ANALISIS PROSES SERANGAN *DENIAL OF SERVIC*E (DOS) DAN *ADDRESS RESOLUTION PROTOCOL* (ARP) *SPOOFING* ANTAR PERANGKAT ESP32 PADA *WIRELESS SENSOR NETWORK* (WSN) BERTOPOLOGI STAR

DEDE KURNIAWAN
H1051211106

SKRIPSI

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

ANALISIS PROSES SERANGAN *DENIAL OF SERVIC*E (DOS) DAN *ADDRESS RESOLUTION PROTOCOL* (ARP) *SPOOFING* ANTAR PERANGKAT ESP32 PADA *WIRELESS SENSOR NETWORK* (WSN) BERTOPOLOGI STAR

DEDE KURNIAWAN
H1051211106

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
2025

LEMBAR PENGESAHAN

Judul Tugas Akhir	: Analisis Proses Serangan *Denial of Service* (DoS) dan *Address Resolution Protocol* (ARP) *Spoofing* antar Perangkat ESP32 pada *Wireless Sensor Network* (WSN) Bertopologi *Star*
Nama Mahasiswa	: Dede Kurniawan
NIM	: H1051211106
Jurusan/Program Studi	: Rekayasa Sistem Komputer
Tanggal Lulus	: 28 Juli 2025
SK Pembimbing	: No.499/UN22.8/TD.06/2025 /Tanggal 19 Februari 2025
SK Penguji	: No.2342/UN22.8/TD.06/2025 /Tanggal 18 Juli 2025

Dosen Pembimbing

Pembimbing I	Pembimbing II
Uray Ristian, S.Kom., M.Kom.	Hafiz Muhardi, S.T., M.Kom.
NIP. 199012012019031017	NIP. 199007232023211017

Dosen Penguji

Ketua Penguji	Anggota Penguji
Kasliono, S.Mat., M.Cs.	Hirzen Hasfani, S.Kom., M.Cs.
NIP. 199306202022031005	NIP. 199305032022031003

Pimpinan Sidang (merangkap anggota penguji)	Sekretaris Sidang (merangkap anggota penguji)
Uray Ristian, S.Kom., M.Kom.	Hafiz Muhardi, S.T., M.Kom.
NIP. 199012012019031017	NIP. 199007232023211017

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	: Dede Kurniawan
NIM	: H1051211106
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, 28 Juli 2025



Dede Kurniawan
NIM. H1051211106

Analisis Proses Serangan *Denial of Servi*ce (DoS) dan *Address Resolution Protocol* (ARP) *Spoofing* antar Perangkat ESP32 pada *Wireless Sensor Network* (WSN) Bertopologi *Star*

Abstrak

Perangkat *Internet of Things* (IoT) seperti ESP32, meskipun populer karena murah dan fitur Wi-Fi, memiliki keterbatasan sumber daya yang membuatnya rentan terhadap serangan siber. Penelitian ini menganalisis bagaimana serangan dapat dimplementasikan menggunakan ESP32 dan dampak dari dua jenis serangan umum, yaitu *Denial of Service* (DoS) melalui ICMP *Flood* dan *Address Resolution Protocol* (ARP) *Spoofing*, dalam lingkungan *Wireless Sensor Network* (WSN) bertopologi *star*. Dalam penelitian ini, satu perangkat ESP32 diprogram sebagai penyerang untuk menyerang salah satu dari tiga perangkat ESP32 *client* lain yang terhubung ke sebuah *server* lokal melalui protokol WebSocket. Tujuan penelitian ini adalah untuk menganalisis pengimplementasian serangan, dampak performa perangkat target, dan dampak terhadap metrik *Quality of Service* (QoS) seperti *latency*, *jitter*, *throughput*, dan *packet loss*, serta kinerja perangkat (CPU *load* dan memori). Hasil penelitian menunjukkan bahwa serangan ARP *Spoofing* yang dilancarkan oleh satu perangkat ESP32 efektif dan dapat digunakan sebagai serangan DoS karena mampu memutus koneksi *client* target dari *server* dengan tingkat *packet loss* mencapai hampir 100%. Sebaliknya, serangan ICMP *Flood* dari satu perangkat ESP32 penyerang tidak berhasil mematikan perangkat target tetapi secara konsisten meningkatkan beban CPU-nya mencapai 17,63%. Penelitian ini membuktikan bahwa perangkat berdaya rendah seperti ESP32 dapat digunakan sebagai platform serangan yang efektif dalam jaringan lokal, menyoroti pentingnya keamanan pada lapisan jaringan bahkan di antara perangkat sejenis.

