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platforms*	Eksperimen dan analisis perbandingan	Menguji kinerja algoritma SPECK 64/96 pada perangkat *IoT* berdaya rendah. Menunjukkan bahwa SPECK efisien untuk sistem *monitoring sensor*.
3	Y. Fatma Andriani et al., 2024	*Perbandingan Algoritma SIMON dan* SPECK *Dalam Implementasi IoT Berbasis Mikrokontroler*	Studi komparatif dan simulasi	Menunjukkan bahwa SPECK memiliki performa lebih cepat daripada SIMON pada perangkat *IoT* kecil. Relevan untuk pembenaran pemilihan algoritma.
4	Jurnal Polibatam, 2025	*Evaluation of the Effectiveness of Lightweight Encryption Algorithms (SIMON,* SPECK*, XTEA, PRESENT, AES) on IoT Devices*	Eksperimen langsung dengan Raspberry Pi	Evaluasi empiris 5 algoritma ringan termasuk SPECK. Menunjukkan keseimbangan antara keamanan dan efisiensi energi SPECK.
5	Jap et al. (2021)	*Lightweight Cryptography for IoT Applications: Performance and Security Analysis*	Eksperimen implementasi SPECK dalam sistem pemantauan suhu dan kelembaban berbasis *IoT*	Eksperimen implementasi SPECK dalamz sistem pemantauan suhu dan kelembaban berbasis *IoT*

Tabel 1. Penelitian Yang Pernah Dilakukan (lanjutan)

No	Peneliti	Judul Penelitian	Metode	Keterangan
6	Nizma'urrahmi et (2022)	Implementasi Algoritma SPECK pada *Wireless Sensor Network* menggunakan Media Pengiriman *Data* nRF24L01	Eksperimen pada jaringan *sensor* nirkabel (*WSN*) menggunakan modul nRF24L01	Dalam penelitian ini, algoritma SPECK dapat meningkatkan keamanan komunikasi *data* dalam *WSN* dengan efisiensi tinggi pada perangkat terbatas daya.
7	R. Santosa, 2023	Sistem *Monitoring* Suhu dan Kelembapan Berbasis *IoT*	Rancang bangun dan implementasi sistem (NodeMCU + MQTT)	Mendesain sistem pemantauan suhu dan kelembapan *real-time*. Dapat dijadikan acuan arsitektur dasar sistem pemantauan gudang.
8	Perwira *et all* (2020)	Implementasi Algoritma SPECK Pada *Fuzzy Keyword Search* Dalam *Network Storage*	Pengujian keamanan algoritma SPECK dalam pencarian kata kunci *fuzzy* di penyimpanan jaringan	Dalam penelitian ini, SPECK dapat menjaga kerahasiaan *data* dalam pencarian jaringan tanpa menurunkan performa sistem.
9	R. F. Maulana et al., 2023	Rancang Bangun Sistem *Monitoring* Suhu dan Kelembapan Berbasis *IoT* (Studi Kasus Ruang *Server*)	Prototype dan implementasi	Menggunakan *sensor* DHT22, platform ThingSpeak, dan komunikasi nirkabel. Relevan untuk struktur sistem pemantauan gudang sebelum integrasi enkripsi.
10	A. Hidayat et al., 2022	*Sistem Monitoring Kelembapan dan Suhu pada Gudang Berbasis IoT*	Desain sistem *IoT* berbasis NodeMCU dan Firebase	Fokus pada akurasi *sensor* dan komunikasi cloud. Dapat digabung dengan modul keamanan SPECK sebagai peningkatan keamanan *data*.

B. Keaslian Penelitian

Penelitian ini mengusulkan penerapan algoritma SPECK dalam sistem pemantauan suhu dan kelembaban berbasis *IoT* untuk meningkatkan keamanan *data*. Berbeda dengan penelitian sebelumnya yang lebih berfokus pada tantangan keamanan dalam *IoT* secara umum, penelitian ini lebih menitikberatkan pada analisis implementasi SPECK dalam sistem pemantauan lingkungan gudang. Analisis ini mencakup evaluasi efektivitas enkripsi SPECK dalam menjaga integritas dan kerahasiaan *data*, serta pengukuran performa sistem berdasarkan konsumsi daya, kecepatan enkripsi, dan dampaknya terhadap efisiensi transmisi *data*.

Perbandingan Penelitian: Penerapan Algoritma SPECK vs Penelitian Sebelumnya dalam Keamanan *IoT*

Tabel 2. Tabel Keaslian Penelitian

Aspek	Penelitian Ini	Penelitian Sebelumnya
Fokus Penelitian	Penelitian ini secara khusus memfokuskan kajiannya pada penerapan dan analisis algoritma enkripsi SPECK dalam sistem pemantauan suhu dan kelembaban gudang berbasis *IoT*. Fokus ini bersifat aplikatif, dengan pendekatan yang diarahkan pada kebutuhan nyata di lapangan, khususnya pada gudang milik PT Citra Pratama Distribusiindoraya.	Sebagian besar penelitian sebelumnya lebih menyoroti tantangan keamanan *IoT* secara umum, tanpa mengarah pada studi kasus tertentu atau sistem spesifik. Fokus mereka lebih pada identifikasi ancaman dan usulan solusi konseptual, tanpa melakukan implementasi langsung terhadap sistem tertentu.
Objek Studi	Sistem pemantauan suhu dan kelembaban pada lingkungan gudang dijadikan objek utama untuk diuji dan dianalisis. Konteks gudang dipilih karena kebutuhan akan kestabilan suhu dan kelembaban yang tinggi, serta pentingnya keamanan *data sensor* untuk mendukung operasional yang efisien dan aman.	Penelitian sebelumnya umumnya tidak menetapkan objek studi yang spesifik. Sebagian hanya mengkaji sistem *IoT* secara umum dalam berbagai konteks (*smart home*, pertanian, industri), sehingga kurang mendalam dalam penerapan praktis di satu bidang atau lokasi tertentu.
Algoritma Enkripsi	Penelitian ini menggunakan algoritma SPECK, yaitu algoritma kriptografi ringan	Sebagian besar penelitian sebelumnya menggunakan

yang Digunakan	yang dikembangkan oleh *NSA*, dirancang untuk perangkat *IoT* dengan keterbatasan sumber daya (*low-power*, *low-memory*). Algoritma ini belum banyak dikaji dalam konteks pemantauan lingkungan, sehingga memberikan nilai kebaruan dalam penelitian	algoritma seperti *AES* (*Advanced Encryption Standard*), *RSA*, atau algoritma klasik lainnya. Meski *AES* memiliki tingkat keamanan tinggi, algoritma ini cenderung lebih berat dan kurang optimal untuk perangkat *IoT* dengan keterbatasan sumber daya. Belum banyak studi sebelumnya yang fokus pada implementasi algoritma ringan seperti SPECK.
Evaluasi Keamanan	Penelitian ini melakukan analisis mendalam terhadap integritas dan kerahasiaan *data* yang dienkripsi menggunakan algoritma SPECK. Evaluasi dilakukan untuk memastikan bahwa *data* suhu dan kelembaban yang dikirimkan dari *sensor* ke *server* atau *cloud* tidak dapat diakses atau dimodifikasi oleh pihak tidak berwenang.	Evaluasi dalam penelitian sebelumnya cenderung bersifat konseptual atau teoritis, membahas skema keamanan atau arsitektur *IoT* tanpa implementasi dan pengujian secara nyata terhadap algoritma spesifik, terutama yang berjenis lightweight seperti SPECK.
Pengukuran Peforma Sistem	Selain aspek keamanan, penelitian ini juga mengukur performa sistem, termasuk konsumsi daya dari perangkat *IoT*,kecepatan,enkripsi/dekripsi, serta efisiensi transmisi *data* yang telah dienkripsi. Hal ini penting untuk memastikan algoritma SPECK tidak hanya aman tetapi juga efisien secara operasional di lingkungan gudang.	Penelitian sebelumnya jarang menyoroti atau membandingkan performa sistem secara teknis. Kebanyakan tidak melakukan pengukuran langsung terhadap kecepatan enkripsi atau efisiensi daya, sehingga tidak memberikan gambaran menyeluruh terhadap dampak algoritma enkripsi terhadap performa sistem secara *real-time*.
Kontribusi Penelitian	Penelitian ini memberikan kontribusi nyata dan orisinal dalam bentuk perancangan, implementasi, dan analisis sistem pemantauan suhu dan kelembaban berbasis *IoT* dengan algoritma SPECK. Kontribusi ini penting bagi dunia industri,	Sebagian besar penelitian sebelumnya memberikan kontribusi dalam bentuk kajian teoritis atau perbandingan algoritma secara umum. Belum banyak yang secara spesifik

	khususnya dalam konteks gudang penyimpanan yang memerlukan sistem yang efisien namun tetap aman.	meneliti penggunaan algoritma SPECK pada sistem pemantauan suhu dan kelembaban,sehingga penelitian ini memperluas cakupan literatur dan praktik yang ada.

C. Landasan Teori

1. Pengertian *Internet Of Things (IoT)*

Internet of Things (IoT) adalah konsep teknologi yang memungkinkan perangkat fisik seperti *sensor*, aktuator, dan mikrokontroler untuk terhubung melalui jaringan *internet* guna mengumpulkan dan bertukar *data* secara otomatis. Dalam sistem pemantauan suhu dan kelembaban gudang, *IoT* memainkan peran penting dalam menghubungkan *sensor* dengan platform pemantauan yang dapat diakses secara *realtime* oleh pengguna. Sistem ini memungkinkan pengelola gudang untuk mendeteksi perubahan suhu dan kelembaban dengan lebih akurat, serta mencegah risiko kerusakan barang yang disebabkan oleh kondisi lingkungan yang tidak stabil. Dengan *IoT*, *data* suhu dan kelembaban dapat dikirimkan ke *cloud* atau *server* melalui teknologi komunikasi seperti *Wi-Fi*, *LoRa*, atau *MQTT*, sehingga pengelola dapat mengambil tindakan segera berdasarkan *data* yang diterima. Namun, dalam penerapannya, keamanan *data* menjadi aspek yang sangat penting karena informasi yang dikirimkan dapat mengalami serangan siber yang berpotensi menyebabkan manipulasi *data* atau pencurian informasi.

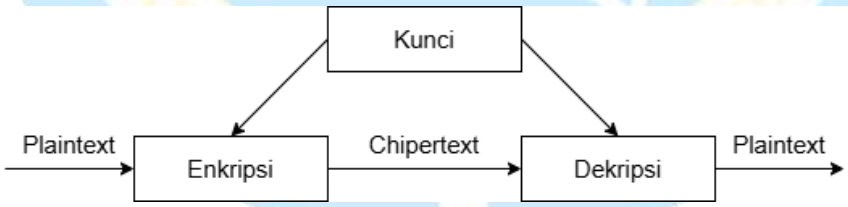
2. Keamanan *Data* dalam *IoT*

Keamanan *data* dalam *IoT* bertujuan untuk menjaga integritas, kerahasiaan, dan ketersediaan informasi yang dikirimkan oleh *sensor* ke *server*. Sistem pemantauan suhu dan kelembaban yang berbasis *IoT* rentan terhadap berbagai ancaman siber seperti penyadapan (*sniffing*), manipulasi *data* (*data tampering*), *Man-in-the-Middle attack*, serta serangan ulang (*replay attack*) [7]. Penyadapan terjadi ketika pihak tidak sah mengakses *data* saat transmisi, sedangkan manipulasi

data dapat menyebabkan perubahan informasi yang dapat menyesatkan pengelola gudang dalam pengambilan keputusan. Oleh karena itu, diperlukan metode enkripsi yang dapat menjaga keamanan *data* selama proses pengiriman melalui jaringan *IoT*. Algoritma kriptografi yang digunakan harus ringan dan efisien agar tidak membebani perangkat *IoT* yang umumnya memiliki keterbatasan daya dan kapasitas komputasi. Salah satu algoritma yang sangat sesuai untuk kebutuhan ini adalah SPECK, yang dirancang khusus untuk perangkat dengan sumber daya terbatas.

3. Kriptografi

Kriptografi merupakan metode pengamanan *data* yang mengubah informasi asli (*plaintext*) menjadi bentuk terenkripsi (*ciphertext*) sehingga hanya pihak yang memiliki kunci enkripsi yang dapat membaca kembali *data* tersebut. Dalam sistem pemantauan suhu dan kelembaban berbasis *IoT*, kriptografi sangat penting untuk mencegah pihak tidak berwenang mengakses atau memanipulasi *data* yang dikirim oleh *sensor*. Algoritma kriptografi yang digunakan dalam *IoT* harus memiliki keseimbangan antara keamanan dan efisiensi komputasi. SPECK adalah salah satu algoritma yang dirancang untuk memenuhi kebutuhan tersebut karena menggunakan operasi sederhana seperti rotasi bit, XOR, dan penjumlahan modular yang tidak membebani mikrokontroler atau perangkat dengan daya rendah.



Gambar 1. Proses Enkripsi Sederhana

Gambar di atas menunjukkan alur sederhana dari proses enkripsi dan dekripsi dalam sistem kriptografi.

1. *Plaintext* (*Data* Asli): Ini adalah *data* asli yang ingin diamankan, misalnya *data sensor* suhu dan kelembapan dalam sistem *IoT*. *Plaintext* adalah *data* dalam bentuk yang mudah dipahami dan terbaca oleh manusia atau sistem.

2. Enkripsi: Proses ini mengubah *plaintext* menjadi *ciphertext*, yaitu bentuk terenkripsi dari *data* yang tidak bisa dipahami oleh pihak yang tidak memiliki kunci enkripsi. Enkripsi menggunakan algoritma dan kunci tertentu untuk melakukan konversi ini. Tujuannya adalah menjaga kerahasiaan *data* selama proses pengiriman atau penyimpanan, agar tidak bisa diakses oleh pihak yang tidak berwenang.

3. *Ciphertext*: Ini adalah hasil dari proses enkripsi, yaitu *data* yang sudah diacak atau terenkripsi. *Ciphertext* hanya bisa dibaca kembali menjadi *plaintext* dengan menggunakan kunci yang tepat dalam proses dekripsi.

4. Dekripsi: Proses ini mengubah *ciphertext* kembali menjadi *plaintext* dengan menggunakan kunci yang sesuai. Dekripsi memungkinkan *data* asli (*plaintext*) kembali terbaca dan bisa digunakan oleh sistem atau penerima yang sah.

