V1-Implementasi-Orange-Pi-Sebagai-DNS-Filtering-Untuk-Menangkal-Situs-Terlarang-10

by JASA CEK PLAGIASI WHATSAPP: 085935293540

Submission date: 23-Nov-2025 12:00PM (UTC+0200)

Submission ID: 2818041690

File name: V1-Implementasi-Orange-Pi-Sebagai-DNS-Filtering-Untuk-Menangkal-Situs-Terlarang-10.docx (1.01M)

Word count: 2844

Character count: 18036

Implementasi Orange Pi Sebagai DNS Filtering Untuk Menangkal Situs Terlarang

Yoga Mahendra Putra*[1], Azmuri Wahyu Azinar[2], Arif Senja Fitrani[3]
[1,2,3]Universitas Muhammadiyah Sidoarjo
e-mail: ***[1]yogamahendraputra3@gmail.com**, [2]azmuri@umsida.ac.id, [3]asfjim@umsida.ac.id

Abstrak

Pemanfaatan internet yang semakin luas menghadirkan tantangan serius dalam penyaringan konten negatif, khususnya pada jaringan RT/RW Net yang belum memiliki sistem keamanan memadai. Penelitian ini bertujuan mengembangkan sistem *DNS filtering* berbasis perangkat *Orange Pi Zero 3* untuk menangkal akses ke situs terlarang seperti pornografi, perjudian, dan konten SARA. Metode penelitian menggunakan *Secure Policy Development Life Cycle* (SPDLC) yang mencakup lima tahap: *analysis, design, implementation, enforcement, dan enhancement*. Perangkat *Orange Pi* dikonfigurasi dengan sistem operasi ringan *DietPi* serta aplikasi *Pi-hole* sebagai *DNS sinkhole* untuk memblokir *domain* dalam daftar *blacklist*. Hasil implementasi menunjukkan sistem mampu menghambat akses ke situs terlarang dengan tingkat keberhasilan 100%, dimana kategori pornografi, judi online, SARA, dan *phishing/malware* berhasil diblokir. Sistem juga dilengkapi pembaruan otomatis daftar blokir serta filter untuk menghindari duplikasi dengan daftar nasional. Solusi ini terbukti efektif, ringan dan dapat diterapkan pada jaringan lokal skala kecil hingga menengah dalam mendukung kebijakan internet sehat pemerintah.

Kata kunci— DNS Filtering, Orange Pi, Pihole, Situs Terlarang, SPDLC

Abstract

The increasingly widespread use of the internet poses serious challenges in filtering negative content, especially on RT/RW Net networks that do not yet have adequate security systems. This study aims to develop a DNS filtering system based on the Orange Pi Zero 3 device to block access to prohibited sites such as pornography, gambling, and SARA content. The research method uses the Secure Policy Development Life Cycle (SPDLC), which includes five stages: analysis, design, implementation, enforcement, and enhancement. The Orange Pi device is configured with the lightweight DietPi operating system and the Pi-hole application as a DNS sinkhole to block domains on the blacklist. The implementation results show that the system is capable of blocking access to prohibited sites with a 100% success rate, where the categories of pornography, online gambling, SARA, and phishing/malware were successfully blocked. The system is also equipped with automatic updates to the block list and filters to avoid duplication with the national list. This solution has proven to be effective, lightweight, and widely applicable to small to medium-sized local networks in supporting the government's healthy internet policy.

Keywords— DNS Filtering, Orange Pi, Pihole, Restricted Sites, SPDLC

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa dampak signifikan dalam kehidupan masyarakat, termasuk dalam bidang pendidikan, bisnis, hingga hiburan. Akses internet yang semakin luas memberikan kemudahan dalam memperoleh informasi dan meningkatkan produktivitas. Namun, di balik berbagai keuntungan tersebut, kemudahan akses ini juga menghadirkan tantangan besar, khususnya dalam hal keamanan siber dan perlindungan pengguna dari konten negatif[1], [2]. Paparan terhadap konten berbahaya seperti pornografi, perjudian, penipuan, serta konten

yang mengandung unsur SARA (suku, agama, ras, dan antargolongan) kini dapat terjadi dengan sangat mudah, termasuk pada kalangan anak-anak dan remaja[3], [4]. Hal ini menjadi perhatian serius, terutama di lingkungan jaringan lokal seperti RT/RW Net, di mana akses *internet* sering kali digunakan bersama oleh berbagai kalangan usia dan tanpa pengawasan yang memadai.

