



PROPOSAL SKRIPSI

ANALISIS PERFORMA DNS SINKHOLE SEBAGAI ADBLOCK PADA JARINGAN WI-FI MENGGUNAKAN ESP32

**Disusun Sebagai Syarat Memperoleh Gelar Sarjana Teknik
Jurusan Teknik Informatika Fakultas Teknik
Universitas Malikussaleh**

DISUSUN OLEH:

**NAMA : YOUNG YOLVI FEDDO RESTIEN
NIM : 190170150
PROGRAM STUDI : TEKNIK INFORMATIKA**

**JURUSAN INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MALIKUSSALEH
LHOKSEUMAWE**

2023

DAFTAR ISI

DAFTAR ISI	i
DAFTAR TABEL	ii
DAFTAR GAMBAR	iii
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Tujuan Penelitian	3
1.4. Manfaat Penelitian	3
1.5. Ruang Lingkup.....	4
BAB II TINJAUAN PUSTAKA	5
2.1. DNS Sinkhole	5
2.2. ESP32	5
2.3. Iklan.....	6
2.3.1. Kelas Iklan.....	6
2.4. Penggunaan DNS Sinkhole dalam Pemblokiran Iklan.....	7
2.5. ESP32 Sebagai Alat Pemblokiran Iklan	8
2.6. Penelitian Terdahulu	8
BAB III METODE PENELITIAN	18
3.1. Tempat dan Waktu Penelitian.....	18
3.2. Tahap Penelitian.....	18
3.3. Alat dan Bahan.....	19
3.3.1. ESP32	19
3.3.2. Router	20
3.3.3. Perangkat Keras (<i>Hardware</i>).....	21
3.3.4 Perangkat lunak (<i>Software</i>)	21
3.4. Perancangan Sistem	21
3.5. Implementasi.....	22
DAFTAR PUSTAKA	23

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu.....	8
Tabel 3. 1 Spesifikasi ESP32	19

DAFTAR GAMBAR

Gambar 2. 1 ESP32.....	6
Gambar 3. 1 Router.....	20
Gambar 3. 2 Skema Sistem	22

BAB I

PENDAHULUAN

1.1. Latar Belakang

Penggunaan internet saat ini telah menjadi kebutuhan pokok bagi masyarakat di seluruh dunia. Dalam kehidupan sehari-hari, banyak orang yang mengandalkan internet untuk berbagai macam keperluan, seperti bekerja, belajar, berkomunikasi, berbelanja, dan lain-lain. Dalam proses mengakses informasi melalui internet, pengguna seringkali dihadapkan pada iklan yang mengganggu. Iklan-iklan ini tidak hanya mengurangi kenyamanan pengguna saat menjelajah internet, tetapi juga dapat mempengaruhi kecepatan akses dan memakan kuota data pengguna. Oleh karena itu, diperlukan solusi yang efektif untuk memblokir iklan pada jaringan Wi-Fi.

Peningkatan penggunaan berbagai bentuk iklan digital seperti banner, iklan pop-up, sponsorship, hyperlink dan lainnya telah menyebabkan ketidaknyamanan di kalangan pengguna. Hal ini disebabkan karena iklan-iklan tersebut seringkali tidak relevan. Banyak perusahaan memasukkan iklan mereka di berbagai platform, seperti situs web, blog, media sosial, dan permainan *Online*, yang kemudian menjadi sasaran dari aplikasi pemblokir iklan. Karena alasan tersebut, sebagian besar pengguna internet telah mulai menggunakan perangkat lunak pemblokiran iklan (Apriyatna & Zulfikar, 2023).

Salah satu cara untuk memblokir iklan pada jaringan Wi-Fi adalah dengan menggunakan teknik DNS Sinkhole. DNS Sinkhole merupakan server DNS yang mampu menyediakan alamat IP palsu (*spoofing*) sebagai respons terhadap permintaan DNS, yang mengakibatkan domain yang dicari tidak lagi dapat diakses (Jung et al., 2020). Dalam konteks pemblokiran iklan, DNS Sinkhole akan mengalihkan permintaan DNS yang berasal dari server iklan ke alamat IP lokal yang tidak memiliki konten, sehingga iklan tersebut tidak dapat ditampilkan pada perangkat pengguna.

ESP32 adalah jenis mikrokontroler yang dikembangkan oleh Espressif Systems, sebuah perusahaan yang berlokasi di Shanghai, China. ESP32 menyediakan solusi jaringan Wi-Fi terintegrasi, berfungsi sebagai penghubung

antara mikrokontroler yang ada dan jaringan Wi-Fi. ESP32 merupakan sebuah mikrokontroler dengan kapabilitas jaringan Wi-Fi yang dapat digunakan untuk berbagai aplikasi IoT (Internet of Things). ESP32 memiliki keunggulan dalam hal ukuran, biaya, dan konsumsi daya yang rendah, sehingga menjadi pilihan yang tepat untuk digunakan sebagai platform pemblokiran iklan pada jaringan Wi-Fi. Dengan memanfaatkan kemampuan ESP32 dalam mengendalikan aliran data jaringan Wi-Fi, pengguna dapat mengimplementasikan DNS Sinkhole untuk memblokir iklan yang mengganggu.

