PENERAPAN ALGORITMA KRIPTOGRAFI RIVEST-SHAMIR-ADLEMAN (RSA) PADA PENGIRIMAN DATA PENGGUNAAN ENERGI LISTRIK DI KAMAR INDEKOS

RAJAWALI
H1051211029

SKRIPSI

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2025

PENERAPAN ALGORITMA KRIPTOGRAFI RIVEST-SHAMIR-ADLEMAN (RSA) PADA PENGIRIMAN DATA PENGGUNAAN ENERGI LISTRIK DI KAMAR INDEKOS

RAJAWALI
H1051211029

Skripsi
Sebagai alah satu syarat untuk memperoleh gelar
Sarjana Komputer pada Program Studi Rekayasa Sistem Komputer

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2025

LEMBAR PENGESAHAN

Judul Tugas Akhir	: Penerapan Algoritma Kriptografi Rivest-Shamir-Adleman (RSA) pada Pengiriman Data Penggunaan Energi Listrik di Kamar Indekos
Nama Mahasiswa	: Rajawali
NIM	: H1051211029
Jurusan/Program Studi	: Rekayasa Sistem Komputer
Tanggal Lulus	: 18 Juli 2025
SK Pembimbing	: 3691/UN22.8/TD.06/2024 /Tanggal 13 November 2024
SK Penguji	: 2208/UN22.8/TD.06/2025 /Tanggal 15 Juli 2025

Dosen Pembimbing

Pembimbing I	Pembimbing II
Syamsul Bahri, S.Kom.,M.Cs.	Kasliono, S.Mat., M.Cs.
NIP. 198802272015041001	NIP. 199306202022031005

Dosen Penguji

Ketua Penguji	Anggota Penguji
Ikhwan Ruslianto, S.Kom., M.Cs.	Hafiz Muhardi, S.T., M.Kom.
NIP. 198607012014041001	NIP. 199007232023211017

Pimpinan Sidang (merangkap anggota penguji)	Sekretaris Sidang (merangkap anggota penguji)
Syamsul Bahri, S.Kom.,M.Cs.	Kasliono, S.Mat., M.Cs.
NIP. 198802272015041001	NIP. 199306202022031005

Mengesahkan
Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Tanjungpura

Prof. Dr. Gusrizal, S.Si., M.Si.
NIP. 197108022000031001

PERNYATAAN INTEGRITAS AKADEMIK

Saya yang bertanda tangan di bawah ini:

Nama	: Rajawali
NIM	: H1051211029
Program Studi/ Jurusan	: Rekayasa Sistem Komputer
Fakultas	: Matematika dan Ilmu Pengetahuan Alam

dengan ini menyatakan bahwa dokumen ilmiah Tugas Akhir yang disajikan ini tidak mengandung unsur pelanggaran integritas akademik sesuai Peraturan Menteri Pendidikan, Kebudayaan, Riset, Dan Teknologi Republik Indonesia Nomor 39 Tahun 2021. Apabila di kemudian hari dokumen ilmiah Tugas Akhir ini mengandung unsur pelanggaran integritas akademik sesuai ketentuan perundangan tersebut, maka saya bersedia menerima sanksi akademik dan/atau sanksi hukum yang berlaku.

Demikian pernyataan ini untuk digunakan sebagaimana mestinya.

Pontianak, 21 Juli 2025



Rajawali
NIM. H1051211029

Penerapan Algoritma Kriptografi Rivest-Shamir-Adleman (RSA) pada Pengiriman Data Penggunaan Energi Listrik di Kamar Indekos