Pemerintah melalui Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif, menetapkan bahwa penyelenggara layanan internet wajib melakukan pemblokiran terhadap situs-situs yang memuat konten negatif. Peraturan ini bertujuan untuk menciptakan ekosistem *internet* yang sehat dan aman, serta mendorong penyelenggara jaringan untuk turut serta dalam melindungi masyarakat dari dampak buruk konten berbahaya[5], [6].

Permasalahan yang muncul adalah banyak jaringan RT/RW Net belum memiliki mekanisme penyaringan konten yang sesuai dengan ketentuan tersebut. Akses ke situs-situs negatif masih terbuka lebar, sehingga meningkatkan risiko terhadap penyalahgunaan internet serta paparan informasi yang tidak layak.

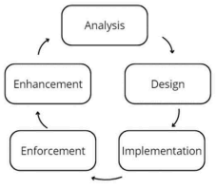
Salah satu metode yang efektif dan ekonomis untuk menyaring konten negatif adalah melalui teknologi *DNS filtering*. Teknologi ini bekerja pada level *Domain Name System (DNS)* dengan cara mengarahkan atau memblokir permintaan ke situs-situs yang telah masuk dalam daftar blokir[7]. Ketika pengguna mencoba mengakses situs yang termasuk dalam kategori bermuatan negatif, *DNS filter* akan mencegah akses tersebut, sehingga situs tidak dapat ditampilkan.

Untuk mendukung implementasi *DNS filtering* di lingkungan RT/RW Net, perangkat seperti *Orange Pi* dapat dimanfaatkan. *Orange Pi* adalah *mini-PC* berbasis *ARM* yang hemat daya dan biaya[8], [9], namun cukup kuat untuk menjalankan aplikasi jaringan seperti *Pi-hole*. *Pi-hole* sendiri adalah perangkat lunak *DNS sinkhole open-source* yang dapat digunakan untuk memblokir situs berdasarkan daftar blokir yang dapat dikustomisasi sesuai kebutuhan[10], [11].

Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem DNS filtering berbasis perangkat Orange Pi dan aplikasi Pi-hole guna memblokir akses ke situs terlarang pada jaringan RT/RW Net.

2. METODE PENELITIAN

Penelitian ini bertujuan untuk merancang dan mengembangkan sistem pemblokiran akses ke situs terlarang menggunakan perangkat Orange Pi, dengan menerapkan metode *Secure Policy Development Life Cycle* (SPDLC) yang mencakup tahap *analysis, design, implementation, enforcement,* dan *enhancement[12]-[14]*. Proses penelitian yang dilakukan diilustrasikan dalam urutan pada Gambar 1.



Gambar 1 Metode penelitian

2.1 *Analysis*

Pada tahap *Analysis*, dilakukan proses identifikasi secara mendalam terhadap kebutuhan *hardware* dan *software*. Tahap ini bertujuan untuk memahami kondisi lingkungan jaringan dan sistem yang akan digunakan dalam penerapan sistem pemblokiran situs terlarang menggunakan Orange Pi.

a. Tabel Kebutuhan Hardware

Detail kebutuhan hardware dapat dilihat pada Tabel 1 kebutuhan hardware berikut.

Tabel 1. Kebutuhan Hardware

No	*Hardware*	Spesifikasi	Sistem Operasi
1	Orange PI Zero 3	Allwinner H618 Quad-Core Cortex-A53, RAM 2 GB	DietPi
2	Laptop	Processor	Windows

		I7 Gen 9	11
3	Micro SD Card	32 GB	
4	Power Adaptor	5V/3A	
5	Kabel Ethernet		

b. Tabel Kebutuhan Software

Detail kebutuhan software dapat dilihat pada Tabel 2 kebutuhan hardware berikut.

