

**PERANCANGAN SISTEM KEAMANAN DATA PADA
PERANGKAT *INTERNET OF THINGS* (IOT)
DENGAN ALGORITMA *PRESENT***



Skripsi

Untuk memenuhi syarat memperoleh derajat
Sarjana Teknik (S.T.)

Oleh:

IRVANTONI ILHAM

NIM 2001020027

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2024**

PERANCANGAN SISTEM KEAMANAN DATA PADA
PERANGKAT *INTERNET OF THINGS* (IOT)
DENGAN ALGORITMA *PRESENT*



Skripsi

Untuk memenuhi syarat memperoleh derajat
Sarjana Teknik (S.T.)

Oleh:

IRVANTONI ILHAM

NIM 2001020027

Telah mengetahui dan disetujui oleh:

Pembimbing I,



Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D.

NIP. 198903252019031014

Pembimbing II,



Muhammad Radzi Rathomi, S.Kom., M.Cs.


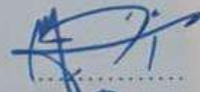


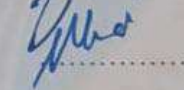
NIP. 198404022014041001

HALAMAN PENGESAHAN

Judul Skripsi : Perancangan Sistem Keamanan Data Pada Perangkat
Internet of Things (IoT) Dengan Algoritma PRESENT
Nama Mahasiswa : Irvantoni Ilham
NIM : 2001020027
Jurusan : Teknik Informatika

Telah dipertahankan di depan Dewan Penguji dan dinyatakan lulus
pada tanggal 18 Juli 2024

Susunan Tim Pembimbing dan Penguji

Jabatan	Nama	Tanda Tangan	Tanggal
Pembimbing I	: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D.	
Pembimbing II	: Muhamad Radzi Rathomi, S.Kom., M.Cs.		31/7/2024
Ketua Penguji	: Nola Ritha, S.T., M.Cs.	
Anggota Penguji I	: Novrizal Fattah Fahmitra, S.Kom., M.Kom.		31/7/2024
Anggota Penguji II	: Tekad Matulatan, S.Sos., S.Kom., M.Inf.Tech		21/7/2024

Tanjungpinang, 31 Juli 2024
Universitas Maritim Raja Ali Haji
Dekan Fakultas Teknik dan Teknologi Kemaritiman



PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa skripsi saya yang berjudul Perancangan Sistem Keamanan Data Pada Perangkat *Internet of Things* (IoT) Dengan Algoritma *PRESENT* 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.

Jika kemudian hari ternyata terbukti pernyataan saya ini tidak benar dan melanggar peraturan yang sah dalam karya tulis dan hak intelektual maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji.

Tanjungpinang, 05 Juli 2024

Yang menyatakan



Irvantoni Yham

HALAMAN PERSEMBAHAN

Alhamdulillah rabbil'alamin, dengan izin Allah SWT, skripsi ini saya persembahkan untuk:

*Diri sendiri yang telah jatuh bangun menyelesaikannya,
Kedua orang tua, keluarga, guru, sahabat, seluruh civitas UMRAH, seluruh mentor Infinite Learning terkhusus Web & Mobile, dan untuk seluruh teman angkatan saya, Teknik Informatika 2020 yang tidak muat disebutkan satu persatu di halaman kata pengantar :*

Agnes Alramadhan Alifa Alwan Arya Aznul Boyke Dela Ejika Ervan Ezy Fadli Fadhly Fariz Ferya Fian Ghora Icad Irpan Jupri Jefri Leo Liha Mia Nanda Nifia Ori Raka Rama Raju Rezi Riswan Samuel Sekar Seto Siska Syahri Tata Teti Tiwi Wan Alfi Wan Fariz Yudha

Dan untuk program studi saya Teknik Informatika, fakultas saya tercinta Fakultas Teknik dan Teknologi Kemaritiman dan untuk almamater kebanggaanku, Universitas Maritim Raja Ali Haji

HALAMAN MOTO

“Skripsi yang baik adalah skripsi yang selesai”

“Hidup berakal, mati beriman”

“Coder... code explore execute”

“Infinite learning... anyone, anything”

“Infinite learning... this is us!”

“Sysadmin... glory, stronger than all, we are root!”