Abstrak

Perkembangan *Internet of Things* (IoT) telah memungkinkan sistem *monitoring* energi listrik diterapkan pada lingkungan kamar indekos. Namun, sistem ini rentan terhadap ancaman keamanan seperti serangan *Man-in-the-Middle* (MitM) yang dapat menyebabkan manipulasi data selama transmisi. Penelitian ini bertujuan untuk mengamankan pengiriman data energi listrik dari modul PZEM-004T menggunakan algoritma kriptografi Rivest-Shamir-Adleman (RSA) melalui proses enkripsi, autentikasi digital (*signature*), dan dekripsi. Data dienkripsi oleh NodeMCU ESP32 menggunakan kunci publik RSA, kemudian dikirim ke *local server* dan diverifikasi dengan tanda tangan digital sebelum disimpan. Hasil pengujian menunjukkan bahwa sistem dengan RSA mampu menolak data yang dimanipulasi saat terjadi serangan yang disimulasikan menggunakan *tools* Ettercap, sehingga data tidak tercatat di *database*. Penolakan terhadap data tidak valid ini memicu terjadinya *packet loss*. Dengan demikian, *packet loss* dalam sistem ini bukan hanya disebabkan oleh gangguan jaringan, tetapi juga dapat menjadi indikator awal terjadinya serangan atau aktivitas mencurigakan. Nilai *packet loss* sebesar 2,08% masih berada dalam kategori "Sangat Bagus" menurut standar TIPHON. Selain itu, data yang gagal dikirim akan disimpan sementara dan dikirim ulang pada siklus berikutnya dalam kondisi utuh. Penerapan RSA terbukti mampu menjaga integritas dan keaslian data, serta meningkatkan keandalan sistem *monitoring* energi listrik di kamar indekos.

Kata kunci: Kriptografi, RSA, *Monitoring* Listrik, *Packet Loss*, ASCII

Implementation of the Rivest-Shamir-Adleman (RSA) Cryptographic Algorithm in the Transmission of Electricity Usage Data in Boarding House Rooms

Abstract

The Internet of Things (IoT) enables real-time electricity usage monitoring in boarding houses. However, such systems are vulnerable to security threats, particularly Man-in-the-Middle (MitM) attacks that can manipulate data during transmission. This study applies the Rivest-Shamir-Adleman (RSA) cryptographic algorithm to secure the transmission of electricity usage data from the PZEM-004T module. The system implements encryption using the RSA public key, digital signature authentication, and decryption using the private key. Data is encrypted and signed on the NodeMCU ESP32, then transmitted to a local server where it is verified before being stored. Testing shows that the system effectively rejects manipulated data during simulated MitM attacks using Ettercap, ensuring that invalid data is not recorded in the database. This rejection causes packet loss, indicating that packet loss may not only result from network issues but can also signal attempted attacks. The observed packet loss of 2.08% is still categorized as "Very Good" according to the TIPHON standard. Moreover, undelivered data is retained by the ESP32 and resent in the next transmission cycle, preserving data accuracy. The results confirm that the RSA algorithm enhances data integrity, authenticity, and the overall reliability of the electricity monitoring system under both normal and attack conditions.

Keywords: *Cryptography, RSA, Electricity Monitoring, Packet Loss, ASCII*

PRAKATA

Segala puji dan syukur panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul **"Penerapan Algoritma Kriptografi Rivest-Shamir-Adleman (RSA) pada Pengiriman Data Penggunaan Energi Listrik di Kamar Indekos"** Tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom.) pada Jurusan Rekayasa Sistem Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Tanjungpura Pontianak.

Semua hasil yang diperoleh ini tidak lepas dari segala dukungan dan bantuan dari berbagai pihak yang terus mendorong penulis untuk menyelesaikan tugas akhir ini dengan baik. Sebagai penghargaan, izinkanlah penulis mengucapkan rasa terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. Gusrizal, S.Si., M.Si., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.
2. Bapak Tedy Rismawan, S.Kom., M.Cs., selaku Ketua Jurusan Rekayasa Sistem Komputer FMIPA Universitas Tanjungpura Pontianak.
3. Bapak Syamsul Bahri, S.Kom.,M.Cs., sebagai dosen Pembimbing Pertama yang telah memberikan masukan serta meluangkan waktu dan pikiran yang memberikan dorongan dalam bimbingan penulisan skripsi, serta sekaligus sebagai Pembimbing Akademik (PA) yang telah memberi masukan dan motivasi yang membangun selama masa perkuliahan.
4. Bapak Kasliono, S.Mat., M.Cs., sebagai dosen Pembimbing Kedua yang telah memberikan masukan serta meluangkan waktu dan pikiran yang memberikan dorongan dalam bimbingan penulisan skripsi.
5. Bapak Ikhwan Ruslianto, S.Kom.,M.Cs., selaku dosen penguji Pertama yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.
6. Bapak Hafiz Muhardi, S.T., M.Kom., selaku dosen Penguji Kedua, yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.