Tabel 2. Kebutuhan Software

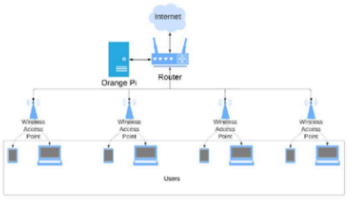
Operating System			
No	Nama	Versi	Keterangan
1	DietPi	9.8	Sistem operasi untuk Orange Pi
Software			
No	Nama	Versi	Keterangan
1	Balena Etcher	1.19.25	Aplikasi untuk *flash* sistem operasi DietPi
2	Pi-hole	5.18.3	Aplikasi *open source DNS filtering*
3	Putty	0.81.0.0	Aplikasi *remote server* (CLI)

2.2 *Design*

Pada tahap ini, peneliti merancang topologi jaringan serta *flowchart* yang menjelaskan cara kerja sistem. Rancangan ini bertujuan untuk memvisualisasikan pengaturan jaringan dan alur proses sistem.

a. Desain Topologi Jaringan

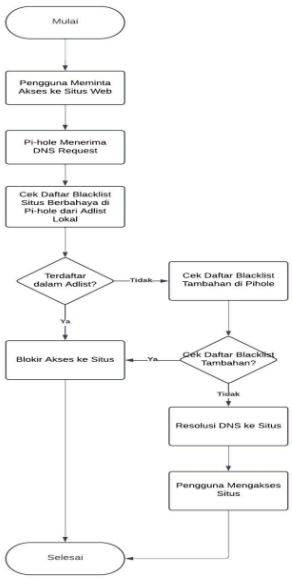
Desain Topologi jaringan yang digunakan dalam penelitian ini terdiri dari Orange Pi sebagai DNS *server* yang terhubung ke *router*. Gambar 2 memperlihatkan desain topologi jaringan.



Gambar 2 Topologi jaringan

b. *Flowchart*

Flowchart ini menggambarkan alur kerja mekanisme pemblokiran situs terlarang menggunakan Pi-hole. Proses dimulai ketika pengguna meminta akses ke suatu situs *web*. Pi-hole kemudian menerima permintaan *DNS* dan memeriksa domain yang diminta pada daftar *blacklist* baik dari *adlist* lokal maupun daftar tambahan. Jika domain ditemukan dalam daftar tersebut, akses ke situs akan diblokir. Namun, jika tidak ditemukan, Pi-hole akan meneruskan permintaan *DNS*, sehingga pengguna dapat mengakses situs tersebut. *Flowchart* dapat dilihat pada Gambar 3.



Gambar 3 Flowchart pemblokiran situs terlarang

2.3 *Implementation*

Tahap *implementation* melibatkan penerapan sistem di lingkungan jaringan menggunakan Orange Pi. Proses ini mencakup:

a. *Flashing image* DietPi ke dalam penyimpanan *microSD card.*
b. Melakukan instalasi Dietpi pada orange pi zero 3.

c. Instalasi dan konfigurasi Pi-hole untuk pemblokiran situs terlarang.

2.4 *Enforcement*

Pada tahap ini, sistem yang telah dibuat diuji untuk menilai seberapa efektif kemampuannya dalam memblokir akses ke situs terlarang. Pengujian ini dilakukan dengan cara mengakses berbagai situs yang terdaftar sebagai situs terlarang dan memantau hasil pemblokirannya.

2.5 *Enhancement*

Tahap terakhir dalam metode SPDLC adalah evaluasi dan peningkatan sistem berdasarkan hasil pengujian yang telah dilakukan. langkah yang akan diambil pada tahap ini adalah evaluasi efektivitas sistem dalam memblokir situs berbahaya berdasarkan data yang dikumpulkan selama tahap enforcement.

3. HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan sebuah sistem pemfilteran DNS berbasis Orange Pi yang berfungsi untuk memblokir akses ke situs-situs terlarang dalam jaringan RT/RW Net. Sistem ini memanfaatkan perangkat mini-PC Orange Pi Zero 3 yang telah dipasang sistem operasi ringan DietPi, serta aplikasi Pi-hole sebagai *DNS sinkhole*. Dengan konfigurasi yang tepat, sistem berhasil mengintervensi permintaan DNS dari klien dan mencegah akses ke domain yang masuk dalam daftar *blacklist.*

3.1 Implementasi Sistem *DNS Filtering*

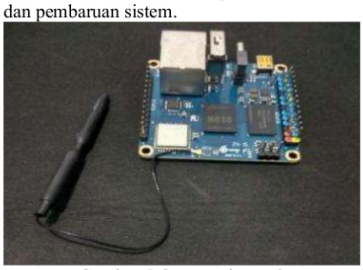
Tahap implementasi dimulai dengan *flashing image* DietPi ke dalam microSD dan pemasangan sistem operasi pada Orange Pi. Setelah itu, Pi-hole diinstal dan dikonfigurasi melalui akses SSH menggunakan aplikasi PuTTY.

a. Instalasi Sistem Operasi DietPi

Langkah awal dalam implementasi adalah instalasi sistem operasi DietPi ke dalam perangkat Orange Pi. File image DietPi diflash ke microSD menggunakan aplikasi Balena Etcher seperti pada Gambar 4.