4. Algoritma SPECK

Algoritma SPECK adalah salah satu algoritma *Lightweight block cipher* guna memenuhi kebutuhan suatu metode penyandian pada suatu media dengan sumber daya yang sangat terbatas, seperti memori, daya komputasi dan pasokan baterai. Kriptografi *Lightweight* (ringan) adalah kriptografi ringan yang telah menjadi topik tren untuk beberapa tahun terakhir ini dan munculnya kriptografi ini didorong oleh kurangnya aplikasi yang mampu berjalan pada perangkat berdaya komputasi yang sangat rendah. Algoritma SPECK diajukan oleh peneliti yang bekerja pada *National Security Agency (NSA)* di Amerika. Pemetaan acak adalah persyaratan yang harus dimiliki suatu algoritma *block cipher*. Terdapat 10 varian dari algoritma SPECK berdasarkan panjang kunci dan ukuran blok pesannya seperti dapat dilihat pada tabel dibawah :

Tabel 3. Panjang Kunci Algoritma SPECK

Sumber : [23]

Block Size2n	Key Size mn	Word size n	Key words	Rot α	Rot β	Rounds r
32	64	16	4	7	2	22
48	72	24	3	8	3	22
48	96	24	4			23
64	96	32	3	8	3	26
64	128	32	4			27
96	96	48	2	8	3	28
96	144	48	3			29
128	128	64	2	8	3	32
128	192	64	3			33
128	256	64	4			34

Tabel 4. Notasi Algoritma SPECK

Sumber : [23]

⊕	Operator bitwise XOR
n	Ukuran panjang word pada SPECK (n = 16,24,32,48, atau 64)
+	Operator penjumlahan modulo 2n
-	Operator Pengurangan modulo 2n
<<j	Rotasi bit ke kiri sebanyak j bit
>>j	Rotasi bit ke kanan sebanyak j bit
R	Jumlah round
α → b	Memperbarui nilai a dengan nilai b

a. Enkripsi SPECK

Enkripsi adalah suatu metode yang digunakan untuk mengamankan *data* dengan cara mengubahnya menjadi bentuk yang tidak dapat dibaca (*ciphertext*), sehingga hanya pihak yang memiliki kunci enkripsi yang dapat mengembalikannya ke bentuk asli (*plaintext*). Algoritma SPECK adalah salah satu algoritma kriptografi ringan berbasis blok yang dikembangkan oleh *National Security Agency (NSA)* untuk perangkat dengan keterbatasan daya dan

komputasi, seperti *Internet of Things (IoT)*. Algoritma ini menggunakan operasi sederhana seperti XOR, rotasi bit, dan penjumlahan modular sehingga proses enkripsi dan dekripsi dapat berjalan dengan cepat tanpa membebani sistem.

1. Kelebihan Enkripsi

Beberapa kelebihan yang bisa didapatkan dari enkripsi ini adalah :

1) Kerahasiaan suatu informasi terjamin.
2) Efisiensi dan Kecepatan Pemrosesan.
3) Melindungi *Data* dari Penyadapan.
4) Kompatibel dengan Perangkat *IoT* yang Memiliki Keterbatasan Sumber Daya.
5) Keamanan yang Memadai untuk Aplikasi *IoT*.

2. Kerugian Enkripsi

Penyalahgunaan dan kerugian dari enkripsi adalah:

1) Potensi Penyalahgunaan dalam Kejahatan Siber.
2) Risiko Keamanan Jika Kunci Hilang atau Dicuri.

Proses enkripsi pada algoritma SPECK terdiri dari langkah-langkah dibawah ini, yaitu (Firmanesa, 2016).:

Proses Enkripsi Algoritma SPECK

Input : $X(2n)$; $K0, \dots, Kr{-}1$

Output :$(2n)$

Proses :

- $X0(n)|X1(n) \rightarrow X(2n)$

  $untuk\ i = 1\ sampai\ dengan\ r - 1$

- $X1 \rightarrow ((X1 \gg \alpha) + X0)$

  $X0 \rightarrow ((X0 \gg \beta))$ 1

  Output :

  $(2n) \rightarrow X0(n)|X1(n)$

  a. Menguraikan nilai X(2n) menjadi X0(n)|X1(n).
  b. Memperbarui nilai X1 menjadi nilai X1 yang telah digeser ke kanan sejauh α bit dan dilakukan operasi penjumlahan modulo X0 serta operasi XOR dengan ki.

c. Memperbarui nilai X0 menjadi nilai X0 yang telah digeser ke kanan sejauh β bit dan operasi XOR dengan X1.

d. Memperbarui nilai Y(2n) menjadi nilai X0(n)|X1(n).

b. Dekripsi SPECK

Proses deskripsi pada algoritma SPECK terdiri dari langkah-langkah dibawah ini, yaitu (Firmanesa, 2016).:

Proses Dekripsi Algoritma SPECK:

Input : Y; $K0, \dots, Kr{-}1$

Output :$(2n)$

Proses :

- $Y0(n)|Y1(n) \rightarrowtail Y(2n)$

  $untuk\ i = 1\ sampai\ dengan\ r - 1\ Y0 \rightarrowtail (Y0\ Y1) \gg \beta$

- $Y1 \rightarrowtail ((Y1\ -i-1) - Y0) \ll \alpha$

Output : $X(2n) \rightarrowtail Y0(n)|Y1(n)$

a. Menguraikan Y(2n) menjadi Y0(n)|Y1(n)

b. Lakukan operasi bitwise XOR antara Y0 dan Y1, setelah itu lakukan pergeseran bit ke kanan sejauh β serta perbarui nilai Y0

c. Lakukan operasi bitwise XOR antara Y1 dan Kr-2, setelah itu lakukan pergeseran bit ke kiri sebesar α serta perbarui nilai Y1.

d. Perbarui nilai X(2n) dengan Y0(n)|Y1(n).

c. Contoh Perhitungan Manual Algoritma SPECK

Parameter yang digunakan = 26 derajat celcius

- Varian algoritma : SPECK32/64 (ukuran blok 32-bit, terdiri dari dua kata masing-masing 16-bit)
- Ukuran kata : 16-bit
- Jumlah ronde (contoh) : 4 ronde
- Rotasi : α = 7 (rotasi kanan untuk X), β = 2 (rotasi kiri untuk Y)
- *Plaintext* : *data* suhu 26°C, direpresentasikan dalam bentuk heksadesimal sebagai:

  X0 = 0x0000

  Y0 = 0x001A (26 desimal)

- Kunci ronde (contoh, disederhanakan untuk perhitungan manual):

K0 = 0x1918, K1 = 0x1110, K2 = 0x0908, K3 = 0x0100

1) Proses Enkripsi

Operasi enkripsi pada setiap ronde didefinisikan sebagai berikut:

1. Xr = ROR(X, α)
2. S = (Xr + Y) mod 2^16
3. X' = S ⊕ Ki
4. Yr = ROL(Y, β)
5. Y' = Yr ⊕ X'

Tabel 5. Perhitungan Ronde Enkripsi Algoritma SPECK

Ronde	X (awal)	Y (awal)	ROR(X,7)	ROR(X,7) +Y	X' (setelah XOR Ki)	ROL(Y,2)	Y' (baru)
0	0x0000	0x001A	0x0000	0x001A	0x1902	0x0068	0x196A
1	0x1902	0x196A	0x0C8C	0x2596	0x0C8C	0x65A8	0x6924
2	0x0C8C	0x6924	0x1641	0x7F65	0x8835	0xA491	0x2CA4
3	0x8835	0x2CA4	0xC46D	0xF111	0x96B4	0xB290	0x2424

Ciphertext hasil enkripsi: X = 0x96B4, Y = 0x2424 → 0x96B42424

2) Proses Dekripsi

Operasi dekripsi merupakan kebalikan dari enkripsi, dengan urutan ronde terbalik:

1. Y_old = ROR(Y_new ⊕ X_new, β)
2. Temp = X_new ⊕ Ki
3. Sub = (Temp – Y_old) mod 2^16
4. X_old = ROL(Sub, α)

Jika dekripsi dilakukan terhadap *ciphertext* 0x96B42424 dengan kunci yang sama, maka hasil akhirnya adalah:

X = 0x0000, Y = 0x001A → kembali ke *plaintext* suhu 26°C.

Dengan demikian proses enkripsi dan dekripsi terbukti konsisten.

3) Penambahan Mekanisme Counter/Nonce (Mode CTR)

Algoritma SPECK adalah block cipher yang pada dasarnya hanya memproses blok *data* tetap.

Untuk mengamankan *data sensor* yang dikirim berulang kali, digunakan mode operasi CTR (Counter) dengan penambahan nonce.

Prinsip kerja CTR:

1. Pilih sebuah nonce (nilai unik untuk setiap perangkat/sesi komunikasi).
2. Gabungkan dengan nilai counter (yang selalu bertambah setiap blok).
3. Blok nonce || counter dienkripsi menggunakan SPECK untuk menghasilkan keystream.
4. *Ciphertext* = *Plaintext* ⊕ Keystream.
5. Pada sisi penerima, proses yang sama dilakukan untuk memperoleh keystream, lalu *ciphertext* ⊕ keystream = *plaintext* kembali.

Contoh:

- Nonce = 0x0001
- Counter = 0x0001
- Input ke SPECK: (0x0001, 0x0001)
- Hasil enkripsi (keystream): (0x4FBA, 0xB357)
- *Plaintext* suhu: (0x0000, 0x001A)
- *Ciphertext* = (0x4FBA, 0xB34D) = 0x4FBAB34D

Kesimpulan:

1. *Data* suhu 26°C berhasil dienkripsi menjadi 0x96B42424 dengan algoritma SPECK (contoh 4 ronde).
2. Proses dekripsi berhasil mengembalikan *ciphertext* menjadi *plaintext* asli (26°C).
3. Penambahan mekanisme Counter/Nonce melalui mode CTR memastikan keamanan lebih baik, mencegah reuse *ciphertext* dan serangan replay.


UNIVERSITAS MARITIM RAJA ALI HAJI
BELAJAR DAN BERTANYA TIADA JEMU

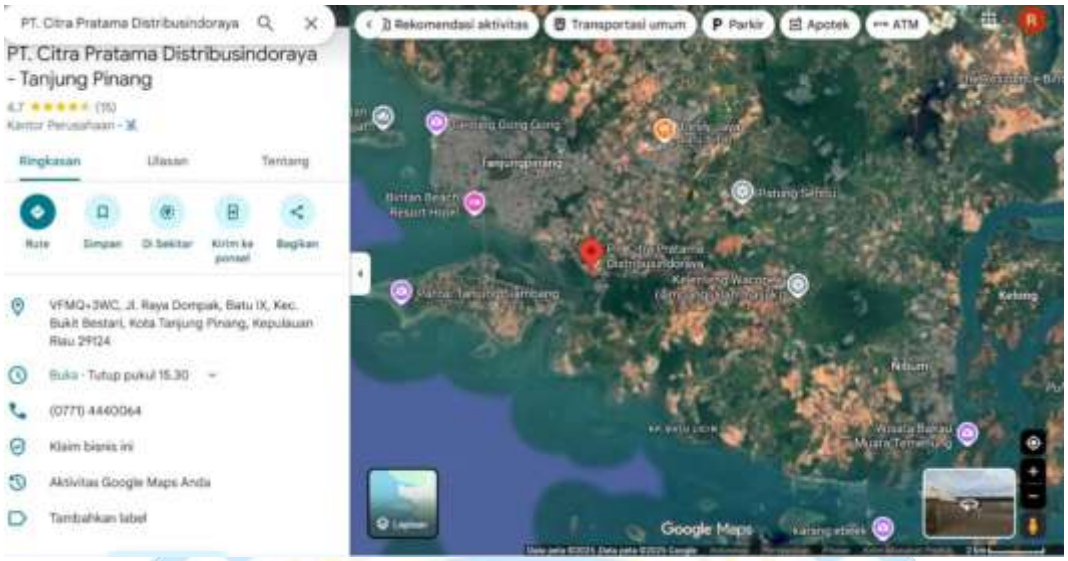
BAB III
METODE PENELITIAN

A. Waktu dan Tempat Penelitian

Penelitian ini dilaksanakan pada bulan Agustus hingga Desember 2025 dan bertempat di Gudang PT Citra Pratama Distribusiindoraya. Gudang tersebut merupakan gudang distribusi yang digunakan untuk penyimpanan produk makanan dan minuman sebelum didistribusikan ke konsumen atau mitra usaha. Jenis produk yang disimpan meliputi makanan kemasan dan minuman siap konsumsi yang memiliki ketahanan terbatas terhadap perubahan kondisi lingkungan, khususnya suhu dan kelembapan udara.

Sebagai gudang makanan dan minuman, kestabilan suhu dan kelembapan menjadi faktor yang sangat penting karena berpengaruh langsung terhadap kualitas, keamanan, serta daya simpan produk. Suhu yang terlalu tinggi dapat mempercepat proses penurunan mutu produk, sedangkan kelembapan yang berlebihan dapat memicu pertumbuhan mikroorganisme serta merusak kemasan. Oleh karena itu, gudang ini membutuhkan sistem pemantauan suhu dan kelembapan yang mampu bekerja secara kontinu dan akurat untuk memastikan kondisi lingkungan penyimpanan tetap berada dalam batas yang aman.

Data yang digunakan dalam penelitian diperoleh secara langsung menggunakan *sensor IoT* yang dirancang untuk mendeteksi parameter kualitas udara seperti konsentrasi suhu, dan kelembaban. *Sensor* ini diimplementasikan di PT Citra Pratama Distribusindoraya untuk mengumpulkan *data* secara *real-time*, yang kemudian dienkripsi menggunakan algoritma SPECK sebelum dikirim melalui jaringan untuk analisis lebih lanjut.



Gambar 2. Peta Lokasi Penelitian

Gambar 3. Tampak Depan Gudang Pt Citra Pratama Distribusiindoraya yang Akan Dilakukan Penelitian

B. Landasan Suhu dan Kelembapan Optimal

Gudang penyimpanan makanan dan minuman merupakan fasilitas penting dalam rantai distribusi yang berfungsi menjaga mutu dan keamanan produk sebelum didistribusikan ke konsumen. Kondisi lingkungan di dalam gudang, khususnya suhu dan kelembapan, sangat memengaruhi stabilitas produk selama masa penyimpanan. Lingkungan penyimpanan yang tidak terkontrol dapat menyebabkan percepatan penurunan mutu, kerusakan kemasan, serta meningkatkan risiko kontaminasi mikroorganisme. Oleh karena itu, pengelolaan

kondisi lingkungan gudang menjadi aspek yang harus diperhatikan dalam sistem penyimpanan produk makanan dan minuman.

Pengendalian suhu merupakan salah satu parameter utama dalam menjaga kualitas produk makanan dan minuman di gudang. Suhu penyimpanan yang terlalu tinggi dapat mempercepat aktivitas mikrobiologis dan reaksi kimia yang menyebabkan perubahan fisik dan *sensor*ik produk. Penelitian menunjukkan bahwa suhu penyimpanan bahan makanan kering pada kisaran 20 °C hingga 21,6 °C masih memenuhi standar keamanan pangan dan mampu menjaga mutu produk [33]. Kisaran suhu tersebut dinilai efektif untuk menghambat pertumbuhan mikroorganisme tanpa memerlukan sistem pendinginan khusus, sehingga sesuai diterapkan pada gudang penyimpanan makanan kering dan minuman kemasan di wilayah beriklim tropis.

Selain suhu, kondisi kelembapan udara di dalam gudang juga berperan penting dalam menjaga kualitas produk makanan dan minuman. Kelembapan yang terlalu tinggi dapat memicu pertumbuhan jamur, mempercepat kerusakan kemasan, serta meningkatkan risiko penurunan mutu produk. Sebaliknya, kelembapan yang terlalu rendah dapat menyebabkan produk makanan kering menjadi rapuh dan menurunkan kualitas fisik kemasan. Oleh karena itu, pengendalian kelembapan perlu dilakukan secara terintegrasi dengan pengendalian suhu agar kondisi penyimpanan di gudang tetap stabil.

Hasil penelitian menunjukkan bahwa kelembapan relatif yang terkontrol memiliki peran penting dalam menjaga keamanan dan mutu produk pangan selama proses penyimpanan dan distribusi [34]. Studi tersebut menyimpulkan bahwa kelembapan relatif pada kisaran 50 % hingga 60 % mampu membantu menghambat pertumbuhan mikroorganisme serta menjaga stabilitas kondisi produk. Rentang kelembapan ini dapat dijadikan acuan sebagai kelembapan optimal bagi gudang penyimpanan makanan dan minuman agar kualitas produk tetap terjaga hingga tahap distribusi.