“Mereka yang kuat mungkin jadi pemenang, tapi mereka yang mampu beradaptasi lah yang akan mampu bertahan”

“Sedikit lebih beda lebih baik, daripada sedikit lebih baik”

“Helping people, is helping yourself”

“Kehidupan dimasa yang akan datang, seperti sepiring tempe. Tidak ada yang tahu”

“Fokus pada penyelesaian masalahnya, bukan pada masalahnya”

“Hidup yang tak pernah dipertaruhkan, tidak akan dimenangkan”

KATA PENGANTAR

Puji dan syukur tak henti terucap dari lisan penulis, atas segala nikmat, anugrah dan kesempatan yang diberikan oleh-Nya sehingga penulis dapat menyelesaikan laporan akhir yang berjudul Perancangan Sistem Keamanan Data Pada Perangkat Internet of Things (IoT) Dengan Algoritma PRESENT sebagai skripsi yang ditujukan untuk memperoleh derajat Sarjana Teknik (S.T). Alhamdulillah.

Dalam perjalanannya, penulis banyak sekali menemui hambatan dan tantangan yang datang dari diri sendiri maupun dari luar diri. Namun sekali lagi, penulis mengucapkan syukur Alhamdulillah masih dikelilingi orang-orang baik dan berhasil melewatinya dengan bantuan dan semangat dari mereka yang sangat berjasa bagi penulis dan untuk itu penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Lestariah B.Sc dan Masrul.HB selaku orangtua tercinta. Kepada 3 abangku, Bang Yoga, Bang Bobby, dan Bang Elvan. 2 kakak ipar, Kak Novi dan Kak Diena. Serta 5 ponakanku yang lucu, Luthfi, Kenzie, Aira, Zayn, dan Sheena yang telah menjadi support sistem sempurna penulis.
2. Bapak Sapta Nugraha, S.T., M.Eng., selaku Dekan Fakultas Teknik dan Teknologi Kemaritiman Universitas Maritim Raja Ali Haji.
3. Bapak Muhamad Radzi Rathomi, S. Kom., M.Cs., selaku Kepala Program Studi Teknik Informatika UMRAH.
4. Bapak Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D. selaku Dosen Pembimbing I dan Bapak Muhamad Radzi Rathomi, S. Kom., M.Cs. selaku Dosen Pembimbing II yang telaten membimbing penulis.
5. Hafara Putri Fardyan Awalza yang telah menjadi orang spesial untuk diajak berdiskusi, berkeluh kesah, bertukar pikiran dan penyemangat bagi penulis.

