IMPLEMENTASI *FIREWALL LIGHTWEIGHT* PADA ESP32 UNTUK MENCEGAH SERANGAN *DENIAL OF SERVICE* (DOS)

DANIEL FADHILAH LUTVIE
H1051211049

SKRIPSI

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2026

IMPLEMENTASI *FIREWALL LIGHTWEIGHT* PADA ESP32 UNTUK MENCEGAH SERANGAN *DENIAL OF SERVICE* (DOS)

DANIEL FADHILAH LUTVIE
H1051211049

Skripsi
Sebagai salah 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
2026

LEMBAR PENGESAHAN

Judul Tugas Akhir	: Implementasi *Firewall Lightweight* Pada Esp32 Untuk Mencegah Serangan *Denial of Service* (DoS)
Nama Mahasiswa	: Daniel Fadhilah Lutvie
NIM	: H1051211049
Jurusan/Program Studi	: Rekayasa Sistem Komputer
Tanggal Lulus	: 29 Juni 2026
SK Pembimbing	: No.2255/UN22.8/TD.06/2025 /Tanggal 17 Juli 2025
SK Penguji	: No.3528/DST/UN22.8/T.00.9/ 2026 /Tanggal 29 Juni 2026

Dosen Pembimbing

Pembimbing I	Pembimbing II
Kasliono, S.Mat., M.Cs.	Dwi Marisa Midyanti, S.T., M.Cs.
NIP. 199306202022031005	NIP. 198003192015042001

Dosen Penguji

Ketua Penguji	Anggota Penguji
Hafiz Muhardi, S.T., M.Kom.	Uray Ristian, S.Kom., M.Kom.
NIP. 199007232023211017	NIP. 199012012019031017

Pimpinan Sidang (merangkap anggota penguji)	Sekretaris Sidang (merangkap anggota penguji)
Kasliono, S.Mat., M.Cs.	Dwi Marisa Midyanti, S.T., M.Cs.
NIP. 199306202022031005	NIP. 198003192015042001

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	: Daniel Fadhilah Lutvie
NIM	: H1051211049
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 pernyatan ini untuk digunakan sebagaimana mestinya.

Pontianak, 07 Juli 2026

Materai

Daniel Fadhilah Lutvie
NIM. H1051211081

Implementasi *Firewall Lightweight* Pada Esp32 Untuk Mencegah Serangan *Denial Of Service* (DoS)

ABSTRAK

Perangkat *Internet of Things* (IoT) seperti mikrokontroler ESP32 sangat rentan terhadap serangan *Denial of Service* (DoS) berjenis *UDP Flood* akibat keterbatasan sumber daya komputasi dan memori. Sistem perlindungan konvensional terlalu berat untuk diterapkan pada infrastruktur IoT yang terbatas. Penelitian ini bertujuan mengimplementasikan dan menganalisis kemampuan *lightweight firewall* berbasis algoritma *rate limiting threshold* pada ESP32 dalam memitigasi ancaman tersebut. Pengujian komparatif dilakukan menggunakan topologi *Star* antara perangkat ber-*firewall* (ambang batas 200 *Packets Per Second*/PPS) dan sistem *baseline* tanpa perlindungan. Evaluasi kinerja dilakukan melalui simulasi serangan *UDP Flood* menggunakan metode *ramp-up* dengan intensitas 100 hingga 5.000 PPS. Hasil pengujian menunjukkan bahwa pada intensitas serangan rendah hingga menengah, algoritma *firewall* mencatatkan *Blocking Rate* yang optimal dalam membuang lalu lintas anomali, sehingga menjaga *CPU Load* tetap stabil di bawah beban sistem *baseline*. Pada intensitas serangan tinggi (di atas 2.500 PPS), kapasitas perangkat keras mencapai titik jenuh yang ditandai dengan *CPU Load* 100% dan *packet loss* 100% (*Request Time Out*). Meskipun demikian, sebelum mencapai kelumpuhan operasional total, sistem ber-*firewall* mampu mempertahankan tingkat penerimaan data sensor yang jauh lebih baik dibandingkan sistem *baseline*. Implementasi *lightweight firewall* ini mampu bertindak sebagai pertahanan dasar (*endpoint security*) yang andal pada perangkat IoT, meskipun perlindungan tambahan pada tingkat *gateway* tetap direkomendasikan untuk menahan serangan berintensitas masif.