Gambar 4 Flashing DietPi

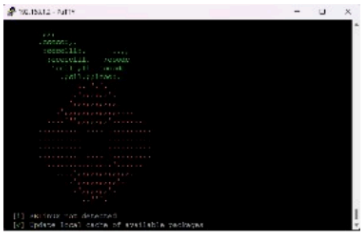
Setelah *flashing* berhasil, microSD dimasukkan ke Orange Pi dan perangkat dinyalakan seperti pada Gambar 5. DietPi secara otomatis memulai proses inisialisasi dan pembaruan sistem.



Gambar 5 Orange pi zero 3

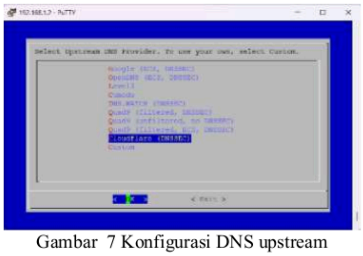
b. Instalasi Pi-hole

Setelah sistem DietPi aktif, Orange Pi dikonfigurasi melalui koneksi SSH menggunakan aplikasi PuTTY seperti pada Gambar 6. Dari terminal SSH, dilakukan pemasangan Pi-hole.



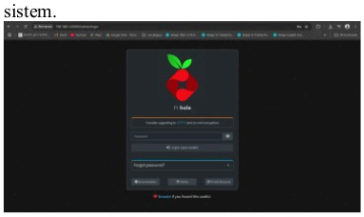
Gambar 6 Penginstalan pihole

Proses ini mencakup pemilihan interface jaringan, konfigurasi DNS upstream, serta aktivasi antarmuka admin berbasis web dilakukan seperti Gambar 7.



Gambar 7 Konfigurasi DNS upstream

Setelah instalasi dan konfigurasi awal selesai, pengguna dapat mengakses dashboard Pi-hole seperti pada Gambar 8 melalui browser dengan login ke halaman utama sistem.



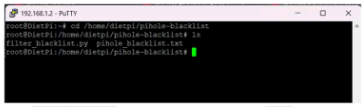
Gambar 8 Halaman login web pihole

Gambar 9 menunjukkan tampilan *dashboard* Pi-hole yang menampilkan statistik permintaan DNS, jumlah domain yang diblokir, serta persentase pemblokiran. Melalui halaman ini, pengguna dapat memantau aktivitas jaringan dan efektivitas pemblokiran situs secara *real-time*.

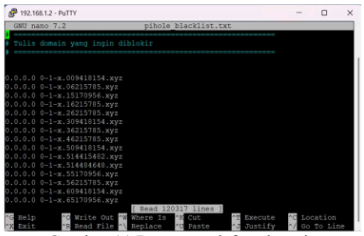
Gambar 9 Tampilan halaman utama web pihole

c. Konfigurasi Pi-hole dan Integrasi dengan Jaringan

Setelah Pi-hole terpasang, dibuat file daftar domain (*blocklist*) yang akan digunakan dalam proses *filtering*. Pembuatan file daftar domain ditunjukkan pada Gambar 10 dan Gambar 11.

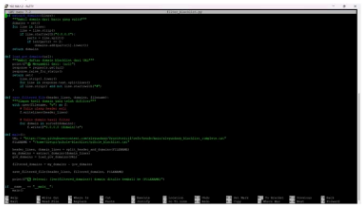


Gambar 10 File daftar domain dan filter



Gambar 11 Potongan daftar domain

Agar daftar domain yang digunakan tidak menyalin entri yang sudah diblokir oleh pemerintah, dibuat sebuah skrip *Python* untuk memfilter domain sehingga hanya domain yang belum tercantum dalam daftar resmi pemerintah yang akan dimasukkan ke dalam daftar blokir Pi-hole dilakukan seperti Gambar 12.