Tanjungpinang, 7 Juli 2024

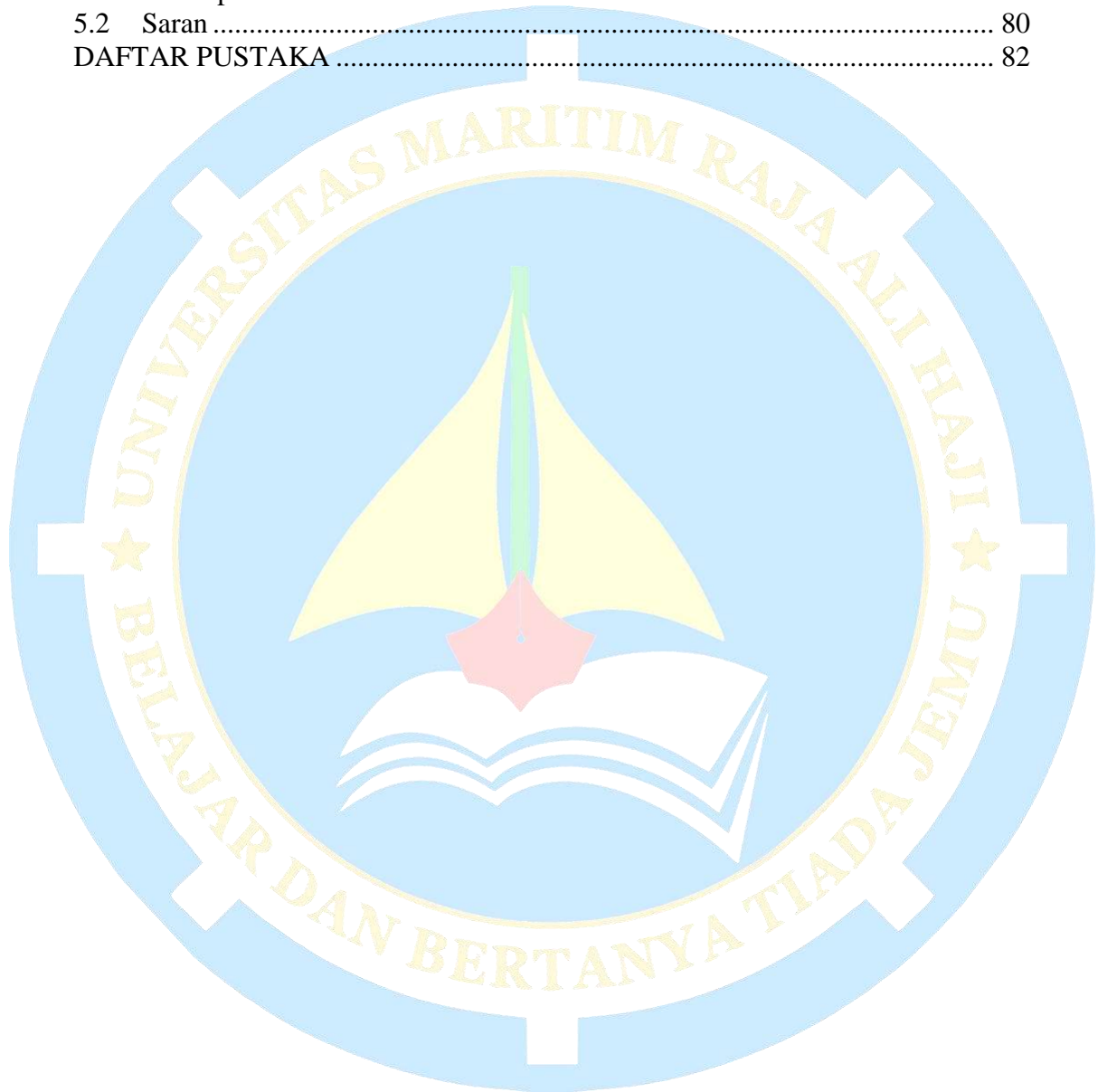


Irvantoni Ilham

DAFTAR ISI

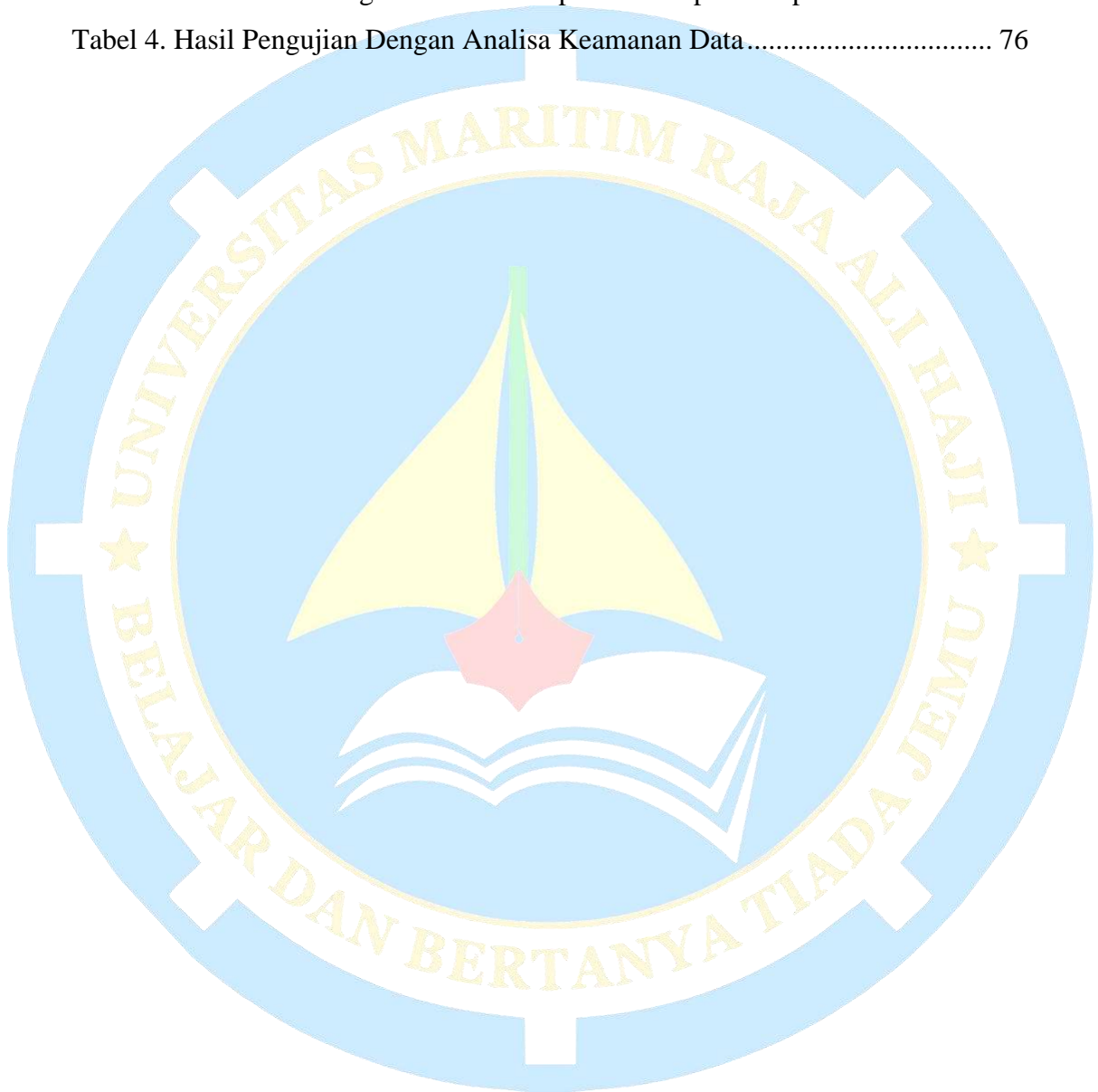
HALAMAN JUDUL.....	i
LEMBAR PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
PERNYATAAN ORISINALITAS	iv
HALAMAN PERSEMBAHAN	v
HALAMAN MOTO	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	x
DAFTAR GAMBAR	xi
GLOSARIUM.....	xiii
ABSTRAK.....	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	5
1.3 Batasan Masalah	5
1.4 Tujuan Penelitian	6
1.5 Manfaat Penelitian	6
1.6 Sistematika Penulisan	8
BAB II TINJAUAN PUSTAKA.....	10
2.1 Kajian Literatur.....	10
2.2 Landasan Teori	13
2.2.1 Keamanan Data.....	13
2.2.2 Internet of Things.....	14
2.2.3 Kriptografi	16
2.2.4 Algoritma <i>PRESENT</i>	17
2.2.5 Man in the Middle.....	21
BAB III METODE PENELITIAN.....	23
3.1 Waktu dan tempat penelitian	23
3.2 Tahapan Penelitian.....	23
3.3 Jenis Penelitian	24
3.4 Alat dan Instrumen Penelitian.....	24
3.5 Analisis dan Perancangan	26
3.5.1 Analisis Data.....	26
3.5.2 Analisis Prototype Sistem.....	27
3.5.3 Perancangan Algoritma Enkripsi <i>PRESENT</i>	28
3.5.4 Perancangan Algoritma Dekripsi <i>PRESENT</i>	35
3.5.5 Skema Pengujian dengan Network Sniffing.....	38
3.6 Implementasi.....	42
3.6.1 Perancangan IoT	42
3.6.2 Perancangan WebServer.....	46
3.6.3 Perancangan Database	58

3.6.4 Perancangan Web Client.....	58
3.7 Pengujian	66
BAB IV HASIL DAN PEMBAHASAN	69
4.1 Analisis Hasil Pengujian Prototype Sistem	69
4.2 Analisis Hasil Perancangan Sistem Keamanan Lewat Pengujian Serangan	70
BAB V PENUTUP.....	80
5.1 Kesimpulan.....	80
5.2 Saran	80
DAFTAR PUSTAKA	82