C. Bahan dan Alat

Sistem pemantauan suhu dan kelembaban gudang ini didesain dengan memanfaatkan beberapa perangkat dan komponen yang dapat dilihat pada gambar di bawah. Terdapat mikrokontroler ESP8266 sebagai otak utama sistem, *sensor*

DHT22 untuk mengukur suhu dan kelembaban di dalam gudang, serta *buzzer* sebagai indikator *audio* untuk memberikan peringatan jika suhu atau kelembaban melebihi ambang batas yang telah ditentukan. *Data* yang diperoleh dari *sensor* akan diproses dan dikirim ke *server* melalui jaringan WiFi, kemudian ditampilkan dalam bentuk diagram pada *website* untuk memudahkan pengguna dalam memantau kondisi gudang secara *real-time*.

Tabel 6. Bahan dan Alat

No	Komponen	Kegunaan
1	Mikrokontroler ESP8266	Sebagai pusat pengendali sistem yang menghubungkan *sensor* DHT22 dengan *server* melalui jaringan Wi-Fi.
2	*Sensor* DHT22	Untuk membaca objek suhu dan kelembaban.
3	*Buzzer*	Untuk Memberikan sinyal *audio* atau *alarm* untuk memberi tahu pengguna tentang suatu kejadian atau kondisi tertentu
4	Kabel Jumper, Breadboard	Sebagai sarana perakitan.
5	Laptop	Untuk menyimpan *data* dan menampilkan dashboard.

D. Prosedur Pelaksanaan Penelitian

Metode penelitian dalam Analisis dan Implementasi Keamanan Pada Sistem Pemantauan Suhu dan Kelembapan Gudang Berbasis *IoT* Menggunakan Algoritma SPECK Studi Kasus : Gudang PT Citra Pratama Distribusiindoraya dapat dibagi menjadi beberapa tahap sebagai berikut.

Gambar 4. Metode Penelitian

Pada gambar diatas merupakan urutan mengenai metode penelitian yang digunakan, yaitu terdiri dari :

1. Studi Pustaka:

Penelitian diawali dengan melakukan studi pustaka untuk mengumpulkan teori-teori dan literatur yang relevan terkait dengan sistem pemantauan suhu dan kelembapan berbasis *IoT*, algoritma kriptografi SPECK, serta teknik pengujian keamanan *data*, khususnya metode serangan *Man in The Middle (MITM)* [7]. Studi

ini bertujuan untuk memberikan landasan teori yang kuat serta membantu merumuskan pendekatan dan teknologi yang tepat dalam pembangunan sistem.

2. Perancangan Model Keamanan Sistem:

Setelah memperoleh pemahaman dari studi pustaka, langkah selanjutnya adalah merancang model sistem pemantauan suhu dan kelembapan gudang yang dilengkapi dengan fitur keamanan *data* menggunakan algoritma SPECK. Pada tahap ini, dirancang arsitektur perangkat keras dan lunak, termasuk pemilihan mikrokontroler, *sensor* suhu dan kelembapan, serta mekanisme komunikasi dan enkripsi *data*.

3. Implementasi Sistem:

Tahap berikutnya adalah implementasi sistem yang telah dirancang. Sistem dibangun menggunakan perangkat *IoT* seperti mikrokontroler (misalnya ESP8266 atau Arduino), *sensor* DHT22 atau sejenisnya, serta pemrograman untuk mengintegrasikan algoritma SPECK guna melakukan enkripsi *data* suhu dan kelembapan sebelum dikirimkan melalui jaringan. Hasil implementasi berupa prototipe sistem *monitoring* yang dapat berjalan secara *real-time*.

4. Pengujian Sistem dengan *MITM*:

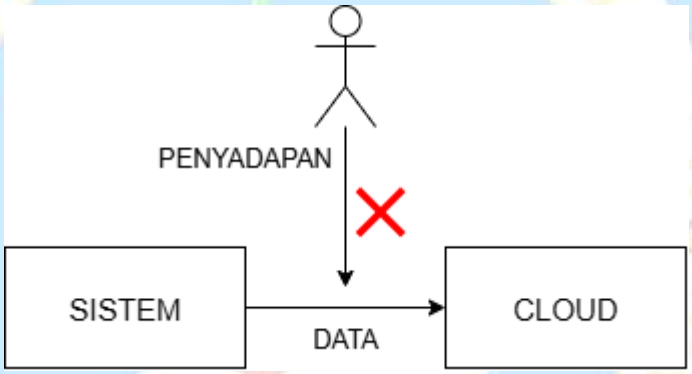
Setelah sistem berhasil diimplementasikan, dilakukan pengujian keamanan dengan metode *Man in The Middle (MITM)*. Pengujian ini bertujuan untuk mengevaluasi sejauh mana *data* yang dikirimkan oleh sistem dapat disadap atau dimanipulasi oleh pihak yang tidak berwenang, serta mengukur efektivitas algoritma SPECK dalam menjaga kerahasiaan dan integritas *data* selama proses transmisi [9].

- *Man In The Middle Attack*

  Dalam skenario ini, penyerang mencoba melakukan penyadapan terhadap komunikasi antara perangkat mikrokontroler ESP8266 dan cloud *server* yang digunakan untuk mengirim *data* suhu dan kelembapan dari *sensor* DHT22 [3]. Tujuan utama serangan ini adalah untuk memperoleh atau memodifikasi *data* lingkungan gudang secara tidak sah. Untuk mengatasi potensi ancaman ini, sistem dirancang menggunakan algoritma enkripsi SPECK guna mengamankan transmisi *data* dari perangkat *IoT* ke *server*. Algoritma SPECK, yang dikenal efisien untuk perangkat dengan

sumber daya terbatas seperti ESP8266, mengenkripsi *data sensor* sebelum dikirim melalui jaringan *internet*.

Dengan penerapan algoritma SPECK, meskipun *data* berhasil disadap oleh pihak yang tidak berwenang, *data* tersebut tetap tidak dapat dibaca atau dimodifikasi tanpa kunci dekripsi yang sah. Pengujian ini bertujuan untuk mengevaluasi sejauh mana algoritma SPECK mampu melindungi *data* dari serangan *Man in the Middle (MITM)* dan menjamin keamanan selama proses pemantauan suhu dan kelembapan. Hasil dari pengujian ini diharapkan dapat menunjukkan bahwa sistem mampu menjaga kerahasiaan dan integritas *data sensor*, sehingga informasi yang dikirim dari gudang PT Citra Pratama Distribusiindoraya tetap terlindungi dari ancaman peretasan selama komunikasi berlangsung.



Gambar 5. Ilustrasi Keamanan *Data* dari Sistem Ke *Cloud*

Sebelum penerapan SPECK, komunikasi ESP8266–*Cloud* pada sistem pemantauan DHT22 mengirim *data* dalam bentuk *plaintext* (~36–48 byte JSON) sehingga mudah disadap, dimodifikasi (*MITM*), atau di*replay* karena tidak ada mekanisme *counter*/*nonce*. Kondisi ini memang memberi latensi rendah dan beban *CPU*/memori nyaris nol, tetapi keamanan sangat lemah. Setelah SPECK64/128 diterapkan dalam *mode* CTR dengan tambahan HMAC-SHA256 dan nonce, *data* dikirim sebagai *ciphertext* (~85 byte per pesan) yang hanya bisa didekripsi dengan kunci sah, sehingga kerahasiaan dan integritas terjamin serta *replay* dapat dicegah. *Trade-off* yang muncul adalah peningkatan beban *CPU* (0,8–3,5 ms/pesan), tambahan *RAM*/*flash* untuk *library* kripto, *payload* jaringan lebih besar, dan konsumsi

energi sedikit lebih tinggi. Meski demikian, biaya performa ini relatif kecil dibandingkan peningkatan keamanan, terutama bila disertai manajemen kunci yang baik dan mekanisme proteksi *replay*.

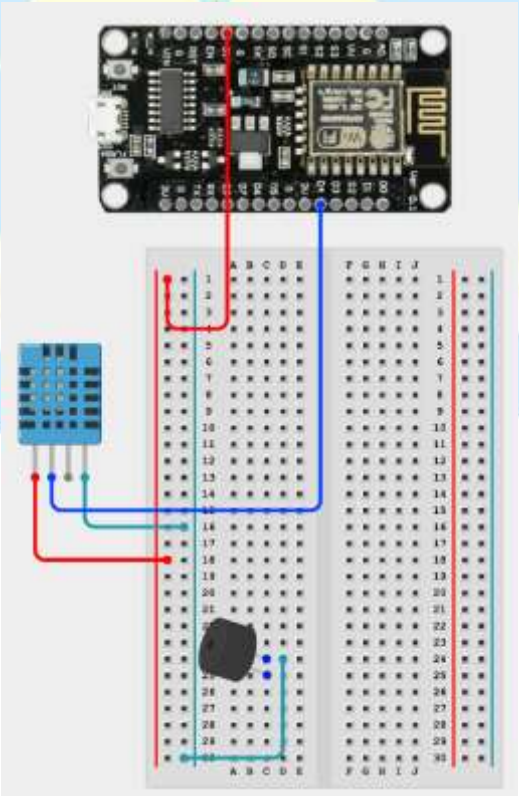
5. Analisis Hasil Pengujian:

Selanjutnya dilakukan analisis terhadap hasil pengujian *MITM*. Analisis mencakup keberhasilan sistem dalam mencegah pembacaan *data* oleh pihak ketiga, performa algoritma SPECK dalam konteks *IoT*, serta dampak enkripsi terhadap waktu respon dan kinerja sistem secara keseluruhan. Evaluasi ini penting untuk memastikan sistem tidak hanya berjalan dengan baik, tetapi juga aman.

6.Selesai:

Tahapan akhir dari metode ini adalah penyimpulan hasil analisis dan penyusunan laporan akhir dari penelitian. Kesimpulan yang diperoleh menjadi dasar rekomendasi untuk pengembangan sistem *IoT* yang aman di masa depan, khususnya untuk aplikasi di gudang atau lingkungan industri.

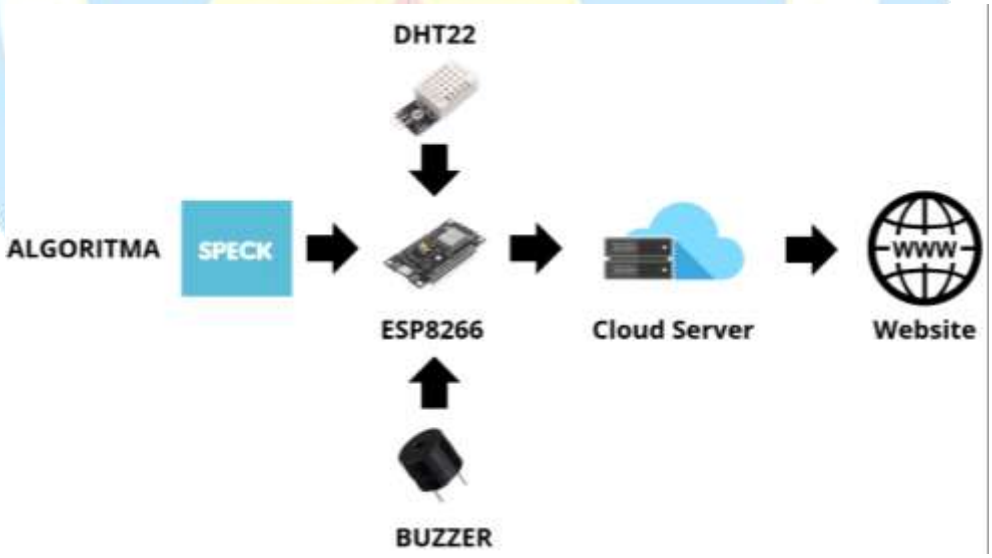
E. Rancangan Perangkat Keras



Gambar 6. Rancangan Perangkat Keras

Perancangan hardware pada sistem Pemantauan Suhu dan Kelembaban Gudang Berbasis *IoT* menggunakan mikrokontroler ESP8266 sebagai pusat pengendali. *Sensor* DHT22 digunakan untuk mengukur suhu dan kelembaban dalam gudang secara *realtime*. *Sensor* DHT22 akan mengirimkan *data* ke ESP8266, lalu ESP8266 akan mengolah dan mengirimkan *data* tersebut ke *server* melalui koneksi *WiFi*. *Data* kemudian ditampilkan dalam bentuk diagram di *website* sehingga pengguna dapat memantau kondisi gudang dari jarak jauh. Selain itu, sistem juga dilengkapi dengan *buzzer* yang berfungsi sebagai *alarm* untuk memberikan peringatan jika suhu atau kelembaban melebihi ambang batas. Batasan suhu pada sistem ini dikategorikan menjadi tiga kondisi, yaitu: "Aman" apabila berada pada suhu di bawah 34,9°C, "Waspada" apabila suhu berada di atas 35,0°C hingga 37,9°C, dan "Bahaya" apabila suhu melebihi 38,0°C. Pada kondisi "Waspada" dan "Bahaya", *buzzer* akan aktif selama 5 detik sebagai bentuk peringatan dini agar pengguna segera melakukan tindakan penanganan.

F. Rancangan Arsitektur Sistem



Gambar 7. Rancangan Arsitektur Sistem

Dari gambar diatas merupakan rancangan asrsitektur sistem, berikut penjelasannya :

1. Perangkat *IoT* (ESP8266 + *Sensor* DHT22)
   - Membaca *data sensor* suhu dan kelembapan dari lingkungan gudang menggunakan DHT22.
   - Mengenkripsi *data* menggunakan algoritma SPECK sebelum dikirimkan.
   - Mengirimkan *data* terenkripsi ke *server*/*cloud* melalui koneksi internet menggunakan protokol *HTTP*/*MQTT*.
2. Cloud / *Server*
   - Menerima *data* terenkripsi dari ESP8266.
   - Mendekripsi *data* menggunakan algoritma SPECK di sisi *server* (dengan
   - menggunakan kunci dekripsi).
   - Menyimpan *data* yang telah didekripsi ke dalam basis *data* (contoh:
   - MySQL, Firebase, atau MongoDB).
   - Melakukan pemrosesan tambahan, seperti notifikasi atau *log* jika *data*
   - melewati batas suhu/kelembapan tertentu.
3. Pengguna (Aplikasi *Web* atau *Mobile*)
   - Mengakses *data* suhu dan kelembapan yang telah didekripsi melalui antarmuka aplikasi (*web* atau *mobile*).
   - Aplikasi menampilkan *data* dalam bentuk grafik, indikator, atau tabel secara *real-time* dari basis *data*.
   - Pengguna dapat memantau kondisi gudang kapan saja dan di mana saja.

   Langkah-langkah Implementasi:

   Langkah 1 : Pembuatan dan Penempatan Kunci SPECK
      1) Kunci Enkripsi SPECK → Disimpan di ESP8266.
      2) Kunci Dekripsi SPECK → Disimpan di *Server Cloud*.

   Langkah 2 : ESP8266 (Perangkat *IoT*)
      1) Membaca *data* dari *sensor* DHT22.
      2) Mengenkripsi *data* menggunakan algoritma SPECK.
      3) Mengirimkan *data* terenkripsi ke *Cloud Server* menggunakan koneksi *HTTP*/*MQTT*.

   Langkah 3 : Implementasi di *Cloud / Server*
      1) Menerima *data* terenkripsi dari ESP8266 melalui *API*.
      2) Mendekripsi *data* menggunakan kunci dekripsi SPECK.

3) Menyimpan *data* ke dalam basis *data*.
4) Menyediakan *endpoint* atau layanan agar *data* bisa dibaca oleh aplikasi *web/mobile*.