Kata kunci: *Denial of Service* (DoS), *ARP Spoofing*, ESP32, *Internet of Things* (IoT), *Quality of Service* (QoS)

Analysis of Denial of Service (DoS) and Address Resolution Protocol (ARP) Spoofing Attacks among ESP32 Devices in a Wireless Sensor Network Based on Star Topology.

Abstract

Internet of Things (IoT) devices such as the ESP32, despite their popularity due to low cost and Wi-Fi capabilities, possess limited resources that render them vulnerable to cyberattacks. This research analyzes the implementation using ESP32 and impact of two common attack types, Denial of Service (DoS) via ICMP Flood and Address Resolution Protocol (ARP) Spoofing, within a star topology Wireless Sensor Network (WSN) environment. In this study, one ESP32 device was programmed as an attacker to target one of three other ESP32 client devices connected to a local server via the WebSocket protocol. The objective of this research is to analyze the implementation of these attacks, their impact on the target device's performance, and their effect on Quality of Service (QoS) metrics specifically latency, jitter, throughput, and packet loss as well as device performance (CPU load and memory). The results indicate that an ARP Spoofing attack launched from a single ESP32 is effective and can function as a DoS attack, successfully disconnecting the target client from the server with a packet loss rate approaching 100%. Conversely, the ICMP Flood attack from a single attacking ESP32 did not succeed in shutting down the tar get device but consistently increased its CPU load by 17.63%. This study demonstrates that low-power devices like the ESP32 can be utilized as effective attack platforms within a local network, highlighting the critical importance of network layer security, even among similar devices.

Keywords: *Denial of Service, ARP Spoofing, ESP32, Internet of Things, Quality of Service.*

PRAKATA

Segala puji dan syukur panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul **"Analisis Proses Serangan Denial of Service (DoS) dan Address Resolution Protocol (ARP) Spoofing antar Perangkat ESP32 pada Wireless Sensor Network (WSN) Bertopologi Star"** 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 yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.
3. Bapak Uray Ristian, S.Kom., M.Kom., sebagai dosen Pembimbing Pertama yang telah memberikan masukan serta meluangkan waktu dan pikiran yang memberikan dorongan dalam bimbingan penulisan skripsi.
4. Bapak Hafiz Muhardi, S.T., M.Kom., selaku dosen Pembimbing Kedua, yang telah memberikan masukan serta meluangkan waktu dan pikiran yang memberikan dorongan dalam bimbingan penulisan skripsi.
5. Bapak Kasliono, S.Mat., M.Cs., selaku dosen Penguji Pertama, yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.
6. Bapak Hirzen Hasfani, S.Kom., M.Cs., sebagai dosen Penguji Kedua yang telah memberikan kontribusi dengan memberikan masukan dan pertanyaan yang memperkaya isi dari tugas akhir ini.

7. Ibu Rahmi Hidayati, S.Kom., M.Cs., 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. Semua pihak yang terlibat langsung maupun yang tidak langsung dalam penulisan tugas akhir ini.

Pontianak, 28 Juli 2025

Dede Kurniawan

DAFTAR ISI

DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xiii
DAFTAR KODE PROGRAM xiv
BAB 1 PENDAHULUAN 15
1.1 Latar Belakang 15
1.2 Rumusan Masalah 18
1.3 Batasan Masalah 18
1.4 Tujuan Penelitian 19
1.5 Manfaat Penelitian 19
1.6 Sistematika Penulisan 19
BAB 2 LANDASAN TEORI 21
2.1 Perbandingan dengan penelitian terdahulu 21
2.2 *Wireless Sensor Network* (WSN) 24
2.3 ESP32 24
2.4 *Server* 25
2.5 Websocket 25
2.6 *Gateway* 25
2.7 *Virtual Machine* 26
2.8 Kali Linux 26
2.9 Wireshark 27
2.10 Visual Studio Code 27
2.11 PlatformIO 28
2.12 ESP-IDF 28
2.13 Node.js 28
2.14 SQLite 29
2.15 *Denial of Service* (DoS) 29
2.16 *Internet Control Message Protocol* (ICMP) 30
2.17 *Address Resolution Protocol (ARP) Spoofing* 31
2.18 *Quality of Service* (QoS) 31