Oleh karena itu, penelitian ini dirancang untuk menganalisis performa DNS Sinkhole dalam pemblokiran iklan pada jaringan Wi-Fi menggunakan ESP32. Tujuan dari penelitian ini adalah untuk memahami sejauh mana performa dan efektivitas ESP32 dalam penerapan metode DNS Sinkhole untuk pemblokiran iklan, serta untuk memberikan rekomendasi bagi penggunaan ESP32 dalam konteks ini di masa mendatang.

Diharapkan, hasil dari penelitian ini dapat memberikan kontribusi dalam meningkatkan kenyamanan pengguna saat menjelajah internet dan menghemat kuota data pengguna dengan mengurangi tampilan iklan yang tidak diinginkan. Selain itu, penelitian ini juga diharapkan dapat menjadi referensi bagi pengembang perangkat lunak dan perangkat keras dalam mengembangkan solusi pemblokiran iklan yang lebih efisien dan efektif.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas, maka permasalahan yang penulis rumuskan dalam penelitian ini, adalah:

1. Bagaimana performa DNS sinkhole menggunakan ESP32 dalam memblokir iklan pada jaringan Wi-Fi?
2. Apa kelebihan dan kekurangan menggunakan ESP32 sebagai perangkat dalam memblokir iklan pada jaringan Wi-Fi?
3. Bagaimana DNS Sinkhole mempengaruhi performa Wi-Fi saat dipasangkan dengan ESP32?
4. Bagaimana DNS Sinkhole mempengaruhi performa Wi-Fi?

1.3. Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah yang telah diuraikan di atas, berikut ini adalah tujuan dari penelitian ini:

1. Untuk mengevaluasi performa DNS Sinkhole yang menggunakan ESP32 dalam memblokir iklan pada jaringan Wi-Fi.
2. Penelitian ini juga bertujuan untuk memahami kelebihan dan kekurangan menggunakan ESP32 sebagai perangkat dalam memblokir iklan pada jaringan Wi-Fi.
3. Selain itu, penelitian ini juga mencoba untuk mengevaluasi pengaruh DNS Sinkhole pada performa Wi-Fi saat dipasangkan dengan ESP32.
4. Penelitian ini juga berupaya untuk mengetahui bagaimana DNS Sinkhole mempengaruhi performa Wi-Fi secara umum, baik dengan ESP32 maupun tanpa ESP32. Tujuan ini bertujuan untuk memberikan gambaran yang lebih luas tentang dampak DNS Sinkhole pada jaringan Wi-Fi dan bagaimana perangkat seperti ESP32 dapat mempengaruhi efek ini.

Secara keseluruhan, tujuan utama dari penelitian ini adalah untuk memberikan pemahaman yang lebih mendalam tentang bagaimana DNS Sinkhole dan ESP32 bisa bekerja sama dalam memblokir iklan pada jaringan Wi-Fi, dan bagaimana hal itu dapat mempengaruhi performa jaringan.

1.4. Manfaat Penelitian

Manfaat dari penelitian yang dilakukan ini adalah:

1. Meningkatkan pemahaman mengenai performa DNS Sinkhole dalam konteks pemblokiran iklan menggunakan ESP32.
2. Dengan memblokir iklan yang tidak diinginkan pada jaringan Wi-Fi, pengguna dapat menikmati pengalaman browsing yang lebih nyaman dan fokus pada konten yang mereka cari tanpa terganggu oleh iklan.
3. Dengan memblokir iklan pada jaringan Wi-Fi, konsumsi bandwidth yang digunakan oleh iklan akan berkurang, sehingga menghemat penggunaan data dan meningkatkan kecepatan akses internet.

4. Memberikan rekomendasi bagi penggunaan ESP32 dalam pemblokiran iklan pada jaringan Wi-Fi, yang dapat bermanfaat bagi pengguna individu, penyedia layanan internet, dan perusahaan.
5. Memberikan referensi bagi peneliti lain yang ingin melakukan penelitian serupa atau lebih lanjut dalam topik ini.

1.5. Ruang Lingkup

Ruang lingkup dari penelitian meliputi sebagai berikut:

1. Penelitian ini akan fokus pada analisis performa DNS Sinkhole dalam pemblokiran iklan pada jaringan WiFi dengan menggunakan ESP32.
2. Analisis ini akan mencakup pengukuran efektivitas metode ini dalam konteks pemblokiran iklan.
3. Penelitian ini tidak akan mencakup metode pemblokiran iklan lainnya atau penggunaan ESP32 dalam konteks lain.
4. Penelitian ini akan fokus pada pemblokiran iklan *Online* umum yang muncul saat menjelajahi web. Jenis iklan lain seperti pop-up, video, atau iklan dalam aplikasi mungkin tidak sepenuhnya dibahas dalam penelitian ini.