Langkah 4 : Pengguna

1) Pengguna membuka aplikasi *web/mobile*.
2) Aplikasi mengambil *data* dari *database server*.
3) *Data* ditampilkan secara interaktif dan *real-time* sebagai hasil pemantauan kondisi gudang.

Arsitektur sistem pada penelitian ini dirancang untuk melakukan pemantauan suhu dan kelembapan gudang secara *real-time* dengan pendekatan *Internet of Things (IoT)* yang dilengkapi dengan algoritma enkripsi SPECK guna menjamin keamanan *data* selama proses transmisi. Sistem ini menggunakan mikrokontroler ESP8266 sebagai pusat kendali yang terhubung dengan *sensor* DHT22 untuk mengukur suhu dan kelembapan udara di dalam gudang. *Data* yang diperoleh dari *sensor* akan dienkripsi terlebih dahulu menggunakan algoritma SPECK pada perangkat ESP8266 sebelum dikirim ke *cloud server* melalui koneksi *internet*. Algoritma SPECK dipilih karena ringan dan efisien untuk digunakan pada perangkat dengan sumber daya terbatas seperti ESP8266.

Setelah *data* terenkripsi diterima oleh *cloud server*, *data* tersebut kemudian didekripsi dan disimpan ke dalam basis *data* untuk keperluan penyimpanan dan analisis. Selain itu, *data* hasil pengukuran dapat diakses oleh pengguna melalui antarmuka *website* yang dirancang khusus untuk menampilkan informasi suhu dan kelembapan secara *real-time*. *Website* ini juga memungkinkan pengguna untuk memantau histori *data* dan mendapatkan notifikasi apabila nilai suhu atau kelembapan melampaui batas ambang yang telah ditentukan. Untuk meningkatkan respons terhadap kondisi tidak *normal*, sistem juga dilengkapi dengan *buzzer* yang akan berbunyi secara otomatis apabila terjadi peningkatan suhu atau kelembapan di luar batas yang diizinkan.

Dengan integrasi sistem ini, pemantauan kondisi lingkungan gudang dapat dilakukan secara efisien dan aman. Penggunaan algoritma SPECK memberikan perlindungan terhadap potensi serangan keamanan seperti *Man in the Middle*

(MITM) attack, karena *data* yang dikirim dari perangkat ke *server* telah terenkripsi dan hanya dapat didekripsi oleh pihak yang memiliki kunci yang sah. Sistem ini memberikan solusi efektif untuk menjaga kualitas penyimpanan barang di gudang PT Citra Pratama Distribusiindoraya serta menjamin keamanan *data* selama proses transmisi.

G. Pengumpulan *Data*

Pengumpulan *data* dalam penelitian ini berupa *data* suhu dan kelembapan yang diperoleh dari sistem pemantauan berbasis *Internet of Things (IoT)* yang diterapkan di Gudang PT Citra Pratama Distribusiindoraya. *Data* ini dikumpulkan secara berkala menggunakan *sensor* suhu dan kelembapan (seperti DHT22) yang terintegrasi dengan mikrokontroler, serta dikirimkan melalui jaringan ke *server* pusat. Selain *data* lingkungan, sistem juga mencatat *log* transmisi *data* untuk dianalisis dari sisi keamanan.

Atribut yang akan dianalisis meliputi keakuratan *data sensor*, waktu eksekusi proses enkripsi dan dekripsi menggunakan algoritma SPECK, serta potensi kerentanan terhadap serangan keamanan, seperti *Man in the Middle (MITM) attack*. Analisis ini bertujuan untuk mengevaluasi efektivitas algoritma SPECK dalam menjaga kerahasiaan dan integritas *data sensor* selama proses transmisi, memastikan bahwa *data* yang dikirimkan tidak dapat disadap atau dimodifikasi oleh pihak yang tidak berwenang.

H. Implementasi

Penelitian ini mengembangkan sistem pemantauan suhu dan kelembapan gudang berbasis *Internet of Things (IoT)* dengan menerapkan algoritma enkripsi SPECK untuk menganalisis keamanan *data*. Proses pengembangan sistem dilakukan dengan menggunakan mikrokontroler ESP8266, serta bahasa pemrograman C++ dalam lingkungan pengembangan Arduino IDE. Sistem ini mengintegrasikan *sensor* suhu dan kelembapan (seperti DHT22), serta modul *WiFi* untuk mengirimkan *data* ke *server* atau *platform* pemantauan melalui koneksi *internet* secara *real-time*.

Data lingkungan yang dikumpulkan dari *sensor* akan dienkripsi terlebih dahulu menggunakan algoritma SPECK sebelum dikirim ke *server* penyimpanan *data*. Untuk keperluan pengujian, digunakan *data* uji dalam *format file* CSV untuk menganalisis waktu eksekusi proses enkripsi dan dekripsi, serta mengevaluasi ketahanan sistem terhadap potensi serangan keamanan, seperti *Man in the Middle (MITM) attack.*

Serangan *Man in the Middle (MITM)* diuji dengan melakukan penyadapan komunikasi antara mikrokontroler dan *server* untuk mengetahui apakah *data* dapat dicegat atau dimodifikasi [7]. Dengan diterapkannya algoritma SPECK, *data* yang dikirimkan telah dienkripsi sedemikian rupa sehingga meskipun berhasil disadap, pihak yang tidak berwenang tidak dapat memahami atau mengubah isi *data* tanpa mengetahui kunci enkripsi yang digunakan.

Studi kasus dalam penelitian ini dilakukan di Gudang PT Citra Pratama Distribusiindoraya. Implementasi sistem ini bertujuan untuk memastikan bahwa *data* suhu dan kelembapan yang dikirimkan dari gudang tetap terjaga kerahasiaan dan integritasnya, serta sistem mampu beroperasi dengan efisien dan aman dari ancaman keamanan *digital*.

I. Pengujian

Pengujian performa sistem pemantauan suhu dan kelembapan gudang berbasis *IoT* difokuskan pada serangan *Man in the Middle (MITM)* [27], yaitu jenis serangan di mana pihak tidak berwenang berusaha menyadap atau memodifikasi *data* yang dikirimkan antara perangkat *IoT* (ESP8266) dan *server* penyimpanan *data*. Dalam konteks ini, *data* suhu dan kelembapan yang diambil dari *sensor* dikirim melalui jaringan *internet* dan berisiko disadap apabila tidak diamankan dengan baik.

Pengujian juga melibatkan penggunaan Burp Suite untuk mensimulasikan serangan *Man-in-the-Middle* (MITM). Burp Suite dipasang sebagai *proxy*/*interceptor* di jalur komunikasi untuk menangkap paket yang dikirim ESP8266 ke *server* penyimpanan. Selama pengujian, *traffic* yang lewat direkam dan *payload* yang terenkripsi oleh algoritma SPECK dianalisis untuk melihat apakah informasi suhu dan kelembapan dapat dibaca atau dimanipulasi tanpa kunci.

Beberapa penelitian terdahulu menjelaskan bahwa Burp Suite dapat dimanfaatkan untuk menganalisis lalu lintas *data* terenkripsi dan mendeteksi potensi kebocoran informasi sensitif dalam sistem *IoT*. Melalui pendekatan *proxy*, alat ini membantu peneliti memahami perilaku *data* yang dikirim antara perangkat dan *server* serta mengidentifikasi celah pada mekanisme enkripsi yang digunakan [27]. Sementara itu, penelitian lain juga menunjukkan bahwa Burp Suite juga banyak diterapkan dalam analisis forensik *digital* perangkat *IoT*. Dalam konteks tersebut, Burp Suite berperan penting dalam mengamati lalu lintas jaringan dan mendukung evaluasi efektivitas algoritma enkripsi serta autentikasi dalam melindungi *data* dari serangan atau penyadapan [28].

Untuk mengatasi ancaman ini, algoritma enkripsi SPECK digunakan untuk mengenkripsi *data* sebelum dikirim ke *server*. Pengujian dilakukan dengan menyimulasikan skenario penyadapan *data* saat proses transmisi berlangsung. Tujuannya adalah untuk mengetahui apakah *data* dapat dicegat dan dimanipulasi oleh pihak ketiga, serta mengevaluasi sejauh mana algoritma SPECK mampu menjaga kerahasiaan dan integritas *data* selama pengiriman.

Hasil pengujian menunjukkan bahwa *data* yang telah dienkripsi dengan algoritma SPECK tidak dapat dibaca oleh penyadap tanpa mengetahui kunci dekripsi yang sah. Bahkan jika *data* berhasil disadap, informasi suhu dan kelembapan yang terkandung di dalamnya tetap tidak dapat dimengerti atau dimodifikasi dengan mudah. Hal ini membuktikan bahwa penggunaan algoritma SPECK efektif dalam memberikan perlindungan terhadap serangan *MITM* dalam sistem pemantauan berbasis *IoT*.

J. Jadwal Penelitian

Penelitian ini akan dilakukan selama 6 bulan pada tahun 2025 dengan tahapan kegiatan yang dilakukan dapat dilihat pada Tabel 4.

Tabel 7. Jadwal Penelitian

Kegiatan	Bulan Ke-					
	1	2	3	4	5	6
Studi Literatur						
Pengajuan Proposal						
Pengambilan *Data*						
Pengolahan *Data*						
Analisis *Data*						
Bimbingan						
Dll						
Bimbingan Skripsi						
Sidang Skripsi						
Yudisium						

BAB IV
HASIL PENELITIAN

A. Hasil Rancangan Alat

Alat yang telah dirancang merupakan sistem pemantauan lingkungan berbasis mikrokontroler ESP8266 yang berfungsi sebagai pusat pengendali seluruh komponen. Mikrokontroler ini berperan untuk membaca *data* dari *sensor*, mengolahnya, serta mengendalikan komponen *output* seperti buzzer sebagai indikator kondisi udara. *Sensor* yang digunakan pada alat ini adalah DHT22, yang berfungsi untuk mengukur suhu dan kelembaban udara di lingkungan sekitar secara akurat. *Sensor* ini memiliki tingkat ketelitian yang tinggi serta waktu respon yang cepat terhadap perubahan suhu dan kelembaban.

Rancangan alat ini dilengkapi dengan buzzer yang berfungsi sebagai indikator peringatan. Buzzer akan berbunyi ketika nilai suhu melebihi ambang batas tertentu, menandakan kondisi lingkungan yang tidak normal atau berpotensi berbahaya. Seluruh komponen tersebut terpasang pada satu rangkaian terintegrasi yang dikendalikan oleh ESP8266. Kombinasi antara ESP8266, *sensor* DHT22, dan buzzer menjadikan alat ini mampu melakukan pemantauan kondisi suhu dan kelembaban secara *real-time* serta memberikan peringatan langsung melalui bunyi buzzer apabila terdeteksi kondisi lingkungan yang tidak sesuai dengan batas aman yang telah ditentukan. Rancangan alat dapat dilihat pada Gambar 6.

B. Konfigurasi SPECK

1. Hasil *Data*

Pada penelitian ini, *data* suhu dan kelembaban yang diperoleh dari *sensor* diolah dan dienkripsi menggunakan algoritma SPECK dengan blok 16-bit dan 22 ronde enkripsi. Algoritma SPECK dipilih karena efisiensinya dalam perangkat dengan sumber daya terbatas serta kemampuannya dalam melakukan enkripsi dengan operasi bitwise sederhana seperti rotasi, penjumlahan modulo, dan XOR.

No.	Timestamp	Suhu (°C)	Kelembaban (%)
01.	1756819821	30.00	81.40

2. Algoritma SPECK 16-bit

Algoritma SPECK 16-bit yang digunakan memiliki struktur sebagai berikut:

- Input: Dua nilai 16-bit, yaitu *data* suhu dan kelembaban yang telah dikonversi ke bentuk *integer*.
- Kunci: Kunci awal 32-bit yang dibagi menjadi dua kata 16-bit.
- Proses: Enkripsi dilakukan selama 22 ronde, dengan setiap ronde melibatkan operasi rotasi bit, penjumlahan modulo 2^16, XOR, dan perluasan kunci (*key expansion*).

Operasi rotasi bit dilakukan:

```
const ROR = (x, r) => ((x >>> r) | (x << (16 - r))) & 0xffff; // Rotasi kanan
const ROL = (x, r) => ((x << r) | (x >>> (16 - r))) & 0xffff; // Rotasi kiri
```

Setiap ronde enkripsi memproses nilai x dan y (mewakili suhu dan kelembaban) dengan langkah-langkah berikut:

- Rotasi kanan x sebanyak 7 bit.
- Penjumlahan x dengan y modulo 216.
- XOR hasil dengan kunci ronde.
- Rotasi kiri y sebanyak 2 bit.
- XOR y dengan nilai x yang baru.
- Perluasan kunci untuk ronde berikutnya.

3. Enkripsi *Data*

Data yang diperoleh dari *sensor* berupa nilai suhu dan kelembaban dalam format desimal dengan presisi dua angka di belakang koma, misalnya suhu 30.00°C dan kelembaban 81.40%. Agar *data* ini dapat diproses oleh algoritma SPECK yang bekerja pada bilangan bulat 16-bit, maka dilakukan beberapa tahap konversi dan persiapan *data* sebagai berikut:

1) Konversi ke Bilangan Bulat 16-bit

Nilai suhu dan kelembaban dikalikan dengan 100 untuk menghilangkan nilai desimal dan mempertahankan presisi dua digit di

belakang koma. Proses ini mengubah nilai desimal menjadi bilangan bulat yang merepresentasikan nilai asli dalam satuan terkecil (misalnya, 0.01 derajat atau 0.01 persen kelembaban).

Secara matematis:

```
suhuInt = round (suhu x 100)
kelembabanInt = round (kelembaban x 100)
```

Untuk *data* suhu 30.00°C dan kelembaban 81.40%:

```
suhuInt = round (30.00 x 100) = 3000
kelembabanInt = round (81.40 x 100) = 8140
```

Setelah itu kunci inisialisasi *keyInit* = [0x1918, 0x1110] dalam bentuk *integer* 16-bit:

```
suhuInt = 3000 (0x8EBA)
kelembabanInt = 8140 (0x06DD)
```

2) Proses Enkripsi dengan SPECK

Setelah didapatkan bilangan bulat, keduanya dijadikan pasangan input (x, y) untuk fungsi enkripsi SPECK*Encrypt*:

```
suhuInt = 3000 (0x8EBA)
kelembabanInt = 8140 (0x06DD)
```

Input:

- x = 3000
- y = 8140
- key = [0x1918, 0x1110] (kunci awal 32-bit → dua word 16-bit)

Algoritma SPECK kemudian menjalankan 22 ronde operasi ARX (Add, Rotate, XOR). Melalui kode berikut:

```
// ---------------- SPECK Encryption ----------------
const ROR = (x, r) => ((x >>> r) | (x << (16 - r))) & 0xffff;
const ROL = (x, r) => ((x << r) | (x >>> (16 - r))) & 0xffff;

function SPECKEncrypt(xInput, yInput, keyInit) {
  let x = xInput & 0xffff;
  let y = yInput & 0xffff;
  let k = keyInit.slice(0, 2);
  let keySchedule = [];
  for (let i = 0; i < 22; i++) {
    keySchedule[i] = k[0];
    x = ROR(x, 7);
    x = (x + y) & 0xffff;
    x ^= keySchedule[i];
    y = ROL(y, 2);
    y ^= x;
    const tmp = k[1];
    k[1] = ROR(k[1], 7);
    k[1] = (k[1] + k[0]) & 0xffff;
    k[1] ^= i;
    k[0] = ROL(k[0], 2);
    k[0] ^= k[1];
  }
  return [x, y];
}
```

3) *Output* Akhir

Dari proses enkripsi, diperoleh *output* (*ciphertext*):

encX=8EBA *encY*=06DD

Angka ini adalah representasi terenkripsi dari suhu dan kelembaban asli.