2.19 *Throughput* 32
2.20 *Latency* 32
2.21 *Jitter* 33
2.22 *Packet Loss* 34
BAB 3 METODE PENELITIAN 36
3.1 Studi Literatur 36
3.2 Analisis Kebutuhan 37
3.2.1 Kebutuhan Perangkat Keras 37
3.2.2 Kebutuhan Perangkat Lunak 37
3.3 Perancangan Sistem 37
3.3.1 Perancangan Perangkat Keras 38
3.3.2 Perancangan Perangkat Lunak 38
3.3.3 Perancangan *Server* 38
3.3.4 Perancangan Basis Data 39
3.3.5 Perancangan Antar Muka 39
3.3.6 Perancangan Serangan 39
3.4 Implementasi Sistem 39
3.5 Pengujian Sistem 40
3.6 Kesimpulan dan Saran 40
BAB 4 PERANCANGAN 41
4.1 Deskripsi Sistem 41
4.2 Perancangan Arsitektur Sistem 41
4.3 Perancangan Perangkat Keras 42
4.4 Perancangan Perangkat Lunak 43
4.4.1 Perangkat Lunak *Client* (ESP32) 44
4.4.2 Perangkat Lunak *Attacker* (ESP32) 44
4.4.3 Perancangan *Server* 44
4.4.4 Perancangan Basis Data 45
4.4.5 Tabel Logs pada Basis Data 45
4.5 Perancangan Antar Muka 46
4.6 Perancangan Serangan 46
4.7 Perancangan Serangan ICMP *Flood* 47

4.8 Perancangan Serangan ARP *Spoofing* 47
4.9 Perancangan Serangan ICMP *Flood* dan ARP *Spoofing* 48
BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN 49
5.1 Implementasi Perangkat Keras 49
5.2 Implementasi Perangkat Lunak 50
5.2.1 Perangkat Lunak *Client* (ESP32) 51
5.2.2 Perangkat Lunak *Attacker* (ESP32) 53
5.2.3 Implementasi *Server* 56
5.2.4 Implementasi Basis Data 59
5.2.5 Implementasi Tabel Logs pada Basis Data 59
5.3 Implementasi Antar Muka 60
5.4 Implementasi Serangan 61
5.4.1 Serangan ICMP *Flood* 62
5.4.2 Serangan ARP *Spoofing* 64
5.4.3 Serangan ICMP Flood dan ARP Spoofing 68
5.5 Pengujian Sistem 68
5.5.1 Dampak Serangan terhadap *Quality of Service* (QoS) 69
5.5.2 Dampak Serangan terhadap Kinerja Perangkat 73
5.5.3 Analisis Kapabilitas ESP32 75
5.6 Pembahasan 76
BAB 6 PENUTUP 80
6.1 Kesimpulan 80
6.2 Saran 81
DAFTAR PUSTAKA 83
LAMPIRAN 86

DAFTAR GAMBAR

Gambar 2.1 Wireless Sensor Network 24
Gambar 2.2 ESP32 24
Gambar 2.3 Koneksi WebSocket 25
Gambar 2.4 Logo Kali Linux 26
Gambar 2.5 Aplikasi Wireshark 27
Gambar 2.6 Logo Aplikasi Visual Studio Code 27
Gambar 2.7 Logo Aplikasi PlatformIO 28
Gambar 2.8 Logo Aplikasi Node.js 29
Gambar 2.9 Logo SQLite 29
Gambar 2.10 Serangan *Denial of Service* 30
Gambar 2.11 Ilustrasi Serangan ARP *Spoofing* 31
Gambar 3.1 Diagram Alir Penelitian 36
Gambar 4.1 Arsitektur Sistem 41
Gambar 4.2 Tampilan *Dashboard Web* pada Jaringan Lokal 46
Gambar 4.3 Perancangan Serangan ICMP *Flood* 47
Gambar 4.4 Perancangan Serangan ARP Spoofing 48
Gambar 4.5 Perancangan Serangan Gabungan 48
Gambar 5.1 Keseluruhan Arsitektur Sistem 50
Gambar 5.2 Tampilan Serial Monitor pada ESP32-Client_01 pada saat Serangan ARP Spoofing 52
Gambar 5.3 Kondisi Lalu Lintas Jaringan menggunakan Wireshark saat serangan ICMP *Flood*. 54
Gambar 5.4 Tampilan Serial Monitor pada ESP32 *Attacker* serangan ICMP *Flood Request* 54
Gambar 5.5 Tampilan Serial Monitor pada ESP32 *Attacker* saat Serangan ARP *Spoofing* 56
Gambar 5.6 Interface wlan0 sebelum diubah menjadi Mode Monitor 56
Gambar 5.7 Proses mengubah *Interface* Wlan0 *Station* menjadi Wlan0 *Monitor* 57
Gambar 5.8 Interface wlan0 setelah diubah menjadi Mode Monitor 57
Gambar 5.9 Tampilan Isi Database dari Aplikasi DB Browser 60