BAB II

TINJAUAN PUSTAKA

2.1. DNS Sinkhole

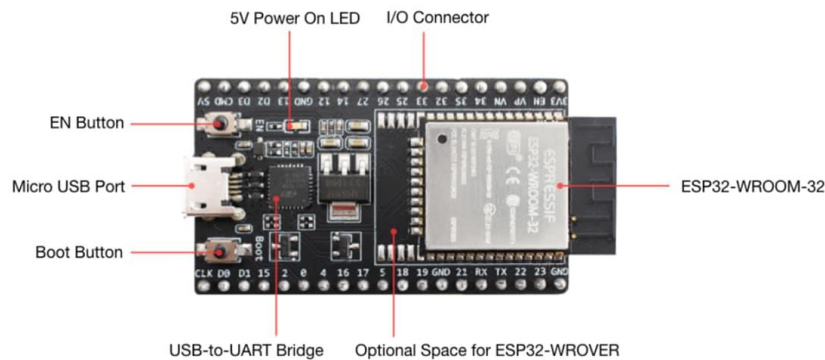
Sistem nama domain (DNS) adalah salah satu aspek yang sangat vital namun sering kali dilupakan dalam fungsi Internet. DNS dibutuhkan karena mengingat sejumlah besar alamat IP, yang merupakan serangkaian angka, dapat menjadi tugas yang sulit. DNS adalah sistem yang mengelola basis data besar yang memetakan alamat IP ke nama domain. Fungsi utamanya adalah mengambil URL yang kita ketikkan ke dalam browser web kita, mencari alamat IP server web yang menaungi situs tersebut, dan kemudian memberikan alamat IP tersebut kepada kita (Jokić & Šarac, 2022).

DNS Sinkhole merupakan server DNS yang mampu menyediakan alamat IP palsu (spoofing) sebagai respons terhadap permintaan DNS, yang mengakibatkan domain yang dicari tidak lagi dapat diakses (Jung et al., 2020). Sinkhole DNS, yang dikenal sebagai blackhole DNS, bertindak untuk menipu server DNS dengan tujuan menghentikan proses penyelesaian nama host dari URL tertentu. Sinkhole berfungsi sebagai metode untuk memblokir lalu lintas Internet yang berpotensi merusak. Hal ini dilakukan dengan cara mengatur pengalihan DNS sehingga menghasilkan alamat IP yang tidak asli ketika ditujukan ke URL spesifik (Jokić & Šarac, 2022). DNS Sinkhole memanfaatkan daftar domain yang akan diblokir (Jung et al., 2020). DNS Sinkhole dapat digunakan untuk membatasi akses ke situs-situs tertentu yang melanggar aturan perusahaan, termasuk konten media sosial yang tidak pantas (Jokić & Šarac, 2022).

2.2. ESP32

ESP32 merupakan sebuah sistem yang dilengkapi dengan dua CPU Xtensa LX6 berarsitektur Harvard yang terintegrasi (built-in) di dalam chip. Semua jenis memori pada ESP32, baik itu memori program (flash), RAM, dan RTC, juga perangkat-perangkat luar seperti modul Wi-Fi dan Bluetooth, antarmuka jaringan, GPIO, I2C, SPI, UART, dan lain-lain, terhubung ke bus data dan/atau bus instruksi CPU yang sama. Hal ini memungkinkan kedua CPU untuk mengakses

memori dan periferan secara bersamaan dan bekerja secara independen atau saling berbagi tugas untuk meningkatkan kinerja sistem secara keseluruhan (Farikha et al., 2020).



Gambar 2. 1 ESP32

Sumber: <https://www.mouser.co.id/>

2.3. Iklan

Iklan adalah suatu elemen yang dimasukkan ke dalam halaman yang tidak termasuk dalam konten utama dan umumnya didanai oleh sponsor. Konten yang disampaikan dengan tujuan untuk memperkenalkan suatu produk kepada audiens dengan platform media tertentu. Selain itu, kami telah mengelompokkan iklan ke dalam empat kelas yang memiliki ciri-ciri unik dan spesifik (IEEE Computer Society & Institute of Electrical and Electronics Engineers, n.d.).

2.3.1. Kelas Iklan

Terdapat beragam jenis iklan *Online* yang telah dikelompokkan ke dalam empat kelas yang berbeda. Yaitu sebagai berikut:

2.3.1.1. Iklan Tautan Teks

Iklan Tautan Teks mencakup semua jenis iklan yang muncul di dalam konten yang sama dari situs web atau aplikasi, dengan teks sebagai mode utama untuk periklanan. Dalam konteks ini, "contoh yang sama" mengacu pada iklan yang tidak termasuk dalam kategori Iklan Pop-up.

2.3.1.2. Iklan Gambar/ Grafis Iklan Gambar/Grafis

Iklan Gambar/Grafis memiliki kemiripan dengan Iklan Tautan Teks, di mana keduanya dapat mengandung teks. Namun, perbedaan utamanya terletak

pada dominasi elemen gambar dalam sebagian besar iklan ini. Teks dapat ditampilkan di atas gambar, namun elemen inti dari iklan ini biasanya berupa gambar.