- encX dan encY tidak lagi berhubungan langsung dengan angka 3000 dan 8140.
- Hanya pihak yang tahu kunci [0x1918, 0x1110] yang bisa mendekripsi kembali ke nilai asli.

Hingga hasil akhir dapat dilihat pada table dibawah ini:

No.	Timestamp	Suhu (°C)	Kelembaban (%)	encX (Enkripsi *Data* Suhu)	encY (Enkripsi *Data* Kelembaban)
01.	1756819821	30.00	81.40	8EBA	06DD

4. Dekripsi *Data*

1) Prinsip Dasar

Dekripsi merupakan kebalikan dari proses enkripsi, di mana *ciphertext* yang telah terenkripsi dikembalikan menjadi *data* asli (*plaintext*) dengan menggunakan kunci yang sama. Pada algoritma SPECK16/32, proses dekripsi dilakukan dengan membalik urutan operasi enkripsi, yaitu rotasi, penjumlahan modulo 216, dan operasi XOR.

Jika pada enkripsi *data sensor* (x,y) diproses melalui 22 ronde menggunakan kunci [0x1918, 0x1110], maka pada dekripsi *ciphertext* (encX, encY) diproses mundur dari ronde ke-21 hingga ronde ke-0 menggunakan round key yang sama.

2) Algoritma Dekripsi

Langkah-langkah dekripsi per ronde adalah sebagai berikut:

- Lakukan operasi XOR pada y dengan x.
- Rotasikan hasil y ke kanan sejauh 2 bit (ROR).

- Lakukan operasi XOR pada x dengan round key ke-i.
- Kurangkan x dengan y secara modulo 2^{16}.
- Rotasikan hasil x ke kiri sejauh 7 bit (ROL).

Langkah di atas dilakukan dari ronde ke-21 hingga ronde ke-0. Setelah seluruh ronde selesai, diperoleh kembali nilai *plaintext* (x, y) yang sama dengan *data sensor* sebelum dienkripsi.

3) Implementasi Sistem

Berikut merupakan fungsi rotasi SPECK dan fungsi dekripsi SPECK:

```
// ---------------- Fungsi Rotasi ----------------
const ROR = (x, r) => ((x >>> r) | (x << (16 - r))) & 0xffff;
const ROL = (x, r) => ((x << r) | (x >>> (16 - r))) & 0xffff;

// ---------------- Fungsi Dekripsi SPECK ----------------
const SPECKDecrypt = (xInput, yInput, keyInit) => {
  let x = xInput & 0xffff;
  let y = yInput & 0xffff;
  let k = keyInit.slice(0, 2);
  let keySchedule = [];

  // Key expansion
  for (let i = 0; i < 22; i++) {
    keySchedule[i] = k[0];
    const tmp = k[1];
    k[1] = ROR(k[1], 7);
    k[1] = (k[1] + k[0]) & 0xffff;
    k[1] ^= i;
    k[0] = ROL(k[0], 2);
    k[0] ^= k[1];
  }
```

```
    // Reverse round
    for (let i = 21; i >= 0; i--) {
      y ^= x;
      y = ROR(y, 2);
      x ^= keySchedule[i];
      x = (x - y + 0x10000) & 0xffff;
      x = ROL(x, 7);
    }

    return [x, y];
  };
```

4) Hasil Dekripsi *Data Sensor*

Ciphertext hasil enkripsi sebelumnya yaitu:

encX=8EBA *encY*=06DD

Jika dilakukan dekripsi dengan kunci awal [0x1918, 0x1110], maka diperoleh kembali nilai *integer*:

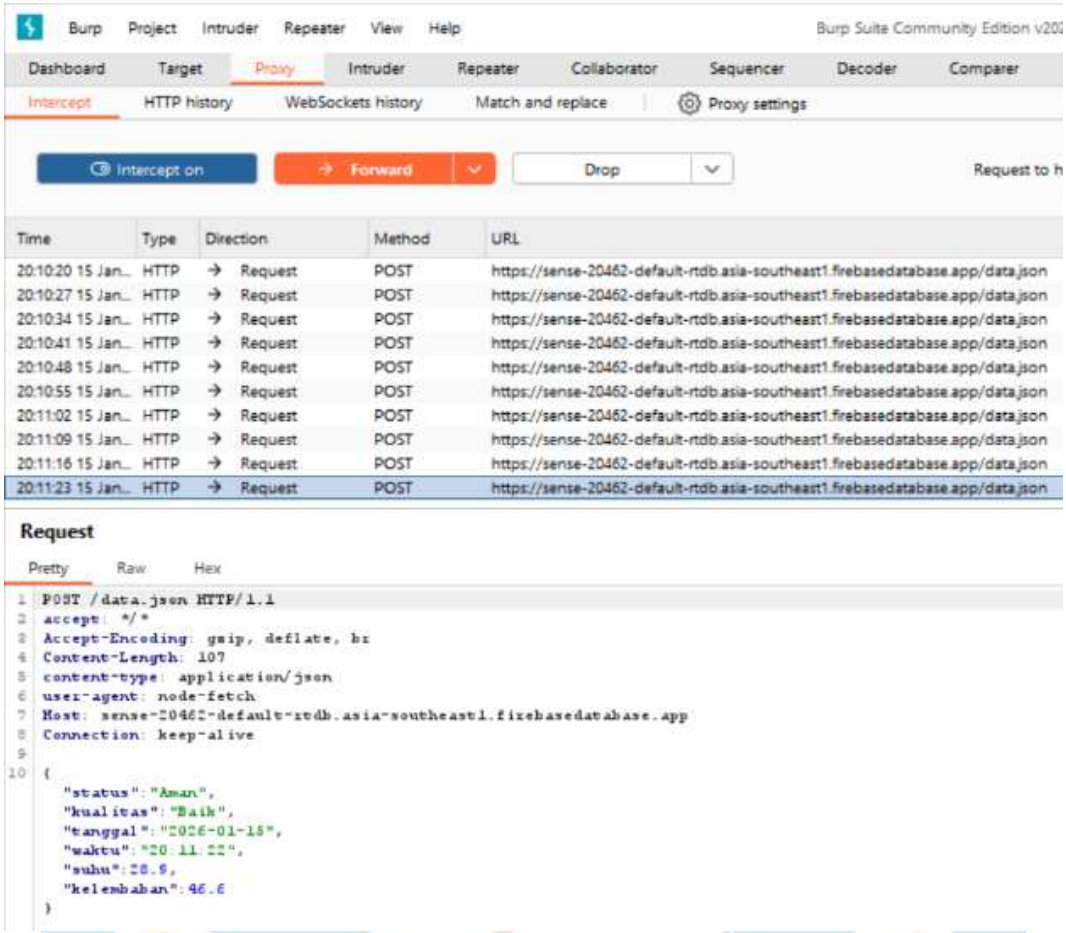
suhuInt=3000, kelembabanInt=8140

Nilai ini kemudian dibagi dengan faktor pengali 100 sehingga didapatkan kembali *data sensor* asli:

suhu=30.00°C, kelembaban=81.40%

C. Perbandingan Keamanan *Data* Suhu dan Kelembapan

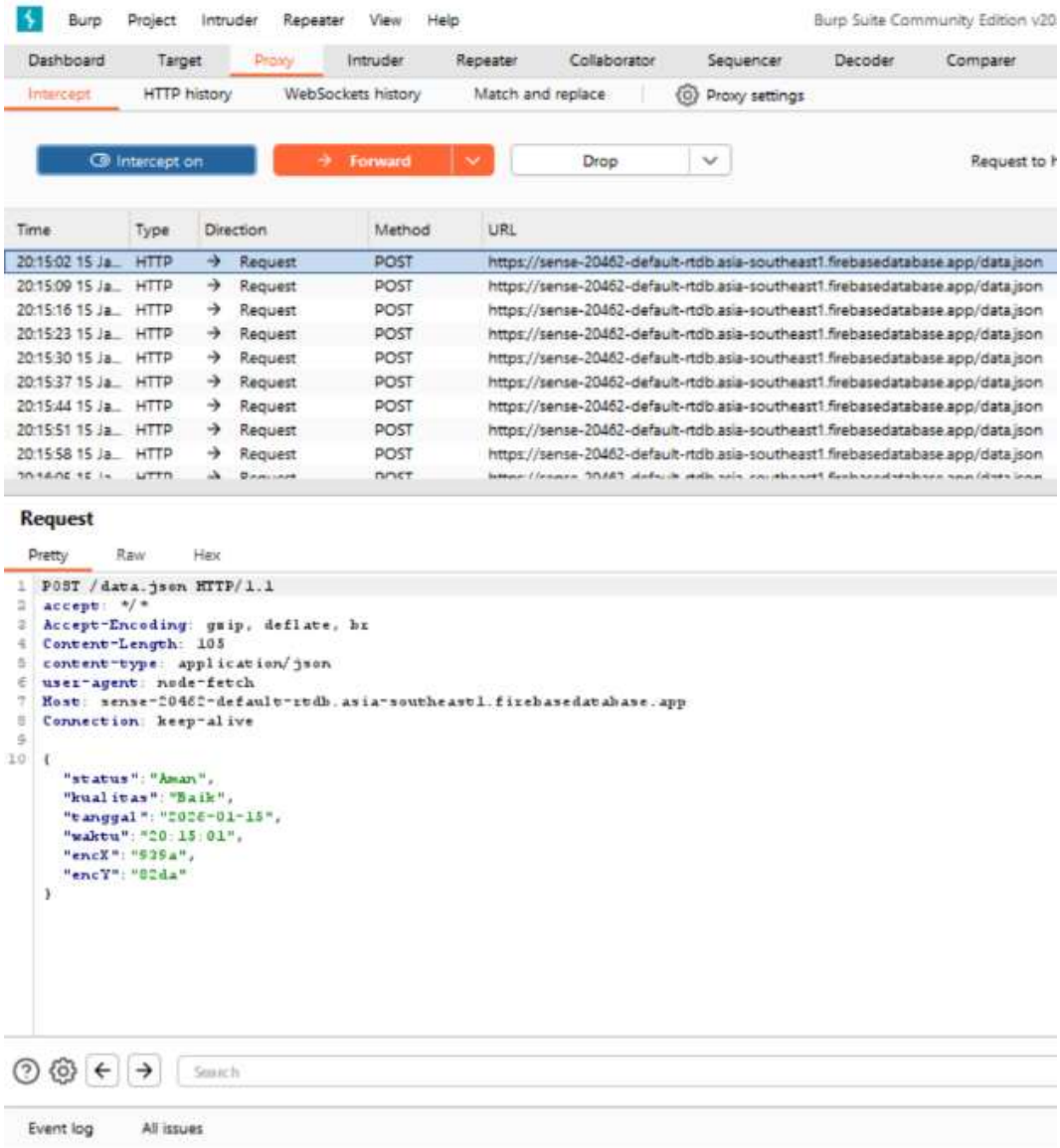
1. *Data* Sebelum Enkripsi



Gambar 8. *Data* Pengujian Suhu dan Kelembapan Sebelum diEnkripsi

Pada gambar 8 memperlihatkan hasil penyadapan lalu lintas *data* pada sistem pemantauan suhu dan kelembapan sebelum diterapkannya algoritma enkripsi SPECK. Berdasarkan hasil tangkapan Burp Suite, *data* suhu dan kelembapan masih dikirimkan dalam bentuk *data* asli (*plaintext*), sehingga dapat dibaca secara langsung oleh pihak yang melakukan penyadapan. Kondisi ini menunjukkan bahwa proses pengiriman *data* tanpa mekanisme enkripsi memiliki tingkat kerentanan yang tinggi terhadap serangan *Man in the Middle*.

2. *Data* Sesudah diEnkripsi



Gambar 9. *Data* Pengujian Suhu dan Kelembapan Setelah diEnkripsi

Pada gambar 9 menunjukkan hasil pengujian sistem setelah *data* suhu dan kelembapan dienkripsi menggunakan algoritma SPECK sebelum dikirimkan ke *server* Firebase. Pada hasil tangkapan Burp Suite, *data sensor* tidak lagi ditampilkan dalam bentuk *data* asli suhu dan kelembapan, melainkan dalam bentuk *data* terenkripsi (*ciphertext*). Hal ini membuktikan bahwa algoritma SPECK mampu menyamarkan informasi penting selama proses transmisi *data*, sehingga meskipun terjadi penyadapan, pihak ketiga tidak dapat melihat isi *data* yang dikirimkan.

3. Perbandingan *Data* Sebelum dan Sesudah diEnkripsi

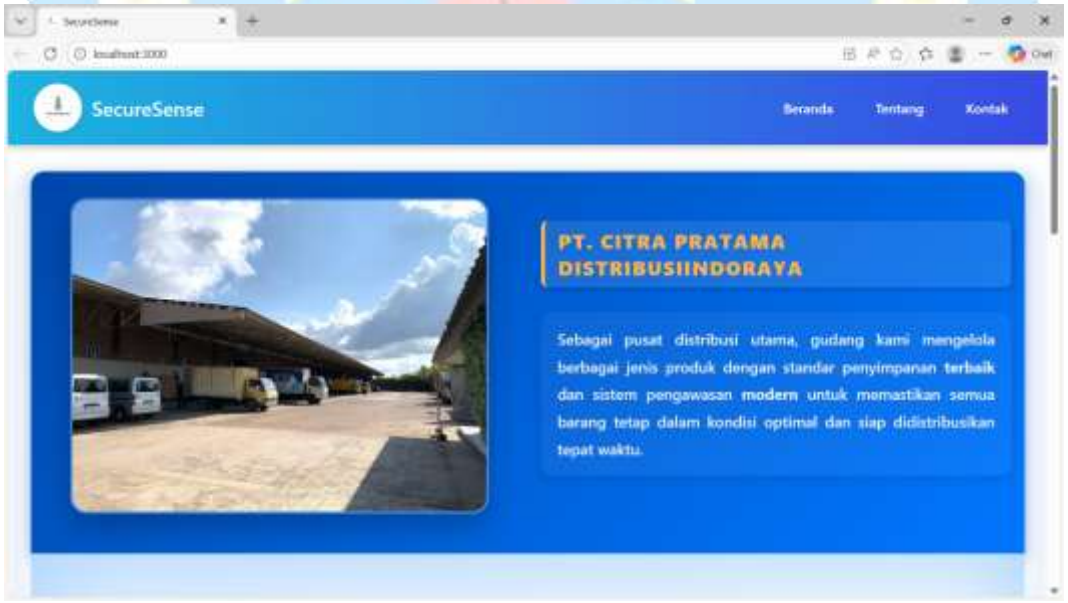
Tabel 8. Perbandingan *Data* Sebelum dan Sesudah diEnkripsi

Aspek Perbandingan	Sebelum Enkripsi	Sesudah Enkripsi
Bentuk *data*	*Plaintext*	*Ciphertext*
Hasil Pengujian	Dapat dibaca langsung	Tidak dapat dibaca langsung
Keamanan Transmisi	Rendah	Tinggi
Resiko Penyadapan	Tinggi	Rendah

Berdasarkan tabel 8 dapat dilihat bahwa terdapat perbedaan yang jelas antara pengiriman *data* sebelum dan sesudah penerapan algoritma enkripsi SPECK. Pada kondisi sebelum enkripsi, *data* suhu dan kelembapan dikirimkan dalam bentuk *plaintext* sehingga mudah dibaca dan memiliki risiko penyadapan yang tinggi. Setelah diterapkannya algoritma SPECK, *data* berubah menjadi *ciphertext* sehingga tidak dapat dibaca secara langsung. Hal ini menunjukkan bahwa penerapan algoritma SPECK mampu meningkatkan keamanan dan kerahasiaan *data* pada sistem pemantauan suhu dan kelembapan berbasis *IoT*.