7. Kepada orang tua yang selalu memberikan dukungan, doa, motivasi, dan kasih sayang tanpa henti sepanjang perjalanan penulisan tugas akhir ini.
8. Teman-teman HIKABAR yang senantiasa menemani, memberi semangat dan bantuan dalam bentuk apapun sehingga tugas akhir ini dapat terselesaikan.
9. Para rekan-rekan seperjuangan mahasiswa khususnya Sistem Komputer Angkatan 2021 (NEMOTIC'21) yang telah memberikan semangat dan dukungan dalam menjalani proses perkuliahan dan penulisan tugas akhir ini.
10. Semua pihak yang terlibat langsung maupun yang tidak langsung dalam penulisan tugas akhir ini.

Pontianak, 21 Juli 2025



Rajawali

DAFTAR ISI

LEMBAR PENGESAHAN ii
PERNYATAAN INTEGRITAS AKADEMIK iii
Abstrak iv
Abstract v
PRAKATA vi
DAFTAR ISI viii
DAFTAR GAMBAR x
DAFTAR TABEL xii
DAFTAR PERSAMAAN xiii
DAFTAR KODE PROGRAM xiv

BAB 1 PENDAHULUAN
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan Penelitian 4
1.5 Manfaat Penelitian 4
1.6 Sistematika Penulisan 5

BAB 2 LANDASAN TEORI
2.1 Perbandingan dengan Penelitian Terdahulu 7
2.2 Algoritma Kriptografi Rivest-Shamir-Adleman (RSA) 8
2.3 Tanda Tangan Digital Menggunakan RSA (RSA *Signature*) 12
2.4 *Packet Loss* (*PL*) 13
2.5 ASCII (*American Standard Code for Information Interchange*) 14
2.6 ARP (*Address Resolution Protocol*) 15
2.7 ARP *Spoofing Attack* 15
2.8 Ettercap 16
2.9 Wireshark 16
2.10 Iperf3 16
2.11 NodeMCU ESP32 17
2.12 Modul PZEM-004T 17
2.13 HI-LINK HLK-PM01 17
2.14 Arduino IDE 18
2.15 *Local Server* 18
2.16 PHP (*Hypertext Preprocessor*) 19
2.17 Balsamiq Wireframes 19
2.18 Diagram Alir (*Flowchart*) 19

BAB 3 METODE PENELITIAN
3.1 Studi Literatur 20
3.2 Analisis Kebutuhan 21
3.2.1 Kebutuhan Perangkat Keras 21

3.2.2 Kebutuhan Perangkat Lunak 21
3.3 Perancangan Sistem 21
3.4 Implementasi Sistem 22
3.5 Pengujian Sistem 22
3.6 Kesimpulan dan Saran 22

BAB 4 PERANCANGAN
4.1 Deskripsi Sistem 23
4.2 Perancangan Arsitektur Sistem 23
4.3 Perancangan Perangkat Keras 25
4.4 Perancangan Perangkat Lunak 27
4.5 Perancangan Basis Data 28
4.5.1 Tabel Sensor Data 29
4.5.2 Tabel *Energy* Reset *Log* 30
4.6 Perancangan Antarmuka 30
4.7 Perancangan Pengujian Sistem Monitoring Listrik Tanpa Enkripsi Data 31
4.8 Perancangan Pengujian Sistem *Monitoring* Listrik Menggunakan Algoritma RSA 34

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN
5.1 Implementasi Perangkat Keras 36
5.2 Implementasi Perangkat Lunak 36
5.2.1 Implementasi Algoritma RSA dalam Enkripsi Penggunaan *Energy* Listrik 37
5.2.2 Implementasi Pengirim Data Dari NodeMCU ESP32 ke *Local Server* 40
5.2.3 Implementasi Algoritma RSA dalam Dekripsi Penggunaan *Energy* Listrik 43
5.2.4 Implementasi Perhitungan *Packet Loss* 44
5.3 Pengujian Sistem 46
5.3.1 Pengujian Sistem *Monitoring* Listrik Tanpa Enkripsi Data 46
5.3.2 Pengujian Sistem *Monitoring* Listrik Menggunakan Algoritma RSA 54
5.4 Analisis dan Pembahasan 67