Kata kunci: ESP32, *Internet of Things* (IoT), *Lightweight Firewall*, *Denial of Service* (DoS), *UDP Flood*

Implementation of lightweight firewall on ESP32 to prevent denial of service (DoS) attacks

ABSTRACT

Internet of Things (IoT) devices, such as the ESP32 microcontroller, are highly vulnerable to Denial of Service (DoS) attacks, specifically UDP Floods, due to their limited computational and memory resources. Traditional protection systems are too resource-intensive to be applied in constrained IoT infrastructures. This study aims to implement and analyze the capability of a lightweight firewall based on a rate limiting threshold algorithm on the ESP32 to mitigate these threats. A comparative evaluation was conducted using a Star topology between a firewall-equipped device (200 Packets Per Second/PPS threshold) and an unprotected baseline system. Performance evaluation was carried out through a UDP Flood attack simulation utilizing a ramp-up method with intensities ranging from 100 to 5,000 PPS. The results indicate that during low to medium-intensity attacks, the firewall algorithm recorded an optimal Blocking Rate by discarding anomalous traffic, thereby maintaining a stable CPU Load well below that of the baseline system. At high attack intensities (above 2,500 PPS), the hardware capacity reached a saturation point characterized by 100% CPU Load and 100% packet loss (Request Time Out). Nevertheless, prior to total operational failure, the firewall system was able to maintain a significantly better reception rate of sensor data compared to the baseline system. The implementation of this lightweight firewall is capable of serving as a reliable primary defense mechanism (endpoint security) on IoT devices, although an additional security layer at the gateway level is still recommended to withstand massive attacks

.

Keywords: *ESP32, Internet of Things (IoT), Lightweight Firewall, Denial of Service (DoS), UDP Flood*

PRAKATA

Segala puji dan syukur panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul "IMPLEMENTASI *FIREWALL LIGHTWEIGHT* PADA ESP32 UNTUK MENCEGAH SERANGAN *DENIAL OF SERVICE* (DOS)" 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. Ibu Rahmi Hidayati S.Kom., M.Cs., selaku Ketua Jurusan Rekayasa Sistem Komputer FMIPA Universitas Tanjungpura Pontianak yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.
3. Bapak Kasliono, S.Mat., M.Cs., sebagai dosen Pembimbing Pertama yang telah memberikan masukan serta meluangkan waktu dan pikiran yang memberikan dorongan dalam bimbingan penulisan skripsi.
4. Ibu Dwi Marisa Midyanti, S.T., M.Cs.selaku dosen Pembimbing Kedua, yang telah memberikan masukan serta meluangkan waktu dan pikiran yang memberikan dorongan dalam bimbingan penulisan skripsi.
5. Bapak Hafiz Muhardi, S.T., M.Kom., selaku dosen Penguji Pertama, yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.
6. Bapak Uray Ristian, S.Kom., M.Kom., sebagai dosen Penguji Kedua yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.

7. Ibu Irma Nirmala, S.T., M.T., sebagai dosen Pembimbing Akademik (PA) yang telah memberi masukan dan motivasi yang membangun selama masa perkuliahan.
8. Kepada orang tua yang selalu memberikan dukungan, doa, motivasi, dan kasih sayang tanpa henti sepanjang perjalanan penulisan tugas akhir ini.
9. Para rekan-rekan seperjuangan mahasiswa khususnya Sistem Komputer 2021 (Nemotic) yang telah memberikan semangat dan dukungan dalam menjalani proses perkuliahan dan penulisan tugas akhir ini.
10. Kepada Diri sendiri yang telah berjuang selama ini dan berhasil untuk tidak menyerah hingga titik ini

Semua pihak yang terlibat langsung maupun yang tidak langsung dalam penulisan tugas akhir ini.

Pontianak, 29 Juli 2026

Daniel Fadhilah Lutvie

DAFTAR ISI

DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xii
DAFTAR KODE PROGRAM xiii
BAB 1 PENDAHULUAN 1
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 7
2.1 Perbandingan dengan penelitian terdahulu 7
2.2 *Wireless Sensor Network (WSN)* 9
2.3 ESP32 9
2.4 *Threshold* 10
2.5 Gateway 10
2.6 *Firewall* 11
2.7 *Firewall Lightweight* 11
2.8 Visual Studio Code 11
2.9 *Denial of Service* (DoS) 12
2.10 ESP-IDF 13
2.11 Arduino IDE 13
2.12 *Blocking Rate* 13
2.13 *CPU Load* 14
2.14 *Packet loss* 14
2.15 *Latency* 15
2.16 DHT22 15
2.17 *Virtual Machine* 16
2.18 Kali Linux 17