2.3.1.3. Iklan Video

Iklan Video adalah jenis iklan yang memenuhi salah satu atau kedua kriteria berikut, dan juga berlaku pada situs web atau aplikasi yang sama:

- 1) Iklan yang disajikan dalam format video, baik dengan pemutaran video atau tanpa pemutaran.
- 2) Iklan yang menginterupsi video, baik dengan menyela di antara segmen video atau ditampilkan di atas konten video yang bukan iklan.

2.3.1.4. Iklan Pop-up

Iklan Pop-up didefinisikan sebagai iklan yang muncul dalam sebuah jendela pop-up.

2.4. Penggunaan DNS Sinkhole dalam Pemblokiran Iklan

DNS Sinkhole merupakan sebuah teknik yang memanfaatkan sistem Domain Name System (DNS) untuk memblokir akses ke domain-domain tertentu, termasuk domain yang digunakan oleh server iklan. Hal ini dilakukan dengan merubah tabel DNS sedemikian rupa hingga permintaan (request) yang ditujukan ke domain-domain tersebut dialihkan ke alamat lain atau bahkan diblokir sama sekali.

Pada konteks pemblokiran iklan, DNS Sinkhole memainkan peran penting. Sebagai contoh, saat pengguna membuka suatu website, bukan hanya konten utama yang dimuat, tetapi juga berbagai elemen lain termasuk iklan. Setiap iklan ini biasanya berasal dari server iklan yang berbeda-beda dan setiap pengunduhan elemen ini akan menggunakan bandwidth.

Dengan menerapkan DNS Sinkhole, permintaan ke server iklan tersebut dapat diblokir sehingga elemen iklan tidak dimuat dan bandwidth yang seharusnya digunakan untuk mengunduh iklan tersebut dapat dihemat. Selain itu, mengurangi jumlah iklan yang muncul di layar juga dapat memberikan pengalaman browsing

yang lebih nyaman bagi pengguna, karena konten yang mereka inginkan dapat ditampilkan dengan lebih dominan tanpa terganggu oleh iklan-iklan yang muncul.

2.5. ESP32 Sebagai Alat Pemblokiran Iklan

ESP32 memberikan konektivitas Wi-Fi yang bertenaga dan mendukung aneka macam mode operasi, seperti mode akses point, mode klien, serta mode dual. Dengan kemampuan ini, ESP32 dapat berfungsi menjadi titik akses Wi-Fi yang memungkinkan perangkat lain terhubung secara langsung ke ESP32, atau ESP32 bisa berperan menjadi perangkat yg terhubung ke jaringan Wi-Fi yg telah ada. Selain itu, ESP32 mempunyai dukungan terintegrasi buat protokol DNS.

Dalam konteks pemblokiran iklan, ESP32 dapat digunakan sebagai basis untuk sistem seperti DNS Sinkhole. Dalam kasus pemblokiran iklan, DNS Sinkhole dapat diatur untuk memblokir alamat IP atau domain yang dikenal digunakan untuk menyajikan iklan. Ketika digunakan dalam sistem seperti ini, ESP32 bertindak sebagai server DNS untuk jaringan Wi-Fi lokal. Ketika perangkat di jaringan mencoba untuk mengakses alamat yang dikaitkan dengan iklan, permintaan DNS akan diarahkan ke ESP32.

2.6. Penelitian Terdahulu

Penelitian terdahulu bertujuan untuk memberikan bahan perbandingan dan acuan. Maka dalam kajian pustaka ini peneliti mencantumkan hasil-hasil penelitian terdahulu sebagai berikut:

Tabel 2. 1 Penelitian Terdahulu

Nama Peneliti	Judul Penelitian	Tujuan/Hasil Penelitian
Salamat, Harlinda dan Nurhayati (2017)	“Perancangan Aplikasi Pemblokir Iklan (Advertisement) pada Browser yang Berbasis Android”	Tujuannya adalah untuk menyediakan solusi yang melindungi pengguna dari dampak negatif iklan dan memberikan rasa aman saat menggunakan <i>smartphone android</i> untuk mengunjungi

Tabel 2. 1 Penelitian Terdahulu (Lanjutan)

Nama Peneliti	Judul Penelitian	Tujuan/Hasil Penelitian
		<p><i>situs web</i>. Melalui penggunaan algoritma <i>Text Marnging</i>, yang menggabungkan <i>file host</i> yang ada di internet dengan yang ada pada sistem android. aplikasi ini bisa memblokir iklan dan konten negatif pada <i>web browser</i> berbasis android dengan menggunakan <i>file host</i> yang berisi URL iklan yang dianggap berpotensi merugikan pengguna. Namun, aplikasi ini hanya terbatas pada perangkat android dan menawarkan sedikit kustomisasi.</p>
Widja (2018)	<p>“Sistem IOT Berbasis Protokol MQTT Dengan Mikrokontroler ESP8266 dan ESP32”</p>	<p>Internet of Things (IoT) adalah komponen penting dalam Revolusi Industri 4.0 yang mengubah cara komunikasi antar mesin (Machine to Machine/M2M) yang terhubung melalui internet. IoT memiliki dampak yang luas dan dapat diterapkan dalam berbagai bidang yang membutuhkan kontrol otomatis dalam interaksi antar mesin.</p>