DAFTAR TABEL

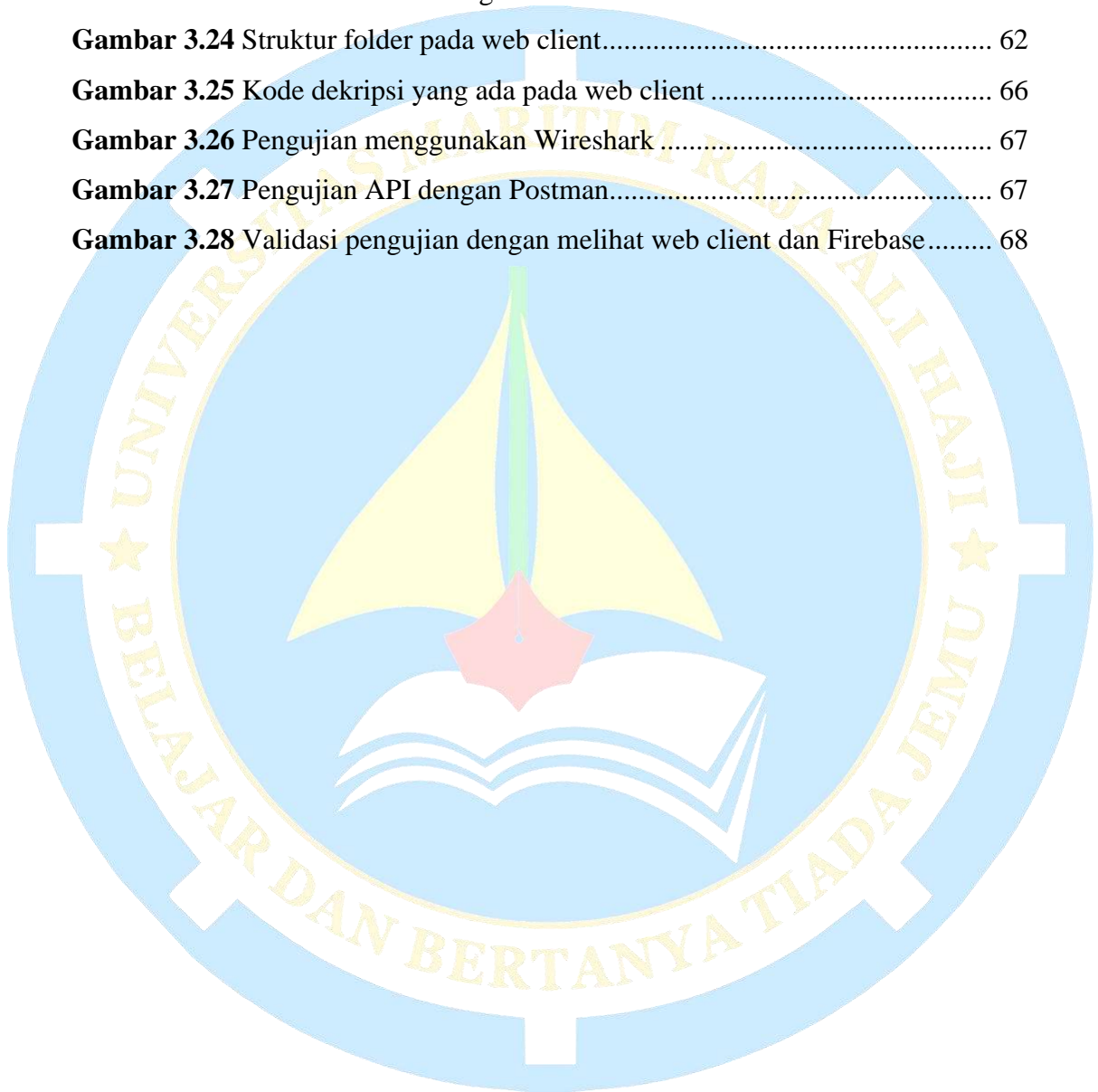
Tabel 1. Alat dan Instrumen Penelitian.....	24
Tabel 2. Komponen Prototype Sistem	42
Tabel 3. Hasil Perbandingan Antara Enkripsi dan Tanpa Enkripsi	70
Tabel 4. Hasil Pengujian Dengan Analisa Keamanan Data.....	76