Gambar 12 Potongan kode filter_blacklist.py

Selanjutnya dibuat file adlist.sh seperti Gambar 13 yang berfungsi mengaktifkan daftar domain dan filter yang telah dibuat.

Gambar 13 Tampilan file adlist.sh

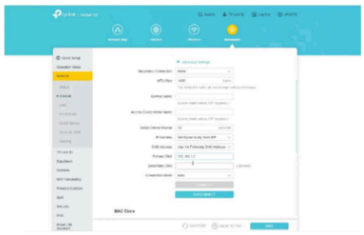
Untuk mengetahui seberapa besar cakupan sistem pemblokiran, dilakukan klasifikasi

terhadap seluruh domain yang dimasukkan dalam daftar blokir. Kategori dan jumlah domain yang diblokir dijabarkan pada Tabel 3 berikut ini:

Tabel 3 Kategori dan Jumlah Domain Yang Diblokir

No	Kategori Konten	Jumlah Domain
1	Pornografi	38.406
2	Perjudian	30.176
3	Phishing & Malware	52.121
4	SARA	16.459
	Total	137.162

Selain itu, dilakukan integrasi sistem dengan jaringan RT/RW Net melalui pengaturan *DNS* pada *router* utama seperti pada Gambar 14. DNS server default diubah ke alamat IP Orange Pi, sehingga semua permintaan *DNS* klien diarahkan ke sistem *Pi-hole*.



Gambar 14 Konfigurasi DNS router

3.2 Pengujian Sistem Filtering

Pengujian sistem filtering dilakukan dengan mengakses lima situs uji pada masing-masing, yaitu pornografi, judi online, SARA, dan phishing/malware. Pemilihan situs uji didasarkan pada daftar domain yang telah dimasukkan ke dalam adlist Pi-hole dan diuji dalam kondisi sebelum dan sesudah menggunakan sistem filtering. Berikut adalah hasil pengujiannya:

a. Pengujian pemblokiran ditunjukkan pada Tabel 4.

Tabel 4. Pengujian Pemblokiran pada Situs Pornografi.

No	**Nama Situs**	**Kategori**	**Tanpa Pi-hole**	**Dengan Pi-hole**	**Status**
1	javdesu.tv	Pornografi	Dapat diakses	Diblokir	Berhasil
2	doujindesu.tv	Pornografi	Dapat diakses	Diblokir	Berhasil
3	igodesu.tv	Pornografi	Dapat diakses	Diblokir	Berhasil
4	missav.ws	Pornografi	Dapat diakses	Diblokir	Berhasil
5	hanime.tv	Pornografi	Dapat diakses	Diblokir	Berhasil
6	melbet.ng	Judi Online	Dapat diakses	Diblokir	Berhasil
7	bj88.ph	Judi Online	Dapat diakses	Diblokir	Berhasil
8	bc.game	Judi Online	Dapat diakses	Diblokir	Berhasil
9	bunga99bet.net	Judi Online	Dapat diakses	Diblokir	Berhasil
10	bk8.world	Judi Online	Dapat diakses	Diblokir	Berhasil
11	buif163.com	Phishing/Malware	Dapat diakses	Diblokir	Berhasil
12	moneycsgo.net	Phishing/Malware	Dapat diakses	Diblokir	Berhasil
13	hellcase.com	Phishing/Malware	Dapat diakses	Diblokir	Berhasil
14	hubchallenge.net	Phishing/Malware	Dapat diakses	Diblokir	Berhasil

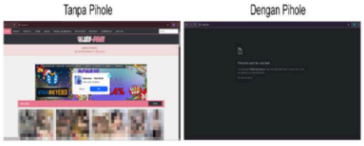
15	rabby.at	Phishing/Malware	Dapat diakses	Diblokir	Berhasil
16	stormfront.org	SARA	Dapat diakses	Diblokir	Berhasil
17	indosarang.com	SARA	Dapat diakses	Diblokir	Berhasil
18	8kun.top	SARA	Dapat diakses	Diblokir	Berhasil
19	4chan.org	SARA	Dapat diakses	Diblokir	Berhasil
20	dailystormer.in	SARA	Dapat diakses	Diblokir	Berhasil

b. Rekapitulasi hasil pengujian pemblokiran situs dengan Pi-hole ditunjukkan pada Tabel 5.