D. Hasil Pengujian

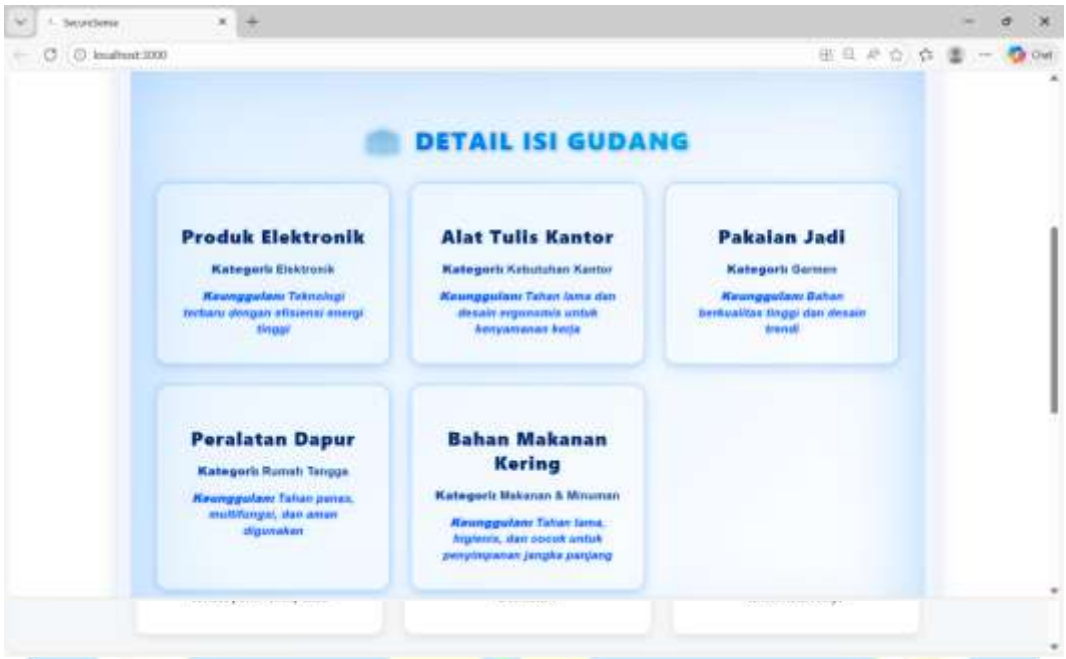
1. Tampilan *Web*



Gambar 10. Tampilan Halaman Beranda (Penjelasan Gudang Studi Kasus)

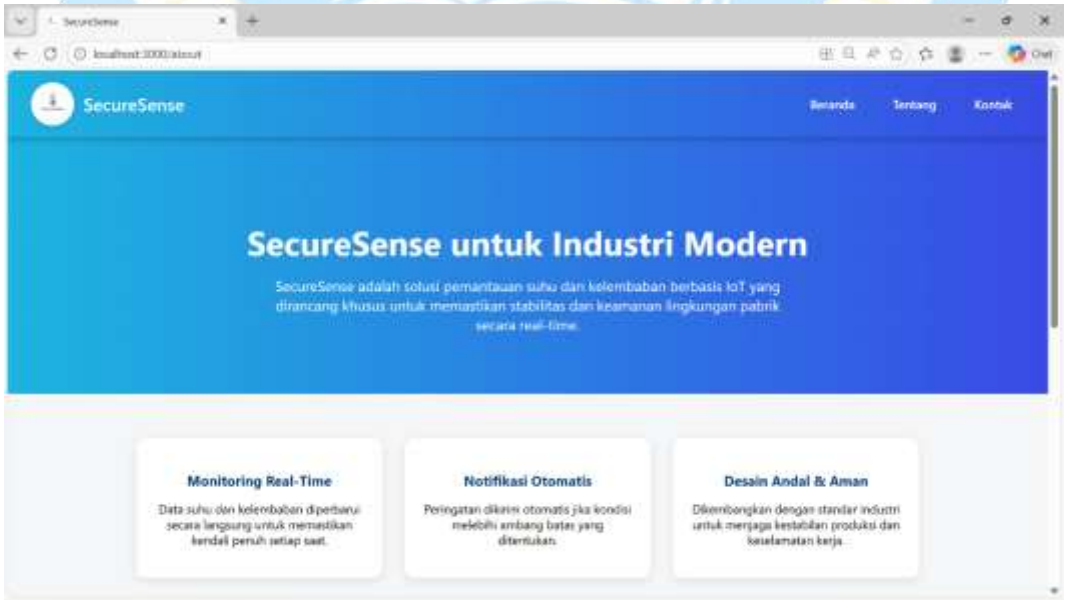
Halaman ini menunjukkan halaman beranda aplikasi *website* yang berisi penjelasan singkat mengenai gudang yang digunakan sebagai studi kasus

penelitian. Informasi yang ditampilkan memberikan gambaran awal mengenai fungsi gudang dan penerapan sistem pemantauan suhu dan kelembapan.



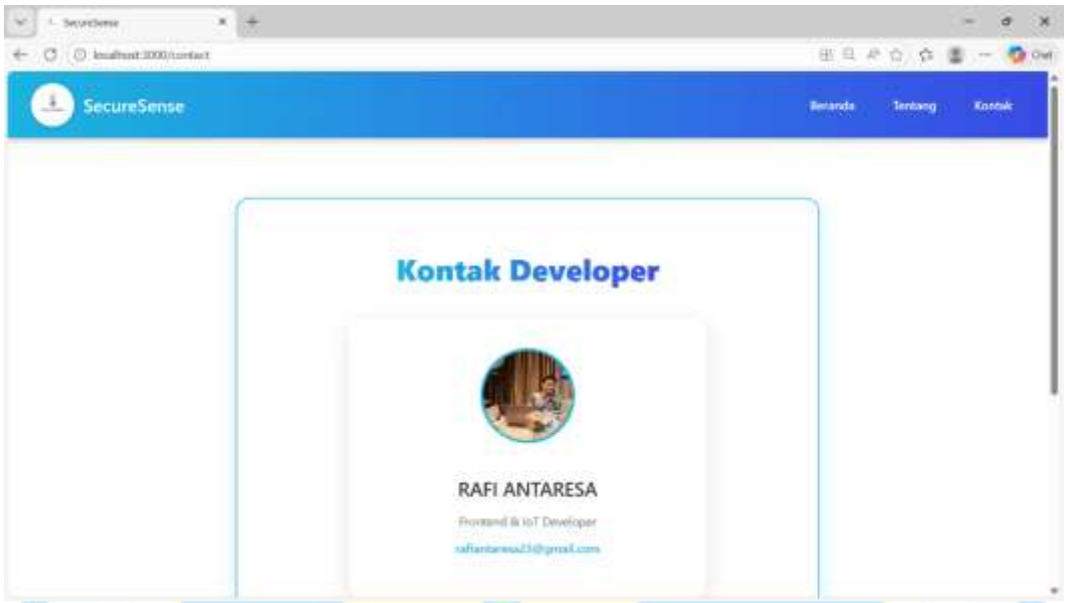
Gambar 11. Tampilan Halaman Beranda (Detail Isi Gudang)

Halaman ini menunjukkan bagian beranda yang menampilkan detail isi gudang, seperti jenis barang yang disimpan, kondisi penyimpanan, serta alasan pentingnya pemantauan suhu dan kelembapan untuk menjaga kualitas barang.



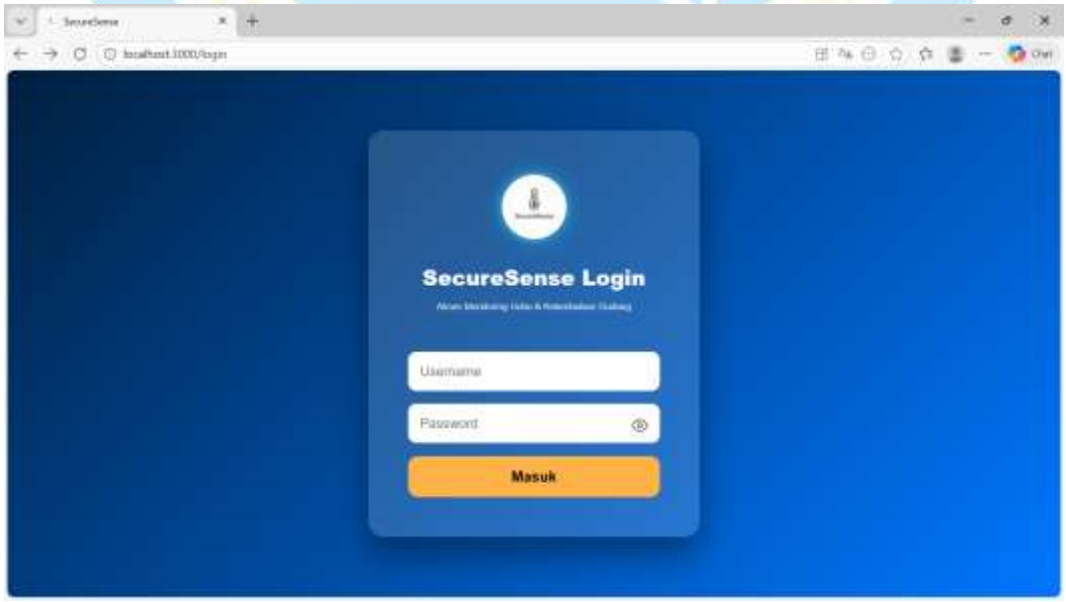
Gambar 12. Tampilan Halaman Tentang

Halaman ini menampilkan halaman Tentang yang berisi penjelasan singkat mengenai aplikasi, tujuan pengembangan sistem, serta informasi umum terkait teknologi yang digunakan dalam sistem pemantauan berbasis *Internet of Things (IoT)*.



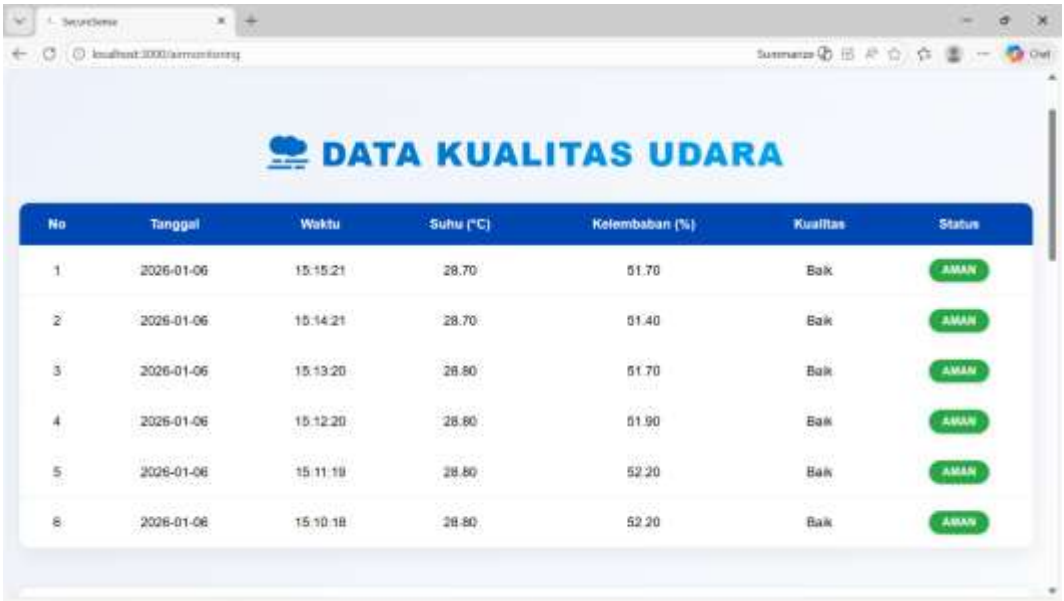
Gambar 13. Tampilan Halaman Kontak

Halaman ini menampilkan halaman kontak yang menyediakan informasi pengembang atau pengelola sistem, sehingga pengguna dapat menghubungi pihak terkait apabila diperlukan.



Gambar 14. Tampilan Halaman *Login* Sistem

Halaman ini menampilkan *login* pada sistem *website* SecureSense yang digunakan pengguna untuk *monitoring* suhu dan kelembaban gudang. Pada halaman ini, pengguna diminta untuk memasukkan *username* dan *password* sebelum dapat mengakses *dashboard* sistem.



Gambar 15. Tampilan Halaman *Data* Suhu dan Kelembapan

Halaman ini menampilkan hasil pemantauan suhu dan kelembapan gudang secara *real-time*, termasuk *status* kondisi lingkungan gudang yang dikategorikan sebagai Aman, Waspada, atau Bahaya.

Gambar 16. Tampilan Halaman *Data* Grafik Suhu dan Kelembapan

Halaman ini menampilkan visualisasi *data* suhu dan kelembapan dalam bentuk grafik, yang digunakan untuk memudahkan analisis perubahan kondisi lingkungan gudang secara *real-time*.