BAB 6 PENUTUP
6.1 Kesimpulan 69
6.2 Saran 69

DAFTAR PUSTAKA 71
LAMPIRAN 74

DAFTAR GAMBAR

Gambar 2.1 Skema Enkripsi dan Dekripsi 12
Gambar 2.2 Tabel ASCII 14
Gambar 2.3 NodeMCU ESP32 17
Gambar 2.4 Modul PZEM-004T 17
Gambar 2.5 HI-LINK HLK-PM01 18
Gambar 2.6 Cara Kerja *Local Server* 19
Gambar 3.1 Diagram Alir Penelitian 20
Gambar 4.1 Arsitektur Sistem Kamar Indekos Tanpa RSA dan dengan RSA 24
Gambar 4.2 Rancangan Blok Diagram Perangkat Keras 25
Gambar 4.3 Rancangan Skema Perangkat Keras 26
Gambar 4.4 Perancangan Perangkat Lunak 27
Gambar 4.5 Rancangan Basis Data 29
Gambar 4.6 Rancangan Halaman *Dahsboard Monitoring* 31
Gambar 4.7 Cara Kerja ARP *Spoofing Attack* 32
Gambar 4.8 Diagram Alir Pengujian Sistem *Monitoring* Listrik Tanpa Enkripsi Data 33
Gambar 4.9 Perancangan Pengujian Sistem *Monitoring* Listrik Menggunakan Algoritma RSA 35
Gambar 5.1 Implementasi Sistem *Monitoring* Penggunaan Energi Listrik 36
Gambar 5.2 Pengiriman Data dari NodeMCU ESP32 ke *Local Server* 40
Gambar 5.3 Hasil Pengujian *Monitoring* Listrik Tanpa Enkripsi pada Serial Monitor Arduino IDE 46
Gambar 5.4 Hasil Pengujian *Monitoring* Listrik Tanpa Enkripsi Data pada *Tools* Wireshark 47
Gambar 5.5 Hasil Pengujian *Monitoring* Listrik Tanpa Enkripsi Data yang Tercatat pada *Database* 47
Gambar 5.6 Hasil *Capture* Menggunakan *Tools* Wireshark 48
Gambar 5.7 Tampilan *Tools* Ettercap 49
Gambar 5.8 Program yang Telah ditulis pada File energy_filter.ecf 50
Gambar 5.9 Hasil perintah *compile* energy_filter.ef yang telah berhasil 51
Gambar 5.10 Hasil Perintah H*ost List* dan Menambahkan Target pada *Tools* Ettercap 51
Gambar 5.11 Perintah ARP *Poisoning* pada *tools* Ettercap 52
Gambar 5.12 *Pop Up* Setelah Memilih Perintah ARP *Poisoning* 52
Gambar 5.13 Hasil memuat *filter* 53
Gambar 5.14 Hasil Data yang Terbaca Pada *Serial Monitor* Arduino IDE 53
Gambar 5.15 Hasil Perubahan Data yang Melewati *Tools* Ettercap 54
Gambar 5.16 Hasil Manipulasi/Perubahan Data 54
Gambar 5.17 *Bandwidth* yang Digunakan Selama Proses Pengujian 55
Gambar 5.18 Data penggunaan *Bandwidth* NodeMCU ESP32 55
Gambar 5.19 Hasil Perubahan Nilai Penggunaan Energi Listrik Menjadi Bentuk RSA dan Konversi RSA ke ASCII serta *Signature* RSA 56
Gambar 5.20 Hasil *Capture* Menggunakan *Tools* Wireshark 59
Gambar 5.21 Hasil Data yang Telah Dienkripsi dan Berhasil Terkirim Ke *Database* 59

Gambar 5.22 Hasil *Capture* Data *Encrypt Energy* Menggunakan *Tools* Wireshark 60
Gambar 5.23 Filter encrypt_energy_filter.ecf 62
Gambar 5.24 *Compile* Filter Encrypt_Energy_Filter.Ecf Telah Berhasil 62
Gambar 5.25 Hasil Penyerangan Menggunakan *Tools* Ettercap..... 63
Gambar 5.26 Data yang Terbaca pada *Serial Monitor* Arduino IDE Selama Proses Penyerangan 64
Gambar 5.27 Data Hasil *Capture* pada Wireshark 65
Gambar 5.28 Data yang Tercatat pada *Database* dan Tidak Terjadi Perubahan Selama Proses Penyerangan 65
Gambar 5.29 Halaman *Dashboard Monitoring* 66