Tabel 2. 1 Penelitian Terdahulu (Lanjutan)

Nama Peneliti	Judul Penelitian	Tujuan/Hasil Penelitian
Kusumah dan Pradana (2019)	“Penerapan Trainer Interfacing Mikrokontroler dan Internet Of Things Berbasis ESP32 Pada Mata Kuliah Interfacing”	Trainer interface mikrokontroler ini dapat digunakan menjadi indera peraga atau indera praktek interface mikrokontroler baik interface SPI, I2C, dan UART. Indera peraga Internet of Things karena pada trainer ini sudah terdapat komponen input berupa potensiometer yg akan memperagakan pembacaan serta pemantauan nilai analog input melalui smartphone yang terkoneksi menggunakan jaringan internet, serta jua terdapat komponen output berupa LED buat memperagakan kontrol LED melalui smartphone.Trainer ini dibuat dengan menyatukan komponen yg diharapkan untuk mempraktekan materi interfacing serta Internet of Things pada satu papan sirkuit terpadu atau PCB agar dapat mengeliminasi kesalahan di saat penghubungan antar komponen menggunakan

Tabel 2. 1 Penelitian Terdahulu (Lanjutan)

Nama Peneliti	Judul Penelitian	Tujuan/Hasil Penelitian
		mikrokontroler yang menjadi salah satu hambatan dalam menelaah interface di mikrokontroler.
Satriawan dan Trisnawan (2021)	“Implementasi Layanan DNS Sinkhole sebagai Pemblokir Iklan menggunakan Arsitektur Cloud”	Adblocker terbukti berfungsi dengan baik di laptop, PC, dan smartphone. Dengan penggunaan adblocker, pengguna mendapatkan pengalaman berselancar di web yang lebih cepat, terbukti dengan penurunan total permintaan rata-rata sebesar 53%, waktu pemuatan halaman yang 56% lebih cepat, dan jumlah konten yang diunduh oleh browser berkurang dengan total sumber daya yang ditransfer berkurang rata-rata sebesar 45%. Selain itu, pengguna aplikasi mobile pada smartphone juga merasa kurang terganggu oleh iklan pada aplikasi yang sering mereka gunakan.

Tabel 2. 1 Penelitian Terdahulu (Lanjutan)

Nama Peneliti	Judul Penelitian	Tujuan/Hasil Penelitian
Apriyatna dan Zulfikar (2023)	“Analisis dan Implementasi Network Ad-blocking Pi-Hole di Raspberry Pi 4 Menggunakan OPNSense DHCP Dengan Metode PPDIOO (Studi Kasus Diskominfo SP Kabupaten Lebak)”	Dari hasil implementasi network ad-blocking Pi-Hole menggunakan OPNSense DHCP dengan fitur Sinkhole atau DNS yang telah dikonfigurasi, dapat disimpulkan bahwa menggunakan Pi-Hole dapat mengarahkan nama domain tertentu dan memfilter konten tertentu, yang mengakibatkan kegagalan akses ke situs yang sebenarnya. Hal ini dapat membantu meningkatkan kecepatan akses konten pada halaman web dengan mengurangi waktu yang diperlukan untuk memuat konten. Fitur Unbound DNS yang ada pada OPNSense juga dapat memberikan kontribusi dalam meningkatkan kecepatan transfer data (bandwidth) yang diperlukan untuk mengakses konten pada halaman web.

Tabel 2. 1 Penelitian Terdahulu (Lanjutan)

Nama Peneliti	Judul Penelitian	Tujuan/Hasil Penelitian
Larasati, Nugroho dan Rizal (2017)	“Implementasi Remote Desktop Melalui VPN Berbasis IPSec pada Smartphone dengan Menggunakan Vyatta OS”	Membuka jalur komunikasi pribadi untuk <i>smartphone</i> yang terhubung ke jaringan LAN perusahaan untuk memantau dan mengakses data. Dalam penelitian ini, dibangun <i>prototipe</i> aplikasi remote desktop melalui VPN berbasis IPSec yang menghasilkan paket ESP (<i>Encapsulating Security Payload</i>), menandakan bahwa konten yang dikirim telah dienkripsi. Hasilnya, penelitian ini berhasil menyediakan layanan akses data, pemantauan sumber daya, dan lalu lintas, serta <i>remote desktop</i> yang aman. Protokol keamanan IPSec bekerja dengan efektif untuk mengenkripsi data yang dikirim, sehingga alat penganalisis (<i>sniffer</i>) tidak mampu membaca lalu lintas yang terjadi antara <i>klien</i> dan <i>server web</i> .