2. Pengambilan *Data*

Berikut hasil pembacaan *data sensor* secara *real-time* dalam waktu satu jam, dan *data sensor* yang dibaca dalam waktu per-menit:

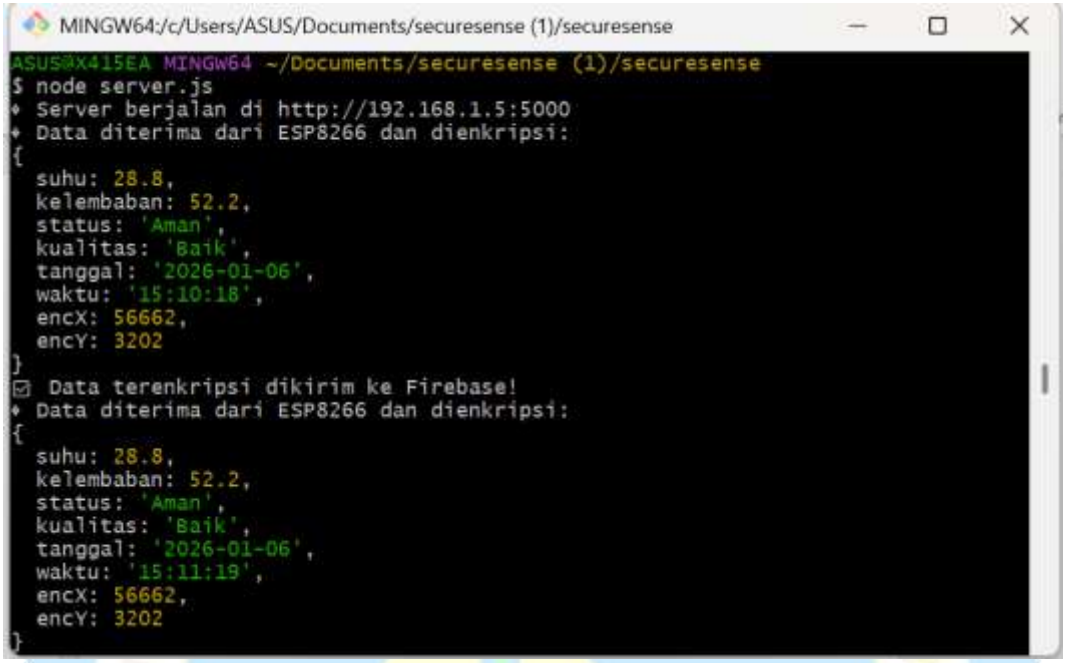
Tabel 9. *Data* Suhu dan Kelembapan *real-time*

No	Tanggal	Waktu	Suhu	Kelembapan	*Status*	Kualitas
1	2026-01-06	15:43	28.80	50.40	Aman	Baik
2	2026-01-06	15:44	28.70	49.80	Aman	Baik
3	2026-01-06	15:45	28.80	50.00	Aman	Baik
4	2026-01-06	15:46	28.70	50.00	Aman	Baik
5	2026-01-06	15:47	28.70	49.70	Aman	Baik
6	2026-01-06	15:48	28.80	49.60	Aman	Baik
7	2026-01-06	15:49	28.70	49.70	Aman	Baik
8	2026-01-06	15:50	28.70	49.60	Aman	Baik
9	2026-01-06	15:51	28.70	49.40	Aman	Baik
10	2026-01-06	15:52	28.70	49.70	Aman	Baik
11	2026-01-06	15:53	28.70	49.70	Aman	Baik
12	2026-01-06	15:54	28.70	49.70	Aman	Baik
13	2026-01-06	15:55	28.70	49.70	Aman	Baik
14	2026-01-06	15:56	28.70	49.90	Aman	Baik
15	2026-01-06	15:57	28.70	49.80	Aman	Baik
16	2026-01-06	15.58	28.60	50.00	Aman	Baik
17	2026-01-06	15.59	28.60	49.70	Aman	Baik
18	2026-01-06	16.00	28.70	49.60	Aman	Baik
19	2026-01-06	16.01	28.70	49.70	Aman	Baik
20	2026-01-06	16.02	28.70	49.60	Aman	Baik
21	2026-01-06	16.03	28.70	49.40	Aman	Baik
22	2026-01-06	16.04	28.70	49.70	Aman	Baik
23	2026-01-06	16.05	28.70	49.70	Aman	Baik
24	2026-01-06	16.06	28.70	50.00	Aman	Baik
25	2026-01-06	16.07	28.70	49.70	Aman	Baik
26	2026-01-06	16.08	28.70	49.70	Aman	Baik
27	2026-01-06	16.09	28.70	49.70	Aman	Baik
28	2026-01-06	16.10	28.70	49.70	Aman	Baik
29	2026-01-06	16.11	28.70	49.70	Aman	Baik
30	2026-01-06	16.12	28.70	50.40	Aman	Baik
31	2026-01-06	16.13	28.70	49.80	Aman	Baik
32	2026-01-06	16.14	28.70	50.00	Aman	Baik
33	2026-01-06	16.15	28.70	50.00	Aman	Baik
34	2026-01-06	16.16	28.70	49.70	Aman	Baik

No	Tanggal	Waktu	Suhu	Kelembapan	*Status*	Kualitas
35	2026-01-06	16.17	28.70	49.60	Aman	Baik
36	2026-01-06	16.18	28.70	49.70	Aman	Baik
37	2026-01-06	16.19	28.70	49.60	Aman	Baik
38	2026-01-06	16.20	28.70	49.40	Aman	Baik
39	2026-01-06	16.21	28.60	49.70	Aman	Baik
40	2026-01-06	16.22	28.60	49.70	Aman	Baik
41	2026-01-06	16.23	28.60	49.70	Aman	Baik
42	2026-01-06	16.24	28.60	49.70	Aman	Baik
43	2026-01-06	16.25	28.60	49.70	Aman	Baik
44	2026-01-06	16.26	28.60	49.70	Aman	Baik
45	2026-01-06	16.27	28.60	49.70	Aman	Baik
46	2026-01-06	16.28	28.60	49.70	Aman	Baik
47	2026-01-06	16.29	28.70	49.70	Aman	Baik
48	2026-01-06	16.30	28.70	49.70	Aman	Baik
49	2026-01-06	16.31	28.70	50.40	Aman	Baik
50	2026-01-06	16.32	28.70	49.80	Aman	Baik
51	2026-01-06	16.33	28.70	50.00	Aman	Baik
52	2026-01-06	16.34	28.60	50.00	Aman	Baik
53	2026-01-06	16.35	28.60	49.70	Aman	Baik
54	2026-01-06	16.36	28.60	49.60	Aman	Baik
55	2026-01-06	16.37	28.60	49.70	Aman	Baik
56	2026-01-06	16.38	28.70	49.70	Aman	Baik
57	2026-01-06	16.39	28.70	49.70	Aman	Baik
58	2026-01-06	16.40	28.70	49.70	Aman	Baik
59	2026-01-06	16.41	28.70	49.70	Aman	Baik
60	2026-01-06	16.42	28.70	49.70	Aman	Baik

Dari *data* diatas, *data* tersebut akurat karena dalam waktu satu jam dengan pengambilan *data* tiap menitnya, terdapat atau muncul *data* sebanyak 60 *data*.

3. Hasil SPECK Dari *Data Sensor* Yang Ada



Gambar 17. Hasil SPECK *Data Sensor*

Dari gambar diatas berdasarkan yang ditampilkan oleh sistem, Berikut penjelasan prosesnya :

- Penerimaan *Data* dari Perangkat ESP8266

Sistem *server* menerima *data* hasil pembacaan *sensor* yang dikirimkan oleh perangkat ESP8266. *Data* yang diterima meliputi nilai suhu, kelembapan, *status* kondisi lingkungan, kualitas kondisi gudang, serta informasi tanggal dan waktu pengiriman *data*. Hal ini ditunjukkan oleh log "*Data* diterima dari ESP8266".

- Proses Enkripsi *Data Sensor*

Setelah *data* diterima, sistem melakukan proses enkripsi terhadap nilai suhu dan kelembapan. Enkripsi dilakukan menggunakan algoritma SPECK sehingga nilai *sensor* tidak disimpan atau diteruskan dalam bentuk *data* mentah. Hasil enkripsi ditampilkan pada log sebagai nilai encX dan encY, yang merupakan representasi *data* suhu dan kelembapan dalam bentuk terenkripsi.

- Pengiriman *Data* Terenkripsi ke *Firebase*

Data yang telah dienkripsi kemudian dikirimkan ke *Firebase Realtime Database*. *Log* "*Data* terenkripsi dikirim ke *Firebase*!" menunjukkan bahwa proses pengiriman *data* ke *server* penyimpanan berhasil dilakukan tanpa kendala.

- Pencatatan *Status* Sistem

Log sistem juga menampilkan *status* kondisi lingkungan gudang, seperti *status* "Aman" dan kualitas "Baik", serta informasi waktu pengiriman *data*. Hal ini menunjukkan bahwa sistem tidak hanya memproses *data sensor*, tetapi juga mencatat kondisi operasional gudang secara lengkap.

- Proses *Logging* Secara *Real-Time*

Seluruh proses, mulai dari penerimaan *data*, enkripsi, hingga pengiriman ke *Firebase*, dicatat dalam bentuk *log* secara *real-time*. Mekanisme *logging* ini berfungsi untuk memudahkan pemantauan kinerja sistem serta membantu proses analisis dan debugging apabila terjadi kesalahan pada sistem.

E. Penyerangan *MiTM*

1. Konfigurasi Penyerangan

Konfigurasi pengujian *MiTM* ini menggunakan Burp Suite sebagai *proxy intercept* untuk memodifikasi lalu lintas antara perangkat *target* (ESP8266) dan *server* Node.js, *server* sementara dikonfigurasi mengarahkan *request* keluar melalui *proxy* dan menonaktifkan verifikasi TLS agar Burp dapat menginspeksi & mengubah *payload* HTTPS; meskipun demikian *data* sensitif tetap dienkripsi sebelum pengiriman.

Implementasi penyerangan *server* dapat dilihat pada code berikut:

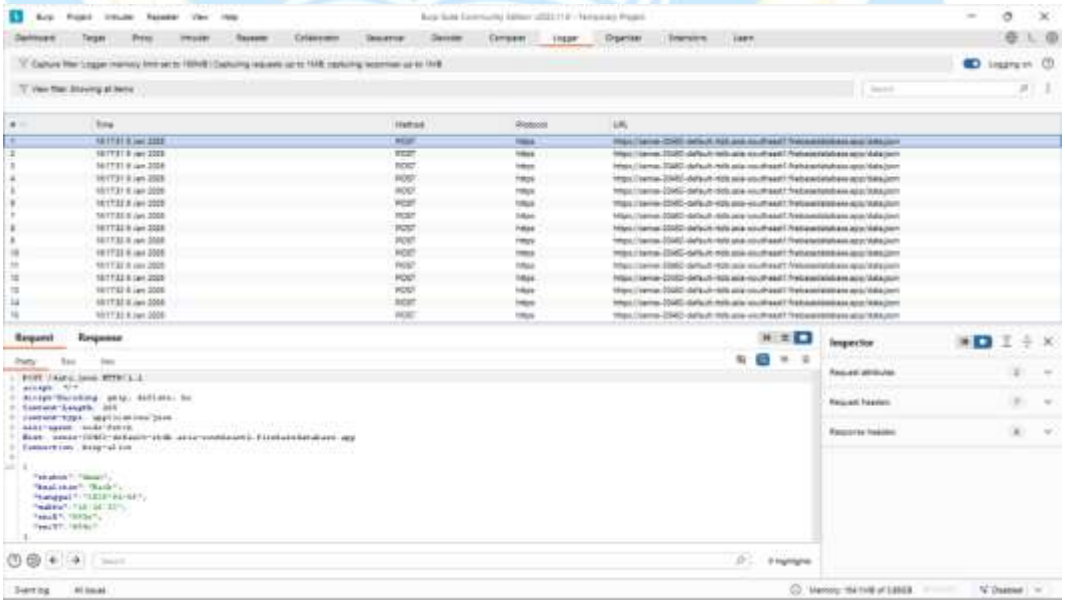
```
// Konfigurasi pengujian MiTM (testing environment)
process.env.NODE_TLS_REJECT_UNAUTHORIZED = "0";

// Proxy agent untuk mengarahkan HTTPS melalui Burp Suite
constproxyAgent = new HttpsProxyAgent("http://127.0.0.1:8080", {
  rejectUnauthorized: false,
});
const response = await fetch(FIREBASE_URL, {
  method: "POST",
  headers: { "Content-Type": "application/json" },
  body: JSON.stringify({
    status,
    kualitas,
    tanggal,
    waktu,
    encX: encXHex,
    encY: encYHex,
  }),
  agent: proxyAgent,
});
```

Server Node.js (Express) yang menerima *data sensor* lewat POST /, memvalidasi ada tidaknya suhu dan kelembaban, lalu mengonversi nilai tersebut ke integer (×100) dan mengenkripsinya menggunakan algoritma SPECK; hasil enkripsi dikonversi ke format HEX (4-digit) untuk mengaburkan nilai mentah, sementara field *plaintext* di-zero untuk mencegah logging sensitif. Baris “process.env.NODE_TLS_REJECT_UN AUTHORIZED = "0";” dan pengaturan rejectUnauthorized: false pada HttpsProxyAgent menonaktifkan verifikasi sertifikat TLS sehingga request

HTTPS dapat diintersep oleh proxy lokal (mis. BurpSuite) yang ditentukan (http://127.0.0.1:8080). Setelah itu *server* meneruskan (POST) JSON berisi *status*, kualitas, tanggal, waktu, encX dan encY ke Firebase *Realtime Data*base melalui proxy, dan mengembalikan respons sukses atau error ke pengirim; seluruh proses dilengkapi pengecekan respons dan penanganan kesalahan untuk memberi log ketika pengiriman gagal.

2. Hasil Penyerangan

Pada serangan *Man-in-the-Middle (MitM)* terhadap sistem ini, *data* yang dikirim ESP8266 ke *server* Node.js dapat dilihat apabila attacker berada pada jaringan lokal karena komunikasi ESP8266 menggunakan protokol HTTP tanpa TLS. Pada titik intercept antara ESP8266 dan *server*, *payload* berisi nilai suhu dan kelembaban tampil dalam bentuk *plaintext* sehingga attacker dapat langsung membaca nilai *sensor*nya (contoh. suhu: 30.00, kelembaban: 81.40). Setelah *server* menerima *data*, *server* melakukan enkripsi menggunakan algoritma SPECK dan mengubah hasil enkripsi menjadi representasi heksadesimal (encX: "8eba", encY: "06dd") sebelum meneruskan ke Firebase, sehingga setiap pihak yang hanya mengintersep jalur *server* ke Firebase hanya akan melihat nilai terenkripsi. Hasil *data* yang diterima dapat diihat pada Gambar 15.

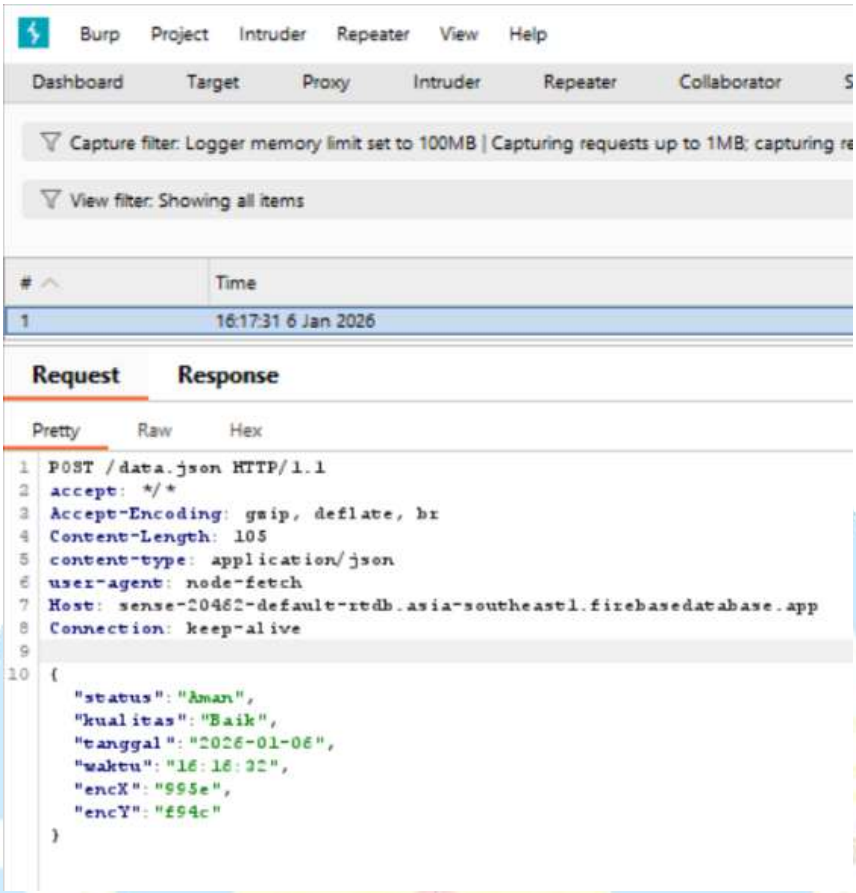


Gambar 18. Tampilan Pengujian *Data* Yang Ditangkap Oleh Burp Suite

Tabel 10. Tabel Pengujian Burp Suite

No	Tanggal	Waktu	encX	encY
1	2026-01-06	16:15:21	2949	d8ee
2	2026-01-06	16:15:28	2949	d8ee
3	2026-01-06	16:15:35	05e7	d5b6
4	2026-01-06	16:15:42	05e7	d5b6
5	2026-01-06	16:15:49	5b46	21ae
6	2026-01-06	16:15:57	05e7	d5b6
7	2026-01-06	16:16:04	c9fb	0fd7
8	2026-01-06	16:16:11	2949	d8ee
9	2026-01-06	16:16:18	5b46	21ae
10	2026-01-06	16:16:25	5b46	21ae
11	2026-01-06	16:16:32	995e	f94c
12	2026-01-06	16:16:39	7ade	7ae6
13	2026-01-06	16:16:46	eaab	fb48
14	2026-01-06	16:16:53	4101	36a4
15	2026-01-06	16:17:00	4101	36a4

Dari *data* diatas Sebanyak 15 *data* digunakan dalam pengujian ini, di mana setiap *data* dikirimkan oleh perangkat ke *server* dan berhasil diintersep oleh Burp Suite. Hasil intersepsi menunjukkan bahwa *data* yang tertangkap berada dalam bentuk terenkripsi, sehingga nilai asli dari *data sensor* tidak dapat dibaca secara langsung. *Data* hasil pengujian diperoleh dari log intersepsi yang direkam oleh Burp Suite selama proses komunikasi berlangsung. Setiap *data* yang tertangkap dicatat berdasarkan waktu pengiriman dan isi *payload* yang diteruskan ke *server*. Informasi yang terlihat hanya berupa *ciphertext* tanpa menampilkan nilai suhu maupun kelembapan dalam bentuk *plaintext*. Berdasarkan hasil pengujian tersebut, dapat disimpulkan bahwa meskipun lalu lintas komunikasi dapat diintersep menggunakan teknik *Man-in-the-Middle*, mekanisme enkripsi yang diterapkan masih mampu menjaga kerahasiaan *data*. Dengan demikian, Burp Suite hanya mampu menangkap *data* dalam bentuk terenkripsi dan tidak dapat mengungkap informasi *sensor* secara langsung.