DAFTAR TABEL

Tabel 2.1 Perbandingan dengan Penelitian Terdahulu 7
Tabel 2.2 *Generate* Kunci RSA 9
Tabel 2.3 Kategori *Packet Loss* Jaringan Berdasarkan Standar TIPHON 14
Tabel 4.1 Penggunaan Pin ESP32 dengan Modul PZEM-004T 26
Tabel 4.2 Rancangan Tabel *Energy* Data 30
Tabel 4.3 Rancangan Tabel *Energy* Reset *Log* 30
Tabel 5.1 Hasil *Capture* Data Penggunaan *Energy* Listrik yang Telah di Enkripsi 60
Tabel 5.2 Data Penggunaan Energi Listrik yang Dienkripsi dan Didapatkan Selama Proses Penyerangan 63

DAFTAR PERSAMAAN

Persamaan 2.1 Mendapatkan nilai n 10
Persamaan 2.2 Mendapatkan Nilai *Totient euler* (n) 10
Persamaan 2.3 Mencari Kunci Dekripsi (d)) 10
Persamaan 2.4 Mencari Kunci Dekripsi (d) 10
Persamaan 2.5 Mencari Nilai d 11
Persamaan 2.6 Mendapatkan *Chipertext* 11
Persamaan 2.7 Mendapatkan *Plaintext* 12
Persamaan 2.8 Mendapatkan nilai tanda tangan digital RSA 13
Persamaan 2.9 Verifikasi *Signature* 13
Persamaan 2.10 Menghitung *Packet Loss* 13
Persamaan 2.11 Konversi ke Karakter ASCII 15
Persamaan 2.12 Membalikkan *Encrypted Energy* (ASCII) ke *Encrypted Energy* (RSA) (nilai integer) 15
Persamaan 2.13 Menghitung *Throughput* 17

DAFTAR KODE PROGRAM

Kode Program 5.1 Pembuatan Kunci Publik dan Privat RSA 37
Kode Program 5.2 Enkripsi Penggunaan Energi Listrik Menggunakan Algoritma RSA 38
Kode Program 5.3 Konversi Hasil Enkripsi RSA Menjadi ASCII..... 39
Kode Program 5.4 Pengiriman Data Dari NodeMCU ESP32 ke *Local Server* .. 41
Kode Program 5.5 Pembuatan *Signature* pada NodeMCU ESP32 42
Kode Program 5.6 Verifikasi Signature pada Server..... 42
Kode Program 5.7 Konversi ASCII Menjadi Enkripsi RSA 43
Kode Program 5.8 Dekripsi RSA 43
Kode Program 5.9 Perhitungan *Packet Loss* 45
Kode Program 5.10 *Filter* Ettercap untuk Manipulasi Data Penggunaan Energi Listrik 49
Kode Program 5.11 Filter Ettercap *Encrypt* Energi listrik 61

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Teknologi *Internet of Things* (IoT) menghubungkan perangkat fisik melalui Internet dan memungkinkan pertukaran data dan informasi secara *real-time*, meningkatkan efisiensi dan produktivitas dalam berbagai bidang seperti industri, kesehatan, pertanian, usaha, dan kehidupan sehari-hari (Baharuddin et al., 2024). Pada bidang usaha, teknologi IoT digunakan dalam usaha kos-kosan untuk mengukur penggunaan energi listrik setiap kamar, dimana kebutuhan setiap orang berbeda-beda, dan besarnya konsumsi energi bergantung pada seberapa banyak dan lama perangkat digunakan (Sahroni et al., 2020). Dengan teknologi ini, pemilik kos bisa mengetahui dan memberikan tarif yang adil kepada setiap penyewa berdasarkan tarif yang ditampilkan oleh *dashboard monitoring*.