Gambar 5.10 Tampilan Implementasi Dashboard pada Web Lokal 61
Gambar 5.11 Proses Pengambilan Informasi terhadap *Client* yang akan dijadikan Target Serangan 62
Gambar 5.12 Alamat IP Target dimasukkan kedalam Program ESP32 *attacker* . 63
Gambar 5.13 Kode Program untuk Paket ICMP Echo Request..... 63
Gambar 5.14 Proses *Firmware* diunggah ke dalam ESP32 *attacker* 63
Gambar 5.15 Tampilan *Serial Monitor* pada ESP32 *Attacker* saat melakukan Serangan ICMP *Flood* 64
Gambar 5.16 Pola Serangan dari ICMP *Flood* pada aplikasi Wireshark..... 64
Gambar 5.17 Proses Pengumpulan Informasi terhadap Perangkat Target..... 65
Gambar 5.18 Alamat IP pada *Server* menggunakan Perintah ifconfig 65
Gambar 5.19 Alamat MAC Perangkat Target dimasukkan kedalam Program ESP32 *Attacker* 66
Gambar 5.20 Kode Program untuk Membangun Paket ARP 66
Gambar 5.21 Proses Kompilasi dan Upload Program ke dalam ESP32 67
Gambar 5.22 Serangan ARP *Reply* terkirim ke Perangkat Target 67
Gambar 5.23 Serangan Gabungan yang dijalankan Secara Bersamaan Dimasukkan kedalam ESP32 *Attacker*..... 68
Gambar 5.24 Paket yang Tertangkap Pada Wireshark ketika Serangan Gabungan berlangsung. 68
Gambar 5.25 Jumlah Paket yang diterima *Server* selama pengujian berlangsung. 69
Gambar 5.26 Grafik Dampak terhadap *Throughput* dari Setiap Serangan. 70
Gambar 5.27 Grafik Dampak terhadap *Latency* dari Setiap Serangan. 71
Gambar 5.28 Grafik Dampak terhadap *Jitter* dari Setiap Serangan..... 72
Gambar 5.29 Grafik Dampak terhadap *Packet Loss* di Setiap Serangan. 73
Gambar 5.30 Grafik Dampak Serangan terhadap CPU *Load* di Setiap Serangan 74
Gambar 5.31 Grafik Dampak Serangan terhadap *Free Heap Memory* di Setiap Serangan. 75

DAFTAR TABEL

Tabel 2.1 Perbandingan dengan Penelitian Terdahulu..... 21
Tabel 2.2 Tabel *Quality of Service*..... 32
Tabel 2.3 Performansi *Throughput* Jaringan Standar TIPHON..... 32
Tabel 2.4 Perfomansi *Latency* Jaringan Standar TIPHON 33
Tabel 2.5 Performansi *Jitter* Jaringan Standar TIPHON 34
Tabel 2.6 Performansi *Packet Loss* Jaringan Standar TIPHON 34
Tabel 4.1 Database pada Tabel Logs 45
Tabel 4.2 Rancangan pada Tabel Logs 45
Tabel 5.1 Kapabilitas ESP32 Penyerang..... 76