Tabel 5. Rekapitulasi Hasil Pengujian Sistem Filtering.

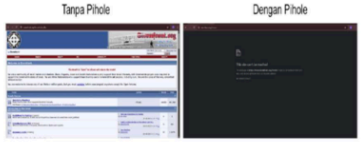
Kategori	Jumlah Situs Diuji	Terblokir	Tidak Terblokir	Persentase Keberhasilan
Pornografi	5	5	0	100%
Judi Online	5	5	0	100%
SARA / Konten Negatif	5	5	0	100%
Phishing/Malware	5	5	0	100%
Total	**20**	**20**	**0**	**100%**

Berdasarkan Tabel 9, Pi-hole menunjukkan performa sangat baik dengan tingkat keberhasilan 100% pada kategori pornografi, judi online, SARA, dan *phishing/malware*. Hasil pengujian tersebut dapat dilihat pada gambar 15 hingga gambar 18 yang menunjukkan hasil perbandingan akses terhadap berbagai jenis situs sebelum dan sesudah menggunakan Pi-hole. Setelah penerapan Pi-hole, situs dengan konten pornografi, judi, SARA, dan *phishing/malware* berhasil diblokir dan tidak dapat diakses.

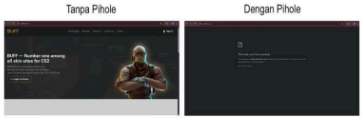


Gambar 15 Perbandingan akses situs pornografi sebelum dan sesudah menggunakan Pi-hole.

Gambar 16 Perbandingan akses situs judi sebelum dan sesudah menggunakan Pi-hole.



Gambar 17 Perbandingan akses situs SARA sebelum dan sesudah menggunakan Pi-hole.

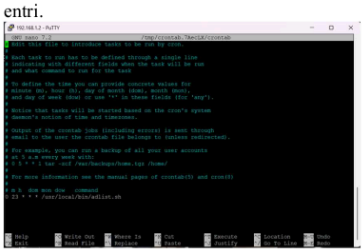


Gambar 18 Perbandingan akses situs phishing sebelum dan sesudah menggunakan Pi-hole.

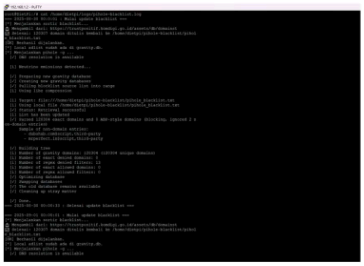
3.3 Evaluasi dan Peningkatan Sistem

Hasil pengujian menunjukkan bahwa sistem *DNS filtering* berbasis *Orange Pi Zero 3* dan *Pi-hole* mampu memblokir situs terlarang dengan tingkat keberhasilan 100%, di mana kategori pornografi, judi online, SARA, dan *phishing/malware*. Untuk menjaga kinerja jangka panjang, pembaruan adlist dijalankan otomatis melalui cronjob setiap

pukul 00.00 WIB yang ditunjukkan pada Gambar 19, sehingga sistem selalu menggunakan daftar terbaru dan cepat beradaptasi terhadap domain berbahaya yang muncul. Selain itu, proses log filter otomatis ditunjukkan pada Gambar 20, yang berfungsi untuk mengecualikan domain dari daftar blokir resmi pemerintah agar terhindar dari duplikasi entri.



Gambar 19 konfigurasi cronjob



Gambar 20 log filter dan pembaruan adlist otomatis

4. KESIMPULAN

Berdasarkan hasil analisis, sistem DNS filtering berbasis Orange Pi Zero 3 dengan DietPi dan Pi-hole terbukti berhasil bekerja dengan sangat efektif, dengan tingkat keberhasilan 100% dalam memblokir situs-situs terlarang pada jaringan RT/RW Net. Namun, pengujian juga menemukan adanya keterbatasan pada mekanisme blacklist, di mana beberapa situs yang tercantum dalam daftar blokir resmi pemerintah masih dapat diakses. Temuan ini mengindikasikan bahwa meskipun sistem mampu menangkal sebagian besar situs berbahaya, keandalan daftar blokir yang digunakan masih perlu ditingkatkan.