Namun, sistem *monitoring* penggunaan energi listrik pada kosan menghadapi tantangan berupa keamanan data, dimana terdapat ancaman dan serangan yang umum terjadi, seperti *Man-in-the-Middle* (MitM), dimana seorang yang tidak berwenang dapat mengamati atau mengubah percakapan antar perangkat di jaringan (Aman, 2023). Hal ini menjadi penting ketika analis keamanan menyadari bahwa sekitar 98% dari seluruh lalu lintas antar perangkat IoT tidak terenkripsi (Fereidouni et al., 2023). Untuk menghadapi tantangan keamanan data dalam sistem *monitoring* penggunaan energi listrik, diperlukan penerapan teknologi kriptografi untuk melindungi integritas dan kerahasiaan data. Salah satu algoritma kriptografi yang umum digunakan adalah Rivest-Shamir-Adleman (RSA), yang merupakan algoritma kriptografi asimetris. Algoritma ini memanfaatkan sepasang kunci, yaitu kunci publik dan kunci privat untuk mengenkripsi dan mendekripsi data.

Dalam konteks penggunaan energi listrik di kamar indekos, RSA dapat digunakan untuk mengamankan pengiriman data dari perangkat pemantauan energi yang terpasang di setiap kamar ke *server* pusat yang digunakan oleh pemilik kos. Dengan penerapan RSA, data yang dikirimkan akan dienkripsi menggunakan kunci publik, sehingga hanya dapat dibaca oleh penerima yang memiliki kunci privat. Hal

ini mengurangi risiko serangan MitM, di mana seorang peretas mencoba mencuri atau mengubah data selama proses transmisi.

Penelitian sebelumnya yang berjudul "*Perancangan Alat Sistem Monitoring Energi Listrik Kos-kosan Berbasis Internet of Thing (IoT)*" (Muhamad et al., 2021). Tantangan dalam pengelolaan kamar indekos terkait penggunaan energi listrik sering muncul karena pemilik kamar kos menetapkan tarif listrik yang sama untuk semua kamar, meskipun konsumsi energi setiap penyewa berbeda-beda. Hal ini menyebabkan kerugian bagi pemilik kos akibat penggunaan listrik yang tidak terkontrol. Untuk mengatasi masalah ini, teknologi *Internet of Things* (IoT) menawarkan solusi melalui sistem pemantauan listrik yang dapat mengukur arus, tegangan, daya, dan energi secara *real-time* menggunakan modul PZEM-004T. Sistem ini terintegrasi dengan aplikasi berbasis *smartphone* melalui *platform* Thunkable, memungkinkan pemilik kos untuk memantau penggunaan listrik di setiap kamar dari jarak jauh. Dengan akurasi sensor lebih dari 99,5%, sistem ini tidak hanya memberikan data yang akurat, tetapi juga mencatat tagihan listrik per kamar, sehingga membantu pemilik kos dalam menentukan tarif yang lebih adil.

Penelitian selanjutnya mengenai ancaman dan solusi keamanan pada teknologi IoT yaitu "*Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things*" (Najib et al., 2020). Penelitian ini menghasilkan tinjauan komprehensif tentang berbagai ancaman yang dihadapi oleh sistem IoT, seperti serangan siber, penyadapan data, dan akses tidak sah. Penelitian ini juga membahas solusi keamanan yang dapat diterapkan untuk mengatasi ancaman tersebut, termasuk penggunaan enkripsi data, autentikasi yang kuat, serta pengembangan protokol keamanan khusus untuk IoT. Dengan memahami ancaman dan menerapkan solusi yang tepat, penelitian ini menekankan pentingnya keamanan dalam penerapan teknologi IoT untuk memastikan integritas, kerahasiaan, dan ketersediaan data yang dikumpulkan dan diproses oleh perangkat IoT.

Penelitian selanjutnya yang berjudul "*Implementasi Algoritma RSA untuk Proses Enkripsi-Autentikasi Publish-Subscribe pada Protokol MQTT Menggunakan ESP8266 Berbasis IoT*" (Akbar et al., 2024). Penelitian ini berfokus pada penerapan algoritma RSA untuk meningkatkan keamanan komunikasi antar perangkat IoT. Dalam penelitian tersebut, algoritma RSA diterapkan untuk

mengenkripsi data yang dikirim melalui protokol MQTT. Algoritma RSA menggunakan sepasang kunci, yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi, memastikan hanya penerima yang berwenang yang dapat mengakses data. Hasil penelitian menunjukkan bahwa penggunaan algoritma enkripsi RSA dalam pengiriman data sensor DHT11 melalui protokol MQTT dengan memanfaatkan ESP8266 telah berhasil meningkatkan keamanan komunikasi, melindungi privasi, serta memastikan integritas data. Algoritma RSA menunjukkan kinerja yang memuaskan dengan tingkat kesalahan yang rendah, sehingga menjadikannya solusi yang efektif dalam lingkungan *Internet of Things* (IoT) yang memerlukan pengiriman data yang aman dan dapat diandalkan.