DAFTAR KODE PROGRAM

Kode Program 5.1 Deklarasi Variabel Konfigurasi Wi-Fi..... 51
Kode Program 5.2 *Task* pada Pengumpulan dan Pengiriman Metrik 51
Kode Program 5.3 Pemeriksaan *Gateway* pada ESP32 *Client* 51
Kode Program 5.4 Output Pengiriman Data Metrik pada *Client* 52
Kode Program 5.5 *Task* ICMP *Flood* pada *Attacker* 53
Kode Program 5.6 Task Serangan ARP Spoof pada Attacker 55
Kode Program 5.7 Inisialisasi *library* yang digunakan pada file server.js 57
Kode Program 5.8 Fungsi *Capture Packet* terhadap *Client* menggunakan *Interface* wlan0mon dan eth0 57
Kode Program 5.9 *Shutdown Server* setelah 30 menit 58
Kode Program 5.10 Implementasi Basis Data pada file Server.js 59
Kode Program 5.11 Tampilan Website Lokal..... 60

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pada beberapa tahun terakhir, ESP32 telah banyak digunakan sebagai *microcontroller* dalam jaringan IoT. Perangkat ini memiliki fitur Wi-Fi yang dapat memudahkan pengguna dalam menghubungkan satu perangkat dengan perangkat yang lain dengan biaya yang sangat murah, namun terdapat tantangan keamanan dalam proses transmisi data. Perangkat IoT sering kali rentan terhadap peretasan dan serangan siber lainnya karena keterbatasan prosesor, kapasitas memori, dan fitur keamanan. Beberapa jenis serangan yang umum dalam IoT meliputi perangkat *spoofing*, serangan *Man-in-the-Middle* (MITM), *Denial of Service* (DoS), *ransomware*, dan akses tidak sah (*unauthorized access*) (Almomani dkk., 2024). Risiko dan ancaman ini muncul dari sifat perangkat yang selalu terhubung, perkembangan teknologi yang pesat, dan meningkatnya permintaan aplikasi IoT di berbagai bidang (Silva dkk., 2024). Pada daya komputasi yang terbatas, perangkat IoT berisiko mengalami serangan siber seperti *Denial of Service* (DoS). *Man in the Middle* (MITM) adalah salah satu serangan yang umum terjadi di jaringan dan sering melibatkan ARP *Spoofing*, yang memungkinkan peretas mencegat dan mengubah komunikasi antara perangkat IoT dan *server* yang terhubung (Alsaaidah dkk., 2024). Langkah mitigasi terhadap *ARP Cache Poisoning* penting diterapkan pada jaringan tradisional dan *Sofware-Defined Networking* (SDN) karena serangan ini dapat membuka celah untuk serangan lain, seperti DoS, MITM, dan *host impersonation* (Shah & Cosgrove, 2019). Selain itu, *malware* seperti *worm*, *virus*, skrip berbahaya, dan *spyware* dapat dimanfaatkan untuk mencuri informasi, merusak data, mengganggu layanan, atau merusak perangkat IoT (Andaraweera dkk., 2022). Serangan DoS, yang semakin umum dalam IoT, bertujuan menghentikan atau mengganggu layanan target (Almomani dkk., 2024). DoS dapat membebani perangkat hingga koneksinya terputus atau responsnya menjadi lambat, sementara ARP *spoofing* memungkinkan penyerang mengelabui jaringan untuk mengakses data yang tidak sah atau mengganggu komunikasi antar perangkat.

Dalam penelitian ini, ESP32 digunakan sebagai target dan perangkat penyerang untuk mensimulasikan beberapa ancaman yang mungkin terjadi dalam lingkungan IoT dengan keterbatasan pada perangkat penyerang yaitu ESP32.