BAB 3 METODE PENELITIAN 18
3.1 Studi Literatur 18
3.2 Analisis Kebutuhan 19
3.2.1 Kebutuhan Perangkat Keras 19
3.2.2 Kebutuhan Perangkat Lunak 19
3.3 Perancangan Sistem 19
3.3.1 Perancangan Perangkat Keras 20
3.3.2 Perancangan Perangkat Lunak 20
3.4 Implementasi Sistem 20
3.5 Pengujian Sistem 21
3.6 Kesimpulan dan Saran 21
BAB 4 PERANCANGAN 22
4.1 Deskripsi Sistem 22
4.2 Perancangan Arsitektur Sistem 22
4.3 Perancangan Perangkat Keras 23
4.4. Perancangan Perangkat Lunak 24
4.4.1 Perangkat Lunak ESP32 24
4.4.2 Perancangan Server 25
4.4.3 Perancangan Firewall 25
4.4.4 Perancangan Antar Muka 26
4.4.5 Perancangan Pengambilan Data 26
4.5 Perancangan Serangan 27
4.5.1 Perancangan Serangan UDP Flood 27
4.5.2. Perancangan Serangan Kali Linux 28
4.6 Perancangan Terhadap sistem 29
4.6.1 Perancangan Serangan terhadap *CPU Load* 29
4.6.2 Perancangan Serangan terhadap *Blocking rate* Keamanan 29
4.6.3 Perancangan Serangan terhadap *Quality of Service* 30
BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN 31
5.1 Implementasi Perangkat Keras 31
5.2 Implementasi Perangkat Lunak 32
5.2.1 Tampilan Antarmuka 32

5.2.2 Implementasi Antar Muka 33
5.2.3 Perangkat Lunak ESP32 33
5.2.4 Implementasi *Firewall* 35
5.2.5 Implementasi *Server* 37
5.2.6 Implementasi Pengambilan Data 39
5.3 Implementasi Serangan 42
5.3.1 Implementasi Serangan DoS UDP Flood 42
5.3.2 Implementasi Serangan Kali Linux 45
5.4 Pengujian Sistem 45
5.4.1 Dampak Serangan terhadap *CPU Load* 48
5.4.2 Dampak Serangan terhadap *Blocking rate* Keamanan 50
5.4.3 Dampak Serangan terhadap Quality of Service 52
5.5 Pembahasan 56
BAB 6 PENUTUP 59
6.1 Kesimpulan 59
6.2 Saran 60
DAFTAR PUSTAKA 61
LAMPIRAN 63
1. Kode Sumber 63
Lampiran 1 Kode Sumber ESP32 Baseline 63
Lampiran 2 Kode Sumber ESP32 Firewall 65
Lampiran 3 Kode Sumber Skrip Attacker Python 68
Lampiran 4 Kode Sumber Pengambilan Data 70
Lampiran 5 Kode Sumber WebSocket 73
Lampiran 6 Kode Sumber Server WebSocket 79
2. Data Hasil Penelitian 80
Lampiran 6 Tabel Hasil Pengujian 80

DAFTAR GAMBAR

Gambar 2.1 Wireless Sensor Network 9
Gambar 2.2 ESP32 10
Gambar 2.3 Logo Visual Studio Code..... 12
Gambar 2.4 Serangan *Denial of Service*..... 12
Gambar 2.5 DHT22 16
Gambar 3.1 Diagram Alir Penelitian..... 18
Gambar 4.1 Arsitektur Sistem 23
Gambar 4.2 Tampilan *web* pada jaringan lokal..... 26
Gambar 5.1 Keseluruhan Arsitektur Sistem..... 31
Gambar 5.2 Tampilan Implementasi Dashboard pada Web Lokal 32
Gambar 5.3 Grafik Dampak Serangan terhadap CPU *Load*..... 49
Gambar 5.4 Grafik *Firewall* CPU *Load* Pada Batas Saturation..... 50
Gambar 5.5 Grafik *Baseline* CPU *Load* Pada Batas Saturation..... 50
Gambar 5.6 Grafik Kinerja Pertahanan Sistem 51
Gambar 5.7 Grafik *Firewall Blocking Rate* Pada Batas Saturation 52
Gambar 5.8 Grafik *Baseline Blocking Rate* Pada Batas Saturation 52
Gambar 5.9 Grafik Dampak Latensi dari Setiap Serangan 53
Gambar 5.10 Grafik Dampak *Packet Loss* di Setiap Serangan..... 54
Gambar 5.11 Grafik Hasil Data Sensor Firewall..... 55
Gambar 5.12 Grafik Hasil Data Sensor Baseline 56