Berdasarkan dari penelitian sebelumnya, maka dilakukan sebuah penelitian yang berjudul "Penerapan Algoritma Kriptografi Rivest-Shamir-Adleman (RSA) pada Pengiriman Data Penggunaan Energi Listrik di Kamar Indekos". Penelitian ini bertujuan untuk mengamankan data penggunaan energi listrik di kamar indekos, dimana data sensor dapat dienkripsi dan mengirimkannya dalam bentuk *ciphertext* (pesan rahasia), sehingga hanya pihak yang berwenang yaitu pemilik kamar indekos yang dapat memberikan tagihan dari data yang telah didekripsi, dan penyewa kamar hanya mengetahui penggunaan dan tagihan energi listrik yang harus dibayarnya, serta diharapkan terjadinya pencegahan serangan dari pihak yang tidak berwenang.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, terdapat rumusan masalah sebagai berikut:

1. Bagaimana algoritma RSA dapat diterapkan untuk keamanan pengiriman data pada sistem *monitoring* listrik di kamar indekos menggunakan enkripsi, autentikasi, dan dekripsi?
2. Bagaimana pengaruh *packet loss* terhadap proses autentikasi dan penyimpanan data pada sistem *monitoring* listrik di kamar indekos dengan dan tanpa penggunaan algoritma RSA?

1.3 Batasan Masalah

Batasan masalah penelitian ini adalah sebagai berikut:

1. Sistem *monitoring* energi listrik dibangun menggunakan mikrokontroler NodeMCU ESP32 sebagai pengendali utama.
2. Data berasal dari modul PZEM-004T, meliputi parameter tegangan (*voltage*), arus (*current*), daya (*power*), dan energi listrik (*energy*).
3. Pengujian sistem dilakukan dalam dua kondisi, yaitu jaringan normal tanpa gangguan, dan jaringan dalam kondisi serangan yang disimulasikan menggunakan Ettercap, untuk menguji efektivitas RSA dalam menjaga keaslian data dan menangani manipulasi.
4. Pengamanan data menggunakan algoritma kriptografi RSA, yang mencakup proses enkripsi, dekripsi, dan autentikasi digital (*digital signature*).
5. Sistem tidak hanya diuji dari segi keberhasilan transmisi data, tetapi juga dari segi keamanan, terutama terhadap manipulasi data selama proses pengiriman.
6. Pengukuran performa sistem dilakukan dengan mengamati nilai *packet loss* dan keberhasilan proses verifikasi tanda tangan digital RSA di sisi server.
7. Menggunakan Arduino IDE untuk pemrograman pada perangkat keras.
8. Sistem pemantauan menggunakan basis data MySQLi sebagai tempat untuk menyimpan data.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini antara lain sebagai berikut:

1. Menerapkan algoritma RSA untuk mengamankan pengiriman data melalui proses enkripsi, autentikasi, dan dekripsi pada sistem *monitoring* listrik di kamar indekos.
2. Mengetahui pengaruh *packet loss* terhadap proses autentikasi dan penyimpanan data pada sistem *monitoring* listrik di kamar indekos dengan dan tanpa autentikasi RSA.

1.5 Manfaat Penelitian

Penelitian ini memberikan manfaat dalam meningkatkan keamanan data pada sistem *monitoring* listrik di kamar indekos. Dengan menerapkan algoritma kriptografi RSA, data penggunaan energi listrik yang dikirimkan dari perangkat *monitoring* ke *local server* akan dienkripsi dan dilengkapi dengan autentikasi

digital, sehingga hanya pihak yang berwenang yang dapat mengakses dan memverifikasi keaslian data. Hal ini bertujuan untuk mencegah serangan siber seperti *Man-in-the-Middle* (MitM), serta menjamin kerahasiaan dan integritas data selama proses transmisi. Selain itu, sistem ini mendukung efisiensi manajemen, karena pemilik indekos dapat menentukan tarif listrik secara adil berdasarkan konsumsi aktual penyewa, sehingga meningkatkan transparansi dan kepercayaan antara pemilik dan penyewa.