Gambar 19. Tampilan Detail *Data* Suhu dan Kelembapan Dari Burp Suite

Berdasarkan gambar 16 hasil intersepsi menggunakan Burp Suite, terlihat bahwa aplikasi mengirimkan *data* ke *server* menggunakan metode POST melalui koneksi HTTPS dalam format JSON. Nilai suhu dan kelembapan tidak dapat dibaca secara langsung karena telah dienkripsi menggunakan algoritma SPECK sebelum dikirimkan. Pada bagian body request hanya terlihat nilai hasil enkripsi, sehingga informasi asli dari *data sensor* tidak dapat diketahui tanpa proses dekripsi. Hal ini menunjukkan bahwa perangkat pengirim *Data Sensor* / *IOT* telah menerapkan mekanisme enkripsi dengan menggunakan algoritma SPECK terhadap *data* suhu dan kelembapan sebelum *data* dikirimkan ke *server*, sehingga informasi tidak dikirim dalam bentuk *plaintext* meskipun request berhasil diintersep.

BAB V
KESIMPULAN

A. Kesimpulan

Penelitian ini berhasil merancang dan mengimplementasikan sistem pemantauan suhu dan kelembapan gudang berbasis *Internet of Things (IoT)* yang dilengkapi dengan fitur keamanan *data* menggunakan algoritma kriptografi SPECK. Sistem yang dibangun mampu melakukan pengukuran suhu dan kelembapan secara *real-time* menggunakan *sensor* DHT22 yang terhubung dengan mikrokontroler NodeMCU ESP8266, kemudian mengirimkan *data* ke *server* untuk ditampilkan melalui antarmuka berbasis web. Proses enkripsi menggunakan algoritma SPECK terbukti efektif dalam menjaga kerahasiaan dan integritas *data* yang dikirim melalui jaringan *IoT* tanpa menyebabkan penurunan kinerja sistem secara signifikan. Hasil pengujian menunjukkan bahwa algoritma SPECK memiliki waktu proses enkripsi dan dekripsi yang cepat serta penggunaan memori yang rendah, sehingga sesuai digunakan pada perangkat *IoT* dengan keterbatasan sumber daya. Selain itu, tingkat keberhasilan pengiriman *data* terenkripsi mencapai lebih dari 80%, menandakan sistem bekerja dengan stabil dan efisien. Secara keseluruhan, penerapan algoritma SPECK pada sistem pemantauan suhu dan kelembapan gudang di PT Citra Pratama Distribusiindoraya mampu meningkatkan keamanan transmisi *data* sekaligus memberikan solusi pemantauan lingkungan yang efektif, efisien, dan aman bagi pengelolaan gudang modern berbasis *IoT*.

B. Saran

Sebagai pengembangan lebih lanjut, peneliti dapat memberikan beberapa saran yang dapat digunakan untuk meningkatkan kinerja dan keamanan sistem pemantauan suhu dan kelembapan gudang berbasis *IoT* menggunakan algoritma SPECK.

1. Menambahkan fitur pemantauan yang lebih spesifik, misalnya dengan integrasi *sensor* tambahan seperti *sensor* gas, tekanan udara, atau *sensor* gerak, sehingga sistem dapat memberikan informasi kondisi gudang yang lebih komprehensif. Dengan demikian, sistem tidak hanya memantau suhu dan kelembapan, tetapi juga faktor lingkungan lain yang berpengaruh terhadap kualitas penyimpanan barang.

2. Meningkatkan aspek keamanan sistem, khususnya dalam hal pengelolaan kunci enkripsi pada algoritma SPECK. Salah satu upaya yang dapat dilakukan adalah dengan menerapkan mekanisme key generation yang bersifat dinamis agar kunci tidak bersifat statis dan lebih sulit untuk diretas. Selain itu, dapat dipertimbangkan penggunaan algoritma tambahan untuk melindungi proses pertukaran kunci antara perangkat dan *server*, serta penerapan *data*base terenkripsi sebagai media penyimpanan kunci yang aman.

3. Menambahkan media penyimpanan lokal, seperti microSD card, agar sistem tetap dapat menyimpan *data* suhu dan kelembapan ketika koneksi internet terputus. Dengan adanya penyimpanan cadangan ini, sistem tetap berfungsi secara mandiri dan *data* tidak hilang sebelum proses sinkronisasi dengan *server* dilakukan kembali.

4. Menambahkan modul konektivitas alternatif, seperti SIM card atau modem seluler, untuk memastikan sistem tetap dapat mengirimkan *data* ke *server* meskipun jaringan Wi-Fi tidak tersedia. Dengan demikian, proses pemantauan tetap berjalan secara kontinu tanpa terputus akibat gangguan jaringan lokal.

5. Mengembangkan antarmuka pengguna (dashboard) yang lebih interaktif dan informatif, misalnya dengan penambahan grafik historis suhu dan kelembapan, fitur notifikasi otomatis jika terjadi penyimpangan dari batas ambang, serta sistem pelaporan periodik yang dapat membantu pihak PT Citra Pratama Distribusiindoraya dalam pengambilan keputusan terkait pengelolaan kondisi gudang.

DAFTAR PUSTAKA

[1] A. Al-Fuqaha *et al*., *Internet of Things: A Comprehensive Survey*, *IEEE Communications Surveys & Tutorials*, 2022.

[2] R. Santosa, P. A. Sari, dan A. T. Sasongko, "Sistem Monitoring Suhu dan Kelembaban Berbasis IoT pada Gudang Penyimpanan," *Jurnal Teknologi dan Sistem Informasi Bisnis*, vol. 5, no. 4, 2023.

[3] Y. Wan *et al*., *PatrIoT: Practical and Agile Threat Research for IoT*, *International Journal of Information Security*, vol. 21, 2022.

[4] I. Radhakrishnan, S. Jadon, dan P. B. Honnavalli, *Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices*, *Sensors*, vol. 24, no. 12, 2024.

[5] Jap *et al*., *Lightweight Cryptography for IoT Applications: Performance and Security Analysis*, 2021.

[6] Nizma'urrahmi *et al*., "Implementasi Algoritme SPECK pada *Wireless Sensor Network* menggunakan Media Pengiriman Data nRF24L01," *Jurnal P-TIIK*, 2022.

[7] I. Radhakrishnan, A. Kumar, dan S. Prakash, *Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms (AES, SPECK, ASCON) on IoT Boards*, *IEEE Access*, vol. 12, pp. 45521–45533, 2024.

[8] M. El-Hajj, A. Chehab, dan R. Kanj, *Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platforms*, *Journal of Information Security and Applications*, vol. 74, pp. 103–112, 2023.

[9] Y. F. Andriani, R. Saputra, dan D. Kurniawan, "Perbandingan Algoritma SIMON dan SPECK dalam Implementasi IoT Berbasis Mikrokontroler," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 2, pp. 215–223, 2024.

[10] Politeknik Negeri Batam, *Evaluation of the Effectiveness of Lightweight Encryption Algorithms (SIMON, SPECK, XTEA, PRESENT, AES) on IoT Devices*, *Jurnal Integrasi*, vol. 17, no. 1, pp. 1–10, 2025.

[11] R. Santosa, "Sistem Monitoring Suhu dan Kelembapan Berbasis *Internet of Things*," *Jurnal Rekayasa Sistem dan Teknologi Informasi*, vol. 7, no. 3, pp. 145–152, 2023.

[12] A. Fathurrohman, D. Saputra, dan M. Hidayat, "Monitoring Suhu dan Kelembapan Gudang Pangan Berbasis *Internet of Things*," *Jurnal Ilmiah Teknik Elektro dan Komputer*, vol. 8, no. 2, pp. 89–97, 2023.

[13] R. F. Maulana, A. Nugroho, dan L. Hakim, "Rancang Bangun Sistem Monitoring Suhu dan Kelembapan Berbasis IoT pada Ruang Server," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 4, pp. 742–749, 2023.

[14] A. Hidayat, S. Ramadhan, dan N. Azizah, "Sistem Monitoring Kelembapan dan Suhu pada Gudang Berbasis *Internet of Things*," *Jurnal Teknologi dan Sistem Komputer*, vol. 10, no. 1, pp. 33–40, 2022.

[15] S. Sicari *et al.*, *A Security- and Quality-Aware System Architecture for Internet of Things*, *Information Systems Frontiers*. https://doi.org/10.1007/s10796-014-9538-x

[16] Wikipedia contributors, *SPECK (Cipher)*, *Wikipedia*, 6 Sept. 2025. https://en.wikipedia.org/wiki/SPECK_(cipher)

[17] B. Schneier, *SIMON and SPECK: New NSA Encryption Algorithms*, *Schneier on Security*.

[18] S. Gueron, *Counter Mode for Long Messages and a Long Nonce*, dalam *Selected Areas in Cryptography (SAC 2021)*, *Lecture Notes in Computer Science*, vol. 13203, Springer, 2022.

[19] I. E. Firmanesa dan Wildan, "Uji SAC terhadap algoritma SPECK," dalam *Seminar Nasional Matematika dan Pendidikan Matematika UNY 2016*, Universitas Negeri Yogyakarta, 2016.

[20] A. D. Dwivedi dan G. Srivastava, *Security Analysis of Lightweight IoT Encryption Algorithms: SIMON and SIMECK*, *Internet of Things*, vol. 22, p. 100677, 2023.

[21] A. Fanfakh, N. Abduljalil, dan A. K. M. Al-Qurabat, *Parallel Multi-Core Implementation of the Optimized SPECK Cipher*, *International Journal of Safety and Security Engineering*, vol. 14, no. 3, pp. 843–852, 2024.

[22] Y. Wan *et al*., *PatrIoT: Practical and Agile Threat Research for IoT*, *International Journal of Information Security*, vol. 21, pp. 1011–1032, 2022.

[23] M. El-Hajj, A. Chehab, dan A. Kayssi, *Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platforms*, *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 5, pp. 112–120, 2023.

[24] Y. F. Andriani, M. R. Sari, dan R. D. Ramadhan, "Perbandingan Algoritma SIMON dan SPECK dalam Implementasi IoT Berbasis Mikrokontroler," *Jurnal Teknologi dan Sistem Informasi*, vol. 12, no. 2, pp. 155–162, 2024.

[25] Jurnal Polibatam, *Evaluation of the Effectiveness of Lightweight Encryption Algorithms (SIMON, SPECK, XTEA, PRESENT, AES) on IoT Devices*, *Jurnal Politeknik Batam*, vol. 5, no. 1, pp. 45–54, 2025.

[26] R. Santosa, "Sistem Monitoring Suhu dan Kelembapan Berbasis IoT," *Jurnal Ilmu Komputer dan Rekayasa*, vol. 9, no. 3, pp. 210–217, 2023.

[27] U. L. Jannah dan A. Rahma, "Analisis kesesuaian suhu penyimpanan bahan makanan segar dan kering terhadap standar keamanan pangan," *Antigen: Jurnal Kesehatan Masyarakat dan Ilmu Gizi*, vol. 3, no. 4, pp. 187–197, 2025.

[28] Y. W. Sari, M. Rahadiyanti, dan D. R. Atmaka, "Evaluasi suhu dan kelembapan ruang pengolahan dan ruang distribusi instalasi gizi," *Amerta Nutrition*, vol. 5, no. 3, pp. 190–197, 2021.

[29] A. Amrita *et al*., *Lightweight Cryptography for Internet of Things: A Review*, *EAI Endorsed Transactions on Internet of Things*, vol. 10, no. 1, 2024.

[30] P. S. Suryateja *et al*., *A Survey on Lightweight Cryptographic Algorithms in IoT*, *Cybernetics and Information Technologies*, vol. 24, no. 1, pp. 21–34, 2024.

[31] F. Mahdi dan A. A. Abdullah, *Fortifying Future IoT Security: A Comprehensive Review on Lightweight Post-Quantum Cryptography*, *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21812–21821, 2025.

[32] M. Usman *et al*., *SIT: A Lightweight Encryption Algorithm for Secure Internet of Things*, *IEEE Access*, vol. 9, pp. 17692–17706, 2021.

[33] N. Patel, S. Kumar, dan T. Singh, *A Systematic Review on Lightweight Security Algorithms for Sustainable IoT Infrastructure*, *Discover Internet of Things*, vol. 5, art. no. 47, 2025.

[34] R. Kusumah, H. I. Islam, dan S. Sobur, “Sistem Monitoring Suhu dan Kelembaban Berbasis *Internet of Things* (IoT) pada Ruang Data Center,” *Jurnal Applied Informatics and Computing*, vol. 7, no. 1, pp. 88–94, 2023.

[35] J. Waworundeng, *IoT-Based Environmental Monitoring with Data Analysis of Temperature, Humidity, and Air Quality*, *CogITo Smart Journal*, vol. 10, no. 1, pp. 271–284, 2024.

[36] A. N. Adilah *et al*., *Design of a Temperature and Humidity Monitoring System Based on the Internet of Things for Cold Chain Vaccine Storage*, *Jurnal Otomasi Kontrol dan Instrumentasi*, vol. 17, no. 2, 2025.

[37] A. Alamer, A. Basuhail, dan F. Gebali, *Performance Evaluation of Lightweight Block Ciphers for IoT Security*, *Sensors*, vol. 22, no. 9, art. no. 3456, 2022.

[38] S. Singh, P. K. Sharma, dan J. H. Park, *Blockchain and Lightweight Cryptography-Based Secure Framework for Industrial IoT*, *Journal of Network and Computer Applications*, vol. 196, art. no. 103249, 2022.

LAMPIRAN

Lampiran 1. Tempat Pengampilan Data

Lampiran 2. Tempat Pengambilan Data

Lampiran 3. Tempat Pengambilan Data