DAFTAR TABEL

Tabel 2.1 Perbandingan dengan Penelitian Terdahulu 7
Tabel 2.1 Lanjutan 8
Tabel 5.1 Hasil Data Pengujian Firewall 46
Tabel 5.2 Hasil Data Baseline 47
Tabel 5.3 Hasil Data Sensor 55

DAFTAR KODE PROGRAM

Kode Program 5.1 Logika *Proxy Server* 33
Kode Program 5.2 Deklarasi Variabel Konfigurasi Wi-Fi..... 34
Kode Program 5.3 Eksekusi Beban Kerja..... 34
Kode Program 5.4 Simulasi Beban Kerja 35
Kode Program 5.5 Struktur Data Pelacakan Klien..... 35
Kode Program 5.6 Logika Pemblokiran..... 36
Kode Program 5.7 Interupsi Jaringan dengan Pemfilteran Dini 36
Kode Program 5.8 Manajemen Penjadwalan CPU 37
Kode Program 5.9 Konfigurasi Jaringan Statis..... 38
Kode Program 5.10 Pembentukan Respons JSON 38
Kode Program 5.11 Inisialisasi dan Konfigurasi Parameter Uji 39
Kode Program 5.12 Pengambilan Data Metrik..... 40
Kode Program 5.13 Fungsi Perhitungan Metrik 41
Kode Program 5.14 Siklus Perekaman Data 41
Kode Program 5.15 Konfigurasi Target dan Ukuran Payload 42
Kode Program 5.16 Skenario Pengujian Bertahap..... 43
Kode Program 5.17 Logika Injeksi Paket Berpresisi Tinggi 43
Kode Program 5.18 Eksekusi Serentak..... 44

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam ekosistem *Internet of Things* (IoT) yang mengalami pertumbuhan luar biasa, teknologi ini secara fundamental telah mengubah cara perangkat berinteraksi dan berbagi informasi di berbagai domain, mulai dari kota pintar, otomatisasi industri, pemantauan kesehatan, hingga penginderaan lingkungan. Berbagai perangkat keras IoT, termasuk mikrokontroler dengan spesifikasi seperti ESP32, Raspberry Pi, dan Arduino, bertindak sebagai tulang punggung yang memfasilitasi pengumpulan serta transmisi data di dalam jaringan. Namun, sifat heterogen dari perangkat IoT ini, yang dikombinasikan dengan keterbatasan pada kemampuan komputasi, memori, dan kendala energinya (*resource-constrained*), pada akhirnya menciptakan permukaan serangan yang sangat rentan untuk dieksploitasi oleh pelaku kejahatan siber(Pushpa dkk., 2025).

Di antara berbagai ancaman keamanan siber yang ada, serangan *Denial of Service* (DoS) telah muncul sebagai ancaman yang sangat menghancurkan bagi ekosistem ini. Serangan DoS memiliki berbagai vektor untuk dilancarkan, salah satunya dengan membanjiri sistem melalui kelebihan beban lalu lintas jaringan (*network traffic overload*) yang menyuntikkan puluhan hingga ratusan paket berbahaya per detik. Dalam konteks perangkat IoT, serangan DoS menjadi sangat merugikan karena secara langsung mengeksploitasi keterbatasan pemrosesan dan *bandwidth* pada perangkat untuk mengganggu fungsionalitas jaringan serta melumpuhkan ketersediaan layanan secara total (Pushpa dkk., 2025).

Penelitian yang dilakukan menunjukkan bahwa penggunaan *firewall* berbasis *iptables* pada sistem operasi Linux mampu menyaring lalu lintas berbahaya dan memblokir serangan DoS secara efektif, sehingga menjaga kestabilan dan keamanan jaringan (Tambunan & Neyman, 2024). Namun, sistem tersebut memerlukan perangkat keras dengan sumber daya komputasi yang tinggi, sehingga tidak cocok untuk diterapkan pada *platform* ringan seperti ESP32. Hal ini

menciptakan kebutuhan mendesak akan solusi keamanan yang lebih ringan dan efisien.