Tabel 2. 1 Penelitian Terdahulu (Lanjutan)

Nama Peneliti	Judul Penelitian	Tujuan/Hasil Penelitian
Rahma, Rochim dan Widiyanto (2014)	“Analisis Implementasi Infrastructure as A Service (IaaS) Menggunakan Ubuntu Cloud Infrastruktur”	Ini adalah contoh bagaimana layanan IaaS dapat dibangun dalam jaringan lokal untuk mensimulasikan bagaimana IaaS memberikan fleksibilitas dalam memilih sumber daya seperti CPU, Memory, dan Image yang ditawarkan dalam bentuk "flavor" yang dapat dipilih oleh pengguna. Penelitian ini berhasil merancang dan menerapkan Infrastructure as a Service (IaaS) Cloud menggunakan Openstack pada sebuah server yang berjalan pada sistem operasi Ubuntu 12.04 LTS. Ini memungkinkan penyesuaian kapasitas komputasi sesuai kebutuhan pengguna secara on-demand dengan memilih flavor yang ada. Meski arsitektur yang digunakan menawarkan berbagai opsi kustomisasi, namun masih terbatas pada flavor yang telah ditentukan dalam penelitian tersebut.

Tabel 2. 1 Penelitian Terdahulu (Lanjutan)

Nama Peneliti	Judul Penelitian	Tujuan/Hasil Penelitian
Aisyah dan Ariyanti (2017)	“Perbandingan Antara Format Iklan <i>Online</i> Native Advertising dan <i>Online</i> Banner Advertising terhadap Perilaku Konsumen pada Iklan <i>Online</i> ”	Penelitian ini bertujuan untuk membandingkan efektivitas antara <i>Online</i> local advertising dengan <i>Online</i> banner advertising and marketing dengan menggunakan teori bahwa keyakinan tentang secara <i>Online</i> iklan pengaruh pada sikap dan perilaku konsumen terhadap iklan <i>Online</i> . Hasil penelitian menunjukkan bahwa keyakinan terhadap iklan <i>Online</i> berpengaruh positif signifikan terhadap sikap dan perilaku konsumen pada iklan <i>Online</i> . Dibandingkan dengan <i>Online</i> banner advertising and marketing, <i>Online</i> local marketing dianggap lebih dapat diterima oleh responden.
Sani dan Setiawan (2020)	“DNS Tunneling Detection Using Elasticsearch”	Protokol Sistem Nama Domain (DNS) adalah salah satu media yang sering dimanfaatkan oleh malware untuk melakukan kontrol dan mengambil alih komputer yang menjadi korban. Teknik ini dikenal

Tabel 2. 1 Penelitian Terdahulu (Lanjutan)

Nama Peneliti	Judul Penelitian	Tujuan/Hasil Penelitian
		<p>sebagai DNS tunneling. Selain itu, DNS tunneling juga dapat digunakan untuk menghindari captive portal hotspot di lokasi umum dan mempengaruhi kualitas jaringan secara negatif. Namun, dalam tahap yang lebih berbahaya, DNS tunneling juga dapat dimanfaatkan untuk mengambil data dari komputer korban.</p>
Jokiy dan Sarac (2022)	“Cyber Security and Domain Name Systems Deploy and Protect Network With DNS Sinkhole Blackhole”	<p>DNS, yang merupakan singkatan dari Domain Name System, adalah protokol standar yang digunakan oleh komputer personal untuk bertukar data melalui internet, dalam kerangka protokol TCP/IP. Server DNS, juga dikenal sebagai server nama, bertanggung jawab atas pengelolaan database besar yang memetakan nama domain ke alamat IP. Dengan kata lain, DNS adalah pusat operasi jaringan modern yang menerjemahkan nama domain</p>

Tabel 2. 1 Penelitian Terdahulu (Lanjutan)

Nama Peneliti	Judul Penelitian	Tujuan/Hasil Penelitian
		yang dapat dibaca oleh manusia menjadi alamat Protokol Internet (IP) yang dapat digunakan oleh mesin.

BAB III

METODE PENELITIAN

3.1. Tempat dan Waktu Penelitian

Penelitian Implementasi DNS Sinkhole menggunakan ESP32 untuk Pemblokiran iklan pada Jaringan WI-FI dilakukan di tempat yang memiliki akses internet. Penelitian ini dilakukan di Kota Lhokseumawe lebih tepatnya warung kopi. Waktu penelitian dari bulan Juni sampai selesai.

3.2. Tahap Penelitian

Berikut adalah tahapan penelitian yang dilakukan untuk pemblokiran dengan metode DNS Sinkhole menggunakan ESP32:

1. Pengumpulan Data

Sebelum menerapkan DNS sinkhole pada ESP32, diperlukan pengumpulan data awal untuk dapat menghitung performa dari DNS Sinkhole. Data yang dikumpulkan adalah jumlah iklan (visual), *router respon time* (ping router), *server respon time* (ping server), kecepatan *loading* halaman, dan ukuran size halaman.