DAFTAR GAMBAR

Gambar 2.1 NodeMCU ESP8266.....	15
Gambar 2.2 Pinout NodeMCU ESP8266	15
Gambar 2.3 Sensor Water Flow YF-S201	16
Gambar 2.4 Sbox PRESENT.....	17
Gambar 2.5 Pbox PRESENT.....	18
Gambar 2.6 Skema Algoritma Kriptografi PRESENT.....	18
Gambar 2.7 Algoritma Enkripsi PRESENT	19
Gambar 2.8 The S/P network untuk PRESENT	20
Gambar 2.9 Man in the Middle Attack.....	22
Gambar 3.1 Alur tahapan penelitian.....	23
Gambar 3.2 <i>Prototype</i> sistem yang akan dirancang (atas) dan <i>prototype</i> sistem yang terrealisasi (bawah).....	27
Gambar 3.3 Tabel ASCII.....	29
Gambar 3.4 Memilih interface jaringan pada Wireshark	39
Gambar 3.5 Paket yang masuk lewat interface yang dipilih	39
Gambar 3.6 Menggunakan filter pada Wireshark	40
Gambar 3.7 Follow TCP Stream pada salah satu paket	40
Gambar 3.8 Isi dari Paket	41
Gambar 3.9 Formatting JSON pada VSCode.....	41
Gambar 3.10 <i>Source Code</i> untuk NodeMCU ESP8266.....	45
Gambar 3.11 Setelan board dan baudrate	45
Gambar 3.12 Tampilan pada LCD	46
Gambar 3.13 Dependensi pada file ackage.json.....	46
Gambar 3.14 Scripts pada package.json.....	47
Gambar 3.15 Kode pada sever.js bagian 1	50
Gambar 3.16 Kode pada server.js bagian 2	54
Gambar 3.17 Kode index.html untuk web server	57
Gambar 3.18 Tampilan web server pada terminal (kiri) dan ketika frontend nya browser (kanan).....	58

Gambar 3.19 Skema basis data Firebase	58
Gambar 3.20 Tampilan halaman 1 web client.....	59
Gambar 3.21 Tampilan halaman 2 web client.....	59
Gambar 3.22 Tampilan halaman 3 web client.....	60
Gambar 3.23 Autentikasi user dengan Firebase	61
Gambar 3.24 Struktur folder pada web client.....	62
Gambar 3.25 Kode dekripsi yang ada pada web client	66
Gambar 3.26 Pengujian menggunakan Wireshark	67
Gambar 3.27 Pengujian API dengan Postman.....	67
Gambar 3.28 Validasi pengujian dengan melihat web client dan Firebase.....	68



GLOSARIUM

IoT	Konsep ini menggambarkan jaringan objek fisik ("benda") yang dilengkapi dengan sensor, perangkat lunak, dan teknologi lainnya untuk terhubung dan bertukar data dengan perangkat lain dan sistem melalui internet.
Ciphertext	Data yang telah dienkripsi dan tidak bisa dibaca tanpa memiliki kunci dekripsi yang sesuai.
Plaintext	Data yang belum dienkripsi atau dalam bentuk aslinya yang dapat dibaca.
Encryption	Proses mengubah plaintext menjadi ciphertext untuk mengamankan informasi dari akses yang tidak diizinkan.
Decryption	Proses mengubah kembali ciphertext menjadi plaintext, menggunakan kunci yang sesuai.
PRESENT	Algoritma enkripsi blok yang dirancang untuk keamanan yang tinggi dengan efisiensi eksekusi yang baik pada perangkat dengan sumber daya terbatas seperti IoT.
Network Sniffing	Praktik memantau dan menganalisis lalu lintas jaringan untuk mendapatkan informasi yang dapat digunakan oleh penyerang.
Web Server	Server yang menyimpan data dari website dan mengirimkannya ke klien berdasarkan permintaan melalui protokol HTTP.
Web Client	Aplikasi atau browser yang mengakses layanan dari web server melalui internet.
Firebase	Platform pengembangan aplikasi yang disediakan oleh Google, yang menawarkan fungsi seperti penyimpanan basis data, autentikasi pengguna, dan konfigurasi backend.
Data Security	Perlindungan data dari akses, penggunaan, pengungkapan, gangguan, modifikasi, inspeksi, pendaftaran atau penghancuran tidak sah.