Penelitian lain mengusulkan mekanisme *intelligent packet filtering* pada perangkat mikrokontroler dengan menggunakan parameter dari protokol ICMP, TCP, dan UDP (Bertoli et al., 2024). Hasil studi tersebut menunjukkan bahwa penyaringan lalu lintas mencurigakan dapat dilakukan secara efisien tanpa mengorbankan performa perangkat. Pendekatan ini sangat relevan untuk diterapkan pada ESP32 yang tidak dapat mengandalkan metode *firewall* tradisional karena keterbatasan perangkat kerasnya.

Selain itu, terdapat pengembangan pendekatan *lightweight DoS mitigation* yang berjalan pada perangkat *gateway* rumah dan *router* murah dengan memanfaatkan teknik sederhana seperti *queue shuffling* (Yaegashi et al., 2020). Teknik ini memungkinkan perangkat terbatas untuk membuang paket yang mencurigakan dengan efisien tanpa perangkat keras tambahan. Hal ini sejalan dengan pandangan yang menegaskan bahwa perangkat IoT sangat rentan terhadap serangan DoS karena minimnya sumber daya yang dimiliki, sehingga penerapan mekanisme keamanan yang ringan (*lightweight security mechanism*) menjadi sangat penting (Khader & Eleyan, 2021).

Penelitian terbaru juga mengarahkan perhatian pada pendekatan berbasis *deep learning* dan *hybrid detection models* yang menawarkan keakuratan tinggi dalam mendeteksi pola serangan DoS (Ain dkk., 2025). Namun, penerapan pendekatan ini masih terbatas pada sistem dengan kapasitas besar dan belum dapat diimplementasikan secara optimal pada perangkat mikrokontroler sekelas ESP32. Hal ini menunjukkan masih adanya kesenjangan antara efektivitas dan efisiensi dalam pendekatan keamanan jaringan pada sistem IoT.

Berdasarkan tantangan dan temuan-temuan tersebut, penelitian ini bertujuan merancang dan mengimplementasikan sistem *firewall* ringan (*lightweight firewall*) pada ESP32 menggunakan algoritma *rate limiting* berbasis *threshold*. Sistem yang dirancang diharapkan mampu memantau lalu lintas masuk, mengidentifikasi anomali serangan *UDP Flood*, serta melakukan pemblokiran (*early packet drop*) terhadap lalu lintas berlebih tanpa membebani komputasi ESP32. Untuk membuktikan efektivitasnya, pengujian komparatif dilakukan antara sistem ber-

firewall dan sistem *baseline* tanpa perlindungan. Evaluasi tidak hanya difokuskan pada intensitas serangan rendah hingga menengah untuk melihat stabilitas *CPU Load* dan *Blocking Rate*, tetapi juga mengekskalasi beban serangan (*ramp-up*) hingga mencapai batas ketahanan fisik perangkat keras (titik jenuh). Hal ini dilakukan untuk menganalisis dampaknya secara komprehensif terhadap parameter *Quality of Service* (QoS) serta keandalan perangkat dalam mempertahankan transmisi data operasional seperti pembacaan sensor pada kondisi jaringan ekstrem.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana kemampuan implementasi *firewall lightweight* berbasis algoritma *rate limiting threshold* pada ESP32 dalam memitigasi serangan *UDP Flood*, serta bagaimana pengaruhnya terhadap penggunaan sumber daya komputasi perangkat?
2. Bagaimana perbandingan kinerja ditinjau dari parameter *CPU Load* dan *Blocking Rate* antara ESP32 ber-*firewall* dengan sistem *baseline* saat menghadapi serangan *UDP Flood* berintensitas rendah hingga menengah?
3. Bagaimana kondisi perangkat keras ESP32 saat mencapai titik jenuh akibat serangan berintensitas tinggi, serta bagaimana dampak kondisi tersebut terhadap parameter *Quality of Service* (QoS) dan tingkat penerimaan data sensor?

1.3 Batasan Masalah

Batasan masalah penelitian ini adalah sebagai berikut:

1. Perangkat yang digunakan terbatas pada mikrokontroler ESP32, tanpa melibatkan platform IoT lain seperti Raspberry Pi atau Arduino.
2. Jenis serangan yang difokuskan dalam penelitian ini adalah *Denial of Service* (DoS) berbasis flooding, yaitu UDP flood.
3. Firewall yang dirancang bersifat lightweight, tanpa melibatkan algoritma berat seperti, agar tetap sesuai dengan keterbatasan memori dan prosesor ESP32.