Secara keseluruhan, implementasi sistem ini efisien untuk penyaringan konten negatif pada jaringan lokal skala kecil hingga menengah. Kelemahan yang ditemukan pada daftar blokir resmi pemerintah menjadi masukan penting untuk penelitian lanjutan, sehingga pengembangan sistem DNS filtering ke depan dapat semakin akurat, responsif, dan selaras dengan kebijakan internet sehat yang ditetapkan pemerintah.

5. SARAN

Untuk penelitian selanjutnya, perlu dikembangkan metode sinkronisasi dan verifikasi yang lebih akurat terhadap daftar blokir resmi pemerintah, sehingga situs yang seharusnya diblokir tidak lagi dapat diakses. Dengan demikian, sistem akan menjadi lebih adaptif, akurat, dan mampu memberikan perlindungan maksimal terhadap konten berbahaya.

DAFTAR PUSTAKA

[1] A. Si Marhamah *Et Al.*, “Masalah Perubahan Sosial Dan Komunikasi Massa.”

[2] S. P. Br.Sinulingga And M. I. P. Nasution, “Analysis Of Challenges And Opportunities In The Development Of Information And Communication Technology In The Digital Era: Future Perspective,” *Jurnal Ilmiah Ekonomi Dan Manajemen*, Vol. 2, No. 12, Pp. 25–35, Dec. 2024, Doi: 10.61722/Jiem.V2i12.3018.

[3] S. Jauhariatul Masruroh And A. Wardatun, “Regulasi Hukum Dalam Menangani Konten Digital Negatif (Tidak Mendidik) Dan Dampaknya Terhadap Anak Ditinjau Dari Perspektif Maqasid Syari’ah,” 2025.

[4] Ervina Anatasya, Linda Cibya Rahmawati, And Yusuf Tri Herlambang, “Peran Orang Tua Dalam Pengawasan Penggunaan Teknologi Digital Pada Anak,” *Jurnal Sadewa : Publikasi Ilmu Pendidikan, Pembelajaran Dan Ilmu Sosial*, Vol. 2, No. 1, Pp. 301–314, Jan. 2024, Doi: 10.61132/Sadewa.V2i1.531.

[5] Y. Kurniawan, T. Siregar, And S. Hidayani, "Penegakan Hukum Oleh Polri Terhadap Pelaku Tindak Pidana Judi Online (Studi Pada Kepolisian Daerah Sumatera Utara)," *Arbiter: Jurnal Ilmiah Magister Hukum*, Vol. 4, No. 1, Pp. 28–44, Jun. 2022, Doi: 10.31289/Arbiter.V4i1.1203.

[6] V. Alhakim, S. Dewi, And A. Rompis, "Pembentukan Lembaga Independen Dalam Pengawasan Konten Digital: Studi Komparasi Hukum Antara Indonesia Dengan Australia," *Comserva : Jurnal Penelitian Dan Pengabdian Masyarakat*, Vol. 3, No. 09, Pp. 3627–3643, Jan. 2024, Doi: 10.59141/Comserva.V3i09.1150.

[7] H. Mizuardy, B. Yusuf Program Studi Pendidikan Teknologi Informasi Fakultas Tarbiyah Dan Ilmu Keguruan, And U. Ar-Raniry Banda Aceh - Indonesia, "Dns Filtering: A Clean And Positive Internet Environment In Uin Ar-Raniry Banda Aceh," 2018.

[8] W. Setiady, A. Agung, And D. Setyawan, "Rancang Bangun Orange Pi 3 Lts Sebagai Server Untuk Tablet Pendant Dengan Menggunakan Node-Red," Online, 2022.

[9] D. I. Mulyana, F. Ardiyansyah, N. Hidayat, And A. Zulfikar, "Optimasi Keamanan Jaringan Wifi Dari Situs Judi Online Dan Pornografi Dengan Dns Filtering Dan Orangepi," *Malcom: Indonesian Journal Of Machine Learning And Computer Science*, Vol. 4, No. 2, Pp. 647–655, Mar. 2024, Doi: 10.57152/Malcom.V4i2.1274.

[10] M. Rahman, "Implementasi Web Content Filtering Pada Jaringan Rt/Rw Net Menggunakan Pi-Hole Dns Server."