1.6 Sistematika Penulisan

Penulisan skripsi ini dibagi menjadi 6 bab agar permasalahan dapat dijelaskan dan diuraikan untuk menyelesaikan penelitian ini. Adapun sistematika penulisan tugas akhir ini terdiri dari:

BAB 1 PENDAHULUAN

Bab pendahuluan berisi latar belakang untuk menjelaskan tentang permasalahan keamanan data pada sistem IoT (*Internet of Things*) dan kenapa penelitian ini dilakukan, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab landasan teori berisi bahasan mengenai dasar teori pendukung yang digunakan dalam tugas akhir. Adapun landasan teori pada bab ini berupa Algoritma Kriptografi Rivest-Shamir-Adleman (RSA), Tanda Tangan Digital menggunakan RSA (RSA *Signature*), *Packet Loss*, ASCII (*American Standard Code for Information Interchange*), ARP (*Address Resolution Protocol*), ARP *Spoofing Attack*, Ettercap, Wireshark, Iperf3, NodeMcu ESP32, Modul PZEM-004T, Hi-Link HLK-PM01, Arduino IDE, *Local Server*, PHP (*Hypertext Preprocessor*), Balsamiq Wireframes, dan Diagram Alir (*Flowchart*).

BAB 3 METODE PENELITIAN

Bab metode penelitian adalah prosedur atau cara-cara yang dilakukan untuk mengumpulkan dan menganalisis data serta menjawab pertanyaan atau hipotesis yang telah ditetapkan dalam penelitian. Adapun isi dari metode penelitian yaitu diagram alir, studi literatur, analisis kebutuhan, perancangan sistem, implementasi sistem, pengujian sistem, data hasil pengujian, kesimpulan dan saran.

BAB 4 PERANCANGAN

Bab perancangan berisi secara rinci tentang perancangan dan tahapan dalam pelaksanaan penelitian. Pada bab ini secara umum meliputi perancangan pada arsitektur sistem, perangkat keras, perangkat lunak, perancangan basis data, perancangan antar muka, perancangan pengujian sistem *monitoring* listrik tanpa enkripsi data, dan perancangan pengujian sistem *monitoring* listrik menggunakan algoritma RSA. Pada perancangan arsitektur sistem terdiri dari seluruh perancangan dari sistem. Pada perancangan perangkat keras terdiri dari perancangan sistem menggunakan modul PZEM-004T. Perancangan perangkat lunak meliputi perancangan penerapan algoritma kriptografi RSA, proses konversi ASCII, dan komunikasi antara NodeMCU ESP32 dengan *local server*. Perancangan pada basis data terdiri dari tabel penyimpanan data dari modul PZEM-004T. Perancangan antar muka meliputi tampilan informasi dari modul PZEM-004T dan informasi *packet loss*. Perancangan pengujian sistem monitoring listrik tanpa enkripsi data meliputi perancangan proses pembacaan data dan penyerangan ARP *spoofing attack* untuk manipulasi data. Sedangkan pada perancangan pengujian sistem *monitoring* listrik menggunakan algoritma RSA meliputi penerapan algoritma RSA, konversi ASCII, pembuatan *signature digital*, penyerangan menggunakan ARP *spoofing attack*, dan validasi data pada server menggunakan *signature*.

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Bab implementasi, pengujian, dan pembahasan membahas mengenai analisis dan implementasi sistem yang telah dirancang pada tahap sebelumnya. Tahapan ini yaitu implementasi perangkat keras, implementasi perangkat lunak, pengujian, dan pembahasan.

BAB 6 PENUTUP

Bab penutup merupakan bab yang membahas tentang kesimpulan dari penelitian yang telah dilakukan dan saran terhadap masalah yang belum terselesaikan untuk dapat diperbaiki dan dikembangkan pada penelitian berikutnya.