Terdapat keterbatasan sumber daya pada ESP32 sehingga para pengguna perangkat ini membutuhkan protokol yang menggunakan sumber daya yang kecil atau *lightweight* agar proses transmisi data lancar. Hal ini memungkinkan untuk pengguna untuk memilih protokol yaitu WebSocket. Protokol WebSocket, *client* harus membuka koneksi jaringan protokol TCP ke *server* terlebih dahulu. Setelah *server* mengirimkan respon atas permintaan yang telah dikirim, koneksi terbuka dan akan terus tersedia hingga ada perintah untuk menutup koneksi (Ahsy dkk., 2019). Protokol ini sering digunakan juga dilingkungan IoT karena menawarkan layanan yang sangat cocok di perangkat IoT. Keterbatasan sumber daya ini juga dapat dimanfaatkan oleh orang yang tidak bertanggung jawab. Perangkat ESP32 dapat dijadikan target peretas, karena memiliki daya komputasi yang rendah, namun fiturnya melimpah. Tujuannya agar komunikasi antar perangkat terganggu. Selain itu secara teknis pada perangkat ESP32 tidak terdapat sistem operasi dan terdapat pilihan *firmware*. Hal ini tidak memungkinkan untuk meretas perangkat secara *wireless* dengan tujuan mengambil kontrol penuh dari ESP32, kecuali peretas datang langsung dan meretas perangkat tersebut, tetapi tidak menutup kemungkinan perangkat ESP32 tidak dapat diretas, namun dapat dieksploitasi melalui *firmware* dan koneksi jaringan.

Penelitian sebelumnya berjudul "*Forensic Analysis of an IoT ARP Spoofing Attack*" (Friedl & Pernul, 2024). Penelitian ini menganalisis serangan ARP *spoofing* pada jaringan IoT. Studi ini mendalami mekanisme manipulasi tabel ARP yang dilakukan oleh penyerang untuk menyamar sebagai perangkat otoritatif dalam jaringan dengan maksud untuk pengalihan, atau manipulasi lalu lintas data. Fokus utama penelitian ini adalah identifikasi jejak digital yang ditinggalkan oleh penyerang, termasuk pola paket jaringan yang tidak wajar, perubahan tabel ARP, dan anomali komunikasi antar-perangkat. Untuk membantu mitigasi serangan IoT dan mengembangkan lingkungan IoT yang aman, forensik IoT dapat menyediakan pandangan yang dalam mengenai proses dan fungsi dari suatu serangan. Hasil analisis memberikan panduan tentang teknik pengumpulan dan analisis bukti digital

yang efektif untuk mendeteksi serta melacak sumber serangan, sekaligus menyarankan pendekatan mitigasi untuk memperkuat keamanan jaringan IoT terhadap serangan semacam ini.

Penelitian sebelumnya yang berjudul "*Cybersecurity Risk Analysis in the IoT: A Systematic Review*" (AlSalem dkk., 2023) memberikan tinjauan sistematis terhadap berbagai risiko keamanan siber dalam ekosistem *Internet of Things* (IoT). Studi ini menganalisis ancaman utama, termasuk kerentanan terhadap serangan siber seperti *malware*, *ransomware*, ARP *spoofing*, DDoS, dan eksploitasi protokol komunikasi. Faktor-faktor yang memperbesar risiko, seperti keterbatasan sumber daya perangkat, arsitektur jaringan yang heterogen, dan kurangnya standar keamanan yang universal telah teridentifikasi.

Penelitian selanjutnya berjudul "*Security Challenges and Solutions in Internet of Things (IoT): A Review*" (Andaraweera dkk., 2022) mengulas berbagai tantangan keamanan yang dihadapi dalam ekosistem IoT serta solusinya. Studi ini mengidentifikasi risiko utama, seperti kerentanan terhadap serangan jaringan seperti DDoS, ARP *spoofing*, masalah autentikasi, privasi data, dan keterbatasan sumber daya perangkat IoT yang mempersulit penerapan langkah-langkah keamanan tradisional. Pada penelitian ini mengkaji solusi inovatif, termasuk enkripsi ringan, protokol keamanan khusus IoT, dan implementasi teknologi blockchain serta kecerdasan buatan untuk mendeteksi dan mencegah serangan.