[11] O. Abdurahman And T. Umi Kalsum, "Penerapan Pi Hole Dns Server Sebagai Ads-Blocker Dan Sistem Filtering Website Pada Jaringan Hotspot," *Jurnal Media Infotama*, Vol. 18, No. 2, P. 341139, 2022.

[12] D. Yuliandari, W. Walim, B. K. Raja, R. Ningsih, And A. J. Wahidin, "Simulasi Penerapan Sistem Monitoring Jaringan Snort Nids Pada Web Server Menggunakan Metode Spdlc," *Jurnal Infortech*, Vol. 5, No. 2, Pp. 133–138, Dec. 2023, Doi: 10.31294/Infortech.V5i2.17338.

[13] A. Fergina, A. N. Ikhsan, And Z. Alamsyah, "Penggunaan Snort Sebagai Sistem Pendeteksi Serangan Pada Jaringan Menggunakan Notifikasi Telegram (Kasus Dinas Komunikasi Informatika Dan Persandian Kabupaten Sukabumi)," 2024.

[14] I. P. Y. Agus Ariwanta, K. Y. Ernanda Aryanto, And I. G. A. Gunadi, "Suricata Accuracy Optimization Based On Live Analysis Using One-Class Support Vector Machine Method And Streamlit Framework," *Jurnal Teknik Informatika (Jutif)*, Vol. 5, No. 2, Pp. 415–427, Apr. 2024, Doi: 10.52436/1.Jutif.2024.5.2.1822.

V1-Implementasi-Orange-Pi-Sebagai-DNS-Filtering-Untuk-Menangkal-Situs-Terlarang-10

ORIGINALITY REPORT

12%	11%	7%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Sebelas Maret Student Paper	3%
2	jurnal.darmajaya.ac.id Internet Source	1%
3	Riska Kurniyanto Abdullah, Muhammad Thariq Fudhail, Syamsul Mujahidin. "Penggunaan Snort dan Fail2ban sebagai IDS untuk Mengatasi Brute Force Attack dengan Notifikasi Telegram: Studi Kasus pada Institusi XYZ", Jurnal Sistem dan Teknologi Informasi (JustIN), 2024 Publication	1%
4	123dok.com Internet Source	1%
5	id.scribd.com Internet Source	1%
6	Hadian Mandala Putra, Irgi Bayu Delta, 'Alimuddin 'Alimuddin, Ida Wahidah, Suhartini Suhartini. "Rancang Bangun Sistem Pendeteksi Kebakaran Dan Pemantauan Oven Tembakau Berbasis Internet of Things", Jurnal PRINTER: Jurnal Pengembangan Rekayasa Informatika dan Komputer, 2025 Publication	1%
7	Fernando Fernando, Untoro Apsiswanto, Febri Sugandi. "SISTEM INFORMASI DAN	<1%

	IMPLEMENTASI SISTEM PELAYANAN PASIEN PADA KLINIK GIGI AHENG", Jurnal Mahasiswa Ilmu Komputer, 2024 Publication	
8	Submitted to Purdue University Student Paper	<1 %
9	ejurnal.its.ac.id Internet Source	<1 %
10	Rahma Monika, Mustika Mustika, Pujianto Pujianto. "RANCANG BANGUN SISTEM INFORMASI PERSEDIAAN BARANG BERBASIS DESKTOP PADA PT METRO SURYA INOVASI", Jurnal Mahasiswa Sistem Informasi (JMSI), 2023 Publication	<1 %
11	eprints.mdp.ac.id Internet Source	<1 %
12	eprints.ums.ac.id Internet Source	<1 %
13	blog.heylaw.id Internet Source	<1 %
14	core.ac.uk Internet Source	<1 %
15	ojs.uajy.ac.id Internet Source	<1 %
16	repository.upi.edu Internet Source	<1 %
17	eprints.umsida.ac.id Internet Source	<1 %
18	jurnal.fmipa.unila.ac.id Internet Source	<1 %
	www.scilit.net	

19	Internet Source	<1%
20	www.slideshare.net Internet Source	<1%
21	zh.scribd.com Internet Source	<1%
22	Dewi Yuliandari, Walim Walim, Bangkit Kharisma Raja, Rahayu Ningsih, Ahmad Jurnaidi Wahidin. "Simulasi Penerapan Sistem Monitoring Jaringan Snort NIDS Pada Web Server Menggunakan Metode SPDLC", Jurnal Infortech, 2023 Publication	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		