2. Perancangan Sistem

Tahap selanjutnya adalah melakukan perancangan sistem DNS Sinkhole. Perancangan alur kerja ESP32 sebagai server DNS, dan juga perancangan analisis performa web sebelum dan sesudah menggunakan DNS Sinkhole.

3. Implementasi

Setelah merancang sistem, tahap selanjutnya adalah implementasi. Implementasi melibatkan pemrograman ESP32, mengatur jaringan lokal dan pembuatan aplikasi analisis performa web.

4. Pengujian

Setelah implementasi, akan dilakukan pengujian untuk mengevaluasi efektivitas DNS sinkhole dalam memblokir iklan pada jaringan Wi-Fi. Pada tahap ini data jumlah iklan (visual), *router respon time* (ping router),

server respon time (ping server), kecepatan *loading* halaman, dan ukuran size halaman akan di record pada saat menggunakan DNS Sinkhole.

5. Analisis Hasil

Pada tahap ini data sebelum dan sesudah menggunakan DNS Sinkhole akan di bandingkan dan di analisis lebih dalam mengenai efektifitas *adblocking* dan pengaruh DNS Sinkhole pada performa browsing.

3.3. Alat dan Bahan

Alat dan bahan yang digunakan dalam melakukan penelitian ini adalah:

3.3.1. ESP32

ESP32 digunakan sebagai perangkat utama dalam implementasi DNS sinkhole. Pengertian ESP32 sudah dijelaskan pada bab sebelumnya. ESP32 memiliki spesifikasi yang meliputi *prosesor dual core* yang beroperasi dengan instruksi Xtensa LX16, dapat dilihat pada tabel berikut:

Tabel 3. 1 Spesifikasi ESP32

No	Atribut	Detail
1	Tegangan	3.3 Volt
2	Prosesor	Tensilica L108 32 bit
3	Kecepatan Prosesor	Dual 160MHz
4	RAM	520K
5	GPIO	34
6	ADC	7
7	Dukungan 802.11	11b/g/n/e/i
8	Bluetooth	BLE (Bluetooth Low Energy)
9	SPI	3
10	I2C	2
11	UART	3

Berdasarkan spesifikasi yang ditampilkan pada tabel, mikrokontroler ESP32 muncul sebagai pilihan yang layak untuk digunakan dalam perangkat

demonstrasi *interface* mikrokontroler. Mikrokontroler ini dilengkapi dengan *interface* yang komprehensif dan juga fitur Wi-Fi yang terintegrasi, menjadikannya pilihan yang tepat untuk digunakan dalam perangkat demonstrasi atau pelatihan *Internet of Things*.

3.3.2. Router

Sebuah router adalah perangkat jaringan yang digunakan untuk menghubungkan beberapa jaringan komputer, seperti jaringan lokal (Local Area Network/LAN) dengan jaringan luas (Wide Area Network/WAN), seperti internet. Router berperan penting dalam menyediakan akses internet nirkabel kepada perangkat-perangkat yang terhubung.



Gambar 3. 1 Router

Sumber: <https://commons.wikimedia.org/>

Jaringan Wi-Fi digunakan sebagai lingkungan penelitian di mana akan mengimplementasikan sistem pemblokiran iklan menggunakan DNS Sinkhole. Artinya, perangkat ESP32 yang digunakan akan berfungsi sebagai titik akses Wi-Fi (Access Point) yang akan digunakan oleh perangkat lain untuk terhubung ke internet melalui jaringan Wi-Fi tersebut.

Dengan kata lain, jaringan Wi-Fi merupakan infrastruktur yang memungkinkan perangkat yang terhubung di dalam jaringan tersebut untuk saling berkomunikasi dan mengakses internet, dalam penelitian ini digunakan sebagai medium/media untuk mengimplementasikan dan menguji sistem pemblokiran

iklan menggunakan DNS Sinkhole. Untuk Router yang digunakan adalah merk Tenda N301.

3.3.3. Perangkat Keras (*Hardware*)

Perangkat keras (*hardware*) adalah komponen fisik yang berperan dalam menguji efektivitas pemblokiran iklan, melakukan pemrograman ESP32, menganalisis data, menampilkan hasil, serta menjalankan perintah yang telah diprogramkan. Perangkat keras yang digunakan adalah:

1. Laptop Lenovo
2. *Smartphone*
3. Esp32
4. Router

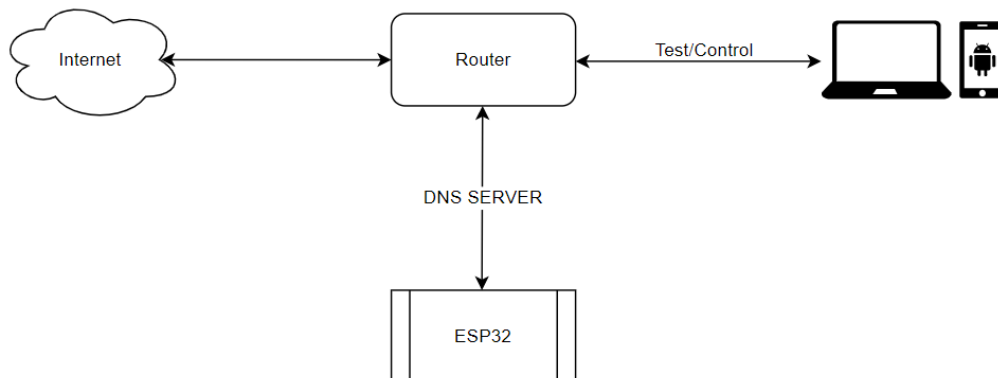
3.3.4 Perangkat lunak (*Software*)

Kebutuhan perangkat lunak (*software*) yang diperlukan dalam pembuatan penelitian ini adalah:

- | | |
|---|-------------------------|
| 1. Sistem Operasi | : Windows 10 Pro 64-bit |
| 2. Microsoft Office | : Word |
| 3. Editor | : Visual Studio Code |
| 4. Browser | : Google Chrome |
| 5. Perancangan dan design <i>User Interface</i> | : Draw io |
| 6. Bahasa Pemograman | : C++ dan JavaScript |

3.4. Perancangan Sistem

ESP32 dapat berfungsi sebagai DNS sinkhole. Untuk menjadikan esp32 agar berperan sebagai dns sinkhole, ip esp32 di daftarkan sebagai dns server pada settingan router. Dengan demikian, router akan mengarahkan permintaan DNS ke ESP32, memungkinkan server DNS lokal untuk memfilter dan memblokir iklan. Tindakan ini memastikan bahwa setiap perangkat yang terhubung ke jaringan Wi-Fi akan melewati ESP32 untuk permintaan DNS, menciptakan lapisan pertahanan yang efektif melawan iklan yang mengganggu. Ini merupakan langkah penting dalam mengimplementasikan solusi pemblokiran iklan dengan menggunakan ESP32 sebagai server DNS lokal pada jaringan Wi-Fi.



Gambar 3. 2 Skema Sistem

3.5. Implementasi

Realisasi dari rancangan implementasi lingkungan sistem sesuai dengan desain yang telah dibuat pada tahap perancangan, merupakan apa yang disebut sebagai implementasi lingkungan uji.

Implementasi DNS Sinkhole menggunakan ESP32 akan melibatkan beberapa tahapan, yaitu:

1. Persiapan Perangkat Keras: ESP32 akan disiapkan dengan menginstal perangkat lunak yang diperlukan dan mengkonfigurasi pengaturan yang relevan.
2. Persiapan *Blacklist*/daftar domain iklan: Daftar domain iklan yang ingin diblokir. Domain-domain ini akan diarahkan ke DNS Sinkhole.
3. Konfigurasi DNS Sinkhole: DNS Sinkhole akan dikonfigurasi untuk memblokir lalu lintas dari domain-domain yang terdaftar dalam daftar hitam.
4. Pengujian dan Evaluasi: Setelah DNS Sinkhole diimplementasikan, akan dilakukan pengujian untuk menentukan efektivitasnya dalam memblokir iklan. Evaluasi ini akan membantu dalam mengetahui apakah sistem ini dapat diimplementasikan dalam skala yang lebih besar.

DAFTAR PUSTAKA

- Apriyatna, M., & Zulfikar, A. F. (2023). Analisis dan Implementasi Network Ad-blocking Pi-Hole di Raspberry Pi 4 Menggunakan OPNSense DHCP Dengan Metode PPDIOO (Studi Kasus Diskominfo SP Kabupaten Lebak). In *OKTAL : Jurnal Ilmu Komputer dan Sains*(Vol. 2, Issue 02, pp. 575–582).
<https://journal.mediapublikasi.id/index.php/oktal/article/view/1036>
- Farikha, I. N., Hafidudin, H., & Ramadan, D. N. (2020). Prototype Detektor Bencana Tanah Longsor Menggunakan Accelerometer And Gyroscope Sensor Dengan Konsep Internet Of Things (iot). *EProceedings of Applied Science*, 6(2).
<https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/13481>
- IEEE Computer Society, & Institute of Electrical and Electronics Engineers. (n.d.). *ICISS 2015 : International Conference on Information Science and Security : 2015 in Seoul, Korea, December 14th-16th*.
- Jokić, A., & Šarac, M. (2022). *Cyber Security and Domain Name Systems Deploy and Protect Network With DNS Sinkhole Blackhole*. 421–426.
<https://doi.org/10.15308/sinteza-2022-421-426>
- Jung, S., Sabharwal, M., Jarauta, A., Sani, A. F., & Setiawan, M. A. (2020). DNS tunneling Detection Using Elasticsearch. *IOP Conference Series: Materials Science and Engineering*, 722(1), 012064.
<https://doi.org/10.1088/1757-899X/722/1/012064>