4. Pengujian dilakukan secara lokal, dengan simulasi serangan DoS dalam jaringan terbatas (closed environment), bukan pada jaringan publik atau skala industri.
5. Penelitian ini tidak membahas deteksi intrusi lainnya seperti malware, phishing, atau serangan multi-vektor yang bukan termasuk dalam kategori DoS.
6. Penelitian ini dibatasi pada level serangan yang mampu ditangani oleh Physical Layer (PHY) dari modul Wi-Fi ESP32.
7. Evaluasi performa hanya mencakup beberapa parameter teknis seperti penggunaan memori, stabilitas koneksi, dan tingkat deteksi/pemblokiran serangan.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini antara lain sebagai berikut:

1. Menganalisis kemampuan implementasi *firewall lightweight* berbasis algoritma *rate limiting threshold* pada ESP32 dalam memitigasi serangan *UDP Flood*, serta mengetahui pengaruhnya terhadap penggunaan sumber daya komputasi perangkat.
2. Mengevaluasi dan membandingkan kinerja ESP32 ber-*firewall* dengan sistem *baseline* ditinjau dari parameter *CPU Load* dan *Blocking Rate* saat menerima serangan *UDP Flood* berintensitas rendah hingga menengah.
3. Menganalisis kondisi perangkat keras ESP32 saat mencapai titik jenuh akibat serangan berintensitas tinggi, serta mengukur dampak kondisi tersebut terhadap parameter *Quality of Service* (QoS) dan tingkat penerimaan data sensor.

1.5 Manfaat Penelitian

Penelitian ini diharapkan bisa bermanfaat antara lain sebagai berikut.

1. Menambah literatur ilmiah mengenai penerapan firewall ringan (lightweight firewall) pada perangkat IoT seperti ESP32.
2. Memberikan dasar bagi penelitian lanjutan terkait keamanan jaringan IoT dan mencegah serangan *Denial of Service* (DoS).

3. Membantu pengembang menciptakan jaringan IoT yang lebih aman dan stabil.
4. Firewall ringan meningkatkan ketahanan, stabilitas, dan efisiensi penggunaan memori pada ESP32 selama terjadi serangan UDP Flood.
5. Menunjukkan solusi praktis agar perangkat IoT tetap beroperasi secara optimal meski terkena serangan jaringan.

1.6 Sistematika Penulisan

Penulisan skripsi ini dibagi menjadi 6 bab agar permasalahan dapat dijelaskan dan diuraikan secara sistematis dalam penyelesaian penelitian ini. Adapun sistematika penulisan skripsi ini adalah sebagai berikut:

BAB 1 PENDAHULUAN

Bab pendahuluan berisi latar belakang yang menjelaskan pentingnya penelitian mengenai implementasi firewall lightweight pada ESP32 untuk mencegah serangan DoS, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, deskripsi penelitian, serta sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab landasan teori membahas teori-teori dasar dan penelitian terdahulu yang mendukung penelitian ini. Teori yang dibahas mencakup konsep Internet of Things (IoT), ESP32, serangan *Denial of Service* (DoS), Wireless Sensor Network (WSN), firewall lightweight, serta perangkat pendukung seperti Arduino IDE.

BAB 3 METODE PENELITIAN

Bab metode penelitian menjelaskan prosedur penelitian yang dilakukan, mulai dari studi literatur, analisis kebutuhan perangkat keras dan perangkat lunak, perancangan sistem, implementasi, hingga pengujian. Tahapan penelitian digambarkan dalam bentuk diagram alir beserta metode pengumpulan data, parameter pengujian, dan teknik analisis hasil.

BAB 4 PERANCANGAN

Bab perancangan menjelaskan tahapan detail mengenai desain sistem yang meliputi perancangan perangkat keras (ESP32, Access Point, laptop attacker) dan perangkat lunak (Arduino IDE). Pada bagian ini juga dipaparkan rancangan topologi jaringan serta logika firewall lightweight yang digunakan untuk mencegah serangan DoS.

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Bab ini membahas implementasi sistem sesuai rancangan pada bab sebelumnya, termasuk proses konfigurasi perangkat keras dan perangkat lunak. Selanjutnya dilakukan pengujian serangan DoS (UDP Flood) terhadap ESP32 dengan dan tanpa firewall, serta analisis hasil pengujian berdasarkan parameter blocking rate, packet loss, penggunaan memori, dan kestabilan sistem.

BAB 6 PENUTUP

Bab penutup memuat kesimpulan dari penelitian yang telah dilakukan sesuai dengan tujuan yang ditetapkan, serta memberikan saran untuk penelitian selanjutnya agar sistem firewall lightweight dapat dikembangkan lebih optimal pada perangkat IoT.