Berdasarkan penelitian yang terkait, maka dilakukan penelitian dengan judul "Analisis Proses Serangan *Denial of Service* (DoS) dan *Address Resolution Protocol* (ARP) *Spoofing* antar Perangkat ESP32 pada *Wireless Sensor Network* (WSN) Bertopologi *Star*". Penelitian ini bertujuan untuk mengetahui bahwa perangkat kecil seperti ESP32 dapat digunakan sebagai perangkat penyerang dengan kapasitas yang terbatas dan mengetahui bagaimana proses terjadinya serangan DoS dan ARP ini di jaringan lokal yang menggunakan 4 ESP32, yaitu 1 unit ESP32 sebagai penyerang, dan sisanya sebagai *client.* Keempat ESP32 ini terhubung dengan 1 *access point* dan dengan *server* lokal. Dari 3 unit ESP32 *client* akan mengirimkan data metrik performa ke *server*, lalu dari penyerang mengintervensi dari komunikasi tersebut. Dengan demikian, proses serangan dan dampak serta paket yang ditransmisikan dapat di analisis.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana proses implementasi serangan *Denial of Service* (DoS) berbasis ICMP *Flood* dan serangan ARP *Spoofing* antar perangkat ESP32 pada *Wireless Sensor Network* (WSN) bertopologi *star*?
2. Bagaimana dampak kuantitatif dari satu perangkat ESP32 penyerang dapat mempengaruhi CPU *load* dan penggunaan memori perangkat ESP32 *client* selama penyerangan ?
3. Bagaimana dampak kuantitatif dari serangan DoS dan ARP *spoofing* terhadap kinerja ESP32 terhadap QoS dalam jaringan (latensi, *throughput*, dan *packet loss*)?

1.3 Batasan Masalah

Batasan masalah penelitian ini adalah sebagai berikut:

1. Penelitian melibatkan 4 unit perangkat ESP32 yang digunakan 1 digunakan sebagai penyerang dan 3 yang lainnya merupakan *client*/korban dalam simulasi serangan.
2. Penelitian dilakukan dalam jaringan lokal dengan topologi star yang terdiri dari 4 perangkat ESP32 yang terhubung ke *gateway* dan *server*.
3. *Server* yang digunakan merupakan *virtual machine* yang diinstal pada laptop.
4. Penelitian dilakukan dalam kondisi penyerang sudah terhubung pada *access point*.
5. Menggunakan 1 unit ESP32 sebagai penyerang dan 3 unit ESP32 *client* yang terhubung dalam jaringan lokal.
6. Komunikasi *client* ESP32 dengan *server* menggunakan protokol WebSocket.
7. Fokus pada serangan DoS melalui paket *ICMP Echo Request* dan paket ARP *Reply* palsu.
8. Analisis QoS akan berfokus pada *throughput*, *latency*, *jitter*, dan *packet loss* di perangkat ESP32 yang diserang.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menerapkan dan menganalisis serangan DoS dan ARP menggunakan ESP32 yang terjadi di jaringan lokal.
2. Menganalisis dampak serangan pada ESP32 terhadap *CPU load* dan penggunaan memori dalam menghadapi serangan DoS dan ARP *spoofing* yang dilakukan oleh perangkat ESP32 penyerang di jaringan lokal.
3. Mengidentifikasi dampak dari serangan tersebut terhadap *Quality of Service* (QoS) dalam jaringan (*throughput*, *latency*, *jitter*, dan *packet loss*).

1.5 Manfaat Penelitian

Terdapat beberapa manfaat pada penelitian ini yaitu:

1. Mengidentifikasi proses dan teknik yang digunakan pada ESP32 untuk melakukan serangan *Denial of Service* (DoS) dan ARP *Spoofing*.
2. Memberikan pemahaman tentang proses serangan, alat yang digunakan, dan dampak yang dihasilkan, sehingga memungkinkan untuk melakukan mitigasi.

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 risiko serangan siber pada perangkat IoT dan mengapa 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 *Wireless Sensor Network* (WSN), ESP32, *Server,* WebSocket, *Gateway*, *Virtual Machine,*

Kali Linux, Wireshark, Visual Studio Code, PlatformIO, ESP-IDF, Node.js, SQLite, *Denial of Service* (DoS), *Internet Control Message Protocol* (ICMP), *Address Resolution Protocol* (ARP) *Spoofing*, *Quality of Service* (QoS), *Throughput*, *Latency*, *Jitter*, dan *Packet Loss*.

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 perangkat keras dan perangkat lunak. Pada perancangan perangkat keras terdiri dari perancangan *server* kali linux, rancangan topologi star menggunakan *access point*, 4 unit ESP32 *client* dan 1 unit ESP32 sebagai penyerang, dan perancangan keseluruhan perangkat keras. Sedangkan pada perancangan perangkat lunak meliputi perancangan sistem komunikasi antara ESP32 *client* dengan *server*, dan perancangan penerapan protokol WebSocket pada *server*.

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.